

Re: Firewall Log Entries Help

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2006-06/msg00021.html>

- *From:* "Louis Vitiello Jr." <louv-mcse@xxxxxxxxxxxx>
 - *Date:* Thu, 1 Jun 2006 23:14:02 -0400
-

Hey Andrew,

TCP 139 is used for Windows File Sharing

TCP 445 is used when NetBIOS over TCP/IP is enabled. It is also a known port for the Sasser worm

TCP 135 port used by Outlook to contact an Exchange Server

TCP 307 is an unassigned port, a program could use this port no use is registered

TCP 309 is registered to EntrustTime

It may seem that some of your ports might be normal network talk. The last two could be hacking attempts, trojan related, or maybe just some third party program trying to communicate through uncommon ports. I would do some more investigating on what's running on the server.

Hope this helps,

—

Louis Vitiello Jr.

MCSE, MCSA, MCP, A+/N+
ERCP XP Pro / Net Concepts

"aboni" <andrew@xxxxxxxxxxxx> wrote in message
[news:%233z2\\$6OhGHA.4388@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%233z2$6OhGHA.4388@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi!

I'm using a Windows 2003 Server with the follow services and ports:

- WebServer, port 80 TCP;
- DNS, port 53 UDP;
- SMTP, port 25 TCP;
- POP3, port 110 TCP;
- Port 53 TCP.

This machine is connected directly with internet and the only firewall is the Windows with the ports above open to Internet.

Re: Firewall Log Entries Help

The entries in the firewall log that begin are listed below. In the big part are attempt connections to ports TCP 139, TCP 445, TCP 135, TCP 307, TCP 309...

This attempt connections signify some thing?

My ethernet card have stop to responds to internet connections since this firewall log entries begin. This attempt connections can have anything related with this?

```
Action-Protocol-Source IP-Destination IP-Source Port-Dest Port
DROP UDP 204.16.208.117 200.162.106.93 40736 1027 308 - - - - -
RECEIVE
DROP TCP 200.162.57.54 200.162.106.92 3506 445 48 S 1493774078 0
64240 - - - RECEIVE
DROP TCP 200.162.57.54 200.162.106.92 3506 445 48 S 1493774078 0
64240 - - - RECEIVE
DROP TCP 200.162.50.5 200.162.106.90 1134 139 48 S 325869944 0 64240 - - -
RECEIVE
DROP TCP 200.162.50.5 200.162.106.90 1134 139 48 S 325869944 0 64240 - - -
RECEIVE
DROP TCP 200.162.50.5 200.162.106.90 4714 139 48 S 639651352 0 64240 - - -
RECEIVE
DROP TCP 200.162.50.5 200.162.106.90 4714 139 48 S 639651352 0 64240 - - -
RECEIVE
DROP TCP 200.151.103.154 200.162.106.90 4691 135 48 S 2710708069 0
8760 - - - RECEIVE
DROP TCP 200.151.103.154 200.162.106.91 4692 135 48 S 2710758501 0
8760 - - - RECEIVE
DROP TCP 200.151.103.154 200.162.106.92 4693 135 48 S 2710816989 0
8760 - - - RECEIVE
DROP TCP 200.151.103.154 200.162.106.93 4694 135 48 S 2710870218 0
8760 - - - RECEIVE
DROP TCP 200.162.57.54 200.162.106.93 4497 445 48 S 3200304490 0
64240 - - - RECEIVE
DROP TCP 200.162.57.54 200.162.106.93 4497 445 48 S 3200304490 0
64240 - - - RECEIVE
DROP TCP 200.104.230.90 200.162.106.93 4612 445 48 S 1385113433 0
16384 - - - RECEIVE
DROP TCP 200.104.230.90 200.162.106.93 4612 445 48 S 1385113433 0
16384 - - - RECEIVE
DROP TCP 200.162.57.54 200.162.106.90 4172 445 48 S 4153052349 0
64240 - - - RECEIVE
DROP TCP 200.162.57.54 200.162.106.90 4172 445 48 S 4153052349 0
64240 - - - RECEIVE
DROP TCP 200.162.50.5 200.162.106.93 2344 135 48 S 1627564286 0
64240 - - - RECEIVE
DROP TCP 200.162.50.5 200.162.106.93 2344 135 48 S 1627564286 0
64240 - - - RECEIVE
DROP TCP 124.8.2.150 200.162.106.90 4593 8080 48 S 1507230536 0
```

Re: Firewall Log Entries Help

16384 --- RECEIVE
DROP TCP 124.8.2.150 200.162.106.93 4639 8080 48 S 2992589925 0
16384 --- RECEIVE
DROP TCP 124.8.2.150 200.162.106.91 4637 8080 48 S 3210896353 0
16384 --- RECEIVE
DROP TCP 124.8.2.150 200.162.106.92 4638 8080 48 S 2639401880 0
16384 --- RECEIVE

Thanks for any help,
Andrew