



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at <http://www.giac.org/registration/gcia>

1.

```
Feb 18 12:38:51 MyServer kernel: Packet log: input DENY eth0
PROTO=17 24.25.227.65:67 X.X.X.X:68 L=341 S=0x00 I=45618 F=0x0000 T=126
(#1)
Feb 18 12:38:51 MyServer kernel: Packet log: input DENY eth0
PROTO=17 24.25.227.65:67 X.X.X.X:68 L=341 S=0x00 I=45874 F=0x0000 T=126
(#1)
```

This is to be a bootp scan for tftp services coming from the same cable modem network.

2.

```
Feb 19 11:28:20 MyServer kernel: Packet log: input DENY eth0
PROTO=17 171.220.22.141:5321 X.X.X.X:23 L=78 S=0x00 I=11211 F=0x0000
T=326 (#6)
Feb 19 11:28:22 MyServer kernel: Packet log: input DENY eth0
PROTO=17 171.220.22.141:5321 X.X.X.X:25 L=78 S=0x00 I=13207 F=0x0000
T=326 (#6)
Feb 19 11:28:23 MyServer kernel: Packet log: input DENY eth0
PROTO=17 171.220.22.141:5321 X.X.X.X:143 L=78 S=0x00 I=41301 F=0x0000
T=326 (#6)
Feb 19 11:28:25 MyServer kernel: Packet log: input DENY eth0
PROTO=17 171.220.22.141:5321 X.X.X.X:111 L=78 S=0x00 I=51303 F=0x0000
T=326 (#6)
Feb 19 11:28:28 MyServer kernel: Packet log: input DENY eth0
PROTO=17 171.220.22.141:5321 X.X.X.X:34555 L=78 S=0x00 I=31806 F=0x0000
T=326 (#6)
Feb 19 11:28:30 MyServer kernel: Packet log: input DENY eth0
PROTO=17 171.220.22.141:5321 X.X.X.X:2049 L=78 S=0x00 I=13608 F=0x0000
T=326 (#6)
Feb 19 11:28:33 MyServer kernel: Packet log: input DENY eth0
PROTO=17 171.220.22.141:5321 X.X.X.X:12345 L=78 S=0x00 I=13309 F=0x0000
T=326 (#6)
```

UDP scan for trojan and available ports from American On-Line. Notice the 34555, wonder if they have included a search for DDOS indicators in the scanning software. Also notice the source port does not change and stays at 5321 (fingerprint?)

3.

```
Feb 24 13:14:57 MyServer kernel: securityalert: tcp if=exp0 from
X.X.4.61:1373 to X.X.X.X on unserved port 23
Feb 24 13:19:18 MyServer kernel: securityalert: udp if=exp0 from
X.X.4.61:63600 to X.X.X.X on unserved port 33441
Feb 24 13:19:18 MyServer kernel: securityalert: udp if=exp0 from
X.X.4.61:63600 to X.X.X.X on unserved port 33442
Feb 24 13:19:18 MyServer kernel: securityalert: udp if=exp0 from
X.X.4.61:63600 to X.X.X.X on unserved port 33443
```

Our DMZ user tried to telnet to the firewall, couldn't and then tried a traceroute.

4.

```
Feb 22 20:58:36 MyServer kernel: securityalert: tcp if=exp0 from
204.7.154.3:47754 to X.X.X.X on unserved port 8080
Feb 22 20:58:37 MyServer kernel: securityalert: tcp if=exp0 from
204.7.154.3:47755 to X.X.X.X on unserved port 8080
```

This person from PSInet is a scanning for a proxy port.

5.

```
Feb 15 10:57:09 MyServer kernel: securityalert: tcp if=exp0 from
211.40.176.54:3951 to X.X.X.X on unserved port 32773
Feb 18 23:32:56 MyServer kernel: securityalert: tcp if=exp0 from
211.40.176.49:4074 to X.X.X.X on unserved port 32773
```

Variation of a back orifice port scan. Notice the different dates and the same class C address... guess our friend from Korea didn't know when to quit.

6.

```
Jan 31 08:01:18 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:3537 to 127.0.0.1 on unserved port 4090
Jan 31 08:02:49 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:3553 to 127.0.0.1 on unserved port 4090
Jan 31 08:10:46 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:3683 to 127.0.0.1 on unserved port 4090
Jan 31 08:11:30 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:3703 to 127.0.0.1 on unserved port 4090
Jan 31 08:26:33 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:3925 to 127.0.0.1 on unserved port 4090
Jan 31 08:37:31 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:4069 to 127.0.0.1 on unserved port 4090
Jan 31 08:43:49 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:4128 to 127.0.0.1 on unserved port 4090
Jan 31 08:56:17 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:4488 to 127.0.0.1 on unserved port 4090
Jan 31 09:02:55 MyServer kernel: securityalert: tcp if=lo0 from
127.0.0.1:4660 to 127.0.0.1 on unserved port 4090
```

This one was interesting...turned out to be a misconfigured internal Netscape browser trying to proxy localhost to localhost on port 4090.

7.

```
Jan 27 16:47:51 MyServer kernel: securityalert: tcp if=exp0 from
195.159.0.90:6667 to X.X.X.X on unserved port 1444
```

Someone from Norway trying to IRC to us on port 1444.

8.

```
Mar 3 12:29:48 MyServer kernel: Packet log: input ACCEPT eth0 PROTO=1
209.184.87.221:8 X.X.X.X:0 L=60 S=0x00 I=49503 F=0x0000 T=23 (#18)
Mar 3 12:29:49 MyServer kernel: Packet log: input ACCEPT eth0 PROTO=1
209.184.87.221:8 X.X.X.X:0 L=60 S=0x00 I=50015 F=0x0000 T=23 (#18)
Mar 3 12:29:50 MyServer kernel: Packet log: input ACCEPT eth0 PROTO=1
209.184.87.221:8 X.X.X.X:0 L=60 S=0x00 I=50527 F=0x0000 T=23 (#18)
Mar 3 12:29:51 MyServer kernel: Packet log: input ACCEPT eth0 PROTO=1
209.184.87.221:8 X.X.X.X:0 L=60 S=0x00 I=51039 F=0x0000 T=23 (#18)
Mar 3 12:37:37 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:3427 X.X.X.X:1 L=44 S=0x10 I=27746 F=0x4000 T=119 SYN (#41)
Mar 3 12:37:37 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:3428 X.X.X.X:2 L=44 S=0x10 I=28002 F=0x4000 T=119 SYN (#41)
Mar 3 12:37:37 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:3429 X.X.X.X:3 L=44 S=0x10 I=28258 F=0x4000 T=119 SYN (#41)
>>> Continues through the entire range of ports<<<<
```

```
Mar 3 12:38:26 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:4443 X.X.X.X:1017 L=44 S=0x10 I=39526 F=0x4000 T=119 SYN
(#41)
Mar 3 12:38:26 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:4444 X.X.X.X:1018 L=44 S=0x10 I=39782 F=0x4000 T=119 SYN
```

```
(#41)
Mar  3 12:38:26 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:4445 X.X.X.X:1019 L=44 S=0x10 I=40038 F=0x4000 T=119 SYN
(#41)
Mar  3 12:38:26 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:4446 X.X.X.X:1020 L=44 S=0x10 I=40294 F=0x4000 T=119 SYN
(#41)
Mar  3 12:38:26 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:4447 X.X.X.X:1021 L=44 S=0x10 I=40806 F=0x4000 T=119 SYN
(#41)
Mar  3 12:38:26 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:4448 X.X.X.X:1022 L=44 S=0x10 I=41062 F=0x4000 T=119 SYN
(#41)
Mar  3 12:38:26 MyServer kernel: Packet log: input DENY eth0 PROTO=6
209.184.87.221:4449 X.X.X.X:1023 L=44 S=0x10 I=41318 F=0x4000 T=119 SYN
(#41)
```

This person from Southwestern Bell scans the entire range of low ports. Points to notice however. Starts with a low port (8) using icmp and stays there when he scans for port zero on my box. Then jumps to a high port (3427) using tcp and increments the source port when scanning the other destination ports (1-1023). Also notice he repeats the port zero scan 4 times before moving on to the other ports. Looks like he may have combined two scanning tool source codes to get this result or he ran two tools in succession.

9.

```
Feb 28 03:42:32 MyServer named[18977]: unapproved AXFR from
[195.153.248.240].4863 for "111.BBB.CCC" (acl)
Feb 28 03:55:14 MyServer named[18977]: unapproved AXFR from
[195.153.248.240].1087 for "222.BBB.CCC" (acl)
Feb 28 04:04:02 MyServer named[18977]: unapproved AXFR from
[195.153.248.240].1118 for "333.BBB.CCC" (acl)
Feb 28 04:21:03 MyServer named[18977]: unapproved AXFR from
[195.153.248.240].1357 for "444.BBB.CCC" (acl)
Feb 28 05:11:36 MyServer named[18977]: unapproved AXFR from
[195.153.248.240].1934 for "555.BBB.CCC" (acl)
Feb 28 05:19:26 MyServer named[18977]: unapproved AXFR from
[195.153.248.240].2021 for "666.BBB.CCC" (acl)
Feb 28 05:29:43 MyServer named[18977]: unapproved AXFR from
[195.153.248.240].2161 for "777.BBB.CCC" (acl)
```

CORPEX-NET (PSInet lan) a web hosting company tried to pull our DNS Zone files unsuccessfully.

10.

```
Nov 20 18:40:24 MyServer pop3[9437]: connect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110
Nov 20 18:40:24 MyServer pop3[9437]: disconnect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110 in=0 out=0
duration=0
Nov 20 18:40:24 MyServer pop3[9438]: connect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110
Nov 20 18:40:24 MyServer pop3[9438]: disconnect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110 in=0 out=0
duration=0
Nov 20 18:40:24 MyServer pop3[9439]: connect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110
Nov 20 18:40:24 MyServer pop3[9439]: disconnect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110 in=0 out=0
duration=0
Nov 20 18:40:27 MyServer pop3[9440]: connect
```

```
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110
Nov 20 18:40:27 MyServer pop3[9440]: disconnect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110 in=0 out=0
duration=0
Nov 20 18:40:28 MyServer pop3[9436]: connect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110
Nov 20 18:40:28 MyServer pop3[9436]: disconnect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110 in=0 out=0
duration=5
Nov 20 18:40:32 MyServer pop3[9447]: connect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110
Nov 20 18:40:32 MyServer pop3[9447]: disconnect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110 in=0 out=0
duration=0
Nov 20 18:40:39 MyServer pop3[9448]: connect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110
Nov 20 18:40:39 MyServer pop3[9448]: disconnect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110 in=0 out=0
duration=0
Nov 20 18:40:50 MyServer pop3[9449]: connect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110
Nov 20 18:40:50 MyServer pop3[9449]: disconnect
host=oo7.st.hmc.edu/134.173.46.38 destination=X.X.X.X/110 in=0 out=0
duration=0
```

<shortened for brevity>

This one is pretty obvious. Attacker from Claremont College tried to brute force the pop server user accounts verified by reviewing the login log.

© SANS Institute 2000 - 2005, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Boston SEC503	Boston, MA	Oct 09, 2017 - Oct 14, 2017	Community SANS
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced