Global Information Assurance Certification Paper

Jim Clausing
Practical to SANS 2000 IDIC exam

==========

1. Unknown probe

Desc: Crafted packet attempting to exploit unknown trojan or system vulnerability.

Analysis: This would appear to be an exploit attempt rather mapping, because with a source of loopback (127.0.0.1) the attacker can't expect to get a reply. IANA says

```
#                           Sudhakar Rajamannar <mobius1@cerfnet.com>
gridgen-elmd    1542/tcp    gridgen-elmd
#                           John R. Chawner +1 817 354-1004
simba-cs        1543/tcp    simba-cs
```

I don't know what either of those services is, but there is nothing running on any of my machines on either of those ports. None of the trojan port lists I no of listed either of those ports. The attacker is likely scanning a number of machines or is at least busy doing other things, notice the difference in IP ID #'s, indicating 46 other packets between the first 2 and 105 packets between the next 2 (assuming that ID's are incremented by 256 for each packet). Notice the backoff between attempts (3 seconds, then 6, then 12) a very nice exponential backoff. My firewall is blocking unrouteable addresses, so I am not vulnerable, but I wish I could see more network traffic to see if this was being directed against more machines than just mine on this network.

Severity: Medium/high (would be high if fw weren't blocking 127.x.x.x)

```
Mar 18 02:03:10 gauss kernel: Packet log: input DENY ppp0 PROTO=6
127.0.0.1:31509 my.machine.at.home:1542 L=40 S=0x00 I=50435 F=0x0000 T=64 (#9)
Mar 18 02:03:13 gauss kernel: Packet log: input DENY ppp0 PROTO=6
127.0.0.1:31509 my.machine.at.home:1542 L=40 S=0x00 I=62211 F=0x0000 T=64 (#9)
Mar 18 02:03:19 gauss kernel: Packet log: input DENY ppp0 PROTO=6
127.0.0.1:31509 my.machine.at.home:1542 L=40 S=0x00 I=23556 F=0x0000 T=64 (#9)
Mar 18 02:03:31 gauss kernel: Packet log: input DENY ppp0 PROTO=6
127.0.0.1:31509 my.machine.at.home:1542 L=40 S=0x00 I=11013 F=0x0000 T=64 (#9)
Mar 18 02:03:44 gauss kernel: Packet log: input DENY ppp0 PROTO=6
127.0.0.1:31509 my.machine.at.home:1543 L=40 S=0x00 I=61189 F=0x0000 T=64 (#9)
Mar 18 02:03:47 gauss kernel: Packet log: input DENY ppp0 PROTO=6
127.0.0.1:31509 my.machine.at.home:1543 L=40 S=0x00 I=9734 F=0x0000 T=64 (#9)
Mar 18 02:03:53 gauss kernel: Packet log: input DENY ppp0 PROTO=6
127.0.0.1:31509 my.machine.at.home:1543 L=40 S=0x00 I=37126 F=0x0000 T=64 (#9)
```

---

2. A couple of people trolling for NetBus

Desc: Probes for the NetBus trojan

Analysis: These folks are just trolling hoping to find a machine running netbus (known trojan that runs on port 12345). In the first and third cases, the IP ID #'s increase by 256 indicating they are consecutive packets from the source machine. They aren't particularly fast, but still clearly automated. In the second case, the IP ID numbers differ by 1536 indicating 6 packets in 3 seconds, not fast but the machine is obviously doing something else as well. In the fourth one, the machine is also doing something else, though not very

heavily loaded. The IP ID numbers differ by 512 (indicating another packet in between) and the 2 packets are 3 seconds apart. Since the target is a Unix box, these probes are merely annoying.

Severity: Low

```
Apr  7 21:25:52 gauss kernel: Packet log: input DENY ppp0 PROTO=6
24.29.76.142:1514 me.at.home.186:12345 L=48 S=0x00 I=6775 F=0x4000 T=112 SYN
(#26)
Apr  7 21:25:55 gauss kernel: Packet log: input DENY ppp0 PROTO=6
24.29.76.142:1514 me.at.home.186:12345 L=48 S=0x00 I=7031 F=0x4000 T=112 SYN
(#26)


Apr  7 21:26:47 gauss kernel: Packet log: input DENY ppp0 PROTO=6
209.90.222.153:1800 me.at.home.186:12345 L=44 S=0x00 I=55315 F=0x4000 T=111 SYN
(#26)
Apr  7 21:26:50 gauss kernel: Packet log: input DENY ppp0 PROTO=6
209.90.222.153:1800 me.at.home.186:12345 L=44 S=0x00 I=56851 F=0x4000 T=111 SYN
(#26)


04/07-22:19:47.635071 209.143.42.87:1584 ->  me.at.home.186:12345
TCP TTL:121 TOS:0x0 ID:18698  DF
**S***** Seq: 0x21C8F9   Ack: 0x0   Win: 0x2000
TCP Options =>  MSS: 536 NOP NOP SackOK

04/07-22:19:48.665048 209.143.42.87:1584 ->  me.at.home.186:12345
TCP TTL:121 TOS:0x0 ID:18954  DF
**S***** Seq: 0x21C8F9   Ack: 0x0   Win: 0x2000
TCP Options =>  MSS: 536 NOP NOP SackOK

04/07-22:19:50.605059 209.143.42.87:1584 ->  me.at.home.186:12345
TCP TTL:121 TOS:0x0 ID:19210  DF
**S***** Seq: 0x21C8F9   Ack: 0x0   Win: 0x2000
TCP Options =>  MSS: 536 NOP NOP SackOK

04/07-22:19:51.625055 209.143.42.87:1584 ->  me.at.home.186:12345
TCP TTL:121 TOS:0x0 ID:19466  DF
**S***** Seq: 0x21C8F9   Ack: 0x0   Win: 0x2000
TCP Options =>  MSS: 536 NOP NOP SackOK


04/07-22:23:00.535062 148.235.8.111:1816 ->  me.at.home.186:12345
TCP TTL:18 TOS:0x0 ID:59149  DF
**S***** Seq: 0x3498BD   Ack: 0x0   Win: 0x2000
TCP Options =>  MSS: 1460

04/07-22:23:03.935088 148.235.8.111:1816 ->  me.at.home.186:12345
TCP TTL:18 TOS:0x0 ID:59661  DF
**S***** Seq: 0x3498BD   Ack: 0x0   Win: 0x2000
TCP Options =>  MSS: 1460
```

---

3. NULL scan

   Desc: A TCP packet with no flags set

   Analysis: These are crafted packets (implying intent) designed to evade defenses and possibly to do TCP stack fingerprinting (OS identification). Interestingly, the attacker probably already has some information about the target since it is going to the https port and the target machine does, in fact, happen to be our web server. The attacker also may be quite busy, notice the jump in IP ID #'s. This isn't the final attack, this is

still in the information gathering stage, but does bear some watching. The changing window sizes (1075, 1840, and 4472) seem a little odd as do the 3rd & 4th bytes (7E 7E). That may be useful as a signature if the tool doing the probe can be identified.

Severity: low (but keep your eyes open)

```
[**] NULL Scan [**]
03/16-11:47:10.043580 171.222.226.202:10311 ->  forune.500.com.webserver:443
TCP TTL:49 TOS:0x0 ID:266  DF
****** Seq: 0x5FCC3D0   Ack: 0x0   Win: 0x433
1C DC 7E 7E 6C 73                                ..~~ls

[**] NULL Scan [**]
03/16-11:47:17.421317 171.222.226.202:10312 ->  forune.500.com.webserver:443
TCP TTL:49 TOS:0x0 ID:279  DF
****** Seq: 0x79543D0   Ack: 0x0   Win: 0x730
56 6B 7E 7E 37 61                                Vk~~7a

[**] NULL Scan [**]
03/16-11:49:16.944876 171.222.226.202:10319 ->  forune.500.com.webserver:443
TCP TTL:49 TOS:0x0 ID:368  DF
****** Seq: 0x5458426   Ack: 0x0   Win: 0x1178
D0 38 7E 7E 0A 3C                                .8~~. <
```

---

4. Unsolicited port unreach messages - forgive me for being so chatty with this trace, but I spent probably too much time investigating this one, and so you get the long version of the story.

   Desc:
   So there I am, sitting at home reading the GIAC page and running snort in another window, not really expecting to see much because this is a PPP connection, when I start getting these messages, about 1 per minute. The thing that piques my interest is that this is all of the activity, I don't see packets going out that could be generating this.

   Analysis:
   Aha, says I, someone spoofing my address. But what exactly is all this data in the packet (and which port on which machine was unreachable)? I run right over to my bookshelf and pull out my handy, dandy _TCP/IP Illustrated, Vol. 1_.

   Well, according to the book, the ICMP unreachable messages consist of 1 byte of type(3), 1 byte of code(also 3 for port unreach), 2 bytes of checksum, 4 bytes of 0's and the IP header and 1st 8 bytes of the IP datagram (but I see a lot more than 8 bytes, there, well, we'll assume we have more of the packet). Okay, snort must have decoded the type, code, and checksum, but I see 4 bytes of 0 and stuff that looks suspiciously like an IP packet.

   Okay, if I look at byte 9 of the encapsulated packet, it appears to be TCP (protocol 6). Looking further I find my IP address in hex as the src IP. The dest IP isn't immediately familiar to me (and by now, I've gone off-line). Next are source and destination ports, 1131 and 23185. Neither of those ports look familiar to me. Okay, if this contains more of the TCP packet, then that 11 on the 4th line is the byte with the flags and the 11 suggests a FIN/ACK. Okay, probably nothing too serious, but still strange. On further examination, these aren't all the same, they seem to be alternating. The second (and subsequent even numbered)

packet(s) have source port 1130 and dest port 21. Okay, earlier I had been ftp-ing some things, but they had all long since completed or been aborted. So, who is 140.142.4.227 (the dest IP address in the encapsulated packet). When I get back on-line the next day at work, I do a quick DNS lookup and discover, the IP address belongs to ftp2.cac.washington.edu. Sigh, one of the things I had been ftp-ing was pine-4.21 from (you guessed it) cac.washington.edu. Mystery solved (sort of).

I still am uncertain why these were coming in at such regular intervals when I wasn't seeing any stimulus coming from my machine, but I will chalk this one up as a false positive (and an education in ICMP).

Severity: None

```
04/07-22:23:40.065163 another.mach.at.my-isp ->   my.machine.at.home
ICMP TTL:255 TOS:0xC0 ID:21198
DESTINATION UNREACHABLE: PORT UNREACHABLE
00 00 00 00 45 00 00 34 52 CD 00 00 40 06 14 00  ....E..4R...@...
xx xx xx xx 8C 8E 04 E3 04 6B 5A 91 86 CD D4 C3  xxxx.....kZ.....
86 22 4A F7 80 11 7C 70 A3 E7 00 00 01 01 08 0A  ."J...|p........
00 11 CC 44 2B 5F C8 7F 02 00 00 00 CC 00 78 00  ...D+_........x.
BE 00 00 00 10 00 00 03 01 00 00 00               ............

04/07-22:24:41.125150 another.mach.at.my-isp ->   my.machine.at.home
ICMP TTL:255 TOS:0xC0 ID:21284
DESTINATION UNREACHABLE: PORT UNREACHABLE
00 00 00 00 45 00 00 34 53 23 00 00 40 06 00 2C  ....E..4S#..@..,
xx xx xx xx 8C 8E 04 E3 04 6A 00 15 86 7A 35 4C  xxxx.....j...z5L
85 3B B7 9B 80 11 7F 88 3E 45 00 00 01 01 08 0A  .;......>  E......
00 11 E4 1E 2B 5C A1 BD 02 00 00 00 FE 01 49 00  ....+\........I.
F1 01 18 00 10 00 00 02 0B 00 00 00               ............

04/07-22:25:40.065154 another.mach.at.my-isp ->   my.machine.at.home
ICMP TTL:255 TOS:0xC0 ID:21361
DESTINATION UNREACHABLE: PORT UNREACHABLE
00 00 00 00 45 00 00 34 53 70 00 00 40 06 14 00  ....E..4Sp..@...
xx xx xx xx 8C 8E 04 E3 04 6B 5A 91 86 CD D4 C3  xxxx.....kZ.....
86 22 4A F7 80 11 7C 70 75 07 00 00 01 01 08 0A  ."J...|pu.......
00 11 FB 24 2B 5F C8 7F 02 00 00 00 CC 00 78 00  ...$+_........x.
BE 00 00 00 10 00 00 03 01 00 00 00               ............

04/07-22:26:41.125163 another.mach.at.my-isp ->   my.machine.at.home
ICMP TTL:255 TOS:0xC0 ID:21453
DESTINATION UNREACHABLE: PORT UNREACHABLE
00 00 00 00 45 00 00 34 53 CC 00 00 40 06 00 2C  ....E..4S...@..,
xx xx xx xx 8C 8E 04 E3 04 6A 00 15 86 7A 35 4C  xxxx.....j...z5L
85 3B B7 9B 80 11 7F 88 0F 65 00 00 01 01 08 0A  .;.......e......
00 12 12 FE 2B 5C A1 BD 02 00 00 00 FE 01 49 00  ....+\........I.
F1 01 18 00 10 00 00 02 0B 00 00 00               ............
```

---

5. Source port 0 probe

Desc: Crafted packet. TCP port 0 is reserved according to IANA so I shouldn't see any packets with it as source or destination.

Analysis: The strange part is the destination ports, they don't correspond to anything I've been able to find on any of the trojan port lists. Interesting that these are resets, window size of 0 and those pesky 7E 7E bytes (see NULL scan above). They are spaced out quite a bit in time so I'm wondering if this isn't in response to queries to web servers (as noted

```
        below, the machine being probed is the HTTP proxy).
        Unfortunately, I no longer have access to the proxy
        logs to attempt a correlation.  The source of the probe is
        IP address space registerd to Exodus Communications, but there
        doesn't appear to be a web server running there.

        Severity: Medium

[**] TCP Source port 0 probe [**]
03/14-15:13:34.162394 216.35.17.230:0 ->  our.http.proxy.server:57616
TCP TTL:54 TOS:0x0 ID:28824
**R*A* Seq: 0x349050FE   Ack: 0x8C3B8268   Win: 0x0
F5 B6 7E 7E 2F 31                              ..~~/1

[**] TCP Source port 0 probe [**]
03/14-16:27:16.986748 216.35.17.230:0 ->  our.http.proxy.server:47440
TCP TTL:54 TOS:0x0 ID:8130
**R*A* Seq: 0x684C1A7D   Ack: 0xF31CCB92   Win: 0x0
02 BA 7E 7E B4 6C                              ..~~.l

[**] TCP Source port 0 probe [**]
03/15-10:11:48.265833 216.35.17.230:0 ->  our.http.proxy.server:53485
TCP TTL:54 TOS:0x0 ID:18004
**R*A* Seq: 0x1B4F0F7D   Ack: 0x7330D71C   Win: 0x0
AA 08 7E 7E 56 3D                              ..~~V=

[**] TCP Source port 0 probe [**]
03/16-10:36:34.812340 216.35.17.230:0 ->  our.http.proxy.server:60006
TCP TTL:54 TOS:0x0 ID:55314
**R*A* Seq: 0xF47D2AAA   Ack: 0xBA74F269   Win: 0x0
46 15 7E 7E 67 20                              F.~~g

-------------------------------------------------------------------------

6.      pcAnywhere probe

Note: this detect came from the GIAC page on 13 Apr.

        Desc: pcAnywhere probe

        Analysis: versions of pcAnywhere prior to 7.52 used udp port
        22 for its status port (tells you if someone is already
        using pcanywhere).  This was not properly registered with IANA.
        Beginning with version 7.52 they used properly registered ports
        and the status port was moved to port 5632.  Versions 8.x and
        9.x will by default check both unless a registry change is made.
        Unfortunately, pcAnywhere also has an annoying tendency to go
        out and look for other pcAnywhere machines on the same subnet
        (unless you explicitly configure it not to).  This could be
        extremely dangerous to the advertiser with a cable
        modem as appears to be the case here.  Given, that the 2 machines
        involved here are on the same subnet, and that there doesn't
        appear to have been any follow up attempts to connect other
        than the status query that is likely what is happening here.

        Severity: Low/medium (since pcAnywhere is inherently so dangerous anyway)

        Suggested further reading:
        <http://service1.symantec.com/SUPPORT/pca.nsf/pfdocs/1998122810210812>
        <http://www.infosecuritymag.com/july99/remote.htm>

Apr 11 21:59:17 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:3758 to 24.3.21.199 on unserved port 22
Apr 11 22:25:48 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:4007 to 24.3.21.199 on unserved port 22
Apr 11 22:26:18 cc1014244-a kernel: securityalert: udp if=ef0 from
```

