GIAC Level II Certification Practical

Intrusion Detection: 10 Detects with Analyses

San Jose, CA 2000 Class

Author: Scott Brown
Date: May 26, 2000

Note: All destination IP addresses have been removed to protect the identity of the scanned network systems. Limited detail is given as to the type of hosts that were scanned in each of the detects, such as: Firewall, Mail Server, Web Server, etc, under the analysis section. All detects in this document were discovered in the wild, on a single class C IP subnet. Nothing except the IP addresses have been altered in any of the detects listed below. Comments or questions regarding this document may be addressed to **scott.brown@fmr.com.**

Detect #1

SNORT Alert:

```
[**] SMB Name Wildcard [**]
05/18-09:12:10.560006 209.219.129.2:137 -> xxx.xxx.xxx.5:137
UDP TTL:116 TOS:0x0 ID:16964
Len: 58
 [**] SMB Name Wildcard [**]
05/18-09:58:26.649223 209.219.128.96:137 -> xxx.xxx.xxx.5:137
UDP TTL:116 TOS:0x0 ID:44998
Len: 58
[**] SMB Name Wildcard [**]
05/19-09:22:35.491108 209.219.129.2:137 -> xxx.xxx.xxx.5:137
UDP TTL:116 TOS:0x0 ID:7781
Len: 58
```

TCPDUMP Log:

```
09:12:10.560006 P 209.219.129.2.netbios-ns > xxx.xxx.xxx.5.netbios-ns:NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0xDBF8:OpCode=0:NmFlags=0x1:Rcode=0:QueryCount=1:AnswerCount=0:AuthorityCount=0:AddressRecCount=0 (ttl 116, id
16964)
09:12:12.030737 P 209.219.129.2.netbios-ns > xxx.xxx.xxx.5.netbios-ns:NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0xDC1E:OpCode=0:NmFlags=0x1:Rcode=0:QueryCount=1:AnswerCount=0:AuthorityCount=0:AddressRecCount=0 (ttl 116, id
36420)
09:12:13.532410 P 209.219.129.2.netbios-ns > xxx.xxx.xxx.5.netbios-ns:NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0xDC56:OpCode=0:NmFlags=0x1:Rcode=0:QueryCount=1:AnswerCount=0:AuthorityCount=0:AddressRecCount=0 (ttl 116, id
55620)
09:58:26.649223 P 209.219.128.96.netbios-ns > xxx.xxx.xxx.5.netbios-ns:NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0xD84E:OpCode=0:NmFlags=0x1:Rcode=0:QueryCount=1:AnswerCount=0:AuthorityCount=0:AddressRecCount=0 (ttl 116, id
44998)
09:58:28.122672 P 209.219.128.96.netbios-ns > xxx.xxx.xxx.5.netbios-ns:NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0xD872:OpCode=0:NmFlags=0x1:Rcode=0:QueryCount=1:AnswerCount=0:AuthorityCount=0:AddressRecCount=0 (ttl 116, id
61894)
09:58:29.648510 P 209.219.128.96.netbios-ns > xxx.xxx.xxx.5.netbios-ns:NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
TrnID=0xD892:OpCode=0:NmFlags=0x1:Rcode=0:QueryCount=1:AnswerCount=0:AuthorityCount=0:AddressRecCount=0 (ttl 116, id
5831)
```

WHOIS:

```
[Query: 209.219.128.96, Server: whois.arin.net]

@Home Network / @Work Division (NETBLK-ATWORK-4) ATWORK-4
                                   209.218.0.0 - 209.219.255.255
Micronetix Corp. (NETBLK-ATWORK-MICRONETIX2) ATWORK-MICRONETIX2
                                  209.219.128.0 - 209.219.129.255
```

Diagnosis: Mis-Configured Cable Modem or Host

Severity
-4
LOW

Analysis of Detect #1:

The above detect was discovered on our local network and picked up by SNORT 1.6 Network Intrusion Detection Software (NIDS). The xxx.xxx.xxx.5 machine receiving the request is a Sparc Firewall system protecting the local network from the Internet via Network Address Translation (NAT). Due to the limited severity of this detect and the repeated occurrence on our network, the network address does not appear to be spoofed as far as can be determined. The host is reachable via an ICMP Echo request, and an Operating System fingerprint of the detected host determines it is running on a Windows platform

It appears to the best of my knowledge that this detect is the cause of a mis-configured windows machine attempting to communicate via the Windows NETBIOS Name Service (port 137/tcp). This is further seen in the TCPDUMP output where the host appears to be performing name service broadcast queries on the Internet looking for Network Name Resolution. Being that this detect is not an attack against a given host, there is not attack mechanism that may be discussed.

Correlations that can be drawn from this detect are the following: The host responds to requests, the OS fingerprint believes it is running the windows operating system, and the detect is seen many times in a given day to our host. I do not believe there is any active targeting involved in this detect, only a host not configured correctly.

I would rate the severity of this detect as extremely Low. Using the severity formula provided by the SANS organization, the detect would be calculated as (5+1) – (5+5) = -4. The request was against a firewall system with all current patches, yet it failed because correct filtering is in place on the firewall system.

There would not be any defensive measures required for this detect because it is non-threatening in nature and merely a misguided host.

Test Question:

The above detect shows a?

A: Stealth port scan
B: Mis-configured system
C: DDoS attack
D: Normal Traffic

Detect #2

SNORT Alert:

```
[**] spp_portscan: PORTSCAN DETECTED from 216.112.217.218 [**]
05/23-02:44:45.802935
[**] spp_portscan: portscan status from 216.112.217.218: 10 connections across 10 hosts:
TCP(10), UDP(0) [**]
05/23-02:44:51.050454
[**] spp_portscan: End of portscan from 216.112.217.218 [**]
05/23-02:44:57.635895
```

TCPDUMP Data:

```
May 23 02:44:46 216.112.217.218:4320 -> xxx.xxx.xxx.86:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4239 -> xxx.xxx.xxx.5:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4241 -> xxx.xxx.xxx.7:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4397 -> xxx.xxx.xxx.163:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4398 -> xxx.xxx.xxx.164:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4404 -> xxx.xxx.xxx.170:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4409 -> xxx.xxx.xxx.175:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4411 -> xxx.xxx.xxx.177:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4413 -> xxx.xxx.xxx.179:53 SYN **S*****
May 23 02:44:45 216.112.217.218:4416 -> xxx.xxx.xxx.182:53 SYN **S*****
```

WHOIS:

```
Concentric Network Corporation (NETBLK-CONCENTRIC-BLK3)
   1400 Parkmoor Avenue
   San Jose, CA 95126
   US

   Netname: CONCENTRIC-BLK3
   Netblock: 216.112.0.0 - 216.112.255.255
   Maintainer: CRC
```

Diagnosis: Networking Mapping for DNS Services

Severity

-3

LOW

Analysis of Detect #2:

The above detect was received on our local network in the middle of the day on May 23, 2000. The network detect was picked up while running SNORT 1.6 Network Intrusion Detection Software (NIDS) in the DMZ outside our firewall.

This scan appears to have not come from a spoofed network address. The scanning host does answer to standard ICMP echo requests, and the address is classed in the public IP addressing scheme provided by the InterNIC. This does not mean that the scanning host was not compromised and used to perform reconnaissance against our host.

The attack appears to be a TCP SYN scan looking for DNS servers on our network. I would assume that the scan was performed by some type of application, not hand crafted, because of the limited time in between hosts, and the appearance of random order in the scan.

This scan is used to locate hosts running a given vulnerable network service that may be compromised for future mischief. Upon gathering additional data on the above scanning host, the domain name and the IP address are registered to what appears to be a close domain name to the scanning name except that the top-level domain is different.

This may be an attempt to gather information about our company and what we do for business, compared to their business. This detect may involve active targeting, not just a random scan for DNS systems because of the close resemblance of our domain names.

As determined with the SANS Organization severity formula this detect would be rated as a –3. This detect was rated using (5+0) – (4+4) = -3 because it is a DNS scan against hosts that are not running the DNS service. There are no recommendations for protecting the subnet from a TCP SYN scan without removing the subnet from the Internet, which is not possible.

Test Question:

The above detect best describes a

A: DNS Zone Transfer
B: Normal Traffic
C: TCP SYN Scan
D: Stealth UDP Scan

Detect #3

Portsentry Log:

```
Active System Attack Alerts
=-=-=-=-=-=-=-=-=-=-=-=-=-=
May 16 01:47:34 www portsentry[883]: attackalert: Unknown Type: Packet Flags: SYN: 1 FIN: 1
ACK: 0 PSH: 0 URG: 0 RST: 0 from host: 210.92.146.66/210.92.146.66 to TCP port: 31337
May 16 01:47:34 www portsentry[883]: attackalert: Host 210.92.146.66 has been blocked via
wrappers with string: "ALL: 210.92.146.66"
May 16 01:47:34 www portsentry[883]: attackalert: Host 210.92.146.66 has been blocked via
dropped route using command: "/sbin/ipchains -I input -s 210.92.146.66 -j DENY -l"
```

WHOIS:

```
inetnum:      210.92.0.0 - 210.95.255.255
netname:      KRNIC-KR-9
descr:        National Computerization Agency
descr:        Korea Network Information Center
country:      KR
admin-c:      WK1-AP
tech-c:       SH3-KR
tech-c:       SL40-AP
remarks:      KRNIC Allocation Block

person:       Weon Kim
address:      Korea Network Information Center (KRNIC)
address:      Narajongkeum B/D 14F, 1328-3, Seocho-dong, Seocho-Ku
address:      Seoul, 137-070, Republic of Korea

inetnum:      210.92.146.64-210.92.146.127
netname:      YEONKYUNG
descr:        Yeon kyung Electronics Co.LTD
descr:        175-5 Dodang-Dong Wonmi-Gu Boochun-Si
descr:        KYONGGI
country:      KR
admin-c:      Sangseob Kim
tech-c:       Sangseob Kim
changed:      hostmaster@nic.or.kr 990104
source:       KRNIC
```

Diagnosis: SYN/FIN Scan Host Mapping or BackOrifice probe

Severity

-6

LOW

Analysis of Detect #3:

The above attack was gathered from a local host running Portsentry a host based Intrusion Detection System (IDS), early in the morning on May 16, 2000. Portsentry provides a reactive host based detection system that drops any attempt to access a port or service not running on the scanned machine. Because of the reactive nature of the Portsentry product the entire scan is not collected. Portsentry scanner silently dropped and filtered the attacker via IPChains.

It is not believed that the IP address in this detect was spoofed. It is highly likely that the system located at "Yeon Kyung Electronics Co.LTD" was compromised, or an employee of the company produced the above scan upon the host.

Knowing that the scan is for a well-known hacking port of 31337 (*eleet* in hacker speak), I would guess the scanning host has been compromised and is being used as a reconnaissance staging ground looking for hosts open on port 31337. It should be noted that this hacking port is associated mostly with "BackOrifice", a well known Trojan. The scanner may be looking for machines running the BO Trojan allowing system access.

This detect had not been seen in our company until this detect, yet it is well known that people perform massive host scans for open Trojans on the Internet to locate machines that are compromised. I do not believe that we were part of an active targeting during this detect. It appears that the scanner attempted one host in our subnet then moved on to another network. There may be some limited active targeting to this host for the following reason. Our network address may have been placed on a hacking list in the past because the host was compromised previously while running an un-secure OS.

Because this host has had few attempts on hacking once it was hardened, I do not think it was truly an active target. Using the SANS Organization severity formula I would rate this attack as follows (2+0)-(5+3) = -6. There are no current defensive recommendations because this host continues to run a current version of the Portsentry host based intrusion detection system and contains all OS security patches.

Test Question:

The above detect best describes a

A: Trojan Scan
B: TearDrop Attack
C: TCP SYN Scan
D: TraceRoute

Detect #4

Severity
-2
LOW

Portsentry Log:

```
Active System Attack Alerts
=-=-=-=-=-=-=-=-=-=-=-=-=-=
Apr  5 17:19:37 www portsentry[596]: attackalert: SYN/Normal scan from host:
p152_165.kyungpook.ac.kr/155.230.152.165 to TCP port: 3024
Apr  5 17:19:37 www portsentry[596]: attackalert: Host 155.230.152.165 has been blocked via
wrappers with string: "ALL: 155.230.152.165"
Apr  5 17:19:37 www portsentry[596]: attackalert: Host 155.230.152.165 has been blocked via
dropped route using command: "/sbin/ipchains -I input -s 155.230.152.165 -j DENY -l"
```

WHOIS:

```
Kyungpook National University (NET-KPNU-NET)
   San-Gyuk-3-Dong
   Puk-Gu
   Taegu, Korea

   Netname: KPNU-NET
   Netnumber: 155.230.0.0

   Coordinator:
      Han, Ki Jun  (KJH13-ARIN)  kjhan@tol.kpu.ac.kr
      001-82-053-950-5557

   Domain System inverse mapping provided by:

   BH.KYUNGPOOK.AC.KR             155.230.10.2
   KNUHEP.KYUNGPOOK.AC.KR  155.230.20.10
   NS.KREONET.RE.KR        134.75.30.1
```

Diagnosis: Scan from Korea (port 3024 Trojan)

Analysis of Detect #4:

The above scan was collected from a Linux host running the host based intrusion detection software Portsentry. The detect was received via a host located inside the company DMZ, which lies between the Internet router and the corporate firewall.

As with many of the probe scans that are used to detect Trojans, the information during the probe is sent back to the scanning host. It appears that the scan may be a port scan looking for the WinCrash Trojan, or some other application running services by performing a search of port 3024. It appears that a user would scan for responding hosts then try to compromise the system using the installed application.

We have not seen this attack on our local networks in the past, so there is very little information that we can correlate about the attack, and if it really is a Trojan probe or just a standard high numbered port scan. Because of the reactiveness of the host based intrusion detection software, we are unable to determine if this attack is an indication of active targeting against a given host or the subnet.

Portsentry dropped the scanner silently with no other detects received by other hosts on our subnet. It does appear that the company receives many scans from locations over seas in the Asian countries on high TCP ports. The severity of the detect, as rated by the SANS Organization, would be (2+5) – (5+4) = -2.

This system is currently being protected by having Portsentry active, so no further defensive measure would be required for this detect. Also, this host is a workstation system running a Unix flavor of operating system.

Test Question:

The above detect best describes a

A: NuBus Probe
B: Trojan Scan
C: BO Probe
D: All the above

Detect #5

Severity
-1
LOW

SNORT Alert:

```
[**] spp_portscan: portscan status from 4.34.131.13: 20 connections across 10 hosts: TCP(20), UDP(0) [**]
05/19-17:40:08.007118
[**] spp_portscan: End of portscan from 4.34.131.13 [**]
05/19-17:40:11.480629
[**] WinGate 1080 Attempt [**]
05/19-17:40:23.126975 4.34.131.13:1088 -> xxx.xxx.xxx.86:1080
TCP TTL:117 TOS:0x0 ID:60686  DF
**S***** Seq: 0x32C163C3   Ack: 0x0   Win: 0x4000
TCP Options => MSS: 1460 NOP NOP SackOK
[**] WinGate 1080 Attempt [**]
05/19-17:40:23.139708 4.34.131.13:1091 -> xxx.xxx.xxx.163:1080
TCP TTL:117 TOS:0x0 ID:60689  DF
**S***** Seq: 0x32C3CB39   Ack: 0x0   Win: 0x4000
TCP Options => MSS: 1460 NOP NOP SackOK
[**] WinGate 1080 Attempt [**]
05/19-17:40:23.147293 4.34.131.13:1093 -> xxx.xxx.xxx.164:1080
TCP TTL:117 TOS:0x0 ID:60691  DF
**S***** Seq: 0x32C527CB   Ack: 0x0   Win: 0x4000
TCP Options => MSS: 1460 NOP NOP SackOK
[**] WinGate 1080 Attempt [**]
05/19-17:40:23.160397 4.34.131.13:1096 -> xxx.xxx.xxx.170:1080
TCP TTL:117 TOS:0x0 ID:60694  DF
**S***** Seq: 0x32C7CEDF   Ack: 0x0   Win: 0x4000
TCP Options => MSS: 1460 NOP NOP SackOK
```

TCPDUMP Data:

```
17:40:03.423344 P 4.34.131.13.1062 > xxx.xxx.xxx.86.socks: S 845365149:845365149(0) win 16384 <mss
1460,nop,nop,sackOK> (DF) (ttl 117, id 59771)
17:40:05.606723 P 4.34.131.13.1066 > xxx.xxx.xxx.163.socks: S 846106316:846106316(0) win 16384 <mss
1460,nop,nop,sackOK> (DF) (ttl 117, id 59891)
17:40:05.610122 P 4.34.131.13.1068 > xxx.xxx.xxx.164.socks: S 846202760:846202760(0) win 16384 <mss
1460,nop,nop,sackOK> (DF) (ttl 117, id 59893)
17:40:05.622784 P 4.34.131.13.1071 > xxx.xxx.xxx.170.socks: S 846363868:846363868(0) win 16384 <mss
1460,nop,nop,sackOK> (DF) (ttl 117, id 59896)
```

WHOIS:

```
BBN Planet (NET-SATNET)
   150 Cambridge Park Dr.
   Cambridge, MA 02138
   US
   Netname: SATNET
   Netblock: 4.0.0.0 - 4.255.255.255
```

NS Lookup:

```
Translated Name: evrtwa1-ar4-131-013.dsl.gtei.net
IP Address: 4.34.131.13
```

Diagnosis: Non-Stealth Port Scan then WinGate Scan

Analysis of Detect #5:

The above detect was gathered on our local network running a SNORT 1.6 probe in the DMZ between our Internet router and the company firewall system. The source address does not appear to be a spoofed address because the one probing the network would want to use a valid address to use the information in the probe. The probing address of this scan responds to both an NS Lookup and ICMP echo request, proving the host exists. The attack, as documented above, shows first a port scan across many hosts in our DMZ. After the scan is complete the attacker proceeds to test each host looking for WinGate log access. This attack is well documented in Bugtraq and the CVE databases as shown below.

Qbik WinGate Log Service Vulnerability
bugtraq id: 507
class: Unknown
cve remote Yes
local Yes
published: February 22, 1999
updated: April 11, 2000
vulnerable
Qbik WinGate 3.0
- Microsoft Windows 98
- Microsoft Windows 95
- Microsoft Windows NT 4.0
- Microsoft Windows NT 3.5

CVE Version: 20000425
Name: CVE-1999-0441
Description: Remote attackers can perform a denial of service in WinGate machines using a buffer overflow in the Winsock Redirector Service.
References
EEYE:AD02221999
XF:wingate-redirector-dos
SF:509

The attack above is used to give a remote user the ability to exploit the log files of a system running a Wingate service. This attack appears to indicate active targeting. The attacker first scanned the network for hosts, and then probed the scanned hosts only for the given exploit. This would show that the attacker is intentional in what he/she are looking for. This sample is a small portion of the total scan that was done across more than 30 hosts in our DMZ. The severity of this attack using the SANS severity formula would calculate to (5+3)- (5+4) = -1. The rating takes into consideration that the scans were against many of our hosts including the firewall system, and all hosts in the DMZ do not run and of the Microsoft Windows operating systems. There are no current recommendations for defensive measures because of the lack of hosts in the DMZ that are vulnerable.

Test Question:

The above detect best describes a

A: Application Exploit
B: Buffer Overflow Exploit
C: Christmas Tree Scan
D: None of the Above

Detect #6

SNORT Alert:

```
May 23 02:36:47 202.103.43.11:40487 -> xxx.xxx.xxx.25:80 SYN **S*****
May 23 02:36:44 202.103.43.11:40479 -> xxx.xxx.xxx.25:80 NOACK 21SFR*** RESERVEDBITS
May 23 02:36:50 202.103.43.11:40496 -> xxx.xxx.xxx.25:80 SYN **S*****
May 23 02:36:48 202.103.43.11:40489 -> xxx.xxx.xxx.25:80 NOACK 21S****U RESERVEDBITS
May 23 02:36:49 202.103.43.11:40493 -> xxx.xxx.xxx.25:80 NOACK **S**P*U
May 23 02:36:51 202.103.43.11:40500 -> xxx.xxx.xxx.25:80 SYN **S*****
```

WHOIS:

```
[Query: 202.103.43.11, Server: whois.apnic.net]

inetnum:      202.103.43.0 - 202.103.43.255
netname:      N02-MIDDL
descr:        No.2 Accessory middle school Administration
country:      CN
admin-c:      QL12-AP
tech-c:       QL12-AP
mnt-by:       MAINT-CHINANET-HB
changed:      liqiongf@public.wh.hb.cn 19991105
source:       APNIC

person:       Qiongfang Li
address:      10th Floor,ZhongChao Building,
address:      No.11 Wansong Garden,Hankou Wuhan,
address:      China
phone:        +86-27-85806797-36
fax-no:       +86-27-85751699
e-mail:       liqiongf@public.wh.hb.cn
nic-hdl:      QL12-AP
mnt-by:       MAINT-NEW
changed:      liqiongf@public.wh.hb.cn 19990811
source:       APNIC
```

Diagnosis: Returned Traffic with Interesting Packets

Severity

-2

LOW

Analysis of Detect #6:

This network attempt was discovered using a SNORT Intrusion Detection System (IDS), located inside our DMZ. The information was gathered using the portscan-lib module implemented in SNORT v1.6, and extracted from the portscan.log file located in /var/log directory of the SNORT machine.

The probability that the source address was spoofed is limited because of the nature of the attack. The attack appears to be an operating system fingerprinting technique by setting different combinations of TCP flags. The attacker would then receive the packet responses from the scanned host, and analyze the set flags for various TCP stack implementations across different operating systems.

The limited time allowed between attempts would suggest that the packets are created using some application or script rather than crafted by hand. The generated data may be a portion of a fingerprint scan from a well-known tool called ‘nmap’, using the ‘-O’ option. We have discovered this scan occurring many times early in the morning eastern standard time, which would suggest that the data is coming from the destination found during a whois probe of the IP. The whois command also tells us that the scan is coming from a Middle School located inside China. The time of the scan would correlate with the time school would be in progress in China.

I do not see that this scan is active targeting against our network systems, but an information reconnaissance probe searching for specific operating system fingerprints. The severity of the attack, using the rating formula provided by the SANS Organization, would be as follows: (4+1) – (5+2) = -2. This would class the attack in the very low category.

There is no real way of preventing or defending against this type of fingerprinting without removing the host from an active network. In the above case it is an email server, making this solution not an option.

Test Question:

The above detect best describes a

A: OS Fingerprinting
B: TCP Reset Scan
C: Christmas Tree Scan
D: Normal Traffic

Detect #7

SNORT Alert:

```
[**] PCAnywhere [**]
05/23-10:09:11.996648 207.86.117.126:16626 -> 207.121.140.230:5632
UDP TTL:112 TOS:0x0 ID:28306
Len: 10

[**] PCAnywhere [**]
05/23-10:09:11.996714 207.86.117.126:12950 -> 207.121.140.230:22
UDP TTL:112 TOS:0x0 ID:28562
Len: 10
```

TCPDUMP:

```
10:09:11.996648 P 207.86.117.126.16626 > 207.121.140.230.5632: udp 2
10:09:11.996714 P 207.86.117.126.12950 > 207.121.140.230.22: udp 2
```

WHOIS:

```
DIGEX, Inc. (NETBLK-DIGEX-BLK12)
   One Digex Plaza
   Beltsville, MD 20705

   Netname: DIGEX-BLK12
   Netblock: 207.86.0.0 - 207.87.255.255
   Maintainer: DIGX

   Coordinator:
      Hostmaster Role Account  (DIGEX2-ARIN)  dns@DIGEX.NET
      301.847.5000
```

Diagnosis: PC Anywhere Probe

Severity

-5

LOW

Analysis of Detect #7:

The above detect was collected from a SNORT v1.6 sensor located in the company DMZ, between the corporate firewall and the internet router. This scan appears to be against a web server that is also located in the company DMZ.

The probability that the source address is spoofed is highly unlikely. The attack appears to be a probe attempting to locate PCAnywhere servers on our network. By finding this service running on a system, one would then be able to use special exploits against the box to gain control. The attacker could then attempt to attack the administrator password to fully compromise the system because of lax security and encryption in PCAnywhere and Windows NT.

We have not seen this probe attempt on any of the other systems within the DMZ over the past few weeks of running SNORT. This suggests a mis-configured host on the Internet attempting a connection to a PCAnywhere server may have generated the probe. A user typing in the wrong IP address, located in the PCAnywhere connection screen, could cause the same scan pattern as found above.

There does not appear to be any form of active targeting involved in the above attack because the server is not running the service, and none of the other hosts located in the DMZ were scanned. The severity of the attack, as calculated by the SANS severity formula, would be (2+1) – (5+3) = -5.

The defensive measures to prevent this attempt in the future are in place by not running the service on the server and continuing to sense the network with SNORT for further probes.

Test Question:

The above detect best describes a

A: PCAnywhere Probe
B: Willey Attack
C: Trace Route
D: Secure Shell Probe

Detect #8

Portsentry Alert:

```
Apr 23 13:32:37 www portsentry[591]: attackalert: SYN/Normal scan from host:
210.95.255.65/210.95.255.65 to TCP port: 98
Apr 23 13:32:37 www portsentry[591]: attackalert: Host 210.95.255.65 has been blocked via
wrappers with string: "ALL: 210.95.255.65"
Apr 23 13:32:37 www portsentry[591]: attackalert: Host 210.95.255.65 has been blocked via
dropped route using command: "/sbin/ipchains -I input -s 210.95.255.65 -j DENY -l"
```

WHOIS:

```
descr:       Sungnamso Elementary School
descr:       5090-1 Taspyoung3-dong Sujung-gu Sungnam-Si
descr:       KYONGGI
country:     KR
admin-c:     Geunkyoung Lee
tech-c:      Geunkyoung Lee
remarks:     This information has been partially mirrored by APNIC from
remarks:     KRNIC. To obtain more specific information, please use the
remarks:     KRNIC whois server at whois.krnic.net.
changed:     hostmaster@nic.or.kr 981002
source:      KRNIC
```

Diagnosis: Scan for LinuxConf Port

Severity

-1

LOW

Analysis of Detect #8:

The above scan was received on a few of our UNIX machines staged outside our firewall, located in the DMZ. The detect was collected by Portsentry, a host based Intrusion Detection System (HIDS) that detects probes on ports that are not currently active. This scan was discovered on over fifteen of our hosts in a short amount of time making it appear to be an automated probe.

There is limited probability that the source port was spoofed during the probe because it is used for reconnaissance, and the probing host would like to receive the data gathered after the scan. The attack is a scan of machines outside our firewall that respond to the Linuxconf service located on port 98. Attackers are able to exploit this service to compromise machines running Linux that have not been hardened down.

As stated above, the number of hosts that were scanned and probed for the Linuxconf service can correlate this attack. There does not seem to be any active targeting of any one machine in our network during this probe, but the attacker is looking only for this one exploit and moving on. It appears that the attacker is mapping out machines on the Internet that may be compromised for future use of hacking activities.

The severity of this attack, calculated via the SANS severity formula, would be (2+5)-(4+4) = -1. If the machines outside the firewall were running this service they may have been compromised, yet all hosts have this service currently disabled. It is interesting that the WHOIS shows the attack coming from an Elementary school in Korea.

There are no current recommendations for defensive measures in the case of this attack. All hosts have been hardened in the DMZ and are running an active host based intrusion detection system.

Test Question:

The above detect best describes a

A: Trojan Scan
B: Loki Traffic
C: TCP SYN/FIN Scan
D: Linuxconf Scan

Detect #9

SNORT Alert:

```
[**] Source Port traffic [**]
05/20-10:44:21.666678 213.196.4.16:53 -> xxx.xxx.xxx.25:53
TCP TTL:236 TOS:0x0 ID:37199
****R*** Seq: 0x7A8E8D63   Ack: 0x0   Win: 0x0

[**] MISC-DNS-version-query [**]
05/20-10:44:22.029451 213.196.4.16:3078 -> xxx.xxx.xxx.25:53
UDP TTL:45 TOS:0x0 ID:37208
Len: 38

[**] Source Port traffic [**]
05/20-10:44:22.076736 213.196.4.16:53 -> xxx.xxx.xxx.50:53
TCP TTL:23 TOS:0x0 ID:39426
**SF**** Seq: 0x28BD3F2A   Ack: 0x20AA632   Win: 0x404
```

TCPDUMP DATA:

```
10:44:21.576788 P 213.196.4.16.domain > xxx.xxx.xxx.25.domain: SF 2056162658:2056162658(0) win
1028 (ttl 23, id 39426)
10:44:21.666678 P 213.196.4.16.domain > xxx.xxx.xxx.25.domain: R 2056162659:2056162659(0) win 0
(ttl 236, id 37199)
10:44:22.029451 P 213.196.4.16.3078 > xxx.xxx.xxx.25.domain: 43068+ [b2&3=0x180] TXT CHAOS)?
version.bind. (30) (ttl 45, id 37208)
10:44:22.076736 P 213.196.4.16.domain > xxx.xxx.xxx.50.domain: SF 683491114:683491114(0) win
1028 (ttl 23, id 39426)
```

WHOIS:

```
European Regional Internet Registry/RIPE NCC (NETBLK-213-RIPE)
   These addresses have been further assigned to European users.
   Contact information can be found in the RIPE database, via the
   WHOIS and TELNET servers at whois.ripe.net, and at
   http://www.ripe.net/db/whois.html

   Netname: RIPE-213
   Netblock: 213.0.0.0 - 213.255.255.255
   Maintainer: RIPE

   Coordinator:
      RIPE Network Coordination Centre  (RIPE-NCC-ARIN)  nicdb@RIPE.NET
      +31 20 535 4444
Fax- - +31 20 535 4445
```

Diagnosis: Source Port Traffic with DNS probe

Severity

0

LOW

Analysis of Detect #9:

The above detect was gathered from a SNORT v6.1 sensor located on the company DMZ between our Internet router, and firewall protecting the company users. The host probed on port 53 with the last octet being .25 is the company's DNS server.

The probability that the address from the above detect is being spoofed is not likely because of the nature of the scan. The scanner wants to gather information from the scanned hosts, and spoofing the address would deny the scanner the data he was requesting.

