*** Northcutt, There is no use of an analysis process and this shows why this is dangerous unless you do this every day. Note in several of these there are two answers. Still the student has clearly done a lot of work and is clearly on the right path! 70 *

Craig M. Woods

Detects Submitted for GIAC certification after taking classes at SANS 2000 in Orlando.

All times are PST (GMT -8)

The detects (except for #10) are from Shadow running on my Road Runner cable modem link at home. I used a temporary system with a default Red Hat linux 6.1 install. Sort of a honeypot, as it were. It did attract a couple extra probes but not many. I don't think the hacker community expects many linux systems to be running on cable modem links.

Detect #1

A lone, unsolicited reset packet seeming to come from a web server. My computer was dead idle at the time. I hadn't run a web browser for hours. The source IP belongs to the NIC in Australia. Since the source is the Australian NIC web server I'm going to guess this is a legitimate packet that was mis-aimed. The server may have been responding to connections with forged source addresses.

```
20:51:39.713202 203.37.255.97.www > 24.xxx.xxx.xxx.1146: R
79784840:79784840(0) ack 1557352944 win 24820 (DF)
```

Detect #2

Since my default Red Hat 6.1 install has ftpd running, the tcpd answered a mystery user at 1:17 in the morning from a system hooked to Cogeco Cable Solutions. The interesting thing is that no data was transmitted in either direction and there was a 5 second gap. I'm going to guess that the gap was caused by my tcpd trying to do a reverse DNS lookup on the source ip. Since I had no DNS configured there were no DNS packets from my system during the gap. Tcpd did it's job and tried to nicely drop the connection. I believe there was some intent to probe here, maybe OS fingerprinting?

```
01:17:32.957317 24.141.160.215.3942 > 24.xxx.xxx.xxx.ftp: S
14713440:14713440(0) win 8192 <mss 1460,nop,nop,sackOK>
(DF)
01:17:32.958209 24.xxx.xxx.xxx.ftp > 24.141.160.215.3942: S
278875109:278875109(0) ack 14713441 win 32120 <mss
1460,nop,nop,sackOK> (DF)
01:17:33.108978 24.141.160.215.3942 > 24.xxx.xxx.xxx.ftp: .
14713441:14713441(0) ack 278875110 win 8760 (DF)
01:17:33.116738 24.141.160.215.3942 > 24.xxx.xxx.xxx.ftp: .
14713441:14713441(0) ack 278875110 win 16384 (DF)
01:17:38.240754 24.xxx.xxx.xxx.ftp > 24.141.160.215.3942: F
278875110:278875110(0) ack 14713441 win 32120 (DF)
01:17:38.389382 24.141.160.215.3942 > 24.xxx.xxx.xxx.ftp: .
14713441:14713441(0) ack 278875111 win 16384 (DF)
01:17:38.405914 24.141.160.215.3942 > 24.xxx.xxx.xxx.ftp: R
14713441:14713441(0) win 0 (DF)
```

Detect #3

Same night, at 1:35 am there was attempt to connect to BackOrifice trojan from somebody @home in California. No question this was a malicious probe.

```
01:35:51.658397 24.19.135.26.31790 > 24.xxx.xxx.xxx.31789:
udp 1
01:35:51.658649 24.xxx.xxx.xxx > 24.19.135.26: icmp:
24.xxx.xxx.xxx udp port 31789 unreachable [tos 0xc0]
```

Detect #4

An ssh connection? From another Road Runner user? I'm still scratching my head about this one. Could be just an honest mistake by a tele-commuter logging in in the morning.
The low source port number reinforces my claim.

```
07:05:50.395298 24.25.211.70.1025 > 24.xxx.xxx.xxx.ssh: udp
2
07:05:50.417732 24.xxx.xxx.xxx > 24.25.211.70: icmp:
24.xxx.xxx.xxx udp port ssh unreachable [tos 0xc0]
```

