Global Information Assurance Certification Paper

Dana McLaughlin
GCIA Practical Assignment
Capitol Hill 2000

Assignment #1: Network Detects

Detect #1

```
10/16-16:55:26.342617  [**] site exec - Possible wu-ftpd exploit -
GIAC000623 [**] 24.31.88.99:62275 -> MY.NET.221.82:21
10/16-16:57:49.491247  [**] site exec - Possible wu-ftpd exploit -
GIAC000623 [**] 24.31.88.99:62281 -> MY.NET.221.82:21
```

1. **Source of Trace:**
   This trace came from the SnortA3.txt file included in the data for Assignment #2 of this practical. As the data will not be available after the due date for the practical, I am not including the link to the data source.

2. **Detect was generated by:**
   This detect was generated by Snort. There is no rule with this text in the Snort rule set I downloaded. I searched the www.sans.org site and found a reference at http://www.sans.org/y2k/063000.htm as shown below that would potentially match this detect.

   alert tcp any any -> $HOME_NET 21 (msg:"site exec – Possible wu-ftpd exploit – GIAC000623"; content: "SITE EXEC";)

3. **Probability the source address was spoofed:**
   The wu-ftpd site exec attack purpose is to gain root privileges on the victim system. In order to use gained privileges, the attacker would need to have two-way communication between his machine and his victim's. This is most likely not a spoofed source address.

4. **Description of attack:**
   Nslookup on the address, 24.31.88.99, shows it as being a client system, a24b31client99.hawaii.rr.com, of the ISP Road Runner in Hawaii. This is possibly a wu-ftpd site exec attempt by a user with an anonymous ftp connection to the FTP server, MY.NET.221.82. The packet is coming in from the Internet to tcp port 21 on the server with the words "site exec" in the payload.

   An authenticated, or anonymous, user on the victim FTP system can execute codes on the system. If the user passes a specialized set of arguments to the printf() function, they can then run commands with root privileges. Several c programs that can demonstrate this exploit are located on Bugtraq, http://www.securityfocus.com.

   There are a few 'site exec' vulnerabilities in wu-ftpd listed in the CVE database,

http://cve.mitre.org, CVE-1999-0080 and CVE-1999-0955, including one candidate listed, CAN-2000-0573.

5. **Attack mechanism:**
   The IDS caught two potential wu-ftpd site exec packets coming from this source, a few minutes apart. The source is attempting some action on the target system against the ftpd service. There were no scans caught in the downloaded data for this practical from this source, so a scan had been done earlier or the source had some other way of locating and choosing this target. As the detect does not list the tcp flags that were set, if any, there is a possibility that the attacker is running a script without ensuring that a connection to the target was made first. Without proof otherwise, I will assume that the two packets sent were for two different set of instructions to the server via one of the downloadable exploit scripts.

6. **Correlations:**
   A search of the data downloaded for this practical, the SANS site, and a general web search came up blank for other activity from the source address. The wu-ftpd site exec detect is reasonably common, so further attempting further correlation will doubtfully bring anything new to light.

7. **Evidence of active targeting:**
   This was a direct attack to a server that was running an ftpd daemon. Active targeting is needed to effectively launch the attack.

8. **Severity:**
   Severity = (4 [Criticality] + 5 [Lethality]) – (3 [System Countermeasures] + 2 [Network Countermeasures]) = 9 – 5 = 4

   Criticality: 4 The system targeted was an FTP server.

   Lethality: 5 If this attack is successful, the attacker will be able to execute code with root privileges.

   System Countermeasures: 3 The potential attacker most likely had a current connection on the server, and very likely was able to determine the version of the ftp application, I suspect it was vulnerable (not patched or updated) to this attack.

   Network Countermeasures: 2 I'm assuming that the Snort IDS is not on the Internet (outside) connection of a router or firewall. As the potential attacker was already connected to the server to launch this attack, the network countermeasures are not very effective against this.

9. **Defensive recommendation:**
   As per AUSCERT Advisory AA-2000.02, ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-2000.02, upgrade to the latest wu-ftpd version and / or ensure it is properly patched.

Another step that should be taken, if possible, is to limit access to the ftp server to only known entities that absolutely must have access, or remove wu-ftpd if it is not needed on the system.

10. **Multiple choice test question:**
    FTP commonly uses what port?

    A. 23
    B. 21
    C. 53
    D. 19

    Answer: B

Detect #2

```
10/10-00:48:57.758520  [**] WinGate 1080 Attempt [**] 128.46.156.117:20
-> MY.NET.202.202:1080
```

1. **Source of Trace:**
   This trace came from the SnortA10.txt file included in the data for Assignment #2 of this practical. As the data will not be available after the due date for the practical, I am not including the link to the data source.

2. **Detect was generated by:**
   This detect was generated by Snort. The below entry from the complete snort ruleset downloadable from http://www.snort.org matches closely with what could have created this detect.

   alert tcp !$HOME_NET !53 -> $HOME_NET 1080 (msg:"MISC-WinGate-1080-Attempt";flags:S;)

3. **Probability the source address was spoofed:**
   Most likely, this is not a spoofed address as the tcp connection could not be of any assistance to the attacker without completing a connection. The system involved may be a compromised system under the control of the attacker, or it could be the source is the true source.

4. **Description of attack:**
   The source address lists as csociety-ftp.ecn.purdue.edu in nslookup. The block of addresses, 128.46.0.0 – 128.46.255.255, of which the source address belongs is registered on http://www.arin.net as Purdue University's Engineering Computer Network Electrical Engineering Building.

   The non-local source is attempting to make a connection from port 20 to tcp port 1080 on the target system. This should be an initial connection, as only the syn flag is set.

This does not appear to be a standard WinGate proxy attempt for anonymous surfing, as that would standardly be a browser indicated by an ephemeral source port. The source machine is instead apparently an ftp server, as the nslookup name refers and the port involved. This detect may signify a potential attempt to upload something to the target system, or use the WinGate proxy to mask an ftp connection to another system.

5. **Attack mechanism:**
   The source, an apparent ftp server, attempts a connect to a system running the socks service. This syn packet should stimulate some type of action from the target system, whether from the socks service or the system answering with port unreachable. This makes the detect a potential attack against the socks proxy service on a WinGate server or a slow reconnaissance to map systems with the sock service running.

6. **Correlations:**
   A similar attempt from the same source and port but to a different destination was recorded in file SnortA28.txt and listed below:

   10/05-05:35:27.654656 [**] WinGate 1080 Attempt [**] 128.46.156.117:20 -> MY.NET.218.22:1080

   The source address system has had information available via the web, as a search came up with a page logged with http://www.altavista.com, http://csociety.ecn.purdue.edu/stats/csociety.users/csociety.users.html, that no longer is available for access but the entry description is listed as:

   Users logged in. System: csociety in EE14 West Lafayette, IN Maintainer: admin@csociety .ecn.purdue.edu Interface: Users IP: csociety.ecn.purdue.edu (128.46.156.117) The statistics were last updated Saturday, 5 ...

   A search of the SANS site turned up no hits on this source address. A search of WinGate+20+1080 on the SANS site also turned up no hits.

7. **Evidence of active targeting:**
   With more knowledge of the target systems, I would be more convinced on active targeting vs scanning. If the two target systems listed are SOCKS servers, I would be fairly convinced that active targeting is happening. This belief comes from the catch of only two detects among the downloaded data. If the target systems aren't SOCKS servers, then I would guess, using the same belief just mentioned, that this is slow reconnaissance. I do not believe these are 'wrong numbers' as two different target addresses were sought by the same system, rather than an occasional hit from one system to another.

8. **Severity:**
   Severity = (3 [Criticality] + 4 [Lethality]) – (4 [System Countermeasures] + 2 [Network Countermeasures]) = 7 – 6 = 1

Criticality: 3 I feel rather ambiguous about this as how critical this attempt is depends on whether or not the target system is a server, so I decided to go middle of the road.

Lethality: 4 The source is an ftp port. As this is for file transfer, and I'm not positive that this couldn't be an attack against the target system itself, I believe its potential to be highly lethal. The lethality may apply to another victim if MY.NET system is indeed a WinGate proxy and a different system is actually the target. If this was just recon, I would bring the lethality down to a 3.

System Countermeasures: 4 No other activity was seen to the same target by this system so I'm guessing the source wasn't attempting to exploit a weakness, or the system rejected a connection.

Network Countermeasures: 2 I'm assuming that the Snort IDS is not on the Internet (outside) connection of a router or firewall. With this assumption, the connection attempt to 1080 most likely got to the target system.

9. **Defensive recommendation:**
Block access at the borders to inside services that outside systems don't need to reach. Also, if the target systems above are WinGate servers, test their configurations, ensuring that connections can only be accepted from the appropriate interface.

A potential addition to the IDS detect signatures would be to make some specific for systems of concern. These would then be targeted to alert more specifically thus removing some of the guess work on the potential intent of a detect.

10. **Multiple choice test question:**
A standard browser uses _____ to connect to a server.

A. an ephemeral port
B. port 21
C. port 80
D. port 8088

Answer: A

Detect #3

```
10/24-21:53:25.252969  [**] spp_portscan: PORTSCAN DETECTED from
24.188.153.23 (STEALTH) [**]
10/24-21:53:27.360840  [**] spp_portscan: portscan status from
24.188.153.23: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH
[**]
10/24-21:53:29.653651  [**] spp_portscan: End of portscan from
24.188.153.23 (TOTAL HOSTS:1 TCP:1 UDP:0) [**]
```

```
10/24-21:53:56.842101  [**] spp_portscan: PORTSCAN DETECTED from
24.188.153.23 (STEALTH) [**]
10/24-21:41:22.103583  [**] Null scan! [**] 24.188.153.23:6699 ->
MY.NET.204.146:1913
10/24-21:53:58.870031  [**] spp_portscan: portscan status from
24.188.153.23: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH
[**]
10/24-21:54:00.988066  [**] spp_portscan: End of portscan from
24.188.153.23 (TOTAL HOSTS:1 TCP:1 UDP:0) [**]
10/24-22:05:38.775418  [**] spp_portscan: PORTSCAN DETECTED from
24.188.153.23 (STEALTH) [**]
10/24-21:51:26.525010  [**] Null scan! [**] 24.188.153.23:6699 ->
MY.NET.204.146:1917
10/24-22:05:40.263461  [**] spp_portscan: portscan status from
24.188.153.23: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH
[**]
10/24-22:05:42.331162  [**] spp_portscan: End of portscan from
24.188.153.23 (TOTAL HOSTS:1 TCP:1 UDP:0) [**]
```

1. **Source of Trace:**
   This trace came from the SnortA29.txt file included in the data for Assignment #2 of this practical. As the data will not be available after the due date for the practical, I am not including the link to the data source.

2. **Detect was generated by:**
   This detect was generated by Snort. The below entry from the complete snort ruleset downloadable from http://www.snort.org matches closely with what could have created this detect.

   alert tcp !$HOME_NET any -> $HOME_NET any (msg:"IDS04 - SCAN-NULL Scan";flags:0; seq:0; ack:0;)

3. **Probability the source address was spoofed:**
   A standard use of tools that set improper tcp flags is for OS fingerprinting or to slip packets by filtering devices. The fingerprinting possibility would mean the source address was the true one, else the information would be lost. If the packets had some sort of payload, there is a possibility that it could be seeking to do damage, thus could be spoofed.

   As the target ports are ephemeral ports on what I am suspecting is a PC, and 6699 is a common Napster port, I am more inclined to believe 24.188.153.23 is the true source.

4. **Description of attack:**
   The source address is listed in DNS as ool-18bc9917.dyn.optonline.net, a client in the block of addresses registered in ARIN, http://whois.arin.net, for

   Optimum Online (Cablevision Systems) (NETBLK-NETBLK-OOL) NETBLK-OOL
   24.188.0.0 - 24.191.255.255
   Cablevision Systems Corp (NETBLK-OOL-6HNTNNY8-0101) OOL-6HNTNNY8-0101
   24.188.153.0 - 24.188.153.63

The detect shows the source system sending 2 tcp packets with no flags set, an improper condition for tcp communications.

5. **Attack mechanism:**
I'm suspecting that the target system was using Napster and we aren't seeing the more standard conversation that was in progress at the time of the scan packets arrival. The destination ports are a rough grouping of ephemeral ports that generally occur when an application is in operation, opening and closing tcp ports that count up from a starting port during the application's use.

I believe Snort detected an odd set of packets during a general conversation. It is known that setting improper flag combinations, or not setting any, will cause different types of target systems to react in different ways – allowing for the potential of determining what type of system (fingerprinting) is at the other end of a conversation. It is also known that some filtering systems will allow improper tcp flag combinations to pass through, in a way fingerprinting or mapping a doorway. I would not be surprised if the Napster application is trying to determine a way to get past a potential filtering system.

I know that the Napster software, and some of its clones are supposed to have some vulnerabilities but I do not see this odd tcp packet set as being a threat to application vulnerabilities.

6. **Correlations:**
A search of the rest of the data downloaded for the practical yielded the following out of SnortS30.txt:

Oct 24 21:40:34 24.188.153.23:6699 -> MY.NET.204.146:1912 UNKNOWN
21S***A* RESERVEDBITS
Oct 24 21:41:22 24.188.153.23:6699 -> MY.NET.204.146:1913 NULL ********
Oct 24 21:51:26 24.188.153.23:6699 -> MY.NET.204.146:1917 NULL ********

I found some potential correlating data with Crist Clark's Network Detect #1 Napster Strikes Back practical portion, http://www.sans.org/y2k/practical/Crist_Clark_GCIA.html. This set of data looks very similar to his write-up and potential correlation with the 'Analyze This' practical data that he reviewed. He also suspects some form of fingerprinting.

A search of the SANS site and of the Internet found no other listings for the 24.188.153.23 address. This appears to be a standard cable modem connected system, great for the speed needed to be active on Napster.

7. **Evidence of active targeting:**
There was one target machine involved which I strongly suspect was using Napster. I believe that this activity is why the packets were sent by the source, thus active

targeting.

8. **Severity:**
   Severity = (2 [Criticality] + 1 [Lethality]) – (1 [System Countermeasures] + 2 [Network Countermeasures]) = 3 - 3 = 0

   Criticality: 2 The target system was most likely a user's PC.

   Lethality: 1 Most likely there are limited extra privileges to be gained by compromising the PC.

   System Countermeasures: 1 I suspect the Napster application was installed and in use, thus the connections would be valid to the destination ports on the PC.

   Network Countermeasures: 2 I'm assuming that the IDS is on the inside of a firewall or filtering router, thus the Napster session was fully operational.

9. **Defensive recommendation:**
   Disallow, through filtering, Napster and other applications that 'share' directories among systems without regard to who will have access.

10. **Multiple choice test question:**
    What tcp flags are set in Null Scan packets?

    A. syn, ack
    B. none
    C. fin, ack
    D. all

    Answer: B

Detect #4

```
*Jan 31 16:53:54: %SEC-6-IPACCESSLOGP: list lan2378-in denied tcp
192.168.27.23(0) -> 10.23.78.15(0), 11 packets
*Jan 31 16:55:54: %SEC-6-IPACCESSLOGP: list lan2378-in denied tcp
192.168.27.26(0) -> 10.23.78.15(0), 6 packets
```

1. **Source of Trace:**
   The trace is from my network.

2. **Detect was generated by:**
   The trace comes from the log of a Cisco router. The generating access list entry was 'deny ip 192.168.0.0 0.0.255.255 any log'. The lan2378-in list is active on the incoming side of an Internet-connected router. Thus, these packets were inbound to my site from the Internet.

   The first item that caught my eye about these were the source addresses that are

specificied for private use, http://www.isi.edu/in-notes/rfc1918.txt. These addresses should not be routing across the Internet.

