Global Information Assurance Certification Paper

*** Northcutt, Gil reads the traces to us and shows he fully comprehends the material. Solid use of an analysis process. 76 *

Gil Trenum
Submitted as the practical requirement for the Level2 IDIC exam taken on 25 March 2000.

Since I am an active duty member of the Navy stationed at an Intelligence command, I think I might be drawn & quartered if I used actual traces from my job (the Navy having been especially burned by security issues the last couple of decades). Therefore, I tried to use interesting traces from the GIAC site.

Trace #1 -- 3 March Archives

Mar 2 03:55:30 dns3 portsentry[301]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 03:55:40 dns3 portsentry[301]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 03:55:46 dns3 portsentry[301]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 03:56:22 dns3 portsentry[301]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 04:02:46 dns3 portsentry[301]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 79

Mar 2 04:02:46 dns3 in.telnetd[9210]: refused connect from 24.66.233.245.ab.wave.home.com

Mar 2 04:02:46 dns3 portsentry[301]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 04:02:47 dns3 in.telnetd[9211]: refused connect from 24.66.233.245.ab.wave.home.com

Mar 2 04:04:19 dns3 portsentry[301]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 79

Mar 2 04:04:19 dns3 in.telnetd[9213]: refused connect from 24.66.233.245.ab.wave.home.com

Mar 2 04:04:20 dns3 portsentry[301]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 04:04:20 dns3 in.telnetd[9214]: refused connect from 24.66.233.245.ab.wave.home.com

Above grouping repeated 2 more times

Mar 2 03:55:30 dns1 portsentry[172871]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 03:55:40 dns1 portsentry[172871]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 03:55:46 dns1 portsentry[172871]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 03:56:22 dns1 portsentry[172871]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 04:02:46 dns1 portsentry[172871]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 79

Mar 2 04:02:46 dns1 telnetd[120098]: refused connect from 24.66.233.245.ab.wave.home.com

Mar 2 04:02:47 dns1 portsentry[172871]: attackalert: Connect from host: 24.66.233.245.ab.wave.home.com/24.66.233.245 to TCP port: 143

Mar 2 04:02:47 dns1 telnetd[131546]: refused connect from 24.66.233.245.ab.wave.home.com

Above grouping repeated 3 more times

This trace reveals targeting of the DNS servers (dns3 & dns1). Each server gets four Imap probes (port 143) followed by an interesting packet pattern:

- Finger (port 79)
- Telnet
- Imap (port 143)
- Telnet

This group of four packets comes in about two seconds, waits for a few minutes, and then repeats. If the trace information is rearranged and sorted by time it becomes obvious that identical packets are coming in to the two DNS servers simultaneously.

The initial set of imap probes initially looked like they could either be scripted, or possibly (although very unlikely) manually executed. When you factor in the simultaneous activity on both DNS servers, it is almost surely scripted. After this the attacker apparently switched tools, based on the 6-minute delay between the initial flurry of Imap probes and the start of the repeating four-packet grouping described. This second activity is definitely automated (eight packets to at least two separate machines in approx 2 seconds). Big question; what is happening in the time interval between the repeated patterns, is the attacker waiting, or is he going after more machines on other networks. Based on the nature of the activity and the notoriety of the source (home.com) I would definitely call this activity hostile. Also, since the attacker apparently changed tools, I would expect to see more activity with different tools if this attack doesn't work.

Severity = (Criticality + Lethality) – (System CM + Network CM)
= (5 + 3) – (3 + 3) = 2
Must always be concerned about activity directed at DNS servers.

Trace #2 – 16 Feb Archives

1. Feb 10 16:14:50.644 firewall kernel: 226 IP packet dropped (advancedmed-gw.atlantic.net[209.208.13.2]->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN FIN] Port 0->109): Bad IP Header (received on interface 10.0.0.1)
2. Feb 11 13:47:32.280 firewall kernel: 226 IP packet dropped (ns.victim.com[192.168.161.2]->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN FIN] Port 0->109): Bad IP Header (received on interface 10.0.0.1)
3. Feb 11 15:51:48.965 firewall kernel: 232 Sending ICMP port unreachable. Original packet (apopkavine-ubr-c5s1-37.cfl.rr.com[24.26.110.37]-> firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN] Port 3207->111) received on interface 10.0.0.1
4. Feb 11 15:53:10.683 firewall kernel: 226 IP packet dropped (ns.victim.com[192.168.161.2]->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN FIN] Port 0->109): Bad IP Header (received on interface 10.0.0.1)

5. Feb 11 19:33:52.263 firewall kernel: 226 IP packet dropped (209.113.97.2->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN FIN] Port 0->109): Bad IP Header (received on interface 10.0.0.1)
6. Feb 11 23:53:26.226 firewall kernel: 226 IP packet dropped (133.11.148.231->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN] Port 25910->1243): Restricted Port: Protocol=TCP[SYN] Port 25910->1243 (received on interface 10.0.0.1)
7. Feb 12 19:51:10.402 firewall kernel: 226 IP packet dropped (210.220.213.240->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN] Port 2860->2766): Restricted Port: Protocol=TCP[SYN] Port 2860->2766 (received on interface 10.0.0.1)
8. Feb 13 04:00:02.869 firewall kernel: 232 Sending ICMP port unreachable. Original packet (24.130.49.191->firewall.mydomain.edu[10.0.0.1]: Protocol=UDP Port 7430->31337) received on interface 10.0.0.1
9. Feb 13 20:40:07.834 firewall kernel: 232 Sending ICMP port unreachable. Original packet (141.41.96.151->firewall.mydomain.edu[10.0.0.1]: Protocol=UDP Port 31790->31789) received on interface 10.0.0.1

Three distinct types of activity in this trace:
1. Probing of port 109 (POP2)
2. SunRPC probing
3. "Trojan trolling"

The POP2 probes (alerts 1, 2, 4, & 5) are obviously hostile: Both the SYN and the FIN flags are set, and the source port of 0 both indicated crafted packets. Reports 2 & 4 are from the same source ip, but a little over two hours apart.