Detect #5

Whoa, some hack3r on New Ulm Telecom in Minnesota is really trying to contact a Netbus trojan they think is running on my system. Judging from the time gaps they must have been clicking the mouse button, trying to get through for 40 seconds or so. But why does the source port jump around like that? Does the Netbus controller program do that?

```
00:05:38.821689 209.32.248.193.2126 > 24.xxx.xxx.xxx.12345:
S 9192944:9192944(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:05:42.368160 209.32.248.193.2126 > 24.xxx.xxx.xxx.12345:
S 9192944:9192944(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:05:47.630131 209.32.248.193.2126 > 24.xxx.xxx.xxx.12345:
S 9192944:9192944(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:05:48.968796 209.32.248.193.2213 > 24.xxx.xxx.xxx.12345:
S 9203028:9203028(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:05:51.736746 209.32.248.193.2213 > 24.xxx.xxx.xxx.12345:
S 9203028:9203028(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:05:57.639761 209.32.248.193.2213 > 24.xxx.xxx.xxx.12345:
S 9203028:9203028(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:05:58.848958 209.32.248.193.2270 > 24.xxx.xxx.xxx.12345:
S 9213109:9213109(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:05:59.944076 209.32.248.193.2126 > 24.xxx.xxx.xxx.12345:
S 9192944:9192944(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:06:01.909710 209.32.248.193.2270 > 24.xxx.xxx.xxx.12345:
S 9213109:9213109(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:06:07.880662 209.32.248.193.2270 > 24.xxx.xxx.xxx.12345:
S 9213109:9213109(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:06:09.782515 209.32.248.193.2213 > 24.xxx.xxx.xxx.12345:
S 9203028:9203028(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:06:19.819362 209.32.248.193.2270 > 24.xxx.xxx.xxx.12345:
S 9213109:9213109(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
```

Detect #6

Somebody on Shaw Fiberlink in Canada sent me these three NBT-NS requests. Don't know if it's malicious or not. Windows systems are notorious for sending these out on the 'Net, gratis.

```
14:35:26.437142 24.66.24.208.netbios-ns >
24.xxx.xxx.xxx.netbios-ns:
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0x3D9C
OpCode=0
NmFlags=0x1
Rcode=0
QueryCount=1
AnswerCount=0
```

```
AuthorityCount=0
AddressRecCount=0
QuestionRecords:
Name=*               NameType=0x00 (Workstation)
QuestionType=0x21
QuestionClass=0x1


14:35:27.935796 24.66.24.208.netbios-ns >
24.xxx.xxx.xxx.netbios-ns:
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0x3D9E
OpCode=0
NmFlags=0x1
Rcode=0
QueryCount=1
AnswerCount=0
AuthorityCount=0
AddressRecCount=0
QuestionRecords:
Name=*               NameType=0x00 (Workstation)
QuestionType=0x21
QuestionClass=0x1


14:35:29.415441 24.66.24.208.netbios-ns >
24.xxx.xxx.xxx.netbios-ns:
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0x3DA0
OpCode=0
NmFlags=0x1
Rcode=0
QueryCount=1
AnswerCount=0
AuthorityCount=0
AddressRecCount=0
QuestionRecords:
Name=*               NameType=0x00 (Workstation)
QuestionType=0x21
QuestionClass=0x1
```

Detect #7

Two probes for rpcbind from somebody @Home somewhere in Europe. How widely is @Home installed in Europe? Definitely a mal-probe. From a compromised system perhaps?

```
18:33:57.354092 212.120.113.180.3773 >
24.xxx.xxx.xxx.sunrpc: S 3320461405:3320461405(0) win 32120
<mss 1460,sackOK,timestamp 72355698 0,nop,wscale 0> (DF)
18:34:00.506786 212.120.113.180.3773 >
24.xxx.xxx.xxx.sunrpc: S 3320461405:3320461405(0) win 32120
<mss 1460,sackOK,timestamp 72355998 0,nop,wscale 0> (DF)
```

Detect #8

I got these from BackOfficer Friendly on my Windows box after I took down my shadow system.
Several HTTP connection attempts from somewhere in Taipei, a system on Capital Internet Service in McClean, VA, and another system in Taiwan. I confess, need some help with these. Does anyone know what these requests are trying to do?

```
Mon Apr 03 18:12:06    HTTP request from 139.175.57.200:
GET /ftp/
Mon Apr 03 18:12:10    HTTP request from 139.175.57.200:
GET /ftp/
Mon Apr 03 20:35:50    HTTP request from 205.252.144.24:
GET /ftp/??????/URA%20COLLECT/06_2.JPG
Mon Apr 03 20:35:50    HTTP request from 205.252.144.24:
GET /ftp/??????/URA%20COLLECT/01_2.JPG
Mon Apr 03 20:35:50    HTTP request from 205.252.144.24:
GET /ftp/??????/URA%20COLLECT/06_2.JPG
Mon Apr 03 20:35:50    HTTP request from 205.252.144.24:
GET /ftp/??????/URA%20COLLECT/01_2.JPG
Mon Apr 03 20:40:46    HTTP request from 205.252.144.24:
GET /ftp/
Mon Apr 03 20:40:46    HTTP request from 205.252.144.24:
GET /ftp/
Mon Apr 03 20:44:19    HTTP request from 163.31.24.147: GET
/ftp/%E5%A3%BA%E5%9C%96%E8%9B%8B%E5%B0%88%E7%94%A8%E5%8D%80
/URA%20COLLECT/06_2.JPG
Mon Apr 03 20:44:22    HTTP request from 163.31.24.147: GET
/ftp/%E5%A3%BA%E5%9C%96%E8%9B%8B%E5%B0%88%E7%94%A8%E5%8D%80
/URA%20COLLECT/01_2.JPG
```

Detect #9

A probe to port 27374 from an IP on the RoadRunner cable system in Albany. This port is listed as the asp port in

/etc/services. But it's also a port served by the SubSeven trojan daemon. Yet another malicious probe.

```
20:27:29.677527 204.210.179.140.23004 >
xxx.xxx.xxx.xxx.asp: S 94737722:94737722(0) win 8192 <mss
512,nop,nop,sackOK> (DF)
20:27:29.761850 xxx.xxx.xxx.xxx.asp >
204.210.179.140.23004: R 0:0(0) ack 94737723 win 0
20:27:30.326454 204.210.179.140.23004 >
xxx.xxx.xxx.xxx.asp: S 94737722:94737722(0) win 8192 <mss
512,nop,nop,sackOK> (DF)
20:27:30.326606 xxx.xxx.xxx.xxx.asp >
204.210.179.140.23004: R 0:0(0) ack 94737723 win 0
20:34:22.255500 204.210.179.140.22419 >
xxx.xxx.xxx.xxx.asp: S 95143287:95143287(0) win 8192 <mss
512,nop,nop,sackOK> (DF)
20:34:22.255690 xxx.xxx.xxx.xxx.asp >
204.210.179.140.22419: R 0:0(0) ack 95143288 win 0
```

Detect #10

This last detect is pulled from the GIAC web site. I ran out of time before I got enough detects from my cable modem connection at home. The scans and probes of cable modem systems seem to run in waves. My home connection has been quiet for a couple of weeks now.

So I'll analyze a detect from Binette on an @home cable system posted to GIAC on Apr 19.

The connection attempts to tcp 8080 may be scans for Ring Zero. That's more likely than someone trying to attach to www caching proxy, which is what would normally run on that port. The attempt to tcp 1080 may be a scan for a little known trojan daemon called Winhole. Or it could be an attempt to sniff out a socks server. I think the winhole scan is more likely the purpose. The attempts to 27374 are most likely scans looking for SubSeven trojan daemons. The attempts to tcp 98 and 25789 I can't tell for sure. It's likely they could just be some trojan daemon that has been re-compiled by the attacker to use a different port number. If the victim IP address was a web site I would say that the udp packet to 137 is benign. (an attempt by Windows browser client to log into the web site server) But because it's a user's cable modem account this packet is more suspicious. Could be an attempt to find open windows 95/98 shares or just an Windows OS targeted scan.

My conclusion is that all of these are malicious probes.

The IP addresses:
206.100.37.200 is somewhere on the network owned by Cable & Wireless.
210.68.177.120 is from Digital United, Inc. in Taipei.
202.99.81.139 is from CHINANET Tianjin province network, a division of China Telecom.
63.27.191.123 is from somewhere in UUNET land.
207.181.96.5 is from Netcom Canada, Inc.
166.90.27.249 is from Level 3 Communications.
171.217.239.90 is from America Online.

```
             Apr 15 23:38:23 cc1014244-a kernel:
securityalert:
             tcp if=ef0 from 206.100.37.200:4917 to
24.3.21.199 on unserved port 8080
             Apr 15 23:38:23 cc1014244-a kernel:
securityalert:
             tcp if=ef0 from 206.100.37.200:4918 to
24.3.21.199 on unserved port 1080
             Apr 16 05:58:15 cc1014244-a kernel:
securityalert:
             tcp if=ef0 from 210.68.177.120:16147 to
24.3.21.199 on unserved port 98
             Apr 16 11:24:13 cc1014244-a kernel:
securityalert:
             tcp if=ef0 from 202.99.81.139:1961 to
24.3.21.199 on unserved port 8080
             Apr 16 12:41:53 cc1014244-a kernel:
securityalert:
             udp if=ef0 from 63.27.191.123:1130 to
24.3.21.199 on unserved port 137
             Apr 16 14:36:32 cc1014244-a kernel:
securityalert:
             tcp if=ef0 from 207.181.96.5:1101 to
24.3.21.199 on unserved port 27374
             Apr 16 17:35:07 cc1014244-a kernel:
securityalert:
             tcp if=ef0 from 166.90.27.249:3042 to
24.3.21.199 on unserved port 27374
             Apr 16 17:53:06 cc1014244-a kernel:
securityalert:
```

```
                 tcp if=ef0 from 171.217.239.90:3050 to
24.3.21.199 on unserved port 25789
```