The attack appears to be information gathering, looking for DNS servers on the company subnet. An interesting component of the above scan shows a request for DNS version information with the text of 'CHAOS' included in the packet payload. I have attempted to gather additional information on BugTraq and CVE with no success as to the reason for the 'CHAOS' text. I have also posted the scan data on many of the security forms without any responses as of the writing of this document.

The above scan works when an attacker first locates servers running the DNS service. Upon locating the service, the attacker then tries to gather information from the service as to what version of BIND it is running. Once the BIND version is obtained, an attack can then attempt to run exploits against the servers running BIND.

It is interesting that the detect was generated by the European Regional Internet Registry/RIPE. This may provide some detail as to the information-gathering attempt. The detect may be gathering information on DNS services that are running in the US to provide quicker responses to UK internet services by load-balancing DNS requests.

The above detect does not show a direct correlation of active targeting. It appears to be a scan for DNS services and the version of BIND running on that service.

The calculation of severity, using the SANS Organization formula, would be (5+3) – (4+4) = 0.

A defensive measure, that may be incorporated, would be to change the version number returned by the scanning host. Also packets requesting BIND version information could be blocked or dropped quietly at the router or DNS server.

Test Question:

The above detect best describes a

A: Normal DNS Traffic
B: Network Mapping
C: Reset Stealth Scan
D: DNS Probe

Detect # 10

SNORT Alert:

```
[**] Classifieds CGI access attempt [**]
05/23-11:32:21.608362 209.244.142.236:2572 -> xxx.xxx.xxx.66:80
TCP TTL:113 TOS:0x0 ID:2136  DF
*****PA* Seq: 0xE5FA3B5   Ack: 0x6A13BFB2   Win: 0x2180
```

WHOIS:

```
[Query: 209.244.142.236, Server: whois.arin.net]

Level 3 Communications, LLC (NETBLK-LEVEL3-CIDR)
   1450 Infinite Drive
   Louisville, CO 80027
   US

   Netname: LEVEL3-CIDR
   Netblock: 209.244.0.0 - 209.247.255.255
   Maintainer: LVLT

   Coordinator:
      Level 3 Communications, LLC  (LC-ORG-ARIN)  ipadmin@LEVEL3.NET
      +1 (877) 453-8353
```

NS Lookup:

```
[209.244.142.236]
Translated Name: dialup-209.244.142.236.Providence1.Level3.net
IP Address: 209.244.142.236
```

Diagnosis: CGI vulnerability attempt

Severity

2

LOW/MED

Analysis of Detect #10:

The above detect was generated by a host running SNORT v1.6 located in our DMZ between the outside Internet router and the corporate firewall. It was generated when an attacker directed a packet containing CGI commands in the payload toward a web server located inside the DMZ.

The source address above does not appear to be spoofed for this type of attack, because it would limit the information gathered during the exploit. Information provided from an NS Lookup states that the attacking IP address is from a dial-up host, hampering the ability to track down the attacker without the aid of the remote ISP.

The attack appears to be an attempt to compromise web servers that are running the classifieds.cgi script on the host. The attack allows users to input commands into the CGI hoping to gain an exploit that would provide host access. Information on this attack was also located on the CVE web site listed below.

CVE-1999-0935
CVE Version: 20000425
Name: CVE-1999-0935
Description: classifieds.cgi allows remote attackers to execute arbitrary commands by specifying them in a hidden variable in a CGI form.
References
EL8:19991215 Classifieds (classifieds.cgi)

The attacker is able to deliver commands to the given CGI script hoping to gain user access to the given host, or to provide a denial of service by attacking the given application on the host. We have seen two other attempts on other servers that are located inside our company DMZ, yet none of the hosts are running the required CGI script.

We are able to correlate that an attacker is attempting this CGI exploit against our hosts because he first scans the subnet for systems that respond to the HTTP service on port 80.

The above attack does not appear to be created by someone who is actively targeting our company. It looks as if the attacker is scanning hosts, checking for openings via the CGI exploit, then moving onto the next host running the HTTP service. We have not seen any further attempts on hosts in our network after the initial probing.

Using the severity formula provided by the SANS Organization, this attack would be rated as follows: (4+5) – (4+3) = 2.

Defensive measures for this attack are not required. The current hosts located in the DMZ that are running HTTP service do not currently have the exploitable CGI script installed. No other action is required for this attempt.

Test Question:

The above detect best describes a

A: Ping of Death
B: Normal Web Traffic
[✓ C: CGI Attack]
D: None of the Above