Global Information Assurance Certification Paper

*** Northcutt, 70

Subj: PRACTICAL PORTION OF INTRUSION DETECTION

From: James J. Butterworth
To: SANS Institute

SUBJ: PRACTICAL PORTION OF INTRUSION DETECTION IMMERSION CURRICULUM

1. All detects were taken from the GIAC web site.

Detect #1

Apr 1 00:06:15 cc1014244-a kernel: securityalert: tcp if=ef0 from
216.70.121.134:1119 to A.B.C.199 on unserved port 1080
Apr 1 01:55:53 cc1014244-a kernel: securityalert: tcp if=ef0 from
210.109.56.32:3944 to A.B.C.199 on unserved port 111
Apr 1 08:35:12 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:2469 to A.B.C.199 on unserved port 22

What caused the alert?
     Attempts to access ports that have been secured.
What signatures might signify intent?
     Port 1080 is used for Socks, but has also been used for the Trojan
"WinHole". Port 111, an attempt to see if the Portmapper would respond.
Port 22 is SSH, but is also a PC Anywhere port, well known for getting in.
Degree of effort?
     Non-coordinated, but deliberate and targeted. Although these packets
arrived (seemingly) from three different sources and dispersed in time, they
are very direct in nature and attempt to illicit a specific response.

Detect #2

```
Apr 2 10:18:46 hostr portsentry[418]: attackalert:
Connect from host: 225user158.ctinets.com/203.80.225.158
to TCP port: 143
Apr 2 10:18:50 hostb portsentry[334]: attackalert:
Connect from host: 225user158.ctinets.com/203.80.225.158
to TCP port: 143
Apr 2 10:21:26 hostd portsentry[416]: attackalert:
Connect from host: 225user158.ctinets.com/203.80.225.158
to TCP port: 143
Apr 2 10:37:33 hostk portsentry[21439]: attackalert:
Connect from host: 225user158.ctinets.com/203.80.225.158
to TCP port: 143
Apr 2 10:37:37 hosty portsentry[438328]: attackalert:
Connect from host: 225user158.ctinets.com/203.80.225.158
to TCP port: 143
```

What caused the alert?
A Host scan looking for an IMAP port
What signatures might signify intent?
Individual may have previous knowledge of the network. Scans are directed at specific hosts(r/b/d/k/y) on this network. It would be interesting to know the purpose of these host machines. Are they servers or workstations?
Degree of effort?
This is on a Sunday late morning. Chances are this is a recreational effort. A look at the time between scans might indicate a pattern similar to "Read - try - reread - retry - rereread - reretry"

Detect #3

```
04/01-15:59:26.043293 158.94.234.51:1674 ->
MY.NET.70.227:6346
TCP TTL:117 TOS:0x0 ID:27853 DF
SFR**U21 Seq: 0x97FCBA Ack: 0x1141D Win: 0x5018
TCP Options => EOL EOL Opt 80 (40): 579C BBE0 E44A 83B0
0EC3
```

```
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000
0E C3 ..
04/01-16:00:33.741385 158.94.234.51:230 ->
MY.NET.70.227:1674
TCP TTL:117 TOS:0x0 ID:3310 DF
SF**** Seq: 0x18CA0098 Ack: 0x5C0B141D Win: 0x5018
TCP Options => EOL EOL Opt 163 (40): E9E3 DC07 D411 A275
0060
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000
04/01-16:04:40.716885 158.94.234.51:1674 ->
MY.NET.70.227:6346
TCP TTL:117 TOS:0x0 ID:61266 DF
SFRP**1 Seq: 0x996CFA Ack: 0x141D Win: 0x5018
TCP Options => EOL EOL Opt 238 (26): 0AE5 E007 D411 9F79
0010
0000 0000 0000 0000 0000 0000 0000 EOL EOL EOL EOL EOL EOL
EOL
EOL EOL EOL EOL EOL
04/01-16:06:18.182252 158.94.234.51:1674 ->
MY.NET.70.227:6346
TCP TTL:117 TOS:0x0 ID:46459 DF
SF*P*U1 Seq: 0xC30099 Ack: 0xDBD9141E Win: 0x5018
06 8A 18 CA 00 C3 00 99 DB D9 14 1E 06 AB 50 18
..............P.
00 00 D3 0A 00 00 A0 15 49 6C C4 07 D4 11 9F 25
........Il.....%
00 10 ..
04/01-16:07:17.708685 24.201.15.107:0 -> MY.NET.202.6:4623
TCP TTL:112 TOS:0x0 ID:53039 DF
SF**AU2 Seq: 0x4C0A90 Ack: 0x9B8D0564 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 98 (39): 1E61
040C 000A
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
0000 0000 0000
04/01-16:10:45.964767 158.94.234.51:1674 ->
MY.NET.70.227:6346
TCP TTL:117 TOS:0x0 ID:5343 DF
SFRPAU21 Seq: 0xDB009A Ack: 0x7786141E Win: 0x5018
39 FF 50 18 00 00 EC A2 00 00 7B 15 49 6C C4 07
9.P.......{.Il..
D4 11 9F 25 00 10 ...%..
04/01-16:15:31.394180 24.201.15.107:4623 -> MY.NET.202.6:76
TCP TTL:112 TOS:0x0 ID:34903 DF
SF*P** Seq: 0xA909B8D Ack: 0x5A063E Win: 0x5010
```

```
00 00 00 00 00 00 ......
04/01-16:38:37.904840 129.123.236.50:1116 ->
MY.NET.70.227:6346
TCP TTL:110 TOS:0x0 ID:2907 DF
SFR***1 Seq: 0x47D9DA59 Ack: 0x1C81443 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL Opt 85 (40): 2054
5950 453D
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
0000 0000 0000
04/01-17:15:33.055773 24.112.44.237:6688 ->
MY.NET.205.106:4042
TCP TTL:115 TOS:0x0 ID:27570 DF
SF*P*U21 Seq: 0x405819 Ack: 0xF01F38 Win: 0xA010
22 38 BD CB 00 00 01 01 05 12 1F 38 64 37 1F 38
"8.........8d7.8
69 EB i.
04/01-17:49:35.202459 24.68.74.248:6699 ->
MY.NET.206.202:2019
TCP TTL:114 TOS:0x0 ID:24611 DF
SF*P*U21 Seq: 0x12F710 Ack: 0x485 Win: 0x8010
TCP Options => EOL EOL NOP NOP Sack: 1157@54251 EOL EOL EOL
EOL
EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL
```

What caused the alert?

Mutant TCP Flag byte settings.

What signatures might signify intent?

Looking at the source/destination ports does not reveal much. Port 1674 is reportedly used as "Intel Proshare Multicast" and 76 used for "Distributed External Object Store".

The TTL values are in the same general numeric value, even though this packet spans the US/UK/CAN. I have found conflicting default values for WINNT 4.0 (128 & 120) reported, but regardless, they seem all around the same range (plus or minus a few). Might this be a pattern of an certain OS? It interests me that all of these packets have a similar TTL.

Degree of effort?

No known trojans operate on these ports. It does not seem to be a

coordinated effort, and spans a 2 hour period. If these are the only packets
received, I would call it an anomoly but wait, there is more!, Further
investigation has revealed that this may be a signature of the GnutellaNet.
Go to http://gnutella.wego.com for more information. It turns out that
the default TCP port for "out of the box" installations of gnutella is 6346
and, get this, the TTL is fully changeable in a windows GUI style box. Want
120 as TTL? enter it! You can click on the Developer's corner to look at
the protocol information.

Detect #4
NetBios StatIP at risk 151.200.18.38
Date/Time Destination IP Repeat Elapsed Additional Message
Count Time
(Seconds)
4/2/00 6:34:02AM 18.238.1.51 10 Source Port = 1197;
Destination Port = 137;
Source MAC Address = 00-60-08-90-46-57; Destination MAC Address =
00-50-73-6F-91-1F;
4/2/00 4:03:21AM 24.13.134.18 10 Source Port = 1197;
Destination Port = 137;
Source MAC Address = 00-60-08-90-46-57; Destination MAC Address =
00-50-73-6F-91-1F;
4/2/00 3:13:20AM 152.19.225.68 10 Source Port = 1197;
Destination Port =
137; Source MAC Address = 00-60-08-90-46-57; Destination MAC Address =
00-50-73-6F-91-1F;
4/2/00 1:26:31AM 24.30.152.47 10 Source Port = 1197;
Destination Port = 137;
Source MAC Address = 00-60-08-90-46-57; Destination MAC Address =
00-50-73-6F-91-1F;
4/2/00 1:08:21AM 206.84.89.187 10 Source Port = 1197;
Destination Port =
137; Source MAC Address = 00-60-08-90-46-57; Destination MAC Address =
00-50-73-6F-91-1F;

4/2/00 12:35:02AM 63.20.61.151 0 Source Port = 1197;
Destination Port= 137;
Source MAC Address = 00-60-08-90-46-57; Destination MAC
Address =
00-50-73-6F-91-1F;
4/2/00 12:30:25AM 165.230.143.111 0 Source Port = 1197;
Destination Port=
137; Source MAC Address = 00-60-08-90-46-57; Destination
MAC Address =
00-50-73-6F-91-1F;
4/2/00 12:14:52AM 24.108.24.1681 0 Source Port = 1197;
Destination Port=
137; Source MAC Address = 00-60-08-90-46-57; Destination
MAC Address =
00-50-73-6F-91-1F;<snip>

What caused the alert?
     Packets from the web going to a netbios port (this is
a bad thing!)
What signatures might signify intent?
     Could not find information on port 1197's use.
Sources are ISP's
and EDU's, even one so far as Chile. Since Chile is on the
same time zone
as this victim site, that would imply some late night
activity. The same
holds true for all of the cases.
Degree of effort?
     Due to the nature of this host, and the repeated
connect attempts to
the same machine, on the same port, during a 6 hour period,
this could very
well be a low and slow attack. It would be interesting to
know what .38 was
being used for.

Detect #5
Mar 31 19:09:34 203.85.30.129:1542 -> A.B.C.30:98 SYN
S***
Mar 31 19:09:34 203.85.30.129:1545 -> A.B.C.33:98 SYN
S***
Mar 31 19:09:38 203.85.30.129:1710 -> A.B.C.197:98 SYN
S***

```
Mar 31 19:09:38 203.85.30.129:1714 -> A.B.C.201:98 SYN
**S*****
Mar 31 19:09:38 203.85.30.129:1717 -> A.B.C.204:98 SYN
**S*****
Mar 31 19:09:38 203.85.30.129:1720 -> A.B.C.207:98 SYN
**S*****
Mar 31 19:09:38 203.85.30.129:1727 -> A.B.C.214:98 SYN
**S*****
Mar 31 19:09:38 203.85.30.129:1728 -> A.B.C.215:98 SYN
**S*****
Mar 31 19:09:38 203.85.30.129:1731 -> A.B.C.218:98 SYN
**S*****
Mar 31 19:09:36 203.85.30.129:1748 -> A.B.C.235:98 SYN
**S*****
Mar 31 19:09:36 203.85.30.129:2021 -> A.B.D.252:98 SYN
**S*****
Mar 31 19:09:37 203.85.30.129:1531 -> A.B.C.19:98 SYN
**S*****
Mar 31 19:09:39 203.85.30.129:2006 -> A.B.D.237:98 SYN
**S*****
Mar 31 19:09:39 203.85.30.129:2073 -> A.B.E.48:98 SYN
**S*****

What caused the alert?
     A host scan looking for a reply from port 98.
What signatures might signify intent?
     This is the linuxconf portscan.
Degree of effort?
     Judging from the time it took and the sequence numbers
being
generated, this is an automated tool.  This reportedly is
coming from Hong
Kong.  If this was indeed true, and if this trace was from
the US, then the
time in HK could range from 7-10AM.  The hosts being
scanned are not exactly
incrementing, it is skipping some numbers.  The scanner is
either looking
for a response on port 80 to exploit, or mapping this
subnet for linux
boxes.
```

detect #6
Apr 1 01:07:09 dns3 portsentry[6017]: attackalert: Connect from host:
1Cust152.tnt1.morganton.nc.da.uu.net/63.16.52.152 to TCP port: 1524
Apr 1 01:07:09 dns1 portsentry[438328]: attackalert: Connect from host:
1Cust152.tnt1.morganton.nc.da.uu.net/63.16.52.152 to TCP port: 1524
Apr 1 01:07:51 dns3 portsentry[6017]: attackalert: Connect from host:
1Cust152.tnt1.morganton.nc.da.uu.net/63.16.52.152 to TCP port: 1524
Apr 1 01:08:08 dns1 portsentry[438328]: attackalert: Connect from host:
1Cust152.tnt1.morganton.nc.da.uu.net/63.16.52.152 to TCP port: 1524

What caused the alert?
     That a machine was able to connect to our DNS servers
What signatures might signify intent?
     Port 1524 is ingreslock. The Ingreslock is misconfigured in certain
unpatched versions of Solaris and can lead to inadvertent disclosure of a
root shell.
Degree of effort?
     The above description, coupled with the purpose of the machines
under attack, it is apparent that the attacker is focused and knows what he
wants. This may be an attempt to gain a root shell on the DNS.

Detect #7
Apr 1 07:52:07 209.91.87.116:53 -> a.b.c.d:53 SYNFIN **SF****
Apr 1 07:58:36 209.91.87.116:53 -> a.b.c.d:53 SYNFIN **SF****

```
--------[**] spp_portscan: portscan status from
209.91.87.116: 1 connections
across 1 hosts: TCP(1), UDP(0) STEALTH [**]
04/01-07:58:46.908267 [**] spp_portscan: End of portscan
from 209.91.87.116
[**]04/01-07:58:53.300246
```

What caused the alert?
     OOB flag bit settings.
What signatures might signify intent?
     The syn/fin combination is never expected from another DNS server
Degree of effort?
     Probably a manual effort, tried the packet once, then 6 seconds later sent it again. Looking to see if DNS service is running on that host

```
Detect #8
Mar 31 13:07:10 dns3 snort[9658]:
SCAN-SYN FIN: 209.91.87.116:53 -> a.b.c.98:53
--------
[**] SCAN-SYN FIN [**]
03/31-13:07:10.106996 209.91.87.116:53 -> a.b.c.98:53
TCP TTL:24 TOS:0x0 ID:39426
**SF**** Seq: 0x16D8E494 Ack: 0x65E8A466 Win: 0x404
00 00 00 00 00 00 ......

Mar 31 13:07:10 dns1 snort[4415]: spp_portscan:
PORTSCAN DETECTED from 209.91.87.116
Mar 31 13:07:10 dns1 snort[4415]: SCAN-SYN FIN:
209.91.87.116:53 -> a.b.c.34:53
--------
[**] SCAN-SYN FIN [**]
03/31-13:07:10.123109 209.91.87.116:53 -> a.b.c.34:53
TCP TTL:24 TOS:0x0 ID:39426
**SF**** Seq: 0x16D8E494 Ack: 0x65E8A466 Win: 0x404
00 00 00 00 00 00 ......
--------
```

What caused the alert?
     OOB Flag bit settings
What signatures might signify intent?
     The syn/fin combination is never expected from another DNS server

Degree of effort?
     What is interesting to note is how this trace relates to detect #8!.
The same source is listed in detects #8 & #9! Also, detect #8 takes place
one day after detect #9. It would appear that this individual is in the
intelligence gathering phase of a brute DNS port scan. A call placed to
Danicor Technologies in Alberta, Canada might be necessary to inquire into
this acty.

Detect #9

```
192.168.111.101.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.101.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.111.102.1028 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.102.1028 > SVRLOC.MCAST.NET.427: udp 90
192.168.111.111.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.111.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.111.114.1026 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.114.1026 > SVRLOC.MCAST.NET.427: udp 90
192.168.111.164.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.111.164.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.139.19.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.139.19.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.139.38.1027 > SVRLOC.MCAST.NET.427: udp 138
192.168.139.38.1027 > SVRLOC.MCAST.NET.427: udp 90
192.168.139.82.1026 > SVRLOC.MCAST.NET.427: udp 138
192.168.139.82.1026 > SVRLOC.MCAST.NET.427: udp 90
192.168.40.112.1025 > SVRLOC.MCAST.NET.427: udp 138
192.168.40.112.1025 > SVRLOC.MCAST.NET.427: udp 90
192.168.40.58.1026 > SVRLOC.MCAST.NET.427: udp 138
192.168.40.58.1026 > SVRLOC.MCAST.NET.427: udp 90
192.168.46.23.427 > SVRLOC.MCAST.NET.427: udp 49
```

What caused the alert?
     Well, using a IANA reserved private IP addresses (unless purposely
changed here to protect even the misaligned)

What signatures might signify intent?

The source ports are not behaving normally for that range. We would expect to see these ephemeral ports incrementing. Interestingly enough, the well known ports end at 1024, the fact that these start right in that area, and repeatedly, might indicate a script in action. RFC 2608 gives some insight into the behavior of the Service Location Protocol. The reserved listening port for Service Location Protocol is 427. This is the destination port for all SLP messages. SLP messages MAY be transmitted on an ephemeral port however, replies and acknowledgements are sent to the port from which the request was issued.

Degree of effort?

This may be a signature of this service.

```
Detect #10
04/15-03:20:27.908740 MY.NET.202.98:0 -> 207.172.3.46:1524
TCP TTL:126 TOS:0x0 ID:11251 DF
2*SF*PA* Seq: 0x77007F Ack: 0x1CF162D1 Win: 0x5010
04/15-03:21:38.871505 MY.NET.202.98:1524 ->
207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:25889 DF
21SFRPAU Seq: 0x7F1FA1 Ack: 0x6434 Win: 0x5010
22 38 9D 4B 20 20 20 20 20 00 "8.K .
04/15-03:21:49.809391 MY.NET.202.98:1524 ->
207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:63271 DF
*1SF**A* Seq: 0x7F2011 Ack: 0x6467C476 Win: 0x5010
05 F4 00 77 00 7F 20 11 64 67 C4 76 00 93 50 10 ...w..
.dg.v..P.
11 1C 2F 4D 20 20 20 20 20 00 ../M .
04/15-03:22:28.212319 MY.NET.202.98:0 -> 207.172.3.46:1524
TCP TTL:126 TOS:0x0 ID:49983 DF
**SF***U Seq: 0x77007F Ack: 0x21B16521 Win: 0x5010
04/15-03:22:38.731101 MY.NET.202.98:147 ->
207.172.3.46:1524
TCP TTL:126 TOS:0x0 ID:38470 DF
21SFRPAU Seq: 0x77007F Ack: 0x22316555 Win: 0x5010
```

```
TCP Options => Opt 32 (32): 2020 2000 3839 3031 3233 3435
0000 0000 0000 0000 0000 0000 0000 0000 0000
EOL EOL EOL EOL EOL EOL EOL EOL
04/15-03:22:47.337904 MY.NET.202.98:0 -> 207.172.3.46:1524
TCP TTL:126 TOS:0x0 ID:25420 DF
21SFR*** Seq: 0x77007F Ack: 0x22916583 Win: 0x5010
22 91 65 83 22 C7 50 10 22 38 BC 44 20 20 20 20
".e.".P."8.D
20 00 .
04/15-03:22:50.497148 MY.NET.202.98:1524 ->
207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:31566 DF
2*SF*PAU Seq: 0x7F22B1 Ack: 0x6593 Win: 0x5010
33 7B 50 10 22 38 AB 60 20 20 20 20 20 00 3{P."8.` .
```

What caused the alert?

Mutant TCP flag bits set

What signatures might signify intent?

Destination port 0 to ingreslock port 1524; ingreslock port 1524 pushing data to the NNTP port 119. Hummmm, can't be good! Of note, the Happy99 trojan also lives on port 119.

Degree of effort?

The attacker is either pushing data to an unknown program or attempting a DoS. This sysadmin might want to modify his packet filters to include the source IP, and any traffic destined to or originating from ports 1524 and 119.