24.3.21.225:4013 to 24.3.21.199 on unserved port 5632

---

7. Trojan Probe 1
Note: This detect and the one that follows are from the GIAC page, 11-Apr-2000.

Desc: SubSeven & NetBus probes

Analysis: The machine in question is being scanned in pretty short order for variations of 2 well known trojans, SubSeven and NetBus (I have noted which immediately before it). Both allow remote control of a Windows box. The attack is clearly automated and targeted at specific trojans. There is a firewall blocking access to these ports, so the target is at relatively low risk.

Severity: Low

Sub7
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from 216.77.245.249:2606 to 24.3.21.199 on unserved port 1243
NetBus
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from 216.77.245.249:2607 to 24.3.21.199 on unserved port 12345
NetBus 2 Pro
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from 216.77.245.249:2608 to 24.3.21.199 on unserved port 20034
Sub7
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from 216.77.245.249:2609 to 24.3.21.199 on unserved port 27374

---

8. Multi-trojan scan
Note: This detect is from the GIAC page, 11-Apr-2000.

Desc: Scan for multiple trojans

Analysis: One thing I must say for this gal/guy, s/he has a much more complete trojan list than I have been able to find. Where I have been able to find the info, I have identified the trojan they are probing for (with thanx to the folks that have produced the various trojan lists, my favorites are listed below). Given the timestamps, this is a serious automated probe. This machine is probably the only one being probed at the moment (based on the fact that there are no gaps in the increasing source ports). I would guess that the purpose is to compile a list of machines infected with the various trojans in order to go back later with the targeted exploit (God help us all if this person has a tool that automatically launches the exploit, too).

The source IP belongs to a class C registered to FutureNet Internet Solutions and coming out of Turkey.

http://www.sans.org/y2k/ports.htm
http://www.simovits.com/nyheter9902.html
http://www.commodon.com/threat/threat-all.htm
http://www.silverdragon.dyndns.org/trojans/

Severity: Medium/high

Sub7
Apr 6 19:44:05.798874 193.192.119.110,2435 -> 10.0.8.87,1243 PR tcp len 20 48 -S

```
Netsphere
Apr 6 19:44:05.799356 193.192.119.110,2436 -> 10.0.8.87,30100 PR tcp len 20 48 -S
School Bus
Apr 6 19:44:05.803185 193.192.119.110,2437 -> 10.0.8.87,54321 PR tcp len 20 48 -S
Deep Throat
Apr 6 19:44:05.829239 193.192.119.110,2438 -> 10.0.8.87,6670 PR tcp len 20 48 -S
Unknown (prosiak?  they already do 22222 & 33333)
Apr 6 19:44:05.829796 193.192.119.110,2439 -> 10.0.8.87,55555 PR tcp len 20 48 -S
Unknown
Apr 6 19:44:05.830331 193.192.119.110,2440 -> 10.0.8.87,1257 PR tcp len 20 48 -S
Unknown
Apr 6 19:44:05.830749 193.192.119.110,2443 -> 10.0.8.87,6500 PR tcp len 20 48 -S
GirlFriend (passwd stealer)
Apr 6 19:44:05.831771 193.192.119.110,2444 -> 10.0.8.87,21554 PR tcp len 20 48 -S
WinCrash
Apr 6 19:44:05.835240 193.192.119.110,2446 -> 10.0.8.87,5742 PR tcp len 20 48 -S
NetMonitor
Apr 6 19:44:05.835268 193.192.119.110,2447 -> 10.0.8.87,7307 PR tcp len 20 48 -S
Priority
Apr 6 19:44:05.870399 193.192.119.110,2448 -> 10.0.8.87,16969 PR tcp len 20 48 -S
Psyber Stream Server (streaming audio)
Apr 6 19:44:05.870428 193.192.119.110,2449 -> 10.0.8.87,1170 PR tcp len 20 48 -S
Millenium?
Apr 6 19:44:05.881925 193.192.119.110,2450 -> 10.0.8.87,20000 PR tcp len 20 48 -S
ICQtrojan?
Apr 6 19:44:05.893451 193.192.119.110,2451 -> 10.0.8.87,4950 PR tcp len 20 48 -S
EvilFTP, UglyFTP, WhackJob
Apr 6 19:44:05.905064 193.192.119.110,2452 -> 10.0.8.87,23456 PR tcp len 20 48 -S
WinHole, WinGate, SOCKS proxy server
Apr 6 19:44:05.919541 193.192.119.110,2453 -> 10.0.8.87,1080 PR tcp len 20 48 -S
Attack FTP, Back Construction, Satanz Backdoor, ServeU
Apr 6 19:44:05.919871 193.192.119.110,2454 -> 10.0.8.87,666 PR tcp len 20 48 -S
Blade Runner, Back Construction
Apr 6 19:44:05.920495 193.192.119.110,2455 -> 10.0.8.87,5400 PR tcp len 20 48 -S
Doly
Apr 6 19:44:05.921098 193.192.119.110,2456 -> 10.0.8.87,1011 PR tcp len 20 48 -S
NetBus 2 Pro
Apr 6 19:44:08.885068 193.192.119.110,2434 -> 10.0.8.87,20034 PR tcp len 20 48 -S

---------------------------------------------------------------------

9.      SubSeven probe

        Desc: Probe for the SubSeven trojan

        Analysis: While I was sitting here working on these, I got probed
        for SubSeven.  This is a pretty well known remote control trojan
        that runs on Windows machines.  The packet filter blocks incoming
        SYN connections, and the windows boxes behind it are NAT-ed, so
        we are not at terrible risk here.  This is probably trolling (or
        perhaps the previous machine to have this IP address was vulnerable).
        Given the jump in IP ID, this machine could be scanning a large
        number of machines (since this is a ppp connection, we can't really
        see if other machines on the same subnet are also being scanned).

        Severity:  Low

Apr 15 13:36:17 gauss kernel: Packet log: input DENY ppp0 PROTO=6
209.179.44.199:2418 my.machine.at.home:1243 L=48 S=0x00 I=20784 F=0x4000
T=116 SYN (#26)
Apr 15 13:36:20 gauss kernel: Packet log: input DENY ppp0 PROTO=6
209.179.44.199:2418 my.machine.at.home:1243 L=48 S=0x00 I=63024 F=0x4000
T=116 SYN (#26)

---------------------------------------------------------------------
```

10. port scan

Desc: Port scan (probably nmap)

Analysis: First, the attacker pings my machine (which my machine responds to). Then it begins probing a large number of ports (I have just given the first few). It starts off with port 80 (HTTP) and TCP port 53 (DNS), then starts probing various other ports, it returns to each port several times. Then it starts probing without the SYN flag set. If this is nmap it is probably using other strange combinations of flags. Note, it tries each port 3 times in a row when it tries without the SYN. Also, note that there are few gaps in the IP ID number indicating that I am the only target at the time of the probe. This appears to be purely information gathering and not active exploit attempts.

Severity: Medium

```
Apr  7 21:28:47 gauss kernel: Packet log: input ACCEPT ppp0 PROTO=1 216.112.42.62:8
me.at.home.186:0 L=28 S=0x00 I=56234 F=0x4000 T=46 (#12)
Apr  7 21:28:47 gauss kernel: Packet log: output ACCEPT ppp0 PROTO=1 me.at.home.186:0
216.112.42.62:0 L=28 S=0x00 I=6476 F=0x0000 T=255 (#11)
Apr  7 21:28:47 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:47620
me.at.home.186:80 L=40 S=0x00 I=56235 F=0x4000 T=31 (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41691
me.at.home.186:53 L=44 S=0x00 I=56236 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41692
me.at.home.186:469 L=44 S=0x00 I=56237 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41693
me.at.home.186:5714 L=44 S=0x00 I=56238 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41694
me.at.home.186:940 L=44 S=0x00 I=56239 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41695
me.at.home.186:543 L=44 S=0x00 I=56240 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41696
me.at.home.186:332 L=44 S=0x00 I=56241 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41697
me.at.home.186:357 L=44 S=0x00 I=56242 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41698
me.at.home.186:58 L=44 S=0x00 I=56243 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41699
me.at.home.186:72 L=44 S=0x00 I=56244 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41700
me.at.home.186:1664 L=44 S=0x00 I=56245 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41701
me.at.home.186:628 L=44 S=0x00 I=56246 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41706
me.at.home.186:53 L=44 S=0x00 I=56247 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41707
me.at.home.186:469 L=44 S=0x00 I=56248 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41708
me.at.home.186:5714 L=44 S=0x00 I=56249 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41709
me.at.home.186:940 L=44 S=0x00 I=56250 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41710
me.at.home.186:543 L=44 S=0x00 I=56251 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41711
me.at.home.186:332 L=44 S=0x00 I=56252 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41712
me.at.home.186:357 L=44 S=0x00 I=56253 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41713
me.at.home.186:58 L=44 S=0x00 I=56254 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41714
me.at.home.186:72 L=44 S=0x00 I=56255 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41715
```

```
me.at.home.186:1664 L=44 S=0x00 I=56256 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41716
me.at.home.186:628 L=44 S=0x00 I=56257 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41726
me.at.home.186:53 L=44 S=0x00 I=56258 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41727
me.at.home.186:469 L=44 S=0x00 I=56259 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41728
me.at.home.186:5714 L=44 S=0x00 I=56260 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41729
me.at.home.186:940 L=44 S=0x00 I=56261 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41730
me.at.home.186:543 L=44 S=0x00 I=56262 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41731
me.at.home.186:332 L=44 S=0x00 I=56263 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41732
me.at.home.186:357 L=44 S=0x00 I=56264 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41733
me.at.home.186:58 L=44 S=0x00 I=56265 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41734
me.at.home.186:72 L=44 S=0x00 I=56266 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41735
me.at.home.186:1664 L=44 S=0x00 I=56267 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:48 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41736
me.at.home.186:628 L=44 S=0x00 I=56268 F=0x4000 T=245 SYN (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41691
me.at.home.186:53 L=40 S=0x00 I=56269 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41706
me.at.home.186:53 L=40 S=0x00 I=56270 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41726
me.at.home.186:53 L=40 S=0x00 I=56271 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41692
me.at.home.186:469 L=40 S=0x00 I=56272 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41707
me.at.home.186:469 L=40 S=0x00 I=56273 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41727
me.at.home.186:469 L=40 S=0x00 I=56274 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41694
me.at.home.186:940 L=40 S=0x00 I=56278 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41709
me.at.home.186:940 L=40 S=0x00 I=56279 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41729
me.at.home.186:940 L=40 S=0x00 I=56280 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41695
me.at.home.186:543 L=40 S=0x00 I=56281 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41710
me.at.home.186:543 L=40 S=0x00 I=56282 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41730
me.at.home.186:543 L=40 S=0x00 I=56283 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41696
me.at.home.186:332 L=40 S=0x00 I=56284 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41711
me.at.home.186:332 L=40 S=0x00 I=56285 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41731
me.at.home.186:332 L=40 S=0x00 I=56286 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41697
me.at.home.186:357 L=40 S=0x00 I=56287 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41712
me.at.home.186:357 L=40 S=0x00 I=56288 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41732
me.at.home.186:357 L=40 S=0x00 I=56289 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41698
me.at.home.186:58 L=40 S=0x00 I=56290 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41713
me.at.home.186:58 L=40 S=0x00 I=56291 F=0x4000 T=245 (#26)
```

```
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41733
me.at.home.186:58 L=40 S=0x00 I=56292 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41699
me.at.home.186:72 L=40 S=0x00 I=56293 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41714
me.at.home.186:72 L=40 S=0x00 I=56294 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41734
me.at.home.186:72 L=40 S=0x00 I=56295 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41701
me.at.home.186:628 L=40 S=0x00 I=56299 F=0x4000 T=245 (#26)
Apr  7 21:28:49 gauss kernel: Packet log: input DENY ppp0 PROTO=6 216.112.42.62:41736
me.at.home.186:628 L=40 S=0x00 I=56301 F=0x4000 T=245 (#26)
...this continues for another 7 minutes...
```

Last Updated: September 26th, 2017

Upcoming Training

SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	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
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	Tysons, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 16, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced