Global Information Assurance Certification Paper

*** Northcutt, the lessons learned section was really nice to read, there is some solid work here, this was a bit hard to read due to no formatting and so there is a deduction there. 75 *

Joseph S. Dietz, Jr.

Here is the format for my practical detect analysis:

Detect #: Title
Detect Tool:
Detect Details:
Time:
Source IP Characteristics:
Source Port Characteristics:
Destination IP Characteristics:
Destination Port Characteristics:
Log excerpt:
Date Time Source IP Dest IP Sport Dport
Total of xxx log entries.

A little about the Detect Tool:

Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Summary of Lessons Learned:

* Disabled IP redirected broadcasts on border router.
* Need to say current with web sites listing known attacks.
* Need to deploy an ID tool that is able to pick up detects at a deeper level in the IP/TCP/UDP header. I concede that my detects are limited to what can be assessed from our firewall logs. I am blind to attacks that use inappropriate tcp flag settings, inappropriate fragmentation...etc..

Thank you,

Joseph S. Dietz, Jr.
Lead Network Engineer

Joseph S. Dietz, Jr.

Detect 1: SMURF-like using limited broadcast. UDP instead of ICMP.

Detect Tool:
Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Detect Details:
This probe was detected because of the destination address 255.255.255.255. How would we ever get this packet? I would offer that most likely our border router did an ip redirect-broadcast. The packet may have originated something like 1.2.0.255. This redirect-broadcast capability was immediately disabled using the "no ip redirect-broadcast" feature of the IOS on our border router.

Time:
The probe is over several days. This was not a continuous probe. The timestamps of the probe vary.

Source IP Characteristics:
Source changes.

IP	www.arin.net whois
210.23.143.10	Asia-Pacific address space
198.142.1.242	AUSNet Services Inc.
129.130.76.13	Kansas State University
63.224.141.241	U S WEST Communications ISP
203.164.12.151	Asia-Pacific address space

There are no DNS reverse lookups for these address.

Source Port Characteristics:
Source port changes from somewhat random high ports > 1023, to upd-7 aka echo-udp

Destination IP Characteristics:
This is a probe against the broadcast address 255.255.255.255 This may have arrived as 1.2.0.255 and our router helped out by redirecting the broadcast :-(

Destination Port Characteristics:
In general ports are > 1023.
The destination port does dip below 1024

Log excerpt:

```
Date       Time                Source IP     Dest IP         Sport
Dport

25Mar2000;
0:38:13;inbound;udp;210.23.143.10;255.255.255.255;30532;47264;
25Mar2000;
0:38:34;inbound;udp;210.23.143.10;255.255.255.255;42831;31946;
25Mar2000;
0:38:54;inbound;udp;210.23.143.10;255.255.255.255;48291;10134;
25Mar2000;
0:39:15;inbound;udp;210.23.143.10;255.255.255.255;43792;41509;
25Mar2000;
0:39:35;inbound;udp;210.23.143.10;255.255.255.255;16517;20307;
25Mar2000;
0:39:56;inbound;udp;210.23.143.10;255.255.255.255;27386;1434;
...
25Mar2000;
0:53:44;inbound;udp;210.23.143.10;255.255.255.255;39203;36429;
25Mar2000;
0:54:27;inbound;udp;210.23.143.10;255.255.255.255;25671;15533;
25Mar2000;
0:54:48;inbound;udp;210.23.143.10;255.255.255.255;33416;54367;
...

Destination port does dip below 1024
Date       Time                Source IP     Dest IP         Sport
Dport

30Mar2000; 4:08:58;inbound;udp;198.142.1.242;255.255.255.255;echo-
udp;892;
...

Source port changes to upd-7,echo-udp
Date       Time                Source IP     Dest IP         Sport
Dport

29Mar2000;22:39:32;inbound;udp;139.130.76.13;255.255.255.255;echo-
udp;44515;
29Mar2000;22:39:52;inbound;udp;139.130.76.13;255.255.255.255;echo-
udp;60477;
29Mar2000;23:09:40;inbound;udp;63.224.141.241;255.255.255.255;echo-
udp;60651
;
29Mar2000;23:09:41;inbound;udp;63.224.141.241;255.255.255.255;echo-
udp;61230
;
29Mar2000;23:13:02;inbound;udp;203.164.12.151;255.255.255.255;echo-
udp;65164
;
29Mar2000;23:14:04;inbound;udp;203.164.12.151;255.255.255.255;echo-
udp;36888
;

Total of 1418 log entries.
```

Joseph S. Dietz, Jr.

Detect 2: UDP based network mapping. WinTel'ish in style.

Detect Tool:
Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Detect Details:
This probe was detected because of the destination address 1.2.255.255
This might be categorized as a slow network mapping with a Windows 95/98/NT style. The nbdatagram 138 may be repeated to hide the port scan.

Time:
The probe is repeated over several days. This was not a continuous probe. The timestamps of the probe are grouped together but not consistent. Each probes last for about eight hours. The probe is slow and it uses destination broadcast address.

Source IP Characteristics:
The source of 216.133.8.10 is static. No reverse lookup via DNS available. Www.arin.net's whois returns "Epoch Internet" owns this address space.

Source Port Characteristics:
Static always udp port 138 = nbdatagram Win95/98/NT

Destination IP Characteristics:
This is a probe against the broadcast address of one of our class-B networks 1.2.0.0

Destination Port Characteristics:
Ports increment from 1-138
In addition there are anywhere from 1-5 hits to port 138 between the individual port increments. This could be an effort to try and hide the port scan.

Log excerpt:

```
Date      Time                 Source IP    Dest IP     Sport
Dport

28Feb2000;15:57:32;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;nbda
tagra
m;
28Feb2000;16:02:48;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;nbda
tagra
m;
28Feb2000;16:07:58;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;nbda
tagra
m;
28Feb2000;16:09:18;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;33;
28Feb2000;16:09:31;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;nbda
tagra
m;
28Feb2000;16:11:42;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;34;
28Feb2000;16:13:08;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;nbda
tagra
m;
28Feb2000;16:18:18;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;nbda
tagra
m;
28Feb2000;16:21:16;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;36;
28Feb2000;16:21:32;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;nbda
tagra
m;
28Feb2000;16:23:28;inbound;udp;216.133.8.10;1.2.255.255;nbdatagram;nbda
tagra
m;

Total of 527 log entries
```

Joseph S. Dietz, Jr.

Detect 3: DNS Load Balancing "measurement" using UDP & TCP.

Detect Tool:
Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Detect Details:
      This probe was detected because of the high number of hits to a
      short list of destination ports. These hits were linked to
      1.2.3.11 and 1.2.3.12 which are our DNS and MAIL forwarders.
      The BSDi Unix man pages mentions that traceroute runs using
      UDP with the default port being 33434. This may be a load
balancer
      trying to do a measurement that looks like traceroute. The
pattern
      looks similar to DNS load balancing for a web site.

Time:
      The probes is repeated over several days. The probes are
clustered
      together in groups of 2-5 hits.

Source IP Characteristics:
      The source IP address as limited to:
       209.67.123.169   www.rivalcom.net
       38.185.173.6   psi.net
       206.191.171.4   Rival Communications Network
       206.191.171.11   no DNS reverse lookup
       209.67.78.203   Exodus Communications Inc.
       208.178.110.7   Global Crossing
      This looks like co-location for perhaps "www.rivalcom.net"

Source Port Characteristics:
      Fairly static at UDP-33434 and TCP-53

Destination IP Characteristics:
      1.2.3.11 & 1.2.3.12 are our DNS forwarders for a split horizon
DNS
      configuration. These addresses are specifically targeted.

Destination Port Characteristics:
      The destination ports cycle. Some examples are:
            2400,2401,2402 & 3311,3312,3313,3314,115
      The protocol does switch from UDP to TCP on at least on occasion.

Log excerpt:

Date   Time   Source IP   Dest IP Sport Dport
21Mar2000; 0:21:23;inbound;udp;209.67.123.169;1.2.3.12;33434;2400;
21Mar2000; 0:21:23;inbound;udp;209.67.123.169;1.2.3.12;33434;2401;
21Mar2000; 0:21:23;inbound;udp;209.67.123.169;1.2.3.12;33434;2402;
21Mar2000; 0:21:48;inbound;tcp;209.67.123.169;1.2.3.12;domain-tcp;2400;
21Mar2000; 0:21:48;inbound;tcp;209.67.123.169;1.2.3.12;domain-tcp;2401;
21Mar2000; 0:21:48;inbound;tcp;209.67.123.169;1.2.3.12;domain-tcp;2402;

21Mar2000; 1:26:40;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2301;
21Mar2000; 1:26:40;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2302;

21Mar2000; 2:12:36;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2400;
21Mar2000; 2:12:36;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2401;
21Mar2000; 2:12:36;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2402;
21Mar2000; 2:26:48;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2400;

```
21Mar2000; 3:39:36;inbound;udp;206.191.171.4;1.2.3.12;33434;2301;
21Mar2000; 3:39:36;inbound;udp;206.191.171.4;1.2.3.12;33434;2302;
21Mar2000; 3:40:11;inbound;tcp;206.191.171.4;1.2.3.12;domain-tcp;2301;
21Mar2000; 3:40:11;inbound;tcp;206.191.171.4;1.2.3.12;domain-tcp;2302;
21Mar2000; 3:45:17;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2301;
21Mar2000; 3:45:17;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2302;

21Mar2000; 4:14:37;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2400;
21Mar2000; 4:14:37;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2401;
21Mar2000; 4:14:37;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2402;
21Mar2000; 4:14:37;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2402;

21Mar2000; 4:24:45;inbound;udp;206.191.171.11;1.2.3.11;33434;2302;
21Mar2000; 4:24:45;inbound;udp;206.191.171.11;1.2.3.11;33434;2301;
21Mar2000; 4:25:35;inbound;tcp;206.191.171.11;1.2.3.11;domain-tcp;2301;
21Mar2000; 4:25:35;inbound;tcp;206.191.171.11;1.2.3.11;domain-tcp;2302;
21Mar2000; 4:58:54;inbound;tcp;38.185.173.6;1.2.3.12;domain-tcp;2301;


Different day similar detect
This looks more like regular traceroute.

Date      Time                 Source IP     Dest IP Sport Dport
30Mar2000;21:16:01;inbound;udp;208.178.110.7;1.2.3.12;33434;2202;
30Mar2000;21:16:01;inbound;udp;208.178.110.7;1.2.3.12;33434;2200;
30Mar2000;21:16:01;inbound;udp;208.178.110.7;1.2.3.12;33434;2201;

30Mar2000;22:23:05;inbound;udp;209.67.111.70;1.2.3.11;33434;2400;
30Mar2000;22:23:05;inbound;udp;209.67.111.70;1.2.3.11;33434;2401;
30Mar2000;22:23:05;inbound;udp;209.67.111.70;1.2.3.11;33434;2402;

30Mar2000;22:41:31;inbound;udp;208.184.3.84;1.2.3.12;33434;2100;
30Mar2000;22:41:31;inbound;udp;208.184.3.84;1.2.3.12;33434;2101;
30Mar2000;22:41:31;inbound;udp;208.184.3.84;1.2.3.12;33434;2102;
...
31Jan2000; 7:42:54;inbound;udp;209.67.78.203;1.2.3.12;33434;3311;
31Jan2000; 7:42:55;inbound;udp;209.67.78.203;1.2.3.12;33434;3312;
31Jan2000; 7:42:56;inbound;udp;209.67.78.203;1.2.3.12;33434;3313;
31Jan2000; 7:42:57;inbound;udp;209.67.78.203;1.2.3.12;33434;3314;
31Jan2000; 7:42:58;inbound;udp;209.67.78.203;1.2.3.12;33434;3315;

31Jan2000; 8:07:38;inbound;udp;209.67.78.203;1.2.3.12;33434;3311;
31Jan2000; 8:07:39;inbound;udp;209.67.78.203;1.2.3.12;33434;3312;
31Jan2000; 8:07:40;inbound;udp;209.67.78.203;1.2.3.12;33434;3313;
31Jan2000; 8:07:42;inbound;udp;209.67.78.203;1.2.3.12;33434;3314;
31Jan2000; 8:07:43;inbound;udp;209.67.78.203;1.2.3.12;33434;3315;

Total of 8108 log entries.



                                                        Joseph S.
Dietz, Jr.

Detect 4: Proxy Server targeted detect.

Detect Tool:
```

```
        Firewall-1 logs with home grown perl scripts to summarize the
        daily detects.  Logs are summarized every twenty-four hours.
Probes
        of 25 hits or more are reported in the daily summary.  The
        daily summaries are manually reviewed.  Additional
investigation and
        analysis is completed manually as necessary.  Only dropped
packets
        are logged.  It is not guaranteed that every dropped packet
        will be logged.

Detect Details:
      This probe was detected because of the number of hits to port
8080.
      This was targeted at our proxy servers specifically.  This was
      not a scan of our entire network for proxy servers.
      Our security policies do not allow "Internet"to initiate
connections
      to our proxy servers.  Our proxy servers actually run on port-80.

Time:
      Total detect period was about 11 hours.  Some hits were clustered
      together.  These are normal working hours.

Source IP Characteristics:
      Fairly static but the majority are from the excite.com address.
       199.172.148.172 swirly-rwcmex.excite.com
       208.184.172.168 h-208-184-172-168.aureate.com
       205.139.29.131  psun45-25e.and.navisite.com

Source Port Characteristics:
      Most hits came from port tcp-4101.

Destination IP Characteristics:
      1.2.139.20, 1.2.254.27 are our proxy servers.

Destination Port Characteristics:
      Static at HTTP proxy port 8080.

Log excerpt:

Date      Time                Source IP     Dest IP      Sport Dport

27Mar2000; 6:57:32;inbound;tcp;199.172.148.172;1.2.139.20;4101;8080;
27Mar2000; 6:59:11;inbound;tcp;199.172.148.172;1.2.139.20;4101;8080;
27Mar2000; 7:00:54;inbound;tcp;199.172.148.172;1.2.139.20;4101;8080;
27Mar2000; 7:04:18;inbound;tcp;199.172.148.172;1.2.139.20;4101;8080;
...
27Mar2000;10:24:21;inbound;tcp;208.184.172.168;1.2.254.27;3129;8080;
...
27Mar2000;17:52:34;inbound;tcp;205.139.29.131;1.2.139.20;4908;8080;

Total of 40 log entries.
```

Joseph S. Dietz, Jr.

Detect 5: Network Mapping search for portmap

Detect Tool:
Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Detect Details:
This probe was detected because of the high number of hits from the source address 210.200.75.51 and the high number of hits to the port tcp-111, portmapper aka rpcbind. The source and destination ports stay the same. This probe targeted our DMZ and screened networks.

Time:
This was a fast scan. It took place in one minute.

Source IP Characteristics:
Static 210.200.75.51
www.arin.net whois returns Asia Pacific Network

Source Port Characteristics:
Static tcp-111 rpcbind

Destination IP Characteristics:
These three networks are part of our firewall screened network and DMZ environments.
Increment from 1.2.3.1 - 1.2.3.255
Increment from 1.2.4.1 - 1.2.4.255
Increment from 1.2.5.x - 1.2.5.y (partial scan)

Destination Port Characteristics:
Static tcp-111 rpcbind

Log excerpt:

```
Date      Time                 Source IP     Dest IP Sport Dport

19Mar2000; 9:54:16;inbound;tcp;210.200.75.51;1.2.3.1;111;111;
19Mar2000; 9:54:16;inbound;tcp;210.200.75.51;1.2.3.5;111;111;
19Mar2000; 9:54:16;inbound;tcp;210.200.75.51;1.2.3.6;111;111;
19Mar2000; 9:54:16;inbound;tcp;210.200.75.51;1.2.3.7;111;111;
...
19Mar2000; 9:54:31;inbound;tcp;210.200.75.51;1.2.3.251;111;111;
19Mar2000; 9:54:31;inbound;tcp;210.200.75.51;1.2.3.252;111;111;
19Mar2000; 9:54:31;inbound;tcp;210.200.75.51;1.2.3.253;111;111;
```

```
19Mar2000; 9:54:31;inbound;tcp;210.200.75.51;1.2.3.254;111;111;
19Mar2000; 9:54:31;inbound;tcp;210.200.75.51;1.2.3.255;111;111;

Total of 517 log entries.
```

Joseph S. Dietz, Jr.