The SunRPC probe in report # 3 is an attempt to identify services on a given host – i.e. fingerprinting. Although this information was not returned, the ICMP port unreachable error does convey useful information in that the host is not present, helping the intruder to map out the network.

Three of last four reports are efforts to locate various well-known Trojans.
6 is looking for the SUB 7.2 trojan
7 is probing the TCP port 2766 - From my research, this is a TCP listen port that (I think) is/was used in BSD-based versions of Unix for printing. Could be someone looking for vulnerable print daemons to exploit.
8 is probing for the standard Back Orifice port
9 is checking for Hack 'a' Tack on its well known port

Since .edu networks are such popular targets, there doesn't appear to be anything overly sophisticated in the above trace. The most likely explanation is that these are unrelated incidents of various interlopers looking for targets of opportunity.

The repeated POP2 probe is an exception. This activity is coming from another US educational institution (not sure if we can name names) which doesn't tell us a whole lot, either. The actual packet contents would provide more information in that it might be possible to identify a common tool used to craft the malformed packets, providing a more concrete connection.

One interesting thing to note from the last four reports is that three of them are originating from outside the US. This is not in and of itself unusual, but if you assume that they are all from compromised machines you can lay the foundation for a "low & slow" exploitation effort. It's a pretty long stretch, but a paranoid mindset is always a safe way to look at things.

Once again, the ICMP "port unreachable" replies in the last two packets provide a bottom level layer of information for network mapping.

Severity = (Criticality + Lethality) – (System CM + Network CM)
= (2 + 3) – (3 + 4) = -1

