Global Information Assurance Certification Paper

GCIA Practical Exam for SANS Snap in San Jose IDIC Course

Analysis by

Robert Newhouse

May 31, 2000

Detect 1

```
"23May2000"  " 9:55:58"  "drop"  "domain"  "213.1.248.131"  "x.y.z.199"  "tcp"
" len 40"
"23May2000"  " 9:55:58"  "accept"  "domain"  "213.1.248.131"  "x.y.z.200"  "tcp"
" len 40"
"23May2000"  " 9:55:58"  "accept"  "domain"  "213.1.248.131"  "x.y.z.201"  "tcp"
" len 40"
"23May2000"  " 9:55:58"  "drop"  "domain"  "213.1.248.131"  "x.y.z.202"  "tcp"
" len 40"
"23May2000"  " 9:56:08"  "reject"  "domain"  "213.1.248.131"  "x.y.z.201"  "tcp"
" message SYN -> SYN-ACK -> RST"
"23May2000"  " 9:56:08"  "reject"  "domain"  "213.1.248.131"  "x.y.z.200"  "tcp"
" message SYN -> SYN-ACK -> RST"
"23May2000"  " 9:56:09"  "accept"  "domain"  "213.1.248.131"  "x.y.z.200"  "tcp"
" len 60"
"23May2000"  " 9:56:09"  "accept"  "domain"  "213.1.248.131"  "x.y.z.201"  "tcp"
" len 60"
"23May2000"  " 9:56:09"  "accept"  "domain-udp"  "213.1.248.131"  "x.y.z.201"
"udp"  " len 71"
"23May2000"  " 9:56:09"  "accept"  "domain-udp"  "213.1.248.131"  "x.y.z.201"
"udp"  " len 55"
"23May2000"  " 9:56:09"  "accept"  "domain-udp"  "213.1.248.131"  "x.y.z.200"
"udp"  " len 55"
"23May2000"  "18:01:20"  "drop"  "domain"  "141.44.25.99"  "x.y.z.199"  "tcp"  "
len 40"
"23May2000"  "18:01:20"  "drop"  "domain"  "141.44.25.99"  "x.y.z.200"  "tcp"  "
len 40"
"23May2000"  "18:01:20"  "drop"  "domain"  "141.44.25.99"  "x.y.z.201"  "tcp"  "
len 40"
"23May2000"  "18:01:20"  "drop"  "domain"  "141.44.25.99"  "x.y.z.202"  "tcp"  "
len 40"
```

1. Source of Trace
My network.

2. Detect was generated by:
ISS RealSecure first identified the incident, then the firewall logs showed the history of the attack which is shown above. Fields shown are: date, time, action, port, source ip, destination ip, protocol, info.

3. Probability the source address was spoofed
Probably not spoofed since the attacker was accepted on port 53 tcp through the firewall.

4. Description of attack
This was an IP Halfscan attack on a range of hosts on the dns tcp port that have valid internet addresses. We have two authoritative dns servers that the attacker was able to connect to but was unable to perform a zone transfer due to the security on the dns servers do not allow zone transfers. Later on that same day another IP Halfscan attack was launched from another ip address.

5. Attack mechanism
The first attack was successful to a point. He was able to find our dns servers via port 53 tcp but was unable to perform a zone transfer due to our restrictive dns servers zone files. The second attack was not successful and they could not see our dns servers.

6. Correlations

We receive the ip halfscan on port 53 tcp about once a month on average. The trace above shows two attacks on the same day but they are probably not the same person due to the fact that the first person was successful on finding our dns servers so there would be no point to try it again. The second person was unsuccessful at finding our dns servers because I had already changed the firewall rules to allow only port 53 udp to our dns servers.

7. Evidence of active targeting
Both attacks were actively targeting our range of internet connected hosts via the dns tcp port. Once the first attack found where the dns servers were, he tried actively targeting our two dns servers on port 53 udp after trying port 53 tcp to find out more information.

8. Severity
(5+2) – (4+5) = -2

9. Defensive recommendations
A stateful firewall will catch this type of scanning. Once the first attack was successful on port 53 tcp, the firewall rules were changed to only allow port 53 udp.
When the second attack came in they saw nothing.

10. Question
What information does port 53 tcp give to attackers?
A. nothing more then port 53 udp
B. list of known internet servers
C. list of mx records
D. both b and c

Detect 2

Priority	Date		From	From Port	To	To Port
Information						
High	05/03/2000	5:38:33	192.5.41.41	123	my.host.1.2	742
High	05/11/2000	5:00:36	192.5.41.40	123	my.host.1.2	701
High	05/11/2000	6:36:34	192.5.41.40	123	my.host.1.2	969

1. Source of Trace
My network.

2. Detect was generated by:
ISS RealSecure.

3. Probability the source address was spoofed
There is a high probability that it could have been spoofed since the attacker tried each destination port via udp which doesn't require a 3 way handshake. After further investigation the source is not spoofed and it is coming from tick and tock at the usno.navy.mil site.

4. Description of attack
This is a UDP Port Scan attack. The two source ip addresses are coming from the ntp port and going to our server that is hosting ntp and trying various ports.

5. Attack mechanism
The attack does not work because the firewall is blocking all ports going to this host. They are trying multiple ports to see if anything responds. The interesting thing about this attack is the source port is the ntp port and coming from tick and tock at the usno.navy.mil site.

6. Correlations
We see this type of attack at least once a month coming from the same two source ip addresses. Here is actually what is happening. We have our internal ntp server connect to tick and tock at the navy.mil site via port 123 udp. Then at least once a month their servers are trying to contact our ntp servers via port 123 udp and the firewall is not allowing them to come back in so it is searching other ports for ntp.

7. Evidence of active targeting
It is definitely active targeting since it is always the same destination ip address.

8. Severity
(3+1) – (4+5) = -5

9. Defensive recommendations
No need for anymore restrictions. The ntp server is highly restricted by the firewall. No connections are allowed in from the internet.

10. Question
What is port 123 used for?
A. portmapper
B. ident
C. pop3
D. ntp

Detect 3

Priority	Date		From	From Port	To	To Port
Information						
High	05/01/2000	9:29:08	24.11.112.177	0	my.network.x.y	0
High	05/01/2000	9:31:26	171.211.29.204	0	my.network.x.y	0
High	05/01/2000	9:34:48	208.135.165.43	0	my.network.x.y	0
High	05/01/2000	9:37:14	24.218.249.198	0	my.network.x.y	0
High	05/01/2000	9:39:05	24.115.39.110	0	my.network.x.y	0
High	05/01/2000	9:40:33	24.65.95.26	0	my.network.x.y	0
High	05/01/2000	9:46:06	12.74.98.224	0	my.network.x.y	0
High	05/01/2000	9:50:16	24.30.60.210	0	my.network.x.y	0
High	05/01/2000	9:53:37	207.222.16.107	0	my.network.x.y	0
High	05/01/2000	9:59:09	199.227.173.42	0	my.network.x.y	0

```
"1May2000"  "21:29:07"  "accept"  ""  "my.network.x.y"  "24.11.112.177"  "icmp"
" icmp-type 8 icmp-code 0"
"1May2000"  "21:31:24"  "accept"  ""  "my.network.x.y"  "208.135.165.43"  "icmp"
" icmp-type 8 icmp-code 0"
"1May2000"  "21:31:25"  "accept"  ""  "my.network.x.y"  "171.211.29.204"  "icmp"
" icmp-type 8 icmp-code 0"
"1May2000"  "21:34:46"  "accept"  ""  "my.network.x.y"  "208.135.165.43"  "icmp"
" icmp-type 8 icmp-code 0"
"1May2000"  "21:34:51"  "accept"  ""  "my.network.x.y"  "171.211.29.204"  "icmp"
" icmp-type 8 icmp-code 0"
"1May2000"  "21:35:39"  "accept"  ""  "my.network.x.y"  "24.11.112.177"  "icmp"
" icmp-type 8 icmp-code 0"
```

1. Source of Trace
My network.

2. Detect was generated by:

First detected by ISS RealSecure then investigated more fully on the firewall logs. The firewall fields shown are: date, time, action, port, source ip, destination ip, protocol, info.

3. Probability the source address was spoofed
Highly probable that the source is spoofed since it is using icmp. Many icmp attacks are denial of service attacks which are spoofed addresses.

4. Description of attack
The IDS log shows a possible Smurf attack since there are quite a few icmp packets coming in at a semi-quick pace. If icmp replies were to come in faster through a packet filtering firewall, it would possibly bring the services down on the server.

5. Attack mechanism
The smurf attack is one of the most well-known denial of service attacks in which the attacker has multiple spoofed hosts send icmp replies to an internet connected server. If allowed in through the firewall, the host will try to respond to a non-existent address which will not timeout quick enough before the buffer overflows.

6. Correlations
We get these alerts almost everyday. After further investigation and looking through the firewall logs, the firewall logs show each icmp reply was in response to an icmp request coming from inside our network. The culprit is an application called "Napster" which goes out to the internet finding music files and will first send out icmp request to find the quickest server available.

7. Evidence of active targeting
It does look like active targeting because the destination ip address is always the same which is the ip address we use for connecting to the internet.

8. Severity
Since this is a false positive the formula is: (0+0) – (4+5) = -9

9. Defensive recommendations
No defensive action needed. We have requested from our users not to use napster.

10. Question
What protocol does a smurf attack utilitze?
A. icmp
B. tcp
C. udp
D. none of the above

Detect 4

`Host IP: my.email.host.ip`

To Port	Priority	Date		From	From Port	Information
0	Medium	05/02/2000	2:37:40A	194.217.242.90	0	TCP header length too large
0	Medium	05/02/2000	4:18:36A	194.217.242.6	0	TCP header length too large
0	Medium	05/02/2000	5:23:13A	194.217.242.34	0	IP+TCP headers exceed total IP length
0	Medium	05/02/2000	5:23:17A	194.217.242.34	0	TCP header length too large
0	Medium	05/02/2000	5:54:06A	194.217.242.14	0	TCP header length too large

0	Medium	05/02/2000	5:54:07A	194.217.242.14	0	TCP header length too large
0	Medium	05/02/2000	5:54:09A	194.217.242.14	0	TCP header length too large
0	Medium	05/02/2000	9:28:14A	194.217.242.89	0	TCP header length too large
0	Medium	05/02/2000	9:40:20A	194.217.242.91	0	TCP header length too large
0	Medium	05/02/2000	9:40:29A	194.217.242.91	0	TCP header length too large
0	Medium	05/02/2000	10:42:30A	194.217.242.89	0	TCP header length too large
0	Medium	05/02/2000	10:43:39A	194.217.242.35	0	TCP header length too large
0	Medium	05/02/2000	10:43:42A	194.217.242.35	0	TCP header length too large
0	Medium	05/02/2000	10:43:49A	194.217.242.35	0	TCP header length too large
0	Medium	05/02/2000	10:43:50A	194.217.242.35	0	TCP header length too large

1. Source of Trace
My network.

2. Detect was generated by:
ISS RealSecure.

3. Probability the source address was spoofed
It's possible that the ip address is spoofed since the 3 way tcp handshake never occurs due to bad tcp headers.

4. Description of attack
This is an IP protocol violation attack. The tcp header length doesn't match with what the tcp header length field is indicating. This attack appears to be trying to bring down our email server with invalid tcp header information.

5. Attack mechanism
This attack can cause failures at the destination host and is a denial of service attack. This can work on older operating systems but many newer systems with security patches in place can eliminate this attack from working.

6. Correlations
This attack we receive everyday and is always demon.net. According to demon.net, their Ascend routers are overly busy and corrupting packets when going out. This attack was not successful against our server.

7. Evidence of active targeting
This attack always goes to our email server, therefore it appears to be active targeting on a daily basis.

8. Severity
(4+1) – (4+5) = -4

9. Defensive recommendations
Keep applying new patches to email server and be as restrictive as possible on the firewall.

10. Question
This trace shows what kind of attack?

A. trinoo
B. protocol violation
C. teardrop
D. smurf

Detect 5

Priority Information	Date	From	From Port	To	To Port		
Event:	**IPFrag**						
High	02/26/2000 2:29:35	38.195.127.9	0	my.usenet.server	0		
High	02/26/2000 2:29:35	216.164.126.100	0	my.usenet.server	0		
High	02/26/2000 2:29:35	38.195.127.9	0	my.usenet.server	0		
High	02/26/2000 2:29:35	216.164.126.100	0	my.usenet.server	0		
High	02/26/2000 2:29:35	38.195.127.9	0	my.usenet.server	0		
High	02/26/2000 2:29:35	216.164.126.100	0	my.usenet.server	0		
High	02/26/2000 2:29:35	38.195.127.9	0	my.usenet.server	0		
High	02/26/2000 2:29:35	216.164.126.100	0	my.usenet.server	0		
High	02/26/2000 2:29:35	38.195.127.9	0	my.usenet.server	0		
High	02/26/2000 2:29:35	216.164.126.100	0	my.usenet.server	0		
High	02/26/2000 2:29:35	38.195.127.9	0	my.usenet.server	0		
Event:	**TFTP_Get**						
Medium	02/29/2000 11:15:01	38.195.127.254	8285	my.ftp.server	69	FILE	help.txt
Medium	02/29/2000 11:15:02	38.195.127.254	8285	my.ftp.server	69	FILE	help.txt
Medium	02/29/2000 11:15:04	38.195.127.254	8285	my.ftp.server	69	FILE	help.txt
Medium	02/29/2000 11:15:08	38.195.127.254	8285	my.ftp.server	69	FILE	help.txt
Medium	02/29/2000 11:15:16	38.195.127.254	8285	my.ftp.server	69	FILE	help.txt

1. Source of Trace
My network.

2. Detect was generated by:
ISS RealSecure.

3. Probability the source address was spoofed
Probably one of the ip addresses were spoofed since during the ip frag attack two ip addresses made the attack at the same exact time.

4. Description of attack
Two attacks were done over a three day period. One was an ip frag attack against our news server. It looks like they were trying to fragment ip packets to get past the firewall and gain access to our news server. The other attack was a tftp get attack against our ftp server. It appears that they were looking to retrieve a help file which would give them more information on what the system had installed on it.

5. Attack mechanism
Both the ip frag attack and the tftp get attack are usual signs of unauthorized access attempts on operating systems. The ip frag attack tries to fragment ip packets so a packet type of firewall won't detect any malicious attempts and pass on the other packets to the host. The tftp get tries to download files from a server without any authentication. In this case it looks like the attacker was trying to retrieve a help file which they thought may give them more information about the operating system and what was installed on it.

6. Correlations
This has never been seen on our network before. After further investigation, I found out that this was a planned attack against our servers to look for potential holes in security. We passed with flying colors.

7. Evidence of active targeting
This shows active targeting to two hosts. This means that a reconnaissance mission was already established to know which servers to attack.

8. Severity
(3+5) – (4+4) = 0

9. Defensive recommendations
Create rule on firewall to drop anything coming from the source networks. Upgrade to the latest security patches on the host machines.

10. Question
The attacks shown above are used for?
A. passing through packet filters
B. gaining authorization access
C. password cracking
D. all of the above

Detect 6

Doing a little network mapping with ICMP? xxx.xxx.xxx.8 is the network address of this subnet, no other hosts were pinged(I drop pings and other unneeded ICMP). Note the 4 pings occur over the course of 13 hours.

```
[**] PING-ICMP Error [**]
05/08-11:11:55.384633 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x46
63.209.170.1 -> xxx.xxx.xxx.8 ICMP TTL:243 TOS:0x0 ID:0
DESTINATION UNREACHABLE: HOST UNREACHABLE

[**] PING-ICMP Error [**]
05/08-13:13:33.016245 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x46
63.209.170.1 -> xxx.xxx.xxx.8 ICMP TTL:243 TOS:0x0 ID:0
DESTINATION UNREACHABLE: HOST UNREACHABLE

[**] PING-ICMP Error [**]
05/09-01:32:43.269498 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x46
63.209.170.1 -> xxx.xxx.xxx.8 ICMP TTL:243 TOS:0x0 ID:0
DESTINATION UNREACHABLE: HOST UNREACHABLE

[**] PING-ICMP Error [**]
05/09-01:32:43.791297 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x46
63.209.170.1 -> xxx.xxx.xxx.8 ICMP TTL:243 TOS:0x0 ID:0
DESTINATION UNREACHABLE: HOST UNREACHABLE
-----------------------------------------------
```

1. Source of Trace
http://www.sans.org/y2k/051800.htm

2. Detect was generated by:
Snort.

3. Probability the source address was spoofed
The IP address was probably not spoofed since it looks like they are slowly trying to map a network.

4. Description of attack

At first glance it looks like a smurf attack but since this takes place over 13 hours, it is probably ping mapping to a broadcast address.

5. Attack mechanism
The attacker is pinging the low broadcast address of the network possibly hoping for a reply from an older BSD operating system. The older BSD operating system's would reply on the low broadcast address. This does not appear to have been successful.

6. Correlations
Network mapping using icmp broadcasts is common and a stealthy approach of reconnaissance.

7. Evidence of active targeting
The attacker is actively targeting a broadcast address but no specific host other then hoping an older BSD system will respond.

8. Severity
(3+1) – (4+3) = -3

9. Defensive recommendations
Do not allow icmp coming into internal network. If older operating systems exist then update to the latest version and apply security patches.

10. Question
In this trace, what is the attacker looking for?
A. Windows NT server
B. Macintosh system
C. Solaris 2.7 system
D. Old BSD server

Detect 7

```
May 14 23:44:17 hostb rpcbind: refused connect from 203.66.211.246 to dump()
May 14 23:45:31 hostp in.ftpd[10966]: connect from 203.66.211.246
May 14 23:45:31 hostp in.ftpd[10967]: connect from 203.66.211.246
May 14 23:45:34 hostb in.ftpd[10143]: refused connect from 203.66.211.246
May 14 23:45:39 hostr smc.ftpd[21273]: connect from 203.66.211.246
May 14 23:47:14 hostd in.ftpd[4329]: refused connect from 203.66.211.246
May 14 23:47:16 hosts ftpd[29551]: refused connect from 203.66.211.246
May 14 23:47:17 hostz ftpd[17385]: refused connect from 203.66.211.246
May 14 23:56:48 dns3 in.ftpd[3295]: refused connect from 203.66.211.246
May 14 23:56:50 dns1 ftpd[167206]: refused connect from 203.66.211.246
May 14 23:57:07 dns1 ftpd[167606]: refused connect from 203.66.211.246
May 14 23:57:10 hostl proftpd[20419] hostl (203.66.211.246[203.66.211.246]):
connected - local : z.y.x.222:21
May 14 23:57:10 hostl proftpd[20419] hostl (203.66.211.246[203.66.211.246]):
connected - remote : 203.66.211.246:1840
May 14 23:57:10 hostl proftpd[20419] hostl (203.66.211.246[203.66.211.246]):
FTP session closed.
May 14 23:57:14 hostc in.ftpd[27143]: refused connect from 203.66.211.246
May 15 04:16:49 hostr rpcbind: refused connect from 203.66.211.246 to dump()
May 15 04:16:49 hostb rpcbind: refused connect from 203.66.211.246 to dump()
May 15 04:18:08 hostr smc.ftpd[21537]: connect from 203.66.211.246
May 15 04:18:09 hostb in.ftpd[10306]: refused connect from 203.66.211.246
May 15 04:18:09 hostp in.ftpd[11813]: connect from 203.66.211.246
May 15 04:18:09 hostp in.ftpd[11812]: connect from 203.66.211.246
```

```
May 15 04:19:47 hostd in.ftpd[4485]: refused connect from 203.66.211.246
May 15 04:19:51 hosts ftpd[1839]: refused connect from 203.66.211.246
May 15 04:19:54 hostz ftpd[9197]: refused connect from 203.66.211.246
May 15 04:29:15 dns1 ftpd[167945]: refused connect from 203.66.211.246
May 15 04:29:16 dns2 in.ftpd[2648]: refused connect from 203.66.211.246
May 15 04:29:16 dns3 in.ftpd[3648]: refused connect from 203.66.211.246
May 15 04:29:35 dns1 ftpd[167687]: refused connect from 203.66.211.246
May 15 04:29:35 hostl proftpd[21301] hostl (203.66.211.246[203.66.211.246]):
connected - local : z.y.x.222:21
May 15 04:29:35 hostl proftpd[21301] hostl (203.66.211.246[203.66.211.246]):
connected - remote : 203.66.211.246:2167
May 15 04:29:35 hostl proftpd[21301] hostl (203.66.211.246[203.66.211.246]):
FTP session closed.
May 15 04:29:37 hostc in.ftpd[27524]: refused connect from 203.66.211.246
=-=-=-=-=-=-=-=-=-=-=
```

1. Source of Trace
http://www.sans.org/y2k/051900.htm
Chunghwa Telecom Co., Ltd. Data communication Business Group, Taipei, Taiwan

2. Detect was generated by:
Not familiar with this type of log but looks like a Unix style IDS.

3. Probability the source address was spoofed
The ip address was probably not spoofed since the attacker did connect to a host via ftp and also it appears to be a reconnaissance mission.

4. Description of attack
This was an attack against using the ftp port to scan a network range for information gathering and also the attacker was trying to gather operating system information via the rpc service.

5. Attack mechanism
The attack resembles information gathering and appears to be successful. They now know what hosts respond to ftp and that rpc is not available.

6. Correlations
Scanning networks via well-known ports are common information gathering on everyone's networks.

7. Evidence of active targeting
They were actively targeting a specific network range but not a specific host.

8. Severity
(3+2) – (3+4) = -2
System and network counter measures are hard to determine due to lack of knowledge of this network.

9. Defensive recommendations
Be restrictive on firewall and update ftp server with latest operating systems and patches and maybe apply tcp wrappers to secure host.

10. Question
This trace shows an example of scanning networks. Is the attack and reconnaissance successful?
A. True
B. False

Detect 8

05/13-23:46:09.435818 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:11.988071 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:12.718346 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:16.484537 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:17.045668 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:17.729597 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:18.197718 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:18.789096 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:18.976436 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:19.917760 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:20.575339 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:20.760641 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:20.948555 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:21.513919 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:22.096154 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:22.184958 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:22.325167 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:22.503635 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:23.517339 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:24.502077 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:24.736772 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:25.170625 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771
05/13-23:46:25.559089 [**] Attempted Sun RPC high port access [**] 206.151.76.5:7777 -> MY.NET.97.15:32771

1. Source of Trace
http://www.sans.org/y2k/051900.htm
(Attacks extracted from Andy Johnston's .edu network.)

2. Detect was generated by:
Snort.

3. Probability the source address was spoofed
The ip address was probably not spoofed since the attack was trying to connect to the rpc service which would give them information on the operating system.

4. Description of attack
The attacker was trying to connect to the sun rpc ports for gaining access to the operating system or hoping to see the type of file system.

5. Attack mechanism
This attack could have been an automated script since the source port never changes.

6. Correlations
RPC attacks are rare. This is probably not seen often on this network.

7. Evidence of active targeting
Yes, this is evidence of active targeting since only one specific host is involved. The attacker must have already done reconnaissance earlier to find this host.

8. Severity
(3+2) – (3+3) = -1

9. Defensive recommendations
Make sure portmapper is blocked as well as rpc ports on host or firewall connected to host.

10. Question
What information can be obtained by accessing rpc ports?
A. file system information
B. access to operating system
C. buffer overflow
D. all of the above

Detect 9

05/13-06:48:33.077902 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:48:38.673005 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:48:42.061413 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:48:42.117097 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:48:49.492004 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:48:55.887470 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:48:59.534086 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:49:11.084133 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:49:23.885588 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:49:48.086347 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:50:03.191298 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:50:26.860234 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:50:29.763281 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:50:36.562220 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:50:51.802674 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:51:10.493462 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346
05/13-06:51:19.740349 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.7:1657 -> MY.NET.221.198:6346

1. Source of Trace
http://www.sans.org/y2k/051900.htm
(Attacks extracted from Andy Johnston's .edu network.)

2. Detect was generated by:
Snort.

3. Probability the source address was spoofed
It does not appear to be spoofed. Appears to be trying to access a trojan port.

4. Description of attack
This is an attack against port 6346 which is not a well-known port. Maybe the attacker is trying a trojan attack.

5. Attack mechanism
The attack appears to be an automated script since the source port never changes.

6. Correlations
This attack must have happened earlier since it is in a watchlist on the IDS.

7. Evidence of active targeting
Definitely active targeting since the attacker is going to one host and one port.

8. Severity
(3+3) – (4+3) = -1
Hard to determine since I'm not sure if critical server and the attacker is possibly trying to take over system.

9. Defensive recommendations
Keep on watchlist and update server with the latest operating system and patches. Check files on server to see if any known trojan files exists.

10. Question
Attacking a high level unknown port is usually what type of attack?
A. denial of service
B. trojan
C. land attack
D. reconnaissance

Detect 10

05/13-23:26:07.708820 [**] WinGate 8080 Attempt [**] 209.49.30.67:3360 -> MY.NET.253.105:8080
05/13-23:26:08.561642 [**] WinGate 8080 Attempt [**] 209.49.30.67:3361 -> MY.NET.253.105:8080
05/13-23:26:23.277027 [**] WinGate 8080 Attempt [**] 209.49.30.67:3369 -> MY.NET.253.105:8080
05/13-23:27:14.345923 [**] WinGate 8080 Attempt [**] 209.49.30.67:3375 -> MY.NET.253.105:8080
05/13-23:27:31.118141 [**] WinGate 8080 Attempt [**] 209.49.30.67:3390 -> MY.NET.253.105:8080
05/13-23:27:31.418062 [**] WinGate 8080 Attempt [**] 209.49.30.67:3392 -> MY.NET.253.105:8080
05/13-23:27:45.453602 [**] WinGate 8080 Attempt [**] 209.49.30.67:3393 -> MY.NET.253.105:8080
05/13-23:27:45.635353 [**] WinGate 8080 Attempt [**] 209.49.30.67:3394 -> MY.NET.253.105:8080
05/13-23:29:37.984678 [**] WinGate 8080 Attempt [**] 209.49.30.67:3405 -> MY.NET.253.105:8080
05/13-23:29:41.734190 [**] WinGate 8080 Attempt [**] 209.49.30.67:3410 -> MY.NET.253.105:8080
05/13-23:29:51.903081 [**] WinGate 8080 Attempt [**] 209.49.30.67:3413 -> MY.NET.253.105:8080
05/13-23:30:39.095912 [**] WinGate 8080 Attempt [**] 209.49.30.67:3426 -> MY.NET.253.105:8080
05/13-23:31:07.296184 [**] WinGate 8080 Attempt [**] 24.3.26.53:1132 -> MY.NET.253.105:8080
05/13-23:34:07.855451 [**] WinGate 8080 Attempt [**] 24.3.26.53:1135 -> MY.NET.253.105:8080

1. Source of Trace
http://www.sans.org/y2k/051900.htm
(Attacks extracted from Andy Johnston's .edu network.)

2. Detect was generated by:
Snort.

3. Probability the source address was spoofed
It is unlikely the ip address is spoofed because the attacker is trying to gain access to a proxy server.

4. Description of attack
The attacker is trying quickly to obtain access to a proxy server or make use of a proxy server by its caching capabilities. Within a few minutes he has tried to access what hi thinks is a proxy server. After no success, he tries coming from another ip address hopefully expecting better results.

5. Attack mechanism
The attack came primarily from one main ip address after many failures he tried coming from a different ip address to see if the response changed or possibly not to look suspicious. It doesn't appear to be successful since the attacker tried different ip addresses.

6. Correlations
Since the attack is aimed at port 8080 for proxying, it is perhaps the attacker's intent on using a proxy server for its caching capabilities. This could also be a wrong number and the user thought this was a valid proxy server for use.

7. Evidence of active targeting
It is definitely active targeting since the ip address of the destination host doesn't change. The attacker might have done reconnaissance at an earlier time to find out that the host that is being targeted is a proxy server.

8. Severity
(3+1) – (3+4) = -3

9. Defensive recommendations
Defense was fine. It looks like attack was unsuccessful. Possibly check proxy logs to find out anymore information about the attack.

10. Question
This trace indicates:
A. trojan attack
B. denial of service
C. active targeting
D. reconnaissance