Detect 6: RTSP Detect

Detect Tool:
Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Detect Details:
This probe was detected because of the high number of hits to our proxy server with the destination port tcp-554. Our security policies do not allow for real time steaming proxy,(RTSP) services.
It is possible that our own users are attempting to connect to a steaming server. The proxy would make the connection then the steaming server would try to connect to our server. I do not have the hard data to verify this theory.

Time:
The probe lasted about 30 minutes with a few hits per minute

Source IP Characteristics:
Static 209.247.74.23 Level 3 Communications CIDR

Source Port Characteristics:
Source ports repeat

Destination IP Characteristics:
Static 1.2.2.40
This is one of our proxy servers.

Destination Port Characteristics:
Static RTSP = tcp/udp 554

Log excerpt:

Date	Time	Source IP	Dest IP	Sport	Dport

```
21Mar2000; 1:10:26;inbound;tcp;209.247.74.23;1.2.2.40;2385;rtsp;
21Mar2000; 1:10:26;inbound;tcp;209.247.74.23;1.2.2.40;2387;rtsp;

21Mar2000; 1:10:26;inbound;tcp;209.247.74.23;1.2.2.40;2374;rtsp;
21Mar2000; 1:10:26;inbound;tcp;209.247.74.23;1.2.2.40;2397;rtsp;

21Mar2000; 1:11:58;inbound;tcp;209.247.74.23;1.2.2.40;2374;rtsp;
21Mar2000; 1:11:59;inbound;tcp;209.247.74.23;1.2.2.40;2397;rtsp;

21Mar2000; 1:11:59;inbound;tcp;209.247.74.23;1.2.2.40;2385;rtsp;
21Mar2000; 1:12:52;inbound;tcp;209.247.74.23;1.2.2.40;2387;rtsp;

21Mar2000; 1:13:32;inbound;tcp;209.247.74.23;1.2.2.40;2374;rtsp;
21Mar2000; 1:13:35;inbound;tcp;209.247.74.23;1.2.2.40;2397;rtsp;

Total of 59 log entries.
```

Joseph S. Dietz, Jr.

Detect 7: Scan for "RC" trojan on port 65535.

Detect Tool:
Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Detect Details:
This probe was detected because of the high number of hits from source port 109. In addition the Source address does not change. The destination port was very interesting after reviewing a list of known trojan programs. The trojan "RC" has been found on port 65535.

Time:
This was a very fast scan. It took place in one second..? The timestamp may be a feature of our firewall log. We can safely say that this took place in the same minute.

Source IP Characteristics:
Static 199.4.121.210 www.arin.net whois reports that Best Internet Communications, Inc owns this address space.

Source Port Characteristics:
Static TCP port 109 aka pop-2

Destination IP Characteristics:

1.2.3.0 and 1.2.4.0 our CIDR addresses
Increments somewhat haphazardly threw this address space.

Destination Port Characteristics:
Static TCP port 65535. According to the list of trojans at
Von Braun's web site a trojan called "RC" is known to run on
65535.

Log excerpt:

```
Date      Time                 Source IP    Dest IP Sport Dport
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.3.1;pop-2;65535;
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.3.7;pop-2;65535;
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.3.8;pop-2;65535;
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.3.14;pop-2;65535;
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.3.21;pop-2;65535;
...
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.4.234;pop-2;65535;
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.4.241;pop-2;65535;
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.4.242;pop-2;65535;
4Mar2000;13:07:26;inbound;tcp;199.4.121.210;1.2.4.249;pop-2;65535;
```

Total of 115 log entries.

Joseph S. Dietz, Jr.

Detect 8: Network mapping using tcp-discard

Detect Tool:
Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Detect Details:
This probe was detected because of the unusual amount of hits to destination port tcp-9 and the source ip does not change.

Time:
This probe lasted for about 15 minutes. Several hits per minute.

Source IP Characteristics:
Static 129.16.13.132 DNS entry mcquack.ced.chalmers.se

Source Port Characteristics:
Appears to be somewhat random

Destination IP Characteristics:
      1.2.0.0 & 3.4.0.0 is our class-B address space.
      Destination varied back and forth between our two class-B addresses

Destination Port Characteristics:
      Static TCP-9 discard

Log excerpt:

Date   Time   Source IP   Dest IP   Sport Dport

1Apr2000;18:13:24;inbound;tcp;129.16.13.132;1.2.99.19;23655;discard-tcp;
1Apr2000;18:13:29;inbound;tcp;129.16.13.132;1.2.74.59;16238;discard-tcp;
1Apr2000;18:14:14;inbound;tcp;129.16.13.132;3.4.20.120;41141;discard-tcp;
1Apr2000;18:14:50;inbound;tcp;129.16.13.132;3.4.22.24;33588;discard-tcp;
1Apr2000;18:14:52;inbound;tcp;129.16.13.132;1.2.74.49;43908;discard-tcp;
1Apr2000;18:15:26;inbound;tcp;129.16.13.132;1.2.4.21;20228;discard-tcp;
...
1Apr2000;18:29:16;inbound;tcp;129.16.13.132;3.4.185.122;60257;discard-tcp;
1Apr2000;18:29:37;inbound;tcp;129.16.13.132;3.4.94.27;14403;discard-tcp;
1Apr2000;18:30:06;inbound;tcp;129.16.13.132;3.4.243.118;17831;discard-tcp;

Total of 100 log entries.

Joseph S. Dietz, Jr.

Detect 9: Hellnine host mapping & scan for well known ports.

Detect Tool:
      Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours. Probes of 25 hits or more are reported in the daily summary. The daily summaries are manually reviewed. Additional investigation and analysis is completed manually as necessary. Only dropped packets are logged. It is not guaranteed that every dropped packet will be logged.

Detect Details:
      This probe was detected because of the number of hits from the source address. Attempts connection to well known ports under 1024.

Source port stays the same while it tries well known destination ports.

Time:
The probes separated over sever days.

Source IP Characteristics:
Static 161.58.239.94 dns returns hellnine2000.org

Source Port Characteristics:
Changes but limited to these tcp ports 1934,1055,1295,1440

Destination IP Characteristics:
Several different ip addresses in our class-B networks
1.2.0.0 & 3.4.0.0

Destination Port Characteristics:
Well know ports < 1024. Telnet, FTP, SSH, DNS tcp-53

Log excerpt:

```
Date      Time                 Source IP    Dest IP   Sport Dport

5Mar2000; 6:42:01;inbound;tcp;161.58.239.94;1.2.222.50;1934;ftp;
5Mar2000; 6:42:07;inbound;tcp;161.58.239.94;1.2.237.28;1055;ftp;
5Mar2000; 6:42:08;inbound;tcp;161.58.239.94;3.4.8.105;1295;ftp;
5Mar2000; 6:42:12;inbound;tcp;161.58.239.94;1.2.222.50;1934;telnet;
5Mar2000; 6:42:14;inbound;tcp;161.58.239.94;1.2.237.28;1055;SSH-22;
5Mar2000; 6:42:17;inbound;tcp;161.58.239.94;3.4.23.83;1440;ftp;
5Mar2000; 6:42:21;inbound;tcp;161.58.239.94;1.2.237.28;1055;telnet;
5Mar2000; 6:42:29;inbound;tcp;161.58.239.94;1.2.13.66;1934;ftp;
5Mar2000; 6:42:38;inbound;tcp;161.58.239.94;1.2.28.44;1055;ftp;
...
...a few weeks later more...
...
19Mar2000;11:31:50;inbound;tcp;161.58.239.94;3.4.3.24;1295;ftp;
19Mar2000;11:32:06;inbound;tcp;161.58.239.94;3.4.18.2;1440;ftp;
19Mar2000;11:32:25;inbound;tcp;161.58.239.94;1.2.49.54;1055;domain-tcp;
19Mar2000;11:32:25;inbound;tcp;161.58.239.94;1.2.8.113;1934;ftp;
19Mar2000;11:32:26;inbound;tcp;161.58.239.94;3.4.76.2;1295;domain-tcp;
19Mar2000;11:32:29;inbound;tcp;161.58.239.94;1.2.2.39;1055;telnet;
```

Total of 13950 log entries.

Joseph S. Dietz, Jr.

Detect 10: Network mapping Deep Throat-like ports using UDP.

Detect Tool:
Firewall-1 logs with home grown perl scripts to summarize the daily detects. Logs are summarized every twenty-four hours.
Probes

```
      of 25 hits or more are reported in the daily summary.  The
        daily summaries are manually reviewed.  Additional
investigation and
        analysis is completed manually as necessary.  Only dropped
packets
        are logged.  It is not guaranteed that every dropped packet
      will be logged.

Detect Details:
      This probe was detected because of the high number of hits from
      the source address.  The source and destination port do not
change.
      Deep Throat has been found to run on TCP ports 2140 and 60000.
      It is interesting that this probe uses these same port numbers
via
UDP.

Time:
      This was a fast scan.  It took place in one minute.

Source IP Characteristics:
      Static 213.46.18.151 DNS reverse lookup d18151.dtk.chello.nl

Source Port Characteristics:
      Static UDP 2140

Destination IP Characteristics:
      1.2.0.0 is one of our class-B addresses
      Increments through one segment 1.2.0.1 - 1.2.0.255

Destination Port Characteristics:
      Static UDP 60000

Log excerpt:

Date      Time                Source IP     Dest IP Sport Dport

16Mar2000; 4:08:10;inbound;udp;213.46.18.151;1.2.0.1;2140;60000;
16Mar2000; 4:08:10;inbound;udp;213.46.18.151;1.2.0.2;2140;60000;
16Mar2000; 4:08:10;inbound;udp;213.46.18.151;1.2.0.3;2140;60000;
16Mar2000; 4:08:10;inbound;udp;213.46.18.151;1.2.0.4;2140;60000;
16Mar2000; 4:08:10;inbound;udp;213.46.18.151;1.2.0.5;2140;60000;
16Mar2000; 4:08:10;inbound;udp;213.46.18.151;1.2.0.6;2140;60000;
...
16Mar2000; 4:08:32;inbound;udp;213.46.18.151;1.2.0.250;2140;60000;
16Mar2000; 4:08:32;inbound;udp;213.46.18.151;1.2.0.251;2140;60000;
16Mar2000; 4:08:32;inbound;udp;213.46.18.151;1.2.0.252;2140;60000;
16Mar2000; 4:08:32;inbound;udp;213.46.18.151;1.2.0.253;2140;60000;
16Mar2000; 4:08:32;inbound;udp;213.46.18.151;1.2.0.254;2140;60000;
16Mar2000; 4:08:32;inbound;udp;213.46.18.151;1.2.0.255;2140;60000;

Total of 255 log entries.
```

Last Updated: April 21st, 2018

Upcoming Training

SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201805,	May 02, 2018 - Jun 14, 2018	vLive
Community SANS Virginia Beach SEC503	Virginia Beach, VA	May 07, 2018 - May 12, 2018	Community SANS
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
Mentor Session - SEC503	Houston, TX	Jun 18, 2018 - Jul 18, 2018	Mentor
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Minneapolis 2018 - SEC503: Intrusion Detection In-Depth	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LA	Jul 30, 2018 - Aug 06, 2018	Live Event
San Antonio 2018 - SEC503: Intrusion Detection In-Depth	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS London September 2018	London, United Kingdom	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NV	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS Brussels October 2018	Brussels, Belgium	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Northern VA Fall- Tysons 2018	Tysons, VA	Oct 13, 2018 - Oct 20, 2018	Live Event
SANS Denver 2018	Denver, CO	Oct 15, 2018 - Oct 20, 2018	Live Event
SANS October Singapore 2018	Singapore, Singapore	Oct 15, 2018 - Oct 28, 2018	Live Event
Mentor Session - SEC503	Ballston, VA	Nov 01, 2018 - Dec 06, 2018	Mentor
SANS Dallas Fall 2018	Dallas, TX	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS San Diego Fall 2018	San Diego, CA	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Stockholm 2018	Stockholm, Sweden	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced