Global Information Assurance Certification Paper

SANS 2000 GIAC IDIC CERTIFICATION PRACTICAL

TEN INTRUSION DETECTS WITH ANALYSIS

Raymond EW Zellmer
June 14, 2000

Detect 1

73638	24-May-00	15:10:53	Elnk32	drop	207.90.69.205	192.xxx.xxx.xx1	icmp	2 icmp-type 3 icmp-code 3
73639	24-May-00	15:10:53	Elnk32	drop	207.90.69.205	192.xxx.xxx.xx1	icmp	2 icmp-type 3 icmp-code 3

1. Source of Trace
   Sandbox at work (destination address sanitized)
2. Detect was generated by:
   a. Checkpoint FW-1
   b. Explanation of fields:
   73638 **[Log Number]** 24-May-00 **[Date Stamp]** 15:10:53 **[Timestamp]** Elnk32 **[Hardware Interface: External]** drop **[Action]** 207.90.69.205 **[Source Address]** 192.xxx.xxx.xx1 **[Destination Address]** icmp **[Protocol]** 2 **[Blocking Rule]** icmp-type 3 icmp-code 3 **[Extra Info]**
3. Probability the source address was spoofed:
   Based on the detect above, the source address is not spoofed. This is actually a case where the attacker has used my address as the source address when sending packets bound for 207.90.69.205.
4. Description of the attack:
   The basic premise of this attack is a very slow port scan. The attacker is doing one of two things: he is either using me as a smoke screen hoping to hide his real identity (this can be done through functionality within a tool like Nmap) or he is crafting the packet with my source address and sniffing the response from the wire. In either case the attacker has sent either a TCP or UDP packet to a specific port on 207.90.69.205 using my address as the source address of the packet. When the packet reached its destination the device being probed responded with an icmp message stating that the port was closed. The most likely reason for this traffic is that my address is being used as a smoke screen to offer the attacker a degree of protection.
5. Attack Mechanism:
   This attack is most likely being perpetrated through the use of a tool like Nmap. Nmap has the functionality to help attackers hide behind a wall of traffic in the hopes that their true identity will not be found.
6. Correlations:
   In an attempt to rule out the chance that this traffic originated from my sandbox, I reviewed all the traffic that passed through the firewall during the day that this traffic occurred (as this firewall is part of a small network all traffic which passes through it is logged). There was no instance where any machine on my network sent traffic to this machine.
   I have also started to note that similar packets are received from the site noted above and two other sites at a rate of two packets a day per site.
7. Evidence of active targeting:
   This is not a case of active targeting for my network. The attacker has proceeded to probe for ports on 207.90.69.205 and possibly others on a daily basis, but has not actively targeted my network.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+1) – (3+5) = -2
9. Defensive Recommendations:
   In this case the packets themselves present little danger to my sandbox, as I am not the intended target. For the recipients of this scan I would recommend hardening any servers in their DMZ by eliminating unnecessary services and closing down all ports that are not needed. In addition to this, reviewing firewall and IDS logs would be key to discovering this slow port scan.
10. Multiple Choice Question:
    This trace is best described as:
    a. A Land Attack
    b. A DoS Attack
    c. An attempt to map my network
    d. A slow port scan where my address is used as a smoke screen
    Answer: D

Detect 2

100071	26-May-00	20:34:13	Elnk32	drop	nbname	ip169.milwaukee7	192.xxx.xxx.xx1	udp	2 nbname	len 78	
100072	26-May-00	20:36:04	Elnk32	drop		ip169.milwaukee7	192.xxx.xxx.xx1	icmp	2	icmp-type 8 icmp-code 0	
100075	26-May-00	20:39:55	Elnk32	drop		ip169.milwaukee7	192.xxx.xxx.xx1	icmp	2	icmp-type 8 icmp-code 0	
100076	26-May-00	20:39:56	Elnk32	drop	nbname	ip169.milwaukee7	192.xxx.xxx.xx1	udp	2 nbname	len 78	

1. Source of Trace
   Sandbox at work (destination address sanitized)
2. Detect was generated by:
   a. Checkpoint FW-1
   b. Explanation of fields:
   100071 **[Log Number]** 26-May-00 **[Date Stamp]** 20:34:13 **[Timestamp]** Elnk32 **[Hardware Interface: External]** drop **[Action]** nbname **[Destination Port]** ip169.milwaukee7 **[Source Address]** 192.xxx.xxx.xx1 **[Destination Address]** udp **[Protocol]** 2 **[Blocking Rule]** nbname **[Source Port]** icmp-type 3 icmp-code 3 **[Extra Info]**
3. Probability the source address was spoofed:
   The source address is likely not spoofed. The attacking host address resolves to an account with an ISP in Milwaukee.
4. Description of the attack:
   At first glimpse this seems to be two separate attacks. The first is a netbios name request and the second a simple echo request. In truth this is all part of an attempt to discover shares on a Windows NT server. The first packet is sent in order to discover the netbios name of the target server. When no response was received, a simple echo request is sent to determine if the target host exists and if it is alive. A second echo request is sent once no reply is received from either of the first two packets. Finally, one last attempt is made to determine the netbios name of the server. Based on the amount of time between packets, this attack could be perpetrated through the use of command line functions. Another possibility is that an automated tool, such as Red Button, was utilized.
5. Attack Mechanism:
   Assuming that Red Button was utilized the first step in the attack would be to determine if the target server had the nbname port open. If this were found to be true, the attacking system would then attempt to illuminate administrative accounts and shares through the use of null sessions. Once the shares and users are discovered the attacker can attempt to brute force a password and gain access to the target server.
6. Correlations:
   a. Unprotected or insecure shares was highlighted on the SANS top ten threats listing
   b. Attempt to discover share information utilizing the Red Button tool after discovering the detect noted above. Firewall displayed similar pattern as noted in the detect above.
7. Evidence of active targeting:
   This is a case of active targeting. The attack noted has a very specific purpose.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+2) – (3+5) = -1
9. Defensive Recommendations:
   a. When drives are shared it is best that specific directories or folders be shared and not the entire drive.
   b. With Windows NT, anonymous illumination of users, groups, and system configuration should be prevented through null sessions.
   c. Protect all shares with strong passwords that include alphanumerical characters.
10. Multiple Choice Question:
    Netbios Shares are best protected through the use of:
    a. Strong Passwords
    b. Not allowing null connections
    c. Sharing only the directories of folders that are necessary
    d. All of the Above
    Answer: D

Detect 3

141081	13-Jun-00	20:41:16	Elnk32	drop	1	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1113	len 48
141082	13-Jun-00	20:41:16	Elnk32	drop	2	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1114	len 48
141083	13-Jun-00	20:41:16	Elnk32	drop	3	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1115	len 48
141084	13-Jun-00	20:41:16	Elnk32	drop	4	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1116	len 48
141085	13-Jun-00	20:41:16	Elnk32	drop	5	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1117	len 48
141086	13-Jun-00	20:41:16	Elnk32	drop	6	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1118	len 48
141087	13-Jun-00	20:41:16	Elnk32	drop	echo-tcp	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1119	len 48
(snip)											
141294	13-Jun-00	20:41:21	Elnk32	drop	216	ip169.milwaukee7	192.xxx.xxx.xxl	tcp	2	1328	len 48
141295	13-Jun-00	20:41:21	Elnk32	drop	217	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1329	len 48
141296	13-Jun-00	20:41:21	Elnk32	drop	218	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1330	len 48
141297	13-Jun-00	20:41:21	Elnk32	drop	219	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1331	len 48
141298	13-Jun-00	20:41:21	Elnk32	drop	220	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1332	len 48
141299	13-Jun-00	20:41:21	Elnk32	drop	221	ip169.milwaukee7	192.xxx.xxx.xx1	tcp	2	1333	len 48

1. Source of Trace
   Sandbox at work (destination address sanitized)
2. Detect was generated by:
   a. Checkpoint FW-1
   b. Explanation of fields:
   141081 **[Log Number]** 13-Jun-00 **[Date Stamp]** 20:41:16 **[Timestamp]** Elnk32 **[Hardware Interface: External]** drop **[Action]** 1 **[Destination Port]** ip169.milwaukee7 **[Source Address]** 192.xxx.xxx.xx1 **[Destination Address]** tcp **[Protocol]** 2 **[Blocking Rule]** 1113 **[Source Port]** len **[Extra Info]**
3. Probability the source address was spoofed:
   The source address is likely not spoofed. The attacking host address resolves to an account with an ISP in Milwaukee.
4. Description of the attack:
   This is a classic port scan. The attacker sends a TCP SYN packet to each port. The attacker will then listen to determine which ports respond with a SYN-ACK and which ports do not reply or reply with a port unreachable. Once open ports are determined the attacker will then proceed to access the target system using the open ports as the gateway.
5. Attack Mechanism:
   Based on the speed at which the packets are being received it is a safe assumption that the attacker is using an automated tool to complete the scan.
6. Correlations:
   a. Various detects posted to the GIAC website report similar port scans.
   b. This is often one of the first steps performed as part of information gathering (reconnaissance) by the attacker.
7. Evidence of active targeting:
   This is a case of active targeting. The attack noted has a very specific purpose.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+2) – (3+5) = -1
9. Defensive Recommendations:
   a. Harden firewall host and apply security patches as they become available.
   b. Review firewall logs for suspicious activity such as a large number of connections from a single source.
10. Multiple Choice Question:
    The purpose of a port scan is:
    a. To set off intrusion detection systems
    b. To determine is a target host is alive
    c. To determine the operating system for a target
    d. To obtain a listing of ports which are open on the target host
    Answer: D

Detect 4

```
Jun 7 04:48:00 fwall 15 deny: TCP from 209.156.190.95.39557 to fwall.23
  seq 105B2, ack 0x0, win 8192, SYN
Jun 7 04:48:09 fwall 15 deny: TCP from 209.156.190.95.39557 to fwall.23
  seq 105B2, ack 0x0, win 8192, SYN
Jun 7 04:48:21 fwall 15 deny: TCP from 209.156.190.95.39557 to fwall.23
  seq 105B2, ack 0x0, win 8192, SYN
```

1. Source of Trace
   http://www.sans.org/y2k/060900-1030.htm (Drew Brunson)
2. Detect was generated by:
   a. Firewall
   b. Explanation of fields:

Jun 7 04:48:00 **[Timestamp]** fwall 15 deny: TCP **[Protocol]** from 209.156.190.95**[Source Address]**.39557**[Source Port]** to fwall**[Destination Address]**.23**[Destination Port]** seq 105B2, ack 0x0, win 8192, SYN**[Tcp Flags Set]**

3. Probability the source address was spoofed:
   The source address is likely not spoofed. In this case the source address corresponds with a host within the targets own ISP. This box is either compromised or someone at the ISP is attempting an unauthorized connection.
4. Description of the attack:
   The premise of the attack is to gain a telnet connection with the target box. Once this connection is established the attacker will have the ability to work within the target system to possibly even execute commands. As seen above this is the initial attempt to establish a connection, as only the SYN flag is set.
   Another question to ask is whether the packets were crafted. In this case neither the source port nor the sequence number increment, as they should. This in itself does not mean that the packets are crafted. The final piece that must be looked at is the timestamp. In this case the time between packets is close, but not close enough to be a single attempt at establishing a connection. These packets are crafted.
5. Attack Mechanism:
   Telnet is a command that is issued either from the command line or a connection can be established through a hyper-terminal session
6. Correlations:
   a. Very common attempt to connect and communicate with target.
7. Evidence of active targeting:
   This is a case of active targeting. The attack noted has a very specific purpose.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+5) – (3+5) = 2
9. Defensive Recommendations:
   a. Harden firewall host and apply security patches as they become available.
   b. Prevent telnet and any other unnecessary service from accessing the internal network through firewall policy.
10. Multiple Choice Question:
    What attribute of this packet shows that this is an initial attempt to connect:
    a. The Timestamp
    b. The source port number
    c. The window size
    d. The SYN flag is set
    Answer: D

Detect 5
UUNET an MCI WorldCom Company, Hilliard OH, USA

```
Jun 5 13:11:33 dns1 snort [248951]: spp_portscan:
  PORTSCAN DETECTED from 216.192.107.19
Jun 5 13:11:33 dns1 snort [248951]: SCAN-SYN FIN:
  216.192.107.19:109 -> z.y.w.34:109
Jun 5 13:11:39 dns1 snort[248951]: spp_portscan:
  portscan status from 216.192.107.19: 1 connections across 1 hosts:
  TCP(1), UDP(0) STEALTH
Jun 5 13:11:45 dns1 snort[248951]: spp_portscan:
  End of portscan from 216.192.107.19
Jun 5 13:14:27 dns1 snort[248951]: spp_portscan:
  PORTSCAN DETECTED from 216.192.107.19 SYN
```

1. Source of Trace
   http://www.sans.org/y2k/060700.htm (Laurie)
2. Detect was generated by:
   a. Snort IDS
   b. Explanation of fields:

```
Jun 5 13:11:33[Timestamp] dns1[Hostname] snort[248951]:
spp_portscan:[Type of Attack] PORTSCAN DETECTED from 216.192.107.19
[Source Address]
```

3. Probability the source address was spoofed:
   The source address is likely not spoofed.
4. Description of the attack:
   This is a stealth port scan as identified by Snort. The purpose of a stealth scan is to evade detection through scanning using anomalous flag bits set, most commonly SYN-FIN. In this case the attacker is attempting to find which ports on the target machine are open. Once this is discovered, the attacker can attempt to fingerprint the OS, determine the purpose of the host and even attempt to connect through telnet to the open port. In this case one port replied as being open, port 34.
5. Attack Mechanism:
   Several tools can be used to complete scans of this type. The most commonly used is Nmap. Nmap is extremely configurable and allows the attacker the ability to send a variety of packets with anomalous flag bits set in an attempt to evade detection.
6. Correlations:
   a. Common scan as noted on various detects per the GIAC website.
   b. Common method of completing reconnaissance.
7. Evidence of active targeting:
   This is a case of active targeting. The attack noted has a very specific purpose.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+3) – (3+3) = 2
9. Defensive Recommendations:
   a. Configure IDS to detect packets with anomalous flag bits set.
   b. Drop these packets at firewall through use of established policy.
10. Multiple Choice Question:
    A SYN-FIN scan is deemed stealthy because:
    a. It is believed that many firewalls or IDS do not detect these packets.
    b. They have a low radar profile
    c. The reply can not be seen by any one but the attacker
    d. The SYN flag is set
    Answer: A

Detect 6

```
May 17 12:03:17 dns1 snort[51901]: IDS007 -
  MISC-Source Port Traffic 53 TCP: 194.219.84.38:53 -> z.y.w.34:111
May 17 12:03:17 dns3 snort[3439]: IDS007 -
  MISC-Source Port Traffic 53 TCP: 194.219.84.38:53 -> z.y.w.98:111
```

1. Source of Trace
   http://www.sans.org/y2k/052300-0800.htm (Laurie)
2. Detect was generated by:
   a. Snort IDS
   b. Explanation of fields:

```
May 17 12:03:17[Timestamp] dns1[Hostname] snort[51901]: IDS007 -
  MISC-Source Port Traffic 53 TCP:[Type of Attack] 194.219.84.38:53
[Source Address] -> z.y.w.34:111[Destination Address]
```

3. Probability the source address was spoofed:
   The source address is likely not spoofed.
4. Description of the attack:
   This attack is an attempt to connect to a privileged port (111 portmap or sunrpc) through the guise of DNS traffic. This type of traffic should not naturally occur as DNS traffic usually passes from port 53 UDP to port 53 UDP. In certain cases when a connection can not be established over UDP, TCP will be utilized. The traffic will then be passed over 53 TCP. What is anomalous in this case is that the connection goes from 53 TCP to a privileged port of 111. This attack attempts to infiltrate the internal network by bypassing misconfigured or old packetfilters that allow all apparent DNS traffic to pass.
5. Attack Mechanism:
   The attacker is attempting to establish a connection to port 111. By connecting to this port the attacker is establishing that the port is indeed open.
   Per **http://www.rednet.co.uk/rednet-new/technical/faq/leasedline/certfilters.html**

"*Port 111 is only a directory service. If you can guess the ports the actual data services are on, you can still talk to them. Most RPC services do not have fixed port numbers. You should find the ports that these services can be on and block them."

6. Correlations:
   a. **http://www.rednet.co.uk/rednet-new/technical/faq/leasedline/certfilters.html**
7. Evidence of active targeting:
   This is a case of active targeting. The attack noted has a very specific purpose.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+5) – (5+3) = 2
9. Defensive Recommendations:
   a. Configure firewall to drop TCP DNS traffic.
   b. Close off unnecessary ports on a server by server basis and prevent configure firewall to drop packets bound for well-known ports.
10. Multiple Choice Question:
    DNS traffic:
    a. Can be UDP or TCP
    b. Connects over port 53
    c. Is not by attackers
    d. Both A and B
    Answer: D

Detect 7

```
[**] SMB Name Wildcard [**]
05/10-07:59:09.863865 0:E0:D0:15:11:94 -> 0:0:C0:29:8F:D2 type:0x800 len:0x5C
10.0.0.140:137 -> xxx.xxx.xxx.11:137 UDP TTL:111 TOS:0x0 ID:394
Len: 58
[**] SMB Name Wildcard [**]
05/10-07:59:11.360830 0:E0:D0:15:11:94 -> 0:0:C0:29:8F:D2 type:0x800 len:0x5C
10.0.0.140:137 -> xxx.xxx.xxx.11:137 UDP TTL:111 TOS:0x0 ID:906
Len: 58
[**] SMB Name Wildcard [**]
05/10-07:59:12.861827 0:E0:D0:15:11:94 -> 0:0:C0:29:8F:D2 type:0x800 len:0x5C
10.0.0.140:137 -> xxx.xxx.xxx.11:137 UDP TTL:111 TOS:0x0 ID:1418
Len: 58
```

1. Source of Trace
   http://www.sans.org/y2k/051800.htm
2. Detect was generated by:
   c. Snort IDS
   d. Explanation of fields:

```
[**] SMB Name Wildcard [**][Attack Identified]
05/10-07:59:09.863865[Timestamp] 0:E0:D0:15:11:94 -> 0:0:C0:29:8F:D2
type:0x800 len:0x5C
10.0.0.140:137[Source Address: Source Port] ->
xxx.xxx.xxx.11:137[Destination Address: Destination Port] UDP
[Protocol] TTL:111 TOS:0x0 ID:394
Len: 58
```

3. Probability the source address was spoofed:
   This is not a case of a spoofed address. It is more a lack of egress filtering and misconfigured NAT.
4. Description of the attack:
   Not necessarily an attack. Due to the unroutable nature of restricted addresses any response to this packet would not get back to the originating source. The possibility does exist that this is some sort of DoS, but going on the assumption that only three packets arrived at the destination, it hardly behooves coming to this conclusion.
5. Attack Mechanism:
   Again, not necessarily an attack. Chances are that this is more an attempt by a host to make contact with an external host, but due to misconfigured NAT, the restricted internal address was not converted to a public IP. As such, the source host will not ever receive traffic back.
6. Correlations:
   Had the proper addressing scheme been utilized the attacking host would be attempting to connect to the target to retrieve data relating to shares.
   a. Unprotected or insecure shares was highlighted on the SANS top ten threats listing
   b. If unprotected shares are found through a scan of this sort, the attacker will attempt to access these shares to create further exploits.
7. Evidence of active targeting:
   The host above was certainly the target for the above traffic.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (3+5) – (5+3) = 0
9. Defensive Recommendations:
   a. Configure border router ACL to filter all traffic from restricted addresses.
   b. Close off unnecessary ports on a server by server basis (especially netbios from the external) and configure firewall to drop packets bound for well-known ports.
10. Multiple Choice Question:
    A restricted network address should:
    a. Be filtered during an egress filter
    b. Be filtered as part of an ingress filter
    c. Is routable externally
    d. Both a and b
    Answer: D

Detect 8

```
Apr 21 15:26:52 s1 named[13168]: refused query on
non-query socket from [216.87.91.3].2018
Apr 21 16:46:52 s1 named[13168]: refused query on
non-query socket from [216.87.91.3].2138
Apr 21 18:04:05 s1 named[13168]: refused query on
non-query socket from [216.87.91.3].4490
Apr 21 18:49:01 s1 named[13168]: refused query on
non-query socket from [216.87.91.3].4309
```

1. Source of Trace
   http://www.sans.org/y2k/042400.htm (Martin)
2. Detect was generated by:
   a. Server
   b. Explanation of fields:

```
Apr 21 15:26:52[Timestamp] s1[Server Name] named[13168]:[Destination Port: Error Number]
refused query on non-query socket from [216.87.91.3].2018[Source Address: Source Port]
```

3. Probability the source address was spoofed:
   Based on the detect above, the source address is not spoofed. This is actually a case where the attacker has used the server's address as the source address when sending packets bound for 216.87.91.3.
4. Description of the attack:
   This is an example of the DOOMDNS DoS. Assuming that the above is the complete trace, the number of packets that actually hit this server is small. Thus the DoS is not being perpetrated against the server, but against 216.87.91.3. In the case of the DOOMDNS the attacker will spoof the source address of the server above and make several DNS queries to 216.87.91.3. The response from 216.87.91.3 will then be sent to the above spoofed server.
5. Attack Mechanism:
   a. UDP packets (DNS queries are initially sent using UDP to port 53) do not provide adequate authentication. As such, it is possible to complete a DoS attack by flooding the actual target with a large number of DNS queries.
   b. A small DNS query of just 20 bytes can elicit a response from a DNS server of over 400 bytes.
6. Correlations:
   a. **http://www.sans.org/y2k/010700-0900.htm**
      The above site provides the signature for the DOOMDNS attack.
   b. It is possible to flood a server with DNS queries, thus effectively completing a DoS attack.
7. Evidence of active targeting:
   The target of this second hand traffic is not the initial target. As such, the server was not being actively targeted.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+4) – (5+2) = 2
9. Defensive Recommendations:
   As the server is not the target of the attack no recommendations are necessary. The host that is being attacked should have the bandwidth dedicated to answering DNS queries throttled.
10. Multiple Choice Question:
    The server above is not the target of a Dos because:
    a. The attack is not a DoS
    b. The small amount of traffic bound for the server
    c. The server is only receiving secondary traffic
    d. Both b and c
    Answer: D

Detect 9

```
May 10 09:20:33.328 UTC: %SEC-6-IPACCESSLOGP: list 100 denied tcp
10.1.2.73(0) -> 192.231.90.254(0), 1 packet
May 10 09:26:04.564 UTC: %SEC-6-IPACCESSLOGP: list 100 denied tcp
10.1.2.73(0) -> 192.231.90.254(0), 4 packets
May 10 09:26:34.260 UTC: %SEC-6-IPACCESSLOGP: list 100 denied tcp
10.0.0.57(0) -> 192.231.90.254(0), 1 packet
May 10 09:32:04.708 UTC: %SEC-6-IPACCESSLOGP: list 100 denied tcp
```

10.0.0.57(0) -> 192.231.90.254(0), 20 packets

1. Source of Trace
   http://www.sans.org/y2k/050900.htm
2. Detect was generated by:
   a. Cisco Router ACL Log
   b. Explanation of fields:

```
May 10 09:20:33.328[Timestamp] UTC: %SEC-6-IPACCESSLOGP: list 100[ACL Number]
denied[Action Taken] tcp[Protocol] 10.1.2.73(0)[Source Address (Source Port)] ->
192.231.90.254(0)[Destination Address (Destination Port)], 1 packet
```

3. Probability the source address was spoofed:
   There is a good chance that this packet is crafted with the sole purpose to evade detection.
4. Description of the attack:
   This is an attack that is meant to bypass the packet filtering completed by the router.
5. Attack Mechanism:
   a. This attacks sole purpose is to evade the router and possibly the firewall by attacking source port 0. Chances are that the attacker is attempting to gain information relating to the network where this packet is being sent. In other words the attacker is attempting to find a backdoor into the network.
6. Correlations:
   a. A similar attack was noted by Terry on May 15, 2000
      http://www.sans.org/y2k/051500.htm
7. Evidence of active targeting:
   This is an example of active targeting as the attacker is attempting to exploit a specific weakness in order to gain access to the target network.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+2) – (4+3) = 0
9. Defensive Recommendations:
   The ACL on the router was enough to block this attack, but the true effectiveness of this ACL is only realized when the router logs are regularly reviewed.
10. Multiple Choice Question:
    This attack was blocked by:
    a. The default router configuration
    b. The Firewall
    c. A server
    d. A properly configured ACL
    Answer: D

Detect 10

```
May 12 04:43:19 hosth snort[87556]: spp_portscan: PORTSCAN DETECTED
from 64.27.91.190
May 12 04:43:25 hosth snort[87556]: spp_portscan: portscan status
from 64.27.91.190: 15 connections across 15 hosts: TCP(0), UDP(15)
May 12 04:43:31 hosth snort[87556]: spp_portscan: End of portscan
from 64.27.91.190
--------
May 12 04:43:18 64.27.91.190:1135 -> a.b.e.13:53 UDP
May 12 04:43:19 64.27.91.190:3352 -> a.b.e.63:53 UDP
May 12 04:43:19 64.27.91.190:4234 -> a.b.e.79:53 UDP
May 12 04:43:19 64.27.91.190:4998 -> a.b.e.91:53 UDP
May 12 04:43:19 64.27.91.190:1227 -> a.b.e.101:53 UDP
May 12 04:43:19 64.27.91.190:1360 -> a.b.e.99:53 UDP
May 12 04:43:19 64.27.91.190:4090 -> a.b.e.128:53 UDP
May 12 04:43:20 64.27.91.190:3143 -> a.b.e.171:53 UDP
May 12 04:43:20 64.27.91.190:4029 -> a.b.e.182:53 UDP
May 12 04:43:20 64.27.91.190:4531 -> a.b.e.195:53 UDP
May 12 04:43:20 64.27.91.190:1202 -> a.b.e.201:53 UDP
May 12 04:43:20 64.27.91.190:1269 -> a.b.e.200:53 UDP
May 12 04:43:20 64.27.91.190:1586 -> a.b.e.208:53 UDP
May 12 04:43:20 64.27.91.190:2236 -> a.b.e.216:53 UDP
May 12 04:43:20 64.27.91.190:2282 -> a.b.e.217:53 UDP
```

1. Source of Trace
   http://www.sans.org/y2k/051900.htm
2. Detect was generated by:
   c. Snort IDS
   d. Explanation of fields:

May 12 04:43:19**[Timestamp]** hosth**[Hostname]** snort[87556]**[ID number]**: spp_portscan**[Type of Attack]**: PORTSCAN DETECTED from 64.27.91.190 **[Source Address]**

3. Probability the source address was spoofed:
   The source address in this trace is not spoofed as the attacker is attempting to gain information about the target network.
4. Description of the attack:
   This was a port scan completed with the sole purpose of mapping devices with the Domain port open. In this case 15 devices responded as having port 53 open.
   There is a good chance that these packets are crafted as the source ports do not increment as they should when compared to the timestamps.
5. Attack Mechanism:
   The purpose of this attack is to determine possible DNS servers. Several attacks can be used against DNS servers including Evil DNS. This is more than likely a reconnaissance scan.
6. Correlations:
   a. A similar attack was noted by Laurie and Sean on May 12, 2000
      http://www.sans.org/y2k/051200.htm
7. Evidence of active targeting:
   This is an example of active targeting as the attacker is attempting to exploit a specific weakness in order to identify devices with a specific service.
8. Severity:
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+2) – (4+3) = 0
9. Defensive Recommendations:
   DNS servers should be hardened to eliminate services and ports that are not necessary. Additional controls might include protecting these severs inside the DMZ and monitoring them with host based intrusion detection.
10. Multiple Choice Question:
    DNS queries can occur on:
    a. Port 53 UDP
    b. Port 111 TCP
    c. Port 53 TCP
    d. Both a and c
    Answer: D