Global Information Assurance Certification Paper

GIAC - GCIA Certification Practical

Phred Broughton

Detect 1

Dec 30 23:30:31 morannon named[415]: unapproved query from [207.222.133.11].1522 for "version.bind"
Dec 30 23:40:14 morannon named[415]: unapproved query from [129.137.151.25].3427 for "version.bind"
Dec 30 23:42:24 morannon named[415]: unapproved query from [209.35.116.194].1355 for "21.240.21.208.in-addr.arpa"
Dec 30 23:42:32 morannon named[415]: unapproved query from [209.35.116.194].1431 for "qoqo.sex.app.org"
Dec 30 23:47:08 morannon named[415]: unapproved query from [207.71.8.71].1446 for "version.bind"

1. Source of trace

http://www.sans.org/y2k/123199-1305.htm

2. Detect was generated by:

Syslog

3. Probability the source address was spoofed

Since reconnaisance would be the primary motive for this type of activity, the likelihood that all of these are spoofed is very low, however, it could be that only one is real and the others are just a smoke screen as all three requests for “version.bind” come from different networks within a 17 minute period.

4. Description of attack:

There are many known exploits against DNS. Older and unpatched versions of Bind were susceptible to various attacks from denial of service to root access compromise. Reconnaissance is the first step. Armed with the version and possibly the type of OS, the attacker can exploit the known weaknesses.

Name	Description
CVE-1999-0009	Inverse query buffer overflow in BIND 4.9 and BIND 8 Releases.
CVE-1999-0010	Denial of Service vulnerability in BIND 8 Releases via maliciously formatted DNS messages.
CVE-1999-0011	Denial of Service vulnerabilities in BIND 4.9 and BIND 8 Releases via CNAME record and zone transfer.
CVE-1999-0024	DNS cache poisoning via BIND, by predictable query IDs.
CVE-1999-0184	When compiled with the -DALLOW_UPDATES option, bind allows dynamic updates to the DNS server, allowing for malicious
CVE-1999-0189	Solaris rpcbind listens on a high numbered UDP port, which may not be filtered since the standard port number is 111.
CVE-1999-0190	Solaris rpcbind can be exploited to overwrite arbitrary files and gain root access.
CVE-1999-0312	HP ypbind allows attackers with root privileges to modify NIS data.
CVE-1999-0385	The LDAP bind function in Exchange 5.5 has a buffer overflow that allows a remote attacker to conduct a denial of service or
CVE-1999-0833	Buffer overflow in BIND 8.2 via NXT records.
CVE-1999-0835	Denial of service in BIND named via malformed SIG records.

CVE-1999-0837	Denial of service in BIND by improperly closing TCP sessions via so_linger.
CVE-1999-0848	Denial of service in BIND named via consuming more than "fdmax" file descriptors.
CVE-1999-0849	Denial of service in BIND named via maxdname.
CVE-1999-0851	Denial of service in BIND named via naptr.

5. Attack mechanism:

Once the version of bind and its vulnerabilities are known, the attacker can get to work. Typically after gaining access, they will remove all systems logs and install whatever tools are necessary to get complete administrative control of the host. Once in control, this host can be used to attack other hosts while helping to disguise the real attacker's identity.

6. Correlations:

http://www.sans.org/topten.htm

7. Evidence of active targeting:

Not able to determine from this trace if other hosts were involved.

8. Severity:

Criticality	5 DNS Server
Lethality	5 Can potentially gain root access
System Countermeasures	4 Trace would indicate that there are system countermeasures in place.
Network Countermeasures	4 Assuming that system is indicative of network countermeasures

(5 + 5) – (5 + 4) = 1

9. Defensive recommendation:

Defenses are fine, attack was blocked by countermeasures. Recommend review of system and network countermeasures. ….

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) DNS Zone Transfer
b) DNS Inverse Query
c) DNS Version Scan
d) DNS buffer overflow

answer: c

Detect 2

Server used for this query: [whois.apnic.net]
inetnum: 203.252.128.0 - 203.252.191.255
netname: KONKUNE
descr: Konkuk University
descr: 93 - 1 mojindong kwangjingu
descr: Seoul
country: KR
remarks: national isp
source: APNIC

```
Jul 31 01:00:46 hostre rpcbind:
  refused connect from 203.252.148.170 to dump()
Jul 31 01:00:46 hostbe rpcbind:
  refused connect from 203.252.148.170 to dump()
Jul 31 01:02:27 hostba rpcbind:
  refused connect from 203.252.148.170 to dump()
Jul 31 01:02:45 hostma snort[2517]: RPC Info Query:
  203.252.148.170:2430 -> z.y.v.28:111
--------
[**] RPC Info Query [**]
07/31-01:02:45.095951 203.252.148.170:2430 -> z.y.v.28:111
TCP TTL:48 TOS:0x0 ID:8557 DF
*****PA* Seq: 0x81DCE691 Ack: 0xA745CD25 Win: 0x7D78
80 00 00 28 4B BC 05 B7 00 00 00 00 00 00 00 02 ...(K...........
00 01 86 A0 00 00 00 02 00 00 00 04 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 ............
--------
Jul 31 01:03:59 hostma portsentry[148]: attackalert:
  Connect from host: 203.252.148.170/203.252.148.170
  to TCP port: 111
Jul 31 01:05:15 hostma portsentry[148]: attackalert:
  Connect from host: 203.252.148.170/203.252.148.170
  to TCP port: 111
```

1. Source of trace

http://www.sans.org/y2k/012800.htm

2. Detect was generated by:

Snort intrusion detection system and PortSentry.

3. Probability the source address was spoofed

Not likely as the purpose is reconnaissance

4. Description of attack:

Attempt to connect to rpc and issue a dump() command. This will provide the attacker with a complete listing of all running services and their ports.

5. Attack mechanism:

The attack works by connecting to the well known port 111 or portmapper. If successful, the attacker can request a dump() from the service which provides valuable information toward compromising the system. If successful, the attacker will be able to control this host and use it to launch attacks against other hosts.

6. Correlations:

Name	Description
CVE-1999-0168	The portmapper may act as a proxy and redirect service requests from an attacker, making the request appear to come from the

7. Evidence of active targeting:

Only information we have indicates one server being targeted, but unable to tell from supplied information.

8. Severity:

Criticality	4 We are not given any information as to the type of host or it's purpose, will assume critical.
Lethality	5 Potential root compromise and access to other hosts on the network.
System Countermeasures	4 Correlating traces would indicate healthy countermeasures
Network Countermeasures	4 Correlating traces would indicate healthy countermeasures

(4 + 5) – (4 + 4) = 1

9. Defensive recommendation:

Countermeasures appear to be doing their job. Report to CIRT and monitor.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

Which statement best describes the above traffic logs.

a) Normal traffic
b) DNS Query
c) Portmapper Attack
d) Bind buffer overflow

answer: c

Detect 3

Firewall Log
start_time="2000-8-5 15:17:09" src=my.prod.host.122 dst=216.33.210.40 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:17:57" src=my.prod.host.122 dst=216.33.210.41 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:17:12" src=my.prod.host.122 dst=216.33.210.40 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:17:17" src=my.prod.host.122 dst=216.33.210.40 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:17:30" src=my.prod.host.122 dst=216.33.210.40 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:17:53" src=my.prod.host.122 dst=216.33.210.41 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:18:39" src=my.prod.host.122 dst=216.35.217.25 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:18:42" src=my.prod.host.122 dst=216.35.217.25 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:20:09" src=my.prod.host.122 dst=216.35.217.27 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:20:12" src=my.prod.host.122 dst=216.35.217.27 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:20:18" src=my.prod.host.122 dst=216.35.217.27 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:20:30" src=my.prod.host.122 dst=216.35.217.27 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:20:54" src=my.prod.host.122 dst=216.35.217.28 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:20:57" src=my.prod.host.122 dst=216.35.217.28 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:21:39" src=my.prod.host.122 dst=216.35.217.29 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:21:42" src=my.prod.host.122 dst=216.35.217.29 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:23:09" src=my.prod.host.122 dst=216.33.199.80 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:23:12" src=my.prod.host.122 dst=216.33.199.80 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:23:18" src=my.prod.host.122 dst=216.33.199.80 src_port=1213 dst_port=17027 service=unknown policy_id=65
start_time="2000-8-5 15:23:30" src=my.prod.host.122 dst=216.33.199.80 src_port=1213 dst_port=17027 service=unknown policy_id=65

1. Source of trace

Our network.

2. Detect was generated by:

Firewall logs written to syslog server incorporating Email notification on filter match. Fields are identified within the log trace.

3. Probability the source address was spoofed

The address is not spoofed. It originates from our Atlanta center, which is routed through our Birmingham gateway for Internet access.

4. Description of attack:

Repeated attempts by an internal production host, to connect to an unknown port (17027). This host is not configured for, nor should it be attempting, access to the Internet. Not an attack, but disturbing behavior none the less.

(*Update: After reading today's postings to GIAC, I would have to revise my opinion that this is not a high risk.*

"Advertising banners produced by US software firm Conducent gather computer and network information by using a stealth application buried within the freeware program according to security newsletter, The Risk Digest. ")

5. Attack mechanism:

I have no way of knowing how long this has been occurring. We had not previously been capturing outbound traffic blocked by the firewall. When this first turned up I was concerned that it could be some type of Trojan or backdoor attempting to announce its location etc. There are several destination hosts with a distinct repeating pattern. Ran a search for inbound traffic from these destination hosts, but found none. Nslookup returned no names for these hosts. Emailed our support manager in Atlanta, provided the traces and had him investigate the machine. We determined that though they had purchased a license for the Win32 PKZip package that was installed, it had never been applied and was still running in unlicensed mode, which places banner ads in the window. We found a program named TSADBOT.exe in the "run" node of the registry. A quick search of PKZip's web page confirmed that this had indeed been installed with their package and would attempt to connect to servers managed by Conducent Technologies, Inc. http://www.pkware.com/support/tsadbotfaq.html I might add that although I detest this type of activity, it is clearly noted on their download page.

6. Correlations:

http://www.sans.org/y2k/081400.htm

http://www.zdnet.co.uk/news/1999/46/ns-11692.html

7. Evidence of active targeting:

Distinct pattern of destination host, but all outbound traffic.

8. Severity:

Criticality	3 This is one of our production machines
Lethality	"0 As long as this application behaves as it is stated"
	2 Revised due to 8/14/00 posting on GIAC http://www.sans.org/y2k/081400.htm
System Countermeasures	2 Company policies forbiding use of shareware or unlicensed software on a production host are obviously not being effectively enforced.
Network Countermeasures	5 All access to or from this host is blocked at the firewall.
(3 + 2) - (2 + 5) = -2	

9. Defensive recommendation:

Firewall policies are doing their job. We need to do a better job of enforcing company policy on shareware or unlicensed software, and conduct periodic scans of all host for violations of this policy. Installation of NT user policies to prevent software installation by unauthorized personnel might be a good long-term solution.

Implement Strict policy regarding any applications including banner ads. (AOL AIM?)

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

What is the most likely cause of the traffic indicated in the above trace?

a) Covert channel communication
b) Host scan by internal user
c) "Banner Ad" software attempting connection to outside host
d) Trojan scan by internal user

answer: c

Detect 4

inetnum: 194.105.56.0 - 194.105.57.47
netname: SIAINTERNET
descr: Sia Internet
descr: Internet Service Provider Company
country: LV
admin-c: AN1951-RIPE
tech-c: AV736-RIPE
status: ASSIGNED PI
notify: registry@telia.lv
mnt-by: RIPE-NCC-HM-PI-MNT
mnt-by: TELIALV-MNT
changed: hostmaster@ripe.net 19991221
changed: ica@telia.net 20000314
source: RIPE

194.105.56.7 > 208.35.39.5
11:13:14.081920 P 194.105.56.7.pop2 > mail01.mynet.com.pop2: SF 917184249:917184249(0) win 1028
11:13:14.101810 P 194.105.56.7.pop2 > ns01.mynet.com.pop2: SF 917184249:917184249(0) win 1028
11:13:14.204101 P 194.105.56.7.pop2 > ftp01.mynet.com.pop2: SF 917184249:917184249(0) win 1028
11:13:14.224447 P 194.105.56.7.pop2 > ftp02.mynet.com.pop2: SF 917184249:917184249(0) win 1028

1. Source of trace

Our network

2. Detect was generated by:

Shadow IDS system based on tcpdump.

3. Probability the source address was spoofed

Spoofing not likely as a scan of this type is worthless without the response packets.

4. Description of attack:

Host scan or OS reconnaissance using a most likely non-listening “pop2” service to solicit response and SYN-FIN flag combination to fingerprint OS or hoping to avoid detection. Notice constant initial sequence number. Another indicator of crafted packets. This could provide an important clue as to tool used. Also note “Low and Slow” nature. Only 4 packets sent that day. If I had not set my scan threshold to three, this would not have shown up in an hourly wrap up. Most active sites would have too high of a false positive rate to stay at this low number. I’m

glad things are still quiet enough around here to allow this! (Not likely it will stay that way)

5. Attack mechanism:

Many IDS systems match on the SYN flag to watch for connection attempts, but some older IDS systems and firewalls could miss this combination. This scan works by sending packets to a most likely "non-listening" port to solicit a response. Using the SYN-FIN combination could also be an attempt to fingerprint the OS as Linux systems that are not properly patched, would respond with a SYN-FIN-ACK. Particularly disturbing is the very targeted nature of this scan leading me to believe this is not his/her first visit. These hosts reside in a class "C" network, but no other addresses were targeted including our web servers. Subsequent log searches turned up no other traffic from this site on that day. OS knowledge about these servers would give the attacker important knowledge for planning an exploit.

6. Correlations:

SANS DC2000 Track 3.2 Intrusion Detection and Packet Filtering

7. Evidence of active targeting:

Very targeted. The only hosts attempted were our Email, DNS, and FTP servers.

8. Severity:

Criticality	5 Core servers
Lethality	2 Primarily reconnaissance but could provide necessary to launch an attack.
System Countermeasures	3 Not all latest patches and security updates applied!
Network Countermeasures	5 Strict firewall policies and IDS in place. Strong router ACL's

$(5 + 2) - (3 + 5) = -1$

9. Defensive recommendation:

Install all latest security and OS patches. Review firewall policies and router ACL's.

Since our IDS implementation is still in it's infancy, I don't have enough history to see what previous activity has come from this host. Added filter in Shadow system to trigger on this IP address so we can keep a close watch on them. We will continue to monitor and report any new attempts.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

Which statement best describes the above trace?

a) Scan for vulnerable “pop2” servers
b) Random host scan
c) Targeted reconnaissance
d) Incorrectly configured Email client

answer: c

Detect 5

nslookup 144.118.249.198
Canonical name: newtower2-565.resnet.drexel.edu
Addresses:
144.118.249.198

Trying 144.118.249 at ARIN
Drexel University (NET-DREXELSUBNET)
3141 Chestnut Street
Philadelphia, PA 19104
US
Netname: DREXELSUBNET
Netnumber: 144.118.0.0

Expr1
start_time="2000-8-13 01:24:55" src=144.118.249.198 dst=my.class_c.3 src_port=4742 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:24:57" src=144.118.249.198 dst=my.class_c.5 src_port=4744 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:24:59" src=144.118.249.198 dst=my.class_c.101 src_port=4841 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:24:59" src=144.118.249.198 dst=my.class_c.3 src_port=4742 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:25:00" src=144.118.249.198 dst=my.class_c.5 src_port=4744 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:25:00" src=144.118.249.198 dst=my.class_c.6 src_port=4745 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:25:00" src=144.118.249.198 dst=my.class_c.21 src_port=4760 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:25:00" src=144.118.249.198 dst=my.class_c.31 src_port=4770 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:25:06" src=144.118.249.198 dst=my.class_c.21 src_port=4760 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:25:06" src=144.118.249.198 dst=my.class_c.31 src_port=4770 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:25:06" src=144.118.249.198 dst=my.class_c.32 src_port=4771 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:25:06" src=144.118.249.198 dst=my.class_c.33 src_port=4772 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:24:57" src=144.118.249.198 dst=my.class_c.56 src_port=4750 dst_port=21 service=ftp policy_id=30 duration=1 sent=398 rcvd=306 action=Permit

