Detect 1

```
15:17:00.803036 eth0 < 203.149.232.20.domain > x.x.x.230.domain: SF 683090219:683090219(0) win 1028
15:17:00.803629 eth0 < x.x.x.230.domain > 203.149.232.20.domain: R 0:0(0) ack 683090220 win 0
```

1. Source of trace:

The trace was generated from my work network, by a sniffer outside of the firewall.

2. Detect was generated by:

The tcpdump fields shown are time, interface, traffic direction, source address and port, destination address and port, TCP flags, sequence number and window size.

3. Probability the source address was spoofed:

It is unlikely the attacker's address is spoofed since he is looking to receive a packet in return.

4. Description of attack:

The attack is a single TCP packet from port 53 to port 53, looking for DNS servers. The host returned a reset. The presence of both the SYN and FIN flags, with is not logically possible, means that the packet was crafted.

5. Attack mechanism:

The attack sends the packet to the host's DNS port. If the server is running, it will respond with a SYN ACK, but a host without the DNS service, will send a reset. Also, if there were not a host at that IP address, the attacker would receive either a host unreachable message, or nothing, so this method could also be used to map a network. The attacker is hoping the usual packet will confuse a firewall or IDS, and may have also picked sending on port 53 as a way of hiding in the noise of normal DNS traffic.

6. Correlations:

This kind of attack has been seen every few days by GIAC coming from various sources. One example is listed at http://www.sans.org/y2k/060100.htm and multiple detects can be found at http://www.sans.org/y2k/052800-1130.htm. However, at http://www.sans.org/y2k/060200.htm, Dave Turley was hit by the **same** host with the exact same attack and had notified the owner's ISP in Taiwan.

7. Evidence of active targeting:

This looks like a general attempt to locate DNS servers. This host is not a DNS server and was very recently put online as a sniffer. Since it is connected to a switched segment, so we can't see if this was a sweep of our network. However, seeing this attacker reported by another analyst that has an address space numerically close to mine means that this is a general sweep for active DNS servers.

8. Severity:

```
(Critical + Lethal) – (System + Countermeasures) = Severity
    2    +    1    –     5    +        2         =    -4
```

9. Defensive recommendation:

Check any DNS servers on the same network to see if they were scanned and if further were attacks initiated.

10. Multiple choice question:

This trace is noteworthy because:

a) A Reset was generated
b) Both SYN and FIN are set
c) DNS servers do not talk to each other
d) DNS servers do not use TCP

Answer: B

Detect 2

```
Dec 30 07:52:50 mail tcplog[11574]: linuxconf connection attempt from 172.20.20.1:46841
Dec 30 07:52:50 mail tcplog[11575]: linuxconf connection attempt from 172.20.20.1:37073
```

1. Source of trace:

GIAC website - http://www.sans.org/y2k/123099-1030.htm

2. Detect was generated by:

This detect, two syslog of messages from tcplog, has the displayed the following fields: date, hostname, message source, and message, which contains the local port a connection was attempt was and the host address and port the tried to connect.

3. Probability the source address was spoofed:

It is of course possible the source address is false, but it is unlikely.

4. Description of attack:

This log is of a failed probe to TCP port 98, which is where linuxconf runs.

5. Attack mechanism:

Linuxconf is a program for administration of a Linux computer. It can be run via command line, providing a menu interface to configuring many aspects of a Linux computer and its software. It also has a server component, allowing a web browser access to the same features. The attacker is looking to see if this service is running to try to exploit linuxconf. There is a CVE candidate, number CAN-2000-0017, for a possible buffer overflow that could give an attacker root access. In addition, finding this port open means the host is likely to be running Linux. The attacking address is one of the reserved addresses, so either the log was sanitized, the attack was from the internal network, or there are ISPs who are not filtering properly.

6. Correlations:

More recently there is an AUSCert listing http://www.sans.org/y2k/042200.htm.

7. Evidence of active targeting:

There is not really enough information to say that this machine was the victim of a targeted attack.

8. Severity:

(Critical + Lethal) – (System + Countermeasures) = Severity
2 + 5 – 5 + 2 = 0

9. Defensive recommendation:

The machine that generated this log repelled that attempt but others may want to remove linuxconf if it is not used or disable the server component.

10. Multiple choice question:

A tcpdump filter to recognize this attack is:

a) src port 98
b) dst prt 98
c) tcp[98] = 1
d) tcp[0:4] = 0xff

Answer: B

Detect 3

```
Deny inbound icmp src outside:195.13.29.162 dst xxx.xxx.xxx.0 (type 8, code 0)
Deny inbound icmp src outside:195.13.29.162 dst xxx.xxx.xxx.255 (type 8, code 0)
```

1. Source of trace:

GIAC Website - http://www.sans.org/y2k/052600-1130.htm.

2. Detect was generated by:

Firewall or router log. The listed fields show the action taken, packet direction, protocol, source address, destination address, and ICMP message type with code.

3. Probability the source address was spoofed:

The source address is probably valid since the attacker would like to see the responses. If there were a lot more of these packets, then it could be a Smurf attack, and the source address would be faked.

4. Description of attack:

A ping to the broadcast address and the BSD style broadcast.

5. Attack mechanism:

By pinging the broadcast address, hosts on that network will reply. This gives the attacker a map of the live hosts on the network. One exception is that machines running a Microsoft OS do not respond to a broadcast ping. This is also the basis for the Smurf attack. A single packet is amplified by the response of the hosts, flooding the target. However, there is only two packets, so this is not a denial of service attack.

6. Correlations:

The advisory on the Smurf attack is at http://www.cert.org/advisories/CA-98.01.smurf.html.

7. Evidence of active targeting:

Since the attacker is using broadcasts, he is not targeting any host specifically. However, if this network had an unusual subnet mask, and it was used by the attacker, then there should be some concern that he already has performed some reconnaissance to gain this information. If this were a Smurf attack, then the target would be the device listed as the source address.

8. Severity:

(Critical + Lethal) – (System + Countermeasures) = Severity
2 + 2 – 5 + 5 = -6

9. Defensive recommendation:

The log shows that the defenses in place held and the ping was not allowed into the network. The analyst may want to check for the presence of the attacker's IP address in other system logs.

10. Multiple choice question:

A tcpdump filter to detect both forms of broadcast would be:

a) ip[19] = 0xff
b) tcp and dst port = 255
c) ip[19] = 0xff and ip[19] = 0x00
d) tcp[13] & 2 != 0

Answer: C

Detect 4

```
10:28:03.526424 eth0 B 208.171.48.234.3877 > x.x.x.52.28431: udp 1
10:28:03.529961 eth0 < 208.171.48.234.3877 > x.x.x.53.28431: udp 1
10:28:03.530082 eth0 > x.x.x.53 > 208.171.48.234: icmp: x.x.x.53 udp port 28431 unreachable [tos 0xc0]
10:28:03.543055 eth0 B 208.171.48.234.3877 > x.x.x.55.28431: udp 1
```

1. Source of trace:

Home DSL computer.

2. Detect was generated by:

TCPdump. The fields shown are time, interface, traffic direction, source address and port, destination address and port, protocol and data size. The letter B denotes a broadcast instead of a directed packet.

3. Probability the source address was spoofed:

The source address leads to a DSL user from TDS telecom, resolves to mawi48-234.dsl.tds.net, and is probably not spoofed.

4. Description of attack:

The attacking host is sending UDP packet with 1 byte of data to port 28431 of each computer on the network, looking for a response from a Trojan.

5. Attack mechanism:

The sniffer's DSL provider has an extremely small subnet mask, 255.255.255.252, so hitting a broadcast address is very easy and was unintentional. This small UDP packet is likely the start of authenticating to a Trojan. All network traffic at that time is shown in the trace, so we can see that no device answered.

6. Correlations:

Scans on UDP port 28431 are common, as shown by http://www.sans.org/y2k/122599.htm, http://www.sans.org/y2k/122899-1130.htm and http://www.cert.org/y2k-info/y2k-status-20000103-10.html. However, even though each of those sites mentioned seeing the same packet and associates it with Trojan activity, I have not found a Trojan or even a non-malicious program associated with this port.

7. Evidence of active targeting:

This network was targeted randomly, with the attacker is blindly sweeping through the address space.

8. Severity:

(Critical + Lethal) – (System + Countermeasures) = Severity
2 + 5 – 5 + 2 = 0

9. Defensive recommendation:

The packets were allowed into the network and some information was returned to the attacker, so adding port 28431 to the firewall to block and log and also blocking the attacker's IP address would be good preventative measures.

10. Multiple choice question:

The third packet's protocol is:

a) BGP
b) TCP
c) UDP
d) ICMP

Answer: D

Detect 5

```
Jan 26 07:23:12 aeon tcplogd: sunrpc connection attempt from root@raptorshells.dkexpress.com [63.199.97.3]
Jan 26 07:23:11 aeon portmap[21818]: connect from 63.199.97.3 to dump(): request from unauthorized host
Jan 26 07:28:41 aeon tcplogd: sunrpc connection attempt from root@raptorshells.dkexpress.com [63.199.97.3]
Jan 26 07:28:40 aeon portmap[21830]: connect from 63.199.97.3 to dump(): request from unauthorized host
```

1. Source of trace:

GIAC Website - http://www.sans.org/y2k/013000-1200.htm.

2. Detect was generated by:

This syslog has messages from tcplogd, a tool similar to PortSentry, and portmapper.

3. Probability the source address was spoofed:

This form of attack is not normally spoofed.

4. Description of attack:

The attacker is sending the dump command to the sunrpc port of the host via TCP.

5. Attack mechanism:

The dump function lists the rpc services running on a host. With this information, the attacker can choose related exploits to try to compromise the system. There is a long list of vulnerabilities related to rpc programs, see CVE-1999-0320, CVE-1999-0320, CVE-1999-0320, and CVE-1999-0320 for examples. Interestingly, we can see the username of the attacker; so his computer may have the ident service running.

6. Correlations:

Attempts against rpc are plentiful, occurring almost daily. Two examples are at http://www.sans.org/y2k/061000.htm and http://www.sans.org/y2k/020300.htm.

7. Evidence of active targeting:

With this log, we cannot tell if this attacker hit other systems. This box is running the portmapper service, so it is a good candidate for this scan. The attack is probably scripted since it returned 5 minutes after it was denied the first time. There is notenough information to say with certainty that the computer was an active target.

8. Severity:

(Critical + Lethal) – (System + Countermeasures) = Severity
2 + 5 – 5 + 4 = -2

9. Defensive recommendation:

The defenses held, but the analyst should try to determine if the portmapper daemon is really necessary on this host and remove it if possible.

10. Multiple choice question:

A tcpdump filter to detect this packet is:

a) tcp[0:2] = 111
b) tcp[1:2] = 111
c) tcp[2:2] = 111
d) udp[2:3] = 111

Answer: C

Detect 6

```
Jan 25 22:12:24 pooky kernel: Packet log: input DENY eth0 PROTO=6 210.105.156.200:22065 <my host-4>:21 L=44 S=0x00
I=8641 F=0x0000 T=43
```

1. Source of trace:

GIAC Website - http://www.sans.org/y2k/013000-1200.htm.

2. Detect was generated by:

This is a syslog of the Linux 2.2 firewall, ipchains. The fields are date, hostname, message source, packet direction, action, interface protocol number, source address and port, destination address and port.

3. Probability the source address was spoofed:

It is likely that the originating address is correct; the attacker would need to see a response.

4. Description of attack:

This is a normal connection attempt to the ftp server port using TCP.

5. Attack mechanism:

The attacker could be looking for FTP servers that have write permissions in order to store her files, illegal software, or MP3s. It could also be searching for a way to compromise the host with an exploit like a buffer overflow (CVE-1999-0950) or programming error (CVE-1999-0955) in the server software. These exploits can give a remote attacker root access. Finally, there is a chance that this may just be a wrong number.

6. Correlations:

A similar attempt at the ftp server is at http://www.sans.org/y2k/020300.htm, and is part of a larger scan.

7. Evidence of active targeting:

There is no evidence of this system being singled out, and if it was, that was a rather poor choice.

8. Severity:

```
(Critical + Lethal) – (System + Countermeasures) = Severity
    2    +    3    –    3    +        4         =    -2
```

9. Defensive recommendation:

The defenses that the machine had in place worked well. The truly paranoid might entirely block the attacking address from any access of the host.

10. Multiple choice question:

The PROTO = 6 means:

a) Port 6 is open.
b) The protocol is unknown.
c) The protocol is TCP.
d) The protocol is ARP.

Answer: C

Detect 7

```
Mar 24 07:30:59 ardvark kernel: Packet log: input DENY eth0 PROTO=6 194.78.174.5:35525 xxx.xxx.xxx.11:8080 L=44 S=0x00
I=807 F=0x4000 T=238 SYN

[**] WinGate 8080 Attempt [**]
03/24-07:30:59.531919 0:E0:D0:15:11:94 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x3C
194.78.174.5:35522 -> xxx.xxx.xxx.8:8080 TCP TTL:238 TOS:0x0 ID:797 DF S***** Seq: 0xE40B8062 Ack: 0x0 Win: 0x2238
TCP Options => MSS: 1460
00 00 ..
```

1. Source of trace:

GIAC Website - http://www.sans.org/y2k/033000.htm.

2. Detect was generated by:

This is the syslog output of Linux firewall ipchains followed by Snort's detect of the same type of packet on a different host.

3. Probability the source address was spoofed:

It is unlikely the attacker's address is spoofed since he is looking to receive information in return.

4. Description of attack:

The attacker attempts a TCP connection to port 8080, checking for a response from the host. The logs show the attack hitting two hosts during the same second.

5. Attack mechanism:

Wingate is a proxy server. The attacker is hoping to find a proxy that is setup without any security. It can then be used as a jumping off point to the rest of the Internet, hiding the identity and location of the attacker. This attack is a scan on port 8080. Notice the sending port number incremented by three between the two computers. That is the same number as the difference between the two scanned IP addresses. Therefore it is likely that the tool is scanning a range of addresses and is doing it rapidly. Port 8080 is also used as an administrative port by some applications. For example, I have seen a Netscape server setup where the web server answered normally on port 80, but was configured by a second instance running on 8080.

6. Correlations:

Similar traces can be found at http://www.sans.org/y2k/123099-1030.htm.

7. Evidence of active targeting:

There is no evidence of active targeting, and as mentioned above, this is a sweep of the network.

8. Severity:

(Critical + Lethal) – (System + Countermeasures) = Severity
4 + 3 – 5 + 3 = -1

9. Defensive recommendation:

The analyst may want to check any proxy servers on the network to ensure they are configured properly, allowing only authenticated access by the internal network.

10. Multiple choice question:

The destination port of a TCP packet is located at:

a) The first byte
b) The first two bytes
c) The third byte
d) The third and fourth bytes

Answer D

Detect 8

```
Feb 24 10:59:42 host2 snort: SNMP access, public: 212.60.50.151:3696 -> x.x.x.80:161
Feb 24 10:59:45 host2 snort: SNMP access, public: 212.60.50.151:3696 -> x.x.x.83:161
Feb 24 11:00:06 host2 snort: SNMP access, public: 212.60.50.151:3696 -> x.x.x.101:161
Snort:
[**] SNMP access, public [**]
02/24-10:57:56.119759 212.60.50.151:3696 -> x.x.x.14:161
UDP TTL:102 TOS:0x0 ID:59829 Len: 62
30 34 02 01 00 04 06 70 75 62 6C 69 63 A1 27 02 04.....public.'.
03 00 A6 D1 02 01 00 02 01 00 30 1A 30 0B 06 07 ..........0.0...
2B 06 01 02 01 01 01 05 00 30 0B 06 07 2B 06 01 +........0...+..
02 01 01 02 05 00                               ......
```

1. Source of trace:

GIAC Website - http://www.sans.org/y2k/022400.htm.

2. Detect was generated by:

The first section contains syslog messages, generated by Snort, which is followed by an actual Snort log.

3. Probability the source address was spoofed:

It is unlikely the attacker's address is spoofed since he is looking to receive data back.

4. Description of attack:

This is a scan of four hosts for SNMP access using the default community string of public.

5. Attack mechanism:

SNMP is a protocol for managing devices. It can be used to retrieve performance data or change setting and can be run by routers, printers, servers, and almost anything else. The attacker is attempting to access this information. Many devices will happily give out its model, manufacturer, and software version, all of which is invaluable data for an attacker. This could be the resultof a network monitoring station running a discovery that was not properly limited in its search and is now running amok over the Internet. I have seen this happen, and it is apparently easy enough to do with HP OpenView.

6. Correlations:

Another SNMP trace is listed at http://www.sans.org/y2k/122799-10.htm.

7. Evidence of active targeting:

These hosts were not specifically targeted, but were part of a network scan. The analyst may want to double check that it was not caused by the install of a new management tool internally.

8. Severity:

(Critical + Lethal) – (System + Countermeasures) = Severity
2 + 3 – 5 + 2 = -2

9. Defensive recommendation:

Ensure that SNMP is blocked coming into and out of the network and disable it on every device unless necessary. Also, change the default community strings of public and private and password protect them.

10. Multiple choice question:

A UDP packet in unlike TCP because:
a) It does not use ports
b) It does not use IP
c) It is connectionless
d) It cannot hold data

Answer C

Detect 9

```
sentry.gw.tislabs.com/relay.hq.tis.com
Feb 24 17:50:10 dns3 /usr/local/bin/snort[8374]:
SCAN-NULLScan: 192.94.214.100:11896 -> x.x.x.y:24348
 [**] SCAN-NULLScan [**]
02/24-17:50:10.130414 192.94.214.100:11896 -> x.x.x.y:24348
TCL TTL:190 TOS:0x10 ID:1
******** Seq: 0x3039 Ack: 0xD431 Win: 0x400
```

1. Source of trace:

GIAC Website - http://www.sans.org/y2k/022600.htm.

2. Detect was generated by:

The fields after the header of this Snort alert date, source address and port, destination address, time to live value, type of service value, id number, flags, packet sequence number, ack number, and window size.

3. Probability the source address was spoofed:

It is of course possible the source address is false, but it is unlikely.

4. Description of attack:

This is a null scan, a packet without any flags set. In normal TCP communications, there will always flags set, therefore this is a crafted packet

5. Attack mechanism:

This is another way to test for open ports. Closed ports will respond to a null scan with a reset, while an open port does not respond at all. It the attackers was looking to see what port were open on a host, then a null scan would generate an inverse map. Since there are easier ways to do this, and this trace shows a single packet, it is more likely that the attacker is instead looking for live IP addresses. That explains the choice of port number 24348. IANA does not list any program associated with this port, it is also absent from the list of Trojans, and an internet wide search also did not turn up anything. The attacker needs a closedport to get the host to return a reset. A good tool for generating a packet like this and testing how a host responds is hping. It can be found at packetstorm.

6. Correlations:

Another incident of a null scan can be found at http://www.sans.org/y2k/020500.htm.

7. Evidence of active targeting:

The attacker is looking for live hosts, so this was not the result of active targeting.

8. Severity:

(Critical + Lethal) – (System + Countermeasures) = Severity
5 + 1 – 5 + 5 = -4

9. Defensive recommendation:

This IDS is already watching for abnormal packets, so the only additional action recommended would be to monitor traffic from the hostile IP address and to notify their ISP.

10. Multiple choice question:

A tcpdump filter that detects a tcp null packet is:

a) tcp[13] = 0
b) tcp[13] & 2 !=0
c) tcp[13] != 0
d) tcp[13] & 3 != 0

Answer A

Detect 10

```
Dec 26 13:08:29 pellan named[328]: unapproved query from [152.17.228.34].1682 for "version.bind"
Dec 26 16:45:44 pellan named[328]: unapproved query from [200.238.252.183].1531 for "version.bind"
```

1. Source of trace:

GIAC Website - http://www.sans.org/y2k/123099-1030.htm.

2. Detect was generated by:

This syslog entry by named has the following fields: date, hostname, message source, message, source address and port, and query command.

3. Probability the source address was spoofed:

It is unlikely the attacker’s address is spoofed since he is looking to receive information in return.

4. Description of attack:

The attackers are asking the DNS server what version of the software it is running.

5. Attack mechanism:

DNS servers have a long history of security issues, from buffer overflows to cache poisoning and denial of service attacks. CVE-1999-0275 mentions crashing Microsoft’s DNS server with a flood of character, while CVE-1999-0101 is a buffer overflow allowing root access of Solaris and AIX servers. They can also provide a wealth of information about the other computers on the network. If this query had been successful, the attackers would have gained the knowledge to pick the appropriate exploits to run against the server.

6. Correlations:

More queries names server software versions are at http://www.sans.org/y2k/020500-2000.htm.

7. Evidence of active targeting:

The machine is that was queried was a DNS server, so the attacker was hitting the correct box. There may have previously been reconnaissance performed, but then again, DNS servers are not normally hidden.

8. Severity:

(Critical + Lethal) – (System + Countermeasures) = Severity
5 + 2 – 5 + 2 = 0

9. Defensive recommendation:

This server appears to be configured correctly, not accepting queries for unauthorized hosts. Blocking these IP addresses from accessing the server might be too harsh if this trace is not an attack. Without name resolution, those hosts will have difficulty accessing all of the hosts on the network. However, if this were an attack, then it would be a nice stumbling block to put in their path.

10. Multiple choice question:

Protocols associated with DNS are:

a) TCP and UDP port 53
b) ICMP type 8
c) TCP port 21
d) UDP 23

Answer: A

Last Updated: September 22nd, 2017

Upcoming Training

SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	Tysons, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced