



## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		106.160.138.40	5800\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		111.103.215.210	PPTP - Point-to-Point Tunneling Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.212	BOOTP - Client
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.214	5800\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.229	Finger
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.242	End Point Mapper
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		112.26.27.203	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		104.83.105.39	111\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		113.215.126.48	HTTP - Hypertext Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.241	GNUTELLA Service
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		111.103.27.70	SSH - Secure Shell
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.108	5500\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.204	HTTPS - Secure HTTP
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.219	X Window System
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		111.142.55.119	DNS - Domain Name System
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		111.36.131.245	End Point Mapper
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.104	IMAP - Internet Message Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		117.180.12.105	Microsoft Directory Services
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.108	End Point Mapper
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.206	BOOTP - Client
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		107.75.39.135	Microsoft Directory Services
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		118.29.166.228	Microsoft Directory Services
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.216	NNTP - Network News Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.221	DNS - Domain Name System
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.234	BOOTP - Server
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Compromise		110.56.252.33	POP3 - Post Office Protocol Version 3
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Compromise		88.69.1.236	AIM - AOL Instant Messenger
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		109.117.125.53	119\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		109.5.43.42	End Point Mapper
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		118.190.70.171	Microsoft Directory Services
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		120.138.126.247	UPS - Uninterruptible Power Supply
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		120.204.177.106	End Point Mapper
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.222	HTTPS - Secure HTTP
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		105.96.101.134	End Point Mapper
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		115.191.101.229	TELNET
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.200	MSSQL - SQL Server Database
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.218	DNS - Domain Name System
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.225	MSSQL - SQL Server Database
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		103.199.117.191	Microsoft Directory Services
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		115.23.161.181	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.119	NetBIOS - Datagram
03/26/08 08:00 AM	03/28/08 06:00 AM	2.00	General Reconnaissance		108.103.69.15	SSH - Secure Shell
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Compromise		101.136.167.138	MSSQL - SQL Server Monitor
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		110.105.176.46	NetBIOS - Session Service
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		113.159.109.25	IBM Lotus Notes/Domino RPC
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		117.21.49.172	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.223	HTTP - Hypertext Transfer Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.229	111\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Compromise		88.69.1.223	AIM - AOL Instant Messenger
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		101.88.139.234	WLM/MSM - Windows Live Messenger
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		104.151.242.62	End Point Mapper
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		106.71.210.209	End Point Mapper
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		114.229.222.106	110\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		115.71.91.110	NetBIOS - Name Service
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		116.97.118.31	GNUTELLA Service

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		119.31.164.89	Syslog - System Logging Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.213	FTP Command
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.231	MySQL Database System
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.237	PPTP - Point-to-Point Tunneling Protocol
03/26/08 10:00 AM	03/27/08 07:00 PM	2.00	General Reconnaissance		88.69.1.242	Microsoft Directory Services
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		102.27.84.33	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		103.242.202.177	BOOTP - Client
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		106.12.75.97	NetBIOS - Name Service
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		114.183.253.86	MSSQL - SQL Server Monitor
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.112	HTTPS - Secure HTTP
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.220	MySQL Database System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.234	Microsoft Directory Services
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		107.180.80.203	MySQL Database System
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		115.23.161.181	Finger
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		116.97.118.31	LDAP - Lightweight Directory Access Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.212	MySQL Database System
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.233	End Point Mapper
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.251	HTTP - Hypertext Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		104.83.105.39	UPS - Uninterruptible Power Supply
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		113.95.99.218	Microsoft Directory Services
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		119.29.250.161	Microsoft Directory Services
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.229	End Point Mapper
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Compromise		112.26.27.203	NetBIOS - Datagram
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		120.204.177.106	End Point Mapper
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		72.99.11.117	111\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.224	PPTP - Point-to-Point Tunneling Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		101.138.232.109	FTP Command

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		103.242.202.177	119\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		110.91.38.179	DNS - Domain Name System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		115.111.20.104	IMAP - Internet Message Access Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.103	PPTP - Point-to-Point Tunneling Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.213	110\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.245	End Point Mapper
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		118.15.241.93	PPTP - Point-to-Point Tunneling Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		66.2.30.5	Microsoft Directory Services
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.103	BOOTP - Server
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.211	8080\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.214	8080\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.221	NetBIOS - Session Service
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.233	MySQL Database System
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.242	MySQL Database System
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		72.99.11.110	HTTP - Hypertext Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		88.69.1.214	NetBIOS - Datagram
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		105.96.101.72	119\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		106.178.103.206	119\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		107.180.80.203	119\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		116.96.74.233	Kazaa
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		66.2.30.8	TFTP - Trivial File Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.214	MSSQL - SQL Server Monitor
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.227	79\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.244	LDAP - Lightweight Directory Access Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.252	TFTP - Trivial File Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		106.87.12.123	UPS - Uninterruptible Power Supply
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		88.69.1.250	MSSQL - SQL Server Database

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		105.114.60.223	HTTP - Hypertext Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		107.180.80.203	X Window System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.102	HTTP - Hypertext Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.112	PPTP - Point-to-Point Tunneling Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.220	DNS - Domain Name System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.236	BOOTP - Server
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		106.41.42.164	NetBIOS - Name Service
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		109.105.181.83	NetBIOS - Session Service
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		112.26.27.203	WLM/MSM - Windows Live Messenger
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		115.135.147.74	NNTP - Network News Transfer Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		115.23.161.181	Microsoft Directory Services
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		118.66.66.46	End Point Mapper
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		118.95.82.196	MySQL Database System
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		107.240.248.102	Microsoft Directory Services
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		113.198.41.205	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		118.95.82.196	NetBIOS - Datagram
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		119.29.250.161	NetBIOS - Session Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		66.2.30.2	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.238	End Point Mapper
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		107.25.150.43	119\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		109.117.125.53	HTTPS - Secure HTTP
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		110.173.225.94	TFTP - Trivial File Transfer Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		116.76.60.122	5800\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Compromise		116.13.132.192	IMAP - Internet Message Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		106.71.210.209	UPS - Uninterruptible Power Supply
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		107.25.150.43	HTTPS - Secure HTTP

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		110.105.176.46	POP3 - Post Office Protocol Version 3
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		111.103.215.210	111\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		66.2.30.1	HTTP - Hypertext Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		66.2.30.4	Microsoft Directory Services
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.111	NetBIOS - Session Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.237	IBM Lotus Notes/Domino RPC
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		106.160.138.40	End Point Mapper
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		113.53.48.148	End Point Mapper
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		118.95.82.196	NetBIOS - Name Service
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		119.157.88.38	Kazaa
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.117	POP3 - Post Office Protocol Version 3
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		88.69.1.226	MSSQL - SQL Server Database
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		105.241.215.112	WLM/MSM - Windows Live Messenger
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		106.178.103.206	POP3 - Post Office Protocol Version 3
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		108.103.69.15	NetBIOS - Datagram
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		105.248.16.99	NetBIOS - Session Service
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.225	Syslog - System Logging Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.237	Syslog - System Logging Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		66.2.30.6	X Window System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		101.138.232.109	111\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		102.27.84.33	MSSQL - SQL Server Database
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		109.117.125.53	MSSQL - SQL Server Database
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		116.97.118.31	5500\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		117.21.49.172	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		118.190.70.171	MySQL Database System

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.114	LDAP - Lightweight Directory Access Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.217	POP3 - Post Office Protocol Version 3
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.225	DNS - Domain Name System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.243	AIM - AOL Instant Messenger
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		110.91.38.179	Syslog - System Logging Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		117.180.12.105	BOOTP - Client
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		66.2.30.2	NNTP - Network News Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		66.2.30.4	DNS - Domain Name System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		103.44.13.181	Microsoft Directory Services
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		119.29.250.161	IMAP - Internet Message Access Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.223	111\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.251	110\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		105.148.92.222	SMTP - Simple Mail Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		118.19.112.193	HTTP - Hypertext Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.221	NNTP - Network News Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.229	MySQL Database System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		111.142.55.119	DNS - Domain Name System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		101.138.232.109	Microsoft Directory Services
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		108.103.69.15	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		107.1.188.213	GNUTELLA Service
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		110.76.158.164	NNTP - Network News Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.108	BOOTP - Client
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Compromise		88.69.1.208	111\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		102.116.230.67	Kazaa
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		110.76.158.164	TFTP - Trivial File Transfer Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		113.95.99.218	HTTPS - Secure HTTP

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		117.21.49.172	Kazaa
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		120.138.126.247	5500\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.204	LDAP - Lightweight Directory Access Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.206	IMAP - Internet Message Access Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		103.47.20.110	5500\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		107.180.80.203	Kazaa
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		112.229.146.63	IBM Lotus Notes/Domino RPC
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.200	Syslog - System Logging Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.205	AIM - AOL Instant Messenger
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		107.25.150.43	5800\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		109.105.181.83	111\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		110.40.57.83	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		117.180.12.105	111\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		107.1.188.213	HTTP - Hypertext Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		112.176.232.212	BOOTP - Server
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		115.111.20.104	NetBIOS - Name Service
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		117.180.12.105	NetBIOS - Datagram
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		66.2.30.8	MSSQL - SQL Server Database
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.203	POP3 - Post Office Protocol Version 3
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.218	Syslog - System Logging Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.228	IBM Lotus Notes/Domino RPC
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.232	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		66.2.30.5	Microsoft Directory Services
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		66.2.30.8	Finger
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.239	79\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.253	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Compromise		107.75.39.135	HTTPS - Secure HTTP
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		115.111.20.104	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		120.138.126.247	MSSQL - SQL Server Monitor
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		120.204.177.106	TELNET
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		72.99.11.110	POP3 - Post Office Protocol Version 3
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Compromise		72.99.11.117	MSSQL - SQL Server Database
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		102.116.230.67	TFTP - Trivial File Transfer Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.101	IBM Lotus Notes/Domino RPC
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.116	119\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.206	BOOTP - Server
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.228	111\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.228	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		119.84.138.21	Microsoft Directory Services
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		103.253.172.4	UPS - Uninterruptible Power Supply
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		112.26.27.203	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		114.229.222.106	FTP Command
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		66.2.30.4	111\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		66.2.30.9	End Point Mapper
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.114	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.118	MSSQL - SQL Server Monitor
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.248	DNS - Domain Name System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		114.248.62.136	119\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		119.31.164.89	GNUTELLA Service
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.212	DNS - Domain Name System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		105.241.215.112	8080\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		106.23.8.82	WLM/MMS - Windows Live Messenger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		110.40.57.83	111\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		112.26.27.203	Microsoft Directory Services
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		118.66.66.46	BOOTP - Client
03/27/08 05:00 PM	03/28/08 12:00 AM	2.00	General Reconnaissance		88.69.1.207	79\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Compromise		88.69.1.249	HTTPS - Secure HTTP
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		105.219.149.191	79\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		106.23.8.82	AIM - AOL Instant Messenger
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		117.180.12.105	Kazaa
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		103.47.20.110	IBM Lotus Notes/Domino
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		109.129.58.157	RPC
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		66.2.30.5	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.102	111\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.211	GNUTELLA Service
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Compromise		107.1.188.213	IMAP - Internet Message Access Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Compromise		115.71.91.110	NetBIOS - Datagram
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Compromise		119.166.129.99	BOOTP - Server
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Compromise		88.69.1.235	DNS - Domain Name System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		105.248.16.99	MySQL Database System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		106.12.75.97	111\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		118.19.112.193	MySQL Database System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.207	MSSQL - SQL Server
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.218	Monitor
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		105.96.101.72	NetBIOS - Name Service
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		72.99.11.103	POP3 - Post Office Protocol Version 3
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		72.99.11.106	DNS - Domain Name System
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.201	MSSQL - SQL Server Database
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		106.12.75.97	GNUTELLA Service
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		72.99.11.117	End Point Mapper

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		88.69.1.249	HTTP - Hypertext Transfer Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		112.229.146.63	GNUTELLA-RTR
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.223	MySQL Database System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		103.253.172.4	IBM Lotus Notes/Domino RPC
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		112.236.131.84	Microsoft Directory Services
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		113.159.109.25	BOOTP - Server
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		114.183.253.86	LDAP - Lightweight Directory Access Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		115.23.161.181	NetBIOS - Name Service
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.200	DNS - Domain Name System
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		103.44.13.181	TELNET
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		104.83.105.39	119\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		106.87.12.123	DNS - Domain Name System
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		114.17.192.178	TFTP - Trivial File Transfer Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		115.111.20.104	End Point Mapper
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		116.96.74.233	SSH - Secure Shell
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.223	5800\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.246	MySQL Database System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		113.159.109.25	End Point Mapper
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		118.95.82.196	End Point Mapper
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		106.178.103.206	End Point Mapper
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		112.231.167.112	Finger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		118.29.166.228	POP3 - Post Office Protocol Version 3
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		72.99.11.109	MySQL Database System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		72.99.11.118	IBM Lotus Notes/Domino RPC
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.249	NetBIOS - Name Service
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		103.199.117.191	GNUTELLA-RTR
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		110.40.57.83	UPS - Uninterruptible Power Supply
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		111.103.27.70	HTTP - Hypertext Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		120.204.177.106	111\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		103.242.202.177	End Point Mapper
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		103.44.13.181	NNTP - Network News Transfer Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		111.103.27.70	110\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.245	LDAP - Lightweight Directory Access Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Compromise		88.69.1.238	DNS - Domain Name System
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		118.200.95.244	Kazaa
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.230	TFTP - Trivial File Transfer Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		105.248.16.99	HTTPS - Secure HTTP
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		115.191.101.229	NNTP - Network News Transfer Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.210	TFTP - Trivial File Transfer Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.210	UPS - Uninterruptible Power Supply
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Compromise		105.243.17.16	Finger
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		107.75.39.135	119\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		115.111.20.104	5800\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.110	PPTP - Point-to-Point Tunneling Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.233	DNS - Domain Name System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		116.13.132.192	MySQL Database System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		119.29.250.161	5800\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		119.84.138.21	MySQL Database System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.118	GNUTELLA-RTR
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		107.1.188.213	SMTP - Simple Mail Transfer Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		107.240.248.102	NetBIOS - Datagram
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		108.124.40.121	TELNET
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		110.40.57.83	SSH - Secure Shell
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		118.19.112.193	79\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.206	PPTP - Point-to-Point Tunneling Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		119.84.138.21	UPS - Uninterruptible Power Supply
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		120.138.126.247	IMAP - Internet Message Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.1</b>						
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.222	111\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		88.69.1.219	HTTPS - Secure HTTP
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		109.138.207.137	79\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		66.2.30.9	GNUTELLA Service
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		72.99.11.110	8080\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.239	End Point Mapper
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Compromise		88.69.1.239	IMAP - Internet Message Access Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.209	8080\
<b>161.200.1.10</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		88.69.1.241	GNUTELLA-RTR
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		110.40.57.83	PPTP - Point-to-Point Tunneling Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		117.21.49.172	NNTP - Network News Transfer Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		72.99.11.106	119\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		72.99.11.110	5800\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.239	FTP Command
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.248	HTTP - Hypertext Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		110.173.225.94	SMTP - Simple Mail Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.243	111\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		103.242.202.177	Syslog - System Logging Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		119.157.88.38	79\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		119.31.164.89	8080\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.109	Microsoft Directory Services
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.239	End Point Mapper
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.250	End Point Mapper
03/26/08 02:00 AM	03/26/08 09:00 PM	2.00	General Reconnaissance		111.36.131.245	Kazaa
03/26/08 02:00 AM	03/26/08 10:00 PM	2.00	General Reconnaissance		88.69.1.231	End Point Mapper
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		105.148.92.222	MSSQL - SQL Server Monitor
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.200	111\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.236	UPS - Uninterruptible Power Supply

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.237	5500\
03/26/08 03:00 AM	03/26/08 03:00 PM	2.00	General Reconnaissance		112.231.167.112	Microsoft Directory Services
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		115.23.161.181	IBM Lotus Notes/Domino RPC
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		118.95.82.196	SMTP - Simple Mail Transfer Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		119.31.164.89	X Window System
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.203	HTTPS - Secure HTTP
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.207	FTP Command
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.208	110\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.221	BOOTP - Client
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.234	MySQL Database System
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		103.199.117.191	IMAP - Internet Message Access Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		106.148.54.20	UPS - Uninterruptible Power Supply
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		106.71.210.209	5800\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		109.129.58.157	LDAP - Lightweight Directory Access Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		111.103.27.70	NetBIOS - Session Service
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		113.159.109.25	FTP Command
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		113.53.48.148	NNTP - Network News Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		120.138.126.247	MSSQL - SQL Server Database
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		72.99.11.107	NNTP - Network News Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		72.99.11.116	79\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		106.71.210.209	UPS - Uninterruptible Power Supply
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		110.49.174.190	X Window System
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		119.31.164.89	Microsoft Directory Services
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		66.2.30.3	111\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		72.99.11.115	Microsoft Directory Services
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.214	IMAP - Internet Message Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		101.138.232.109	Microsoft Directory Services
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.110	GNUTELLA-RTR
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.118	End Point Mapper
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.244	111\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		111.36.131.245	GNUTELLA-RTR
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		112.211.5.54	SSH - Secure Shell
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		118.29.166.228	X Window System
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.206	PPTP - Point-to-Point Tunneling Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.222	110\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.226	MySQL Database System
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		111.36.131.245	HTTP - Hypertext Transfer Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		116.13.132.192	110\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		66.2.30.3	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.107	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.204	110\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.204	UPS - Uninterruptible Power Supply
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Compromise		115.111.20.104	FTP Command
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		106.12.75.97	5500\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		109.129.58.157	SSH - Secure Shell
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		111.195.14.150	NetBIOS - Name Service
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		112.231.167.112	111\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.102	HTTPS - Secure HTTP
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.104	TELNET
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.118	PPTP - Point-to-Point Tunneling Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.213	5500\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Compromise		115.135.147.74	UPS - Uninterruptible Power Supply
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		103.199.117.191	119\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		104.83.105.39	FTP Command
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		106.71.210.209	5500\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		113.104.243.29	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		114.248.62.136	8080\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		118.95.82.196	Syslog - System Logging Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.116	DNS - Domain Name System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.225	DNS - Domain Name System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.243	8080\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Compromise		66.2.30.2	SMTP - Simple Mail Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		105.241.215.112	FTP Command
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		109.105.181.83	8080\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		109.117.125.53	Finger
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		110.105.176.46	110\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		110.40.57.83	DNS - Domain Name System
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		66.2.30.10	HTTP - Hypertext Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.203	Microsoft Directory Services
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.230	PPTP - Point-to-Point Tunneling Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		101.138.232.109	AIM - AOL Instant Messenger
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		101.138.232.109	BOOTP - Server
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		105.219.149.191	BOOTP - Server
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		105.219.149.191	DNS - Domain Name System
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		111.142.55.119	End Point Mapper
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		115.191.101.229	IMAP - Internet Message Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.103	SMTP - Simple Mail Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.202	8080\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.205	X Window System
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		109.5.43.42	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		116.97.118.31	End Point Mapper
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.215	111\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.224	Microsoft Directory Services
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.242	SMTP - Simple Mail Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		112.250.231.58	FTP Command
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		120.204.177.106	End Point Mapper
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		66.2.30.3	DNS - Domain Name System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.103	DNS - Domain Name System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.237	SMTP - Simple Mail Transfer Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Compromise		119.29.250.161	HTTPS - Secure HTTP
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		111.195.14.150	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		112.229.146.63	End Point Mapper
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		113.104.243.29	Kazaa
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		119.29.250.161	HTTPS - Secure HTTP
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		66.2.30.1	BOOTP - Client
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.112	DNS - Domain Name System
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.253	TFTP - Trivial File Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		103.242.202.177	IBM Lotus Notes/Domino RPC
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		106.148.54.20	LDAP - Lightweight Directory Access Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.209	PPTP - Point-to-Point Tunneling Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		104.151.242.62	NetBIOS - Session Service
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Compromise		88.69.1.231	79\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		112.211.5.54	IMAP - Internet Message Access Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		116.13.132.192	BOOTP - Client
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		119.29.250.161	X Window System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.241	POP3 - Post Office Protocol Version 3
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		106.87.12.123	GNUTELLA Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		107.75.39.135	5500\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		111.103.215.210	FTP Command
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		113.215.126.48	5800\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.209	79\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.222	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.239	BOOTP - Client

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Compromise		116.13.132.192	FTP Command
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Compromise		88.69.1.230	IMAP - Internet Message Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		107.25.150.43	IMAP - Internet Message Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		66.2.30.6	110\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.210	FTP Command
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.210	MSSQL - SQL Server Monitor
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.229	8080\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		109.129.58.157	SMTP - Simple Mail Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.205	LDAP - Lightweight Directory Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.214	Finger
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		105.114.60.223	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		110.195.212.97	110\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		114.248.62.136	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		119.84.138.21	IMAP - Internet Message Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.109	MySQL Database System
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.116	SMTP - Simple Mail Transfer Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.200	FTP Command
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.211	BOOTP - Client
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.214	AIM - AOL Instant Messenger
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.247	110\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		109.117.125.53	HTTP - Hypertext Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		113.95.99.218	FTP Command
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		114.17.192.178	GNUTELLA-RTR
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		115.135.147.74	HTTPS - Secure HTTP
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.217	MSSQL - SQL Server Monitor
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.227	End Point Mapper

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.236	AIM - AOL Instant Messenger
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.238	SMTP - Simple Mail Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.243	BOOTP - Client
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		88.69.1.213	PPTP - Point-to-Point Tunneling Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.119	Microsoft Directory Services
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.230	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.240	X Window System
03/27/08 01:00 AM	03/27/08 04:00 PM	2.00	General Reconnaissance		116.13.132.192	NetBIOS - Session Service
03/27/08 01:00 AM	03/27/08 09:00 PM	2.00	General Reconnaissance		72.99.11.103	GNUTELLA-RTR
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		105.241.215.112	NetBIOS - Session Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		107.180.80.203	SSH - Secure Shell
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		113.104.243.29	NNTP - Network News Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		113.95.99.218	5500\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		116.13.132.192	Microsoft Directory Services
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		120.138.126.247	BOOTP - Server
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		66.2.30.1	DNS - Domain Name System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.100	IMAP - Internet Message Access Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Compromise		72.99.11.117	BOOTP - Server
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		105.96.101.134	End Point Mapper
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		106.71.210.209	NetBIOS - Session Service
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.112	NNTP - Network News Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.253	UPS - Uninterruptible Power Supply
03/27/08 03:00 AM	03/28/08 12:00 AM	2.00	General Reconnaissance		113.104.243.29	X Window System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		102.116.230.67	PPTP - Point-to-Point Tunneling Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		105.96.101.134	TELNET
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		106.148.54.20	HTTP - Hypertext Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		111.103.215.210	Kazaa

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		113.215.126.48	BOOTP - Server
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.110	NNTP - Network News Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.215	Microsoft Directory Services
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.233	X Window System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		107.1.188.213	IMAP - Internet Message Access Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		116.13.132.192	5800\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		66.2.30.6	111\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.214	End Point Mapper
03/27/08 05:00 AM	03/28/08 07:00 AM	2.00	General Reconnaissance		109.5.43.42	Microsoft Directory Services
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		104.83.105.39	111\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		105.114.60.223	DNS - Domain Name System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		107.1.188.213	AIM - AOL Instant Messenger
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		109.117.125.53	TFTP - Trivial File Transfer Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		118.19.112.193	NetBIOS - Name Service
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		66.2.30.9	NetBIOS - Datagram
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.231	8080\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.245	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		109.138.207.137	NetBIOS - Session Service
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		110.40.57.83	79\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		115.135.147.74	MSSQL - SQL Server Monitor
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		118.95.82.196	Microsoft Directory Services
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		120.204.177.106	HTTP - Hypertext Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.112	Kazaa
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Compromise		109.105.181.83	IMAP - Internet Message Access Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		103.199.117.191	HTTPS - Secure HTTP
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		107.1.188.213	MSSQL - SQL Server Monitor
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		107.197.4.193	Kazaa
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		117.83.247.204	110\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Compromise		119.31.164.89	GNUTELLA-RTR
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		66.2.30.1	5800\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		66.2.30.3	Microsoft Directory Services
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		72.99.11.108	GNUTELLA Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.227	UPS - Uninterruptible Power Supply
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		105.148.92.222	MSSQL - SQL Server Database
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		110.49.174.190	FTP Command
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		110.91.38.179	IBM Lotus Notes/Domino RPC
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		112.211.5.54	LDAP - Lightweight Directory Access Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		119.25.113.70	IBM Lotus Notes/Domino RPC
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.101	HTTP - Hypertext Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.114	LDAP - Lightweight Directory Access Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.202	X Window System
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.232	Microsoft Directory Services
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		102.27.84.33	DNS - Domain Name System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		106.12.75.97	DNS - Domain Name System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		107.197.4.193	BOOTP - Client
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		116.97.118.31	Microsoft Directory Services
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		118.200.95.244	IBM Lotus Notes/Domino RPC
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.107	MySQL Database System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.117	End Point Mapper
03/27/08 11:00 AM	03/27/08 04:00 PM	2.00	General Reconnaissance		88.69.1.203	GNUTELLA Service
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		102.27.84.33	SMTP - Simple Mail Transfer Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		105.243.17.16	111\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		109.105.181.83	Finger
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		112.229.146.63	IMAP - Internet Message Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		119.157.88.38	TFTP - Trivial File Transfer Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		72.99.11.114	GNUTELLA-RTR
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.217	Finger
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.227	MySQL Database System
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.251	Finger
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Compromise		72.99.11.100	BOOTP - Server
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		106.87.12.123	IMAP - Internet Message Access Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		118.200.95.244	Microsoft Directory Services
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.5	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.210	Microsoft Directory Services
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.248	NetBIOS - Datagram
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Compromise		101.138.232.109	MSSQL - SQL Server Database
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		103.242.202.177	HTTPS - Secure HTTP
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		109.117.125.53	NetBIOS - Session Service
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		66.2.30.1	Microsoft Directory Services
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		66.2.30.2	UPS - Uninterruptible Power Supply
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		66.2.30.4	GNUTELLA-RTR
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		107.240.248.102	BOOTP - Client
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		111.103.27.70	Finger
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		115.135.147.74	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.107	110\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.218	NNTP - Network News Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.235	UPS - Uninterruptible Power Supply
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.243	BOOTP - Server
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		102.27.84.33	MSSQL - SQL Server Monitor
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		114.183.253.86	BOOTP - Client

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.215	Microsoft Directory Services
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.218	Finger
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.244	Finger
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Compromise		114.128.130.118	119\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.110	Microsoft Directory Services
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.246	110\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.246	TFTP - Trivial File Transfer Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Compromise		88.69.1.248	IMAP - Internet Message Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		103.253.172.4	LDAP - Lightweight Directory Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		105.114.60.223	Kazaa
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		106.41.42.164	PPTP - Point-to-Point Tunneling Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		107.1.188.213	PPTP - Point-to-Point Tunneling Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		109.105.181.83	DNS - Domain Name System
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		115.111.20.104	UPS - Uninterruptible Power Supply
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		118.95.82.196	AIM - AOL Instant Messenger
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		119.166.129.99	MSSQL - SQL Server Monitor
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		119.31.164.89	LDAP - Lightweight Directory Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		119.84.138.21	PPTP - Point-to-Point Tunneling Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		119.84.138.21	TFTP - Trivial File Transfer Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		66.2.30.10	110\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.200	NetBIOS - Name Service
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.215	End Point Mapper
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.218	WLM/MSM - Windows Live Messenger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		113.198.41.205	TFTP - Trivial File Transfer Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		106.87.12.123	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		112.236.131.84	Finger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		113.159.109.25	IBM Lotus Notes/Domino RPC
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		118.15.241.93	SMTP - Simple Mail Transfer Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		119.84.138.21	NetBIOS - Session Service
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		66.2.30.9	8080\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.107	MSSQL - SQL Server Monitor
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.230	X Window System
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.231	HTTPS - Secure HTTP
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.237	TELNET
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Compromise		88.69.1.252	BOOTP - Client
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		105.241.215.112	BOOTP - Client
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.220	MySQL Database System
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		88.69.1.231	AIM - AOL Instant Messenger
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		106.41.42.164	Syslog - System Logging Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		107.1.188.213	5800\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		120.204.177.106	GNUTELLA-RTR
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.216	POP3 - Post Office Protocol Version 3
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		110.49.174.190	Finger
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		113.53.48.148	UPS - Uninterruptible Power Supply
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.119	IBM Lotus Notes/Domino RPC
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		102.27.84.33	GNUTELLA Service
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		106.12.75.97	Kazaa
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		106.160.138.40	BOOTP - Server
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		115.71.91.110	FTP Command
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		66.2.30.3	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.202	110\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.204	LDAP - Lightweight Directory Access Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		102.116.230.67	79\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		112.250.231.58	5800\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.252	Microsoft Directory Services
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		101.88.139.234	Syslog - System Logging Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		104.151.242.62	FTP Command
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		114.248.62.136	MSSQL - SQL Server Database
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		119.29.250.161	IMAP - Internet Message Access Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.243	HTTP - Hypertext Transfer Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.243	IBM Lotus Notes/Domino RPC
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		101.88.139.234	MySQL Database System
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		105.241.215.112	MSSQL - SQL Server Monitor
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		118.19.112.193	TFTP - Trivial File Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		120.204.177.106	IBM Lotus Notes/Domino RPC
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.247	TELNET
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Compromise		115.135.147.74	UPS - Uninterruptible Power Supply
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Compromise		88.69.1.219	IMAP - Internet Message Access Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		101.88.139.234	NetBIOS - Session Service
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		106.23.8.82	POP3 - Post Office Protocol Version 3
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.216	BOOTP - Server
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.218	DNS - Domain Name System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.219	SMTP - Simple Mail Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		109.138.207.137	119\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		110.76.158.164	UPS - Uninterruptible Power Supply
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		118.19.112.193	BOOTP - Server
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		118.190.70.171	DNS - Domain Name System
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.117	NetBIOS - Name Service

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.210	NetBIOS - Session Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.221	PPTP - Point-to-Point Tunneling Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.232	HTTP - Hypertext Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.233	TELNET
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		106.12.75.97	PPTP - Point-to-Point Tunneling Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		112.211.5.54	IMAP - Internet Message Access Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		113.104.243.29	Syslog - System Logging Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		117.21.49.172	5500\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		105.114.60.223	SSH - Secure Shell
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.100	UPS - Uninterruptible Power Supply
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.106	8080\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.225	119\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.233	End Point Mapper
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Compromise		109.105.181.83	NetBIOS - Datagram
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		102.27.84.33	111\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		106.12.75.97	BOOTP - Client
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		106.148.54.20	PPTP - Point-to-Point Tunneling Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		111.36.131.245	79\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		114.183.253.86	LDAP - Lightweight Directory Access Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		114.183.253.86	NetBIOS - Name Service
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		119.31.164.89	111\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.203	BOOTP - Server
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.253	MySQL Database System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		101.110.102.70	MSSQL - SQL Server Database
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		102.27.84.33	119\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		109.5.43.42	110\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		111.103.27.70	5500\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		116.96.74.233	WLM/MSM - Windows Live Messenger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.10</b>						
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		119.84.138.21	8080\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.250	SMTP - Simple Mail Transfer Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		113.104.243.29	LDAP - Lightweight Directory Access Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		116.96.74.233	MSSQL - SQL Server Database
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.111	HTTP - Hypertext Transfer Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.239	119\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.239	End Point Mapper
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		118.19.112.193	TELNET
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		66.2.30.7	Kazaa
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		72.99.11.102	UPS - Uninterruptible Power Supply
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		72.99.11.120	GNUTELLA-RTR
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.201	TFTP - Trivial File Transfer Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.234	HTTPS - Secure HTTP
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.237	GNUTELLA-RTR
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		101.138.232.109	Microsoft Directory Services
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		106.41.42.164	LDAP - Lightweight Directory Access Protocol
<b>161.200.1.2</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		72.99.11.108	POP3 - Post Office Protocol Version 3
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		104.151.242.62	MSSQL - SQL Server Database
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		106.12.75.97	111\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		106.12.75.97	TELNET
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		114.248.62.136	UPS - Uninterruptible Power Supply
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		118.19.112.193	DNS - Domain Name System
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		72.99.11.111	DNS - Domain Name System
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.214	Finger
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.221	IMAP - Internet Message Access Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.226	111\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		103.199.117.191	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		103.44.13.181	TELNET
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		115.23.161.181	WLM/MSM - Windows Live Messenger
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		66.2.30.5	NNTP - Network News Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.102	Kazaa
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.105	WLM/MSM - Windows Live Messenger
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Compromise		115.111.20.104	HTTP - Hypertext Transfer Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		112.236.131.84	IBM Lotus Notes/Domino RPC
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.112	BOOTP - Server
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Compromise		72.99.11.117	FTP Command
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		108.103.69.15	Finger
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		66.2.30.1	SSH - Secure Shell
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.117	DNS - Domain Name System
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.200	NetBIOS - Session Service
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.219	IBM Lotus Notes/Domino RPC
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Compromise		115.135.147.74	HTTPS - Secure HTTP
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Compromise		88.69.1.243	110\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		105.241.215.112	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		106.148.54.20	IBM Lotus Notes/Domino RPC
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		111.103.215.210	NNTP - Network News Transfer Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		116.97.118.31	Finger
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.205	NetBIOS - Session Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.238	5500\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Compromise		110.76.158.164	NNTP - Network News Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		107.1.188.213	Finger
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.200	8080\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.250	5500\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		104.83.105.39	BOOTP - Server
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		106.160.138.40	DNS - Domain Name System
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		111.103.215.210	TELNET
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		111.195.14.150	SMTP - Simple Mail Transfer Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		118.19.112.193	X Window System
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		72.99.11.116	5500\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.211	Finger
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.230	LDAP - Lightweight Directory Access Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		103.47.20.110	IMAP - Internet Message Access Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		111.142.55.119	LDAP - Lightweight Directory Access Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		117.21.49.172	WLM/MMS - Windows Live Messenger
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		118.95.82.196	IBM Lotus Notes/Domino RPC
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.117	MSSQL - SQL Server Monitor
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.216	8080\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.232	DNS - Domain Name System
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.243	GNUTELLA-RTR
03/26/08 07:00 AM	03/27/08 03:00 PM	2.00	General Reconnaissance		111.103.215.210	IBM Lotus Notes/Domino RPC
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		101.88.139.234	BOOTP - Client
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		102.116.230.67	PPTP - Point-to-Point Tunneling Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		106.87.12.123	Microsoft Directory Services
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		112.229.146.63	BOOTP - Client
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		114.229.222.106	DNS - Domain Name System
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		119.29.250.161	79\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.209	End Point Mapper
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.245	111\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.105	MySQL Database System
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.118	5500\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.221	HTTP - Hypertext Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.250	End Point Mapper
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		114.128.130.118	MySQL Database System
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		117.21.49.172	BOOTP - Client
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.113	PPTP - Point-to-Point Tunneling Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.204	HTTP - Hypertext Transfer Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.212	HTTP - Hypertext Transfer Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.236	POP3 - Post Office Protocol Version 3
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		104.151.242.62	IMAP - Internet Message Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		118.95.82.196	PPTP - Point-to-Point Tunneling Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		103.47.20.110	BOOTP - Server
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		110.105.176.46	111\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		113.104.243.29	110\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		113.198.41.205	LDAP - Lightweight Directory Access Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.203	HTTP - Hypertext Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.229	Syslog - System Logging Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		103.44.13.181	5800\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		106.87.12.123	111\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		110.76.158.164	End Point Mapper
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		112.250.231.58	PPTP - Point-to-Point Tunneling Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		114.128.130.118	111\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		114.128.130.118	X Window System
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		115.23.161.181	Syslog - System Logging Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		116.13.132.192	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		118.29.166.228	110\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		119.157.88.38	NetBIOS - Name Service
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.115	LDAP - Lightweight Directory Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		106.71.210.209	TFTP - Trivial File Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		114.17.192.178	DNS - Domain Name System
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		118.95.82.196	GNUTELLA-RTR
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		119.84.138.21	NetBIOS - Name Service
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		72.99.11.120	BOOTP - Client
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.226	Microsoft Directory Services
03/26/08 02:00 PM	03/27/08 05:00 AM	2.00	General Reconnaissance		88.69.1.235	IMAP - Internet Message Access Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		103.47.20.110	SSH - Secure Shell
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		105.96.101.72	DNS - Domain Name System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		109.138.207.137	NetBIOS - Name Service
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		112.250.231.58	POP3 - Post Office Protocol Version 3
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		66.2.30.9	TELNET
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.109	110\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Compromise		118.29.166.228	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		110.56.252.33	BOOTP - Server
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.100	NetBIOS - Datagram
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.240	BOOTP - Server
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		66.2.30.10	5500\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		72.99.11.111	LDAP - Lightweight Directory Access Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.207	Microsoft Directory Services
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.233	119\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		110.105.176.46	MySQL Database System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		110.195.212.97	PPTP - Point-to-Point Tunneling Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.223	Microsoft Directory Services
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.223	X Window System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.231	GNUTELLA-RTR
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		102.27.84.33	5800\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		105.243.17.16	110\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		111.36.131.245	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		117.180.12.105	BOOTP - Client
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		66.2.30.4	TFTP - Trivial File Transfer Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		72.99.11.114	DNS - Domain Name System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		72.99.11.117	BOOTP - Client
03/26/08 07:00 PM	03/27/08 03:00 PM	2.00	General Reconnaissance		112.229.146.63	POP3 - Post Office Protocol Version 3
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		101.110.102.70	HTTP - Hypertext Transfer Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		106.148.54.20	PPTP - Point-to-Point Tunneling Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		106.41.42.164	NetBIOS - Datagram
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		109.105.181.83	AIM - AOL Instant Messenger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		116.96.74.233	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		66.2.30.3	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.228	Microsoft Directory Services
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.247	Finger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.251	FTP Command
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Compromise		109.117.125.53	111\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		105.243.17.16	TFTP - Trivial File Transfer Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		105.248.16.99	8080\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		113.53.48.148	AIM - AOL Instant Messenger
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		72.99.11.103	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.234	GNUTELLA Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Compromise		88.69.1.200	X Window System
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Compromise		88.69.1.246	UPS - Uninterruptible Power Supply
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		103.44.13.181	BOOTP - Server
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		105.241.215.112	DNS - Domain Name System
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		116.96.74.233	FTP Command
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		119.157.88.38	Finger
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		120.204.177.106	Kazaa

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.203	IMAP - Internet Message Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.250	111\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		113.53.48.148	DNS - Domain Name System
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		66.2.30.1	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		66.2.30.4	BOOTP - Server
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.105	Finger
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.208	AIM - AOL Instant Messenger
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.223	NetBIOS - Datagram
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		105.114.60.223	AIM - AOL Instant Messenger
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		109.138.207.137	DNS - Domain Name System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		112.176.232.212	5500\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.110	TFTP - Trivial File Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.114	111\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.210	BOOTP - Client
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.220	110\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.120	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.200	111\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.201	FTP Command
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.235	GNUTELLA Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		112.236.131.84	Microsoft Directory Services
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		111.103.27.70	AIM - AOL Instant Messenger
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		112.250.231.58	IBM Lotus Notes/Domino RPC
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		112.250.231.58	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		115.135.147.74	End Point Mapper
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		120.138.126.247	LDAP - Lightweight Directory Access Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.118	TELNET
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.239	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.243	Microsoft Directory Services
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		108.124.40.121	Microsoft Directory Services
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.116	HTTP - Hypertext Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.118	SMTP - Simple Mail Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		115.23.161.181	LDAP - Lightweight Directory Access Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		101.136.167.138	End Point Mapper
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		105.96.101.134	IMAP - Internet Message Access Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	2.00	General Reconnaissance		106.160.138.40	X Window System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		106.178.103.206	BOOTP - Client
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		107.180.80.203	SSH - Secure Shell
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		117.83.247.204	GNUTELLA Service
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		118.95.82.196	Microsoft Directory Services
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.231	MSSQL - SQL Server Monitor
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.246	WLM/MSM - Windows Live Messenger
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Compromise		105.96.101.134	111\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Compromise		111.195.14.150	GNUTELLA Service
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		102.27.84.33	Finger
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		107.180.80.203	End Point Mapper
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		109.138.207.137	MSSQL - SQL Server Database
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		119.135.23.192	IMAP - Internet Message Access Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.216	PPTP - Point-to-Point Tunneling Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		104.151.242.62	IBM Lotus Notes/Domino RPC
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		109.5.43.42	BOOTP - Client
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		88.69.1.214	111\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		66.2.30.7	110\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		72.99.11.106	110\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		72.99.11.111	IBM Lotus Notes/Domino RPC
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.206	FTP Command
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.242	TELNET
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		106.178.103.206	MySQL Database System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		110.91.38.179	UPS - Uninterruptible Power Supply
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		111.103.27.70	IBM Lotus Notes/Domino RPC
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		113.104.243.29	NetBIOS - Session Service
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		117.21.49.172	MySQL Database System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		66.2.30.1	TFTP - Trivial File Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		66.2.30.4	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		66.2.30.6	5500\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		66.2.30.8	MySQL Database System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.109	BOOTP - Client
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.226	MSSQL - SQL Server Monitor
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Compromise		120.204.177.106	TELNET
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		103.47.20.110	MySQL Database System
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		104.151.242.62	MSSQL - SQL Server Monitor
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		116.96.74.233	End Point Mapper
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		119.29.250.161	Microsoft Directory Services
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		72.99.11.103	HTTP - Hypertext Transfer Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.203	TFTP - Trivial File Transfer Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.211	DNS - Domain Name System
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.227	119\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.239	MSSQL - SQL Server Database
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.244	NetBIOS - Datagram
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.251	MySQL Database System
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		117.180.12.105	WLM/MSM - Windows Live Messenger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		72.99.11.120	NetBIOS - Name Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.212	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		113.104.243.29	POP3 - Post Office Protocol Version 3
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		66.2.30.6	UPS - Uninterruptible Power Supply
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.213	X Window System
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.227	HTTP - Hypertext Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		113.95.99.218	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		107.75.39.135	NNTP - Network News Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		110.76.158.164	5800\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		112.229.146.63	111\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		112.231.167.112	POP3 - Post Office Protocol Version 3
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		113.53.48.148	GNUTELLA-RTR
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		116.13.132.192	MySQL Database System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		120.138.126.247	110\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		66.2.30.4	PPTP - Point-to-Point Tunneling Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.210	End Point Mapper
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.249	119\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		110.49.174.190	8080\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		115.23.161.181	DNS - Domain Name System
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		116.96.74.233	BOOTP - Client
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		119.84.138.21	GNUTELLA Service
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.229	DNS - Domain Name System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		107.1.188.213	SMTP - Simple Mail Transfer Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		113.159.109.25	IMAP - Internet Message Access Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		116.97.118.31	NetBIOS - Datagram
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.241	Syslog - System Logging Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.246	SMTP - Simple Mail Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.247	111\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		109.5.43.42	BOOTP - Server
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		119.29.250.161	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.246	POP3 - Post Office Protocol Version 3
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		113.159.109.25	NNTP - Network News Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		119.29.250.161	NetBIOS - Datagram
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		66.2.30.5	MySQL Database System
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		101.110.102.70	GNUTELLA Service
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		115.71.91.110	TFTP - Trivial File Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.213	IMAP - Internet Message Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.232	LDAP - Lightweight Directory Access Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Compromise		107.25.150.43	End Point Mapper
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		106.148.54.20	NetBIOS - Datagram
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		110.105.176.46	X Window System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		118.190.70.171	Finger
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.228	79\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.238	110\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		106.71.210.209	End Point Mapper
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		109.5.43.42	Microsoft Directory Services
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		66.2.30.10	8080\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.107	Syslog - System Logging Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.117	WLM/MMS - Windows Live Messenger
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.241	MySQL Database System
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Compromise		107.75.39.135	AIM - AOL Instant Messenger
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Compromise		114.128.130.118	UPS - Uninterruptible Power Supply
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		102.27.84.33	LDAP - Lightweight Directory Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		105.114.60.223	119\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		105.114.60.223	HTTPS - Secure HTTP
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		106.41.42.164	Microsoft Directory Services
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		107.25.150.43	BOOTP - Client
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		120.204.177.106	111\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.216	End Point Mapper
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.216	Microsoft Directory Services
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.227	BOOTP - Server
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.236	SMTP - Simple Mail Transfer Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.251	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		105.248.16.99	NetBIOS - Datagram
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		112.176.232.212	110\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		112.229.146.63	End Point Mapper
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.112	SMTP - Simple Mail Transfer Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.243	WLM/MSM - Windows Live Messenger
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		101.136.167.138	NetBIOS - Session Service
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		105.248.16.99	PPTP - Point-to-Point Tunneling Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		106.148.54.20	MSSQL - SQL Server Monitor
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		112.176.232.212	NetBIOS - Datagram
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		72.99.11.115	UPS - Uninterruptible Power Supply
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		103.47.20.110	IBM Lotus Notes/Domino RPC
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		106.23.8.82	TELNET
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		113.159.109.25	MySQL Database System
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		72.99.11.105	BOOTP - Client
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.241	End Point Mapper
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.250	FTP Command
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		109.105.181.83	5500\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		115.135.147.74	IBM Lotus Notes/Domino RPC
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		119.157.88.38	5800\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		120.138.126.247	BOOTP - Server
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		66.2.30.7	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.111	79\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.112	NetBIOS - Datagram
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.217	DNS - Domain Name System
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.222	NetBIOS - Name Service
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Compromise		119.31.164.89	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		114.128.130.118	GNUTELLA-RTR
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		116.13.132.192	HTTPS - Secure HTTP
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		118.15.241.93	HTTPS - Secure HTTP
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		118.200.95.244	119\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		118.200.95.244	MySQL Database System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.219	HTTPS - Secure HTTP
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.242	HTTPS - Secure HTTP
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		66.2.30.10	TELNET
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		72.99.11.110	5500\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.206	DNS - Domain Name System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		110.91.38.179	MSSQL - SQL Server Monitor
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		112.211.5.54	MySQL Database System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.206	LDAP - Lightweight Directory Access Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.217	LDAP - Lightweight Directory Access Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.220	119\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.220	HTTP - Hypertext Transfer Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.238	BOOTP - Client
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.239	8080\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		104.83.105.39	5800\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		112.231.167.112	FTP Command
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.251	111\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		112.236.131.84	5800\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.223	Kazaa
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.224	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		105.148.92.222	BOOTP - Server
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		105.241.215.112	GNUTELLA-RTR
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		105.243.17.16	8080\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		108.124.40.121	119\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		110.173.225.94	UPS - Uninterruptible Power Supply
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		118.200.95.244	BOOTP - Client
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		66.2.30.2	IMAP - Internet Message Access Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.222	MSSQL - SQL Server Database
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.244	End Point Mapper
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.249	BOOTP - Server
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		101.110.102.70	IMAP - Internet Message Access Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.101	End Point Mapper
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.106	POP3 - Post Office Protocol Version 3
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		102.116.230.67	FTP Command
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		102.27.84.33	AIM - AOL Instant Messenger
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		106.87.12.123	HTTP - Hypertext Transfer Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		113.104.243.29	Microsoft Directory Services
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		66.2.30.3	TELNET
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.104	111\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.110	TELNET
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Compromise		113.95.99.218	UPS - Uninterruptible Power Supply
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		111.103.27.70	8080\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.207	TFTP - Trivial File Transfer Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.209	FTP Command
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.233	111\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Compromise		109.117.125.53	Microsoft Directory Services
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		103.242.202.177	5800\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		110.91.38.179	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.2</b>						
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		116.97.118.31	POP3 - Post Office Protocol Version 3
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.106	HTTPS - Secure HTTP
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.109	UPS - Uninterruptible Power Supply
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.204	Syslog - System Logging Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.241	79\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		106.87.12.123	AIM - AOL Instant Messenger
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		109.117.125.53	NNTP - Network News Transfer Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		66.2.30.5	End Point Mapper
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.110	MSSQL - SQL Server Monitor
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.237	POP3 - Post Office Protocol Version 3
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.252	AIM - AOL Instant Messenger
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		88.69.1.225	Microsoft Directory Services
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		105.148.92.222	FTP Command
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.226	BOOTP - Server
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.234	HTTPS - Secure HTTP
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Compromise		104.83.105.39	DNS - Domain Name System
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		105.248.16.99	WLM/MSM - Windows Live Messenger
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		114.128.130.118	5800\
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		72.99.11.105	119\
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.233	8080\
<b>161.200.1.3</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		72.99.11.103	MySQL Database System
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		101.88.139.234	POP3 - Post Office Protocol Version 3
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		114.128.130.118	HTTPS - Secure HTTP
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		118.29.166.228	NetBIOS - Session Service
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		120.138.126.247	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.213	MSSQL - SQL Server Monitor
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.228	NetBIOS - Datagram
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		109.129.58.157	79\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		114.17.192.178	UPS - Uninterruptible Power Supply
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		106.87.12.123	End Point Mapper
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		113.159.109.25	BOOTP - Server
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.104	GNUTELLA-RTR
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.204	UPS - Uninterruptible Power Supply
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.217	111\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		105.148.92.222	WLM/MSM - Windows Live Messenger
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		106.41.42.164	BOOTP - Server
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		116.96.74.233	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		119.135.23.192	GNUTELLA Service
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.210	BOOTP - Client
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.208	TELNET
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.209	79\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		105.96.101.72	End Point Mapper
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		109.105.181.83	Kazaa
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		115.23.161.181	111\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		117.21.49.172	111\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		119.84.138.21	PPTP - Point-to-Point Tunneling Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		120.138.126.247	WLM/MSM - Windows Live Messenger
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.111	POP3 - Post Office Protocol Version 3
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.112	NetBIOS - Datagram
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.219	IBM Lotus Notes/Domino RPC
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.235	110\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		106.12.75.97	MSSQL - SQL Server Monitor
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		106.41.42.164	TFTP - Trivial File Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		117.83.247.204	GNUTELLA Service
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		66.2.30.2	HTTP - Hypertext Transfer Protocol
03/26/08 05:00 AM	03/27/08 08:00 PM	2.00	General Reconnaissance		88.69.1.240	BOOTP - Server
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Compromise		110.40.57.83	Microsoft Directory Services
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.207	SMTP - Simple Mail Transfer Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		104.151.242.62	FTP Command
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		106.12.75.97	Kazaa
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		119.29.250.161	PPTP - Point-to-Point Tunneling Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		109.117.125.53	BOOTP - Server
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		114.128.130.118	DNS - Domain Name System
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		118.95.82.196	SSH - Secure Shell
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.221	NetBIOS - Datagram
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.233	POP3 - Post Office Protocol Version 3
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Compromise		88.69.1.206	DNS - Domain Name System
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		118.66.66.46	HTTP - Hypertext Transfer Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.106	8080\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.201	MySQL Database System
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.212	UPS - Uninterruptible Power Supply
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.226	GNUTELLA Service
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		104.83.105.39	MySQL Database System
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		114.248.62.136	PPTP - Point-to-Point Tunneling Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		118.66.66.46	BOOTP - Server
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		66.2.30.9	Microsoft Directory Services
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.210	Microsoft Directory Services
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.243	POP3 - Post Office Protocol Version 3
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		106.87.12.123	111\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		109.5.43.42	X Window System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		110.173.225.94	5800\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		119.135.23.192	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.103	Finger
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.105	DNS - Domain Name System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.105	IMAP - Internet Message Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.224	SMTP - Simple Mail Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.248	NetBIOS - Datagram
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		105.243.17.16	GNUTELLA Service
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		112.211.5.54	119\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		113.95.99.218	BOOTP - Server
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		66.2.30.10	PPTP - Point-to-Point Tunneling Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		72.99.11.104	111\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.224	5500\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		110.40.57.83	MSSQL - SQL Server Monitor
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		114.17.192.178	SSH - Secure Shell
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		115.111.20.104	111\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.109	NNTP - Network News Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.204	110\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.211	BOOTP - Server
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.234	SMTP - Simple Mail Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		106.160.138.40	NetBIOS - Datagram
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		116.76.60.122	DNS - Domain Name System
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		116.97.118.31	GNUTELLA-RTR
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		118.29.166.228	Kazaa
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		66.2.30.3	IBM Lotus Notes/Domino RPC
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Compromise		115.71.91.110	Syslog - System Logging Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		118.66.66.46	SMTP - Simple Mail Transfer Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		66.2.30.1	HTTP - Hypertext Transfer Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.102	BOOTP - Server

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.107	GNUTELLA Service
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Compromise		88.69.1.202	Syslog - System Logging Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		105.148.92.222	5500\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		105.148.92.222	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		106.12.75.97	111\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		109.105.181.83	NNTP - Network News Transfer Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.203	119\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		88.69.1.231	NNTP - Network News Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		114.183.253.86	NNTP - Network News Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		118.190.70.171	IBM Lotus Notes/Domino RPC
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		72.99.11.110	NetBIOS - Datagram
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		107.75.39.135	TFTP - Trivial File Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		103.47.20.110	FTP Command
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		111.103.27.70	POP3 - Post Office Protocol Version 3
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		115.135.147.74	TFTP - Trivial File Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		115.23.161.181	5500\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		66.2.30.2	End Point Mapper
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.103	IMAP - Internet Message Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.207	IMAP - Internet Message Access Protocol
03/26/08 06:00 PM	03/28/08 07:00 AM	2.00	General Reconnaissance		107.180.80.203	DNS - Domain Name System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Compromise		88.69.1.250	TFTP - Trivial File Transfer Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		103.242.202.177	IMAP - Internet Message Access Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		111.36.131.245	5500\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		112.211.5.54	8080\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.205	FTP Command
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.246	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		103.44.13.181	HTTP - Hypertext Transfer Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		108.124.40.121	AIM - AOL Instant Messenger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		110.49.174.190	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.104	NNTP - Network News Transfer Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.224	Syslog - System Logging Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.252	POP3 - Post Office Protocol Version 3
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Compromise		88.69.1.208	HTTP - Hypertext Transfer Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		119.157.88.38	End Point Mapper
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		72.99.11.103	GNUTELLA-RTR
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.207	110\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.218	BOOTP - Client
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.230	IMAP - Internet Message Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.240	DNS - Domain Name System
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		119.25.113.70	MSSQL - SQL Server Database
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		66.2.30.5	HTTP - Hypertext Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.107	WLM/MSM - Windows Live Messenger
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.112	NetBIOS - Session Service
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		103.253.172.4	5800\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		106.41.42.164	DNS - Domain Name System
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		109.117.125.53	TFTP - Trivial File Transfer Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		118.15.241.93	8080\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		66.2.30.7	DNS - Domain Name System
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.228	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		113.159.109.25	LDAP - Lightweight Directory Access Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		106.12.75.97	PPTP - Point-to-Point Tunneling Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		110.195.212.97	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		120.138.126.247	111\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.103	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.200	NetBIOS - Datagram
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		106.148.54.20	Microsoft Directory Services
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.100	DNS - Domain Name System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.228	119\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.234	5500\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		88.69.1.243	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		108.103.69.15	MSSQL - SQL Server Monitor
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		111.103.215.210	Syslog - System Logging Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		66.2.30.10	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.203	TELNET
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.218	HTTP - Hypertext Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.230	119\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.240	NetBIOS - Name Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.241	MySQL Database System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.243	Syslog - System Logging Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		104.83.105.39	GNUTELLA Service
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		105.241.215.112	GNUTELLA Service
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		106.12.75.97	MySQL Database System
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		109.129.58.157	NetBIOS - Datagram
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		112.26.27.203	End Point Mapper
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		114.183.253.86	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		116.96.74.233	TELNET
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		120.204.177.106	111\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.211	5800\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.206	UPS - Uninterruptible Power Supply
03/27/08 04:00 AM	03/27/08 04:00 PM	2.00	General Reconnaissance		110.56.252.33	NetBIOS - Name Service

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		103.47.20.110	DNS - Domain Name System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		110.105.176.46	NNTP - Network News Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		110.91.38.179	GNUTELLA Service
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		66.2.30.4	Microsoft Directory Services
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		66.2.30.7	TELNET
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		72.99.11.117	Microsoft Directory Services
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.231	GNUTELLA-RTR
03/27/08 05:00 AM	03/27/08 08:00 PM	2.00	General Reconnaissance		112.229.146.63	X Window System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		109.5.43.42	79\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		115.191.101.229	DNS - Domain Name System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Compromise		88.69.1.223	NNTP - Network News Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		103.242.202.177	MSSQL - SQL Server Monitor
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		106.71.210.209	Syslog - System Logging Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		107.1.188.213	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		111.103.27.70	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		112.211.5.54	BOOTP - Server
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		114.128.130.118	UPS - Uninterruptible Power Supply
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.120	GNUTELLA Service
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.120	X Window System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.218	SMTP - Simple Mail Transfer Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		104.83.105.39	AIM - AOL Instant Messenger
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		105.219.149.191	MSSQL - SQL Server Database
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		66.2.30.1	5500\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		66.2.30.7	MSSQL - SQL Server Monitor
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		72.99.11.100	MSSQL - SQL Server Database
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.234	DNS - Domain Name System
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.249	GNUTELLA-RTR

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.252	DNS - Domain Name System
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Compromise		106.41.42.164	UPS - Uninterruptible Power Supply
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		106.12.75.97	TELNET
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		113.104.243.29	NetBIOS - Name Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		118.29.166.228	110\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		66.2.30.3	End Point Mapper
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		102.27.84.33	119\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		103.242.202.177	Microsoft Directory Services
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		110.49.174.190	5800\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		119.31.164.89	NetBIOS - Datagram
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.102	Kazaa
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.216	NetBIOS - Datagram
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.230	NetBIOS - Datagram
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.237	DNS - Domain Name System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		109.138.207.137	Kazaa
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		119.135.23.192	HTTPS - Secure HTTP
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		119.25.113.70	8080\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		66.2.30.5	79\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.206	SSH - Secure Shell
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.225	DNS - Domain Name System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.232	5800\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.233	5500\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.249	AIM - AOL Instant Messenger
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		103.47.20.110	HTTPS - Secure HTTP
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		106.87.12.123	End Point Mapper
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		110.40.57.83	HTTPS - Secure HTTP
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		111.36.131.245	NetBIOS - Datagram
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		119.135.23.192	Syslog - System Logging Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.247	TFTP - Trivial File Transfer Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		107.197.4.193	110\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		119.135.23.192	Finger
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.200	5500\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.204	HTTPS - Secure HTTP
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.213	AIM - AOL Instant Messenger
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.217	DNS - Domain Name System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.224	IBM Lotus Notes/Domino RPC
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.227	BOOTP - Client
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.248	Syslog - System Logging Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		103.44.13.181	110\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		111.142.55.119	SSH - Secure Shell
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.250	MSSQL - SQL Server Monitor
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.252	IBM Lotus Notes/Domino RPC
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		110.173.225.94	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		112.231.167.112	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		113.53.48.148	GNUTELLA Service
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.104	HTTP - Hypertext Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.202	DNS - Domain Name System
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.223	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.232	MySQL Database System
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.243	NetBIOS - Session Service
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.250	IMAP - Internet Message Access Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		105.148.92.222	Finger
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		110.105.176.46	8080\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.216	LDAP - Lightweight Directory Access Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.226	POP3 - Post Office Protocol Version 3
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		112.250.231.58	5800\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		66.2.30.1	BOOTP - Client
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.112	TELNET

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.253	WLM/MSM - Windows Live Messenger
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		110.76.158.164	BOOTP - Client
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		114.248.62.136	GNUTELLA-RTR
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		115.23.161.181	DNS - Domain Name System
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.242	End Point Mapper
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		105.241.215.112	LDAP - Lightweight Directory Access Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		114.128.130.118	IMAP - Internet Message Access Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		119.84.138.21	HTTP - Hypertext Transfer Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		66.2.30.1	NetBIOS - Session Service
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.204	119\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.207	FTP Command
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		103.242.202.177	SMTP - Simple Mail Transfer Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		113.215.126.48	FTP Command
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		113.53.48.148	DNS - Domain Name System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		72.99.11.112	BOOTP - Client
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		116.76.60.122	119\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.236	TFTP - Trivial File Transfer Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		105.219.149.191	PPTP - Point-to-Point Tunneling Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		112.250.231.58	WLM/MSM - Windows Live Messenger
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		113.159.109.25	UPS - Uninterruptible Power Supply
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.112	119\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.209	Microsoft Directory Services
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		116.97.118.31	IBM Lotus Notes/Domino RPC
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		103.44.13.181	DNS - Domain Name System
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		112.250.231.58	110\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		113.215.126.48	TELNET
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		119.157.88.38	BOOTP - Client
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		66.2.30.3	BOOTP - Server

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		88.69.1.213	UPS - Uninterruptible Power Supply
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		106.12.75.97	TFTP - Trivial File Transfer Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		110.173.225.94	DNS - Domain Name System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		113.53.48.148	TFTP - Trivial File Transfer Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		113.95.99.218	111\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		114.183.253.86	SSH - Secure Shell
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		72.99.11.101	WLM/MSM - Windows Live Messenger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.208	LDAP - Lightweight Directory Access Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.227	110\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		105.243.17.16	LDAP - Lightweight Directory Access Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		110.195.212.97	111\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		110.49.174.190	LDAP - Lightweight Directory Access Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		110.91.38.179	8080\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		103.47.20.110	111\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		107.240.248.102	5800\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		111.195.14.150	End Point Mapper
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		112.211.5.54	MySQL Database System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		114.248.62.136	BOOTP - Client
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		116.76.60.122	NetBIOS - Session Service
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		120.138.126.247	UPS - Uninterruptible Power Supply
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		66.2.30.10	NetBIOS - Name Service
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		66.2.30.8	UPS - Uninterruptible Power Supply
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		72.99.11.108	IMAP - Internet Message Access Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Compromise		88.69.1.219	DNS - Domain Name System
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		106.148.54.20	79\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		114.248.62.136	SMTP - Simple Mail Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		117.180.12.105	PPTP - Point-to-Point Tunneling Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		119.157.88.38	Finger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		120.204.177.106	HTTPS - Secure HTTP
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.112	TFTP - Trivial File Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.220	FTP Command
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.247	SSH - Secure Shell
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.248	MSSQL - SQL Server Database
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		72.99.11.101	UPS - Uninterruptible Power Supply
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		117.83.247.204	5500\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		66.2.30.7	BOOTP - Server
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.212	WLM/MSM - Windows Live Messenger
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.232	TFTP - Trivial File Transfer Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		104.151.242.62	HTTP - Hypertext Transfer Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		109.105.181.83	DNS - Domain Name System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		66.2.30.7	GNUTELLA Service
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.206	MySQL Database System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		101.88.139.234	FTP Command
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		66.2.30.1	WLM/MSM - Windows Live Messenger
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.100	NetBIOS - Session Service
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.211	TFTP - Trivial File Transfer Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.244	MSSQL - SQL Server Database
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		102.116.230.67	MySQL Database System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		107.180.80.203	8080\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		115.111.20.104	Microsoft Directory Services
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		115.111.20.104	WLM/MSM - Windows Live Messenger
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		115.135.147.74	5500\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		115.71.91.110	8080\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.202	NetBIOS - Session Service
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.203	BOOTP - Server

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.3</b>						
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.204	NetBIOS - Name Service
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.212	DNS - Domain Name System
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Compromise		107.25.150.43	GNUTELLA-RTR
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		106.148.54.20	111\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		106.23.8.82	PPTP - Point-to-Point Tunneling Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		110.173.225.94	Finger
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		118.190.70.171	POP3 - Post Office Protocol Version 3
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		66.2.30.6	NetBIOS - Name Service
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.214	HTTPS - Secure HTTP
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.223	PPTP - Point-to-Point Tunneling Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.253	IMAP - Internet Message Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		106.41.42.164	79\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		106.160.138.40	5800\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		113.104.243.29	UPS - Uninterruptible Power Supply
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		119.84.138.21	79\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		72.99.11.103	NNTP - Network News Transfer Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Compromise		110.105.176.46	NetBIOS - Session Service
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		109.129.58.157	IMAP - Internet Message Access Protocol
<b>161.200.1.4</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		103.253.172.4	IMAP - Internet Message Access Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		106.87.12.123	Syslog - System Logging Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		66.2.30.1	TELNET
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.206	HTTPS - Secure HTTP
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.208	IBM Lotus Notes/Domino RPC
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.214	IMAP - Internet Message Access Protocol
03/26/08 12:00 AM	03/27/08 12:00 PM	2.00	General Reconnaissance		88.69.1.252	8080\

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		103.253.172.4	IMAP - Internet Message Access Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		114.17.192.178	Finger
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		109.129.58.157	NetBIOS - Datagram
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		117.83.247.204	110\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		119.31.164.89	GNUTELLA Service
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.106	DNS - Domain Name System
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.223	SMTP - Simple Mail Transfer Protocol
03/26/08 01:00 AM	03/26/08 02:00 PM	2.00	General Reconnaissance		110.49.174.190	GNUTELLA-RTR
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		101.136.167.138	BOOTP - Server
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		101.88.139.234	119\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		110.173.225.94	111\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		110.56.252.33	BOOTP - Client
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.234	Kazaa
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.240	MySQL Database System
03/26/08 02:00 AM	03/26/08 04:00 AM	2.00	General Reconnaissance		105.148.92.222	5800\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		102.27.84.33	NetBIOS - Name Service
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		103.44.13.181	BOOTP - Client
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		105.148.92.222	FTP Command
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		106.178.103.206	AIM - AOL Instant Messenger
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		107.180.80.203	Microsoft Directory Services
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		112.229.146.63	79\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		118.29.166.228	SMTP - Simple Mail Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.248	5500\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.250	Microsoft Directory Services
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Compromise		118.15.241.93	111\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		106.178.103.206	End Point Mapper
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		110.91.38.179	IMAP - Internet Message Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		112.236.131.84	NNTP - Network News Transfer Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		116.13.132.192	8080\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		117.21.49.172	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		66.2.30.7	NetBIOS - Name Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.111	IMAP - Internet Message Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.208	GNUTELLA-RTR
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		107.25.150.43	111\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		115.111.20.104	UPS - Uninterruptible Power Supply
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		66.2.30.5	NetBIOS - Session Service
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		72.99.11.109	5500\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		72.99.11.112	79\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		102.27.84.33	HTTPS - Secure HTTP
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		102.27.84.33	MSSQL - SQL Server Database
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Compromise		101.88.139.234	IBM Lotus Notes/Domino RPC
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		119.166.129.99	MSSQL - SQL Server Database
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		119.25.113.70	End Point Mapper
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.114	POP3 - Post Office Protocol Version 3
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.211	X Window System
03/26/08 07:00 AM	03/26/08 05:00 PM	2.00	General Reconnaissance		72.99.11.108	AIM - AOL Instant Messenger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		101.88.139.234	111\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		103.242.202.177	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		107.25.150.43	119\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.252	5800\
03/26/08 08:00 AM	03/27/08 11:00 PM	2.00	General Reconnaissance		66.2.30.7	IBM Lotus Notes/Domino RPC
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Compromise		120.138.126.247	5500\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		101.136.167.138	Kazaa
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		110.56.252.33	79\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		111.103.215.210	111\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		113.215.126.48	111\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		66.2.30.4	AIM - AOL Instant Messenger
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.204	HTTPS - Secure HTTP

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.207	DNS - Domain Name System
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.238	WLM/MSM - Windows Live Messenger
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		105.148.92.222	111\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		109.105.181.83	NetBIOS - Session Service
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		110.105.176.46	MSSQL - SQL Server Monitor
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		112.26.27.203	FTP Command
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.218	NetBIOS - Name Service
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.236	LDAP - Lightweight Directory Access Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.237	TFTP - Trivial File Transfer Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.241	IMAP - Internet Message Access Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.242	Syslog - System Logging Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		106.23.8.82	FTP Command
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		107.240.248.102	MySQL Database System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		110.49.174.190	IMAP - Internet Message Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		111.142.55.119	Finger
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		112.250.231.58	5500\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		112.250.231.58	IBM Lotus Notes/Domino RPC
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		114.17.192.178	111\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.109	MSSQL - SQL Server Database
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.219	Syslog - System Logging Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.235	SMTP - Simple Mail Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.248	FTP Command
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		111.103.27.70	AIM - AOL Instant Messenger
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		113.53.48.148	BOOTP - Server
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		116.97.118.31	NetBIOS - Datagram
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		117.83.247.204	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		72.99.11.104	HTTP - Hypertext Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.212	LDAP - Lightweight Directory Access Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.219	GNUTELLA Service
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.221	MSSQL - SQL Server Monitor
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.229	Microsoft Directory Services
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Compromise		88.69.1.216	SMTP - Simple Mail Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Compromise		88.69.1.227	Microsoft Directory Services
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		113.53.48.148	Microsoft Directory Services
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		116.13.132.192	UPS - Uninterruptible Power Supply
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		107.1.188.213	End Point Mapper
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		107.75.39.135	MSSQL - SQL Server Database
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		116.96.74.233	HTTP - Hypertext Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		116.97.118.31	110\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		72.99.11.111	End Point Mapper
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		72.99.11.113	GNUTELLA Service
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		72.99.11.114	119\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.202	Microsoft Directory Services
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.230	TFTP - Trivial File Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.245	Kazaa
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		117.83.247.204	HTTPS - Secure HTTP
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.107	HTTP - Hypertext Transfer Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.218	SSH - Secure Shell
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.242	111\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		106.71.210.209	IBM Lotus Notes/Domino RPC
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		107.240.248.102	DNS - Domain Name System

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		110.173.225.94	5800\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		117.21.49.172	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.109	HTTP - Hypertext Transfer Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.212	5800\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.233	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.247	MySQL Database System
03/26/08 04:00 PM	03/27/08 06:00 PM	2.00	General Reconnaissance		72.99.11.111	SSH - Secure Shell
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		105.248.16.99	5800\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		110.40.57.83	5500\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		113.215.126.48	WLM/MSM - Windows Live Messenger
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		66.2.30.8	119\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.236	MSSQL - SQL Server Monitor
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.238	Kazaa
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		111.36.131.245	Kazaa
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		112.26.27.203	PPTP - Point-to-Point Tunneling Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		114.183.253.86	End Point Mapper
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		119.166.129.99	5500\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		66.2.30.2	BOOTP - Client
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		66.2.30.9	IBM Lotus Notes/Domino RPC
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.112	WLM/MSM - Windows Live Messenger
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.213	5800\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		103.199.117.191	Syslog - System Logging Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		103.242.202.177	Finger
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		104.83.105.39	FTP Command
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		105.243.17.16	Microsoft Directory Services
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		105.243.17.16	MSSQL - SQL Server Monitor
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		72.99.11.105	TELNET

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.215	WLM/MSM - Windows Live Messenger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		101.136.167.138	MSSQL - SQL Server Database
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		105.248.16.99	FTP Command
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		113.53.48.148	POP3 - Post Office Protocol Version 3
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.101	Finger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.105	5800\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.111	MySQL Database System
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.247	MSSQL - SQL Server Database
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		117.21.49.172	5500\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		66.2.30.5	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		66.2.30.9	WLM/MSM - Windows Live Messenger
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		107.240.248.102	MSSQL - SQL Server Monitor
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.190.70.171	LDAP - Lightweight Directory Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.200	5500\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		72.99.11.117	WLM/MSM - Windows Live Messenger
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		106.12.75.97	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		114.128.130.118	TELNET
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		116.13.132.192	Microsoft Directory Services
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.118	POP3 - Post Office Protocol Version 3
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.119	POP3 - Post Office Protocol Version 3
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		105.248.16.99	SMTP - Simple Mail Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		105.241.215.112	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		105.96.101.134	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		113.104.243.29	111\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		113.159.109.25	MSSQL - SQL Server Database

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		66.2.30.8	POP3 - Post Office Protocol Version 3
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.223	End Point Mapper
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		88.69.1.212	DNS - Domain Name System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		112.26.27.203	111\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		113.104.243.29	IMAP - Internet Message Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		113.95.99.218	NetBIOS - Session Service
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		66.2.30.4	HTTP - Hypertext Transfer Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.112	AIM - AOL Instant Messenger
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.206	UPS - Uninterruptible Power Supply
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.208	WLM/MSM - Windows Live Messenger
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.233	IBM Lotus Notes/Domino RPC
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.234	TELNET
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		107.1.188.213	IBM Lotus Notes/Domino RPC
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		114.248.62.136	X Window System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		119.166.129.99	TELNET
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		120.204.177.106	119\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		66.2.30.9	110\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.107	MSSQL - SQL Server Database
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.118	X Window System
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Compromise		105.148.92.222	MSSQL - SQL Server Monitor
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		103.47.20.110	NNTP - Network News Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		106.41.42.164	HTTPS - Secure HTTP
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		107.180.80.203	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		116.96.74.233	NetBIOS - Name Service
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		118.15.241.93	MSSQL - SQL Server Database
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		66.2.30.10	FTP Command

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.100	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.218	FTP Command
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.229	79\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		110.105.176.46	DNS - Domain Name System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		106.178.103.206	End Point Mapper
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		106.178.103.206	PPTP - Point-to-Point Tunneling Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		112.211.5.54	PPTP - Point-to-Point Tunneling Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		112.231.167.112	LDAP - Lightweight Directory Access Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		113.215.126.48	NetBIOS - Datagram
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		119.31.164.89	POP3 - Post Office Protocol Version 3
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		66.2.30.8	UPS - Uninterruptible Power Supply
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.210	5500\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.210	UPS - Uninterruptible Power Supply
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.251	Syslog - System Logging Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		106.41.42.164	SMTP - Simple Mail Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		107.180.80.203	8080\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		109.117.125.53	111\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.252	X Window System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		88.69.1.253	NNTP - Network News Transfer Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		101.88.139.234	SSH - Secure Shell
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		103.199.117.191	NetBIOS - Name Service
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		105.96.101.134	IMAP - Internet Message Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		109.138.207.137	AIM - AOL Instant Messenger
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		110.40.57.83	X Window System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		111.36.131.245	BOOTP - Server
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		115.191.101.229	PPTP - Point-to-Point Tunneling Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		72.99.11.108	BOOTP - Server
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.200	DNS - Domain Name System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.217	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		109.5.43.42	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		115.135.147.74	IMAP - Internet Message Access Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.205	NetBIOS - Session Service
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.222	IMAP - Internet Message Access Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.227	BOOTP - Client
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		101.136.167.138	POP3 - Post Office Protocol Version 3
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		104.83.105.39	110\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		108.124.40.121	PPTP - Point-to-Point Tunneling Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.214	Kazaa
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.243	MySQL Database System
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.253	NNTP - Network News Transfer Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		103.242.202.177	MSSQL - SQL Server Database
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		113.198.41.205	AIM - AOL Instant Messenger
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		114.229.222.106	Syslog - System Logging Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.205	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.245	IMAP - Internet Message Access Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.250	DNS - Domain Name System
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Compromise		106.160.138.40	IMAP - Internet Message Access Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		101.136.167.138	SSH - Secure Shell
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		105.114.60.223	111\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		118.95.82.196	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.248	IBM Lotus Notes/Domino RPC

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		105.114.60.223	DNS - Domain Name System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		105.114.60.223	UPS - Uninterruptible Power Supply
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		108.103.69.15	IMAP - Internet Message Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.102	BOOTP - Server
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.210	LDAP - Lightweight Directory Access Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		109.129.58.157	HTTP - Hypertext Transfer Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		112.236.131.84	Finger
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.200	8080\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.204	GNUTELLA-RTR
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		102.116.230.67	Microsoft Directory Services
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		109.5.43.42	MSSQL - SQL Server Monitor
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		110.49.174.190	DNS - Domain Name System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.1	MSSQL - SQL Server Database
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Compromise		72.99.11.105	5500\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		107.25.150.43	DNS - Domain Name System
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		112.211.5.54	5800\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.101	DNS - Domain Name System
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.101	SSH - Secure Shell
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.117	SSH - Secure Shell
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.217	UPS - Uninterruptible Power Supply
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.232	GNUTELLA Service
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		118.29.166.228	110\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		119.135.23.192	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.102	NetBIOS - Session Service
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.211	POP3 - Post Office Protocol Version 3
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.246	TFTP - Trivial File Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.250	Finger
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		105.96.101.134	TELNET

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		113.215.126.48	End Point Mapper
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		66.2.30.5	SSH - Secure Shell
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		72.99.11.100	Syslog - System Logging Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Compromise		88.69.1.210	Microsoft Directory Services
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		113.215.126.48	GNUTELLA-RTR
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		119.157.88.38	HTTPS - Secure HTTP
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.101	UPS - Uninterruptible Power Supply
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.119	5500\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.215	119\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.217	MySQL Database System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.225	WLM/MSM - Windows Live Messenger
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.241	Microsoft Directory Services
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Compromise		88.69.1.236	111\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		119.157.88.38	110\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		120.138.126.247	End Point Mapper
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		72.99.11.107	IBM Lotus Notes/Domino RPC
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.239	BOOTP - Server
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		102.27.84.33	NetBIOS - Datagram
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		106.23.8.82	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		109.129.58.157	MySQL Database System
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		113.95.99.218	111\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		119.84.138.21	SSH - Secure Shell
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Compromise		105.96.101.134	AIM - AOL Instant Messenger
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		106.87.12.123	NetBIOS - Datagram
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		114.183.253.86	111\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		72.99.11.107	NetBIOS - Datagram
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		72.99.11.120	TFTP - Trivial File Transfer Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.236	X Window System
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		72.99.11.119	SSH - Secure Shell

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.253	PPTP - Point-to-Point Tunneling Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		107.75.39.135	PPTP - Point-to-Point Tunneling Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		112.26.27.203	POP3 - Post Office Protocol Version 3
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.202	79\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.215	Microsoft Directory Services
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.245	GNUTELLA-RTR
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.250	LDAP - Lightweight Directory Access Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		105.243.17.16	SMTP - Simple Mail Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		114.17.192.178	TELNET
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		120.204.177.106	LDAP - Lightweight Directory Access Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		72.99.11.100	GNUTELLA Service
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Compromise		110.105.176.46	End Point Mapper
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		111.142.55.119	SSH - Secure Shell
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		113.198.41.205	UPS - Uninterruptible Power Supply
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		72.99.11.110	Finger
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		72.99.11.110	NetBIOS - Session Service
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		72.99.11.111	NetBIOS - Session Service
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		72.99.11.119	BOOTP - Client
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.202	110\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.248	8080\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		112.229.146.63	DNS - Domain Name System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		114.183.253.86	8080\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		114.248.62.136	Microsoft Directory Services
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.203	DNS - Domain Name System
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		106.71.210.209	NetBIOS - Name Service
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		113.95.99.218	FTP Command
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Compromise		88.69.1.239	AIM - AOL Instant Messenger
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		105.148.92.222	IMAP - Internet Message Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		107.180.80.203	GNUTELLA Service
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		116.96.74.233	NetBIOS - Session Service
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		117.83.247.204	GNUTELLA-RTR
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		105.96.101.134	BOOTP - Server
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		108.124.40.121	Microsoft Directory Services
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		113.53.48.148	NetBIOS - Name Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		115.135.147.74	BOOTP - Server
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.119	Microsoft Directory Services
03/28/08 04:00 AM	03/28/08 07:00 AM	2.00	General Reconnaissance		88.69.1.204	5800\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		66.2.30.1	Kazaa
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		105.241.215.112	DNS - Domain Name System
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		111.142.55.119	IBM Lotus Notes/Domino RPC
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		119.84.138.21	IMAP - Internet Message Access Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		66.2.30.4	NetBIOS - Datagram
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.105	Kazaa
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		103.44.13.181	MSSQL - SQL Server Database
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.112	End Point Mapper
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.241	MSSQL - SQL Server Database
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.242	LDAP - Lightweight Directory Access Protocol
03/28/08 06:00 AM	03/28/08 08:00 AM	2.00	General Reconnaissance		107.25.150.43	End Point Mapper
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		105.114.60.223	FTP Command
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		111.195.14.150	IMAP - Internet Message Access Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.217	Finger
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		101.110.102.70	GNUTELLA-RTR
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		103.199.117.191	NetBIOS - Datagram
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.207	111\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.243	111\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Compromise		119.135.23.192	MSSQL - SQL Server Monitor
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		109.138.207.137	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.4</b>						
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		112.176.232.212	PPTP - Point-to-Point Tunneling Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		112.236.131.84	MSSQL - SQL Server Monitor
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		120.138.126.247	110\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		66.2.30.5	Finger
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		72.99.11.110	Kazaa
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.202	NetBIOS - Datagram
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.223	WLM/MSM - Windows Live Messenger
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		103.253.172.4	PPTP - Point-to-Point Tunneling Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.232	111\
<b>161.200.1.5</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		72.99.11.113	TFTP - Trivial File Transfer Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		66.2.30.6	IMAP - Internet Message Access Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		66.2.30.6	TFTP - Trivial File Transfer Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.209	HTTPS - Secure HTTP
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.212	8080\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.217	MSSQL - SQL Server Database
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.237	Finger
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		112.229.146.63	GNUTELLA-RTR
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		120.204.177.106	NetBIOS - Session Service
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.120	Microsoft Directory Services
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.204	POP3 - Post Office Protocol Version 3
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.216	5500\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.221	LDAP - Lightweight Directory Access Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Compromise		88.69.1.209	Finger
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		108.103.69.15	5800\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		108.124.40.121	GNUTELLA Service

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		108.124.40.121	LDAP - Lightweight Directory Access Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		112.211.5.54	BOOTP - Server
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		113.215.126.48	GNUTELLA Service
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		113.53.48.148	BOOTP - Client
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		114.229.222.106	Syslog - System Logging Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		107.240.248.102	IBM Lotus Notes/Domino RPC
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		118.190.70.171	SMTP - Simple Mail Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		66.2.30.10	NetBIOS - Name Service
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.101	NNTP - Network News Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.230	Microsoft Directory Services
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.235	5500\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.240	BOOTP - Client
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.250	5800\
03/26/08 03:00 AM	03/26/08 04:00 PM	2.00	General Reconnaissance		118.95.82.196	TFTP - Trivial File Transfer Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		105.114.60.223	IMAP - Internet Message Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		112.26.27.203	BOOTP - Client
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		118.29.166.228	SSH - Secure Shell
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.215	POP3 - Post Office Protocol Version 3
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.253	UPS - Uninterruptible Power Supply
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Compromise		101.136.167.138	End Point Mapper
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		104.151.242.62	UPS - Uninterruptible Power Supply
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		107.75.39.135	5500\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		114.183.253.86	Microsoft Directory Services
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		115.135.147.74	TFTP - Trivial File Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		66.2.30.2	WLM/MSM - Windows Live Messenger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		72.99.11.105	NetBIOS - Name Service
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.204	5500\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.214	LDAP - Lightweight Directory Access Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		103.253.172.4	UPS - Uninterruptible Power Supply
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		105.114.60.223	NetBIOS - Session Service
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		105.148.92.222	FTP Command
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		119.84.138.21	Syslog - System Logging Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		119.84.138.21	WLM/MSM - Windows Live Messenger
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		66.2.30.4	NNTP - Network News Transfer Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.229	UPS - Uninterruptible Power Supply
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.242	HTTP - Hypertext Transfer Protocol
03/26/08 06:00 AM	03/26/08 11:00 PM	2.00	General Reconnaissance		103.44.13.181	WLM/MSM - Windows Live Messenger
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		112.229.146.63	FTP Command
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.114	IMAP - Internet Message Access Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.231	110\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Compromise		110.173.225.94	BOOTP - Client
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Compromise		115.71.91.110	AIM - AOL Instant Messenger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		105.96.101.72	79\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		110.105.176.46	NetBIOS - Session Service
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		112.250.231.58	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		116.97.118.31	AIM - AOL Instant Messenger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		119.135.23.192	SSH - Secure Shell
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		119.157.88.38	Syslog - System Logging Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		119.29.250.161	MSSQL - SQL Server Monitor
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.114	79\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.115	SMTP - Simple Mail Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.120	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.208	5800\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.252	IBM Lotus Notes/Domino RPC
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Compromise		115.111.20.104	111\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		103.199.117.191	BOOTP - Client
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		106.12.75.97	TELNET
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		109.117.125.53	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		111.195.14.150	119\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		112.231.167.112	DNS - Domain Name System
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		113.53.48.148	Kazaa
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		115.191.101.229	End Point Mapper
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		116.13.132.192	FTP Command
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		118.66.66.46	5500\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		66.2.30.10	End Point Mapper
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.113	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.206	5800\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		102.27.84.33	UPS - Uninterruptible Power Supply
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		110.49.174.190	GNUTELLA-RTR
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		115.191.101.229	5500\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		117.83.247.204	GNUTELLA Service
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		119.166.129.99	IMAP - Internet Message Access Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		119.25.113.70	BOOTP - Client
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		66.2.30.5	GNUTELLA Service
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Compromise		88.69.1.201	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		110.56.252.33	IBM Lotus Notes/Domino RPC
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		111.103.215.210	BOOTP - Server
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		115.111.20.104	End Point Mapper
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.221	HTTPS - Secure HTTP

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.227	End Point Mapper
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.239	IMAP - Internet Message Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.245	End Point Mapper
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.246	End Point Mapper
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		106.178.103.206	NetBIOS - Session Service
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		107.25.150.43	GNUTELLA Service
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		107.25.150.43	MySQL Database System
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		111.103.215.210	BOOTP - Client
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		116.76.60.122	End Point Mapper
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		119.25.113.70	79\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		66.2.30.9	GNUTELLA-RTR
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.205	UPS - Uninterruptible Power Supply
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.216	8080\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.216	MSSQL - SQL Server Monitor
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.242	110\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.244	Microsoft Directory Services
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.246	HTTP - Hypertext Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		103.242.202.177	UPS - Uninterruptible Power Supply
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		103.44.13.181	TFTP - Trivial File Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.119	UPS - Uninterruptible Power Supply
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.211	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.237	IMAP - Internet Message Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.239	POP3 - Post Office Protocol Version 3
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		109.105.181.83	GNUTELLA-RTR
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		113.198.41.205	GNUTELLA Service
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		115.191.101.229	Microsoft Directory Services
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		116.96.74.233	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		117.83.247.204	DNS - Domain Name System
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		118.29.166.228	WLM/MSM - Windows Live Messenger
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		66.2.30.8	TELNET
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		105.96.101.134	NNTP - Network News Transfer Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		106.148.54.20	UPS - Uninterruptible Power Supply
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		107.1.188.213	IMAP - Internet Message Access Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		109.129.58.157	GNUTELLA Service
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		115.191.101.229	NetBIOS - Name Service
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		117.21.49.172	Finger
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		117.83.247.204	111\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Compromise		72.99.11.104	BOOTP - Server
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		105.148.92.222	110\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		112.236.131.84	111\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		118.66.66.46	PPTP - Point-to-Point Tunneling Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.207	119\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.209	5500\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		103.199.117.191	Syslog - System Logging Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		112.229.146.63	TFTP - Trivial File Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		72.99.11.104	NNTP - Network News Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.205	Finger
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.222	LDAP - Lightweight Directory Access Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.228	MSSQL - SQL Server Database
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		109.129.58.157	HTTPS - Secure HTTP
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		115.135.147.74	DNS - Domain Name System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		117.21.49.172	IMAP - Internet Message Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		66.2.30.3	DNS - Domain Name System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		66.2.30.3	GNUTELLA-RTR
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.106	BOOTP - Client

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.110	79\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.244	LDAP - Lightweight Directory Access Protocol
03/26/08 06:00 PM	03/27/08 06:00 PM	2.00	General Reconnaissance		112.176.232.212	HTTP - Hypertext Transfer Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		110.76.158.164	BOOTP - Client
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		112.250.231.58	PPTP - Point-to-Point Tunneling Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		116.97.118.31	79\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.231	MSSQL - SQL Server Database
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Compromise		107.25.150.43	NetBIOS - Name Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Compromise		66.2.30.7	NetBIOS - Session Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Compromise		88.69.1.243	WLM/MSM - Windows Live Messenger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		103.44.13.181	DNS - Domain Name System
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		109.138.207.137	5800\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		110.195.212.97	NetBIOS - Session Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		111.36.131.245	FTP Command
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		113.215.126.48	79\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		120.138.126.247	NetBIOS - Session Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.103	BOOTP - Client
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.231	79\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		102.27.84.33	MSSQL - SQL Server Monitor
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		110.195.212.97	UPS - Uninterruptible Power Supply
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		111.195.14.150	End Point Mapper
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		114.248.62.136	AIM - AOL Instant Messenger
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.227	LDAP - Lightweight Directory Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		112.26.27.203	BOOTP - Server
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		116.76.60.122	5800\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.95.82.196	Microsoft Directory Services
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.114	NNTP - Network News Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.119	GNUTELLA-RTR

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.211	BOOTP - Server
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.215	119\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.239	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		110.56.252.33	GNUTELLA Service
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		103.47.20.110	5800\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		106.178.103.206	SSH - Secure Shell
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		115.71.91.110	X Window System
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		119.84.138.21	GNUTELLA Service
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.215	UPS - Uninterruptible Power Supply
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.249	BOOTP - Client
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		105.243.17.16	HTTPS - Secure HTTP
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		106.178.103.206	MySQL Database System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		108.124.40.121	119\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		110.91.38.179	119\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		112.250.231.58	DNS - Domain Name System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.219	5500\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		88.69.1.204	Kazaa
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		88.69.1.216	DNS - Domain Name System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		103.199.117.191	HTTPS - Secure HTTP
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		110.105.176.46	HTTP - Hypertext Transfer Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		115.111.20.104	NNTP - Network News Transfer Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.100	Finger
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.104	Kazaa
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.218	110\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.220	NetBIOS - Name Service
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.224	SMTP - Simple Mail Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		105.243.17.16	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		106.12.75.97	X Window System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		110.76.158.164	NetBIOS - Session Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		119.31.164.89	X Window System
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		109.117.125.53	GNUTELLA-RTR

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		109.129.58.157	GNUTELLA-RTR
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		113.104.243.29	5800\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		116.96.74.233	BOOTP - Server
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		119.84.138.21	POP3 - Post Office Protocol Version 3
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.105	HTTPS - Secure HTTP
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.110	End Point Mapper
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.240	MSSQL - SQL Server Monitor
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		106.12.75.97	FTP Command
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		107.240.248.102	LDAP - Lightweight Directory Access Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		109.117.125.53	AIM - AOL Instant Messenger
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		110.40.57.83	TFTP - Trivial File Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		119.166.129.99	LDAP - Lightweight Directory Access Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.103	119\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.111	SSH - Secure Shell
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.221	WLM/MSM - Windows Live Messenger
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		101.110.102.70	UPS - Uninterruptible Power Supply
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		101.88.139.234	MSSQL - SQL Server Database
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		115.135.147.74	NNTP - Network News Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		115.71.91.110	GNUTELLA-RTR
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		117.21.49.172	8080\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.243	TFTP - Trivial File Transfer Protocol
03/27/08 05:00 AM	03/27/08 06:00 PM	2.00	General Reconnaissance		72.99.11.107	UPS - Uninterruptible Power Supply
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		88.69.1.229	SMTP - Simple Mail Transfer Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		101.88.139.234	110\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		106.71.210.209	SMTP - Simple Mail Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.202	NetBIOS - Name Service
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.236	110\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		113.104.243.29	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		118.190.70.171	TFTP - Trivial File Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.100	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.116	79\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.217	GNUTELLA Service
03/27/08 07:00 AM	03/27/08 05:00 PM	2.00	General Reconnaissance		72.99.11.112	110\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		101.138.232.109	GNUTELLA Service
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		114.183.253.86	5800\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		66.2.30.2	SMTP - Simple Mail Transfer Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.248	IMAP - Internet Message Access Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.252	GNUTELLA Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		101.138.232.109	5800\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		102.27.84.33	NetBIOS - Session Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.212	5800\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.222	End Point Mapper
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.226	NetBIOS - Datagram
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		103.253.172.4	IMAP - Internet Message Access Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		112.211.5.54	AIM - AOL Instant Messenger
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		112.229.146.63	NetBIOS - Session Service
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		112.250.231.58	BOOTP - Client
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		112.250.231.58	TELNET
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		113.53.48.148	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		114.183.253.86	GNUTELLA Service
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		115.135.147.74	MySQL Database System
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		118.200.95.244	119\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		120.138.126.247	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		66.2.30.1	Finger
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.113	MSSQL - SQL Server Monitor

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.115	HTTP - Hypertext Transfer Protocol
03/27/08 10:00 AM	03/27/08 02:00 PM	2.00	General Reconnaissance		104.83.105.39	Microsoft Directory Services
03/27/08 10:00 AM	03/28/08 01:00 AM	2.00	General Reconnaissance		72.99.11.118	MSSQL - SQL Server Database
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		103.242.202.177	PPTP - Point-to-Point Tunneling Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		118.19.112.193	111\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.117	POP3 - Post Office Protocol Version 3
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.201	IBM Lotus Notes/Domino RPC
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.215	BOOTP - Server
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		105.148.92.222	IMAP - Internet Message Access Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		110.76.158.164	POP3 - Post Office Protocol Version 3
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.213	IMAP - Internet Message Access Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.249	NNTP - Network News Transfer Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Compromise		103.242.202.177	BOOTP - Client
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		106.41.42.164	PPTP - Point-to-Point Tunneling Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		111.36.131.245	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		113.53.48.148	110\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.8	MySQL Database System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.9	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		72.99.11.101	AIM - AOL Instant Messenger
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		109.129.58.157	UPS - Uninterruptible Power Supply
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		113.104.243.29	MySQL Database System
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		118.19.112.193	79\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		118.95.82.196	NetBIOS - Datagram
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		119.31.164.89	LDAP - Lightweight Directory Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.111	Microsoft Directory Services
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.112	SMTP - Simple Mail Transfer Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.249	IMAP - Internet Message Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		88.69.1.203	Microsoft Directory Services
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		104.83.105.39	Kazaa
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		115.191.101.229	UPS - Uninterruptible Power Supply
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.207	BOOTP - Server
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.252	79\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.215	HTTP - Hypertext Transfer Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.226	NetBIOS - Session Service
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.238	Finger
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Compromise		88.69.1.213	Finger
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		106.87.12.123	PPTP - Point-to-Point Tunneling Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.227	Kazaa
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		109.138.207.137	NetBIOS - Name Service
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		115.191.101.229	BOOTP - Server
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		118.190.70.171	IMAP - Internet Message Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		72.99.11.109	NetBIOS - Datagram
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.232	DNS - Domain Name System
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.240	IBM Lotus Notes/Domino RPC
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		111.195.14.150	POP3 - Post Office Protocol Version 3
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		113.215.126.48	BOOTP - Server
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		66.2.30.3	BOOTP - Client
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		66.2.30.4	GNUTELLA Service
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.111	IBM Lotus Notes/Domino RPC
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.203	End Point Mapper
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.232	SMTP - Simple Mail Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/27/08 07:00 PM	03/28/08 04:00 AM	2.00	General Reconnaissance		72.99.11.108	DNS - Domain Name System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		101.88.139.234	Finger
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.223	NNTP - Network News Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		109.105.181.83	IMAP - Internet Message Access Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		88.69.1.205	NetBIOS - Session Service
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		111.103.27.70	TELNET
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		111.36.131.245	WLM/MSM - Windows Live Messenger
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		115.191.101.229	FTP Command
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.205	BOOTP - Server
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.241	111\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		119.157.88.38	X Window System
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		88.69.1.235	IMAP - Internet Message Access Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		116.97.118.31	FTP Command
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		66.2.30.6	GNUTELLA-RTR
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.208	110\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.251	MySQL Database System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Compromise		66.2.30.4	79\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		106.148.54.20	IMAP - Internet Message Access Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		113.95.99.218	111\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		114.229.222.106	119\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		119.84.138.21	111\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		72.99.11.101	SMTP - Simple Mail Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.219	110\
03/27/08 11:00 PM	03/28/08 01:00 AM	2.00	General Reconnaissance		110.76.158.164	NetBIOS - Name Service
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		106.87.12.123	Finger
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		107.197.4.193	Microsoft Directory Services
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.245	PPTP - Point-to-Point Tunneling Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		109.105.181.83	79\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		88.69.1.212	111\

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		111.103.27.70	MSSQL - SQL Server Database
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.205	BOOTP - Client
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.206	NetBIOS - Name Service
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		110.91.38.179	79\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		111.36.131.245	Syslog - System Logging Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		72.99.11.105	SSH - Secure Shell
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Compromise		101.138.232.109	111\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		113.104.243.29	PPTP - Point-to-Point Tunneling Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		72.99.11.109	111\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.205	119\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.209	MSSQL - SQL Server Database
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.235	X Window System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.237	End Point Mapper
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		107.180.80.203	UPS - Uninterruptible Power Supply
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		107.197.4.193	HTTP - Hypertext Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		112.176.232.212	79\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		112.176.232.212	SMTP - Simple Mail Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		114.128.130.118	UPS - Uninterruptible Power Supply
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		66.2.30.9	TFTP - Trivial File Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.106	UPS - Uninterruptible Power Supply
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.224	End Point Mapper
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		115.191.101.229	UPS - Uninterruptible Power Supply
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		102.27.84.33	111\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		103.44.13.181	PPTP - Point-to-Point Tunneling Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		106.41.42.164	DNS - Domain Name System
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		112.250.231.58	WLM/MSM - Windows Live Messenger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		117.180.12.105	LDAP - Lightweight Directory Access Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		118.95.82.196	PPTP - Point-to-Point Tunneling Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.118	PPTP - Point-to-Point Tunneling Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.250	HTTP - Hypertext Transfer Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		112.229.146.63	111\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		66.2.30.3	NetBIOS - Name Service
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.114	SMTP - Simple Mail Transfer Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Compromise		105.248.16.99	MySQL Database System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Compromise		106.41.42.164	DNS - Domain Name System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		105.148.92.222	DNS - Domain Name System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		112.211.5.54	Microsoft Directory Services
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.117	111\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.203	SMTP - Simple Mail Transfer Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.229	8080\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.241	5800\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Compromise		119.25.113.70	X Window System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		112.250.231.58	111\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		118.200.95.244	UPS - Uninterruptible Power Supply
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.115	119\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.242	IMAP - Internet Message Access Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		103.44.13.181	MSSQL - SQL Server Database
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		118.200.95.244	5500\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.224	NetBIOS - Datagram
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		107.197.4.193	NetBIOS - Datagram
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		107.75.39.135	AIM - AOL Instant Messenger
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		110.195.212.97	UPS - Uninterruptible Power Supply

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.5</b>						
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		72.99.11.104	IMAP - Internet Message Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.227	HTTP - Hypertext Transfer Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.228	PPTP - Point-to-Point Tunneling Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.241	Kazaa
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		110.76.158.164	LDAP - Lightweight Directory Access Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.230	MSSQL - SQL Server Monitor
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.237	X Window System
<b>161.200.1.6</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		101.136.167.138	LDAP - Lightweight Directory Access Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		104.83.105.39	Microsoft Directory Services
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		113.53.48.148	GNUTELLA-RTR
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		114.183.253.86	DNS - Domain Name System
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		118.15.241.93	MSSQL - SQL Server Monitor
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		118.15.241.93	Syslog - System Logging Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		103.253.172.4	8080\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		112.176.232.212	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		112.211.5.54	NetBIOS - Name Service
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		119.29.250.161	Microsoft Directory Services
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		120.204.177.106	5800\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		66.2.30.6	AIM - AOL Instant Messenger
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.209	Finger
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.211	Kazaa
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.232	POP3 - Post Office Protocol Version 3
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.234	Kazaa
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		101.110.102.70	IBM Lotus Notes/Domino RPC

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		104.151.242.62	8080\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		109.129.58.157	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		112.236.131.84	Finger
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		113.159.109.25	TFTP - Trivial File Transfer Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.112	MSSQL - SQL Server Monitor
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.207	Microsoft Directory Services
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.226	NNTP - Network News Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		105.248.16.99	AIM - AOL Instant Messenger
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		112.211.5.54	NetBIOS - Datagram
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		66.2.30.2	Kazaa
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.102	UPS - Uninterruptible Power Supply
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Compromise		112.26.27.203	NetBIOS - Datagram
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		112.231.167.112	DNS - Domain Name System
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.216	NetBIOS - Session Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.218	IMAP - Internet Message Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	2.00	General Reconnaissance		88.69.1.223	110\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.244	HTTP - Hypertext Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		112.231.167.112	PPTP - Point-to-Point Tunneling Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		112.231.167.112	SMTP - Simple Mail Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.210	BOOTP - Server
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.224	X Window System
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		109.117.125.53	110\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		110.76.158.164	GNUTELLA-RTR
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		119.25.113.70	8080\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.222	MSSQL - SQL Server Monitor
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.240	HTTPS - Secure HTTP
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		66.2.30.1	111\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Compromise		119.31.164.89	TFTP - Trivial File Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Compromise		88.69.1.209	NNTP - Network News Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		106.160.138.40	IBM Lotus Notes/Domino RPC
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		66.2.30.2	POP3 - Post Office Protocol Version 3
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.107	NNTP - Network News Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.208	WLM/MSM - Windows Live Messenger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.252	X Window System
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		105.114.60.223	GNUTELLA Service
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		105.248.16.99	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		105.96.101.72	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		106.87.12.123	UPS - Uninterruptible Power Supply
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		110.91.38.179	111\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		111.103.27.70	GNUTELLA-RTR
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		112.231.167.112	GNUTELLA-RTR
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		116.76.60.122	UPS - Uninterruptible Power Supply
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		119.31.164.89	Microsoft Directory Services
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.110	IMAP - Internet Message Access Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.119	8080\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.246	IMAP - Internet Message Access Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Compromise		88.69.1.236	AIM - AOL Instant Messenger
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		105.96.101.72	UPS - Uninterruptible Power Supply
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		108.103.69.15	End Point Mapper
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		113.104.243.29	DNS - Domain Name System
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.117	AIM - AOL Instant Messenger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.229	BOOTP - Server
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		101.136.167.138	BOOTP - Server
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		108.103.69.15	DNS - Domain Name System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		109.117.125.53	BOOTP - Client
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		111.142.55.119	NetBIOS - Session Service
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.245	110\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		104.151.242.62	DNS - Domain Name System
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		109.138.207.137	SMTP - Simple Mail Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		112.26.27.203	FTP Command
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		115.71.91.110	5500\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.218	5800\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.232	BOOTP - Server
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.222	119\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.230	HTTP - Hypertext Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		106.71.210.209	End Point Mapper
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		109.129.58.157	NetBIOS - Session Service
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		110.195.212.97	TELNET
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		112.26.27.203	GNUTELLA Service
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		116.13.132.192	111\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		120.204.177.106	NetBIOS - Name Service
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		66.2.30.10	UPS - Uninterruptible Power Supply
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.212	79\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.226	MSSQL - SQL Server
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.228	Monitor
03/26/08 02:00 PM	03/27/08 03:00 PM	2.00	General Reconnaissance		88.69.1.226	8080\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		103.47.20.110	IBM Lotus Notes/Domino RPC
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		111.103.215.210	8080\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.203	111\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.243	Microsoft Directory Services
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.245	IMAP - Internet Message Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Compromise		116.76.60.122	NetBIOS - Name Service
						Finger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		107.197.4.193	BOOTP - Client
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		112.229.146.63	NetBIOS - Name Service
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		118.190.70.171	MySQL Database System
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		66.2.30.5	FTP Command
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.104	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.115	111\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		110.105.176.46	8080\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		110.173.225.94	79\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		118.19.112.193	BOOTP - Client
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		72.99.11.120	PPTP - Point-to-Point Tunneling Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.229	FTP Command
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		108.124.40.121	110\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		110.195.212.97	NetBIOS - Name Service
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		114.128.130.118	FTP Command
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		116.76.60.122	End Point Mapper
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		119.84.138.21	111\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.116	SSH - Secure Shell
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.227	MSSQL - SQL Server Database
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.236	NNTP - Network News Transfer Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		105.114.60.223	SMTP - Simple Mail Transfer Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		110.105.176.46	111\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		116.97.118.31	NetBIOS - Session Service
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		118.66.66.46	SSH - Secure Shell
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		66.2.30.9	SSH - Secure Shell
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.202	HTTP - Hypertext Transfer Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.223	Kazaa
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		119.25.113.70	Finger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		119.84.138.21	MSSQL - SQL Server Database
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.101	NetBIOS - Datagram
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.113	IBM Lotus Notes/Domino RPC

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.201	GNUTELLA-RTR
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.217	End Point Mapper
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		118.19.112.193	BOOTP - Server
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		72.99.11.102	8080\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		72.99.11.115	X Window System
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.212	TFTP - Trivial File Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		101.136.167.138	GNUTELLA-RTR
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		105.241.215.112	111\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		105.241.215.112	NetBIOS - Name Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		105.96.101.134	Kazaa
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.200.95.244	Syslog - System Logging Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.105	NetBIOS - Session Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.107	DNS - Domain Name System
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.107	GNUTELLA Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.111	IMAP - Internet Message Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.114	BOOTP - Client
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.119	GNUTELLA-RTR
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.214	UPS - Uninterruptible Power Supply
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.219	MSSQL - SQL Server Database
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		72.99.11.115	HTTPS - Secure HTTP
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		102.27.84.33	IMAP - Internet Message Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		107.75.39.135	Kazaa
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		111.103.215.210	HTTP - Hypertext Transfer Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		112.211.5.54	Syslog - System Logging Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		119.29.250.161	BOOTP - Server
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.103	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		105.148.92.222	IMAP - Internet Message Access Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		109.138.207.137	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		113.95.99.218	Kazaa
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		115.191.101.229	Kazaa
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		119.166.129.99	111\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		119.31.164.89	FTP Command
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		119.84.138.21	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.120	DNS - Domain Name System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.232	Syslog - System Logging Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		114.183.253.86	PPTP - Point-to-Point Tunneling Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		88.69.1.231	IMAP - Internet Message Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		88.69.1.235	DNS - Domain Name System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		102.116.230.67	79\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		102.27.84.33	111\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		105.243.17.16	UPS - Uninterruptible Power Supply
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		110.195.212.97	NetBIOS - Session Service
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		111.103.27.70	5800\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		111.103.27.70	PPTP - Point-to-Point Tunneling Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		113.198.41.205	GNUTELLA Service
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.100	Microsoft Directory Services
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.208	119\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.217	WLM/MSM - Windows Live Messenger
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.229	Microsoft Directory Services
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		108.124.40.121	5500\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		109.5.43.42	LDAP - Lightweight Directory Access Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		112.26.27.203	NetBIOS - Session Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.100	HTTP - Hypertext Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.245	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		106.160.138.40	PPTP - Point-to-Point Tunneling Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		112.176.232.212	BOOTP - Server
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		113.159.109.25	Microsoft Directory Services
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		113.198.41.205	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		114.248.62.136	TELNET
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		115.191.101.229	MSSQL - SQL Server Monitor
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		105.96.101.72	NetBIOS - Datagram
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		105.96.101.72	TELNET
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.102	UPS - Uninterruptible Power Supply
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.105	MSSQL - SQL Server Monitor
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		103.44.13.181	AIM - AOL Instant Messenger
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		106.87.12.123	NNTP - Network News Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		107.25.150.43	GNUTELLA-RTR
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		66.2.30.10	GNUTELLA Service
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		72.99.11.100	BOOTP - Client
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.210	NetBIOS - Name Service
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.213	MySQL Database System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.235	UPS - Uninterruptible Power Supply
03/27/08 05:00 AM	03/27/08 03:00 PM	2.00	General Reconnaissance		72.99.11.113	NetBIOS - Session Service
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		107.1.188.213	TFTP - Trivial File Transfer Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		104.151.242.62	Finger
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		115.23.161.181	HTTPS - Secure HTTP
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		66.2.30.1	5800\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		72.99.11.110	HTTP - Hypertext Transfer Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		72.99.11.119	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		119.135.23.192	Finger
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		66.2.30.7	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.120	SMTP - Simple Mail Transfer Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.205	WLM/MSM - Windows Live Messenger
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		107.180.80.203	Finger
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		108.103.69.15	UPS - Uninterruptible Power Supply
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		117.83.247.204	79\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		118.29.166.228	5800\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		72.99.11.107	5800\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		102.27.84.33	End Point Mapper
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		117.180.12.105	MSSQL - SQL Server Monitor
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		119.25.113.70	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		72.99.11.107	NetBIOS - Datagram
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		72.99.11.116	GNUTELLA Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.237	MSSQL - SQL Server Database
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.243	IMAP - Internet Message Access Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.252	Microsoft Directory Services
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Compromise		109.105.181.83	DNS - Domain Name System
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		110.195.212.97	GNUTELLA-RTR
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		119.166.129.99	HTTP - Hypertext Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		66.2.30.3	PPTP - Point-to-Point Tunneling Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.100	Kazaa
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.207	5500\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.244	AIM - AOL Instant Messenger
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		106.160.138.40	HTTPS - Secure HTTP
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		110.40.57.83	NetBIOS - Datagram
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		66.2.30.7	HTTPS - Secure HTTP
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.112	SSH - Secure Shell
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.208	X Window System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.215	HTTP - Hypertext Transfer Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.216	Syslog - System Logging Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		104.151.242.62	SMTP - Simple Mail Transfer Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		104.83.105.39	HTTPS - Secure HTTP
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		113.95.99.218	Syslog - System Logging Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.210	GNUTELLA Service
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.237	DNS - Domain Name System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		103.199.117.191	8080\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		103.253.172.4	TFTP - Trivial File Transfer Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		105.114.60.223	HTTPS - Secure HTTP
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		111.195.14.150	End Point Mapper
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		114.183.253.86	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		117.180.12.105	Finger
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		118.190.70.171	111\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.1	End Point Mapper
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		72.99.11.107	SSH - Secure Shell
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		72.99.11.111	Finger
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		112.236.131.84	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		114.128.130.118	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.207	NetBIOS - Datagram
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.230	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		107.197.4.193	End Point Mapper
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		72.99.11.102	HTTP - Hypertext Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		105.248.16.99	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		66.2.30.2	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.226	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/28/08 07:00 AM	2.00	General Reconnaissance		104.83.105.39	MySQL Database System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Compromise		88.69.1.230	119\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		72.99.11.117	HTTP - Hypertext Transfer Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.215	TFTP - Trivial File Transfer Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		108.103.69.15	111\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		113.95.99.218	111\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		118.19.112.193	X Window System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		119.157.88.38	8080\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		119.166.129.99	IMAP - Internet Message Access Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		66.2.30.2	MySQL Database System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.201	PPTP - Point-to-Point Tunneling Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.204	MySQL Database System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.213	110\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.217	AIM - AOL Instant Messenger
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.232	LDAP - Lightweight Directory Access Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.246	LDAP - Lightweight Directory Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Compromise		103.242.202.177	Kazaa
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Compromise		115.111.20.104	MSSQL - SQL Server Database
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		112.236.131.84	NetBIOS - Datagram
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		113.215.126.48	FTP Command
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		118.66.66.46	AIM - AOL Instant Messenger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		111.195.14.150	UPS - Uninterruptible Power Supply
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		114.17.192.178	End Point Mapper
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		66.2.30.5	DNS - Domain Name System
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.206	BOOTP - Client
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.229	PPTP - Point-to-Point Tunneling Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		72.99.11.118	Syslog - System Logging Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.209	POP3 - Post Office Protocol Version 3

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.225	GNUTELLA Service
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		88.69.1.220	UPS - Uninterruptible Power Supply
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		115.111.20.104	NNTP - Network News Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		72.99.11.116	79\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.212	BOOTP - Server
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		102.116.230.67	79\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		113.104.243.29	End Point Mapper
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		114.128.130.118	FTP Command
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		101.136.167.138	End Point Mapper
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		109.129.58.157	NetBIOS - Name Service
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.113	111\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.205	Syslog - System Logging Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		110.195.212.97	X Window System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		113.215.126.48	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		119.29.250.161	GNUTELLA-RTR
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		72.99.11.114	79\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.232	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.248	DNS - Domain Name System
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Compromise		88.69.1.216	GNUTELLA Service
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		105.241.215.112	DNS - Domain Name System
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		106.178.103.206	Microsoft Directory Services
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		110.49.174.190	NetBIOS - Datagram
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		111.103.215.210	MySQL Database System
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.207	WLM/MSM - Windows Live Messenger
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.217	111\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.225	IBM Lotus Notes/Domino RPC
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.231	79\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.241	NetBIOS - Datagram
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		72.99.11.120	Microsoft Directory Services

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		106.87.12.123	GNUTELLA-RTR
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.228	GNUTELLA Service
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		119.166.129.99	DNS - Domain Name System
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		66.2.30.4	TFTP - Trivial File Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.210	UPS - Uninterruptible Power Supply
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.237	TELNET
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		108.124.40.121	SMTP - Simple Mail Transfer Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		72.99.11.108	X Window System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.212	AIM - AOL Instant Messenger
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.218	Microsoft Directory Services
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.235	LDAP - Lightweight Directory Access Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		102.116.230.67	Finger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		105.96.101.134	FTP Command
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		112.250.231.58	WLM/MSM - Windows Live Messenger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		66.2.30.8	TFTP - Trivial File Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.100	WLM/MSM - Windows Live Messenger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.110	119\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.208	Microsoft Directory Services
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.220	110\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.223	GNUTELLA-RTR
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.241	TFTP - Trivial File Transfer Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		101.88.139.234	8080\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		104.83.105.39	AIM - AOL Instant Messenger
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		105.96.101.72	119\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		109.117.125.53	Syslog - System Logging Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.110	PPTP - Point-to-Point Tunneling Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.220	111\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.241	8080\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		101.136.167.138	119\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		110.91.38.179	NetBIOS - Session Service
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		114.128.130.118	Microsoft Directory Services
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		114.229.222.106	5500\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.221	111\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.237	MySQL Database System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		103.199.117.191	TFTP - Trivial File Transfer Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		119.157.88.38	Microsoft Directory Services
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		66.2.30.10	8080\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		66.2.30.6	Microsoft Directory Services
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		66.2.30.8	PPTP - Point-to-Point Tunneling Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.118	TFTP - Trivial File Transfer Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.207	End Point Mapper
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.232	LDAP - Lightweight Directory Access Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.237	110\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.237	POP3 - Post Office Protocol Version 3
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Compromise		88.69.1.226	119\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		109.5.43.42	BOOTP - Server
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		116.96.74.233	LDAP - Lightweight Directory Access Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		66.2.30.6	WLM/MSM - Windows Live Messenger
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.115	5800\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.202	LDAP - Lightweight Directory Access Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.238	Syslog - System Logging Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.6</b>						
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		116.13.132.192	79\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		116.96.74.233	MSSQL - SQL Server Monitor
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.102	5800\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.203	GNUTELLA-RTR
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.249	LDAP - Lightweight Directory Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		106.12.75.97	111\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		110.76.158.164	X Window System
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		112.231.167.112	UPS - Uninterruptible Power Supply
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		113.159.109.25	DNS - Domain Name System
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		113.95.99.218	8080\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.217	LDAP - Lightweight Directory Access Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Compromise		115.191.101.229	79\
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		112.176.232.212	MSSQL - SQL Server Database
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		115.23.161.181	LDAP - Lightweight Directory Access Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		119.166.129.99	POP3 - Post Office Protocol Version 3
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		72.99.11.117	111\
<b>161.200.1.7</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		105.114.60.223	Microsoft Directory Services
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		105.243.17.16	MySQL Database System
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		116.13.132.192	PPTP - Point-to-Point Tunneling Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		66.2.30.1	5800\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		103.253.172.4	NNTP - Network News Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		105.96.101.72	Syslog - System Logging Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		106.23.8.82	UPS - Uninterruptible Power Supply
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		107.240.248.102	5800\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		109.117.125.53	POP3 - Post Office Protocol Version 3

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.213	IBM Lotus Notes/Domino RPC
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.229	HTTP - Hypertext Transfer Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		111.103.27.70	HTTPS - Secure HTTP
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		113.198.41.205	MSSQL - SQL Server Monitor
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		114.17.192.178	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		116.76.60.122	110\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		117.83.247.204	GNUTELLA-RTR
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.208	End Point Mapper
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.208	MSSQL - SQL Server Database
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.227	HTTPS - Secure HTTP
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.245	DNS - Domain Name System
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Compromise		108.124.40.121	Finger
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		112.26.27.203	BOOTP - Client
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		118.66.66.46	LDAP - Lightweight Directory Access Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		119.31.164.89	MSSQL - SQL Server Database
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.101	SSH - Secure Shell
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.214	TFTP - Trivial File Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.218	PPTP - Point-to-Point Tunneling Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.249	TFTP - Trivial File Transfer Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		112.229.146.63	UPS - Uninterruptible Power Supply
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		116.13.132.192	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.110	NetBIOS - Session Service
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		112.231.167.112	MSSQL - SQL Server Monitor
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		113.159.109.25	BOOTP - Client
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.207	X Window System
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.211	FTP Command

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.237	IMAP - Internet Message Access Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.246	8080\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.249	MSSQL - SQL Server Monitor
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.249	PPTP - Point-to-Point Tunneling Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Compromise		109.129.58.157	Microsoft Directory Services
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		105.248.16.99	5500\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		109.5.43.42	FTP Command
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		110.76.158.164	GNUTELLA Service
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		120.138.126.247	MySQL Database System
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.234	Kazaa
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Compromise		88.69.1.236	NetBIOS - Session Service
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		103.242.202.177	111\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		106.148.54.20	119\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		106.178.103.206	111\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		111.103.27.70	DNS - Domain Name System
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		117.180.12.105	119\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		66.2.30.6	POP3 - Post Office Protocol Version 3
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.248	79\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Compromise		103.199.117.191	DNS - Domain Name System
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		104.83.105.39	TFTP - Trivial File Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		116.76.60.122	TFTP - Trivial File Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		117.180.12.105	POP3 - Post Office Protocol Version 3
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.100	WLM/MSM - Windows Live Messenger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.102	DNS - Domain Name System
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.107	PPTP - Point-to-Point Tunneling Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.119	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.231	79\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		105.148.92.222	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		114.183.253.86	End Point Mapper
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.222	DNS - Domain Name System
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.253	BOOTP - Client
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		111.142.55.119	HTTPS - Secure HTTP
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		105.148.92.222	111\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		118.95.82.196	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		120.204.177.106	SMTP - Simple Mail Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		66.2.30.4	UPS - Uninterruptible Power Supply
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.215	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.220	FTP Command
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.246	NetBIOS - Session Service
03/26/08 11:00 AM	03/28/08 12:00 AM	2.00	General Reconnaissance		110.105.176.46	SSH - Secure Shell
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		109.117.125.53	111\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		112.229.146.63	GNUTELLA Service
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		113.53.48.148	Microsoft Directory Services
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.230	Microsoft Directory Services
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.248	MSSQL - SQL Server Database
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		105.248.16.99	Microsoft Directory Services
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		117.83.247.204	BOOTP - Server
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		118.190.70.171	X Window System
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		66.2.30.6	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.209	HTTP - Hypertext Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.234	TELNET
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Compromise		119.135.23.192	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		113.215.126.48	SMTP - Simple Mail Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		113.53.48.148	PPTP - Point-to-Point Tunneling Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		66.2.30.1	111\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.242	NNTP - Network News Transfer Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		111.195.14.150	UPS - Uninterruptible Power Supply
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		111.195.14.150	X Window System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		115.191.101.229	TELNET
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.217	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		106.41.42.164	MySQL Database System
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.117	Microsoft Directory Services
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		103.242.202.177	GNUTELLA-RTR
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		115.191.101.229	GNUTELLA Service
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		118.200.95.244	PPTP - Point-to-Point Tunneling Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		119.84.138.21	SSH - Secure Shell
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.240	Microsoft Directory Services
03/26/08 05:00 PM	03/28/08 10:00 AM	2.00	General Reconnaissance		88.69.1.245	AIM - AOL Instant Messenger
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		106.160.138.40	8080\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		110.56.252.33	Microsoft Directory Services
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		115.135.147.74	5500\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.112	BOOTP - Client
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.241	X Window System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.247	Syslog - System Logging Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		103.253.172.4	111\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		103.253.172.4	SSH - Secure Shell
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		116.96.74.233	WLM/MSM - Windows Live Messenger
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		118.15.241.93	LDAP - Lightweight Directory Access Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		118.190.70.171	110\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		66.2.30.5	79\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.204	End Point Mapper
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.205	FTP Command

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.210	HTTP - Hypertext Transfer Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.242	111\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.243	FTP Command
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		107.197.4.193	Syslog - System Logging Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		107.25.150.43	End Point Mapper
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		108.124.40.121	End Point Mapper
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		109.5.43.42	End Point Mapper
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		112.231.167.112	End Point Mapper
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		118.15.241.93	BOOTP - Server
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		66.2.30.1	GNUTELLA-RTR
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		106.23.8.82	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		109.117.125.53	79\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		109.117.125.53	DNS - Domain Name System
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		110.91.38.179	NetBIOS - Name Service
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		117.180.12.105	79\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		119.84.138.21	UPS - Uninterruptible Power Supply
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		66.2.30.7	X Window System
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		72.99.11.114	5800\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.200	MySQL Database System
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.211	UPS - Uninterruptible Power Supply
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.219	PPTP - Point-to-Point Tunneling Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		111.103.215.210	FTP Command
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		111.103.27.70	AIM - AOL Instant Messenger
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.109	PPTP - Point-to-Point Tunneling Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.226	SMTP - Simple Mail Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.251	End Point Mapper
03/26/08 10:00 PM	03/27/08 02:00 PM	2.00	General Reconnaissance		105.219.149.191	TFTP - Trivial File Transfer Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		113.159.109.25	SMTP - Simple Mail Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		105.243.17.16	WLM/MSM - Windows Live Messenger
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		106.23.8.82	TELNET
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		111.36.131.245	HTTP - Hypertext Transfer Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.119	NetBIOS - Session Service
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.221	MSSQL - SQL Server Monitor
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.227	LDAP - Lightweight Directory Access Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		106.12.75.97	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		88.69.1.242	8080\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		112.211.5.54	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		112.250.231.58	X Window System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		114.248.62.136	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.117	SSH - Secure Shell
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.253	IMAP - Internet Message Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		105.219.149.191	NetBIOS - Datagram
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		114.17.192.178	MSSQL - SQL Server Database
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.247	End Point Mapper
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		104.151.242.62	GNUTELLA Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		105.219.149.191	FTP Command
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		109.105.181.83	IMAP - Internet Message Access Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		109.138.207.137	MySQL Database System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		66.2.30.9	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.209	TFTP - Trivial File Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.228	UPS - Uninterruptible Power Supply
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		103.47.20.110	POP3 - Post Office Protocol Version 3
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		104.83.105.39	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		109.117.125.53	FTP Command

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		110.91.38.179	5800\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		111.142.55.119	Kazaa
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		111.142.55.119	NNTP - Network News Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.103	GNUTELLA Service
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.116	79\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.246	BOOTP - Server
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		105.96.101.72	111\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		112.236.131.84	Microsoft Directory Services
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		114.17.192.178	Kazaa
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		118.200.95.244	X Window System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		115.135.147.74	GNUTELLA-RTR
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.227	8080\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		113.104.243.29	111\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Compromise		118.95.82.196	111\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		111.103.215.210	IMAP - Internet Message Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		112.236.131.84	IMAP - Internet Message Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		115.23.161.181	111\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.208	PPTP - Point-to-Point Tunneling Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.242	IBM Lotus Notes/Domino RPC
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.252	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		104.83.105.39	119\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.220	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.230	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.252	WLM/MSM - Windows Live Messenger
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		107.197.4.193	NetBIOS - Name Service
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		112.236.131.84	X Window System
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		114.229.222.106	111\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.244	5500\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Compromise		111.36.131.245	LDAP - Lightweight Directory Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		107.197.4.193	X Window System
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		111.103.27.70	X Window System
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		118.190.70.171	5800\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		66.2.30.1	WLM/MSM - Windows Live Messenger
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		72.99.11.102	TFTP - Trivial File Transfer Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.238	BOOTP - Server
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		111.103.27.70	Finger
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		116.13.132.192	79\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		66.2.30.8	NNTP - Network News Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.112	TFTP - Trivial File Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.253	SSH - Secure Shell
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		66.2.30.8	NetBIOS - Name Service
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		72.99.11.117	8080\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		88.69.1.212	GNUTELLA-RTR
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		105.96.101.72	IMAP - Internet Message Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		110.173.225.94	111\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		114.128.130.118	IMAP - Internet Message Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.108	GNUTELLA-RTR
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.200	79\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.215	119\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.217	NetBIOS - Name Service
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.239	110\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		105.114.60.223	End Point Mapper
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		112.211.5.54	NetBIOS - Name Service
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		112.250.231.58	IMAP - Internet Message Access Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Compromise		88.69.1.221	79\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		114.248.62.136	GNUTELLA Service
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.3	5500\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.7	PPTP - Point-to-Point Tunneling Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.209	MySQL Database System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		102.27.84.33	MSSQL - SQL Server Database
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		113.215.126.48	Microsoft Directory Services
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		119.31.164.89	GNUTELLA-RTR
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.250	NetBIOS - Session Service
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.251	NNTP - Network News Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		112.176.232.212	8080\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		118.15.241.93	WLM/MSM - Windows Live Messenger
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		66.2.30.5	HTTP - Hypertext Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.120	FTP Command
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.219	5500\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.235	IMAP - Internet Message Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.240	LDAP - Lightweight Directory Access Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		109.117.125.53	DNS - Domain Name System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		72.99.11.106	PPTP - Point-to-Point Tunneling Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.204	AIM - AOL Instant Messenger
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.214	IMAP - Internet Message Access Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Compromise		101.88.139.234	HTTP - Hypertext Transfer Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		103.253.172.4	Finger
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		114.128.130.118	8080\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		114.229.222.106	DNS - Domain Name System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		116.96.74.233	UPS - Uninterruptible Power Supply
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		66.2.30.3	GNUTELLA-RTR
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.104	MSSQL - SQL Server Database
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.106	BOOTP - Server
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		106.148.54.20	NetBIOS - Datagram
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		109.129.58.157	NetBIOS - Session Service

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		116.76.60.122	NetBIOS - Datagram
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		101.138.232.109	WLM/MSM - Windows Live Messenger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		118.66.66.46	GNUTELLA-RTR
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		119.25.113.70	BOOTP - Server
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.105	Microsoft Directory Services
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.231	Kazaa
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		115.191.101.229	BOOTP - Server
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		66.2.30.6	X Window System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		72.99.11.102	IBM Lotus Notes/Domino RPC
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		104.83.105.39	NNTP - Network News Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		106.160.138.40	Syslog - System Logging Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		114.17.192.178	Syslog - System Logging Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		106.160.138.40	End Point Mapper
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		116.76.60.122	Finger
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.232	111\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Compromise		101.138.232.109	NetBIOS - Session Service
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		101.110.102.70	Syslog - System Logging Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		107.25.150.43	5500\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		72.99.11.107	LDAP - Lightweight Directory Access Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		72.99.11.118	X Window System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.235	8080\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		106.160.138.40	Microsoft Directory Services
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		115.191.101.229	MSSQL - SQL Server Monitor
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		119.135.23.192	End Point Mapper
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.229	TELNET
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.248	PPTP - Point-to-Point Tunneling Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.252	119\

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		105.248.16.99	IBM Lotus Notes/Domino RPC
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		110.76.158.164	IBM Lotus Notes/Domino RPC
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		66.2.30.8	MSSQL - SQL Server Database
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.233	WLM/MSM - Windows Live Messenger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.236	BOOTP - Client
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Compromise		108.124.40.121	TFTP - Trivial File Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Compromise		88.69.1.245	79\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		113.104.243.29	PPTP - Point-to-Point Tunneling Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		114.248.62.136	SSH - Secure Shell
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		116.96.74.233	Kazaa
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.200	PPTP - Point-to-Point Tunneling Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.203	110\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.238	AIM - AOL Instant Messenger
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.241	AIM - AOL Instant Messenger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		106.41.42.164	TFTP - Trivial File Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		109.138.207.137	Finger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.228	NNTP - Network News Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.243	110\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		120.204.177.106	MSSQL - SQL Server Monitor
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		103.253.172.4	End Point Mapper
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		108.103.69.15	MySQL Database System
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		109.5.43.42	Microsoft Directory Services
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		112.229.146.63	IBM Lotus Notes/Domino RPC
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.107	Finger
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.244	Microsoft Directory Services

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.7</b>						
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.249	8080\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		103.253.172.4	Microsoft Directory Services
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		119.25.113.70	IBM Lotus Notes/Domino RPC
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.224	Finger
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		105.114.60.223	Finger
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		116.97.118.31	Syslog - System Logging Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.104	X Window System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.206	110\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		107.25.150.43	DNS - Domain Name System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.100	IBM Lotus Notes/Domino RPC
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.115	Microsoft Directory Services
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.233	GNUTELLA Service
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Compromise		88.69.1.224	IMAP - Internet Message Access Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		113.159.109.25	TELNET
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.105	MSSQL - SQL Server Database
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.225	BOOTP - Client
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.253	MySQL Database System
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		103.199.117.191	SSH - Secure Shell
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.231	SMTP - Simple Mail Transfer Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		118.200.95.244	LDAP - Lightweight Directory Access Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.216	DNS - Domain Name System
<b>161.200.1.8</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		108.103.69.15	Microsoft Directory Services
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		112.26.27.203	SSH - Secure Shell
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.200	X Window System
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		109.138.207.137	DNS - Domain Name System
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		104.83.105.39	Microsoft Directory Services

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		105.96.101.72	Syslog - System Logging Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		106.87.12.123	PPTP - Point-to-Point Tunneling Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		116.97.118.31	Kazaa
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		119.84.138.21	NNTP - Network News Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.112	UPS - Uninterruptible Power Supply
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.118	Finger
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.207	DNS - Domain Name System
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.210	BOOTP - Client
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		113.104.243.29	FTP Command
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		114.229.222.106	GNUTELLA-RTR
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		115.23.161.181	Kazaa
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		119.157.88.38	POP3 - Post Office Protocol Version 3
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.119	BOOTP - Client
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		115.71.91.110	Kazaa
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		120.204.177.106	DNS - Domain Name System
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.205	Syslog - System Logging Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.216	DNS - Domain Name System
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		109.138.207.137	X Window System
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		110.49.174.190	PPTP - Point-to-Point Tunneling Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		114.128.130.118	End Point Mapper
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		116.96.74.233	5500\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.104	WLM/MSM - Windows Live Messenger
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.109	UPS - Uninterruptible Power Supply
03/26/08 04:00 AM	03/27/08 05:00 AM	2.00	General Reconnaissance		114.229.222.106	FTP Command
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Compromise		111.195.14.150	LDAP - Lightweight Directory Access Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		118.29.166.228	TELNET
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		118.95.82.196	111\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.249	5800\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		101.138.232.109	5500\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		102.27.84.33	Kazaa
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		115.71.91.110	HTTP - Hypertext Transfer Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		72.99.11.119	SMTP - Simple Mail Transfer Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.221	SSH - Secure Shell
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		102.116.230.67	Finger
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		111.103.215.210	DNS - Domain Name System
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		113.53.48.148	DNS - Domain Name System
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		115.23.161.181	119\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.101	FTP Command
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.116	Microsoft Directory Services
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.216	Microsoft Directory Services
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.222	DNS - Domain Name System
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.231	79\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		114.248.62.136	Kazaa
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		114.248.62.136	PPTP - Point-to-Point Tunneling Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		118.200.95.244	GNUTELLA-RTR
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.118	UPS - Uninterruptible Power Supply
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		105.114.60.223	BOOTP - Server
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		110.49.174.190	Syslog - System Logging Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		119.84.138.21	End Point Mapper
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		104.83.105.39	MSSQL - SQL Server Monitor
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		114.17.192.178	IBM Lotus Notes/Domino RPC
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		66.2.30.9	Finger
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.215	DNS - Domain Name System
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.248	MSSQL - SQL Server Database
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		107.180.80.203	UPS - Uninterruptible Power Supply
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		113.159.109.25	GNUTELLA-RTR

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		119.166.129.99	5800\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.111	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.112	TFTP - Trivial File Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.207	MSSQL - SQL Server Monitor
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.245	MSSQL - SQL Server Database
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.250	MSSQL - SQL Server Database
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		114.128.130.118	HTTP - Hypertext Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		66.2.30.6	TFTP - Trivial File Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.201	119\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.248	110\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.253	Syslog - System Logging Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		112.211.5.54	111\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		117.21.49.172	NetBIOS - Session Service
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		118.29.166.228	Microsoft Directory Services
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.107	AIM - AOL Instant Messenger
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.243	NNTP - Network News Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.247	111\
03/26/08 01:00 PM	03/26/08 03:00 PM	2.00	General Reconnaissance		118.95.82.196	110\
03/26/08 01:00 PM	03/28/08 10:00 AM	2.00	General Reconnaissance		88.69.1.224	LDAP - Lightweight Directory Access Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		111.103.27.70	WLM/MSM - Windows Live Messenger
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.244	IMAP - Internet Message Access Protocol
03/26/08 02:00 PM	03/27/08 04:00 PM	2.00	General Reconnaissance		119.135.23.192	NetBIOS - Datagram
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		107.75.39.135	NetBIOS - Name Service
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		110.105.176.46	MSSQL - SQL Server Monitor
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		112.211.5.54	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		115.23.161.181	111\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.231	GNUTELLA-RTR
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.233	BOOTP - Server
03/26/08 03:00 PM	03/28/08 08:00 AM	2.00	General Reconnaissance		88.69.1.218	Syslog - System Logging Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		106.87.12.123	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		113.215.126.48	IMAP - Internet Message Access Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		113.95.99.218	NetBIOS - Datagram
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		106.71.210.209	NNTP - Network News Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		66.2.30.10	IMAP - Internet Message Access Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		66.2.30.8	TFTP - Trivial File Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.203	Kazaa
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.208	IMAP - Internet Message Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		112.236.131.84	NetBIOS - Session Service
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		103.44.13.181	IMAP - Internet Message Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		105.96.101.72	UPS - Uninterruptible Power Supply
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		106.41.42.164	BOOTP - Server
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		111.36.131.245	End Point Mapper
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		117.180.12.105	Kazaa
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		119.157.88.38	NetBIOS - Name Service
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		119.84.138.21	MySQL Database System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.212	GNUTELLA-RTR
03/26/08 06:00 PM	03/27/08 09:00 PM	2.00	General Reconnaissance		88.69.1.222	DNS - Domain Name System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Compromise		66.2.30.5	WLM/MSM - Windows Live Messenger
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Compromise		88.69.1.249	111\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		104.151.242.62	DNS - Domain Name System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		109.129.58.157	Microsoft Directory Services
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		110.49.174.190	HTTP - Hypertext Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		110.91.38.179	Kazaa
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		72.99.11.102	MSSQL - SQL Server Monitor
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.207	Finger
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.247	5800\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		103.47.20.110	FTP Command
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		112.231.167.112	79\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		115.71.91.110	Finger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.113	8080\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.117	HTTPS - Secure HTTP
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.238	IMAP - Internet Message Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.247	DNS - Domain Name System
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Compromise		72.99.11.115	End Point Mapper
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		105.96.101.134	Finger
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		106.87.12.123	Microsoft Directory Services
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		110.173.225.94	MSSQL - SQL Server Database
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		112.236.131.84	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.200	GNUTELLA-RTR
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.248	NetBIOS - Session Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Compromise		107.180.80.203	POP3 - Post Office Protocol Version 3
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		101.136.167.138	Kazaa
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.15.241.93	End Point Mapper
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		119.166.129.99	TELNET
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		120.204.177.106	GNUTELLA Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.100	DNS - Domain Name System
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.101	Kazaa
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		88.69.1.213	Microsoft Directory Services
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		105.96.101.72	111\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		114.248.62.136	SSH - Secure Shell
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		116.13.132.192	MSSQL - SQL Server Monitor
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.210	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.233	SMTP - Simple Mail Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		88.69.1.217	5800\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		101.110.102.70	110\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		105.114.60.223	UPS - Uninterruptible Power Supply
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		106.41.42.164	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		111.195.14.150	HTTP - Hypertext Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		112.176.232.212	DNS - Domain Name System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.206	NetBIOS - Datagram
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.230	TFTP - Trivial File Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.240	X Window System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		88.69.1.234	POP3 - Post Office Protocol Version 3
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		111.195.14.150	X Window System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		66.2.30.2	DNS - Domain Name System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.200	SSH - Secure Shell
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.201	Microsoft Directory Services
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.207	8080\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		113.104.243.29	GNUTELLA Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		113.95.99.218	DNS - Domain Name System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		66.2.30.5	IMAP - Internet Message Access Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		102.116.230.67	BOOTP - Server
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		106.12.75.97	AIM - AOL Instant Messenger
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.219	TELNET
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.228	End Point Mapper
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.232	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.234	119\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.243	GNUTELLA-RTR
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.247	Syslog - System Logging Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		112.211.5.54	BOOTP - Client

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		112.231.167.112	DNS - Domain Name System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.109	GNUTELLA-RTR
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		103.44.13.181	5500\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		110.173.225.94	BOOTP - Client
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		110.56.252.33	NetBIOS - Name Service
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		112.236.131.84	IMAP - Internet Message Access Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		118.95.82.196	X Window System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.217	UPS - Uninterruptible Power Supply
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.252	111\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		105.114.60.223	PPTP - Point-to-Point Tunneling Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		108.124.40.121	IMAP - Internet Message Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.250	LDAP - Lightweight Directory Access Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		103.47.20.110	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		107.75.39.135	NNTP - Network News Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		110.105.176.46	UPS - Uninterruptible Power Supply
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		118.190.70.171	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.102	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.211	79\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.225	End Point Mapper
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		103.47.20.110	HTTP - Hypertext Transfer Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		116.96.74.233	MSSQL - SQL Server Database
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		72.99.11.104	UPS - Uninterruptible Power Supply
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.231	119\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.238	UPS - Uninterruptible Power Supply
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Compromise		105.248.16.99	MSSQL - SQL Server Monitor

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		112.229.146.63	WLM/MSM - Windows Live Messenger
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		114.128.130.118	GNUTELLA Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		116.76.60.122	End Point Mapper
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.207	IBM Lotus Notes/Domino RPC
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.229	Finger
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.252	8080\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.252	NetBIOS - Session Service
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		101.136.167.138	TELNET
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		116.13.132.192	SSH - Secure Shell
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.103	PPTP - Point-to-Point Tunneling Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.212	Microsoft Directory Services
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.248	Syslog - System Logging Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.252	End Point Mapper
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		88.69.1.224	PPTP - Point-to-Point Tunneling Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		107.75.39.135	IMAP - Internet Message Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		109.105.181.83	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		116.96.74.233	BOOTP - Client
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.100	BOOTP - Client
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		106.12.75.97	IMAP - Internet Message Access Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		111.103.215.210	HTTP - Hypertext Transfer Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		72.99.11.100	WLM/MSM - Windows Live Messenger
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		72.99.11.101	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.218	IBM Lotus Notes/Domino RPC
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		105.241.215.112	End Point Mapper
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		106.178.103.206	HTTP - Hypertext Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		110.49.174.190	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		112.236.131.84	IBM Lotus Notes/Domino RPC
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		115.191.101.229	End Point Mapper
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.1	GNUTELLA-RTR
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.203	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Compromise		109.138.207.137	IMAP - Internet Message Access Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		102.27.84.33	119\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		106.160.138.40	TFTP - Trivial File Transfer Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		117.180.12.105	8080\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		101.110.102.70	UPS - Uninterruptible Power Supply
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		101.138.232.109	TFTP - Trivial File Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		106.87.12.123	SSH - Secure Shell
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		114.229.222.106	BOOTP - Client
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.227	BOOTP - Client
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Compromise		72.99.11.102	Microsoft Directory Services
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		103.44.13.181	FTP Command
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		106.12.75.97	79\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		106.178.103.206	NetBIOS - Session Service
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		110.105.176.46	79\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		111.195.14.150	8080\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.213	IMAP - Internet Message Access Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.229	UPS - Uninterruptible Power Supply
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Compromise		88.69.1.230	GNUTELLA Service
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		109.105.181.83	SMTP - Simple Mail Transfer Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		109.129.58.157	LDAP - Lightweight Directory Access Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		112.176.232.212	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.119	LDAP - Lightweight Directory Access Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.203	SMTP - Simple Mail Transfer Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Compromise		88.69.1.249	SMTP - Simple Mail Transfer Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		118.95.82.196	GNUTELLA-RTR
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		66.2.30.5	BOOTP - Client
03/27/08 06:00 PM	03/28/08 04:00 AM	2.00	General Reconnaissance		72.99.11.103	79\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		106.12.75.97	111\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		111.103.27.70	POP3 - Post Office Protocol Version 3
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		114.128.130.118	LDAP - Lightweight Directory Access Protocol Finger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		119.135.23.192	End Point Mapper
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.202	MySQL Database System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		102.27.84.33	End Point Mapper
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		112.231.167.112	PPTP - Point-to-Point Tunneling Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		113.159.109.25	WLM/MSM - Windows Live Messenger
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.223	5800\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		107.75.39.135	GNUTELLA Service
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		111.103.27.70	AIM - AOL Instant Messenger
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		72.99.11.103	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.217	UPS - Uninterruptible Power Supply
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.250	NetBIOS - Session Service
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		106.12.75.97	GNUTELLA Service
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		110.76.158.164	GNUTELLA-RTR
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		114.248.62.136	LDAP - Lightweight Directory Access Protocol Finger
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.208	SMTP - Simple Mail Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Compromise		112.229.146.63	
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		110.91.38.179	

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		112.231.167.112	UPS - Uninterruptible Power Supply
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		119.135.23.192	79\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		72.99.11.111	NetBIOS - Datagram
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.218	SMTP - Simple Mail Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.237	79\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.251	LDAP - Lightweight Directory Access Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Compromise		109.5.43.42	MSSQL - SQL Server Database
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Compromise		110.91.38.179	111\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		111.36.131.245	NetBIOS - Datagram
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		113.53.48.148	HTTPS - Secure HTTP
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		119.84.138.21	5800\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		66.2.30.8	Microsoft Directory Services
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		72.99.11.116	PPTP - Point-to-Point Tunneling Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.244	TELNET
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		103.242.202.177	Kazaa
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		103.47.20.110	HTTPS - Secure HTTP
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		105.114.60.223	WLM/MSM - Windows Live Messenger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		107.75.39.135	End Point Mapper
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		112.211.5.54	End Point Mapper
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		66.2.30.7	HTTPS - Secure HTTP
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		72.99.11.108	SMTP - Simple Mail Transfer Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		72.99.11.117	119\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		106.41.42.164	MSSQL - SQL Server Database
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		113.198.41.205	Microsoft Directory Services
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		116.96.74.233	Finger
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.211	MySQL Database System
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.218	111\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.226	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Compromise		113.198.41.205	Microsoft Directory Services
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		105.114.60.223	LDAP - Lightweight Directory Access Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		107.75.39.135	SSH - Secure Shell
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		119.166.129.99	TFTP - Trivial File Transfer Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.228	HTTP - Hypertext Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		102.116.230.67	GNUTELLA Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		113.215.126.48	LDAP - Lightweight Directory Access Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		114.229.222.106	LDAP - Lightweight Directory Access Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		117.83.247.204	Microsoft Directory Services
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.206	End Point Mapper
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.233	TELNET
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		72.99.11.107	MSSQL - SQL Server Monitor
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		112.26.27.203	WLM/MSM - Windows Live Messenger
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		66.2.30.7	111\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.215	111\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Compromise		72.99.11.107	PPTP - Point-to-Point Tunneling Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		102.116.230.67	UPS - Uninterruptible Power Supply
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		106.178.103.206	NetBIOS - Name Service
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		112.250.231.58	LDAP - Lightweight Directory Access Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		118.190.70.171	111\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		118.66.66.46	AIM - AOL Instant Messenger
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.243	SSH - Secure Shell
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.250	NetBIOS - Name Service
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		105.248.16.99	IBM Lotus Notes/Domino RPC
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		113.104.243.29	110\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		120.138.126.247	WLM/MSM - Windows Live Messenger
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.201	PPTP - Point-to-Point Tunneling Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.246	BOOTP - Client
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.252	BOOTP - Server
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Compromise		102.116.230.67	MySQL Database System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Compromise		107.180.80.203	IMAP - Internet Message Access Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		109.105.181.83	Microsoft Directory Services
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		112.250.231.58	IMAP - Internet Message Access Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		115.23.161.181	DNS - Domain Name System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		118.200.95.244	IMAP - Internet Message Access Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.224	HTTP - Hypertext Transfer Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.234	MSSQL - SQL Server Monitor
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		103.253.172.4	110\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		109.138.207.137	SMTP - Simple Mail Transfer Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.117	Microsoft Directory Services
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.234	End Point Mapper
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		116.13.132.192	End Point Mapper
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		88.69.1.232	111\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		101.88.139.234	MySQL Database System
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		102.27.84.33	GNUTELLA Service
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		105.219.149.191	GNUTELLA-RTR
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		105.243.17.16	Syslog - System Logging Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		105.96.101.72	TFTP - Trivial File Transfer Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.235	MSSQL - SQL Server Monitor
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.244	GNUTELLA-RTR
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.245	5800\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.8</b>						
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.246	NetBIOS - Name Service
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		117.21.49.172	5800\
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.203	Finger
<b>161.200.1.9</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		117.83.247.204	Kazaa
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		117.180.12.105	8080\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		66.2.30.10	HTTP - Hypertext Transfer Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		66.2.30.2	NNTP - Network News Transfer Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		66.2.30.9	TELNET
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		72.99.11.115	PPTP - Point-to-Point Tunneling Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.206	110\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.219	BOOTP - Client
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.231	5800\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		110.105.176.46	NetBIOS - Datagram
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		114.248.62.136	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		116.13.132.192	IBM Lotus Notes/Domino RPC
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.110	Microsoft Directory Services
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.115	POP3 - Post Office Protocol Version 3
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.116	MySQL Database System
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.234	TFTP - Trivial File Transfer Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		106.12.75.97	IBM Lotus Notes/Domino RPC
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		111.195.14.150	NetBIOS - Datagram
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		119.166.129.99	119\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		119.29.250.161	NetBIOS - Session Service
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.223	FTP Command
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.248	IMAP - Internet Message Access Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Compromise		106.87.12.123	POP3 - Post Office Protocol Version 3

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		112.229.146.63	HTTP - Hypertext Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		116.13.132.192	111\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.116	NetBIOS - Session Service
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.216	Syslog - System Logging Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.239	GNUTELLA Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		106.41.42.164	Microsoft Directory Services
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		110.195.212.97	DNS - Domain Name System
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		112.250.231.58	NetBIOS - Name Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		116.13.132.192	NetBIOS - Datagram
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.109	Microsoft Directory Services
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.112	TELNET
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.216	79\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		113.95.99.218	AIM - AOL Instant Messenger
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		114.248.62.136	Microsoft Directory Services
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		72.99.11.114	Finger
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.203	SMTP - Simple Mail Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.209	WLM/MSM - Windows Live Messenger
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.210	HTTPS - Secure HTTP
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.234	GNUTELLA-RTR
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Compromise		88.69.1.209	WLM/MSM - Windows Live Messenger
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		110.76.158.164	BOOTP - Client
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		118.19.112.193	8080\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		119.31.164.89	NNTP - Network News Transfer Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		72.99.11.104	LDAP - Lightweight Directory Access Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.203	DNS - Domain Name System
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.204	End Point Mapper
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.247	Microsoft Directory Services

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		117.21.49.172	8080\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.111	NetBIOS - Name Service
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.205	Finger
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.210	MSSQL - SQL Server Database
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.213	UPS - Uninterruptible Power Supply
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.235	NNTP - Network News Transfer Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.239	5800\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		101.110.102.70	SMTP - Simple Mail Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		105.96.101.134	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		112.211.5.54	111\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		112.231.167.112	Microsoft Directory Services
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		119.157.88.38	BOOTP - Server
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.252	NetBIOS - Datagram
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Compromise		88.69.1.223	5800\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		106.87.12.123	IMAP - Internet Message Access Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.102	UPS - Uninterruptible Power Supply
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.207	SMTP - Simple Mail Transfer Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.227	UPS - Uninterruptible Power Supply
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Compromise		72.99.11.115	NNTP - Network News Transfer Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		103.253.172.4	TFTP - Trivial File Transfer Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.112	GNUTELLA Service
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.113	HTTP - Hypertext Transfer Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.115	111\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.244	DNS - Domain Name System
03/26/08 10:00 AM	03/28/08 07:00 AM	2.00	General Reconnaissance		106.71.210.209	HTTPS - Secure HTTP
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Compromise		106.160.138.40	MySQL Database System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		107.180.80.203	NNTP - Network News Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		114.17.192.178	8080\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		118.19.112.193	NetBIOS - Session Service
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		118.95.82.196	MySQL Database System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.102	POP3 - Post Office Protocol Version 3
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.106	FTP Command
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.253	LDAP - Lightweight Directory Access Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Compromise		120.138.126.247	MySQL Database System
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		112.211.5.54	SMTP - Simple Mail Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		114.183.253.86	BOOTP - Server
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.229	GNUTELLA-RTR
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.231	111\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		105.114.60.223	111\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		109.117.125.53	NetBIOS - Session Service
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		109.129.58.157	Microsoft Directory Services
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.247	UPS - Uninterruptible Power Supply
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		101.110.102.70	119\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		104.83.105.39	MSSQL - SQL Server Database
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		105.241.215.112	5800\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		112.211.5.54	GNUTELLA-RTR
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		114.128.130.118	Microsoft Directory Services
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		72.99.11.114	FTP Command
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.211	BOOTP - Client
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.225	NetBIOS - Session Service
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		104.83.105.39	BOOTP - Server
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		106.23.8.82	WLM/MSM - Windows Live Messenger
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		106.71.210.209	End Point Mapper
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		108.103.69.15	110\

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.100	AIM - AOL Instant Messenger
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.206	DNS - Domain Name System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.224	NetBIOS - Session Service
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		106.12.75.97	Microsoft Directory Services
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		110.76.158.164	Microsoft Directory Services
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		110.76.158.164	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		118.19.112.193	IMAP - Internet Message Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.119	MSSQL - SQL Server Monitor
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		106.12.75.97	TELNET
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		108.124.40.121	LDAP - Lightweight Directory Access Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		114.229.222.106	NetBIOS - Session Service
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		120.204.177.106	MSSQL - SQL Server Database
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		72.99.11.111	Syslog - System Logging Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		88.69.1.243	PPTP - Point-to-Point Tunneling Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		104.83.105.39	NetBIOS - Datagram
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		106.12.75.97	BOOTP - Client
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		111.103.215.210	GNUTELLA-RTR
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		114.17.192.178	SMTP - Simple Mail Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		118.15.241.93	NetBIOS - Name Service
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		118.66.66.46	X Window System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		119.135.23.192	79\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		66.2.30.6	DNS - Domain Name System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.234	HTTP - Hypertext Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.252	PPTP - Point-to-Point Tunneling Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		106.160.138.40	NetBIOS - Session Service
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		111.36.131.245	Kazaa

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		119.25.113.70	BOOTP - Server
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.221	End Point Mapper
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		102.27.84.33	TFTP - Trivial File Transfer Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		103.199.117.191	End Point Mapper
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		112.176.232.212	UPS - Uninterruptible Power Supply
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		112.211.5.54	111\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		119.25.113.70	DNS - Domain Name System
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.202	Microsoft Directory Services
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.217	UPS - Uninterruptible Power Supply
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.241	Syslog - System Logging Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		103.199.117.191	IMAP - Internet Message Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.204	Syslog - System Logging Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.233	NetBIOS - Name Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		106.160.138.40	79\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		109.105.181.83	X Window System
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		110.195.212.97	5800\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		113.53.48.148	NNTP - Network News Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.95.82.196	UPS - Uninterruptible Power Supply
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		66.2.30.7	IBM Lotus Notes/Domino RPC
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.225	UPS - Uninterruptible Power Supply
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.231	NetBIOS - Session Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.242	IMAP - Internet Message Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		106.41.42.164	Syslog - System Logging Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		116.13.132.192	SMTP - Simple Mail Transfer Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		120.138.126.247	HTTP - Hypertext Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.110	NetBIOS - Name Service
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.232	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		109.5.43.42	WLM/MSM - Windows Live Messenger
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		110.56.252.33	UPS - Uninterruptible Power Supply
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.105	IMAP - Internet Message Access Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.105	X Window System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.247	Finger
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		88.69.1.227	5800\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		102.27.84.33	MySQL Database System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		105.248.16.99	SMTP - Simple Mail Transfer Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		107.197.4.193	8080\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		115.111.20.104	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.110	Syslog - System Logging Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.245	SMTP - Simple Mail Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		104.151.242.62	IBM Lotus Notes/Domino RPC
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		106.71.210.209	MySQL Database System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		112.231.167.112	119\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		66.2.30.10	SSH - Secure Shell
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		66.2.30.6	Finger
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.205	NetBIOS - Name Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.206	NNTP - Network News Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.212	119\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.218	UPS - Uninterruptible Power Supply
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		118.15.241.93	IBM Lotus Notes/Domino RPC
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.111	End Point Mapper
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.229	BOOTP - Server
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.235	Finger
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.238	Finger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.240	110\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.243	X Window System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		105.248.16.99	110\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		119.31.164.89	111\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		101.138.232.109	End Point Mapper
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		106.178.103.206	PPTP - Point-to-Point Tunneling Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		109.117.125.53	Kazaa
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		116.76.60.122	MSSQL - SQL Server Monitor
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.107	End Point Mapper
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		101.136.167.138	MySQL Database System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		106.160.138.40	8080\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		109.138.207.137	MSSQL - SQL Server Monitor
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		72.99.11.104	FTP Command
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.226	Microsoft Directory Services
03/27/08 05:00 AM	03/27/08 02:00 PM	2.00	General Reconnaissance		102.27.84.33	5500\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		103.242.202.177	X Window System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		119.29.250.161	5500\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		103.242.202.177	79\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		105.219.149.191	X Window System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		105.248.16.99	8080\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		106.148.54.20	DNS - Domain Name System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		106.23.8.82	Microsoft Directory Services
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		110.49.174.190	FTP Command
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		66.2.30.7	GNUTELLA Service
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.219	NetBIOS - Datagram
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.242	8080\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		101.138.232.109	FTP Command
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		105.148.92.222	SSH - Secure Shell
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		105.241.215.112	IMAP - Internet Message Access Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		106.148.54.20	HTTPS - Secure HTTP
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		113.95.99.218	MySQL Database System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		72.99.11.119	POP3 - Post Office Protocol Version 3
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.214	AIM - AOL Instant Messenger
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.231	Microsoft Directory Services
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.232	IMAP - Internet Message Access Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Compromise		88.69.1.230	HTTP - Hypertext Transfer Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		108.103.69.15	SSH - Secure Shell
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		112.231.167.112	HTTP - Hypertext Transfer Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		113.198.41.205	5800\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.235	UPS - Uninterruptible Power Supply
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Compromise		115.23.161.181	111\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		103.253.172.4	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		112.231.167.112	NetBIOS - Datagram
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.119	TELNET
03/27/08 10:00 AM	03/27/08 12:00 PM	2.00	General Reconnaissance		107.75.39.135	NetBIOS - Name Service
03/27/08 10:00 AM	03/27/08 03:00 PM	2.00	General Reconnaissance		72.99.11.113	119\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		105.96.101.134	IMAP - Internet Message Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		105.248.16.99	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		66.2.30.5	NNTP - Network News Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		66.2.30.9	BOOTP - Client
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.118	5500\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.234	SMTP - Simple Mail Transfer Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		106.12.75.97	UPS - Uninterruptible Power Supply
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		106.23.8.82	LDAP - Lightweight Directory Access Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		106.87.12.123	SMTP - Simple Mail Transfer Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		118.19.112.193	TELNET

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		66.2.30.4	GNUTELLA-RTR
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		72.99.11.117	MSSQL - SQL Server Monitor
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.202	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.233	IBM Lotus Notes/Domino RPC
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.248	Syslog - System Logging Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.248	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Compromise		107.240.248.102	BOOTP - Client
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		107.180.80.203	NetBIOS - Session Service
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		107.25.150.43	X Window System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		115.23.161.181	8080\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		72.99.11.119	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.218	LDAP - Lightweight Directory Access Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		106.12.75.97	POP3 - Post Office Protocol Version 3
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		110.173.225.94	HTTPS - Secure HTTP
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		120.204.177.106	LDAP - Lightweight Directory Access Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.118	UPS - Uninterruptible Power Supply
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.218	FTP Command
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.250	Finger
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		88.69.1.214	X Window System
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		107.197.4.193	BOOTP - Client
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.218	MySQL Database System
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.250	TFTP - Trivial File Transfer Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		105.96.101.72	5500\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		110.195.212.97	Microsoft Directory Services
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		115.135.147.74	X Window System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		66.2.30.2	MySQL Database System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.247	110\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.253	PPTP - Point-to-Point Tunneling Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		106.12.75.97	TELNET
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		107.75.39.135	DNS - Domain Name System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		109.105.181.83	HTTP - Hypertext Transfer Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		109.129.58.157	X Window System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.105	MSSQL - SQL Server Monitor
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.201	GNUTELLA Service
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.230	UPS - Uninterruptible Power Supply
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		101.110.102.70	NNTP - Network News Transfer Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		118.200.95.244	UPS - Uninterruptible Power Supply
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		120.138.126.247	Microsoft Directory Services
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		72.99.11.119	DNS - Domain Name System
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.219	GNUTELLA-RTR
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.245	SSH - Secure Shell
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		112.236.131.84	HTTP - Hypertext Transfer Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		113.215.126.48	WLM/MSM - Windows Live Messenger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		118.29.166.228	TELNET
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.116	WLM/MSM - Windows Live Messenger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.238	X Window System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		106.23.8.82	110\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.213	5800\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		88.69.1.215	NNTP - Network News Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		105.96.101.72	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		107.25.150.43	AIM - AOL Instant Messenger
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		112.211.5.54	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.220	WLM/MSM - Windows Live Messenger
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.251	IMAP - Internet Message Access Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		105.248.16.99	WLM/MSM - Windows Live Messenger
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		106.160.138.40	UPS - Uninterruptible Power Supply
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		112.231.167.112	UPS - Uninterruptible Power Supply
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		115.191.101.229	IMAP - Internet Message Access Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		119.84.138.21	TELNET
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.119	BOOTP - Server
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.202	FTP Command
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.218	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		103.44.13.181	TELNET
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		103.47.20.110	SMTP - Simple Mail Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		104.83.105.39	5500\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		105.219.149.191	NetBIOS - Session Service
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		109.129.58.157	Microsoft Directory Services
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		111.195.14.150	BOOTP - Server
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		117.83.247.204	111\
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.222	Finger
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.225	NetBIOS - Name Service
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		116.13.132.192	5500\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		118.29.166.228	8080\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		72.99.11.113	LDAP - Lightweight Directory Access Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		103.242.202.177	IBM Lotus Notes/Domino RPC
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		107.197.4.193	AIM - AOL Instant Messenger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		110.173.225.94	NetBIOS - Name Service
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		66.2.30.10	DNS - Domain Name System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		66.2.30.3	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Compromise		116.76.60.122	AIM - AOL Instant Messenger
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		105.219.149.191	110\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		108.124.40.121	IMAP - Internet Message Access Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		116.76.60.122	IBM Lotus Notes/Domino RPC
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.200	NetBIOS - Datagram
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.214	POP3 - Post Office Protocol Version 3
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.228	Kazaa
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.248	TFTP - Trivial File Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.252	5800\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		104.151.242.62	PPTP - Point-to-Point Tunneling Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		106.148.54.20	IBM Lotus Notes/Domino RPC
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		114.17.192.178	NetBIOS - Session Service
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		72.99.11.101	End Point Mapper
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.209	Syslog - System Logging Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.235	111\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Compromise		66.2.30.10	DNS - Domain Name System
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		103.199.117.191	5800\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.202	TELNET
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.223	AIM - AOL Instant Messenger
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		119.84.138.21	IMAP - Internet Message Access Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.101	NNTP - Network News Transfer Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		107.240.248.102	AIM - AOL Instant Messenger
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		107.75.39.135	Syslog - System Logging Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		109.5.43.42	Microsoft Directory Services
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		117.180.12.105	111\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		118.95.82.196	5500\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.111	IMAP - Internet Message Access Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.229	PPTP - Point-to-Point Tunneling Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.231	111\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.238	GNUTELLA-RTR
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		109.117.125.53	5500\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		114.128.130.118	TELNET
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		66.2.30.6	X Window System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.106	GNUTELLA-RTR
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.116	BOOTP - Server
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.216	NetBIOS - Datagram
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		105.219.149.191	SMTP - Simple Mail Transfer Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		109.138.207.137	LDAP - Lightweight Directory Access Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		111.195.14.150	MySQL Database System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		112.229.146.63	5500\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		118.66.66.46	8080\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		120.138.126.247	WLM/MSM - Windows Live Messenger
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.119	Syslog - System Logging Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.120	8080\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.202	IBM Lotus Notes/Domino RPC
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.212	DNS - Domain Name System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.245	Microsoft Directory Services
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Compromise		88.69.1.246	MSSQL - SQL Server Monitor
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		109.105.181.83	110\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		113.159.109.25	IMAP - Internet Message Access Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.107	LDAP - Lightweight Directory Access Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.110	LDAP - Lightweight Directory Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>161.200.1.9</b>						
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.243	SMTP - Simple Mail Transfer Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		119.157.88.38	8080\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		103.242.202.177	SMTP - Simple Mail Transfer Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		110.91.38.179	SSH - Secure Shell
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		113.198.41.205	DNS - Domain Name System
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		66.2.30.2	IMAP - Internet Message Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.214	IBM Lotus Notes/Domino RPC
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.223	5800\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.234	BOOTP - Client
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Compromise		72.99.11.116	PPTP - Point-to-Point Tunneling Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		112.231.167.112	HTTPS - Secure HTTP
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		115.135.147.74	NNTP - Network News Transfer Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		118.66.66.46	NetBIOS - Datagram
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		72.99.11.104	Finger
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.220	5800\
<b>172.10.1.1</b>						
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		192.168.1.28	UPS - Uninterruptible Power Supply
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		userpc10	119\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		userpc16	MSSQL - SQL Server Monitor
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		192.168.1.6	111\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		192.168.1.19	POP3 - Post Office Protocol Version 3
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		userpc8	8080\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		192.168.1.2	SSH - Secure Shell
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.17	MySQL Database System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		192.168.1.24	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		192.168.1.8	HTTPS - Secure HTTP
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		userpc12	NNTP - Network News Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.1</b>						
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.24	MySQL Database System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		userpc12	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		192.168.1.12	Microsoft Directory Services
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		192.168.1.23	IMAP - Internet Message Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		userpc7	NetBIOS - Name Service
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		userpc12	NetBIOS - Session Service
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		192.168.1.32	POP3 - Post Office Protocol Version 3
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		192.168.1.6	5800\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		userpc7	MySQL Database System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		192.168.1.3	DNS - Domain Name System
<b>172.10.1.10</b>						
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		192.168.1.15	GNUTELLA-RTR
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		userpc13	POP3 - Post Office Protocol Version 3
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		192.168.1.19	NetBIOS - Session Service
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		192.168.1.29	End Point Mapper
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		192.168.1.9	LDAP - Lightweight Directory Access Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		192.168.1.27	110\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		192.168.1.6	119\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.32	110\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		userpc1	WLM/MSM - Windows Live Messenger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		userpc3	HTTPS - Secure HTTP
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		userpc5	Kazaa
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		userpc2	POP3 - Post Office Protocol Version 3
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.23	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		192.168.1.28	End Point Mapper
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		userpc6	5500\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.22	DNS - Domain Name System
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		192.168.1.2	111\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.10</b>						
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		192.168.1.33	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		192.168.1.32	UPS - Uninterruptible Power Supply
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		192.168.1.1	MSSQL - SQL Server Monitor
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		192.168.1.15	111\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		userpc8	79\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.22	IMAP - Internet Message Access Protocol
<b>172.10.1.11</b>						
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		userpc11	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		192.168.1.20	TFTP - Trivial File Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		192.168.1.8	AIM - AOL Instant Messenger
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		userpc9	111\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		userpc6	GNUTELLA-RTR
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		192.168.1.25	BOOTP - Client
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		192.168.1.11	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		192.168.1.29	End Point Mapper
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		192.168.1.18	POP3 - Post Office Protocol Version 3
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		userpc2	79\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		userpc7	TFTP - Trivial File Transfer Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.28	IBM Lotus Notes/Domino RPC
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		userpc15	Finger
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Compromise		192.168.1.25	NNTP - Network News Transfer Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		192.168.1.27	Finger
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Compromise		192.168.1.8	PPTP - Point-to-Point Tunneling Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		192.168.1.17	POP3 - Post Office Protocol Version 3
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		192.168.1.17	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.11</b>						
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		userpc13	79\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		userpc15	End Point Mapper
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		userpc8	MSSQL - SQL Server Database
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		192.168.1.26	TFTP - Trivial File Transfer Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.33	NNTP - Network News Transfer Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		userpc10	IBM Lotus Notes/Domino RPC
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		192.168.1.28	111\
<b>172.10.1.12</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.6	End Point Mapper
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		userpc7	TELNET
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		192.168.1.6	MSSQL - SQL Server Database
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		userpc15	119\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		userpc11	Finger
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		userpc14	Kazaa
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		192.168.1.15	Microsoft Directory Services
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.26	GNUTELLA Service
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		userpc1	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		userpc9	119\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		192.168.1.31	POP3 - Post Office Protocol Version 3
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		userpc16	MSSQL - SQL Server Monitor
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.2	SMTP - Simple Mail Transfer Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.25	LDAP - Lightweight Directory Access Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		192.168.1.23	IMAP - Internet Message Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		192.168.1.9	X Window System
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		192.168.1.26	111\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		192.168.1.5	110\

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.12</b>						
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		userpc15	WLM/MSM - Windows Live Messenger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		192.168.1.11	Microsoft Directory Services
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		192.168.1.7	UPS - Uninterruptible Power Supply
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		192.168.1.17	PPTP - Point-to-Point Tunneling Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		userpc10	NetBIOS - Session Service
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		userpc7	IMAP - Internet Message Access Protocol
<b>172.10.1.13</b>						
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		192.168.1.4	BOOTP - Client
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.17	GNUTELLA Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		userpc7	NNTP - Network News Transfer Protocol
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		192.168.1.33	Microsoft Directory Services
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		userpc15	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.16	8080\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		userpc14	79\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		userpc10	End Point Mapper
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		192.168.1.20	MSSQL - SQL Server Monitor
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		192.168.1.2	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		userpc6	BOOTP - Client
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		192.168.1.4	HTTPS - Secure HTTP
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		192.168.1.12	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		192.168.1.16	DNS - Domain Name System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		192.168.1.23	NNTP - Network News Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		userpc2	LDAP - Lightweight Directory Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		userpc7	5500\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		userpc7	IMAP - Internet Message Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.13</b>						
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		192.168.1.27	8080\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		192.168.1.33	IMAP - Internet Message Access Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.33	IMAP - Internet Message Access Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.9	Syslog - System Logging Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		192.168.1.30	PPTP - Point-to-Point Tunneling Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		userpc10	IMAP - Internet Message Access Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		192.168.1.26	AIM - AOL Instant Messenger
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		userpc14	SMTP - Simple Mail Transfer Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		192.168.1.3	AIM - AOL Instant Messenger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		192.168.1.30	HTTPS - Secure HTTP
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		userpc8	GNUTELLA Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		userpc5	Microsoft Directory Services
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		192.168.1.20	GNUTELLA Service
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		192.168.1.5	SMTP - Simple Mail Transfer Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		userpc12	LDAP - Lightweight Directory Access Protocol
<b>172.10.1.14</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.6	119\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		userpc8	MSSQL - SQL Server Database
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.33	X Window System
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		192.168.1.2	110\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		192.168.1.33	110\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		userpc14	UPS - Uninterruptible Power Supply
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		userpc3	119\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		userpc4	NNTP - Network News Transfer Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.14</b>						
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		userpc1	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		192.168.1.3	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		userpc9	BOOTP - Client
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.3	End Point Mapper
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		userpc3	110\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		192.168.1.27	BOOTP - Client
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.13	Finger
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		192.168.1.12	Finger
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		192.168.1.20	IMAP - Internet Message Access Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		192.168.1.24	End Point Mapper
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		192.168.1.29	FTP Command
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		192.168.1.17	End Point Mapper
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		192.168.1.25	NetBIOS - Datagram
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.15	IBM Lotus Notes/Domino RPC
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		192.168.1.32	UPS - Uninterruptible Power Supply
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		192.168.1.4	IMAP - Internet Message Access Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.30	UPS - Uninterruptible Power Supply
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		192.168.1.10	DNS - Domain Name System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		192.168.1.17	IMAP - Internet Message Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		192.168.1.1	HTTP - Hypertext Transfer Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		userpc12	MSSQL - SQL Server Database
<b>172.10.1.15</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.1	HTTPS - Secure HTTP
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.10	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.12	GNUTELLA-RTR
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.3	FTP Command

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.15</b>						
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		192.168.1.8	SMTP - Simple Mail Transfer Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		192.168.1.32	5500\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		192.168.1.6	IMAP - Internet Message Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		192.168.1.16	End Point Mapper
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Compromise		userpc8	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.9	End Point Mapper
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		userpc7	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		192.168.1.9	8080\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.22	BOOTP - Server
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		userpc7	111\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		userpc2	End Point Mapper
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.12	IMAP - Internet Message Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		userpc8	MSSQL - SQL Server Monitor
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.25	UPS - Uninterruptible Power Supply
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		userpc6	BOOTP - Server
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		userpc7	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		192.168.1.29	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		192.168.1.16	AIM - AOL Instant Messenger
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.16	5500\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		192.168.1.25	PPTP - Point-to-Point Tunneling Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		192.168.1.5	FTP Command
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.28	SMTP - Simple Mail Transfer Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		192.168.1.16	NetBIOS - Datagram
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		192.168.1.6	FTP Command
<b>172.10.1.16</b>						
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		192.168.1.25	FTP Command
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		192.168.1.31	BOOTP - Client

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.16</b>						
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		192.168.1.24	79\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		192.168.1.9	NetBIOS - Name Service
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		userpc8	DNS - Domain Name System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.25	POP3 - Post Office Protocol Version 3
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.9	HTTPS - Secure HTTP
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		userpc6	WLM/MSM - Windows Live Messenger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		userpc7	MSSQL - SQL Server Database
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		192.168.1.16	DNS - Domain Name System
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		192.168.1.33	HTTP - Hypertext Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		userpc11	NNTP - Network News Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		userpc13	79\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		192.168.1.5	119\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		userpc5	IBM Lotus Notes/Domino RPC
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		192.168.1.8	Microsoft Directory Services
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		192.168.1.6	X Window System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.8	TELNET
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		userpc5	UPS - Uninterruptible Power Supply
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		192.168.1.19	MSSQL - SQL Server Monitor
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		192.168.1.9	TELNET
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		userpc1	HTTPS - Secure HTTP
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		userpc1	WLM/MSM - Windows Live Messenger
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		192.168.1.14	End Point Mapper
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.13	GNUTELLA Service
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		192.168.1.7	Microsoft Directory Services
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		192.168.1.22	Syslog - System Logging Protocol

### 172.10.1.17

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.17</b>						
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		192.168.1.11	NetBIOS - Name Service
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		192.168.1.2	NetBIOS - Name Service
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		192.168.1.17	TELNET
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Compromise		192.168.1.24	SSH - Secure Shell
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.1	FTP Command
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		192.168.1.24	GNUTELLA-RTR
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		userpc5	MSSQL - SQL Server Database
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		192.168.1.20	NetBIOS - Datagram
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		192.168.1.4	DNS - Domain Name System
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.8	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		192.168.1.25	UPS - Uninterruptible Power Supply
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		userpc12	IMAP - Internet Message Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		userpc6	POP3 - Post Office Protocol Version 3
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		192.168.1.11	Finger
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		userpc3	79\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		192.168.1.6	LDAP - Lightweight Directory Access Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Compromise		userpc7	NetBIOS - Session Service
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.24	8080\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.8	POP3 - Post Office Protocol Version 3
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.9	Finger
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		192.168.1.20	110\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Compromise		192.168.1.1	WLM/MSM - Windows Live Messenger
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		192.168.1.8	IBM Lotus Notes/Domino RPC
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		userpc4	119\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		192.168.1.32	110\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		userpc16	HTTPS - Secure HTTP
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		userpc11	UPS - Uninterruptible Power Supply
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		userpc4	SMTP - Simple Mail Transfer Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.17</b>						
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		userpc8	5500\
<b>172.10.1.18</b>						
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		userpc2	NetBIOS - Datagram
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		192.168.1.17	DNS - Domain Name System
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		userpc11	BOOTP - Client
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		userpc7	HTTPS - Secure HTTP
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		192.168.1.8	79\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		userpc13	79\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		192.168.1.15	TFTP - Trivial File Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		192.168.1.4	MySQL Database System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		userpc2	End Point Mapper
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.18	8080\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.29	MSSQL - SQL Server Database
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		192.168.1.4	PPTP - Point-to-Point Tunneling Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		userpc1	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.31	TELNET
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		192.168.1.17	MySQL Database System
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		192.168.1.20	TELNET
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		192.168.1.25	End Point Mapper
<b>172.10.1.19</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.20	GNUTELLA Service
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.32	HTTP - Hypertext Transfer Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		userpc4	HTTPS - Secure HTTP
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		192.168.1.6	NetBIOS - Session Service
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		userpc9	119\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		192.168.1.10	119\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		192.168.1.21	BOOTP - Client
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		192.168.1.20	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.26	111\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		userpc4	Microsoft Directory Services

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.19</b>						
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		192.168.1.4	GNUTELLA-RTR
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		userpc13	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		192.168.1.32	5800\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		192.168.1.1	Syslog - System Logging Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		192.168.1.21	5800\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		userpc10	X Window System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		userpc2	IBM Lotus Notes/Domino RPC
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.21	Microsoft Directory Services
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.10	SMTP - Simple Mail Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		userpc9	DNS - Domain Name System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		userpc15	119\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.14	GNUTELLA-RTR
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		192.168.1.13	Microsoft Directory Services
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		192.168.1.19	POP3 - Post Office Protocol Version 3
<b>172.10.1.2</b>						
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.12	FTP Command
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		userpc5	WLM/MMS - Windows Live Messenger
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		userpc1	AIM - AOL Instant Messenger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		192.168.1.22	FTP Command
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		192.168.1.31	NetBIOS - Name Service
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		192.168.1.26	X Window System
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		userpc16	BOOTP - Client
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Compromise		192.168.1.5	End Point Mapper
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		192.168.1.28	GNUTELLA-RTR
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		192.168.1.15	GNUTELLA-RTR
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		192.168.1.11	79\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		192.168.1.14	5500\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		192.168.1.7	DNS - Domain Name System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		192.168.1.24	111\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.2</b>						
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		192.168.1.28	111\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		192.168.1.27	111\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		192.168.1.31	BOOTP - Server
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		192.168.1.27	PPTP - Point-to-Point Tunneling Protocol
<b>172.10.1.20</b>						
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.28	110\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		192.168.1.16	X Window System
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		192.168.1.22	GNUTELLA Service
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		userpc16	79\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		userpc16	BOOTP - Server
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		192.168.1.22	Microsoft Directory Services
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		192.168.1.6	HTTPS - Secure HTTP
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.16	WLM/MSM - Windows Live Messenger
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		192.168.1.22	111\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		192.168.1.30	MSSQL - SQL Server Database
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		192.168.1.21	Kazaa
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.30	NetBIOS - Session Service
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		192.168.1.28	GNUTELLA Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		192.168.1.4	PPTP - Point-to-Point Tunneling Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		192.168.1.14	X Window System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		userpc9	5500\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		192.168.1.12	5800\
<b>172.10.1.3</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.2	GNUTELLA Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.17	111\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		192.168.1.14	POP3 - Post Office Protocol Version 3
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		userpc16	8080\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.28	HTTP - Hypertext Transfer Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		userpc9	UPS - Uninterruptible Power Supply

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.3</b>						
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		192.168.1.14	NetBIOS - Session Service
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		userpc15	NetBIOS - Datagram
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		userpc11	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		192.168.1.10	119\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		192.168.1.30	BOOTP - Server
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.16	Microsoft Directory Services
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.33	FTP Command
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Compromise		userpc13	End Point Mapper
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		userpc10	Syslog - System Logging Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		192.168.1.27	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.19	TELNET
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.21	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		userpc8	SSH - Secure Shell
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		192.168.1.29	111\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		userpc1	TELNET
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		192.168.1.33	NNTP - Network News Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		userpc3	SSH - Secure Shell
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		192.168.1.15	DNS - Domain Name System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.7	SSH - Secure Shell
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.30	GNUTELLA Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		userpc1	POP3 - Post Office Protocol Version 3
<b>172.10.1.4</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		userpc8	MSSQL - SQL Server Database
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		192.168.1.25	FTP Command
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		userpc2	IMAP - Internet Message Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		192.168.1.26	SSH - Secure Shell
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		192.168.1.14	5500\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		userpc13	FTP Command
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.15	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.4</b>						
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		userpc12	8080\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		192.168.1.4	TFTP - Trivial File Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		192.168.1.19	IMAP - Internet Message Access Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		192.168.1.20	NetBIOS - Session Service
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		userpc3	SSH - Secure Shell
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		192.168.1.11	SSH - Secure Shell
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Compromise		192.168.1.30	MySQL Database System
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		userpc9	POP3 - Post Office Protocol Version 3
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		192.168.1.13	GNUTELLA Service
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		192.168.1.13	Microsoft Directory Services
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		192.168.1.20	Finger
<b>172.10.1.5</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		userpc3	SMTP - Simple Mail Transfer Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		192.168.1.16	FTP Command
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Compromise		userpc5	End Point Mapper
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		192.168.1.31	8080\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		192.168.1.1	Kazaa
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		192.168.1.18	HTTPS - Secure HTTP
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		192.168.1.6	Microsoft Directory Services
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		userpc4	End Point Mapper
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		userpc2	8080\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		192.168.1.15	TELNET
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		192.168.1.32	AIM - AOL Instant Messenger
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		userpc15	HTTP - Hypertext Transfer Protocol
<b>172.10.1.6</b>						
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		192.168.1.3	TFTP - Trivial File Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		192.168.1.15	IMAP - Internet Message Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.6</b>						
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		192.168.1.25	Microsoft Directory Services
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		192.168.1.24	TELNET
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance	userpc1		NetBIOS - Session Service
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.19	AIM - AOL Instant Messenger
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.2	TELNET
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		192.168.1.15	DNS - Domain Name System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance	userpc10		Microsoft Directory Services
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance	userpc15		LDAP - Lightweight Directory Access Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance	userpc11		WLM/MSM - Windows Live Messenger
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance	userpc14		LDAP - Lightweight Directory Access Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Compromise		192.168.1.28	FTP Command
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Compromise		192.168.1.31	GNUTELLA Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.14	110\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.31	POP3 - Post Office Protocol Version 3
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.5	End Point Mapper
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance	userpc4		FTP Command
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance	userpc5		GNUTELLA Service
<b>172.10.1.7</b>						
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		192.168.1.32	NNTP - Network News Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		192.168.1.9	HTTP - Hypertext Transfer Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		192.168.1.6	GNUTELLA-RTR
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		192.168.1.17	IMAP - Internet Message Access Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.5	5500\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance	userpc3		NetBIOS - Name Service
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		192.168.1.13	LDAP - Lightweight Directory Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		192.168.1.4	BOOTP - Server
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance	userpc16		NetBIOS - Session Service

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.7</b>						
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		userpc2	MSSQL - SQL Server Monitor
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.20	FTP Command
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		192.168.1.6	NetBIOS - Name Service
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		192.168.1.22	PPTP - Point-to-Point Tunneling Protocol
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		userpc2	NetBIOS - Name Service
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		userpc12	MSSQL - SQL Server Database
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		192.168.1.18	WLM/MSM - Windows Live Messenger
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		192.168.1.23	UPS - Uninterruptible Power Supply
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		192.168.1.13	8080\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		userpc4	Finger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		192.168.1.25	POP3 - Post Office Protocol Version 3
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		userpc16	8080\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		userpc11	5500\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.20	WLM/MSM - Windows Live Messenger
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		192.168.1.26	NNTP - Network News Transfer Protocol
<b>172.10.1.8</b>						
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		userpc10	End Point Mapper
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		192.168.1.28	IMAP - Internet Message Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		userpc3	Finger
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		userpc3	TFTP - Trivial File Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.16	110\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.21	X Window System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.31	FTP Command
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		192.168.1.19	NetBIOS - Datagram
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.10	IMAP - Internet Message Access Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.33	HTTP - Hypertext Transfer Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.8</b>						
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		192.168.1.15	POP3 - Post Office Protocol Version 3
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		192.168.1.4	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		userpc13	NNTP - Network News Transfer Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		192.168.1.13	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		192.168.1.27	TFTP - Trivial File Transfer Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.5	AIM - AOL Instant Messenger
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		192.168.1.6	SMTP - Simple Mail Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		userpc1	119\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		192.168.1.18	SSH - Secure Shell
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		userpc4	NetBIOS - Session Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		userpc13	MSSQL - SQL Server Database
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		userpc14	111\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.14	TELNET
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.24	UPS - Uninterruptible Power Supply
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		userpc10	IBM Lotus Notes/Domino RPC
<b>172.10.1.9</b>						
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		192.168.1.23	AIM - AOL Instant Messenger
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		192.168.1.29	BOOTP - Client
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		192.168.1.8	IBM Lotus Notes/Domino RPC
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.1	AIM - AOL Instant Messenger
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.23	5500\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		192.168.1.18	MSSQL - SQL Server Monitor
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.23	IMAP - Internet Message Access Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>172.10.1.9</b>						
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		192.168.1.10	MSSQL - SQL Server Database
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		192.168.1.1	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		userpc1	NetBIOS - Datagram
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		192.168.1.11	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		userpc9	5500\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		192.168.1.1	TELNET
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		userpc7	79\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Compromise		192.168.1.3	BOOTP - Server
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		userpc12	BOOTP - Server
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		userpc6	X Window System
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		192.168.1.9	GNUTELLA-RTR
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		192.168.1.16	HTTPS - Secure HTTP
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.18	110\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.3	DNS - Domain Name System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.7	Syslog - System Logging Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		192.168.1.30	NetBIOS - Name Service
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		192.168.1.3	End Point Mapper
<b>ftpsrvr.acme.com</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		101.138.232.109	111\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		117.180.12.105	UPS - Uninterruptible Power Supply
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		106.148.54.20	DNS - Domain Name System
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		115.71.91.110	Finger
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		117.83.247.204	Microsoft Directory Services
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.204	TFTP - Trivial File Transfer Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.209	GNUTELLA Service
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.220	UPS - Uninterruptible Power Supply
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.248	FTP Command
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		106.178.103.206	AIM - AOL Instant Messenger

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		112.26.27.203	POP3 - Post Office Protocol Version 3
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		113.53.48.148	POP3 - Post Office Protocol Version 3
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		66.2.30.4	MySQL Database System
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.245	IMAP - Internet Message Access Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		104.151.242.62	WLM/MSM - Windows Live Messenger
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		105.148.92.222	NetBIOS - Session Service
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		105.148.92.222	WLM/MSM - Windows Live Messenger
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		106.71.210.209	IMAP - Internet Message Access Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		112.231.167.112	BOOTP - Client
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.100	End Point Mapper
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.104	IBM Lotus Notes/Domino RPC
03/26/08 02:00 AM	03/27/08 02:00 PM	2.00	General Reconnaissance		113.95.99.218	Microsoft Directory Services
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		104.83.105.39	HTTP - Hypertext Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		106.41.42.164	POP3 - Post Office Protocol Version 3
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.102	HTTP - Hypertext Transfer Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.105	NetBIOS - Datagram
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.107	8080\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.215	End Point Mapper
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		105.219.149.191	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		107.25.150.43	Microsoft Directory Services
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		110.173.225.94	79\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		118.29.166.228	NetBIOS - Session Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.222	NetBIOS - Datagram
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.251	5500\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		105.148.92.222	LDAP - Lightweight Directory Access Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		106.178.103.206	POP3 - Post Office Protocol Version 3
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		111.103.215.210	79\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		112.211.5.54	Kazaa
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		66.2.30.9	Syslog - System Logging Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.242	POP3 - Post Office Protocol Version 3
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		114.17.192.178	Microsoft Directory Services
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		72.99.11.104	LDAP - Lightweight Directory Access Protocol
03/26/08 06:00 AM	03/26/08 10:00 AM	2.00	General Reconnaissance		103.199.117.191	IMAP - Internet Message Access Protocol
03/26/08 06:00 AM	03/27/08 02:00 PM	2.00	General Reconnaissance		88.69.1.207	PPTP - Point-to-Point Tunneling Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.101	GNUTELLA Service
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.209	IMAP - Internet Message Access Protocol
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.229	End Point Mapper
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.248	End Point Mapper
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		103.253.172.4	IMAP - Internet Message Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		105.241.215.112	BOOTP - Server
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		111.195.14.150	IBM Lotus Notes/Domino RPC
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.249	End Point Mapper
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		106.41.42.164	5500\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		116.96.74.233	IMAP - Internet Message Access Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.111	TELNET
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.219	SSH - Secure Shell
03/26/08 09:00 AM	03/27/08 03:00 PM	2.00	General Reconnaissance		72.99.11.106	5800\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Compromise		115.71.91.110	HTTPS - Secure HTTP
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Compromise		88.69.1.229	MSSQL - SQL Server Monitor
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		101.138.232.109	5500\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		106.178.103.206	111\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		113.198.41.205	NetBIOS - Datagram

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		117.180.12.105	BOOTP - Client
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.106	TELNET
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.225	MySQL Database System
03/26/08 10:00 AM	03/27/08 04:00 AM	2.00	General Reconnaissance		66.2.30.2	NNTP - Network News Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Compromise		72.99.11.114	Finger
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		106.87.12.123	Microsoft Directory Services
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		113.104.243.29	NetBIOS - Datagram
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		120.138.126.247	HTTPS - Secure HTTP
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Compromise		105.248.16.99	LDAP - Lightweight Directory Access Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		106.23.8.82	NetBIOS - Name Service
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		113.198.41.205	X Window System
03/26/08 12:00 PM	03/26/08 05:00 PM	2.00	General Reconnaissance		66.2.30.10	SMTP - Simple Mail Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Compromise		107.25.150.43	IMAP - Internet Message Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		101.136.167.138	DNS - Domain Name System
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		105.114.60.223	BOOTP - Client
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		107.240.248.102	WLM/MSM - Windows Live Messenger
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		66.2.30.3	BOOTP - Client
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.119	IBM Lotus Notes/Domino RPC
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Compromise		88.69.1.222	79\
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		102.116.230.67	LDAP - Lightweight Directory Access Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		109.138.207.137	GNUTELLA-RTR
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		111.142.55.119	LDAP - Lightweight Directory Access Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		112.176.232.212	LDAP - Lightweight Directory Access Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		115.111.20.104	SSH - Secure Shell
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.207	IMAP - Internet Message Access Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.237	BOOTP - Server
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.252	GNUTELLA Service
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		105.241.215.112	X Window System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		110.173.225.94	MySQL Database System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		114.248.62.136	MSSQL - SQL Server Database
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		119.135.23.192	Finger
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		119.166.129.99	LDAP - Lightweight Directory Access Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.217	AIM - AOL Instant Messenger
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.228	Kazaa
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.236	NetBIOS - Session Service
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.241	NetBIOS - Name Service
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Compromise		66.2.30.3	NetBIOS - Session Service
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		106.87.12.123	WLM/MSM - Windows Live Messenger
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		115.191.101.229	LDAP - Lightweight Directory Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.102	GNUTELLA-RTR
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.108	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.237	111\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		119.135.23.192	Microsoft Directory Services
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		106.178.103.206	X Window System
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		106.87.12.123	Kazaa
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		113.95.99.218	5500\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		117.180.12.105	AIM - AOL Instant Messenger
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		118.190.70.171	Kazaa
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		119.31.164.89	FTP Command
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		66.2.30.1	SSH - Secure Shell
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		66.2.30.3	End Point Mapper
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		66.2.30.3	NetBIOS - Datagram
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.238	IMAP - Internet Message Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		101.110.102.70	79\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		114.248.62.136	111\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		120.204.177.106	AIM - AOL Instant Messenger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpserver.acme.com</b>						
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		66.2.30.3	119\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.103	BOOTP - Server
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		72.99.11.104	End Point Mapper
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.202	NetBIOS - Name Service
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.253	WLM/MSM - Windows Live Messenger
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		106.148.54.20	MSSQL - SQL Server Database
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		117.21.49.172	End Point Mapper
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		119.25.113.70	MSSQL - SQL Server Monitor
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		72.99.11.102	NetBIOS - Datagram
03/26/08 07:00 PM	03/27/08 03:00 AM	2.00	General Reconnaissance		120.204.177.106	NetBIOS - Session Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		109.117.125.53	AIM - AOL Instant Messenger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		111.195.14.150	AIM - AOL Instant Messenger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		115.111.20.104	PPTP - Point-to-Point Tunneling Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.205	End Point Mapper
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.211	Microsoft Directory Services
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.220	BOOTP - Server
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.234	NetBIOS - Session Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.250	Finger
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		102.116.230.67	IMAP - Internet Message Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		102.116.230.67	NetBIOS - Session Service
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		105.96.101.134	5800\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		106.160.138.40	IMAP - Internet Message Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		107.1.188.213	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		72.99.11.117	NetBIOS - Datagram
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Compromise		110.91.38.179	FTP Command
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		102.27.84.33	End Point Mapper
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		110.91.38.179	Microsoft Directory Services

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		115.191.101.229	IBM Lotus Notes/Domino RPC
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.190.70.171	NNTP - Network News Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		72.99.11.109	NNTP - Network News Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.202	SMTP - Simple Mail Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.213	119\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.245	Kazaa
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.253	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		106.148.54.20	HTTPS - Secure HTTP
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		117.83.247.204	111\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		110.56.252.33	111\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		112.211.5.54	UPS - Uninterruptible Power Supply
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		66.2.30.4	Syslog - System Logging Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.120	Syslog - System Logging Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.204	End Point Mapper
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.207	Syslog - System Logging Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.218	Kazaa
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		106.178.103.206	TFTP - Trivial File Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.223	NetBIOS - Session Service
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.245	NetBIOS - Session Service
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		119.166.129.99	5800\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.111	Microsoft Directory Services
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.217	End Point Mapper
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.227	IMAP - Internet Message Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.239	LDAP - Lightweight Directory Access Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		108.103.69.15	LDAP - Lightweight Directory Access Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpserver.acme.com</b>						
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		115.23.161.181	79\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		119.29.250.161	SSH - Secure Shell
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.109	AIM - AOL Instant Messenger
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.225	Finger
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.244	WLM/MSM - Windows Live Messenger
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		117.21.49.172	WLM/MSM - Windows Live Messenger
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		66.2.30.1	111\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.112	79\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.210	5800\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		109.5.43.42	TFTP - Trivial File Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		118.200.95.244	GNUTELLA-RTR
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.101	HTTP - Hypertext Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.248	IBM Lotus Notes/Domino RPC
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		119.135.23.192	GNUTELLA Service
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		72.99.11.103	MySQL Database System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.208	TFTP - Trivial File Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.247	GNUTELLA Service
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		106.23.8.82	8080\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		107.180.80.203	PPTP - Point-to-Point Tunneling Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		107.75.39.135	End Point Mapper
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		113.198.41.205	MSSQL - SQL Server Monitor
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		72.99.11.117	LDAP - Lightweight Directory Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.227	119\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		109.117.125.53	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		115.111.20.104	SMTP - Simple Mail Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.206	Syslog - System Logging Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpserver.acme.com</b>						
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.217	79\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.235	NetBIOS - Name Service
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		116.97.118.31	TELNET
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		119.166.129.99	79\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.221	LDAP - Lightweight Directory Access Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.228	POP3 - Post Office Protocol Version 3
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Compromise		72.99.11.106	LDAP - Lightweight Directory Access Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		111.36.131.245	MSSQL - SQL Server Database
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		119.135.23.192	111\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		66.2.30.1	111\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.202	IBM Lotus Notes/Domino RPC
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.214	DNS - Domain Name System
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.244	X Window System
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.246	5800\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Compromise		113.159.109.25	PPTP - Point-to-Point Tunneling Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		105.219.149.191	End Point Mapper
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		105.96.101.72	HTTPS - Secure HTTP
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		116.76.60.122	GNUTELLA Service
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.108	NetBIOS - Datagram
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		111.103.27.70	MSSQL - SQL Server Database
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		88.69.1.244	8080\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		112.211.5.54	IMAP - Internet Message Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		118.19.112.193	POP3 - Post Office Protocol Version 3
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		66.2.30.3	POP3 - Post Office Protocol Version 3
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.102	111\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.222	GNUTELLA-RTR
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		105.248.16.99	Syslog - System Logging Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		110.56.252.33	Syslog - System Logging Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		112.176.232.212	IMAP - Internet Message Access Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		114.128.130.118	UPS - Uninterruptible Power Supply
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		114.17.192.178	Syslog - System Logging Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		66.2.30.6	IMAP - Internet Message Access Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		72.99.11.103	IBM Lotus Notes/Domino RPC
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		105.96.101.72	PPTP - Point-to-Point Tunneling Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		106.148.54.20	8080\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		107.75.39.135	MSSQL - SQL Server Monitor
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		111.103.215.210	AIM - AOL Instant Messenger
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		118.200.95.244	NetBIOS - Session Service
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.231	IMAP - Internet Message Access Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.252	MySQL Database System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.253	BOOTP - Client
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		110.40.57.83	TFTP - Trivial File Transfer Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		112.26.27.203	110\
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		116.13.132.192	Syslog - System Logging Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.253	IMAP - Internet Message Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		101.110.102.70	Microsoft Directory Services
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		109.129.58.157	DNS - Domain Name System
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		117.21.49.172	111\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.109	NetBIOS - Datagram
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.117	110\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.214	Microsoft Directory Services
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.230	BOOTP - Server

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		119.166.129.99	Microsoft Directory Services
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		66.2.30.10	MySQL Database System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		66.2.30.4	End Point Mapper
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		72.99.11.115	Kazaa
03/27/08 04:00 PM	03/28/08 05:00 AM	2.00	General Reconnaissance		88.69.1.242	Microsoft Directory Services
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		109.5.43.42	NNTP - Network News Transfer Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		112.231.167.112	Syslog - System Logging Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.114	NetBIOS - Datagram
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		72.99.11.116	LDAP - Lightweight Directory Access Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.208	MSSQL - SQL Server Monitor
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.234	Syslog - System Logging Protocol
03/27/08 05:00 PM	03/27/08 09:00 PM	2.00	General Reconnaissance		111.36.131.245	110\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		109.5.43.42	BOOTP - Server
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		111.103.27.70	MSSQL - SQL Server Monitor
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		114.183.253.86	GNUTELLA Service
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.223	WLM/MSM - Windows Live Messenger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		107.1.188.213	Syslog - System Logging Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		112.176.232.212	119\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		112.236.131.84	LDAP - Lightweight Directory Access Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.114	111\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.253	79\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Compromise		114.17.192.178	BOOTP - Server
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		101.88.139.234	5500\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		112.26.27.203	GNUTELLA Service
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		113.198.41.205	110\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		115.111.20.104	DNS - Domain Name System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		72.99.11.111	MySQL Database System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.239	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.244	IMAP - Internet Message Access Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		102.116.230.67	BOOTP - Server
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		104.83.105.39	UPS - Uninterruptible Power Supply
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		106.148.54.20	TFTP - Trivial File Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		110.105.176.46	WLM/MSM - Windows Live Messenger
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		110.40.57.83	GNUTELLA-RTR
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		110.49.174.190	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		112.229.146.63	POP3 - Post Office Protocol Version 3
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		112.236.131.84	TFTP - Trivial File Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		114.17.192.178	BOOTP - Client
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.217	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.235	111\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.252	IBM Lotus Notes/Domino RPC
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.103	FTP Command
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Compromise		88.69.1.238	IBM Lotus Notes/Domino RPC
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		102.27.84.33	GNUTELLA Service
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		109.5.43.42	MySQL Database System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		66.2.30.5	GNUTELLA-RTR
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		72.99.11.118	SSH - Secure Shell
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.209	Kazaa
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		103.44.13.181	HTTPS - Secure HTTP
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		107.75.39.135	GNUTELLA-RTR
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		111.103.215.210	PPTP - Point-to-Point Tunneling Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		118.200.95.244	111\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		66.2.30.10	TELNET
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		72.99.11.111	111\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.200	POP3 - Post Office Protocol Version 3

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.224	NNTP - Network News Transfer Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.229	HTTPS - Secure HTTP
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		106.148.54.20	111\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		119.84.138.21	X Window System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.220	NetBIOS - Name Service
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		110.56.252.33	GNUTELLA Service
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		115.111.20.104	NetBIOS - Session Service
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		72.99.11.113	SSH - Secure Shell
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		72.99.11.118	BOOTP - Client
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Compromise		88.69.1.206	5800\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		72.99.11.103	SMTP - Simple Mail Transfer Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		72.99.11.109	79\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.249	POP3 - Post Office Protocol Version 3
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		103.199.117.191	Finger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		111.195.14.150	HTTPS - Secure HTTP
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		118.200.95.244	BOOTP - Server
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		120.138.126.247	MSSQL - SQL Server Monitor
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.102	NNTP - Network News Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.207	NNTP - Network News Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.235	8080\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.245	X Window System
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		113.53.48.148	5500\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		116.76.60.122	AIM - AOL Instant Messenger
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.106	DNS - Domain Name System
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.116	GNUTELLA Service
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.221	119\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.228	IMAP - Internet Message Access Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.252	DNS - Domain Name System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		103.253.172.4	DNS - Domain Name System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		106.87.12.123	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>ftpservers.acme.com</b>						
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		110.91.38.179	X Window System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		111.36.131.245	PPTP - Point-to-Point Tunneling Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.111	Syslog - System Logging Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.246	111\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.250	119\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		110.76.158.164	111\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		118.200.95.244	LDAP - Lightweight Directory Access Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.218	119\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.240	BOOTP - Client
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.243	DNS - Domain Name System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		114.17.192.178	PPTP - Point-to-Point Tunneling Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.110	NetBIOS - Datagram
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.203	GNUTELLA Service
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.233	Kazaa
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Compromise		88.69.1.200	NetBIOS - Name Service
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		112.231.167.112	79\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		115.71.91.110	GNUTELLA Service
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		118.190.70.171	MySQL Database System
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		119.25.113.70	111\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.104	119\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.115	8080\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.201	5800\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.251	IMAP - Internet Message Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		111.142.55.119	LDAP - Lightweight Directory Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		107.75.39.135	LDAP - Lightweight Directory Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		115.135.147.74	5500\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.220	MSSQL - SQL Server Monitor
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		72.99.11.118	NetBIOS - Name Service
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		88.69.1.228	LDAP - Lightweight Directory Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		88.69.1.208	IBM Lotus Notes/Domino RPC
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		102.27.84.33	TFTP - Trivial File Transfer Protocol
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		114.128.130.118	BOOTP - Client
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		72.99.11.108	8080\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.204	Microsoft Directory Services
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.224	FTP Command
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.251	5800\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		101.138.232.109	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		106.71.210.209	SMTP - Simple Mail Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		115.191.101.229	DNS - Domain Name System
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		118.15.241.93	IBM Lotus Notes/Domino RPC
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.104	Microsoft Directory Services
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.221	119\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		101.110.102.70	Microsoft Directory Services
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		103.253.172.4	110\
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		109.138.207.137	NetBIOS - Datagram
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Compromise		118.190.70.171	BOOTP - Server
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Compromise		66.2.30.8	FTP Command
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		106.41.42.164	UPS - Uninterruptible Power Supply
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		111.142.55.119	GNUTELLA Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		101.88.139.234	TFTP - Trivial File Transfer Protocol
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		102.116.230.67	GNUTELLA-RTR
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		103.44.13.181	UPS - Uninterruptible Power Supply
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		105.148.92.222	X Window System
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		117.21.49.172	Microsoft Directory Services
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.235	BOOTP - Client
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.238	5800\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		103.242.202.177	GNUTELLA-RTR
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		105.219.149.191	DNS - Domain Name System
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		118.19.112.193	SMTP - Simple Mail Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.239	Microsoft Directory Services
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		104.83.105.39	PPTP - Point-to-Point Tunneling Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		105.219.149.191	LDAP - Lightweight Directory Access Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		109.105.181.83	PPTP - Point-to-Point Tunneling Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		111.142.55.119	119\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		113.53.48.148	MSSQL - SQL Server Database
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		106.160.138.40	BOOTP - Client
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		109.138.207.137	DNS - Domain Name System
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		113.104.243.29	WLM/MSM - Windows Live Messenger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		118.19.112.193	UPS - Uninterruptible Power Supply
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.222	HTTPS - Secure HTTP
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.225	NetBIOS - Name Service
03/26/08 08:00 AM	03/27/08 05:00 AM	2.00	General Reconnaissance		106.71.210.209	Kazaa
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		102.116.230.67	HTTPS - Secure HTTP
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		102.27.84.33	Microsoft Directory Services
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		103.47.20.110	GNUTELLA Service
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		104.151.242.62	PPTP - Point-to-Point Tunneling Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		105.96.101.72	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		108.103.69.15	MSSQL - SQL Server Database
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		116.76.60.122	MSSQL - SQL Server Monitor
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		72.99.11.104	HTTPS - Secure HTTP
03/26/08 09:00 AM	03/26/08 03:00 PM	2.00	General Reconnaissance		88.69.1.243	5500\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		107.197.4.193	111\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		116.97.118.31	AIM - AOL Instant Messenger
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		118.190.70.171	5500\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.108	DNS - Domain Name System
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.118	End Point Mapper
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.119	POP3 - Post Office Protocol Version 3
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.234	BOOTP - Client
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.237	119\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		88.69.1.237	WLM/MSM - Windows Live Messenger
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		105.243.17.16	8080\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		113.104.243.29	IMAP - Internet Message Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		115.135.147.74	MSSQL - SQL Server Database
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.111	DNS - Domain Name System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.213	BOOTP - Client
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.217	DNS - Domain Name System
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.241	119\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		106.41.42.164	110\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		108.124.40.121	111\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		110.91.38.179	Microsoft Directory Services
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		119.29.250.161	IMAP - Internet Message Access Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		72.99.11.104	BOOTP - Server
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.200	GNUTELLA Service
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Compromise		72.99.11.107	End Point Mapper
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		101.136.167.138	TELNET
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		102.27.84.33	End Point Mapper
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		104.151.242.62	NetBIOS - Session Service
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		111.103.215.210	5800\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		112.211.5.54	IMAP - Internet Message Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		114.248.62.136	5800\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		116.13.132.192	TFTP - Trivial File Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		117.180.12.105	POP3 - Post Office Protocol Version 3
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		66.2.30.6	UPS - Uninterruptible Power Supply
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		66.2.30.8	End Point Mapper
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		103.199.117.191	IBM Lotus Notes/Domino RPC
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		113.198.41.205	MSSQL - SQL Server Database
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		114.128.130.118	DNS - Domain Name System
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		116.96.74.233	UPS - Uninterruptible Power Supply
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		72.99.11.105	HTTP - Hypertext Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.253	MSSQL - SQL Server Monitor
03/26/08 02:00 PM	03/28/08 10:00 AM	2.00	General Reconnaissance		72.99.11.109	119\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		105.148.92.222	End Point Mapper
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		109.117.125.53	MySQL Database System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		110.56.252.33	NetBIOS - Name Service
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		113.95.99.218	DNS - Domain Name System
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		120.138.126.247	POP3 - Post Office Protocol Version 3
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		66.2.30.5	UPS - Uninterruptible Power Supply
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Compromise		103.47.20.110	AIM - AOL Instant Messenger
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		105.114.60.223	5500\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		105.96.101.134	PPTP - Point-to-Point Tunneling Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		107.197.4.193	HTTP - Hypertext Transfer Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		113.104.243.29	GNUTELLA-RTR
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		118.95.82.196	IMAP - Internet Message Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.110	TELNET
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.229	5800\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		105.241.215.112	NetBIOS - Datagram
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		88.69.1.208	Finger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		105.248.16.99	Microsoft Directory Services
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		114.128.130.118	NetBIOS - Session Service
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		66.2.30.4	5800\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		72.99.11.104	SSH - Secure Shell
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		72.99.11.105	NetBIOS - Datagram
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		72.99.11.108	UPS - Uninterruptible Power Supply
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.237	AIM - AOL Instant Messenger
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		88.69.1.227	119\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		101.136.167.138	110\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		103.47.20.110	NetBIOS - Name Service
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		110.49.174.190	TFTP - Trivial File Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		112.231.167.112	DNS - Domain Name System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		120.138.126.247	LDAP - Lightweight Directory Access Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.233	5800\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.249	DNS - Domain Name System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Compromise		88.69.1.222	8080\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		107.180.80.203	PPTP - Point-to-Point Tunneling Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		109.5.43.42	TELNET
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		111.103.27.70	UPS - Uninterruptible Power Supply
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		119.29.250.161	Kazaa
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.201	Syslog - System Logging Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.203	DNS - Domain Name System
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		104.151.242.62	MySQL Database System
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		111.103.27.70	HTTPS - Secure HTTP
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		111.195.14.150	Syslog - System Logging Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		66.2.30.8	NetBIOS - Session Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.102	NetBIOS - Name Service
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.107	AIM - AOL Instant Messenger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.215	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.244	AIM - AOL Instant Messenger
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Compromise		101.136.167.138	5500\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		111.36.131.245	DNS - Domain Name System
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		114.229.222.106	POP3 - Post Office Protocol Version 3
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		116.96.74.233	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.200	WLM/MSM - Windows Live Messenger
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.203	GNUTELLA-RTR
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.234	End Point Mapper
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		105.96.101.134	UPS - Uninterruptible Power Supply
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		110.91.38.179	IMAP - Internet Message Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		116.13.132.192	WLM/MSM - Windows Live Messenger
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.208	TFTP - Trivial File Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.232	5800\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.237	8080\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.241	Microsoft Directory Services
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		101.136.167.138	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Compromise		106.41.42.164	LDAP - Lightweight Directory Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		106.178.103.206	GNUTELLA-RTR
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		119.25.113.70	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.247	AIM - AOL Instant Messenger
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.247	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		101.136.167.138	UPS - Uninterruptible Power Supply

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		107.180.80.203	Microsoft Directory Services
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		107.240.248.102	GNUTELLA-RTR
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		109.5.43.42	BOOTP - Server
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		66.2.30.1	PPTP - Point-to-Point Tunneling Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		66.2.30.8	NetBIOS - Datagram
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.230	NetBIOS - Datagram
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		103.253.172.4	111\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		105.96.101.134	Kazaa
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		114.248.62.136	Microsoft Directory Services
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		118.15.241.93	HTTP - Hypertext Transfer Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.244	8080\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		113.198.41.205	FTP Command
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		88.69.1.236	MSSQL - SQL Server Database
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		112.176.232.212	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		113.104.243.29	MSSQL - SQL Server Database
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		113.198.41.205	TFTP - Trivial File Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.108	GNUTELLA-RTR
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.225	Microsoft Directory Services
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		103.199.117.191	Syslog - System Logging Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		112.229.146.63	GNUTELLA-RTR
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		114.248.62.136	Finger
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.238	Kazaa
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		103.242.202.177	HTTPS - Secure HTTP
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		106.41.42.164	MSSQL - SQL Server Monitor
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		107.180.80.203	5800\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.120	NNTP - Network News Transfer Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.238	LDAP - Lightweight Directory Access Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		115.71.91.110	MSSQL - SQL Server Monitor
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		119.157.88.38	POP3 - Post Office Protocol Version 3
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		72.99.11.110	NNTP - Network News Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.221	Finger
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.223	GNUTELLA Service
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.232	8080\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		105.219.149.191	Microsoft Directory Services
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		105.96.101.134	MSSQL - SQL Server Monitor
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		108.124.40.121	MSSQL - SQL Server Database
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		112.211.5.54	110\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		115.135.147.74	119\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		72.99.11.117	DNS - Domain Name System
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.205	8080\
03/27/08 06:00 AM	03/27/08 10:00 PM	2.00	General Reconnaissance		102.116.230.67	UPS - Uninterruptible Power Supply
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Compromise		119.157.88.38	NNTP - Network News Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		110.49.174.190	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		113.104.243.29	POP3 - Post Office Protocol Version 3
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		119.157.88.38	HTTPS - Secure HTTP
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.235	TELNET
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.237	IMAP - Internet Message Access Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.241	MSSQL - SQL Server Monitor
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Compromise		88.69.1.252	Microsoft Directory Services
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		105.241.215.112	PPTP - Point-to-Point Tunneling Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		112.231.167.112	NetBIOS - Name Service

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		118.66.66.46	GNUTELLA Service
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.203	111\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		106.23.8.82	MSSQL - SQL Server Database
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		112.26.27.203	SMTP - Simple Mail Transfer Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		115.111.20.104	DNS - Domain Name System
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		118.15.241.93	PPTP - Point-to-Point Tunneling Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.107	Microsoft Directory Services
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.200	119\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.253	5800\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		114.17.192.178	LDAP - Lightweight Directory Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Compromise		88.69.1.221	NetBIOS - Session Service
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		105.148.92.222	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		105.248.16.99	TFTP - Trivial File Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		118.19.112.193	IMAP - Internet Message Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.115	LDAP - Lightweight Directory Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.237	HTTP - Hypertext Transfer Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.243	Kazaa
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		112.26.27.203	119\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.204	DNS - Domain Name System
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.210	HTTPS - Secure HTTP
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.212	79\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.222	GNUTELLA Service
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.225	X Window System
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.236	Microsoft Directory Services
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Compromise		111.103.215.210	GNUTELLA Service
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		105.241.215.112	SSH - Secure Shell
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		106.12.75.97	NetBIOS - Datagram
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		72.99.11.119	119\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.249	SMTP - Simple Mail Transfer Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		108.103.69.15	X Window System
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		118.19.112.193	NNTP - Network News Transfer Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		120.138.126.247	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		66.2.30.3	GNUTELLA-RTR
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		72.99.11.100	MSSQL - SQL Server Monitor
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.219	MSSQL - SQL Server Database
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		72.99.11.105	HTTPS - Secure HTTP
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		106.12.75.97	IBM Lotus Notes/Domino RPC
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.203	IMAP - Internet Message Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.207	Syslog - System Logging Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.249	GNUTELLA-RTR
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		112.250.231.58	5500\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		115.23.161.181	UPS - Uninterruptible Power Supply
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		116.13.132.192	End Point Mapper
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		102.116.230.67	LDAP - Lightweight Directory Access Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		103.199.117.191	119\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		108.124.40.121	DNS - Domain Name System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		111.36.131.245	BOOTP - Server
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		118.29.166.228	DNS - Domain Name System
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.218	BOOTP - Client
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.252	TELNET
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		101.88.139.234	119\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		103.242.202.177	111\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		113.53.48.148	Syslog - System Logging Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		114.183.253.86	NNTP - Network News Transfer Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		66.2.30.4	Microsoft Directory Services
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		72.99.11.108	IMAP - Internet Message Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		72.99.11.113	IMAP - Internet Message Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.224	UPS - Uninterruptible Power Supply
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		88.69.1.248	8080\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		107.25.150.43	Microsoft Directory Services
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		119.166.129.99	Finger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		104.83.105.39	119\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		111.142.55.119	X Window System
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		117.83.247.204	NNTP - Network News Transfer Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.113	111\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		72.99.11.113	DNS - Domain Name System
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.211	UPS - Uninterruptible Power Supply
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		106.41.42.164	8080\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		110.173.225.94	IMAP - Internet Message Access Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		119.135.23.192	GNUTELLA Service
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		66.2.30.3	110\
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.231	Syslog - System Logging Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		105.96.101.134	SSH - Secure Shell
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		110.91.38.179	NNTP - Network News Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		113.53.48.148	HTTP - Hypertext Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		118.190.70.171	GNUTELLA-RTR
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		119.135.23.192	WLM/MSM - Windows Live Messenger
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		72.99.11.108	NNTP - Network News Transfer Protocol
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.214	119\
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.240	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.246	5800\
03/27/08 09:00 PM	03/28/08 06:00 AM	2.00	General Reconnaissance		72.99.11.110	POP3 - Post Office Protocol Version 3
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		72.99.11.118	Syslog - System Logging Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		110.40.57.83	111\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		119.31.164.89	End Point Mapper
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.103	LDAP - Lightweight Directory Access Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.107	NetBIOS - Session Service
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.211	GNUTELLA-RTR
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.214	PPTP - Point-to-Point Tunneling Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		102.116.230.67	DNS - Domain Name System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		105.219.149.191	SMTP - Simple Mail Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		107.240.248.102	HTTP - Hypertext Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		66.2.30.2	NNTP - Network News Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.206	WLM/MSM - Windows Live Messenger
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.207	SMTP - Simple Mail Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.212	MySQL Database System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.218	TELNET
03/27/08 11:00 PM	03/28/08 08:00 AM	2.00	General Reconnaissance		111.36.131.245	UPS - Uninterruptible Power Supply
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		111.103.27.70	TFTP - Trivial File Transfer Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		112.236.131.84	SSH - Secure Shell
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		116.13.132.192	MSSQL - SQL Server Monitor
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		66.2.30.7	TFTP - Trivial File Transfer Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.201	Finger
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.229	UPS - Uninterruptible Power Supply
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.250	IBM Lotus Notes/Domino RPC

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		105.243.17.16	111\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		116.96.74.233	5500\
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.210	UPS - Uninterruptible Power Supply
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.250	IMAP - Internet Message Access Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Compromise		72.99.11.104	TFTP - Trivial File Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		108.124.40.121	HTTPS - Secure HTTP
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		110.56.252.33	FTP Command
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		114.128.130.118	WLM/MSM - Windows Live Messenger
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		66.2.30.10	DNS - Domain Name System
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		72.99.11.101	X Window System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		103.44.13.181	UPS - Uninterruptible Power Supply
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		106.178.103.206	HTTPS - Secure HTTP
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		107.197.4.193	DNS - Domain Name System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		115.135.147.74	111\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		118.95.82.196	Microsoft Directory Services
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		72.99.11.105	WLM/MSM - Windows Live Messenger
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.207	NetBIOS - Session Service
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.208	79\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.228	Kazaa
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.237	NetBIOS - Datagram
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		107.197.4.193	IBM Lotus Notes/Domino RPC
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		107.75.39.135	PPTP - Point-to-Point Tunneling Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		111.142.55.119	WLM/MSM - Windows Live Messenger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		112.229.146.63	MySQL Database System
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		118.190.70.171	SSH - Secure Shell
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		119.29.250.161	NNTP - Network News Transfer Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		66.2.30.1	SSH - Secure Shell
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		66.2.30.3	Kazaa

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.105	FTP Command
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		72.99.11.119	Finger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.223	NetBIOS - Name Service
03/28/08 04:00 AM	03/28/08 10:00 AM	2.00	General Reconnaissance		119.157.88.38	SMTP - Simple Mail Transfer Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		88.69.1.251	LDAP - Lightweight Directory Access Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		104.83.105.39	MySQL Database System
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		113.53.48.148	DNS - Domain Name System
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		116.76.60.122	SSH - Secure Shell
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		66.2.30.2	NetBIOS - Datagram
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.225	IMAP - Internet Message Access Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Compromise		118.29.166.228	Kazaa
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		105.243.17.16	MySQL Database System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		107.197.4.193	DNS - Domain Name System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		107.75.39.135	HTTPS - Secure HTTP
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		116.96.74.233	AIM - AOL Instant Messenger
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.112	GNUTELLA-RTR
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.248	119\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Compromise		110.76.158.164	5800\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		111.142.55.119	GNUTELLA-RTR
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		118.190.70.171	Microsoft Directory Services
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.116	Finger
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.226	End Point Mapper
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.252	NetBIOS - Session Service
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		103.253.172.4	Microsoft Directory Services
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		112.236.131.84	BOOTP - Server
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.117	PPTP - Point-to-Point Tunneling Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.235	WLM/MSM - Windows Live Messenger
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		103.47.20.110	DNS - Domain Name System
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		105.241.215.112	110\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		113.159.109.25	Finger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>mailserver.acme.com</b>						
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		113.215.126.48	HTTPS - Secure HTTP
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		116.13.132.192	IMAP - Internet Message Access Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		108.103.69.15	TELNET
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		110.76.158.164	MSSQL - SQL Server Database
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		111.195.14.150	X Window System
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		119.25.113.70	MSSQL - SQL Server Monitor
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		88.69.1.214	IBM Lotus Notes/Domino RPC
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		103.253.172.4	UPS - Uninterruptible Power Supply
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		111.195.14.150	NetBIOS - Session Service
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		116.13.132.192	Microsoft Directory Services
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		119.25.113.70	BOOTP - Server
<b>server1</b>						
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		userpc2	110\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		192.168.1.1	5800\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.14	MySQL Database System
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		192.168.1.19	MSSQL - SQL Server Monitor
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		192.168.1.30	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.5	POP3 - Post Office Protocol Version 3
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		userpc9	GNUTELLA-RTR
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		192.168.1.11	IBM Lotus Notes/Domino RPC
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		192.168.1.3	BOOTP - Client
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		192.168.1.2	5500\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		userpc16	NetBIOS - Name Service
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		192.168.1.33	Syslog - System Logging Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		192.168.1.6	MSSQL - SQL Server Monitor
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		userpc6	MSSQL - SQL Server Database

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>server1</b>						
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.30	BOOTP - Server
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Compromise		192.168.1.18	119\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		192.168.1.23	BOOTP - Server
<b>server2</b>						
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.11	DNS - Domain Name System
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.27	BOOTP - Server
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		userpc16	8080\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		userpc5	NetBIOS - Name Service
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		userpc5	Microsoft Directory Services
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		192.168.1.13	GNUTELLA-RTR
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		192.168.1.24	GNUTELLA Service
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		192.168.1.6	5800\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		userpc10	POP3 - Post Office Protocol Version 3
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.17	GNUTELLA Service
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		192.168.1.9	HTTP - Hypertext Transfer Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		192.168.1.14	HTTP - Hypertext Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		userpc10	UPS - Uninterruptible Power Supply
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		192.168.1.17	111\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		userpc15	111\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		192.168.1.1	SMTP - Simple Mail Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		userpc10	8080\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		192.168.1.10	Microsoft Directory Services
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		userpc4	MSSQL - SQL Server Monitor
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		192.168.1.30	Kazaa
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		192.168.1.30	MySQL Database System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.26	DNS - Domain Name System
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		192.168.1.1	8080\
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		userpc1	DNS - Domain Name System
<b>server3</b>						

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>server3</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.13	BOOTP - Client
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		192.168.1.2	FTP Command
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		userpc7	HTTPS - Secure HTTP
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		userpc13	MSSQL - SQL Server Monitor
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		192.168.1.25	UPS - Uninterruptible Power Supply
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		192.168.1.17	NetBIOS - Datagram
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		192.168.1.6	IBM Lotus Notes/Domino RPC
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		userpc1	Syslog - System Logging Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		userpc14	Kazaa
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		userpc12	NetBIOS - Session Service
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		192.168.1.15	X Window System
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.1	5800\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		192.168.1.10	End Point Mapper
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		192.168.1.20	111\
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		192.168.1.14	MSSQL - SQL Server Monitor
<b>server4</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		userpc6	AIM - AOL Instant Messenger
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		192.168.1.11	Finger
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		192.168.1.16	IBM Lotus Notes/Domino RPC
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		userpc9	5800\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		userpc16	LDAP - Lightweight Directory Access Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		userpc3	DNS - Domain Name System
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		userpc10	NetBIOS - Datagram
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		192.168.1.7	110\
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		192.168.1.20	TFTP - Trivial File Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		192.168.1.7	End Point Mapper
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		192.168.1.24	Microsoft Directory Services
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		userpc11	NetBIOS - Datagram

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>server4</b>						
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		userpc10	TFTP - Trivial File Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		userpc6	DNS - Domain Name System
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		192.168.1.15	End Point Mapper
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		192.168.1.30	UPS - Uninterruptible Power Supply
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		userpc10	5500\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		userpc14	AIM - AOL Instant Messenger
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		192.168.1.14	IMAP - Internet Message Access Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		192.168.1.32	MSSQL - SQL Server Database
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		192.168.1.12	NetBIOS - Datagram
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		userpc13	BOOTP - Client
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		192.168.1.29	FTP Command
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		userpc16	DNS - Domain Name System
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		192.168.1.14	NetBIOS - Name Service
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		192.168.1.12	Microsoft Directory Services
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.19	DNS - Domain Name System
<b>server5</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		192.168.1.6	SSH - Secure Shell
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		userpc10	5800\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		userpc13	TELNET
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Compromise		192.168.1.9	Syslog - System Logging Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		192.168.1.2	5800\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		192.168.1.29	NetBIOS - Datagram
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		192.168.1.25	IMAP - Internet Message Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Compromise		192.168.1.12	111\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		192.168.1.27	MSSQL - SQL Server Monitor
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Compromise		userpc9	Microsoft Directory Services
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		userpc16	POP3 - Post Office Protocol Version 3

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>server5</b>						
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		192.168.1.25	79\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		userpc4	TFTP - Trivial File Transfer Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		userpc14	Microsoft Directory Services
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		userpc5	5800\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		192.168.1.11	WLM/MSM - Windows Live Messenger
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		192.168.1.9	UPS - Uninterruptible Power Supply
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		192.168.1.7	111\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		192.168.1.8	LDAP - Lightweight Directory Access Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		userpc7	NNTP - Network News Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		192.168.1.9	5500\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		userpc15	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		192.168.1.30	SSH - Secure Shell
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		userpc5	SMTP - Simple Mail Transfer Protocol
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		192.168.1.6	WLM/MSM - Windows Live Messenger
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Compromise		192.168.1.9	5800\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		192.168.1.13	NNTP - Network News Transfer Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		userpc2	NetBIOS - Session Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		192.168.1.27	111\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		userpc12	IMAP - Internet Message Access Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		userpc16	PPTP - Point-to-Point Tunneling Protocol
<b>webserver1.acme.com</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		105.114.60.223	MSSQL - SQL Server Monitor
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		116.13.132.192	BOOTP - Server
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		119.31.164.89	Kazaa
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		88.69.1.235	SSH - Secure Shell
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		72.99.11.112	NNTP - Network News Transfer Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		88.69.1.222	MSSQL - SQL Server Monitor
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		105.114.60.223	TFTP - Trivial File Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		110.105.176.46	79\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		110.195.212.97	UPS - Uninterruptible Power Supply
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		113.95.99.218	Syslog - System Logging Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		114.229.222.106	Microsoft Directory Services
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		111.103.215.210	NetBIOS - Datagram
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.237	FTP Command
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.246	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 AM	03/28/08 02:00 AM	2.00	General Reconnaissance		119.157.88.38	Kazaa
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Compromise		110.91.38.179	X Window System
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Compromise		118.190.70.171	HTTPS - Secure HTTP
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		101.136.167.138	Finger
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		109.138.207.137	Microsoft Directory Services
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		113.215.126.48	DNS - Domain Name System
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		106.148.54.20	GNUTELLA Service
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		110.49.174.190	5500\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		66.2.30.4	5500\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.111	119\
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.116	TELNET
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Compromise		111.36.131.245	UPS - Uninterruptible Power Supply
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		106.148.54.20	TELNET
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		117.83.247.204	BOOTP - Client
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		101.88.139.234	111\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		106.148.54.20	5500\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		107.75.39.135	UPS - Uninterruptible Power Supply
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		113.198.41.205	IMAP - Internet Message Access Protocol
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		117.83.247.204	5500\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		72.99.11.104	MSSQL - SQL Server Monitor
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		102.27.84.33	IBM Lotus Notes/Domino RPC
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		110.195.212.97	Kazaa
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		116.96.74.233	Kazaa
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		119.166.129.99	Microsoft Directory Services
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		72.99.11.107	NetBIOS - Session Service
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.210	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		103.47.20.110	End Point Mapper
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		106.148.54.20	DNS - Domain Name System
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		112.176.232.212	TELNET
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.110	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.110	Microsoft Directory Services
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.111	5800\
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.202	NNTP - Network News Transfer Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.211	UPS - Uninterruptible Power Supply
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.218	UPS - Uninterruptible Power Supply
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		101.136.167.138	BOOTP - Client
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		66.2.30.5	IMAP - Internet Message Access Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		66.2.30.9	LDAP - Lightweight Directory Access Protocol
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.213	Microsoft Directory Services
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		112.229.146.63	SSH - Secure Shell
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		117.21.49.172	End Point Mapper
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		66.2.30.3	Kazaa
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		72.99.11.116	MSSQL - SQL Server Database
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		119.166.129.99	Syslog - System Logging Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserv1.acme.com</b>						
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		119.84.138.21	WLM/MSM - Windows Live Messenger
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		119.135.23.192	SSH - Secure Shell
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.203	79\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.231	HTTPS - Secure HTTP
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		105.248.16.99	LDAP - Lightweight Directory Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		109.138.207.137	NetBIOS - Datagram
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		110.195.212.97	X Window System
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		115.23.161.181	UPS - Uninterruptible Power Supply
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.114	111\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.116	NNTP - Network News Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.210	IMAP - Internet Message Access Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.226	GNUTELLA Service
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		111.142.55.119	PPTP - Point-to-Point Tunneling Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		112.250.231.58	BOOTP - Client
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		114.128.130.118	TFTP - Trivial File Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		66.2.30.8	TFTP - Trivial File Transfer Protocol
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		72.99.11.114	Microsoft Directory Services
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.207	GNUTELLA-RTR
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.252	HTTPS - Secure HTTP
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		101.110.102.70	111\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		119.29.250.161	Microsoft Directory Services
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.112	TELNET
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		101.138.232.109	Microsoft Directory Services
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		106.23.8.82	FTP Command
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		109.138.207.137	PPTP - Point-to-Point Tunneling Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		66.2.30.2	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		66.2.30.2	POP3 - Post Office Protocol Version 3
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		66.2.30.2	TELNET
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		66.2.30.7	5800\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.235	8080\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Compromise		107.25.150.43	End Point Mapper
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		110.173.225.94	POP3 - Post Office Protocol Version 3
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		110.91.38.179	Finger
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		111.142.55.119	TFTP - Trivial File Transfer Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		114.229.222.106	BOOTP - Client
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		119.135.23.192	TELNET
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		72.99.11.115	POP3 - Post Office Protocol Version 3
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.214	5500\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.229	110\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.249	Syslog - System Logging Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.251	111\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Compromise		88.69.1.200	111\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		105.96.101.72	MSSQL - SQL Server Database
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		106.71.210.209	SMTP - Simple Mail Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		106.87.12.123	UPS - Uninterruptible Power Supply
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		107.1.188.213	Kazaa
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		111.195.14.150	End Point Mapper
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		113.159.109.25	SSH - Secure Shell
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		118.29.166.228	Syslog - System Logging Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.210	Finger
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.233	DNS - Domain Name System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.249	UPS - Uninterruptible Power Supply
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.252	5500\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		105.96.101.134	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		110.173.225.94	DNS - Domain Name System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		118.190.70.171	MySQL Database System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		66.2.30.4	111\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		103.253.172.4	SSH - Secure Shell
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		110.195.212.97	POP3 - Post Office Protocol Version 3
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		115.111.20.104	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		116.13.132.192	GNUTELLA-RTR
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		72.99.11.108	X Window System
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.214	MSSQL - SQL Server Monitor
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.215	FTP Command
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.237	110\
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		110.173.225.94	AIM - AOL Instant Messenger
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		111.103.27.70	HTTP - Hypertext Transfer Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		66.2.30.3	MSSQL - SQL Server Monitor
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.234	110\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		107.75.39.135	BOOTP - Client
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		107.75.39.135	SSH - Secure Shell
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		109.138.207.137	GNUTELLA Service
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		115.191.101.229	LDAP - Lightweight Directory Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.15.241.93	PPTP - Point-to-Point Tunneling Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.190.70.171	End Point Mapper
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		118.200.95.244	GNUTELLA-RTR
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		66.2.30.10	NetBIOS - Datagram
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.200	111\
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.219	FTP Command
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		110.173.225.94	FTP Command
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		111.36.131.245	X Window System
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		116.76.60.122	8080\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.114	110\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserv1.acme.com</b>						
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.233	UPS - Uninterruptible Power Supply
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		103.253.172.4	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		112.229.146.63	IMAP - Internet Message Access Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.108	NetBIOS - Datagram
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.118	5800\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.222	Syslog - System Logging Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.231	POP3 - Post Office Protocol Version 3
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		105.148.92.222	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		105.219.149.191	IMAP - Internet Message Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		106.12.75.97	HTTP - Hypertext Transfer Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		106.160.138.40	NetBIOS - Datagram
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		109.5.43.42	IMAP - Internet Message Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		115.111.20.104	110\
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		117.83.247.204	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		119.29.250.161	UPS - Uninterruptible Power Supply
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		72.99.11.117	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.227	IBM Lotus Notes/Domino RPC
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		107.240.248.102	Microsoft Directory Services
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		102.27.84.33	Microsoft Directory Services
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		115.71.91.110	111\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		119.25.113.70	LDAP - Lightweight Directory Access Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.234	WLM/MSM - Windows Live Messenger
03/27/08 02:00 AM	03/28/08 08:00 AM	2.00	General Reconnaissance		88.69.1.234	DNS - Domain Name System

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Compromise		88.69.1.238	Syslog - System Logging Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		104.151.242.62	Microsoft Directory Services
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		104.83.105.39	DNS - Domain Name System
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		107.1.188.213	110\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		111.103.215.210	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		118.66.66.46	UPS - Uninterruptible Power Supply
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		66.2.30.7	NNTP - Network News Transfer Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.107	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.111	110\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.223	MSSQL - SQL Server Database
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.243	NNTP - Network News Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		107.75.39.135	NetBIOS - Session Service
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		105.114.60.223	POP3 - Post Office Protocol Version 3
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		105.96.101.134	MySQL Database System
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		119.166.129.99	IMAP - Internet Message Access Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		66.2.30.7	Kazaa
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		72.99.11.105	TFTP - Trivial File Transfer Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		106.160.138.40	TELNET
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		106.71.210.209	LDAP - Lightweight Directory Access Protocol
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		111.103.27.70	X Window System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		112.229.146.63	BOOTP - Client
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		116.96.74.233	MSSQL - SQL Server Database
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		118.19.112.193	111\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		119.31.164.89	5800\
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		72.99.11.104	HTTPS - Secure HTTP
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		72.99.11.111	X Window System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.206	DNS - Domain Name System
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.218	AIM - AOL Instant Messenger
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.250	HTTPS - Secure HTTP
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		101.136.167.138	110\
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		110.40.57.83	BOOTP - Server
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		113.95.99.218	GNUTELLA-RTR
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		115.111.20.104	Microsoft Directory Services
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.225	HTTPS - Secure HTTP
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		88.69.1.237	SMTP - Simple Mail Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		106.23.8.82	End Point Mapper
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		107.180.80.203	BOOTP - Server
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		115.191.101.229	110\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		119.25.113.70	Microsoft Directory Services
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.230	UPS - Uninterruptible Power Supply
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.242	119\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		113.104.243.29	FTP Command
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		118.29.166.228	MSSQL - SQL Server Database
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		72.99.11.116	79\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.200	119\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.208	5500\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.210	5800\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.229	MSSQL - SQL Server Database
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.236	TFTP - Trivial File Transfer Protocol
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.240	NNTP - Network News Transfer Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		103.199.117.191	DNS - Domain Name System
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		115.71.91.110	5800\
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.228	End Point Mapper
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.241	110\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		107.180.80.203	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		112.26.27.203	SSH - Secure Shell
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		113.215.126.48	119\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		117.180.12.105	End Point Mapper
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		72.99.11.107	AIM - AOL Instant Messenger
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.221	X Window System
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.237	5500\
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.238	FTP Command
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.247	79\
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		114.248.62.136	Microsoft Directory Services
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.105	DNS - Domain Name System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		72.99.11.117	Microsoft Directory Services
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.229	Finger
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.242	5500\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		101.88.139.234	End Point Mapper
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		107.180.80.203	Syslog - System Logging Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		107.197.4.193	IBM Lotus Notes/Domino RPC
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		117.180.12.105	UPS - Uninterruptible Power Supply
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		118.200.95.244	Syslog - System Logging Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		66.2.30.7	GNUTELLA-RTR
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.203	119\
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.241	IBM Lotus Notes/Domino RPC
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.247	TFTP - Trivial File Transfer Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Compromise		103.47.20.110	110\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		105.96.101.72	WLM/MMS - Windows Live Messenger
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		110.49.174.190	HTTPS - Secure HTTP
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		115.191.101.229	PPTP - Point-to-Point Tunneling Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		115.23.161.181	79\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.2	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		66.2.30.4	UPS - Uninterruptible Power Supply
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		72.99.11.119	Microsoft Directory Services
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.248	IBM Lotus Notes/Domino RPC
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		111.195.14.150	FTP Command
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		118.190.70.171	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		118.95.82.196	GNUTELLA Service
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		66.2.30.5	Kazaa
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		66.2.30.7	Microsoft Directory Services
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.217	IMAP - Internet Message Access Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.245	SSH - Secure Shell
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.248	IMAP - Internet Message Access Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.253	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		105.148.92.222	NNTP - Network News Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		107.180.80.203	End Point Mapper
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		107.25.150.43	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		109.129.58.157	HTTP - Hypertext Transfer Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		72.99.11.119	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.225	MySQL Database System
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.226	Kazaa
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.251	Microsoft Directory Services
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		115.191.101.229	MySQL Database System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		116.13.132.192	X Window System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		118.19.112.193	DNS - Domain Name System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.253	NetBIOS - Session Service

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Compromise		107.180.80.203	MSSQL - SQL Server Monitor
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		113.53.48.148	79\
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		114.128.130.118	BOOTP - Server
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		116.97.118.31	Microsoft Directory Services
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		88.69.1.219	MSSQL - SQL Server Monitor
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		101.88.139.234	IMAP - Internet Message Access Protocol
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		106.87.12.123	HTTPS - Secure HTTP
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		113.159.109.25	111\
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		118.200.95.244	IBM Lotus Notes/Domino RPC
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		72.99.11.106	MySQL Database System
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		105.114.60.223	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		105.241.215.112	FTP Command
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		107.75.39.135	AIM - AOL Instant Messenger
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		110.91.38.179	79\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		116.13.132.192	NetBIOS - Name Service
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.212	UPS - Uninterruptible Power Supply
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.215	MSSQL - SQL Server Database
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.222	HTTP - Hypertext Transfer Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.247	NetBIOS - Datagram
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.252	NetBIOS - Session Service
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		102.27.84.33	GNUTELLA Service
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.208	MSSQL - SQL Server Database
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.230	DNS - Domain Name System
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.239	Microsoft Directory Services
03/27/08 08:00 PM	03/28/08 02:00 AM	2.00	General Reconnaissance		117.180.12.105	BOOTP - Client
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Compromise		72.99.11.111	IMAP - Internet Message Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserv1.acme.com</b>						
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		107.180.80.203	MSSQL - SQL Server Database
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		109.117.125.53	TELNET
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		118.190.70.171	NetBIOS - Name Service
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		72.99.11.106	End Point Mapper
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		101.110.102.70	LDAP - Lightweight Directory Access Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		102.116.230.67	IMAP - Internet Message Access Protocol
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		103.242.202.177	NetBIOS - Datagram
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		115.23.161.181	5800\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		88.69.1.229	UPS - Uninterruptible Power Supply
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Compromise		106.23.8.82	X Window System
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		118.29.166.228	End Point Mapper
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.244	Microsoft Directory Services
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		105.114.60.223	5500\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		107.240.248.102	Finger
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		110.195.212.97	LDAP - Lightweight Directory Access Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		110.49.174.190	119\
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		116.76.60.122	IMAP - Internet Message Access Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		118.200.95.244	LDAP - Lightweight Directory Access Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.219	UPS - Uninterruptible Power Supply
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.236	PPTP - Point-to-Point Tunneling Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Compromise		88.69.1.245	Finger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		102.27.84.33	TELNET
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		103.242.202.177	BOOTP - Server
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		118.15.241.93	IBM Lotus Notes/Domino RPC
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		72.99.11.102	LDAP - Lightweight Directory Access Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		72.99.11.105	8080\

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		72.99.11.117	Microsoft Directory Services
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.227	TFTP - Trivial File Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Compromise		109.129.58.157	111\
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Compromise		118.66.66.46	NNTP - Network News Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		72.99.11.109	Finger
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.216	LDAP - Lightweight Directory Access Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Compromise		88.69.1.247	MSSQL - SQL Server Database
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		101.88.139.234	FTP Command
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		105.219.149.191	IBM Lotus Notes/Domino RPC
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		112.26.27.203	DNS - Domain Name System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		117.180.12.105	MySQL Database System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		119.84.138.21	5800\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		66.2.30.4	IMAP - Internet Message Access Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.241	X Window System
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.253	Finger
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Compromise		88.69.1.208	GNUTELLA Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		103.44.13.181	DNS - Domain Name System
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		66.2.30.10	111\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		116.13.132.192	IBM Lotus Notes/Domino RPC
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		88.69.1.218	NetBIOS - Name Service
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Compromise		88.69.1.236	BOOTP - Client
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		107.25.150.43	BOOTP - Server
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		110.49.174.190	111\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		113.104.243.29	DNS - Domain Name System
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		113.104.243.29	SSH - Secure Shell
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.232	MSSQL - SQL Server Monitor
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		88.69.1.244	BOOTP - Server
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Compromise		72.99.11.111	AIM - AOL Instant Messenger

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Compromise		88.69.1.220	LDAP - Lightweight Directory Access Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		117.21.49.172	MSSQL - SQL Server Database
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		117.83.247.204	FTP Command
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.201	MSSQL - SQL Server Database
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.220	End Point Mapper
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		110.56.252.33	111\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		111.36.131.245	WLM/MSM - Windows Live Messenger
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		115.135.147.74	End Point Mapper
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		117.180.12.105	GNUTELLA-RTR
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		119.135.23.192	5800\
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		119.135.23.192	LDAP - Lightweight Directory Access Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		66.2.30.5	WLM/MSM - Windows Live Messenger
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.116	AIM - AOL Instant Messenger
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.209	5500\
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		72.99.11.107	MySQL Database System
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.203	LDAP - Lightweight Directory Access Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.203	PPTP - Point-to-Point Tunneling Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.235	GNUTELLA-RTR
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.243	UPS - Uninterruptible Power Supply
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		119.135.23.192	TFTP - Trivial File Transfer Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		66.2.30.8	DNS - Domain Name System
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		72.99.11.107	X Window System
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.224	LDAP - Lightweight Directory Access Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		88.69.1.231	DNS - Domain Name System
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Compromise		72.99.11.119	End Point Mapper
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		101.88.139.234	GNUTELLA-RTR
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		113.159.109.25	5500\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver1.acme.com</b>						
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		115.111.20.104	TELNET
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		116.13.132.192	Syslog - System Logging Protocol
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		66.2.30.1	GNUTELLA-RTR
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		72.99.11.114	UPS - Uninterruptible Power Supply
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		72.99.11.114	X Window System
<b>webserver2.acme.com</b>						
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Compromise		106.23.8.82	8080\
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		112.250.231.58	TELNET
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		72.99.11.111	End Point Mapper
03/26/08 12:00 AM	03/26/08 12:00 AM	1.00	General Reconnaissance		72.99.11.115	NetBIOS - Datagram
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Compromise		88.69.1.230	UPS - Uninterruptible Power Supply
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		106.41.42.164	SSH - Secure Shell
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		72.99.11.120	HTTP - Hypertext Transfer Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.200	PPTP - Point-to-Point Tunneling Protocol
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.212	111\
03/26/08 01:00 AM	03/26/08 01:00 AM	1.00	General Reconnaissance		88.69.1.233	UPS - Uninterruptible Power Supply
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		106.160.138.40	TELNET
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		113.159.109.25	HTTPS - Secure HTTP
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		114.229.222.106	X Window System
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		117.83.247.204	HTTPS - Secure HTTP
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.111	NetBIOS - Datagram
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		72.99.11.114	IMAP - Internet Message Access Protocol
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.245	FTP Command
03/26/08 02:00 AM	03/26/08 02:00 AM	1.00	General Reconnaissance		88.69.1.245	LDAP - Lightweight Directory Access Protocol
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		111.142.55.119	5800\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		113.53.48.148	BOOTP - Client
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		72.99.11.106	MSSQL - SQL Server Database
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.238	110\
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.244	Finger

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/26/08 03:00 AM	03/26/08 03:00 AM	1.00	General Reconnaissance		88.69.1.245	WLM/MSM - Windows Live Messenger
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		107.240.248.102	HTTPS - Secure HTTP
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		72.99.11.110	TELNET
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.215	Finger
03/26/08 04:00 AM	03/26/08 04:00 AM	1.00	General Reconnaissance		88.69.1.228	FTP Command
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		101.110.102.70	NNTP - Network News Transfer Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		103.44.13.181	AIM - AOL Instant Messenger
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		107.240.248.102	IMAP - Internet Message Access Protocol
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		111.142.55.119	111\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		113.159.109.25	End Point Mapper
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		117.21.49.172	BOOTP - Server
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.219	111\
03/26/08 05:00 AM	03/26/08 05:00 AM	1.00	General Reconnaissance		88.69.1.250	IBM Lotus Notes/Domino RPC
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		72.99.11.113	Kazaa
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		72.99.11.119	119\
03/26/08 06:00 AM	03/26/08 06:00 AM	1.00	General Reconnaissance		88.69.1.207	TELNET
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		109.117.125.53	AIM - AOL Instant Messenger
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		110.76.158.164	111\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		113.95.99.218	110\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		115.23.161.181	111\
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		115.71.91.110	MSSQL - SQL Server Database
03/26/08 07:00 AM	03/26/08 07:00 AM	1.00	General Reconnaissance		88.69.1.241	GNUTELLA Service
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Compromise		103.47.20.110	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		105.243.17.16	FTP Command
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		109.138.207.137	Finger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		66.2.30.9	AIM - AOL Instant Messenger
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		72.99.11.104	Syslog - System Logging Protocol
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.218	DNS - Domain Name System

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.228	BOOTP - Server
03/26/08 08:00 AM	03/26/08 08:00 AM	1.00	General Reconnaissance		88.69.1.236	111\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Compromise		109.105.181.83	119\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.212	110\
03/26/08 09:00 AM	03/26/08 09:00 AM	1.00	General Reconnaissance		88.69.1.220	DNS - Domain Name System
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		106.87.12.123	119\
03/26/08 10:00 AM	03/26/08 10:00 AM	1.00	General Reconnaissance		118.95.82.196	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Compromise		116.96.74.233	IMAP - Internet Message Access Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Compromise		88.69.1.246	HTTP - Hypertext Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		105.248.16.99	MSSQL - SQL Server Database
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		107.197.4.193	UPS - Uninterruptible Power Supply
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		112.236.131.84	SMTP - Simple Mail Transfer Protocol
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		113.95.99.218	Finger
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		114.17.192.178	IBM Lotus Notes/Domino RPC
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		115.135.147.74	UPS - Uninterruptible Power Supply
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		115.191.101.229	UPS - Uninterruptible Power Supply
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		72.99.11.111	GNUTELLA-RTR
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.217	TELNET
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.237	AIM - AOL Instant Messenger
03/26/08 11:00 AM	03/26/08 11:00 AM	1.00	General Reconnaissance		88.69.1.240	LDAP - Lightweight Directory Access Protocol
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		114.248.62.136	5500\
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		66.2.30.1	End Point Mapper
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		66.2.30.6	NetBIOS - Session Service
03/26/08 12:00 PM	03/26/08 12:00 PM	1.00	General Reconnaissance		88.69.1.225	5500\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		102.27.84.33	MSSQL - SQL Server Database
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		114.183.253.86	GNUTELLA Service
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		114.229.222.106	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		118.29.166.228	119\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		118.29.166.228	TFTP - Trivial File Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		66.2.30.7	AIM - AOL Instant Messenger
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		72.99.11.117	NNTP - Network News Transfer Protocol
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.213	111\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.219	5500\
03/26/08 01:00 PM	03/26/08 01:00 PM	1.00	General Reconnaissance		88.69.1.219	PPTP - Point-to-Point Tunneling Protocol
03/26/08 01:00 PM	03/28/08 09:00 AM	2.00	General Compromise		109.129.58.157	HTTPS - Secure HTTP
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.213	DNS - Domain Name System
03/26/08 02:00 PM	03/26/08 02:00 PM	1.00	General Reconnaissance		88.69.1.231	IMAP - Internet Message Access Protocol
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		110.195.212.97	79\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		110.76.158.164	5800\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		112.229.146.63	UPS - Uninterruptible Power Supply
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		119.84.138.21	HTTPS - Secure HTTP
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		72.99.11.120	111\
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.202	SSH - Secure Shell
03/26/08 03:00 PM	03/26/08 03:00 PM	1.00	General Reconnaissance		88.69.1.238	IMAP - Internet Message Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		113.215.126.48	WLM/MSM - Windows Live Messenger
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		66.2.30.7	POP3 - Post Office Protocol Version 3
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.101	POP3 - Post Office Protocol Version 3
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		72.99.11.116	IBM Lotus Notes/Domino RPC
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.203	8080\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.234	IMAP - Internet Message Access Protocol
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.238	79\
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.239	BOOTP - Client
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.252	GNUTELLA-RTR
03/26/08 04:00 PM	03/26/08 04:00 PM	1.00	General Reconnaissance		88.69.1.253	8080\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserv2.acme.com</b>						
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		103.253.172.4	Microsoft Directory Services
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		105.241.215.112	MSSQL - SQL Server Monitor
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		117.180.12.105	5800\
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		118.200.95.244	MySQL Database System
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		118.66.66.46	IMAP - Internet Message Access Protocol
03/26/08 05:00 PM	03/26/08 05:00 PM	1.00	General Reconnaissance		88.69.1.230	SMTP - Simple Mail Transfer Protocol
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		102.116.230.67	DNS - Domain Name System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		106.41.42.164	119\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		110.49.174.190	DNS - Domain Name System
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		111.36.131.245	End Point Mapper
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		115.135.147.74	SSH - Secure Shell
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		119.135.23.192	110\
03/26/08 06:00 PM	03/26/08 06:00 PM	1.00	General Reconnaissance		88.69.1.222	IMAP - Internet Message Access Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		110.49.174.190	TELNET
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		113.104.243.29	End Point Mapper
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		117.21.49.172	111\
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.200	IMAP - Internet Message Access Protocol
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.205	DNS - Domain Name System
03/26/08 07:00 PM	03/26/08 07:00 PM	1.00	General Reconnaissance		88.69.1.234	Finger
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		101.88.139.234	PPTP - Point-to-Point Tunneling Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		103.47.20.110	110\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		106.160.138.40	5800\
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		112.26.27.203	TFTP - Trivial File Transfer Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		113.53.48.148	LDAP - Lightweight Directory Access Protocol
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		117.83.247.204	UPS - Uninterruptible Power Supply
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		120.204.177.106	TELNET
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.233	BOOTP - Client
03/26/08 08:00 PM	03/26/08 08:00 PM	1.00	General Reconnaissance		88.69.1.249	End Point Mapper

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		66.2.30.9	SMTP - Simple Mail Transfer Protocol
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.224	SSH - Secure Shell
03/26/08 09:00 PM	03/26/08 09:00 PM	1.00	General Reconnaissance		88.69.1.242	LDAP - Lightweight Directory Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		109.5.43.42	TFTP - Trivial File Transfer Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		113.198.41.205	PPTP - Point-to-Point Tunneling Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		114.128.130.118	IMAP - Internet Message Access Protocol
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		66.2.30.8	WLM/MSM - Windows Live Messenger
03/26/08 10:00 PM	03/26/08 10:00 PM	1.00	General Reconnaissance		88.69.1.242	IMAP - Internet Message Access Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		110.56.252.33	HTTPS - Secure HTTP
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		112.229.146.63	79\
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		118.66.66.46	UPS - Uninterruptible Power Supply
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		72.99.11.119	PPTP - Point-to-Point Tunneling Protocol
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.210	NetBIOS - Name Service
03/26/08 11:00 PM	03/26/08 11:00 PM	1.00	General Reconnaissance		88.69.1.252	TELNET
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Compromise		109.5.43.42	TFTP - Trivial File Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		110.105.176.46	End Point Mapper
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		119.135.23.192	DNS - Domain Name System
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		72.99.11.111	5500\
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.201	TFTP - Trivial File Transfer Protocol
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.221	UPS - Uninterruptible Power Supply
03/27/08 12:00 AM	03/27/08 12:00 AM	1.00	General Reconnaissance		88.69.1.234	NetBIOS - Datagram
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		104.151.242.62	LDAP - Lightweight Directory Access Protocol
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		107.180.80.203	IBM Lotus Notes/Domino
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		108.103.69.15	RPC
03/27/08 01:00 AM	03/27/08 01:00 AM	1.00	General Reconnaissance		88.69.1.234	5800\
						Microsoft Directory Services

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Compromise		88.69.1.234	POP3 - Post Office Protocol Version 3
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		105.243.17.16	8080\
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		106.71.210.209	Microsoft Directory Services
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		111.103.27.70	NetBIOS - Session Service
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		114.229.222.106	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		119.157.88.38	UPS - Uninterruptible Power Supply
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		119.25.113.70	SMTP - Simple Mail Transfer Protocol
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		72.99.11.118	POP3 - Post Office Protocol Version 3
03/27/08 02:00 AM	03/27/08 02:00 AM	1.00	General Reconnaissance		88.69.1.245	Microsoft Directory Services
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Compromise		107.75.39.135	IBM Lotus Notes/Domino RPC
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		106.148.54.20	UPS - Uninterruptible Power Supply
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.107	IMAP - Internet Message Access Protocol
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		72.99.11.116	111\
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.206	DNS - Domain Name System
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.211	Finger
03/27/08 03:00 AM	03/27/08 03:00 AM	1.00	General Reconnaissance		88.69.1.241	AIM - AOL Instant Messenger
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		66.2.30.10	IMAP - Internet Message Access Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Compromise		88.69.1.206	BOOTP - Server
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		106.12.75.97	Microsoft Directory Services
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		109.5.43.42	111\
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		114.128.130.118	AIM - AOL Instant Messenger
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		66.2.30.7	TFTP - Trivial File Transfer Protocol
03/27/08 04:00 AM	03/27/08 04:00 AM	1.00	General Reconnaissance		88.69.1.205	POP3 - Post Office Protocol Version 3
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Compromise		119.157.88.38	111\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		105.96.101.72	FTP Command
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.206	End Point Mapper
03/27/08 05:00 AM	03/27/08 05:00 AM	1.00	General Reconnaissance		88.69.1.209	Microsoft Directory Services
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		103.199.117.191	IMAP - Internet Message Access Protocol
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		113.159.109.25	Kazaa
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		115.71.91.110	Microsoft Directory Services
03/27/08 06:00 AM	03/27/08 06:00 AM	1.00	General Reconnaissance		118.190.70.171	PPTP - Point-to-Point Tunneling Protocol
03/27/08 06:00 AM	03/27/08 08:00 AM	2.00	General Reconnaissance		109.5.43.42	MSSQL - SQL Server Monitor
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		103.47.20.110	Finger
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		104.151.242.62	SMTP - Simple Mail Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		105.241.215.112	HTTP - Hypertext Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		109.105.181.83	DNS - Domain Name System
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		109.129.58.157	111\
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		119.25.113.70	Finger
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		72.99.11.106	Kazaa
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.214	TFTP - Trivial File Transfer Protocol
03/27/08 07:00 AM	03/27/08 07:00 AM	1.00	General Reconnaissance		88.69.1.227	NetBIOS - Name Service
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		113.198.41.205	119\
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		115.71.91.110	MySQL Database System
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		118.29.166.228	TELNET
03/27/08 08:00 AM	03/27/08 08:00 AM	1.00	General Reconnaissance		88.69.1.239	IBM Lotus Notes/Domino RPC
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		105.248.16.99	HTTPS - Secure HTTP
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		114.183.253.86	End Point Mapper
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		72.99.11.101	PPTP - Point-to-Point Tunneling Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.226	NNTP - Network News Transfer Protocol
03/27/08 09:00 AM	03/27/08 09:00 AM	1.00	General Reconnaissance		88.69.1.235	UPS - Uninterruptible Power Supply

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)

### Impacted Host



First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		101.88.139.234	UPS - Uninterruptible Power Supply
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		106.12.75.97	GNUTELLA Service
03/27/08 10:00 AM	03/27/08 10:00 AM	1.00	General Reconnaissance		88.69.1.201	DNS - Domain Name System
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		105.248.16.99	LDAP - Lightweight Directory Access Protocol
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		106.71.210.209	BOOTP - Server
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		114.248.62.136	NetBIOS - Datagram
03/27/08 11:00 AM	03/27/08 11:00 AM	1.00	General Reconnaissance		88.69.1.216	FTP Command
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		103.199.117.191	IBM Lotus Notes/Domino RPC
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		105.241.215.112	IMAP - Internet Message Access Protocol
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.215	End Point Mapper
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.239	MSSQL - SQL Server Monitor
03/27/08 12:00 PM	03/27/08 12:00 PM	1.00	General Reconnaissance		88.69.1.249	DNS - Domain Name System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		103.242.202.177	5800\
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		109.117.125.53	MySQL Database System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		111.36.131.245	BOOTP - Client
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		112.231.167.112	HTTP - Hypertext Transfer Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		118.200.95.244	PPTP - Point-to-Point Tunneling Protocol
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		72.99.11.107	MSSQL - SQL Server Monitor
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.207	DNS - Domain Name System
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.228	TELNET
03/27/08 01:00 PM	03/27/08 01:00 PM	1.00	General Reconnaissance		88.69.1.236	SMTP - Simple Mail Transfer Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Compromise		88.69.1.203	DNS - Domain Name System
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		106.87.12.123	Kazaa
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		115.23.161.181	GNUTELLA Service
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		66.2.30.10	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.201	Syslog - System Logging Protocol
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.220	79\

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserv2.acme.com</b>						
03/27/08 02:00 PM	03/27/08 02:00 PM	1.00	General Reconnaissance		88.69.1.224	PPTP - Point-to-Point Tunneling Protocol
03/27/08 02:00 PM	03/28/08 07:00 AM	2.00	General Reconnaissance		88.69.1.218	Kazaa
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		103.242.202.177	PPTP - Point-to-Point Tunneling Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		117.21.49.172	LDAP - Lightweight Directory Access Protocol
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		117.83.247.204	111\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		117.83.247.204	119\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		66.2.30.7	TELNET
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.203	119\
03/27/08 03:00 PM	03/27/08 03:00 PM	1.00	General Reconnaissance		88.69.1.206	AIM - AOL Instant Messenger
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		106.87.12.123	111\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		112.26.27.203	Finger
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		113.95.99.218	UPS - Uninterruptible Power Supply
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		118.66.66.46	GNUTELLA-RTR
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		119.166.129.99	End Point Mapper
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		72.99.11.102	5800\
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.228	DNS - Domain Name System
03/27/08 04:00 PM	03/27/08 04:00 PM	1.00	General Reconnaissance		88.69.1.239	HTTP - Hypertext Transfer Protocol
03/27/08 05:00 PM	03/27/08 05:00 PM	1.00	General Reconnaissance		106.160.138.40	MySQL Database System
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		109.129.58.157	UPS - Uninterruptible Power Supply
03/27/08 06:00 PM	03/27/08 06:00 PM	1.00	General Reconnaissance		119.157.88.38	End Point Mapper
03/27/08 06:00 PM	03/28/08 03:00 AM	2.00	General Reconnaissance		72.99.11.111	BOOTP - Client
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		106.23.8.82	GNUTELLA Service
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		112.250.231.58	PPTP - Point-to-Point Tunneling Protocol
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		115.191.101.229	DNS - Domain Name System
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Compromise		88.69.1.243	MSSQL - SQL Server Monitor
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		105.96.101.72	GNUTELLA-RTR
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		108.103.69.15	111\
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		118.19.112.193	LDAP - Lightweight Directory Access Protocol

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		118.190.70.171	IBM Lotus Notes/Domino RPC
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.207	Microsoft Directory Services
03/27/08 07:00 PM	03/27/08 07:00 PM	1.00	General Reconnaissance		88.69.1.216	HTTP - Hypertext Transfer Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		107.75.39.135	BOOTP - Client
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		107.75.39.135	End Point Mapper
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		66.2.30.10	Finger
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.214	End Point Mapper
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.243	NNTP - Network News Transfer Protocol
03/27/08 08:00 PM	03/27/08 08:00 PM	1.00	General Reconnaissance		88.69.1.246	FTP Command
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		101.110.102.70	MSSQL - SQL Server Monitor
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		101.138.232.109	Kazaa
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		113.198.41.205	HTTPS - Secure HTTP
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		115.191.101.229	End Point Mapper
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		118.200.95.244	Microsoft Directory Services
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		119.166.129.99	NetBIOS - Datagram
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.220	GNUTELLA-RTR
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.222	AIM - AOL Instant Messenger
03/27/08 09:00 PM	03/27/08 09:00 PM	1.00	General Reconnaissance		88.69.1.226	AIM - AOL Instant Messenger
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Compromise		88.69.1.234	MSSQL - SQL Server Database
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		102.27.84.33	DNS - Domain Name System
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		110.76.158.164	5500\
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		112.211.5.54	WLM/MSM - Windows Live Messenger
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		114.128.130.118	Finger
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		66.2.30.2	SSH - Secure Shell
03/27/08 10:00 PM	03/27/08 10:00 PM	1.00	General Reconnaissance		72.99.11.114	Syslog - System Logging Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		101.136.167.138	SMTP - Simple Mail Transfer Protocol

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		103.253.172.4	HTTP - Hypertext Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		112.250.231.58	UPS - Uninterruptible Power Supply
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		115.23.161.181	SMTP - Simple Mail Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		66.2.30.10	UPS - Uninterruptible Power Supply
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		66.2.30.5	HTTP - Hypertext Transfer Protocol
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		72.99.11.100	Microsoft Directory Services
03/27/08 11:00 PM	03/27/08 11:00 PM	1.00	General Reconnaissance		88.69.1.237	DNS - Domain Name System
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		105.241.215.112	DNS - Domain Name System
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		105.96.101.72	IMAP - Internet Message Access Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		107.25.150.43	MSSQL - SQL Server Database
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		109.105.181.83	NetBIOS - Session Service
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		117.83.247.204	TFTP - Trivial File Transfer Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		72.99.11.112	LDAP - Lightweight Directory Access Protocol
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.208	UPS - Uninterruptible Power Supply
03/28/08 12:00 AM	03/28/08 12:00 AM	1.00	General Reconnaissance		88.69.1.246	Finger
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		102.116.230.67	LDAP - Lightweight Directory Access Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		104.151.242.62	End Point Mapper
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		114.248.62.136	TFTP - Trivial File Transfer Protocol
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		116.76.60.122	End Point Mapper
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.241	NetBIOS - Session Service
03/28/08 01:00 AM	03/28/08 01:00 AM	1.00	General Reconnaissance		88.69.1.245	MSSQL - SQL Server Database
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		110.56.252.33	SMTP - Simple Mail Transfer Protocol
03/28/08 02:00 AM	03/28/08 02:00 AM	1.00	General Reconnaissance		88.69.1.241	SSH - Secure Shell
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Compromise		109.138.207.137	5500\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		104.83.105.39	111\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		109.5.43.42	IMAP - Internet Message Access Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		114.17.192.178	79\
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.200	IMAP - Internet Message Access Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.200	PPTP - Point-to-Point Tunneling Protocol
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.221	MSSQL - SQL Server Database
03/28/08 03:00 AM	03/28/08 03:00 AM	1.00	General Reconnaissance		88.69.1.240	Syslog - System Logging Protocol
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Compromise		72.99.11.111	NetBIOS - Session Service
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		105.243.17.16	BOOTP - Server
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		108.103.69.15	BOOTP - Client
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		114.248.62.136	UPS - Uninterruptible Power Supply
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		66.2.30.3	111\
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.202	End Point Mapper
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.204	UPS - Uninterruptible Power Supply
03/28/08 04:00 AM	03/28/08 04:00 AM	1.00	General Reconnaissance		88.69.1.218	SSH - Secure Shell
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		106.178.103.206	Syslog - System Logging Protocol
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		118.190.70.171	UPS - Uninterruptible Power Supply
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		120.138.126.247	79\
03/28/08 05:00 AM	03/28/08 05:00 AM	1.00	General Reconnaissance		72.99.11.103	79\
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Compromise		105.243.17.16	DNS - Domain Name System
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		105.219.149.191	End Point Mapper
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		106.178.103.206	GNUTELLA Service
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		72.99.11.117	IMAP - Internet Message Access Protocol
03/28/08 06:00 AM	03/28/08 06:00 AM	1.00	General Reconnaissance		88.69.1.223	PPTP - Point-to-Point Tunneling Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		105.114.60.223	PPTP - Point-to-Point Tunneling Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		105.96.101.134	NetBIOS - Name Service
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		110.195.212.97	X Window System
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		118.15.241.93	110\

Report prepared for LogRhythm Inc on Mar 28, 2008 05:25 PM (GMT)

Copyright 2007 LogRhythm, Inc. All Rights Reserved

## Security Event Summary

By Impacted Host

Mar 26, 2008 12:00 AM to Mar 29, 2008 12:00 AM (Dates GMT -06:00)



### Impacted Host

First Log	Last Log	Count	Event	Origin Login	Origin Host	Impacted Application
<b>webserver2.acme.com</b>						
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		119.157.88.38	NetBIOS - Datagram
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		66.2.30.9	BOOTP - Server
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		72.99.11.104	IMAP - Internet Message Access Protocol
03/28/08 07:00 AM	03/28/08 07:00 AM	1.00	General Reconnaissance		88.69.1.238	GNUTELLA-RTR
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Compromise		116.97.118.31	Finger
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		109.129.58.157	HTTP - Hypertext Transfer Protocol
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		118.29.166.228	SSH - Secure Shell
03/28/08 08:00 AM	03/28/08 08:00 AM	1.00	General Reconnaissance		88.69.1.248	PPTP - Point-to-Point Tunneling Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		106.23.8.82	LDAP - Lightweight Directory Access Protocol
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		106.71.210.209	Finger
03/28/08 09:00 AM	03/28/08 09:00 AM	1.00	General Reconnaissance		110.105.176.46	POP3 - Post Office Protocol Version 3
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		104.151.242.62	IBM Lotus Notes/Domino RPC
03/28/08 10:00 AM	03/28/08 10:00 AM	1.00	General Reconnaissance		112.176.232.212	110\
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Compromise		112.250.231.58	AIM - AOL Instant Messenger
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Compromise		116.96.74.233	AIM - AOL Instant Messenger
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		113.159.109.25	IMAP - Internet Message Access Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		114.229.222.106	SMTP - Simple Mail Transfer Protocol
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		117.83.247.204	UPS - Uninterruptible Power Supply
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		66.2.30.2	5800\
03/28/08 11:00 AM	03/28/08 11:00 AM	1.00	General Reconnaissance		66.2.30.5	IBM Lotus Notes/Domino RPC