Trace #3 – 21 Feb 1700 Archives

```
-*> Snort! <*-
Version 1.5
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
snaplen = 68
Entering readback mode....
02/20-00:22:41.632332 24.1.45.44:2397 -> 192.0.207.38:6699
TCP TTL:118 TOS:0x0 ID:3254 DF
SF*P*U Seq: 0x680 Ack: 0xCC97022E Win: 0x5010

A
02/20-00:26:42.652956 194.217.188.7:30975 -> 192.0.208.26:49324
TCP TTL:49 TOS:0x0 ID:11191 DF
SFRPAU21 Seq: 0x78FFC0AC Ack: 0x78FFC0AC Win: 0xC0AC
TCP Options => Opt 120 (40): C0AC 78FF C0AC 78FF C0AC 78FF

A
02/20-00:26:55.175378 194.217.188.7:30975 -> 192.0.208.26:34248
TCP TTL:49 TOS:0x0 ID:14515 DF
SFRPAU21 Seq: 0x78FF85C8 Ack: 0x78FF85C8 Win: 0x85C8
TCP Options => Opt 120 (40): 85C8 78FF 85C8 78FF 85C8 78FF

A
02/20-00:26:58.734218 194.217.188.7:30975 -> 192.0.208.26:34248
TCP TTL:49 TOS:0x0 ID:15124 DF
SFRPAU21 Seq: 0x78FF85C8 Ack: 0x78FF85C8 Win: 0x85C8
TCP Options => Opt 120 (40): 85C8 78FF 85C8 78FF 85C8 78FF

A
02/20-00:27:00.634602 194.217.188.7:7766 -> 192.0.208.26:1857
TCP TTL:49 TOS:0x0 ID:15708 DF
SF**A*2 Seq: 0x34A8FC Ack: 0x2048F867 Win: 0xFE41
TCP Options => Opt 236 (40): 61E8 D161 BCF4 9819 EA84 BD08

A
02/20-00:27:05.245930 194.217.188.7:30975 -> 192.0.208.26:1480
TCP TTL:49 TOS:0x0 ID:16793 DF
SFRPAU21 Seq: 0x78FF05C8 Ack: 0x78FF05C8 Win: 0x5C8
TCP Options => Opt 120 (40): 05C8 78FF 05C8 78FF 05C8 78FF

A1
02/20-00:27:05.536097 194.217.188.7:30975 -> 192.0.208.26:50632
TCP TTL:49 TOS:0x0 ID:16821 DF
SFRPAU21 Seq: 0x78FFC5C8 Ack: 0x78FFC5C8 Win: 0xC5C8
TCP Options => Opt 120 (40): C5C8 78FF C5C8 78FF C5C8 78FF

Above packet repeated twice

A
02/20-00:27:45.246240 194.217.188.7:30723 -> 192.0.208.26:16592
TCP TTL:49 TOS:0x0 ID:26481 DF
SF**** Seq: 0x780340D0 Ack: 0x780340D0 Win: 0x40D0
TCP Options => Opt 120 (3): 40D0 Opt 208 (40): 0340 D078 0340 D078 0300

A
02/20-00:28:05.121049 194.217.188.7:30975 -> 192.0.208.26:1480
TCP TTL:49 TOS:0x0 ID:30200 DF
SFRPAU21 Seq: 0x78FF05C8 Ack: 0x78FF05C8 Win: 0x5C8
TCP Options => Opt 120 (40): 05C8 78FF 05C8 78FF 05C8 78FF

.
.
.
Solaris 2.X
02/20-01:02:08.092780 195.173.149.173:30975 -> 192.0.97.195:556
```

```
TCP TTL:240 TOS:0x0 ID:4083
SFRPAU21 Seq: 0x78FF022C Ack: 0x78FF022C Win: 0x22C
TCP Options => Opt 120 (40): 022C 78FF 022C 78FF 022C 78FF

.
.
.

02/20-03:19:09.591863 168.31.239.217:1384 -> 192.0.202.158:6688
TCP TTL:114 TOS:0x0 ID:3711 DF
SFRP*U2 Seq: 0x56E Ack: 0x42D20446 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 56 (40): 3031 3233 3435

02/20-03:19:49.866711 168.31.239.217:1385 -> 192.0.202.158:6688
TCP TTL:114 TOS:0x0 ID:12169 DF
SF*PA*2 Seq: 0x20056F Ack: 0x8F3D0430 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK EOL Opt 21 (40): 5B01 0300

02/20-03:19:52.471396 168.31.239.217:1385 -> 192.0.202.158:6688
TCP TTL:114 TOS:0x0 ID:5770 DF
SF*PA*2 Seq: 0x56F8F3D Ack: 0x200433 Win: 0x5010

02/20-03:20:18.328610 168.31.239.217:1387 -> 192.0.202.158:6688
TCP TTL:114 TOS:0x0 ID:28561 DF
SF**A* Seq: 0x56FEBD8 Ack: 0x433CDEA Win: 0x5010

02/20-03:20:33.899869 168.31.239.217:1388 -> 192.0.202.158:6688
TCP TTL:114 TOS:0x0 ID:20631 DF
SFRP**2 Seq: 0x20056F Ack: 0xF340043D Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK Opt 48 (40): 3233 3435

02/20-03:21:02.392034 168.31.239.217:32 -> 192.0.202.158:1388
TCP TTL:114 TOS:0x0 ID:9378 DF
SFRP**2 Seq: 0x1A20056F Ack: 0xF3400452 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL EOL NOP NOP NOP TS: 1702100992

02/20-03:21:09.206806 168.31.239.217:1388 -> 192.0.202.158:6688
TCP TTL:114 TOS:0x0 ID:34468 DF
SFRP**2 Seq: 0x56FF340 Ack: 0x750457 Win: 0x5010

02/20-03:21:56.676972 168.31.239.217:32 -> 192.0.202.158:1388
TCP TTL:114 TOS:0x0 ID:53429 DF
SFRP**2 Seq: 0x1A20056F Ack: 0xF3400478 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 206 (40): DABA 82D7 0014

02/20-03:22:01.321019 168.31.239.217:13 -> 192.0.202.158:1388
TCP TTL:114 TOS:0x0 ID:30903 DF
SFRP**2 Seq: 0x1A20056F Ack: 0xF340047B Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 118 (40): 2E72 6D69 2E4D

02/20-03:23:24.616519 168.31.239.217:13 -> 192.0.202.158:1392
TCP TTL:114 TOS:0x0 ID:5332 DF
SF*P*U21 Seq: 0x1A200572 Ack: 0x2CB8044D Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK EOL Opt 235 (40): B965 F900
```

Note that these Snort reports were truncated to four lines to conserve space.

This trace exhibits two major threads. In the first set of packets (labeled **A**) host 192.0.208.26 is targeted from 194.217.188.7. Ten packets are directed at it in approximately one and one half minutes. The packets are probing various high valued ports including 49324, 34248, 1480, and 50632. Eight of the packets are coming from the source port 30975. All eight have all TCP flags set. The other two packets also have anomalous flag settings. They all have TTL values of 49.

In the second thread 168.31.239.217 is targeting host 192.0.202.158. Once again ten packets arrive in a fairly short timespan, approximately 4 minutes. In this set of packets various illegal TCP flag combinations are used. The destination ports are mainly 1388 & 6688. THE TTL values of these packets are 114.

In the first set of packets an automated script is being probably being used to probe for trojans at the various high-numbered ports. A “Christmas Tree” probe (i.e. all TCP flags set) is used to indicating crafted packets. The TTL value 49 indicates that some flavor of Unix is probably being used. HPUX, Irix, Linux, and SunOS all have default TTL values of 64. MacOS also has a

default TTL of 64, but that is less likely. Since the packet id values appear to be legitimate, it is reasonable to assume the TTL values are legitimate also. Although ten packets in two minutes is not a DOS-type of rate, it is probably too fast to be manually performed. Further research indicatges that this ip address belongs to the Demon Internet – 'nuff said.

Severity = (Criticality + Lethality) – (System CM + Network CM)
= (4 + 4) – (4 + 3) = 1

A few, seemingly unrelated packets separated the two sections discussed here. It was interesting to note, although probably not relevant, that one of the packets had a TTL of 240 indicating a Solaris2.X originator. The unusual aspect is that it was the only one present with this type of originating OS.

In the second set of packets various TCP flag combinations are directed against the host. Since the packets came in fairly quickly, it is probably an automated tool also. The various TCP flag combinations against just a few ports probably indicates that Queso or some other fingerprinting tool is being used. The originating ip address in this set belongs to the Board of Regents of a major state university system here in the US. We can pretty much be assured that this host has been compromised. There is no evidence to indicate that these two sets are related.

Severity = (Criticality + Lethality) – (System CM + Network CM)
= (3 + 3) – (3 + 3) = 0

Trace #4 – 1 March Archives

Feb 28 02:10:53 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.2.36.142:1586 to 24.3.21.199 on unserved port 27374

Feb 28 06:14:45 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.67.127.237:21093 to 24.3.21.199 on unserved port 1243

Feb 28 14:30:16 cc1014244-a kernel: securityalert: udp if=ef0 from 157.238.15.63:4534 to 24.3.21.199 on unserved port 137

Feb 28 22:08:30 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:2189 to 24.3.21.199 on unserved port 22
Feb 28 22:15:45 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:2198 to 24.3.21.199 on unserved port 22
Feb 28 22:18:31 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:2210 to 24.3.21.199 on unserved port 5632
Feb 28 22:18:31 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:2210 to 24.3.21.199 on unserved port 22
Feb 28 22:24:07 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:2213 to 24.3.21.199 on unserved port 22

The first two packets are both probing for the SubSeven trojan. However, the are probably unrelated. The third packet is looking for the NetBIOS Name Service. Normally this would not attract any attention, but this trace was reported by an @home user. I'm not sure why anyone would need to be looking for NetBIOS on an individuals Internet connection. This is possibly part of a general sweep, but be on the lookout for activity in the future.

The last set of packets is interesting. Two probes to ssh, a probe to PC Anywhere port, followed by two more probes to ssh. This is made even more interesting in that the originating host is also an @home user, and probably on the same subnet! The scary part of this activity is that, if the PCAnywhere service is running and vulnerable – the attacker can get complete control of the victim.

Severity = (Criticality + Lethality) – (System CM + Network CM)
= (2 + 5) – (4 + 1) = 2

Trace #5 – 1 March Archives

Feb 29 08:20:05 dns2 in.telnetd[5298]:

```
refused connect from R-H-186-53.access.net.il
Feb 29 08:20:11 dns2 in.ftpd[5299]: refused
connect from R-H-186-53.access.net.il
Feb 29 08:20:17 dns2 portsentry[301]: attackalert:
Connect from host: R-H-186-53.access.net.il/192.117.186.53
to TCP port: 143
Feb 29 08:20:19 dns2 rpcbind: refused connect
from 192.117.186.53 to dump()
Feb 29 08:21:16 dns1 telnetd[50449]:
refused connect from R-H-186-53.access.net.il
Feb 29 08:21:19 dns2 /usr/local/bin/snort[8374]:
RPC - portmap-request-mountd: 192.117.186.53:918 -> x.x.x.x:111
Feb 29 08:21:19 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:22 dns1 ftpd[50237]: refused
connect from R-H-186-53.access.net.il
Feb 29 08:21:24 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:29 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:34 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:34 dns1 portsentry[172871]: attackalert: Connect
from host: R-H-186-53.access.net.il/192.117.186.53 to TCP port: 143Feb 29
08:21:39 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:44 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:49 dns2 /usr/local/bin/snort[8374]:
RPC - portmap-request-mountd: 192.117.186.53:918 -> x.x.x.x:111
Feb 29 08:21:49 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:59 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:22:14 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
```

In this trace originating from Israel we see an attempt to connect to the dns2 host via telnet, then viaftp, and finally an imap probe. After this we see several numerous failed attempts to connect to the SunRPC port with several packets directed at the dns2 machine sprinkled among them. If these packets are looked at separately, they have the same pattern as the first three packets, (telnet, ftp, imap).

The two sets of three are obvious attempts at trying to compromise a dns server. Probably looking for an unpatched vulnerability to exploit. The series of RPC probes are less clear. What is probably occurring is that the firewall is simply dropping the requests and the attacker is simply retrying to see if he can get a response.

```
Severity = (Criticality + Lethality) – (System CM + Network CM)
         = ( 5 + 3 ) – ( 3 + 3 ) =  2
```

Trace #6 – 1 March Archives

```
Feb 29 12:29:49 host1 portsentry[524]: attackalert:
Connect from host: 206.49.154.100/206.49.154.100 to UDP port: 31337
Feb 29 12:29:49 host1 portsentry[524]: attackalert:
Connect from host: 206.49.154.100/206.49.154.100 to UDP port: 31337
Feb 29 12:29:49 host2 portsentry[420]: attackalert:
Connect from host: 206.49.154.100/206.49.154.100 to UDP port: 31337
Feb 29 12:32:40 host3 portsentry[16512]: attackalert:
Connect from host: 206.49.154.100/206.49.154.100 to UDP port: 31337
```

This is about as straightforward as it gets. A series of packets probing for the BackOrifice trojan. The attacker is simply stepping through the machines on the network. Due to the blatant noise this activity will generate this attacker is either a fairly unsophisticated novice or a more accomplished hacker who is using a "throwaway" box to accomplish his goal more quickly, aware that his actions are probably going to be detected and blocked.

```
Severity = (Criticality + Lethality) – (System CM + Network CM)
         = ( 2 + 5 ) – ( 3 + 3 ) =  1
```

Trace #7 – 22 Feb Archives

Once again Snort reports truncated for brevity.

```
-*> Snort! <*-
Version 1.5
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
snaplen = 68
Entering readback mode....

02/21-00:01:59.837203 192.0.218.166:4618 -> 152.163.244.9:5190
TCP TTL:126 TOS:0x0 ID:18646 DF
SFRP*U21 Seq: 0x179E86B2 Ack: 0x4460D Win: 0x5011
TCP Options => Opt 32 (32): 2020 2000 3C84 3647 9D6B

D  02/21-00:18:35.175490 192.0.205.118:21 -> 216.229.234.199:3547
   TCP TTL:126 TOS:0x0 ID:35117
   SFRPAU1 Seq: 0x10000 Ack: 0x147 Win: 0x5014

B  02/21-00:42:12.071193 24.24.195.129:0 -> 192.0.213.22:2809
   TCP TTL:106 TOS:0x0 ID:17275
   SF****2 Seq: 0x1A2010DD Ack: 0xE0F90080 Win: 0x5010
   TCP Options => EOL EOL CC 3035487176

B  02/21-00:42:48.444625 24.24.195.129:2809 -> 192.0.213.22:6688
   TCP TTL:106 TOS:0x0 ID:59782
   SF****2 Seq: 0x10E1 Ack: 0xBB110080 Win: 0x5010
   TCP Options => EOL EOL Opt 87 (40): AC9E B567 4D54

B  02/21-00:43:48.845467 24.24.195.129:2809 -> 192.0.213.22:6688
   TCP TTL:106 TOS:0x0 ID:16026
   SF****2 Seq: 0x10E718F9 Ack: 0x80 Win: 0x5010
   TCP Options => EOL EOL Opt 188 (40): BA74 1C80 D986

A  02/21-00:48:26.937096 192.0.205.114:1185 -> 207.172.3.46:119
   TCP TTL:126 TOS:0x0 ID:56339 DF
   SFRP**21 Seq: 0x46 Ack: 0xABD78022 Win: 0x5010
   TCP Options => Opt 32 (32): 2020 2000 D02A 1E61 0494

A  02/21-00:52:55.936207 192.0.205.114:1185 -> 207.172.3.46:119
   TCP TTL:126 TOS:0x0 ID:18735 DF
   SF*PA*1 Seq: 0xE60046 Ack: 0xB32C80D0 Win: 0x5010

02/21-00:54:32.449459 192.0.207.230:0 -> 140.103.41.60:6688
TCP TTL:126 TOS:0x0 ID:51393 DF
SF*PA*2 Seq: 0xA6B02B6 Ack: 0x7E274B2E Win: 0x5018
TCP Options => EOL EOL Opt 87 (40): EE78 AEA3 E9BF

A  02/21-01:03:55.421558 192.0.205.114:1275 -> 207.172.3.46:119
   TCP TTL:126 TOS:0x0 ID:26952 DF
   SF*P**1 Seq: 0x52E78E Ack: 0x321012 Win: 0x5010

D  02/21-01:14:50.180395 192.0.205.118:195 -> 216.229.234.199:21
   TCP TTL:126 TOS:0x0 ID:15045
   SF****21 Seq: 0x83C0000 Ack: 0x17A Win: 0x5014
   TCP Options => Opt 32 (32): 2020 2000 0402 13BA 040A

A* 02/21-01:26:15.520937 192.0.205.114:1794 -> 206.132.8.211:20
   TCP TTL:126 TOS:0x0 ID:20880 DF
   SF**AU Seq: 0x6A Ack: 0xF7BFDDEC Win: 0x5010
   TCP Options => Opt 32 (32): 2020 2000 FAC8 E7E9 82B8

A  02/21-01:27:29.791569 192.0.205.114:1275 -> 207.172.3.46:119
   TCP TTL:126 TOS:0x0 ID:39845 DF
   SF**A*21 Seq: 0x52 Ack: 0xFA6A1193 Win: 0x5010

02/21-01:27:38.969005 192.0.219.146:1526 -> 129.210.184.178:20
TCP TTL:126 TOS:0x0 ID:49375 DF
SFRP*U21 Seq: 0x189DA5B Ack: 0x168 Win: 0x5010

C  02/21-01:35:46.383817 192.0.207.114:213 -> 141.219.85.55:6688
   TCP TTL:126 TOS:0x0 ID:48581 DF
   SFR*A*2 Seq: 0x46A02E2 Ack: 0xD28C023A Win: 0x5018
```

```
C  02/21-01:36:07.885789 192.0.207.114:6688 -> 141.219.85.55:1130
   TCP TTL:126 TOS:0x0 ID:19154 DF
   SFR*A*2 Seq: 0x3D02F1 Ack: 0x928C023A Win: 0x5018

C  02/21-01:36:16.756601 192.0.207.114:6688 -> 141.219.85.55:1130
   TCP TTL:126 TOS:0x0 ID:63445 DF
   SFR*A*2 Seq: 0x2F6ECD8 Ack: 0xD5023A Win: 0x5010

C  02/21-01:37:15.223007 192.0.207.114:6688 -> 141.219.85.55:1130
   TCP TTL:126 TOS:0x0 ID:63217 DF
   SFR*A*2 Seq: 0x308 Ack: 0x4BA8023A Win: 0x5018
```

Lots of anomalous activity in this trace from several different sources. The best way to approach this trace is to group the activity by originating host and analyze each group separately. This is done using the labels to the left indicating associated packets.
A: Here we see a set of five packets over a 45-minute time span. Four of the five are targeting the NNTP daemon on port 119, the fifth (denoted by A*) is probing port 20, the ftp data channel. All five packets have unique, illegal TCP flag combinations. This is a low and slow attack targeting host 207.172.3.46. The different TCP flag settings indicate OS fingerprinting of the host. The slow rate of data accumulation indicates a fairly sophisticated host. These packets are very likely being sent manually (vice with a standard script) due to the slow rate and uneven time interval. The originating host ip address resolves to the Demon Internet, giving further support to an assessment of hostile intent.

B: Three SYN FIN packets within 1.5 seconds. This is definitely a scripted attack, probably aimed at network mapping or host fingerprinting. An interesting element is that the first of the three packets has a source port of 0With a destination port of 2809. The next two packets have a source port of 2809 and a destination port of 6688. This port has been associated with fingerprinting activity in other traces.

C: Four packets following a similar pattern to that found in trace segment B. All four packets come in about 1.5 seconds, with the destination port of the first packet the source port of the remainder. Once again the TCP flag options are an impossible combination and are the same for all the packets. Probable host fingerprinting.

D: Two packets from the same host (also from the Demon Internet) with illegal TCP flags, targeting the same system. The first has all TCP flags set, while the second is a SYN FIN packet. These two packets are approx one hour apart. Possibly a small segment of a very low and slow host scan, manually done and very quiet.

Other anomalous packets are directed at different hosts. Normally I would disregard, but in the context of the surrounding traffic they probably deserve a closer look.

For the entire trace:
Severity = (Criticality + Lethality) – (System CM + Network CM)
= (3 + 5) – (2 + 3) = 3

Trace #8 – 22 Feb Archives

```
Feb 21 16:43:12 host1 portsentry[522]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 109
Feb 21 16:43:15 host1 portsentry[522]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 109
```

```
Feb 21 16:43:21 host1 portsentry[522]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 1
Feb 21 16:43:21 host1 portsentry[522]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 109
Feb 21 16:43:21 host1 portsentry[522]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 1
Feb 21 16:43:25 host1 portsentry[522]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 109

Feb 21 16:43:12 host2 in.telnetd[26088]:
refused connect from 151.4.122.250
Feb 21 16:43:12 host2 in.telnetd[26089]:
refused connect from 151.4.122.250
Feb 21 16:43:21 host2 portsentry[418]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 1
Feb 21 16:43:21 host2 rpcbind:
refused connect from 151.4.122.250 to dump()

Feb 21 16:43:12 host3 in.telnetd[20307]:
refused connect from 151.4.122.250
Feb 21 16:43:12 host3 in.telnetd[20308]:
refused connect from 151.4.122.250
Feb 21 16:43:21 host3 portsentry[334]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 1

Feb 21 16:46:29 host4 telnetd[18032]:
refused connect from 151.4.122.250
Feb 21 16:46:30 host4 telnetd[23064]:
refused connect from 151.4.122.250
Feb 21 16:46:39 host4 portsentry[16254]: attackalert:
Connect from host: 151.4.122.250/151.4.122.250 to TCP port: 1
***************
Feb 21 16:49:04 host1 statd[297]: statd:
pathname too long: /var/statmon/sm/3333u1ubb^V
<tt0F^FFf1fF*fFFF1FFfFfLR1FFf?1??.bin@.sh!@F1FvFNV11EPrivet ADMcrew
```

This traffic has been grouped by target – host1, host2, host3 and then host4. Evaluated this way, host1 is scanned with POP2 probes (109) and tcpmux (1) probes (looking for an Irix box?), 6 packets in under a minute. host2 is probed with 4 packets for telnet, SunRPC/portmapper (111), and tcpmux(1), also in under a minute. host3 and host4 are probed with three packets each for telnet and tcpmux.

A closer look at the timestamps indicates that the traffic to host1, host2, and host3 all came in the same minute, indicating a script or tool of some sort. The traffic directed at host4 came three minutes later.

Three minutes after host4 was probed, host1 was atacked with a statd attack. Although there is no source ip address given, presumably this is a result of the probing.

Severity = (Criticality + Lethality) – (System CM + Network CM)
= (3 + 5) – (3 + 3) = 2

Trace #9 – 15 Feb Archives

```
Feb 12 10:16:04 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2088 -> x.x.x.11:32771
Feb 12 10:16:04 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2089 -> x.x.x.12:32771
Feb 12 10:16:04 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2096 -> x.x.x.19:32771
Feb 12 10:16:05 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2109 -> x.x.x.32:32771
Feb 12 10:16:05 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2111 -> x.x.x.34:32771
Feb 12 10:16:05 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2132 -> x.x.x.55:32771
Feb 12 10:16:05 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2133 -> x.x.x.56:32771
Feb 12 10:16:05 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2138 -> x.x.x.61:32771
Feb 12 10:16:05 host1 snort[436]: MISC-Attempted
Sun RPC high port access: 24.0.114.175:2150 -> x.x.x.73:32771
Feb 12 10:16:05 host1 snort[436]: MISC-Attempted
```

```
Sun RPC high port access: 24.0.114.175:2157 ->
: : :

[**] MISC-Attempted Sun RPC high port access [**]
02/12-16:05:07.286134 209.67.232.128:4191 -> y.y.y.19:32771
TCP TTL:52 TOS:0x0 ID:50821 DF
S***** Seq: 0x8FFE23A6 Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 67773715 0 NOP WS: 0

[**] MISC-Attempted Sun RPC high port access [**]
02/12-16:05:07.353471 209.67.232.128:4234 -> y.y.y.62:32771
TCP TTL:52 TOS:0x0 ID:50868 DF
S***** Seq: 0x8F66FA97 Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 67773730 0 NOP WS: 0

[**] MISC-Attempted Sun RPC high port access [**]
02/12-16:05:07.397761 209.67.232.128:4234 -> y.y.y.62:32771
TCP TTL:52 TOS:0x0 ID:50872 DF
****A* Seq: 0x8F66FA98 Ack: 0x44A354C8 Win: 0x7D78

[**] MISC-Attempted Sun RPC high port access [**]
02/12-16:05:07.469307 209.67.232.128:4234 -> y.y.y.62:32771
TCP TTL:52 TOS:0x0 ID:50873 DF
****A* Seq: 0x8F66FA98 Ack: 0x44A354C9 Win: 0x7D78

[**] MISC-Attempted Sun RPC high port access [**]
02/12-16:05:07.892157 209.67.232.128:4234 -> y.y.y.62:32771
TCP TTL:52 TOS:0x0 ID:50876 DF
*F**A* Seq: 0x8F66FA98 Ack: 0x44A354C9 Win: 0x7D78

[**] MISC-Attempted Sun RPC high port access [**]
02/12-16:05:08.020387 209.67.232.128:4243 -> y.y.y.71:32771
TCP TTL:52 TOS:0x0 ID:50885 DF
S***** Seq: 0x8F55C88F Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 67773799 0 NOP WS: 0

[**] MISC-Attempted Sun RPC high port access [**]
02/12-16:05:08.051318 209.67.232.128:4252 -> y.y.y.80:32771
TCP TTL:52 TOS:0x0 ID:50894 DF
S***** Seq: 0x8FACDE5E Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 67773799 0 NOP WS: 0
```

Once again, two different types of activity present in this trace. The first burst of traffic from host 24.0.114.175 is a very straightforward network scan targeting the SunRPC/portmapper port. The script or tool used simply went down a list of network ip addresses hitting at least ten different hosts is less than two seconds. One thing of note is that the ip addresses are not sequential, suggesting that this attacker already has a good feel for the hosts on the network and that this effort is more focused on host mapping.

The second burst of activity also happens very quickly, sending a SYN packet to each host in the network on the RPC port. once again, the attacker appears to already know which hosts are present since he is not sending to a broadcast address and not going through the address space sequentially. An interesting difference (and scary!) is that host y.y.y.62 apparently completed the three way handshake with the attacker. Several more ACK packets are sent, presumably in response to a data push. The attacker then gracefully closed the connection prior to moving on to the next host. I would recommend that host .62 be thoroughly inspected.

Severity = (Criticality + Lethality) – (System CM + Network CM)
= (3 + 3) – (3 + 2) = 1

Trace #4 – Trace provided from Stephen Northcutt

** Andy Johnston (andy@umbc.edu)   *   page: 410-678-8949
** Distributed Systems Manager   * PGP key: (afjumbc98) 1024/F67035E1
** University Computing Services,UMBC *   90 20 AA 8E 24 AD 21 C1
** 410-455-2583 (v)/410-455-1065 (f) *   E0 09 5A A8 1F 0C E4 67

Header information removed for brevity.
****
Snort Alert Report at Mon Mar 27 00:08:49 2000
****
[**] Watchlist 000222 NET-NCFC [**]
03/26-00:12:23.344779 159.226.5.222:3208 -> MY.NET.100.230:113

Series A:
[**] Watchlist 000222 NET-NCFC [**]
03/26-00:12:23.977876 159.226.5.222:25 -> MY.NET.100.230:61561
Repeated 8 times.
[**] Watchlist 000222 NET-NCFC [**]
03/26-00:15:41.753644 159.226.5.222:25 -> MY.NET.100.230:61561

[**] SYN-FIN scan! [**]
03/26-00:28:55.240777 194.70.126.10:17664 -> MY.NET.253.43:152
[**] Null scan! [**]
03/26-00:48:11.538244 194.217.188.38:123 -> MY.NET.97.111:123

Series B:
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/26-01:06:38.299087 212.179.43.195:25 -> MY.NET.100.230:62118
Repeated 3 times.
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/26-01:15:25.129774 212.179.43.195:25 -> MY.NET.100.230:62118

Series C:
[**] Watchlist 000222 NET-NCFC [**]
03/26-01:32:32.617276 159.226.91.37:25 -> MY.NET.100.230:62447
Repeated 3 times.
[**] Watchlist 000222 NET-NCFC [**]
03/26-01:32:51.218010 159.226.91.37:25 -> MY.NET.100.230:62447

Series D:
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/26-04:28:39.773794 212.179.48.87:1159 -> MY.NET.217.254:4687

136 more of these type packets were received between the start and the end of series D. The following packets were mixed in with the 212.179.48.87:1159 traffic.

[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:15.498820 159.226.64.137:18093 -> MY.NET.6.7:25
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:19.064599 159.226.64.137:113 -> MY.NET.6.7:21707
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:20.996468 159.226.64.137:113 -> MY.NET.6.7:21707
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:26.036289 159.226.64.137:113 -> MY.NET.6.7:21707

```
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:26.037599 159.226.64.137:113 -> MY.NET.6.7:21707
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:26.037658 159.226.64.137:18093 -> MY.NET.6.7:25
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:29.881859 159.226.64.137:18093 -> MY.NET.6.7:25
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:31.421785 159.226.64.137:18093 -> MY.NET.6.7:25
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:32.888144 159.226.64.137:18093 -> MY.NET.6.7:25
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:32.889522 159.226.64.137:18093 -> MY.NET.6.7:25
[**] Watchlist 000222 NET-NCFC [**]
03/26-04:33:33.667798 159.226.64.137:18093 -> MY.NET.6.7:25

[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/26-04:38:09.323482 212.179.48.87:1159 -> MY.NET.217.254:4687
```

Series E:

```
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/26-05:05:45.641737 212.179.48.87:1416 -> MY.NET.217.254:4687
Repeated 230 times.
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/26-05:13:57.467086 212.179.48.87:1416 -> MY.NET.217.254:4687
```

Series F:

```
[**] Watchlist 000222 NET-NCFC [**]
03/26-07:48:14.662485 159.226.66.130:1176 -> MY.NET.253.43:25
This activity is seen 130 more times from the same host with source ports of
1176,  1178, 1179, 1182, and 1183.

[**] Watchlist 000222 NET-NCFC [**]
03/26-07:48:46.993363 159.226.66.130:1177 -> MY.NET.6.7:25
Repeated 29 times.

[**] Null scan! [**]
03/26-12:46:36.454463 195.11.50.206:9999 -> MY.NET.60.14:1085
[**] NMAP TCP ping! [**]
03/26-14:29:07.365958 194.241.59.201:65 -> MY.NET.130.81:53
[**] NMAP TCP ping! [**]
03/26-14:29:13.703893 194.241.59.201:65 -> MY.NET.130.81:53
[**] Null scan! [**]
03/26-14:42:55.636552 194.70.126.10:27970 -> MY.NET.253.42:27960
[**] NMAP TCP ping! [**]
03/26-15:00:54.119235 194.241.59.201:65 -> MY.NET.210.77:21
```

Series G:

```
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:47.860982 132.241.80.10:25 -> MY.NET.253.24:35555
Repeated 8 times.
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:53.701981 132.241.80.10:25 -> MY.NET.253.24:35555


[**] Null scan! [**]
03/26-16:08:13.160564 194.217.242.14:27015 -> MY.NET.253.24:1534
[**] Null scan! [**]
```

```
03/26-17:08:24.607078 194.70.126.33:1223 -> MY.NET.100.85:2339
[**] Null scan! [**]
03/26-20:25:14.181445 24.200.40.224:6699 -> MY.NET.209.6:1311
[**] Null scan! [**]
03/26-20:45:38.672469 200.53.240.148:1134 -> MY.NET.201.94:6346
[**] Watchlist 000222 NET-NCFC [**]
03/26-20:47:46.705724 159.226.228.1:113 -> MY.NET.253.42:34841
```

Series H:

```
[**] Watchlist 000222 NET-NCFC [**]
03/26-20:47:47.452461 159.226.228.1:3955 -> MY.NET.253.42:25
Repeated 14 times.
[**] Watchlist 000222 NET-NCFC [**]
03/26-20:51:02.098274 159.226.228.1:3955 -> MY.NET.253.42:25

[**] Null scan! [**]
03/26-21:55:18.336122 194.70.126.10:7799 -> MY.NET.253.43:1544
```

Series I:

```
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-23:44:02.938303 138.234.4.100:25 -> MY.NET.253.52:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-23:44:06.324181 138.234.4.100:25 -> MY.NET.253.52:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-23:44:06.451600 138.234.4.100:25 -> MY.NET.253.52:35555
```

This trace consists of several different series, labeled A through I that have distinctive characteristics. Series A, B, and C are all similar in that 5 – 10 packets are directed at the same target machine from 3 different hosts. In each case, traffic from source port 25 is being sent to a high-level port in the 60,000+ range and the total transmission time is just a few minutes. There is a time gap of ~50 minutes between series A & B and a 17 min gap between series B & C.

Approximately 3 hours later, seried D starts up and two different traffic patterns are notices. In the first pattern, host 212.179.48.87:1159 is communicating with my.net.217.254:4687. The second pattern is host 159.226.64.137 sending packets to my.net.6.7 on ports 25 & 21707.
An interesting point is that the source in the first pattern is the same source as in series A.

After ~140 packets the series stops. A half hour later, the first pattern resumes with a different source port (1416) and is labeled series E. in this series, 232 packets are sent in 8 minutes.

2-½ hours later series F begins. Here we see host 159.226.6.130 sending packets to hosts my.net.253.43:25 and my.net.6.7:25 (again a target).

Series G is essentially the same as series B, but with a different source ip and different target ip, with a target port of 35555.

In series H, another host on the 159.226 network is sending packets to a host on my.net., host 253.42:25 in this instance.

Finally, We see some more activity targeted at port 35555 in series I. The source and destination ip addresses are different.

Seeing as how I have limited experience with this level of traffic, I'm not positive, but my initial reaction to this activity is that it is fairly serious. Apparently, several different networks have been compromised, as the same net id's keep showing up. The destination port 25 traffic could be an attempt to get past the firewall. The large amounts of packets that are transmitted appear to indicate that some for of data transfer is taking place. I would have probably dismissed this as a legitimate form of communication, except that the first three series targeted high-level ports. This is often characteristic of the DDOS tools, and after this spring's activity, I'm probably more paranoid than I would have been before.

Severity = (Criticality + Lethality) – (System CM + Network CM)
= (3 + 5) – (3 + 3) = 2

Hope this is the sort of stuff you were looking for.
Thank You.
Gil Trenum

Last Updated: July 22nd, 2017

Upcoming Training

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 London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 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 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 San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 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 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 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
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced