Global Information Assurance Certification Paper

SANS2000 Certification Practical
David Graham

Detect 1

Mar 15 09:21:33 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.48/111
Mar 15 16:05:22 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.49/111
Mar 16 07:00:09 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.50/111
Mar 17 08:07:43 firewall %PIX-2-106001: Inbound TCP connection denied from 210.240.55.2/53 to aaa.aaa.aaa.52/111 flags SYN
Mar 17 15:37:56 firewall %PIX-2-106001: Inbound TCP connection denied from 210.240.55.2/53 to aaa.aaa.aaa.53/111 flags SYN
Mar 18 02:46:53 firewall %PIX-2-106001: Inbound TCP connection denied from 210.240.55.2/53 to aaa.aaa.aaa.54/111 flags SYN
Mar 18 09:45:41 firewall %PIX-2-106001: Inbound TCP connection denied from 210.240.55.2/53 to aaa.aaa.aaa.55/111 flags SYN
Mar 18 16:13:14 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.56/111
Mar 18 22:45:26 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.57/111
Mar 19 06:44:10 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.58/111
Mar 19 13:25:10 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.59/111
Mar 20 03:59:05 firewall %PIX-2-106001: Inbound TCP connection denied from 210.240.55.2/53 to aaa.aaa.aaa.60/111 flags SYN
Mar 20 12:52:53 firewall %PIX-2-106001: Inbound TCP connection denied from 210.240.55.2/53 to aaa.aaa.aaa.61/111 flags SYN
Mar 21 01:36:14 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.62/111
Mar 21 10:59:04 firewall %PIX-3-106010: Deny inbound tcp src outside:210.240.55.2/53 dst inside:aaa.aaa.aaa.63/111

1. Source of trace:
   - my network
2. Detect was generated by:
   - Cisco PIX firewall version 5.0.3
   - Explanation of fields using the first message: **timestamp(**Mar 15 09:21:33**) firewall**

name(firewall**) PIX message severity and number(**%PIX-3-106010**): firewall action(**Deny inbound tcp**) source interface:ip/port(**src outside:210.240.55.2/53**) destination interface (**dst inside:aaa.aaa.aaa.48/111**).**

- PIX message 106001 is generated when the IP address is in use by an active host and no active connection exists.
- PIX message 106010 is generated when the address is not in use, or is used as a gateway or network/broadcast address.
- PIX message format varies depending on message type, for an in-depth explanation of all PIX message types please look at: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/pix55em/index.htm
- In order to find patterns in the firewall logs, I have created a tool that parses PIX logs and sends the output to a MYSQL database. It's very alpha right now, but you can find it at http://www.infosecworks.com/pixalyze

3. Probability the source address was spoofed:
   - Low - The attacker is looking for open ports and needs to see the targets' response. Also, the firewall did not record a source route attempt.
4. Description of attack:
   - This is a slow portmap scan using source port 53 from a DNS server. The scan occurs at random times and takes six days to cover a /28 subnet.
5. Attack mechanism:
   - Portmapper (and the services it facilitates) has been the subject of numerous buffer overflow exploits. The target systems are misconfigured or unmaintained Unix systems. Also note the attacker is using source port 53 from a (likely) compromised dns server and scanning very slowly to avoid detection.
6. Correlations:
   - I have not seen any other packets from this host although TCP port 111 scans are quite common.
7. Evidence of active targeting:
   - Minimal - It appears to be an interleaved scan from a compromised DNS server on one Exodus network to another.
8. Severity:
   - (Critical + Lethal) - (System + Net Countermeasures) = Severity
   - (5 + 5) - (5 + 5) = 0
9. Defensive recommendation:
   - Make sure all systems are patched. If possible, disable portmap and/or block port 111 at the firewall.
10. Multiple choice question:
    - In the above detect, messages that include TCP flags indicate what?

- a) hosts running portmapper
- b) hosts not running portmapper
- c) active hosts
- d) inactive hosts
- Answer c) active hosts

Detect 2

Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.192/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.193/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.194/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.195/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.196/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.197/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.198/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.199/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.200/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.201/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.202/161
.
<sequential lines deleted>
.
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.219/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.220/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.221/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.222/161
Apr 27 15:40:42 firewall %PIX-2-106006: Deny inbound UDP from 64.244.43.65/2740 to ccc.ccc.ccc.223/161

1. Source of trace:

- my network

2. Detect was generated by:
   - Cisco PIX firewall version 5.0.3
   - Explanation of fields using the first message: **timestamp(**Apr 27 15:40:42**) firewall name(**firewall**) PIX message severity and number(**%PIX-2-106006**): firewall action(**Deny inbound UDP**) source ip/port(**from 64.244.43.65/2740**) destination IP/port(**to ccc.ccc.ccc.192/161**).**
3. Probability the source address was spoofed:
   - Low - Although the attack occurred very quickly (34 packets recorded in a 1 sec window by syslog), it appears to be a scan looking for SNMP daemons. The attacker would need to see the response from the target and there is no evidence of source routing.
4. Description of attack:
   - An attempt to find SNMP daemons (UDP port 161). Notice the source port of 2740 does not change, indicating a forged packet.
5. Attack mechanism:
   - Most SNMP implementations use a very weak authentication mechanism called community strings. Many SNMP enabled devices ship with the SNMP daemon running and using well know community strings by default. If an attacker can find one of these devices, it may be possible to interrupt connectivity or even compromise a server.
6. Correlations:
   - Five days after this scan, the firewall logged an identical scan from the same network using the same source port (2740).
7. Evidence of active targeting:
   - Possibly - Of the hundreds of scans I have seen on this network, I've never seen someone come back twice from the same originating network.
8. Severity:
   - (5 + 4) - (5 + 5) = -1
9. Defensive recommendation:
   - The only SNMP traffic allowed to leave the network does so over IPSec tunnels. Only read-only capability is used with ACLs and random community strings on all devices.
10. Multiple choice question:
    - Which UDP port are SNMP traps sent to?
    - a) 161
    - b) 111
    - c) 160
    - d) 162
    - Answer: d) 162

Detect 3

Feb 17 22:51:06 firewall %PIX-2-106012: Deny IP from aaa.aaa.aaa.58 to bbb.bbb.bbb.235, IP options 0x72710d8
Feb 17 22:51:08 firewall last message repeated 2 times

1. Source of trace:
   - my network
2. Detect was generated by:
   - Cisco PIX firewall version 5.0.3.
   - Explanation of fields using the first message: **timestamp(**Feb 17 22:51:06**) firewall name(**firewall**) PIX message severity and type(**%PIX-2-106012**): firewall action(**Deny IP**) source ip(**from aaa.aaa.aaa.58**) destination ip(**to bbb.bbb.bbb.235**), IP options(**IP options 0x72710d8**).**
3. Probability the source address was spoofed:
   - High - Both networks are behind the firewall and the firewall denied the packets on the outside interface.
4. Description of attack:
   - The attacker tried spoofing an unused IP from an internal network and set the record route IP option.
5. Attack mechanism:
   - There are two networks behind the firewall (aaa.aaa.aaa.48/28 and bbb.bbb.bbb.228/28). The attacker tried to spoof an unused IP address from one of the internal networks in hopes it would bypass the firewall acls. The host that the attacker is targeting is a very critical system. The record route option causes each gateway device (router) to add it's IP address to the IP options field. It is not used very often, because of the 40 byte length limitation of the IP options field. It has largely been replaced by traceroute. I am not aware of any attacks which use the record route option. This may be a very odd attempt at network mapping.
6. Correlations:
   - None, unfortunately. This is one situation where the PIXs' logging capability proves very inadequate. Needless to say, an IDS which captures the entire packet would have helped considerably here.
7. Evidence of active targeting:
   - High - Only four packets are seen and they are destined to a critical system. I could not find any evidence of reconnaissance, but due to the fact that the subnet is very small and we use an unfortunate "naming standard," the critical system could be identified quickly.
8. Severity:
   - (5 + 1) - (5 + 5) = -2
9. Defensive recommendation:

- Due to it's critical nature, the system in question is not allowed to talk directly to the outside world. It is monitored very closely, running only two network based services, and has all available patches installed. Ingress and Egress filtering is applied at the firewall. Also, an IDS system has been put in place since this occurred.

10. Multiple choice question:
    - What is the maximum number of IP addresses that can be stored in the Options field of an IP header?
    - a) 2
    - b) 9
    - c) 8
    - d) 255
    - Answer: b) 9

Detect 4

Mar 14 09:04:53 firewall %PIX-2-106001: Inbound TCP connection denied from 211.58.88.146/3733 to aaa.aaa.aaa.60/666 flags SYN
Mar 14 09:04:53 firewall %PIX-2-106001: Inbound TCP connection denied from 211.58.88.146/3735 to aaa.aaa.aaa.61/666 flags SYN
Mar 14 09:04:53 firewall %PIX-3-106010: Deny inbound tcp src outside:211.58.88.146/3722 dst inside:aaa.aaa.aaa.56/666
Mar 14 09:04:53 firewall %PIX-3-106010: Deny inbound tcp src outside:211.58.88.146/3729 dst inside:aaa.aaa.aaa.57/666
Mar 14 09:04:53 firewall %PIX-3-106010: Deny inbound tcp src outside:211.58.88.146/3730 dst inside:aaa.aaa.aaa.58/666
Mar 14 09:04:53 firewall %PIX-3-106010: Deny inbound tcp src outside:211.58.88.146/3732 dst inside:aaa.aaa.aaa.59/666
Mar 14 09:04:53 firewall %PIX-3-106010: Deny inbound tcp src outside:211.58.88.146/3738 dst inside:aaa.aaa.aaa.62/666
Mar 14 09:04:53 firewall %PIX-3-106010: Deny inbound tcp src outside:211.58.88.146/3739 dst inside:aaa.aaa.aaa.63/666

1. Source of trace:
    - my network
2. Detect was generated by:
    - Cisco PIX firewall version 5.0.3
3. Probability the source address was spoofed:
    - Low - The attacker is looking for open ports and needs to see the targets' response.
4. Description of attack:
    - This scan is looking for trojans on port 666.
5. Attack mechanism:

- This is a very fast scan looking for an open tcp port 666. This port is popular for trojan use due to it's symbolic nature.
- The video game doom also uses port 666. Although it is quite old, it is now making a small resurgence due to it's source code release and updating. We may see more "accidental" traffic on this port in the future.

6. Correlations:
   - About a half hour later, I received another scan from a different location. These two scans are the only port 666 scans I have seen in six months of data collection:

Mar 14 09:43:17 firewall %PIX-2-106001: Inbound TCP connection denied from 216.36.10.183/3633 to bbb.bbb.bbb.232/666 flags SYN
Mar 14 09:43:17 firewall %PIX-2-106001: Inbound TCP connection denied from 216.36.10.183/3634 to bbb.bbb.bbb.233/666 flags SYN
Mar 14 09:43:17 firewall %PIX-2-106001: Inbound TCP connection denied from 216.36.10.183/3635 to bbb.bbb.bbb.234/666 flags SYN
Mar 14 09:43:17 firewall %PIX-2-106001: Inbound TCP connection denied from 216.36.10.183/3637 to bbb.bbb.bbb.236/666 flags SYN
Mar 14 09:43:17 firewall %PIX-2-106001: Inbound TCP connection denied from 216.36.10.183/3638 to bbb.bbb.bbb.237/666 flags SYN
Mar 14 09:43:17 firewall %PIX-3-106010: Deny inbound tcp src outside:216.36.10.183/3640 dst inside:bbb.bbb.bbb.239/666

7. Evidence of active targeting:
   - medium - the full network range is not scanned on either network, but both active and non active IPs are targeted.
8. Severity:
   - (5 + 1) - (5 + 5) = -4
9. Defensive recommendation:
   - All patches are current and the firewall is blocking the probe.
10. Multiple choice question:
    - According to the IANA, what service has TCP and UDP port 666 been assigned to?
    - a) RPCbind
    - b) Doom
    - c) Satanz Backdoor
    - d) IMAPS
    - Answer: b) Doom

Detect 5

May 23 14:04:34 firewall %PIX-2-106016: Deny IP spoof from (aaa.aaa.aaa.54) to aaa.aaa.aaa.54
May 23 14:04:37 firewall last message repeated 3 times

May 23 14:04:43 firewall %PIX-2-106016: Deny IP spoof from (aaa.aaa.aaa.54) to aaa.aaa.aaa.54
May 23 14:04:55 firewall last message repeated 3 times

1. Source of trace:
   - my network
2. Detect was generated by:
   - Cisco PIX firewall version 5.0.3
3. Probability the source address was spoofed:
   - High - Source and destination ip are the same.
4. Description of attack:
   - Someone has crafted a packet that has the same source and destination ip. Eight packets were sent in total.
5. Attack mechanism:
   - This packet was sent to the "virtual IP" of a BigIP box. The BigIP attempts to maintain web site performance and availability by redirecting traffic from the virtual (aliased) IP on it's outside interface to one of many identically configured web servers on it's internal interface. Only eight packets were sent, so this is probably not a DOS attempt. The firewall has blocked it as it should, but unfortunately it blocked it based on the spoof attempt and did not record which protocol and/or ports are being targeted. The attack could be directed at our web site or the BigIP itself. There are also a number of TCP/IP stack implementations which are vulnerable to a DOS when given a packet with the same source and destination IP.
6. Correlations:
   - With the limited packet info it would be hard to correlate. No other anomalies were found around the time this attack was made.
7. Evidence of active targeting:
   - High - This is the "Virtual IP" of our main web site.
8. Severity:
   - (5 + 5) - (4 + 5) = 1
9. Defensive recommendation:
   - The BigIP system is current, as are our web servers. There are no "known" vulnerabilities in the application software for our web servers, but this is always a possibility. An IDS has been added and will aid in finding the intent of this attack in the future.
10. Multiple choice question:
    - Spoofed packets with the same source and destination address typically are used for what type of attack?
    - a) session hijack

- b) denial of service
- c) buffer overflow
- d) network mapping
- Answer b) denial of service

Detect 6

Feb 9 02:54:08 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:bbb.bbb.bbb.224/109
Feb 9 02:54:09 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:bbb.bbb.bbb.239/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.48/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.49/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.50/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.56/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.57/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.58/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.59/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.61/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.62/109
Feb 9 03:23:52 firewall %PIX-3-106010: Deny inbound tcp src outside:168.126.249.33/0 dst inside:aaa.aaa.aaa.63/109

1. Source of trace:
   - my network
2. Detect was generated by:
   - Pix firewall version 5.0.3
3. Probability the source address was spoofed:
   - Low - The attacker is looking for open ports and needs to see the targets' response.
4. Description of attack:
   - The attacker is scanning for active POP2 servers and using a source port of 0.
5. Attack mechanism:
   - POP2 is a mail retrieval protocol. There are a number of POP2 implementations that are

vulnerable to buffer overflows which may give local system access as the user "nobody" (on Unix). On a misconfigured or poorly implemented system it may even give administrative level access.

6. Correlations:
   - CVE: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0042
   - CVE: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0006
7. Evidence of active targeting:
   - Low - This scans my entire subnet, which is part of a large network block at a collocation provider.
8. Severity:
   - (5 + 2) - (5 + 5) = -3
9. Defensive recommendation:
   - Mail retrieval protocol implementations such as POP2, POP3, and IMAP have been the subject of numerous buffer overflow attempts. Make sure that your version is current and do not run the daemon as root.
10. Multiple choice question:
    - On a typical Unix system, a privileged user is one who?
    - a) has the username priv
    - b) has a uid of 0
    - c) is a member of the administrators group
    - d) has a gid of 0
    - Answer: b) has a uid of 0

Detect 7

```
 [**] IDS198/SYN FIN Scan [**]
05/29-06:51:29.870000 208.160.77.4:53 - ddd.ddd.ddd.168:53
TCP TTL:31 TOS:0x0 ID:39426
**SF**** Seq: 0x308CACE5   Ack: 0x54236B6B   Win: 0x404
00 00 00 00 00 00                          ......
[**] IDS198/SYN FIN Scan [**]
05/29-06:51:29.910000 208.160.77.4:53 - ddd.ddd.ddd.170:53
TCP TTL:31 TOS:0x0 ID:39426
**SF**** Seq: 0x308CACE5   Ack: 0x54236B6B   Win: 0x404
00 00 00 00 00 00                          ......
[**] IDS198/SYN FIN Scan [**]
05/29-06:51:29.930000 208.160.77.4:53 - ddd.ddd.ddd.171:53
TCP TTL:31 TOS:0x0 ID:39426
**SF**** Seq: 0x1EAC573D   Ack: 0x96B0FC0   Win: 0x404
```

00 00 00 00 00 00 ......

[**] IDS198/SYN FIN Scan [**]
05/29-06:51:29.950000 208.160.77.4:53 - ddd.ddd.ddd.172:53
TCP TTL:31 TOS:0x0 ID:39426
SF** Seq: 0x1EAC573D Ack: 0x96B0FC0 Win: 0x404
00 00 00 00 00 00 ......

[**] IDS198/SYN FIN Scan [**]
05/29-06:51:29.970000 208.160.77.4:53 - ddd.ddd.ddd.173:53
TCP TTL:31 TOS:0x0 ID:39426
SF** Seq: 0x1EAC573D Ack: 0x96B0FC0 Win: 0x404
00 00 00 00 00 00 ......

[**] IDS198/SYN FIN Scan [**]
05/29-06:51:30.010000 208.160.77.4:53 - ddd.ddd.ddd.175:53
TCP TTL:31 TOS:0x0 ID:39426
SF** Seq: 0x1EAC573D Ack: 0x96B0FC0 Win: 0x404
00 00 00 00 00 00 ......

1. Source of trace:
   - my network
2. Detect was generated by:
   - Snort IDS
   - Explanation of fields using the first message:
     snort ID and description([**] IDS198/SYN FIN Scan [**]**)**
     timestamp(05/29-06:51:29.870000**) source ip:port(**208.160.77.4:53**) - destination ip:port(**ddd.ddd.ddd.168:53**)**
     protocol(TCP**) time-to-live:value(**TTL:31**) type-of-service:value(**TOS:0x0**) IP identification number(**ID:39426**)**
     TCP flags(**SF******) TCP sequence number(**Seq: 0x308CACE5**) TCP acknowledgment number(**Ack: 0x54236B6B**) TCP window size(**Win: 0x404**)**
     data in hex format(00 00 00 00 00 00**) data in ASCII format(**.....**)**
3. Probability the source address was spoofed:
   - Low - The attacker needs to get the returned packet in order to find vulnerable servers.
4. Description of attack:
   - The attacker is scanning for active DNS servers using a crafted packet that has both the SYN and FIN TCP bits set.
5. Attack mechanism:
   - DNS has been a very popular exploit for quite some time. The most widely used implementation has not had a new exploit since it's last patch release in November of 1999, but many unpatched servers are still in use and continue to get exploited. Reference http://www.isc.org/products/BIND/bind-security-19991108.html for specific version information.
6. Correlations:

- CERT: http://www.cert.org/advisories/CA-2000-03.html

7. Evidence of active targeting:
   - Low - Scan covers my entire subnet.
8. Severity:
   - (5 + 5) - (5 + 5) = 0
9. Defensive recommendation:
   - Both of my name servers are running OpenBSD-current with the latest version of BIND, chrooted and running as a non privileged user. Although there is some debate, in most cases, running BIND chrooted reduces the chances of your entire system being compromised in the event that a buffer overflow does work.
10. Multiple choice question:
    - What substatement can you add to your BIND8 configuration file to control zone transfers?
    - a) allow-transfer
    - b) xfer-hosts
    - c) xfernets
    - d) zone-xfrhost
    - Answer: a) allow-transfer

Detect 8

Apr 13 15:33:35 firewall %PIX-3-106010: Deny inbound tcp src outside:62.26.3.15/9 dst inside:aaa.aaa.aaa.50/1783
Apr 13 15:34:33 firewall %PIX-3-106010: Deny inbound tcp src outside:62.26.3.15/79 dst inside:aaa.aaa.aaa.50/1783
Apr 13 15:35:27 firewall %PIX-3-106010: Deny inbound tcp src outside:62.26.3.15/23 dst inside:aaa.aaa.aaa.50/1783
Apr 13 15:36:00 firewall %PIX-3-106010: Deny inbound tcp src outside:62.26.3.15/53 dst inside:aaa.aaa.aaa.50/1783
Apr 13 15:36:37 firewall %PIX-3-106010: Deny inbound tcp src outside:62.26.3.15/143 dst inside:aaa.aaa.aaa.50/1783
Apr 13 15:39:59 firewall %PIX-3-106010: Deny inbound tcp src outside:62.26.3.15/7 dst inside:aaa.aaa.aaa.50/1783

1. Source of trace:
   - my network
2. Detect was generated by:
   - Cisco PIX firewall version 5.0.3
3. Probability the source address was spoofed:
   - Low - Although my address probably was.

4. Description of attack:
    - The attacker is using an inactive IP address on my network as the source address for scanning another network.
5. Attack mechanism:
    - This is part of a decoy scan, where multiple spoofed (inactive) source addresses are mixed in with the real source address. Due to the fact that the destination port on my network does not change and the probed ports are randomized I would guess that this scan was performed using nmap. You could recreate this signature by using: nmap -sS -Daaa.aaa.aaa.50 -p 7,9,23,53,79,143 62.26.3.15. In order to maximize the effectiveness of using a decoy scan, the attacker needs to use inactive IP addresses so the TCP reset is not sent back to the target. If the TCP reset is sent back, the odds of finding the real attacking host increase greatly.
6. Correlations:
    - The attacker must have done some previous reconnaissance to find that my IP address was unused.
7. Evidence of active targeting:
    - I would say the chances are low. The IP address in question has never been active and it fits very well into the definition of a decoy scan.
8. Severity:
    - (1 + 1) - (5 + 5) = -8
9. Defensive recommendation:
    - The PIX firewall has a feature to send resets for invalid connections, you can turn this on by adding "service resetinbound" to your config file. This will return resets for both active and inactive IP addresses. This will make mapping your network more difficult and aid others by not allowing your inactive IPs to be spoofed effectively. It also alleviates problems with the ident protocol.
10. Multiple choice question:
    - On Cisco PIX firewall version 5.0 and higher, what configuration command can you use to generate TCP resets for invalid connection attempts?
    - a) conduit deny tcp any any reset
    - b) fixup reset
    - c) floodguard enable
    - d) service resetinbound
    - Answer d) service resetinbound

Detect 9

Jan 29 16:26:25 firewall %PIX-3-106010: Deny inbound udp src outside:195.250.10.121/60000 dst inside:bbb.bbb.bbb.224/2140

Jan 29 16:26:25 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.225/2140
Jan 29 16:26:26 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.226/2140
Jan 29 16:26:26 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.227/2140
Jan 29 16:26:27 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.228/2140
Jan 29 16:26:27 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.229/2140
Jan 29 16:26:27 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.230/2140
Jan 29 16:26:27 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.231/2140
Jan 29 16:26:27 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.232/2140
Jan 29 16:26:27 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.233/2140
Jan 29 16:26:28 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.234/2140
Jan 29 16:26:28 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.235/2140
Jan 29 16:26:28 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.236/2140
Jan 29 16:26:28 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.237/2140
Jan 29 16:26:28 firewall %PIX-2-106006: Deny inbound UDP from 195.250.10.121/60000 to bbb.bbb.bbb.238/2140
Jan 29 16:26:29 firewall %PIX-3-106010: Deny inbound udp src outside:195.250.10.121/60000 dst inside:bbb.bbb.bbb.239/2140

1. Source of trace:
   - my network
2. Detect was generated by:
   - Cisco PIX firewall version 5.0.3
3. Probability the source address was spoofed:
   - Low - The attacker is looking for active trojans on port 2140.
4. Description of attack:
   - The attacker is scanning for UDP 2140 and using a static source port of 60000.
5. Attack mechanism:
   - This scan is looking probably looking for a Windows9x trojan known as Deep Throat. There is an excellent FAQ that covers Deep Throat on the SANS site: http://www.sans.org/newlook/resources/IDFAQ/DT.htm

6. Correlations:
    - A similar scan was reported to the GIAC (http://www.sans.org/y2k/012900.htm). No other packets have been seen from this host.
7. Evidence of active targeting:
    - Low - This scans my entire subnet, which is part of a large network block at a collocation provider.
8. Severity:
    - (5 + 1) - (5 + 5) = -4
9. Defensive recommendation:
    - The packets were blocked by the firewall and there are no Windows systems on this network.
10. Multiple choice question:
    - What popular messaging system does the Deep Throat server use?
    - a) Yahoo Messenger
    - b) AOL Instant Messenger
    - c) IRC
    - d) ICQ
    - Answer d) ICQ

Detect 10

Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.48 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.48 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47133 dst inside:aaa.aaa.aaa.48/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.49 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.49 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47134 dst inside:aaa.aaa.aaa.49/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.50 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.50 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47135 dst inside:aaa.aaa.aaa.50/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.51 (type 0, code 0)

Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.51 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-2-106006: Deny inbound UDP from 216.34.178.176/47136 to 216.34.178.51/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.52 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.52 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-2-106006: Deny inbound UDP from 216.34.178.176/47138 to 216.34.178.52/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.53 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.53 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-2-106006: Deny inbound UDP from 216.34.178.176/47139 to 216.34.178.53/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.54 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.54 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-2-106006: Deny inbound UDP from 216.34.178.176/47140 to 216.34.178.54/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.55 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.55 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-2-106006: Deny inbound UDP from 216.34.178.176/47141 to 216.34.178.55/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.56 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.56 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47142 dst inside:aaa.aaa.aaa.56/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.57 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.57 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47143 dst inside:aaa.aaa.aaa.57/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.58 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.58 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47144 dst inside:aaa.aaa.aaa.58/27444

Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.59 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.59 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47145 dst inside:aaa.aaa.aaa.59/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.60 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106014: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.60 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-2-106006: Deny inbound UDP from 216.34.178.176/47146 to 216.34.178.60/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.61 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.61 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47147 dst inside:aaa.aaa.aaa.61/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.62 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.62 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47148 dst inside:aaa.aaa.aaa.62/27444
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.63 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound icmp src outside:216.34.178.176 dst inside:aaa.aaa.aaa.63 (type 0, code 0)
Feb 10 14:51:11 216.34.178.49 %PIX-3-106010: Deny inbound udp src outside:216.34.178.176/47150 dst inside:aaa.aaa.aaa.63/27444

1. Source of trace:
   - my network
2. Detect was generated by:
   - Cisco PIX firewall version 5.0.3
3. Probability the source address was spoofed:
   - Low - Although the speed of the echo reply packets are similar to the second order effect of a smurf attack, it appears to be a reconnaissance scan.
4. Description of attack:
   - This is a reconnaissance scan which is sending two echo reply messages and one UDP port 27444 packet.
5. Attack mechanism:
   - The attacker is sending two echo reply messages to bypass the firewall rules and possibly avoid detection, a technique know as "Echo Reply Inverse Scan." This is a very useful

reconnaissance method because most firewalls allow echo replies through. The attacker is also sending a UDP port 2744 packet which is typically used by a trin00 broadcast node. Apparently the attacker is not trying to go stealth, instead he is doing rapid network mapping and looking for trin00 broadcast nodes while he's at it. For more information on trin00 reference:
http://www.sans.org/newlook/resources/IDFAQ/trinoo.htm

- The scan sent 48 packets in under one second and was performed from a host on a different subnet at the same collocation site.

6. Correlations:
   - There have been numerous reports of trin00 scans, although I did not find an identical scan (using two echo replies and a UDP port 27444) elsewhere.
7. Evidence of active targeting:
   - Low - This scans my entire subnet, which is part of a large network block at a collocation provider.
8. Severity:
   - (5 + 4) - (5 + 5) = -1
9. Defensive recommendation:
   - Although there has been much debate, I'm one of the lucky few who have gotten away with not allowing icmp echo requests or echo replies through the firewall. This makes network reconnaissance much more difficult.
10. Multiple choice question:
    - By default, what UDP port is commonly used by trin00 broadcast nodes?
    - a) 2140
    - b) 20710
    - c) 27444
    - d) 20666
    - Answer: c) 27444