Global Information Assurance Certification Paper

*** Northcutt, fine job, clear analysis, might want to revisit 7, the research on the source addresses was good, lil attack research would have been nice and I appreciate the effort to calculate whether a source address was spoofed. The student here did as good as they could do with borrowed traces, but this really shows how important the homefield advantage is to solid analysis, 10 *was* a fun read and we could all conjecture till we turn blue, but more data would be so helpful! 76 *

SANS
GIAC Level II Intrusion Detection
Practical Exam
April 2000

Michael J. Handel

Note: All traces have been taken from the GIAC website archive; I avoided reading analyses submitted with them as much as possible to avoid biasing my conclusions. For various reasons, I am unable to provide traces from our corporate network at this time. Additionally, I have been on a business trip out of the country since leaving SANS 2000, and have not had the resources available to test various hacking tools (nmap, SubSeven, etc.) to identify how they behave in a test environment. Personally, I found detect #10 the most interesting, and hope I came close.

Detect #1

```
Mar 28 00:16:09.225 firewall kernel: 226 IP packet dropped
      (24.66.81.36->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN] Port 2357->27374):
       Restricted Port: Protocol=TCP[SYN] Port 2357->27374 (received on interface
       10.0.0.1)

Mar 28 00:16:09.226 firewall kernel: 226 IP packet dropped
      (24.66.81.36->firewall.mydomain.edu[10.0.0.1]: Protocol=TCP[SYN] Port 2357->27374):
       Restricted Port: Protocol=TCP[SYN] Port 2357->27374 (received on interface
       10.0.0.1)
      [1 duplicates suppressed]
```

Analysis #1

- Description: Trojan search
- Active targeting: Yes
- Techniques:
  - An internet whois search identified the address block 24.64.0.0 - 24.70.95.255 as belonging to Shaw FiberLink, a Canadian cable company offering residential cable modem service.
  - The two traces are extremely close together, and the port numbers are identical; this leads me to believe that this is an automated attack using crafted packets.
  - The source port of 27374 is known to be associated with the default setup for the SubSeven 2.1 trojan.
- Intent:
  - It appears that this attacker was probing for hosts on a network behind a firewall (though it's not evident from the trace if it was trying the same or different hosts; I must assume it was looking for different ones), but unable to get a positive response.
- Evaluation:
  - It is certainly possible that the origin address is not being spoofed, but the increasing number of home cable modem users is also increasing the number of potentially compromised hosts; it is also very possible that a legitimate host on this network has been compromised.
  - This attack was likely attempted by a relatively new and/or unskilled individual.
  - While this attack was unsuccessful, the attacker may have been able to gain some small amount of information about the target network from the firewall's response. The firewall log shows that the packet was dropped; if this is the first time this attacker has probed for this network, it has confirmed that the address space is populated. It's unlikely that two packets (if these were the only two sent) would just disappear without any response.

Detect #2

```
      [**] Watchlist 000222 NET-NCFC [**]
03/27-00:30:28.886151 159.226.40.228:1779 -> MY.NET.70.33:8765
       [**] Watchlist 000222 NET-NCFC [**]
03/27-02:49:45.844964 159.226.39.1:4064 -> MY.NET.253.42:25
      [**] Watchlist 000222 NET-NCFC [**]
03/27-02:49:47.460907 159.226.39.1:4064 -> MY.NET.253.42:25
      [**] Watchlist 000222 NET-NCFC [**]
03/27-02:49:47.470231 159.226.39.1:4064 -> MY.NET.253.42:25
      [**] Watchlist 000222 NET-NCFC [**]
03/27-02:49:55.264670 159.226.39.1:25 -> MY.NET.253.42:39256
      [**] Watchlist 000222 NET-NCFC [**]
03/27-02:49:55.425202 159.226.39.1:4064 -> MY.NET.253.42:25
      [**] Watchlist 000222 NET-NCFC [**]
03/27-02:49:56.051044 159.226.39.1:25 -> MY.NET.253.42:39256
      [**] Watchlist 000222 NET-NCFC [**]
03/27-02:49:56.240307 159.226.39.1:4064 -> MY.NET.253.42:25
       [**] Watchlist 000222 NET-NCFC [**]
03/27-03:52:53.952098 159.226.228.1:1516 -> MY.NET.1.7:25
      [**] Watchlist 000222 NET-NCFC [**]
03/27-03:53:08.855406 159.226.228.1:1516 -> MY.NET.1.7:25
      [**] Watchlist 000222 NET-NCFC [**]
03/27-03:53:10.628575 159.226.228.1:1516 -> MY.NET.1.7:25
```

Analysis #2

- Description: SMTP/possible trojan
- Active targeting: Yes
- Techniques:
  - An internet whois search identified the class B address 159.226.0.0 as belonging to The Computer Network Center-Chinese Academy of Sciences in Beijing, China.
  - Many of the traces are extremely close together, and many of the port numbers are identical. this leads me to believe that this is an automated attack using crafted packets, specifically targeting port 25.
- Intent:
  - The attacker is trying to probe port 25 for available services. The IDS log (which seems to have fired on rule #222) doesn't indicate what action was taken as a result of this detect, so it is unknown whether the probe was successful.
  - Activity to a high port (39256) may indicate potential trojan activity.
- Evaluation:
  - It appears that a filter has been written to specifically target this source address. Perhaps the target network has been receiving an unusual amount of suspicious traffic from the source network.
  - It is likely the address in the IDS log is not spoofed, whether or not it was the actual IP address of the originator. By this, I mean that the attack either came from this address or through it. Due to political considerations, it is nearly impossible to track down or prosecute attackers coming from or through addresses in China and other restricted countries. In some cases, it has been demonstrated that Chinese hackers have been either funded, sponsored, directed, or encouraged in their endeavors by the Chinese government.
  - It appears that the attacker either has prior information about the network topology, or is adding to his existing knowledge by mapping out additional subnets. In the traces listed above, the attacker is probing hosts on 3 separate subnets.
  - While I could find no information associating port 39256 with known trojan activity, I can't help but think that the two probes to that port are unusual when compared with all the other activity to port 25.

Detect #3

```
        [**] Watchlist 000222 NET-NCFC [**]
03/28-01:16:03.594556 159.226.5.222:25 -> MY.NET.100.230:34924
        [**] Watchlist 000222 NET-NCFC [**]
03/28-01:16:11.534850 159.226.5.222:25 -> MY.NET.100.230:34924
        [**] Watchlist 000222 NET-NCFC [**]
03/28-01:16:22.998740 159.226.5.222:25 -> MY.NET.100.230:34924
        [**] Watchlist 000222 NET-NCFC [**]
03/28-01:16:24.591809 159.226.5.222:25 -> MY.NET.100.230:34924
        [**] Watchlist 000222 NET-NCFC [**]
03/28-01:39:50.991660 159.226.5.222:25 -> MY.NET.100.230:35203
        [**] Watchlist 000222 NET-NCFC [**]
03/28-01:39:51.801071 159.226.5.222:25 -> MY.NET.100.230:35203
        [**] Watchlist 000222 NET-NCFC [**]
03/28-01:39:56.702110 159.226.5.222:25 -> MY.NET.100.230:35203
        [**] Watchlist 000222 NET-NCFC [**]
03/28-01:39:58.899038 159.226.5.222:25 -> MY.NET.100.230:35203
        [**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/28-02:11:42.483847 212.179.43.195:25 -> MY.NET.100.230:35652
        [**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/28-02:11:53.560625 212.179.43.195:25 -> MY.NET.100.230:35652
        [**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/28-02:12:30.236599 212.179.43.195:25 -> MY.NET.100.230:35652
        [**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/28-02:12:30.714581 212.179.43.195:25 -> MY.NET.100.230:35652
        [**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/28-02:12:30.714628 212.179.43.195:25 -> MY.NET.100.230:35652
        [**] Watchlist 000222 NET-NCFC [**]
03/28-02:30:11.115551 159.226.91.37:25 -> MY.NET.100.230:35917
        [**] Watchlist 000222 NET-NCFC [**]
03/28-02:30:12.560459 159.226.91.37:25 -> MY.NET.100.230:35917
        [**] Watchlist 000222 NET-NCFC [**]
03/28-02:30:13.437471 159.226.91.37:25 -> MY.NET.100.230:35917
```

Analysis #3

- Description: Host-specific trojan probe
- Active targeting: Yes
- Techniques:
  - We see a series of 4 separate probes, each separated by a period of between 18-32 minutes.
  - Because of the varying times of probes, it's difficult to tell whether this is an automated attack. My best guess would be that it's a combination of both.
- Intent:
  - Activity to high ports (34924, 35203, 35652, 35917) may indicate potential trojan activity.
- Evaluation:
  - Here we see the Computer Network Center-Chinese Academy of Sciences in Beijing, China back at it one more time.
  - Additionally, there are a series of packets from a Class C address space that is assigned to SHEERNETWORKS in Israel. It looks like SHEERNETWORKS has purchased a chunk of addresses from their ISP, ISDN Net (also located in Israel).Again, the pre-defined filter fired when the Chinese probed, and it appears there is another filter written specifically to identify traffic coming from the ISDN Net address space. This would indicate a history of attacks from this source. Additionally, the title of the ISDN Net filter would suggest that such traffic has been identified as potentially problematic since 5/99. It appears that detect #2 was just one in a series of attempts from the Chinese network searching for hidden trojan vulnerabilities.
  - Both source addresses are targeting the same host, which would indicate either a coordinated attack, or the same attacker coming through multiple hosts. Because the longest time gap comes between probes from two different attackers, it would lead me to believe that the Israel host has been compromised, and is being used by the attacker(s) from China as a means of hiding their real identity.

- At this point, it would be wise to completely block the Chinese source address at all points where this network meets the Internet, as it's obvious the source network doesn't have our best interests in mind. A notification to the point of contact for ISDN Net or SHEERNETWORKS would probably be in order to see if they can fix their own problems. If it persists, we should probably block their traffic as well.
- While I could find no information associating ports 34924, 35203, 35652, or 35917 with known trojan activity, the number of probes to unassigned high ports indicated a search for trojans or backdoors.

Detect #4

```
Jan  5 12:36:59 milo named[2095]: security: notice: refused query on non-query socket
                from [209.67.38.48].53
Jan  5 12:37:03 milo named[2095]: security: notice: refused query on non-query socket
                from [199.95.207.65].53
Jan  5 12:37:07 milo named[2095]: security: notice: refused query on non-query socket
                from [204.253.104.74].53
Jan  5 12:37:09 milo named[2095]: security: notice: refused query on non-query socket
                from [209.67.38.48].53
Jan  5 12:37:11 milo named[2095]: security: notice: refused query on non-query socket
                from [199.95.208.86].53
```

Analysis #4

- Description: DNS DoS?
- Active targeting: Yes
- Techniques:
  - The address block 209.67.0.0 - 209.67.255.255 is registered to Exodus Communications, a California-based web hosting corporation. (As an aside, a look at their website plainly states that it is powered by Sun Microsystems computers. I'm not sure, but I can't help but think it's not a good idea to advertise what systems are inside your network. Why invite OS-specific attacks?)
  - The address block 199.92.0.0 - 199.95.255.255 is owned by NearNet, and has either sold or leased the range 199.95.206.0 - 199.95.209.255 to Double Click, Inc., an Internet advertising company that has gained some recent notoriety over its resale of consumer information to third parties.
  - The address block 204.252.0.0 - 204.255.255.0 belongs to UUNet Technologies, Inc. which has also provided a range of addresses (204.253.104.0 - 204.253.105.255) to Double Click.
  - Four separate hosts are simultaneously attempting to connect to the same DNS server on the same destination port, but from an incorrect source port for a DNS query.
- Intent:
  - The source hosts are different, but because the timestamps are so closely interwoven, and the target is so narrowly focused, I believe that this may be either a coordinated effort between multiple attackers or the sign of compromised hosts being used by one attacker to flood this DNS server with requests, preventing it from responding to legitimate requests.
- Evaluation:
  - There's a lot of information missing in this detect (like whether they were TCP or UDP requests), and it would be nice if there was a tcpdump output to look at some more details. I have to assume that the above traces represent all the activity seen of this type.
  - At first, I thought this might be a symptom of load-balancing software, but load-balancing requests emulate a normal DNS query (see below).
  - Normally, a client DNS query will come from a high source port to the DNS server destination port 53. In this case, we see the exact opposite (assuming that "`named[2095]`" indicates the destination port). Perhaps the attacker(s) are trying to fool any routers or firewalls that may be in the way into thinking that these are requests between DNS servers (which may be permitted). I don't believe that either Exodus or Double Click are ISP's, so I would tend think that the source addresses are spoofed. The host-based IDS must have had a rule based on this fact, and fired when it saw the improper port pair combination.

Detect #5

```
Mar 27 02:08:20 ardvark kernel: Packet log: input DENY eth0 PROTO=6 208.10.116.59:53
xxx.xxx.xxx.11:53 L=40 S=0x00 I=39426 F=0x0000 T=31 SYN

[**] Source Port traffic [**]
03/27-02:08:20.143468 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x3C
                      208.10.116.59:53 -> xxx.xxx.xxx.8:53 TCP TTL:30 TOS:0x0 ID:39426
                      SF**** Seq: 0x769E8EF6 Ack: 0x6AA18DD4 Win: 0x40400 00 00 00 00 00
                      ......
[**] Source Port traffic [**]
03/27-02:08:20.204738 0:E0:D0:15:11:94 -> 0:0:C0:29:8F:D2 type:0x800 len:0x3C
                      208.10.116.59:53 -> xxx.xxx.xxx.11:53 TCP TTL:31 TOS:0x0 ID:39426
                      SF**** Seq: 0x769E8EF6 Ack: 0x6AA18DD4 Win: 0x40400 00 00 00 00 00
                      ......
[**] Source Port traffic [**]
03/27-02:08:20.284368 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x3C
                      208.10.116.59:53 -> xxx.xxx.xxx.15:53 TCP TTL:31 TOS:0x0 ID:39426
                      SF**** Seq: 0x769E8EF6 Ack: 0x6AA18DD4 Win: 0x40400 00 00 00 00 00
                      ......
```

Analysis #5

- Description: DNS mapping/OS fingerprinting
- Active targeting: Yes
- Techniques:
  - An internet whois search identified the address block 208.0.0.0 - 208.35.255.255 as belonging to Sprint. It appears that Sprint has sold/leased the Class C space of 208.10.116.0 - 208.10.116.255 to InterConnect, Inc., an Indianapolis-based ISP (inct.net).
  - On first glance, it would appear that the attacker is attempting a DNS zone transfer, since the traffic source and destination ports are both TCP port 53. This is not the case, however, due to the presence of the SYN-FIN flag combination. The attacker does not appear to want to establish a connection at this point.
  - Because of the impossible TCP flag combinations, duplicate ID numbers, and the close packet interval, the attacker is using an automated method of sending crafted packets (possibly QueSO or nmap).
  - Because different OS's respond differently to malformed packets, the attacker may be in the initial phase(s) of finding DNS servers and identifying their OS's.
- Intent:
  - Because the attacker is only probing port 53, this is clearly a search for a DNS server, with the possible additional hope of finding out what OS it's running.
- Evaluation:
  - The attacker is looking for open ports on DNS servers.
  - ipchains detected (and prevented) the attack based on a rule regarding the source port of the packets.
  - Further whois queries indicate that InterConnect, Inc. does have at least 2 registered nameservers (ns1.inct.net & ns2.inct.net), but the attack isn't coming from either of them. This would reinforce the argument that the probe is malicious.
  - This attack may be the work of an intermediate or advanced hacker, as the search to identify a specific OS would imply that the attacker has a broad knowledge of the vulnerabilities of multiple OS's.
  - In this case, our network was spared an intrusion, but ISP notification would probably be a good idea.

Detect #6

```
Mar 27 14:59:06 pooky kernel: Packet log: input DENY eth0 PROTO=6 38.31.117.17:2443
              xxx.xxx.xxx.204:12345 L=48 S=0x00 I=2221 F=0x4000 T=116
Mar 27 14:59:06 morton kernel: Packet log: input DENY eth0 PROTO=6 38.31.117.17:2440
              xxx.xxx.xxx.201:12345 L=48 S=0x00 I=1453 F=0x4000 T=116 SYN
Mar 27 14:59:06 www kernel: Packet log: input DENY eth0 PROTO=6 38.31.117.17:2444
              xxx.xxx.xxx.205:12345 L=48 S=0x00 I=2477 F=0x4000 T=116 SYN
```

Analysis #6

- Description: Trojan probe
- Active targeting: Yes
- Techniques:
  - The Class A address space of 38.0.0.0 – 38.255.255.255 belongs to Performance Systems International (PSI Net), a global ISP headquartered in Herndon, Virginia.
  - The attacker is executing a host scan for open ports associated with known trojans. Based on the close interval of the packets, the attack is definitely automated.
- Intent:
  - The unknown attacker is hoping to find an open port on the scanned hosts to issue malicious commands or requests.
- Evaluation:
  - ipchains rules on 3 different hosts each detected and prevented the attack.
  - Port 12345 is associated with the NetBus and GabanBus trojan programs.

Detect #7

```
Mar 29 18:39:31 morton kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3224
               xxx.xxx.xxx.201:23 L=44 S=0x00 I=32765 F=0x4000 T=43 SYN
Mar 29 18:39:31 pooky kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3230
               xxx.xxx.xxx.204:23 L=44 S=0x00 I=32778 F=0x4000 T=43
Mar 29 18:39:31 www kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3231
               xxx.xxx.xxx.205:23 L=44 S=0x00 I=32782 F=0x4000 T=43 SYN
Mar 29 18:39:33 morton kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3224
               xxx.xxx.xxx.201:23 L=44 S=0x00 I=33116 F=0x4000 T=43 SYN
Mar 29 18:39:34 pooky kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3230
               xxx.xxx.xxx.204:23 L=44 S=0x00 I=33123 F=0x4000 T=43
Mar 29 18:39:34 www kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3231
               xxx.xxx.xxx.205:23 L=44 S=0x00 I=33124 F=0x4000 T=43 SYN
Mar 29 18:39:40 morton kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3224
               xxx.xxx.xxx.201:23 L=44 S=0x00 I=33833 F=0x4000 T=43 SYN
Mar 29 18:39:40 pooky kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3230
               xxx.xxx.xxx.204:23 L=44 S=0x00 I=33841 F=0x4000 T=43
Mar 29 18:39:40 www kernel: Packet log: input DENY eth0 PROTO=6 212.32.167.56:3231
               xxx.xxx.xxx.205:23 L=44 S=0x00 I=33842 F=0x4000 T=43 SYN
```

Analysis #7

- Description: SYN flood/DoS
- Active targeting: Yes
- Techniques:
  - The Class C address space 212.32.164.0 - 212.32.168.255 is registered to NORRNOD-BOSTADEN-NET, a real estate company in Sweden. Because this is a commercial entity, and not an ISP, it is likely that the source address is being spoofed.
  - The attacker is repetetively sending SYN packets sequentially to 3 different hosts at 3-6 second intervals.
- Intent:
  - It appears that the attacker is attempting to SYN flood the victim's telnet port, effectively creating a denial of service by preventing legitimate hosts from connecting.
- Evaluation:
  - I'm not sure what caused ipchains to fire on each of the hosts. It's not a stateful firewall, so it couldn't be that it sensed a certain threshold of packets coming. Perhaps the person who wrote the rules has experienced similar problems coming from these source addresses.
  - While 3 SYN packets to a single host might not seem like enough to cause any real damage or inconvenience, it appears that the attacker is trying to tie up multiple hosts all at the same time, thereby multiplying the impact of the attack.
  - The attacker is spoofing a known live address in an attempt to cover his actual identity.

Detect #8

```
Mar 29 21:48:34 209-30-73-81.flash.net ASCEND: wan2 tcp209.30.73.81;12345 <-
              211.45.208.151;3647 62 syn !pass (totcp-1)
Mar 29 21:48:39 209-30-73-81.flash.net ASCEND: wan3 tcp209.30.73.82;12345 <-
              211.45.208.151;3648 62 syn !pass (totcp-1)
Mar 29 21:48:44 209-30-73-81.flash.net ASCEND: wan3 tcp 209.30.73.83;12345 <-
              211.45.208.151;3649 62 syn !pass (totcp-1)
Mar 29 21:48:49 209-30-73-81.flash.net ASCEND: wan3 tcp209.30.73.84;12345 <-
              211.45.208.151;3650 62 syn !pass (totcp-1)
Mar 29 21:48:54 209-30-73-81.flash.net ASCEND: wan2 tcp209.30.73.85;12345 <-
              211.45.208.151;3651 62 syn !pass (totcp-1)
Mar 29 21:48:59 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.86;12345 <-
              211.45.208.151;3652 62 syn !pass (totcp-1)
Mar 29 21:49:04 209-30-73-81.flash.net ASCEND: wan2 tcp209.30.73.87;12345 <-
              211.45.208.151;3653 62 syn !pass (totcp-1)
Mar 29 21:49:09 209-30-73-81.flash.net ASCEND: wan2 tcp209.30.73.88;12345 <-
              211.45.208.151;3654 62 syn !pass (totcp-1)
Mar 29 21:49:14 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.89;12345 <-
              211.45.208.151;3655 62 syn !pass (totcp-1)
Mar 29 21:49:19 209-30-73-81.flash.net ASCEND: wan2 tcp209.30.73.90;12345 <-
              211.45.208.151;3656 62 syn !pass (totcp-1)
Mar 29 21:49:24 209-30-73-81.flash.net ASCEND: wan2 tcp209.30.73.91;12345 <-
              211.45.208.151;3657 62 syn !pass (totcp-1)
Mar 29 21:49:29 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.92;12345 <-
              211.45.208.151;3658 62 syn !pass (totcp-1)
Mar 29 21:49:34 209-30-73-81.flash.net ASCEND: wan2 tcp209.30.73.93;12345 <-
              211.45.208.151;3659 62 syn !pass (totcp-1)
Mar 29 21:49:40 209-30-73-81.flash.net ASCEND: wan2 tcp209.30.73.94;12345 <-
              211.45.208.151;3660 62 syn !pass (totcp-1)
Mar 29 21:49:45 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.95;12345 <-
              211.45.208.151;3661 62 syn !pass (totcp-1)
```

Analysis #8

- Description: Trojan host scan
- Active targeting: Yes
- Techniques:
  - The Class C address space 211.45.208.128-211.45.208.191 belongs to CYBERZONE-PCGAME, a company in Seoul, South Korea.
  - The packets are coming far apart enough that it could be a manual attack, but it is very methodical. The attacker is sequentially probing for every single host on this particular subnet. The attacker even attempted to probe the host that generated these log entries.
- Intent:
  - This is definitely scanning for the NetBus or GabanBus trojans.
- Evaluation:
  - This is about as noisy as you can get. It's quite apparent that the attacker doesn't care whether or not the attempt is noticed, as no attempt has been made to hide the attack.
  - This is almost certainly the work of a novice attacker. There is a chance that this could be the work of a more advanced hacker working through a "disposable" compromised host. That is, the attacker may not care if the host is discovered or blocked by the target network as long as he/she can complete a network map for a later, more stealthy attack.
  - Based on the change in source ports, whatever program the attacker is using, it appears to be going through the IP stack on the host computer.
  - I don't recognize the format of the log, and can't even tell if this is the log from an IDS or a packet-filtering device, but it is network-based. I'm not sure if the packets were denied or not.

Detect #9

```
Mar 29 06:55:02 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.19:53
Mar 29 06:55:02 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.32:53
Mar 29 06:55:02 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.33:53
Mar 29 06:55:03 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.51:53
Mar 29 06:55:03 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.62:53
Mar 29 06:55:04 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.71:53
Mar 29 06:55:04 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.80:53
Mar 29 06:55:04 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.101:53
Mar 29 06:55:04 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.104:53
Mar 29 06:55:05 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.121:53
Mar 29 06:55:05 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.134:53
Mar 29 06:55:05 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.170:53
Mar 29 06:55:05 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.186:53
Mar 29 06:55:06 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.c.204:53
Mar 29 06:55:08 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.d.52:53
Mar 29 06:55:12 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.d.252:53
Mar 29 06:55:12 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.13:53
Mar 29 06:55:13 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.63:53
Mar 29 06:55:13 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.79:53
Mar 29 06:55:13 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.88:53
Mar 29 06:55:14 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.128:53
Mar 29 06:55:15 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.161:53
Mar 29 06:55:15 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.168:53
Mar 29 06:55:15 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.171:53
Mar 29 06:55:15 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.e.187:53
Mar 29 06:55:17 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.5:53
Mar 29 06:55:17 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.15:53
Mar 29 06:55:18 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.41:53
Mar 29 06:55:18 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.45:53
Mar 29 06:55:18 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.79:53
Mar 29 06:55:19 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.86:53
Mar 29 06:55:19 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.113:53
Mar 29 06:55:19 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.128:53
Mar 29 06:55:19 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.132:53
Mar 29 06:55:20 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.145:53
Mar 29 06:55:20 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.156:53
Mar 29 06:55:22 hosth snort[311]: SCAN-SYNFIN: 210.225.49.2:53 -> a.b.f.254:53
```

Analysis #9

- Description: Network mapping
- Active targeting: Yes
- Techniques:
  - The address space 210.225.49.0 - 210.225.49.15 is registered to FANPRO Corp., in Osaka, Japan.
  - The attacker is sending packets with the SYN and FIN flags set so the target host will respond with a RST packet, thereby identifying itself as being alive, and providing some intelligence about the structure of the network.
- Intent:
  - The attacker is trying to map the network to aid in future attacks.
- Evaluation:
  - This trace is just as noisy and deliberate as the previous one. Someone is trying to identify all the active hosts in this network, likely for use at a later time.
  - Whoever wrote the rule for snort must have had it filter for the abnormal combination of the SYN and FIN TCP flags being set at the same time.
  - Had the FIN flag not been set on these packets, it would indicate the attacker was attempting a DNS zone transfer. The fact that port 53 is being targeted

Detect #10

```
6:00:58.921272 xl0 @0:1 b 12.6.117.195,1541 -> 10.0.3.18,1043 PR udp len 20 36
12:53:57.118386 xl0 @0:1 b 12.6.117.195,1270 -> 10.0.3.22,1856 PR udp len 20 36
12:57:48.130925 xl0 @0:1 b 12.6.117.195,1291 -> 10.0.3.22,1856 PR udp len 20 36
13:00:51.127272 xl0 @0:1 b 12.6.117.195,1324 -> 10.0.3.22,1856 PR udp len 20 36
16:00:58.922605 xl0 @0:1 b 12.6.117.195,1543 -> 10.0.3.7,1043 PR udp len 20 36
16:02:00.960817 xl0 @0:1 b 12.6.117.195,1663 -> 10.0.3.17,1035 PR udp len 20 36
16:02:00.990634 xl0 @0:1 b 12.6.117.195,1667 -> 10.0.3.20,1034 PR udp len 20 36
16:02:01.002684 xl0 @0:1 b 12.6.117.195,1673 -> 10.0.3.19,1533 PR udp len 20 36
16:02:01.008752 xl0 @0:1 b 12.6.117.195,1675 -> 10.0.3.22,1706 PR udp len 20 36
16:02:01.021123 xl0 @0:1 b 12.6.117.195,1679 -> 10.0.3.29,1118 PR udp len 20 36
16:02:01.026963 xl0 @0:1 b 12.6.117.195,1681 -> 10.0.3.12,1110 PR udp len 20 36
16:02:01.033298 xl0 @0:1 b 12.6.117.195,1683 -> 10.0.3.21,1034 PR udp len 20 36
16:02:01.040411 xl0 @0:1 b 12.6.117.195,1685 -> 10.0.3.7,1034 PR udp len 20 36
16:02:01.062040 xl0 @0:1 b 12.6.117.195,1691 -> 10.0.3.13,1068 PR udp len 20 36
16:02:32.100881 xl0 @0:1 b 12.6.117.195,1714 -> 10.0.3.30,1053 PR udp len 20 36
16:02:32.102636 xl0 @0:1 b 12.6.117.195,1716 -> 10.0.3.12,1120 PR udp len 20 36
```

Analysis #10

- Description: Network mapping
- Active targeting: Yes
- Techniques:
  - The range 12.0.0.0 – 12.255.255.255 is owned by AT&T, and the subnet 12.6.117.192 - 12.6.117.255 has been provided to O'Neal Steel, Inc., an Alabama-based metal manufacturing company.
  - The attacker is using the same host address to send packets to all the hosts on a particular subnet in apparently random order. Scans to only two target hosts are repeated.
- Intent:
  - The attacker is attempting to identify the structure of this network, likely for use in future penetration attempts or other potentially malicious activities.
  - Another explanation for this could be that the attacker found something interesting about hosts x.x.x.22 and x.x.x.7, and was trying to hide activity to that host within a large amount of traffic to the other hosts.
- Evaluation:
  - It looks like the attacking computer has more than one probe application running. I can't think of another reason to explain the source port selections. It looks as if the attacker sent one packet to this network, waited 6 hours, sent three more with a different program, waited 3 more hours, then sent the rest with the original program. I don't think it's because the attacker was trying to hide the activity. If that was the case, the packets wouldn't all come so quickly.
  - I suppose the attacker could be a bored O'Neal Steel employee, but the more plausible explanation is that the source host is owned. The attacker must know that such a noisy attack would almost certainly be logged and acted upon, so the host is used in one big burst of activity. If the target network takes any action, the attacker moves on to another one.
  - It's hard to say what caused these packets to be logged, though it may be host address. Perhaps there has been previous malicious activity from the source network.