The next item that caught my eye was the source and destination port of 0, indicated by the "(0)" after the IP addresses. Searches on the Internet found different discussions about detects of port 0 to port 0 activity with no clear explanation that seemed to fit what I was seeing. During one particularly long string of log entries, very similar to those above, to the destination PC, I stopped by the user's desk to see what he was doing. He was reviewing pages at www.intuit.com, www.quicken.com, and www.irs.gov. The fact that packets were being blocked was invisible to him as he was seeing no unusual activity or problems. Periodically reviewing netstat during his session showed no connections that were unexpected.

Later I connected to www.irs.gov to see if I could reproduce log entries like I'd seen earlier in the day. I let the browser stay at the main page and took a look at the router log. A couple of minutes later, the router listed these:

```
*Feb 13 15:29:27: %SEC-6-IPACCESSLOGP: list lan2378-in denied tcp
192.168.19.75(0) -> 10.23.78.121(0), 1 packet
*Feb 13 15:32:47: %SEC-6-IPACCESSLOGP: list lan2378-in denied tcp
192.168.19.77(0) -> 10.23.78.121(0), 1 packet
```

I saw nothing unusual on the page and spoke with the web master. She looked over the code behind the page but found nothing strikingly unusual. I then cleared my cache and history and reconnected to the site, this time with NetXRay capturing packets on the outside interface of the router. I caught quite a string of packets, none of which were from or to port 0 as the router log was indicating.

Router Log Entries:

```
*Feb 13 15:40:08: %SEC-6-IPACCESSLOGP: list lan2378-in denied tcp
192.168.19.75(0) -> 10.23.78.121(0), 5 packets

NetXRay capture decoded with Ethereal, summary:
463 160.378550  192.168.19.75         10.23.78.121        TCP
80 > 22416 [FIN, ACK] Seq=1633620841 Ack=809310 Win=32768 Len=0
464 167.252040  192.168.19.75         10.23.78.121        TCP
80 > 22416 [FIN, ACK] Seq=1633620841 Ack=809310 Win=32768 Len=0
465 180.982588  192.168.19.75         10.23.78.121        TCP
80 > 22416 [FIN, ACK] Seq=1633620841 Ack=809310 Win=32768 Len=0
466 208.438338  192.168.19.75         10.23.78.121        TCP
80 > 22416 [FIN, ACK] Seq=1633620841 Ack=809310 Win=32768 Len=0
467 263.333012  192.168.19.75         10.23.78.121        TCP
80 > 22416 [FIN, ACK] Seq=1633620841 Ack=809310 Win=32768 Len=0
```

The router was not logging the actual ports involved, possibly due to it not having to look deeper into the packet before its deny criteria was met. According to the netstat on my PC, the destination port listed above (22416) was not, nor had it shown as open during the time of the session. It is also very unusual to see any of our PCs speaking on such high ephemeral port for an http connection. Interestingly enough, these packets match the sequence and acknowledment numbers of packet 455 (the second

one) below:

```
454 5.761208    10.23.78.121        192.239.92.40         TCP
1035 > 80 [ACK] Seq=809310 Ack=1633620841 Win=8760 Len=0
455 16.084676   192.239.92.40         10.23.78.121        TCP
80 > 1035 [FIN, ACK] Seq=1633620841 Ack=809310 Win=32768 Len=0
456 16.085022   10.23.78.121        192.239.92.40         TCP
1035 > 80 [ACK] Seq=809310 Ack=1633620842 Win=8760 Len=0
457 18.133652   192.239.92.40         10.23.78.121        TCP
80 > 1036 [FIN, ACK] Seq=1089361921 Ack=810492 Win=32768 Len=0
458 18.133709   192.239.92.40         10.23.78.121        TCP
80 > 1034 [FIN, ACK] Seq=1089017173 Ack=810579 Win=32768 Len=0
459 18.133981   10.23.78.121        192.239.92.40         TCP
1036 > 80 [ACK] Seq=810492 Ack=1089361922 Win=8242 Len=0
460 18.134030   10.23.78.121        192.239.92.40         TCP
1034 > 80 [ACK] Seq=810579 Ack=1089017174 Win=8422 Len=0
461 19.299730   192.239.92.40         10.23.78.121        TCP
80 > 1037 [FIN, ACK] Seq=1089501011 Ack=812703 Win=32768 Len=0
462 19.300018   10.23.78.121        192.239.92.40         TCP
1037 > 80 [ACK] Seq=812703 Ack=1089501012 Win=8115 Len=0
```

The private addressed packets from 192.168.19.75 came at the end of the session with irs.gov. The irs.gov computer, 192.239.92.40, sent its FIN,ACKs. My computer, running the Netscape 4.5 browser, did not do so in kind, just sending ACK responses with no FIN.

I connected again to see if I get a consistant capture set, this type doing a bit of clicking around the site. My capture showed a series of packets such as the below:

```
257 3.743797    192.239.92.40         10.23.78.121        TCP
80 > 1075 [FIN, ACK] Seq=1058169129 Ack=1722527 Win=32768 Len=0
258 3.744119    10.23.78.121        192.239.92.40         TCP
1075 > 80 [ACK] Seq=1722527 Ack=1058169130 Win=8634 Len=0
289 126.682062  192.168.19.77         10.23.78.121        TCP
80 > 23995 [FIN, ACK] Seq=1058169129 Ack=1722527 Win=32768 Len=0
291 128.223503  192.168.19.77         10.23.78.121        TCP
80 > 23995 [FIN, ACK] Seq=1058169129 Ack=1722527 Win=32768 Len=0
293 131.295424  192.168.19.77         10.23.78.121        TCP
80 > 23995 [FIN, ACK] Seq=1058169129 Ack=1722527 Win=32768 Len=0
295 137.413498  192.168.19.77         10.23.78.121        TCP
80 > 23995 [FIN, ACK] Seq=1058169129 Ack=1722527 Win=32768 Len=0
297 149.629291  192.168.19.77         10.23.78.121        TCP
80 > 23995 [FIN, ACK] Seq=1058169129 Ack=1722527 Win=32768 Len=0
```

Again, the same pattern of a FIN,ACK from the web server, only an ACK back from my PC, and a bit over two minutes later a series of 5 FIN,ACKs back to my PC, but a high unopened port, from a private address. There were several patterns such as this, one for each tcp connection that had been made to the site that the web server tried to end with a FIN,ACK.

3. **Probability the source address was spoofed:**
I don't believe this address was spoofed, at least not deliberately. The source had a

private address so I ruled out an reconnaissance attempt, as no answer would get back to the source. The destination port was not active on the PC, nor is it consistent between sessions, so I do not believe it was actively seeking a specific vulnerability. The fact that the packets are so few in number and not against anything that I could find that my PC would answer to, I don't believe this was an attempt at a denial of service attack either.

4. **Description of attack:**
I don't believe this was an attack. The suspect packets came approximately 2 minutes and 20 seconds after the last ACK was sent by my PC. I believe they were in response to the session time-out on the IRS web server, which is running a Netscape Enterprise/2.01 web server on HP-UX according to http://www.netcraft.com.

I suspect that the web server is on a network with a leaky firewall, NAT device, or proxy. My suspicion is that the system masking an internal network where the web server is, has difficulty when a session isn't torn down gracefully, ie my PC not sending FIN,ACKs in response. It may be leaking out the true system address of the web server.

I attempted to connect someone in the IRS' computer support area via e-mail but so far have had no response. I haven't located any phone number that puts me in touch with support personnel, as of this writing.

5. **Attack mechanism:**
As I mentioned above, I don't believe this is an attack. The packets come in to the client after the web server has requested a close of a conversation. They come in a fairly consistent pattern, which indicate a programmed response. Whether the response is generated by a programming bug or a misconfigured system, I can't be sure.

6. **Correlations:**
I did several searches on the web for something similar to this, but came up blank. I believe that part of my lack of success with the searches was not knowing a good was to describe the symptoms I'm seeing.

This activity seems to be consistent with connections to www.irs.gov after the very specific session tear-downs, as I discussed above. I believe this could eventually be troubleshot to some reasonable conclusion by technicians at the site generating the packets. Without being able to reproduce the same symptoms locally or find supporting evidence on the web, I am unable to correlate the detect with anything specific.

7. **Evidence of active targeting:**
There is definitely active targeting for these packets - the PC that had been connected and didn't gracefully close a session.

8. **Severity:**
   Severity = (1 [Criticality] + 1[Lethality]) – (1 [System Countermeasures] + 3 [Network Countermeasures]) = 2 – 4 = -2

   Criticality: 1 The system targeted was a PC.

   Lethality: 1 This wasn't an attack so I would have listed it as a 0, but as it is coming in with an 'untraceable' source it believe it should be a bit higher on the potential seriousness of the issue.

   System Countermeasures: 1 The PC is running a fairly standard build of Windows 95.

   Network Countermeasures: 3 The router is blocking and logging private address activity coming from the Internet.

9. **Defensive recommendation:**
   Hopefully, I will hear back from IRS computer support. It would help tremendously to be able to learn what is causing this to better ensure that our systems don't have this problem in the future.

   As for protecting my site from potential untraceable attacks and limiting the possibility that my site can launch such an attack, as a minimum, I ensure that border routers or systems block improperly addressed packets from entering, or leaving, your site. Private addressed packets from the 10, 172.16 – 31, and 192.168 networks should not be routed from your site nor should the be allowed in from the Internet.

10. **Multiple choice test question:**
    A graceful close of a tcp session consists of what possible packet pattern?

    A. server sends FIN, ACK; client sends RST
    B. client sends FIN, ACK; server sends RST
    C. client sends FIN, ACK; server sends FIN, ACK; client sends ACK
    D. server sends PSH, ACK; client sends FIN, ACK; server sends ACK

    Answer: C.

Assignment #2: "Analyze This" Scenario

The download of files for this "Analyze This" assignment contained 3 sets of Snort intrusion detection system output files. Files with names beginning with 'SnortA' contained alert detects. Files with names beginning with 'SnortS' contained scan detects. Files with names beginning with OOSche contained header output of some scan detects.

The files ranged in dates with names order not matching data order. The following table organizes the files by order of date and time. Some dates in the range were not covered

or potentially not covered fully. As the ooscheck.txt file was so far removed in date from the rest of the compilation, with a date of Aug 17, 2000, I did not consider it in this analysis.

File	Log Day	Log Date	Start Date	End Date
ooscheck		Aug 17 2000	08/17-00:05:05.377870	08/17-19:20:26.256288
snortA15	Wed	Sep 27 00:05:10 2000	09/26-00:00:52.873106	09/26-23:18:44.813310
snortA13	Thu	Sep 28 00:05:11 2000	09/27-00:08:25.610883	09/27-23:49:33.719088
snorts14	Thu	Sep 28 00:10:02 2000	09/27-01:39:55	09/27-23:54:01
snortA12	Fri	Sep 29 00:05:10 2000	09/28-00:01:00.950179	09/28-23:38:15.150179
snorts11	Fri	Sep 29 00:10:10 2000	09/28-01:57:47	09/28-23:32:40
snortA9	Sun	Oct 1 00:05:19 2000	09/30-00:00:37.300435	09/30-23:31:23.130090
snorts10	Sun	Oct 1 00:10:06 2000	09/30-01:56:33	09/30-23:24:24
snortA8	Mon	Oct 2 00:05:12 2000	10/01-00:23:20.600317	10/01-23:46:00.087878
snorts7	Mon	Oct 2 00:10:02 2000	10/01-00:33:44	10/01-23:29:46
oosche6		Oct 1 2000	10/01-00:33:53.429343	10/01-23:58:06.704384
snortA4	Tue	Oct 3 00:05:12 2000	10/02-00:14:09.595508	10/02-23:42:17.341360
snorts5	Tue	Oct 3 00:10:04 2000	10/02-03:05:13	10/02-23:29:18
snortAle	Wed	Oct 4 00:05:09 2000	10/03-00:00:16.597545	10/03-23:50:29.318825
oosche2		Oct 3 2000	10/03-00:32:48.104056	10/03-16:17:23.530147
snortsca	Wed	Oct 4 00:10:05 2000	10/03-02:45:55	10/03-23:58:28
snortA2	Thu	Oct 5 00:05:16 2000	10/04-00:16:10.764345	10/05-00:05:39.819688
oosche29		Oct 4 2000	10/04-00:36:24.832055	10/04-20:09:02.214878
oosche3		Oct 2 2000	10/04-20:09:02.214878	10/02-23:39:46.024078
snorts27	Fri	Oct 6 00:10:05 2000	10/05-00:01:15	10/05-23:50:47
snortA28	Fri	Oct 6 00:05:12 2000	10/05-00:17:08.212488	10/06-00:04:47.346149
snortA26	Sat	Oct 7 00:05:08 2000	10/06-00:00:02.864385	10/07-00:01:18.592704
snortA25	Sun	Oct 8 00:05:09 2000	10/07-00:39:30.686913	10/07-23:43:38.302486
snorts20	Sun	Oct 8 00:10:03 2000	10/07-01:56:57	10/07-23:54:24
snorts23	Sun	Oct 8 00:10:03 2000	10/07-01:56:57	10/07-23:54:24

oosche24		Oct 7 2000	10/07-05:29:21.635298	10/07-23:53:03.792636
snorts21	Mon	Oct 9 00:10:13 2000	10/08-00:05:12	10/08-23:15:58
snortA22	Mon	Oct 9 00:05:14 2000	10/08-00:19:51.200689	10/08-23:41:11.705555
snorts13	Tue	Oct 10 00:10:03 2000	10/09-00:06:20	10/09-23:14:01
snortA14	Tue	Oct 10 00:05:07 2000	10/09-00:20:07.639320	10/09-23:21:59.703069
snortA19	Tue	Oct 10 00:05:07 2000	10/09-00:20:07.639320	10/09-23:31:59.703069
snortA10	Wed	Oct 11 00:05:11 2000	10/10-00:19:56.411913	10/11-00:05:07.091039
oosche25		Oct 10 2000	10/10-01:08:36.902991	10/10-23:29:26.588688
snorts8	Wed	Oct 11 00:10:03 2000	10/10-01:16:16	10/10-23:53:13
snorts22	Thu	Oct 12 00:10:02 2000	10/11-00:06:44	10/11-23:52:57
snortA23	Thu	Oct 12 00:05:07 2000	10/11-00:20:28.174809	10/11-23:13:18.098604
snorts12	Fri	Oct 13 00:10:02 2000	10/12-00:16:55	10/12-23:08:42
snortA20	Fri	Oct 13 00:05:08 2000	10/12-00:32:32.433510	10/12-23:22:24.212366
snortA7	Sat	Oct 14 00:05:11 2000	10/13-00:00:18.504069	10/13-23:49:55.686851
snorts6	Sat	Oct 14 00:10:04 2000	10/13-00:08:50	10/13-23:20:50
snorts4	Sun	Oct 15 00:10:13 2000	10/14-00:12:57	10/14-23:48:17
snortA5	Sun	Oct 15 00:05:18 2000	10/14-00:24:33.503964	10/15-00:03:53.496377
oosche10		Oct 14 2000	10/14-01:03:37.950136	10/14-22:23:40.165066
snortA11	Mon	Oct 16 00:05:10 2000	10/15-00:14:16.519096	10/15-23:53:25.310249
snorts9	Mon	Oct 16 00:10:04 2000	10/15-00:33:03	10/15-23:41:15
snortA3	Tue	Oct 17 00:05:09 2000	10/16-00:00:22.584566	10/16-23:44:33.269370
snorts2	Tue	Oct 17 00:10:06 2000	10/16-01:19:44	10/16-22:39:35
oosche7		Oct 18 2000	10/18-00:01:38.875972	10/18-23:43:20.517671
snortA42	Thu	Oct 19 00:05:09 2000	10/18-00:05:09.269149	10/18-23:25:05.009529
snorts41	Thu	Oct 19 00:10:05 2000	10/18-00:05:19	10/18-23:43:12
snorts39	Fri	Oct 20 00:10:02 2000	10/19-00:13:47	10/19-23:27:00
snortA40	Fri	Oct 20 00:05:07 2000	10/19-00:25:04.781054	10/19-23:48:52.780324
snortA31	Sat	Oct 21	10/20-	10/21-

		00:05:07 2000	00:03:19.375790	00:02:40.271404
snorts32	Sun	Oct 22 00:10:07 2000	10/21-00:32:27	10/21-22:54:30
snortA33	Sun	Oct 22 00:05:12 2000	10/21-00:48:01.097030	10/21-23:44:49.861066
snorts37	Mon	Oct 23 00:10:02 2000	10/22-00:28:18	10/22-22:26:30
snortA38	Mon	Oct 23 00:05:19 2000	10/22-00:41:03.939124	10/22-23:22:13.188264
snortA35	Tue	Oct 24 00:05:10 2000	10/23-00:02:05.243372	10/23-23:47:23.146319
snorts36	Tue	Oct 24 00:10:03 2000	10/23-00:06:34	10/23-22:44:14
oosche34		Oct 23 2000	10/23-02:39:03.930051	10/23-22:41:52.496242
snorts30	Wed	Oct 25 00:10:02 2000	10/24-00:18:00	10/24-23:57:16
snortA29	Wed	Oct 25 00:05:08 2000	10/24-00:32:57.849453	10/24-23:49:02.581906
snortA27	Thu	Oct 26 00:05:07 2000	10/25-00:10:11.456305	10/25-23:56:14.609506
snorts24	Thu	Oct 26 00:10:11 2000	10/25-01:56:30	10/25-23:44:12
snortA21	Fri	Oct 27 00:05:09 2000	10/26-00:28:54.652275	10/26-23:14:56.342711
snorts15	Fri	Oct 27 00:10:02 2000	10/26-01:01:55	10/26-20:47:27
oosche4		Oct 26 2000	10/26-01:19:23.587851	10/26-20:46:53.781794
oosche5		Oct 26 2000	10/26-01:19:23.587851	10/26-20:46:53.781794
snortA24	Sat	Oct 28 00:05:08 2000	10/27-00:23:19.376756	10/28-00:05:01.990640
snorts35	Sun	Oct 29 00:10:07 2000	10/28-00:00:04	10/28-23:54:35
snortA36	Sun	Oct 29 00:05:08 2000	10/28-00:16:10.872009	10/28-23:51:02.429840
snorts38	Mon	Oct 30 00:10:08 2000	10/29-00:19:46	10/29-23:58:52
snortA39	Mon	Oct 30 00:05:10 2000	10/29-00:33:59.543086	10/29-23:26:34.785631
snorts33	Tue	Oct 31 00:10:05 2000	10/30-00:06:04	10/30-23:55:53
snortA34	Tue	Oct 31 00:05:08 2000	10/30-00:19:50.709153	10/30-23:52:46.054102
snorts31	Wed	Nov 1 00:10:02 2000	10/31-00:30:35	10/31-23:56:41
snortA30	Wed	Nov 1 00:05:07 2000	10/31-00:30:35.982751	10/31-23:16:42.439657
snorts3	Thu	Nov 2 00:10:15 2000	11/01-00:03:49	11/01-23:51:38
snortA6	Thu	Nov 2 00:05:11 2000	11/01-00:18:33.791271	11/02-00:01:58.340541
snorts45	Fri	Nov 3 00:10:02 2000	11/02-00:12:57	11/02-23:43:52

snorts34	Sat	Nov 4 00:10:04 2000	11/03-00:17:10	11/03-22:11:22
snortA37	Sat	Nov 4 00:05:14 2000	11/03-00:32:37.439049	11/03-23:40:34.523715
oosche44		Nov 3 2000	11/03-00:34:06.953771	11/03-20:11:09.411026
snortA43	Sun	Nov 5 00:05:13 2000	11/04-00:00:23.667847	11/04-23:48:06.988864
snorts42	Sun	Nov 5 00:10:09 2000	11/04-00:04:48	11/04-22:33:13
oosche46		Nov 4 2000	11/04-00:08:46.542587	11/04-16:40:28.642421
snortA41	Mon	Nov 6 00:05:10 2000	11/05-00:03:06.415098	11/05-23:49:24.590696
snortA44	Tue	Nov 7 00:05:07 2000	11/06-00:04:25.085837	11/07-00:04:13.786585
snortA32	Wed	Nov 8 00:05:08 2000	11/07-00:23:01.066743	11/07-23:41:47.759185
snorts16	Wed	Nov 8 00:10:03 2000	11/07-01:09:51	11/07-23:15:51
oosche17		Nov 7 2000	11/07-03:45:52.156750	11/07-23:15:59.457297
snortA53	Thu	Nov 9 00:05:06 2000	11/08-00:04:28.508468	11/08-23:42:24.092481
snortA52	Fri	Nov 10 00:05:05 2000	11/09-00:17:54.281955	11/09-23:51:17.307783
snortA46	Sat	Nov 11 00:05:09 2000	11/10-00:25:19.577205	11/10-23:51:13.285881
snorts47	Sat	Nov 11 00:10:02 2000	11/10-01:14:12	11/10-23:57:34
oosche45		Nov 10 2000	11/10-01:54:36.103987	11/11-00:00:58.497959
snorts49	Sun	Nov 12 00:10:05 2000	11/11-00:00:31	11/11-23:45:27
oosche50		Nov 11 2000	11/11-00:02:22.682514	11/11-23:45:35.484326
snortA48	Sun	Nov 12 00:05:14 2000	11/11-00:16:37.287076	11/12-00:01:41.978414
snortA51	Mon	Nov 13 00:05:08 2000	11/12-01:38:00.639935	11/12-23:46:59.181677
snorts48	Tue	Nov 14 00:10:02 2000	11/13-00:06:09	11/13-23:44:15
snortA49	Tue	Nov 14 00:05:06 2000	11/13-00:20:00.680006	11/13-23:56:24.384684
snortA45	Wed	Nov 15 00:05:07 2000	11/14-00:05:25.630667	11/14-23:50:16.654602
snorts17	Wed	Nov 15 00:10:07 2000	11/14-00:43:13	11/14-23:47:44
snortA59	Fri	Nov 17 00:05:06 2000	11/16-00:13:36.382240	11/16-23:50:16.276803
snortA55	Sat	Nov 18 00:05:07 2000	11/17-00:29:42.403295	11/17-23:40:42.591940
snorts56	Sat	Nov 18 00:10:03 2000	11/17-01:26:03	11/17-22:44:10
snorts58	Sun	Nov 19	11/18-01:35:14	11/18-23:15:51

		00:10:02 2000		
snortA57	Mon	Nov 20 00:05:08 2000	11/19-00:07:39.344116	11/19-23:23:53.241355
snortA54	Tue	Nov 21 00:05:05 2000	11/20-00:06:08.298476	11/20-23:03:12.739585
snortA50	Wed	Nov 22 00:05:05 2000	11/21-00:12:45.390786	11/22-00:04:51.076770
snortA47	Thu	Nov 23 00:05:10 2000	11/22-00:09:24.744857	11/22-23:32:20.988483
oosche20		Nov 22 2000	11/22-03:15:46.590110	11/22-23:38:18.955836
snorts18	Fri	Nov 24 00:10:17 2000	11/23-02:22:06	11/23-21:15:34
oosche19		Nov 23 2000	11/23-13:51:43.259286	11/23-20:40:29.760537

ALERTS FOUND

Alerts found among the SnortA* files along with the quantity of entries are displayed in Table A1 below. Further discussion on each will follow in alphabetical order. Items labeled with "Portscan" will be discussed together.

Prioritiess of Low, Medium, and High are listed beside each Alert type. I place priorities by what should be handled first. High priority are threats that can be reduced by a reasonably simple configuration change, ie have a quick fix, or for something that may pose a major threat either to systems or bandwidth. The priority for any one alert type should it become more or less frequent, or due to an internal network or system change. A single instance of an alert type may also have a different priority from the alert's general rating depending on the systems involved.

Table A1:

Priority	Quantity	Type of Alert
Medium	2590	Attempted Sun RPC high port access
Medium	1720	Back Orifice
High	1891	Broadcast Ping to subnet 70
	56	Connect to 515 from inside
Low	6561	End of Portscan
High	13	External RPC call
Medium	2	Happy 99 Virus
Low	15	Probable NMAP Fingerprint attempt
Low	96	NMAP TCP Ping
Low	286	Null Scan
Low	6561	Portscan Detected
Low	27752	Portscan Status
Low	147	Queso Fingerprint

Medium	218	SMB Name Wildcard
High	468	SNMP Public Access
High	62	Sun RPC High Port Access
Medium	58832	SYN-FIN Scan
Medium	2893	TCP SMTP Source Port traffic
Medium	7	Tiny Fragments – Possible hostile activity
	31219	Watchlist 220 IL-ISDNNET-990517
	8173	Watchlist 222 NET-NCFC
	4839	WinGate 1080 Attempt
Medium	13	Site exec – Possible wu-ftpd exploit – GIAC000623

ATTEMPTED SUN RPC HIGH PORT ACCESS ALERT

General Statistics:

Unique Sources:	20
Unique Destinations:	33

Top Source IP Addresses:

628	205.188.153.108
517	205.188.153.107
435	205.188.153.116
334	205.188.153.109

Note: All other sources have 146 or less Attempted SUN RPC High Port Access detects.

Top Destination IP Addresses:

488	MY.NET.221.246
435	MY.NET.225.210
365	MY.NET.217.214
347	MY.NET.206.222

Note: All other destinations registered Attempted SUN RPC High Port Access alerts 187 or less times.

BACK ORIFICE ALERT

General Statistics:

Unique Sources:	40
Unique Destinations:	932

Top Source IP Addresses:

306	62.136.90.120
291	63.46.46.143
111	203.148.182.108

99	213.43.69.72

Note: All other sources have 79 or less Back Orifice detects.

Top Destination IP Addresses:

7	MY.NET.98.150
7	MY.NET.97.208
6	MY.NET.98.82
6	MY.NET.98.81
6	MY.NET.98.77
6	MY.NET.98.151
6	MY.NET.98.119
6	MY.NET.97.142

Note: All other destinations registered Back Orifice alerts 5 or less times.

BROADCAST PING TO SUBNET 70 ALERT

There were 1891 Broadcast Pings detected to MY.NET.70.255.

General Statistics:

Unique Sources:	216

Top Source IP Addresses:

101	193.231.169.166
55	193.226.60.179
51	194.102.242.65
50	193.231.220.101
49	213.154.131.131

Note: All other sources have 44 or less Broadcast Ping detects.

CONNECT TO 515 FROM INSIDE ALERT

General Statistics:

Unique Sources:	2
Unique Destinations:	3

Source IP Addresses:

54	MY.NET.101.142
2	MY.NET.179.78

Destination IP Addresses:

54	MY.NET.100.3
1	64.244.202.66
1	64.244.202.110

EXTERNAL RPC CALL ALERT

General Statistics:

Unique Sources:	8
Unique Destinations:	3

Source IP Addresses:

3	63.162.239.69
2	211.46.110.81
2	200.191.80.206
2	200.191.80.181
1	38.200.223.8
1	24.7.227.215
1	24.23.151.112
1	12.34.21.196

Destination IP Addresses:

9	MY.NET.6.15
3	MY.NET.100.130
1	MY.NET.15.127

HAPPY 99 VIRUS ALERT

General Statistics:

Unique Sources:	2
Unique Destinations:	2

Source IP Addresses:

1	216.6.117.11
1	209.94.224.13

Destination IP Addresses:

1	MY.NET.6.35
1	MY.NET.253.41

PROBABLE NMAP FINGERPRINT ATTEMPT ALERT

General Statistics:

Unique Sources:	14
Unique Destinations:	13

Top Source IP Addresses:

2	24.95.192.51

Note: All other sources have 1 Probable NMAP Fingerprint Attempt detects.

Top Destination IP Addresses:

2	MY.NET.211.94
2	MY.NET.207.14

Note: All other destinations registered Probable NMAP Fingerprint Attempt alerts 1 time.

NMAP TCP PING ALERT

General Statistics:

Unique Sources:	21
Unique Destinations:	20

Top Source IP Addresses:

47	192.102.197.234
9	202.187.24.3
6	63.119.91.2
5	205.128.11.157
4	12.43.88.5

Note: All other sources have 3 or less NMAP TCP Ping detects.

Top Destination IP Addresses:

51	MY.NET.1.8
6	MY.NET.1.9
5	MY.NET.1.3
5	MY.NET.100.165

Note: All other destinations registered NMAP TCP Ping alerts 4 or less times.

NULL SCAN ALERT

General Statistics:

Unique Sources:	204
Unique Destinations:	196

Top Source IP Addresses:

8	24.113.148.32
8	24.112.150.20
8	128.253.247.116
7	128.195.229.11
6	207.123.161.43

Note: All other sources have 5 or less Null Scan detects.

Top Destination IP Addresses:

8	MY.NET.218.46
8	MY.NET.214.166
8	MY.NET.105.120
7	MY.NET.227.10
6	MY.NET.253.114

Note: All other destinations registered Null Scan alerts 5 or less times.

PORTSCAN ALERT

Of the 6561 portscans detected, 3836 registered as being Stealth scans.

Top Source IP Addresses:
Note: All other sources have 5 or less Null Scan detects.

QUESO FINGERPRINT ALERT

General Statistics:

Unique Sources:	29
Unique Destinations:	58

Top Source IP Addresses:

48	24.3.161.193
22	195.115.7.2
19	129.242.219.27
17	64.80.63.121
8	24.163.42.82

Note: All other sources have 5 or less Queso Fingerprint detects.

Top Destination IP Addresses:

44	MY.NET.145.9
23	MY.NET.217.26
8	MY.NET.130.116
5	MY.NET.227.10

Note: All other destinations registered Queso Fingerprint alerts 4or less times.

SMB NAME WILDCARD ALERT

General Statistics:

Unique Sources:	33

Unique Destinations:	33

Top Source IP Addresses:

93	MY.NET.101.160
33	141.157.99.21
24	169.254.184.161
20	141.157.98.201

Note: All other sources have 5 or less SMB Name Wildcard detects.

Top Destination IP Addresses:

93	MY.NET.101.192
53	MY.NET.6.15
9	MY.NET.101.53
7	MY.NET.101.153
7	MY.NET.101.117

Note: All other destinations registered SMB Name Wildcard alerts 4or less times.

SNMP PUBLIC ACCESS ALERT

General Statistics:

Unique Sources:	23
Unique Destinations:	1

The destination was MY.NET.101.192. 468 SNMP Public Access alerts were recorded.

Top Source IP Addresses:

58	MY.NET.98.106
49	MY.NET.98.174
44	MY.NET.97.185
40	MY.NET.97.171
37	MY.NET.97.204

Note: All other sources have 36 or less SNMP Public Access detects.

SUN RPC HIGH PORT ACCESS ALERT

General Statistics:

Unique Sources:	13
Unique Destinations:	12

Top Source IP Addresses:

33	216.10.12.30
8	216.148.218.160
4	205.188.3.211

Note: All other sources have 3 or less SUN RPC High Port Access detects.

Top Destination IP Addresses:

23	MY.NET.206.222
20	MY.NET.202.242

Note: All other destinations registered SUN RPC High Port Access alerts 4or less times.

SYN-FIN SCAN ALERT

General Statistics:

Unique Sources:	30
Unique Destinations:	25751

Top Source IP Addresses:

7199	160.78.49.191
6635	208.61.4.207
5164	210.101.101.110
4967	209.92.40.32
3897	63.195.56.20

Note: All other sources have 3860 or less SYN-FIN Scan detects.

Top Destination IP Addresses:

10	MY.NET.223.251
9	MY.NET.70.84
9	MY.NET.224.79
9	MY.NET.221.233
9	MY.NET.1.88
9	MY.NET.104.90

Note: All other destinations registered SYN-FIN Scan alerts 8 or less times.

TCP SMTP SOURCE PORT TRAFFIC ALERT

General Statistics:

Unique Sources:	4
Unique Destinations:	2836

Source IP Addresses:

1789	211.46.110.81
1096	24.7.227.215
6	194.67.168.11
2	194.88.77.240

All destinations registered TCP SMTP Source Port Traffic alerts 2 or less times.

TINY FRAGMENTS – POSSIBLE HOSTILE ACTIVITY ALERT

General Statistics:

Unique Sources:	5
Unique Destinations:	6

Source IP Addresses:

2	62.6.71.0
2	216.43.55.44
1	202.156.51.76
1	192.206.151.152
1	172.157.126.93

Destination IP Addresses:

2	MY.NET.181.144
1	MY.NET.211.2
1	MY.NET.202.102
1	MY.NET.201.2
1	MY.NET.201.198
1	MY.NET.1.8

WATCHLIST 220 IL-ISDNNET-990517 ALERT

General Statistics:

Unique Sources:	61
Unique Destinations:	108

Top Source IP Addresses:

6117	212.179.95.5
4011	212.179.27.6
3950	212.179.79.2
3938	212.179.44.115
1591	212.179.72.226
1353	212.179.41.24

Note: All other sources have 950 or less Watchlist 220 detects.

Top Destination IP Addresses:

4810	MY.NET.211.146
3938	MY.NET.223.98
3914	MY.NET.206.90
1638	MY.NET.203.142
1459	MY.NET.218.142
1353	MY.NET.214.170

Note: All other destinations registered Watchlist 220 alerts 950 or less times.

WATCHLIST 222 NET-NCFC ALERT

General Statistics:

Unique Sources:	45
Unique Destinations:	26

Top Source IP Addresses:

6297	159.226.45.3
1213	159.226.91.20
123	159.226.41.166
96	159.226.5.77
65	159.226.228.1

Note: All other sources have 38 or less Watchlist 222 detects.

Top Destination IP Addresses:

5801	MY.NET.6.7
1300	MY.NET.100.230
463	MY.NET.253.43
186	MY.NET.253.41
157	MY.NET.253.42

Note: All other destinations registered Watchlist 222 alerts 70 or less times.

WINGATE 1080 ATTEMPT ALERT

General Statistics:

Unique Sources:	570
Unique Destinations:	2655

Top Source IP Addresses:

1883	63.193.210.208
225	208.194.161.155
179	198.63.2.192
158	204.117.70.5
139	64.86.5.250
135	207.114.4.46

Note: All other sources have 114 or less WinGate 1080 Attempt detects.

Top Destination IP Addresses:

372	MY.NET.206.118
126	MY.NET.225.154
76	MY.NET.60.11
69	MY.NET.60.8

41	MY.NET.60.16

Note: All other destinations registered WinGate 1080 Attempt alerts 34 or less times.

SITE EXEC – POSSIBLE WU-FTPD EXPLOIT – GIAC000623 ALERT

General Statistics:

Unique Sources:	4
Unique Destinations:	7

Source IP Addresses:

9	208.61.44.215
2	24.31.88.99
1	63.202.13.20
1	202.9.188.89

Destination IP Addresses:

4	MY.NET.205.94
3	MY.NET.130.242
2	MY.NET.221.82
1	MY.NET.99.130
1	MY.NET.97.206
1	MY.NET.130.81
1	MY.NET.100.209

SCANS DETECTED

Scans found among the SnortS* files along with the quantity of entries are displayed in Table S1 below. Further discussion on each will follow in alphabetical order.

Prioritiess of Low, Medium, and High are listed beside each Alert type. I place priorities by what should be handled first. High priority are threats that can be reduced by a reasonably simple configuration change, ie have a quick fix, or for something that may pose a major threat either to systems or bandwidth. The priority for any one alert type should it become more or less frequent, or due to an internal network or system change. A single instance of an alert type may also have a different priority from the alert's general rating depending on the systems involved.

Table S1:

Priority	Quantity	Type of Scan
	482	FIN

	48	FULLXMAS
	786	INVALIDACK
	31	NMAPID
	568	NOACK
	245	NULL
	25	SPAU
High	235499	SYN
	51657	SYNFIN
High	23954	UDP
	218	UNKNOWN
	466	VECNA
	24	XMAS

FIN SCAN

General Statistics:

Unique Sources:	46
Unique Destinations:	387

Top Source IP Addresses:

271	211.46.110.81
77	24.6.151.155
74	24.7.227.215

Note: All other sources have 4 or less FIN scan detects.

Top Destination IP Addresses:

77	MY.NET.162.36
4	MY.NET.227.10
3	MY.NET.213.130
3	MY.NET.209.234
3	MY.NET.202.70

Note: All other destinations were FIN scanned 2 or less times.

FULLXMAS SCAN

General Statistics:

Unique Sources:	40
Unique Destinations:	38

Top Source IP Addresses:

3	24.16.154.101

2	62.158.195.233
2	24.226.167.52
2	24.169.73.27
2	129.82.68.60
2	128.253.247.116
2	128.194.51.187

Note: All other sources have 1 FULLXMAS scan detect.

Top Destination IP Addresses:

3	MY.NET.221.122
3	MY.NET.220.46
3	MY.NET.206.230
2	MY.NET.205.34
2	MY.NET.204.174
2	MY.NET.201.102
2	MY.NET.140.33

Note: All other destinations were FULLXMAS scanned 1 time.

INVALIDACK SCAN

General Statistics:

Unique Sources:	309
Unique Destinations:	273

Top Source IP Addresses:

40	128.253.247.116
37	4.54.37.250
36	4.54.37.238
33	4.54.37.218
26	4.54.37.212
26	4.54.10.35
24	4.54.37.193
24	4.54.10.31

Note: All other sources have 20 or less INVALIDACK scan detects.

Top Destination IP Addresses:

276	MY.NET.5.29
34	MY.NET.227.10
12	MY.NET.204.170
11	MY.NET.201.130

Note: All other destinations were INVALIDACK scanned 9 or less times.

NMAPID SCAN

General Statistics:

Unique Sources:	26
Unique Destinations:	26

Top Source IP Addresses:

2	24.95.192.51
2	24.28.53.170
2	24.1.251.2
2	133.46.212.81
2	128.175.142.243

Note: All other sources have 1 NMAPID scan detect.

Top Destination IP Addresses:

2	MY.NET.222.118
2	MY.NET.220.166
2	MY.NET.211.94
2	MY.NET.211.146
2	MY.NET.204.218

Note: All other destinations were NMAPID scanned 1 time.

NOACK SCAN

General Statistics:

Unique Sources:	320
Unique Destinations:	281

Top Source IP Addresses:

59	128.253.247.116
20	134.88.222.41
17	132.178.218.181

Note: All other sources have 9 or less NOACK scan detects.

Top Destination IP Addresses:

49	MY.NET.227.10
20	MY.NET.212.142
16	MY.NET.204.170
15	MY.NET.130.190
10	MY.NET.223.186
10	MY.NET.211.146

Note: All other destinations were NOACK scanned 9 or less times.

NULL SCAN

General Statistics:

Unique Sources:	179
Unique Destinations:	172

Top Source IP Addresses:

9	24.113.148.32
8	128.253.247.116
6	128.195.229.11
5	24.200.9.10
5	195.132.96.165

Note: All other sources have 4 or less NULL scan detects.

Top Destination IP Addresses:

9	MY.NET.218.46
9	MY.NET.214.166
7	MY.NET.227.10
6	MY.NET.214.90

Note: All other destinations were NULL scanned 4 or less times.

SPAU SCAN

General Statistics:

Unique Sources:	17
Unique Destinations:	17

Top Source IP Addresses:

7	128.253.247.116
2	169.229.55.102
2	131.204.195.71

Note: All other sources have 1 SPAU scan detect.

Top Destination IP Addresses:

7	MY.NET.227.10
2	MY.NET.226.254
2	MY.NET.213.70

Note: All other destinations were SPAU scanned 1 time.

SYN SCAN

General Statistics:

Unique Sources:	306
Unique Destinations:	35788

Top Source IP Addresses:

20649	66.9.27.254
13057	62.252.21.241
11904	194.244.78.145
11717	63.88.175.201
9639	62.157.23.237
8939	62.96.169.86
8763	24.23.151.112
8635	64.50.161.162

Note: All other sources have 7002 or less SYN scan detects.

Top Destination IP Addresses:

11916	MY.NET.220.2
1756	MY.NET.162.77
1304	MY.NET.60.16
1166	MY.NET.204.26
1155	MY.NET.140.57
1128	MY.NET.70.121

Note: All other destinations were SYN scanned 995 or less times.

SYN-FIN SCAN

General Statistics:

Unique Sources:	49
Unique Destinations:	24926

Top Source IP Addresses:

7182	160.78.49.191
6634	208.61.4.207
4956	209.92.40.32
3860	130.89.229.48
3565	210.113.89.200
3545	203.32.161.197

Note: All other sources have 3391 or less SYN-FIN scan detects.

Top Destination IP Addresses:

9	MY.NET.224.79
9	MY.NET.106.204
8	MY.NET.98.131
8	MY.NET.253.82
8	MY.NET.232.44
8	MY.NET.232.31
8	MY.NET.223.251

8	MY.NET.198.219
8	MY.NET.104.90

Note: All other destinations were SYN-FIN scanned 7 or less times.

UDP SCAN

General Statistics:

Unique Sources:	84
Unique Destinations:	1420

Top Source IP Addresses:

9073	63.248.55.245
4702	24.9.152.152
2311	MY.NET.5.25
1535	128.61.37.65
982	24.18.90.197

Note: All other sources have 577 or less UDP scan detects.

Top Destination IP Addresses:

4702	MY.NET.218.50
1784	MY.NET.206.94
1586	MY.NET.120.36
1584	MY.NET.205.214
1360	MY.NET.215.210

Note: All other destinations were UDP scanned 1113 or less times.

UNKNOWN SCAN

General Statistics:

Unique Sources:	150
Unique Destinations:	143

Top Source IP Addresses:

10	128.253.247.116
8	24.180.132.70
6	133.46.212.81
5	24.226.167.52
5	132.178.218.181
5	128.175.135.29

Note: All other sources have 4 or less UNKNOWN scan detects.

Top Destination IP Addresses:

9	MY.NET.211.146

8	MY.NET.224.134
7	MY.NET.227.10
5	MY.NET.201.130

Note: All other destinations were UNKNOWN scanned 4 or less times.

VECNA SCAN

General Statistics:

Unique Sources:	97
Unique Destinations:	440

Top Source IP Addresses:

301	211.46.220.81
48	24.7.227.215

Note: All other sources have 4 or less VECNA scan detects.

Top Destination IP Addresses:

4	MY.NET.224.134
3	MY.NET.211.146
3	MY.NET.208.142
3	MY.NET.201.130

Note: All other destinations were VECNA scanned 2 or less times.

XMAS SCAN

General Statistics:

Unique Sources:	20
Unique Destinations:	18

Top Source IP Addresses:

5	129.97.23.95

Note: All other sources have 1 XMAS scan detect.

Top Destination IP Addresses:

5	MY.NET.221.222
2	MY.NET.217.38
2	MY.NET.214.90

Note: All other destinations were XMAS scanned 1 time.

'ANALYZE THIS' SUMMARY

Assignment #3: Analysis Process

I knew at the start that I was probably at a disadvantage by not being very familiar with Unix or Linux, or scripting tools such as Perl. But, I started out using applications I was familiar with, Windows applications such as Word 97 and Excel 97, and Access 97, thinking that it would be quicker for me to stick with what I know.

The first step I took after unzipping the data was to look at the three types of files to see what they generally looked like. I then checked out how the files were set up for date order. Finding that they didn't flow date order with file name order, I entered the information into an Excel spreadsheet for reference.

From there I spent considerable time trying to compile the files and data into some semblance of order that would allow me to start a reasonable analysis. Unfortunately I found that concatenating this amount of data using the Windows environment was painful, for me and the poor PC that spent plenty of time in the 'application not responding' mode. I also found that Word wanted to reformat, and change, the data without any direction from me, and Excel 97 has a not so nice row limit of 65535 rows. Trying to bring the data into Access without much preprocessing was also extremely time consuming and I wasn't happy with the results.

Finally, after wasting many hours and days, I stopped being stubborn and decided it was time to learn some new tricks. So, into Linux and Perl I delved. My skills with Linux aren't great but I can get around in vim and pico without much hassle, as well as handle basic command line items such as cd, cp, grep, cat, and the ever-needed man. Luckily, I also had a couple of Perl books available and someone to look over my very rusty programming shoulders to point out things like the necessary first line of every Perl program is #![location of the perl interpreter]. (I had only spent a few hours trying to figure out why my little script was getting syntax errors on a line I knew was right and wondering if I'd installed perl on the Linux workstation wrong.) I kept some of the files I had so painstaking created – the breakdown files of the different alerts – and began testing my 'skills' on them. Once I got the first script going, I was seriously kicking myself for time wasted. It only took 5 minutes of running some basic scripts (which took only a couple of days to get figured out and functional) to get done what I'd spent many days trying to accomplish.

I did quite an assortment of concatenations, splits, and sorts to come up with the tallies and comparison files I wanted. This was especially true for when I was wanting to get overall counts on the top talkers. For the top talkers, I excluded the null scan, end of portscan, portscan detected, portscan status, and syn-fin scan alerts, and all oosche* files in order to eliminate duplication.

Being new to Perl, I kept scripts very simple. Below are some sample 'beginner-style' scripts:

I used a pattern like this to separate the concatenated SnortS* file information into separate files for the different type of scans:

```
if (open (ATTACK, "sfiles.log")) {
      }
      else {
            die ("Cannot open input file!");
      }

open (OUTFILE, "> fin.scan");

while ($line = <ATTACK>)  {
      if ($line =~ /FIN/ && $line !~ /SYNFIN/) {
            @words1 = split (/ +/, $line);

            $source = @words1[1];
            $sport = @words1[3];
            $dest = @words1[5];
            $dport = @words1[7];
            $stype = @words1[9];
            $flags = @words1[11];
            $rbits = @words1[13];

            print OUTFILE "$source ";
            print OUTFILE "$sport ";
            print OUTFILE "$dest ";
            print OUTFILE "$dport ";
            print OUTFILE "$stype ";
            print OUTFILE "$flags ";
            print OUTFILE "$rbits\n";
      }
}
close OUTFILE;
```

The following script pattern I used to prepare for source address tallies:

```
if (open (ATTACK, "sfiles.log")) {
      }
      else {
            die ("Cannot open input file!");
      }

open (OUTFILE, "> fin.src");

#--------------------------------------------------------------------
------
# Process the files

while ($line = <ATTACK>)  {
      if ($line =~ /FIN/ && $line !~ /SYNFIN/) {
#           print "fin not synfin";
            @words1 = split (/ +/, $line);
```

```
            $source = @words1[1];

            print OUTFILE "$source\n";
      }
}
close OUTFILE;
```

To sort and count the source addresses, I used the following script pattern:

```
# sort the source only files
system ("sort -o /mnt/windows/giac/gcia/soriginals/counting/fin-so.src
-d /mnt/windows/giac/gcia/soriginals/perl/fin.src");

# Produce a count for each unique source
system("uniq -c /mnt/windows/giac/gcia/soriginals/counting/fin-so.src
/mnt/windows/giac/gcia/soriginals/counting/fin-sun.src");

# Sort the unique source file with counts in reverse numeric order
system("sort -o /mnt/windows/giac/gcia/soriginals/counting/fin.rso -n -
r /mnt/windows/giac/gcia/soriginals/counting/fin-sun.src");
```

Overall, I can say that my stubborn determination to do the concatenations, sorts, counts, etc in an environment that I was quite comfortable, Windows, hurt my overall ability to do full justice to this practical. The time wasted and extreme frustration was not something I would wish on anyone. One of the biggest lessons learned was that some new tricks, such as learning to use Linux and Perl, are very worthwhile and really can save time in the end. In fact, I've become convinced that these skills are mandatory for the type of analysis needed. I wish I'd learned the lesson earlier.