start_time="2000-8-13 01:24:57" src=144.118.249.198 dst=my.class_c.50 src_port=4751 dst_port=21 service=ftp policy_id=32 duration=1 sent=334 rcvd=306 action=Permit
start_time="2000-8-13 01:24:57" src=144.118.249.198 dst=my.class_c.6 src_port=4745 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
start_time="2000-8-13 01:24:57" src=144.118.249.198 dst=my.class_c.21 src_port=4760 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:24:57" src=144.118.249.198 dst=my.class_c.31 src_port=4770 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:24:57" src=144.118.249.198 dst=my.class_c.32 src_port=4771 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:24:57" src=144.118.249.198 dst=my.class_c.33 src_port=4772 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:24:59" src=144.118.249.198 dst=my.class_c.100 src_port=4840 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:02" src=144.118.249.198 dst=my.class_c.100 src_port=4840 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:02" src=144.118.249.198 dst=my.class_c.101 src_port=4841 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:04" src=144.118.249.198 dst=my.class_c.128 src_port=4868 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:05" src=144.118.249.198 dst=my.class_c.3 src_port=4742 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:06" src=144.118.249.198 dst=my.class_c.5 src_port=4744 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:06" src=144.118.249.198 dst=my.class_c.6 src_port=4745 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:08" src=144.118.249.198 dst=my.class_c.100 src_port=4840 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:08" src=144.118.249.198 dst=my.class_c.101 src_port=4841 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 01:25:13" src=144.118.249.198 dst=my.class_c.128 src_port=4868 dst_port=21 service=ftp policy_id=61 duration=0 sent=0 rcvd=0 action=Deny
Start_time="2000-8-13 02:00:12" src=144.118.249.198 dst=my.class_c.56 src_port=1560 dst_port=21 service=ftp policy_id=30 duration=1 sent=334 rcvd=306 action=Permit
Start_time="2000-8-13 02:00:12" src=144.118.249.198 dst=my.class_c.50 src_port=1561 dst_port=21 service=ftp policy_id=32 duration=1 sent=334 rcvd=306 action=Permit

1. Source of trace

Our Network

2. Detect was generated by:

Firewall logging to syslog host.

3. Probability the source address was spoofed

None Trace shows established connections to 2 hosts. DNS name appears to represent a residential or dorm network.

4. Description of attack:

FTP scan of class “C” network. There are many known exploits of the FTP service. (Too many to list here) Unfortunately our IDS was off-line at the time this occurred and our firewall logs only indicate traffic to hosts that are configured for any type of inbound connection. Judging by the range of addresses and the speed of the scan, I feel safe in saying that our entire class “C” was scanned. Without IDS logs I cannot see the content of the packets that resulted in a completed connection, but notice the last 2 log entries. 35 minutes after the scan completed, the attacker returned to the 2 hosts that had responded in the scan. (Our 2 FTP hosts) Also notice that data was sent and received on each connection.

5. Attack mechanism:

Without proper logs with enough content to see what actually transpired, it is difficult to say if anything other than reconnaissance was accomplished. Here are some (certainly not all) possibilities if this attacker is able to find a known weakness.

Name	Description
CVE-1999-0777	IIS FTP servers may allow a remote attacker to read or delete files on the server, even if they have "No Access" permissions.
CVE-1999-0349	A buffer overflow in the FTP list (ls) command in IIS allows remote attackers to conduct a denial of service and, in some cases,
CVE-1999-0017	FTP servers can allow an attacker to connect to arbitrary ports on machines other than the FTP client, aka FTP bounce.

6. Correlations:

With the number of known vulnerabilities in FTP servers, these types of scans are unfortunately quite common.

http://www.cert.org/pub/advisories/CA-97.27.FTP_bounce.html

7. Evidence of active targeting:

Starts with a general sweep of our class “C” but it is obvious they found their mark, as they return 35 minutes later to only the 2 FTP servers.

8. Severity:

Criticality	5	These are production servers and critical to our daily business
Lethality	4	If successful, this could result in the loss of customer data
System Countermeasures	3	Lacking latest security patches and we are required to allow Anonymous login
Network Countermeasures	4	Firewall policies are working, but FTP is allowed. Also IDS was down,

$(5 + 4) - (3 + 4) = 2$

9. Defensive recommendation:

Host systems need to be examined very carefully and local OS logs examined to see if there are any signs of compromise. Hosts need all latest security releases and now would be a good time to question the logic of allowing anonymous login.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

Which statement best describes the activity in the above trace?

a) Unsuccessful host scan
b) Normal FTP traffic
c) FTP connection retries
d) Successful FTP scan

answer: d

GIAC - GCIA Certification Practical

Phred Broughton

Assignment #2

Attack: PapaSmurf second generation Smurf

Description: Directed Broadcast Denial of service attack

A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses (amplifiers), all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses does not have appropriate Access Control Lists (ACL's) in place, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, each multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet.
Both the amplifier and the victim will be impacted although the victim will bear the brunt of this attack as it floods their network with unsolicited echo replies.
In the second generation code **http://netscan.org/broadcast/index.html** a second level of amplification has been added by allowing the perpetrator to use UDP traffic aimed at the UDP "small" services ECHO and Chargen. If these ports are active the Smurf attack can set off a "ping pong" effect between the amplifier and the victim which has the potential to greatly increase the amount of traffic generated effectively shutting down communication to the victim host. "A dialup user with 28.8 kbps of bandwidth, exploiting directed broadcast on our example network, could generate (28.8 * 40) or 1152.0 kbps of traffic, about 2/3 of a T1 link." (Netscan.org)

This second generation provides the following options:

```
-p:   Comma separated list of dest ports (default 7)
            Allows the user to specify multiple ports
-r:   Use random dest ports
            Allows the program to randomize the destination ports
-R:   Use random src/dest ports
            Allows randomizing both source and destination ports
-s:   Source port (0 for random (default))
            Allows user to specify the source port
-P:   Protocols to use.  Either icmp, udp or both
            Allows protocol selection
-S:   Packet size in bytes (default 64)
            Potentially allows building "BIG" packets
-f:   Filename containg packet data (not needed)
            Allows user to create packet data
-n:   Num of packets to send (0 is continuous (default))
            Provides limit to number of packets sent
-d:   Delay inbetween packets (in ms) (default 10000)
            Sets interval between packets
```

Sample Trace:

```
11:55:20.841110 > 117.26.2.4.64725 > 192.168.205.255.echo: udp 64
11:55:20.841655 > 117.26.2.4.59956 > 192.168.205.255.discard: udp 64
11:55:20.842166 > 117.26.2.4.57543 > 192.168.205.255.10: udp 64
11:55:20.861106 > 117.26.2.4.56415 > 192.168.205.0.echo: udp 64
11:55:20.901881 > 117.26.2.4.64912 > 192.168.205.255.discard: udp 64
11:55:20.902390 > 117.26.2.4.44282 > 192.168.205.255.10: udp 64
11:55:20.921591 > 117.26.2.4.43969 > 192.168.205.0.echo: udp 64
11:55:20.922166 > 117.26.2.4.44852 > 192.168.205.0.discard: udp 64
11:55:20.922671 > 117.26.2.4.41685 > 192.168.205.0.10: udp 64
```

Very simple, very effective. This is why you should drop ICMP at the border router with no response. Help make the net a quieter place. Write your ACL today.

Assignment #3

Your organization has been asked to provide a bid to provide security services for this facility. You have been allowed to run a Snort system with a fairly standard rulebase for a month. From time to time, the power has failed, or the disk was full so you do not have data for all days. Your task is to analyze the data, be especially alert for signs of compromised systems or network problems and produce an analysis report.

Assumptions:

1. There are no physical issues (improper IDS placement or filter configuration) that would prevent the IDS from seeing both directions of traffic on the wire.
2. Power failures and "disk full" errors are known to have occurred, but in general, this tracing is indicative of normal traffic patterns.
3. Since we are only working with data representing basically a 24 hour period, we will assume that this was chosen as a day with minimal IDS errors and normal network utilization.

General Observations:

1. There are several time gaps in the data that may just indicate periods of little or no traffic or traffic not logged by the standard ruleset, but this would need to be verified. Also there is no data recorded between 22:33 and 01:00, which is a substantial gap that needs to be verified.
2. Apparently the IDS is only configured to monitor inbound connection attempts as there is evidence of data being transferred with no record of an inbound connection attempt.

Month	day	time	source	dir	dest	type	flags	special
Jun	15	9:39:12 AM	195.11.17.245:4606	->	MY.NET.20.10:53	FIN	***F****	
Jun	15	10:06:04 AM	128.183.10.134:53	->	MY.NET.160.149:2713	UDP		
Jun	15	10:06:05 AM	128.183.10.134:53	->	MY.NET.160.149:2719	UDP		
Jun	15	10:06:05 AM	128.183.10.134:53	->	MY.NET.160.149:2724	UDP		
Jun	15	10:06:06 AM	128.183.10.134:53	->	MY.NET.160.149:2727	UDP		
Jun	15	10:06:06 AM	128.183.10.134:53	->	MY.NET.160.149:2730	UDP		
Jun	15	10:06:06 AM	128.183.10.134:53	->	MY.NET.160.149:2736	UDP		
Jun	15	10:06:06 AM	128.183.10.134:53	->	MY.NET.160.149:2739	UDP		
Jun	15	10:06:06 AM	128.183.10.134:53	->	MY.NET.160.149:2742	UDP		
Jun	15	10:06:06 AM	128.183.10.134:53	->	MY.NET.160.149:2745	UDP		
Jun	15	10:06:08 AM	128.183.10.134:53	->	MY.NET.160.149:2756	UDP		
Jun	15	10:06:09 AM	128.183.10.134:53	->	MY.NET.160.149:2760	UDP		
Jun	15	10:06:13 AM	128.183.10.134:53	->	MY.NET.160.149:2765	UDP		
Jun	15	10:06:14 AM	128.183.10.134:53	->	MY.NET.160.149:2785	UDP		

Jun	15	10:06:14 AM	128.183.10.134:53	->	MY.NET.160.149:2775	UDP		
Jun	15	10:06:15 AM	128.183.10.134:53	->	MY.NET.160.149:2797	UDP		
Jun	15	10:06:18 AM	128.183.10.134:53	->	MY.NET.160.149:2782	UDP		
Jun	15	10:16:36 AM	MY.NET.1.3:53	->	MY.NET.101.89:46642	UDP		

3. There is a high instance of host scanning. Some of the source IP are from European countries and did established connections. International partners need to be identified and firewall policies reviewed.
   194.179.163.253 - IBERNET Telefonica Transmision de Datos Country ES
   195.14.145.214 - UK-RSC The Roaring Silence Company Ltd. Country GB
   194.42.136.74 - UOFCYPRUSNET University of Cyprus Country CY

4. There is evidence that these scans were able to solicit a response as the scan sequence changes from SYNFIN to a UDP connection on certain hosts. These machines and their associated firewall policies need to be inspected more closely.

Month	day	time	source	dir	dest	Type	flags	special
Jun	15	6:24:15 PM	194.179.163.253:53	->	MY.NET.1.4:53	SYNFIN	**SF****	
Jun	15	6:24:21 PM	194.179.163.253:1826	->	MY.NET.1.4:53	UDP		

Month	day	time	source	dir	dest	Type	flags	special
Jun	15	6:24:15 PM	194.179.163.253:53	->	MY.NET.1.5:53	SYNFIN	**SF****	
Jun	15	6:24:21 PM	194.179.163.253:1827	->	MY.NET.1.5:53	UDP		

5. There are an extremely high number of connections to port 53 DNS. All systems should be reviewed for unnecessary processes, especially DNS, as it provides a high potential for compromise.

Month	day	time	source	Dest	type
Jun	15	6:33:28 PM	194.179.163.253:1838	MY.NET.109.38:53	UDP
Jun	15	6:33:28 PM	194.179.163.253:1839	MY.NET.109.40:53	UDP
Jun	15	6:33:28 PM	194.179.163.253:1840	MY.NET.109.41:53	UDP
Jun	15	6:33:47 PM	194.179.163.253:1846	MY.NET.110.110:53	UDP
Jun	15	6:33:32 PM	194.179.163.253:1841	MY.NET.110.16:53	UDP
Jun	15	6:35:17 PM	194.179.163.253:1850	MY.NET.130.122:53	UDP
Jun	15	6:35:17 PM	194.179.163.253:1851	MY.NET.130.134:53	UDP

time	Source	dest	type	flags
9:39:12 AM	195.11.17.245:4606	MY.NET.20.10:53	FIN	***F****
8:45:05 PM	194.217.123.210:27970	MY.NET.20.10:27960	FIN	***F****
9:43:58 PM	130.149.41.70:1747	MY.NET.217.14:995	INVALIDACK	2*S*R*A*
7:44:08 PM	24.188.89.211:38949	MY.NET.106.164:4445	INVALIDACK	***FR*A*
7:48:43 PM	195.11.17.245:1378	MY.NET.20.10:1262	INVALIDACK	21SF**AU
8:45:03 PM	194.217.123.210:27035	MY.NET.20.10:27005	INVALIDACK	*1*FR*A*
8:19:06 PM	194.217.102.216:7766	MY.NET.20.10:1122	INVALIDACK	***FR*A*
1:15:29 PM	194.70.126.33:0	MY.NET.20.10:44113	NOACK	2*S**P*U
9:39:41 PM	24.188.172.115:6699	MY.NET.97.68:1066	NOACK	21*FRP*U
8:45:06 PM	194.217.123.210:27901	MY.NET.20.10:27910	NOACK	2***RP*U
7:04:11 PM	194.217.242.39:27025	MY.NET.1.2:27005	NOACK	*1**R**U
8:09:48 PM	24.188.172.115:6699	MY.NET.97.68:1033	NOACK	21*FRP*U
7:28:31 PM	194.159.243.141:31510	MY.NET.20.10:31501	NOACK	*1*FRP*U
7:29:16 PM	194.159.243.141:7777	MY.NET.20.10:2357	NULL	********
8:21:28 PM	24.188.172.115:237	MY.NET.97.68:6699	NULL	21******
8:10:20 PM	24.188.172.115:237	MY.NET.97.68:6699	NULL	21******
8:22:19 PM	24.188.172.115:6699	MY.NET.97.68:1033	NULL	21******
8:45:03 PM	194.217.123.210:27970	MY.NET.20.10:27960	NULL	********

There is a fair amount f anomalous traffic ncluding “null” ackets and packets ith reserved bits set. ome of this may be ttributed to the “Demon” internet ssue. These types of angled packets have een seen coming from heir network for quite ome time and in fact heir source is Demon. hey state that it is a ardware issue, but ave yet to do anything bout it. These ertainly bear a close atch and review of irewall policy.

Recommendations:

We first need to perform a complete discovery of the network. Each host must be identified by its primary function and access requirements detailed. This information will be invaluable in designing the Firewall access policies. These should be designed with a “deny all except what is absolutely necessary” approach.
Services such as Email, DNS, and FTP should be assigned to designated servers only. These should be further protected with host based intrusion and logging. All internal hosts should have a security audit performed to insure that there are no existing issues that might subvert security policies. (Trojans, backdoors, etc) Strict guidelines for controlling services that

are running on each machine need to be developed and a definite procedure put in place to insure adherence along with periodic security scans.
Determine if there are any specific “partnered” connections that require an “open” architecture. These should be reviewed and ideally configured for some type of VPN to allow the free exchange with these partners without having to relax the firewall policies. These “partners” should also be monitored to prevent their inadvertently creating a back door into the network.
In light of the amount of reconnaissance seen in one day, I would suggest having an IDS sensor installed outside the firewall. We can provide the monitoring and maintenance of this device remotely. This will provide early detection of changes in traffic patterns or indications of successful reconnaissance that could be the precursor to an attack. Our remote monitoring insures that these attempts are logged and forwarded to our CIRT and or SANS for proper categorization.