Global Information Assurance Certification Paper

*** Northcutt, I like the work on detect 4! Nice use of an analysis process. Be sure and let us know the final resolution on detect 6 :) 90 ***

10 Detects for SANS GIAC Intrusion Analyst Certification
Robert Hunt
April 4, 2000

General Information:
We have a Class B network. Our network gateway to the internet is protected by a Gauntlet Firewall. We also have a Gauntlet Firewall for our extranet gateway (multiple frame relay connections to vendors/partners). Our DMZ (in the original sense, between internet firewall and ISP) gateway is protected by a CISCO router, which contains many of the ACL filters that have been discussed. We will be working to tighten it further.

Detect #1:
1 0.00000 ext-netbios.com -> int-ntdomain.com UDP D=137 S=137 LEN=76
2 1.50103 ext-netbios.com -> int-ntdomain.com UDP D=137 S=137 LEN=76
3 1.50226 ext-netbios.com -> int-ntdomain.com UDP D=137 S=137 LEN=76
4 0.00010 ext-firewall -> ext-netbios.com ICMP Destination unreachable (Bad port)

Type of detect:
Extranet Firewall Snoop output

Active targeting: yes

Intent:
NETBIOS communication from vendor NT workstation to Internal NT domain server

Technique:
ext-netbios.com => External NT box at one of our vendor locations
int-ntdomain.com => Internal NT Domain Server
Attempt to establish NETBIOS session, from UDP port 137 to UDP port 137.

History of detect:
These connection attempts have been occurring since our frame relay connection was established with this particular vendor.

Conclusion:
External NT box is attempting to connect to our Internal NT Domain Server on Netbios port 137.
Firewall return ICMP error, bad port. It does not appear to be a brute force attack of any sort, but rather a configuration issue on the NT box. Contacted administrator and verified this as a configuration issue. Will continue monitoring to ensure configuration fix.

INFOCON status: green

Detect #2:
Mar 29 15:29:08 firewall.com unix: securityalert: tcp if=hme2 from 10.10.12
0.52:2861 to 192.168.110.62 on unserved port 53
Mar 29 15:29:08 firewall.com unix: securityalert: tcp if=hme2 from 10.10.12
0.52:2862 to 192.168.110.62 on unserved port 53
Mar 29 15:29:08 firewall.com unix: securityalert: tcp if=hme2 from 10.10.12
0.52:2866 to 192.168.110.62 on unserved port 53
Mar 29 15:29:09 firewall.com unix: securityalert: tcp if=hme2 from 10.10.12
0.52:2870 to 192.168.110.62 on unserved port 53

Mar 29 15:29:09 firewall.com unix: securityalert: tcp if=hme2 from 10.10.12
0.52:2871 to 192.168.110.62 on unserved port 53
Mar 29 15:29:09 firewall.com unix: securityalert: tcp if=hme2 from 10.10.12
0.52:2875 to 192.168.110.62 on unserved port 53

Type of detect:
Extranet Firewall log

Active targeting: yes

Intent:
DNS zone transfer

Technique:
192.168.110.62 is an internal DNS server
10.10.120.52 is a DNS server at a company that we have an extranet connection with
10.10.120.52 attempts to connect with internal DNS server via TCP port 53. Does not appear to be brute force type attack, but rather occasional requests.

History of detect:
10.10.120.52 attempts TCP port 53 connections to our internal DNS server regularly, as far back as our logs go.

Conclusion:
Does not appear to be malicious, but more likely a misconfiguration. Follow-up work with vendor to re-configure DNS resolution for this device.

INFOCON status: green

Detect #3:
Mar 30 15:31:05 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.98.29
Mar 30 15:33:09 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.96.101
Mar 30 15:35:06 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.73.75
Mar 30 15:39:53 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.90.20
Mar 30 15:41:00 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.164.49
Mar 30 15:52:27 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.127.43
Mar 30 16:06:06 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.34.50
Mar 30 16:07:17 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.135.47
Mar 30 16:11:39 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.173.57
Mar 30 16:13:56 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.122.53
Mar 30 16:33:58 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.229.48
Mar 30 16:47:12 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=24.26.145.251 dstaddr=192.168.76.120

Type of detect:
Internet Firewall log

Active targeting: yes

Intent:
Information gathering, possibly for a future attack

Technique:
192.168 addresses are various internal addresses
24.26.145.251 appears to belong to Time Warner, but may be spoofed
Slow ICMP scan from a static source to apparently random internal addresses
It is possibly scanning other networks in the time between hits on our address space.

History of detect:
This particular scan just started.

Conclusion:
Slow scan would probably not be detected by most IDS'. Keep monitoring logs for other related activity.
Configure IDS to gather hits by this source.

INFOCON status: yellow

Detect #4:

```
192.168.108.35 -> 149.1.1.1    IP  D=149.1.1.1 S=192.168.108.35 LEN=28, ID=38888
  149.1.1.1 -> 192.168.108.35 IP  D=192.168.108.35 S=149.1.1.1 LEN=28, ID=55190
192.168.108.35 -> 149.1.1.1    IP  D=149.1.1.1 S=192.168.108.35 LEN=28, ID=39144
  149.1.1.1 -> 192.168.108.35 IP  D=192.168.108.35 S=149.1.1.1 LEN=28, ID=49827
192.168.51.182 -> 149.1.1.1    IP  D=149.1.1.1 S=192.168.51.182 LEN=28, ID=5138
  149.1.1.1 -> 192.168.51.182 IP  D=192.168.51.182 S=149.1.1.1 LEN=28, ID=26362
192.168.51.182 -> 149.1.1.1    IP  D=149.1.1.1 S=192.168.51.182 LEN=28, ID=5394
  149.1.1.1 -> 192.168.51.182 IP  D=192.168.51.182 S=149.1.1.1 LEN=28, ID=30726
```

Type of detect:
Internet Firewall Snoop

Active targeting: yes

Intent:
Information gathering by Internet marketing company

Technique:
192.168 addresses are internal
149.1.1.1 is owned by PSInet (ISP)
Owners of the internal addresses are not intentionally sending ICMP requests to 149.1.1.1
From doing machine scans of each internal machine that matches this detect I find that each contains PKZIP for windows. Visiting the PKWARE website there is an FAQ which describes a function in their shareware version of PKZIP for windows. This function will apparently attempt to connect back to a sponsoring website to provide information using tsadbot.exe, an info gathering tool. I believe this ICMP traffic is said connection.

History of detect:
Various internal addresses, as far back as our detects go.

Conclusion:

Does not appear to be malicious. Is a software control issue, internally. Have asked that users not install shareware version of this software. Have written network logon script that will detect and remove the executable from the users system. Will continue to monitor for related traffic.

INFOCON status: yellow

Detect #5:
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:37 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:38 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:38 PingFlood 192.168.51.26 192.168.135.15 Echo Request
3/8/00 22:29:38 PingFlood 192.168.51.26 192.168.135.15 Echo Request

Type of detect:
ISS Real Secure engine, inside our Internet firewall

Active targeting: yes

Intent:
ICMP echo attempt between two internal addresses

Technique:
The 192.168.51.26 address is one of our internal hosts.
The 192.168.135 network is within our address space, but isn't used.
192.168.51.26 is attempting to ping an address that does not exist.

History of detect:
This is a new detect for this address, but similar detects have been identified in the past.

Conclusion:
Our internal routers are attempting to send these ICMP packets out to our default gateway (Internet Firewall), since the network doesn't exist. The Internet Firewall routes the ICMP packets back inbound, as it knows this network is a part of our internal address space.
A routing loop is causing us to flood ourselves. This is a problem with our current version of RIP. Network operations is aware of issue and working to resolve.

INFOCON status: yellow for Network operations, until issue resolved

Detect #6:
1916 3/9/00 12:23:12 IPUnknownProtocol 54 192.168.84.202 192.168.1.10
1917 3/9/00 12:35:28 IPUnknownProtocol 54 192.168.84.202 192.168.1.10

1918 3/9/00 12:44:26 IPUnknownProtocol 54 192.168.84.202 192.168.1.10
1919 3/9/00 12:55:02 IPUnknownProtocol 54 192.168.84.202 192.168.1.10
1920 3/9/00 13:05:46 IPUnknownProtocol 54 192.168.84.202 192.168.1.10
1922 3/9/00 13:19:00 IPUnknownProtocol 54 192.168.84.202 192.168.1.10

Type of detect:
ISS Real Secure engine, inside Internet firewall

Active targeting: yes

Intent:
Protocol 54 (NBMA Address Resolution Protocol) communication

Technique:
192.168.84.202 is an internal NT workstation
192.168.1.10 is the inside interface of our Internet Firewall
Protocol 54 is NARP (NBMA Address Resolution Protocol). This is a non-broadcast routing protocol. NARP is a non-standard routing protocol within our network.

Conclusion:
192.168.84.202 is misconfigured so that it is using this unsupported routing protocol. This routing protocol is used with cable modem connections, among other things. Have located source, and will look into the reason for and nature of misconfiguration.

INFOCON status: yellow, until questions answered

Detect #7:
Mar 31 14:19:44 ext-firewall.com unix: securityalert: udp if=hme3 from 192.168.10
3.21:137 to 192.168.103.255 on unserved port 137
Mar 31 14:19:44 ext-firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=hme3 srcaddr=192.168.1.3 dstaddr=192.168.103.21
Mar 31 14:19:44 ext-firewall.com unix: securityalert: udp if=hme3 from 192.168.10
3.21:137 to 192.168.103.255 on unserved port 137
Mar 31 14:19:44 ext-firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=hme3 srcaddr=192.168.1.3 dstaddr=192.168.103.21
Mar 31 14:19:45 ext-firewall.com unix: securityalert: udp if=hme3 from 192.168.10
3.21:137 to 192.168.103.255 on unserved port 137
Mar 31 14:19:45 ext-firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=hme3 srcaddr=192.168.1.3 dstaddr=192.168.103.21
Mar 31 14:19:49 ext-firewall.com unix: securityalert: udp if=hme3 from 192.168.10
3.21:137 to 192.168.103.255 on unserved port 137
Mar 31 14:19:49 ext-firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=hme3 srcaddr=192.168.1.3 dstaddr=192.168.103.21
Mar 31 14:19:49 ext-firewall.com unix: securityalert: udp if=hme3 from 192.168.10
3.21:137 to 192.168.103.255 on unserved port 137
Mar 31 14:19:49 ext-firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=hme3 srcaddr=192.168.1.3 dstaddr=192.168.103.21

Type of detect:
Extranet Firewall log

Active targeting: yes

Intent:
Internal netbios connection. 'Normal' day-to-day NT operation

Technique:
192.168.1.3 is the internal address of our Extranet firewall
192.168.103.21 is an internal NT workstation
Attempt NETBIOS connection from 192.168.103.21 to its own network broadcast 192.168.103.255

History of detect:
New connection event.

Conclusion:
Internal routing configuration believes 192.168.103 network is outside our network,
by way of the Extranet firewall
Extranet firewall believes the 192.168.103 network is inside our network
192.168.103.21 attempts to initiate a NETBIOS connection via port 137 to its 192.168.103.255
broadcast address. This traffic is delivered to the inside of our Extranet firewall.
The Extranet firewall will not allow traffic on port 137.
An ICMP message is generated and sent back to 192.168.103.21, but is just as soon routed back
to the extranet firewall (remember the routing loop).
The Extranet firewall receives the packet, which is sourced as itself.
The firewall generates a 'securityalert' log as he believes someone is spoofing the source of the packet.
The actual culprit is misconfigured routing causing a loop between the internal routers and the
extranet firewall.

INFOCON status: yellow, in our network operations center

Detect #8:
Mar 27 02:13:21 firewall.com tn-gw[22157]: permit host=nodnsquery/192.168.35.
215 destination=206.11.147.6 port=23
Mar 27 02:13:22 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=206.11.147.6 dstaddr=192.168.35.215
Mar 27 02:13:22 firewall.com tn-gw[22157]: connected host=nodnsquery/192.168.
35.215 destination=206.11.147.6 port=23
Mar 27 02:13:22 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=206.11.147.6 dstaddr=192.168.35.215
Mar 27 02:13:29 firewall.com tn-gw[22157]: exit host=nodnsquery/192.168.35.21
5 dest=206.11.147.6 in=1913 out=2273 user=unauth duration=8
Mar 27 02:13:29 firewall.com tn-gw[22228]: permit host=nodnsquery/192.168.35.
214 destination=206.11.147.6 port=23
Mar 27 02:13:30 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=206.11.147.6 dstaddr=192.168.35.214
Mar 27 02:13:30 firewall.com tn-gw[22228]: connected host=nodnsquery/192.168.
35.214 destination=206.11.147.6 port=23
Mar 27 02:13:30 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=206.11.147.6 dstaddr=192.168.35.214
Mar 27 02:13:43 firewall.com tn-gw[22228]: exit host=nodnsquery/192.168.35.21
4 dest=206.11.147.6 in=1913 out=2273 user=unauth duration=14

Type of detect:
Internet Firewall log

Active targeting: yes

Intent:

Information gathering. Probably an attempt to actively monitor network connectivity.

Technique:
192.168.35.214 and 215 are servers on our internal network
206.11.147.6 is an external address
Users on 192.168.35.214 and 215 are telneting to 206.11.147.6.
When this connection is made ICMP requests are made back to the originating host.
The ICMP request is automated and transparent to user, as it is immediate every time.

History of detect:
Similar detects date back a month.

Conclusion:
When user connects to external server, an automated ICMP process is initiated. This is probably a tool to monitor the connection (hops, latency, status, etc...). Does not appear to be malicious, but have contacted user department to determine the source of this. ICMP traffic is denied.

INFOCON status: yellow until we hear back from user department

Detect #9:
Mar 30 15:04:53 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.181.0
Mar 30 15:05:33 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.216.0
Mar 30 15:05:35 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.123.0
Mar 30 15:05:42 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.102.0
Mar 30 15:06:03 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.20.0
Mar 30 15:06:13 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.11.0
Mar 30 15:06:20 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.131.0
Mar 30 15:06:45 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.64.0
Mar 30 15:06:58 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.49.0
Mar 30 15:07:50 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.95.0
Mar 30 15:07:51 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.97.0
Mar 30 15:08:03 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.116.0
Mar 30 15:08:18 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.84.0
Mar 30 15:08:23 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.75.0
Mar 30 15:08:33 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.13.0
Mar 30 15:08:37 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.70.0
Mar 30 15:09:06 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=137.65.119.175 dstaddr=192.168.74.0

Type of detect:
Internet Firewall log

Active targeting: yes

Intent:
DOS Smurf attack or aggressive information gathering

Technique:
192.168 networks are all within our internal address range
137.65.119.175 is an external address, possibly spoofed
137.65.119.175 is performing ICMP scan on our network
It seems to be systematically scanning through our class B address range,
using the BSD zero broadcast form.

History of detect:
This is a new detect.

Conclusion:
If the source address is spoofed, then it is most likely a Smurf attack. The replies
to the ICMPs would be a denial of service against the spoofed source.
If the source address is not spoofed, then it is most likely an example of
aggressive mapping of our network. Continued and heightened monitoring of similar activity.

INFOCON status: Yellow to orange, depending on additional information

Detect #10:
Mar 27 16:17:55 firewall.com http-gw[19254]: permit host=nodnsquery/192.168.9
3.77 use of proxy
Mar 27 16:17:55 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=206.132.152.250 dstaddr=192.168.93.77
Mar 27 16:17:55 firewall.com http-gw[19250]: exit host=nodnsquery/192.168.93.
77 cmds=1 in=1488 out=0 user=unauth duration=0
Mar 27 16:17:59 firewall.com http-gw[19254]: exit host=nodnsquery/192.168.93.
77 cmds=1 in=5766 out=0 user=unauth duration=4
Mar 27 16:18:00 firewall.com unix: securityalert: packet denied by forward s
creen: ICMP if=qfe0 srcaddr=209.249.123.189 dstaddr=192.168.93.77
Mar 27 16:18:00 firewall.com http-gw[19385]: log host=nodnsquery/192.168.93.7
7 protocol=HTTP cmd=get dest=209.249.123.189 path=/7/840/614/64d63e00450765/www.
goto.com/images/earthlink/arr.gif

Type of detect:
Internet Firewall log

Active targeting: yes

Intent:
Information gathering attempt. Trying to determine location, etc… about user to direct traffic to a more appropriate server

Techniques:
192.168.93.77 is an internal NT workstation
206.132.152.250 and 209.249.123.189 appear to be Akamai servers (web balancing/redirection)
192.168.93.77 connects to external website which uses Akamai for website balancing/redirection.
Akamai server attempts to connect back to 192.168.93.77 to determine location, etc...

History of detect:
192.168.93.77 has many similar exchanges throughout the day, everyday with many different web servers. Each of the web servers in question appear to be tied to Akamai

Conclusion:
Does not appear to be malicious. Firewall blocks the ICMP traffic. No further action required.

Infocon status: green