GIAC
CERTIFICATIONS

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 permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

Duncan Wallace submits these 10 traces for the Practical examination for the GIAC Intrusion Detection Curriculum attended at SANS2000, San Jose, Ca.

Detect 1

NAI Sniffer Trace:

Flags	Frame	Delta Time	Destination	Source	Protocol	Summary
M [B]	1	0.000.000	mydns.com	[attacker1.com]	TCP	D=53 S=55692 SYN SEQ=1657845382
[B]	2	0.000.007	mydns.com	[attacker1.com]	TCP	D=53 S=55692 SYN SEQ=1657845382
[B]	3	0.000.205	[attacker1.com]	mydns.com	TCP	D=55692 S=53 SYN ACK=1657845383
[B]	4	0.000.006	[attacker1.com]	mydns.com	TCP	D=55692 S=53 SYN ACK=1657845383
[B]	5	0.105.948	mydns.com	[attacker1.com]	TCP	D=53 S=55692 ACK=920011 WIN=6
[B]	6	0.000.008	mydns.com	[attacker1.com]	TCP	D=53 S=55692 ACK=920011 WIN=6
[B]	7	0.005.270	mydns.com	[attacker1.com]	TCP	Retransmitted in frame 8; 47 Bytes of da
# [B]	8	0.000.008	mydns.com	[attacker1.com]	DNS	C ID=22624 OP=QUERY NAME=800.c
[B]	9	0.000.254	[attacker1.com]	mydns.com	TCP	Retransmitted in frame 10; 116 Bytes of
# [B]	10	0.000.014	[attacker1.com]	mydns.com	DNS	R ID=22624 STAT=OK NAME=800.com
[B]	11	0.107.669	mydns.com	[attacker1.com]	TCP	D=53 S=55692 ACK=920107 WIN=6
[B]	12	0.000.007	mydns.com	[attacker1.com]	TCP	D=53 S=55692 ACK=920107 WIN=6
[B]	13	0.001.673	mydns.com	[attacker1.com]	TCP	Retransmitted in frame 14; 47 Bytes of
# [B]	14	0.000.008	mydns.com	[attacker1.com]	DNS	C ID=22625 OP=QUERY NAME=800.c
[B]	15	0.000.391	[attacker1.com]	mydns.com	TCP	Retransmitted in frame 16; 47 Bytes of
# [B]	16	0.000.008	[attacker1.com]	mydns.com	DNS	R ID=22625 STAT=Refused NAME=80
[B]	17	0.107.684	mydns.com	[attacker1.com]	TCP	D=53 S=55692 FIN ACK=920134 SEQ=
[B]	18	0.000.007	mydns.com	[attacker1.com]	TCP	D=53 S=55692 FIN ACK=920134 SEQ=
[B]	19	0.000.181	[attacker1.com]	mydns.com	TCP	D=55692 S=53 ACK=1657845438 W
[B]	20	0.000.007	[attacker1.com]	mydns.com	TCP	D=55692 S=53 ACK=1657845438 W
[B]	21	0.000.243	[attacker1.com]	mydns.com	TCP	D=55692 S=53 FIN ACK=1657845438
[B]	22	0.000.007	[attacker1.com]	mydns.com	TCP	D=55692 S=53 FIN ACK=1657845438
[B]	23	0.107.576	mydns.com	[attacker1.com]	TCP	D=53 S=55692 ACK=920135 WIN=6
[B]	24	0.000.006	mydns.com	[attacker1.com]	TCP	D=53 S=55692 ACK=920135 WIN=6
[B]	25	600.088.658	mydns.com	[attacker2.com]	DNS	C ID=51788 OP=QUERY NAME=800.c
[B]	26	0.000.008	mydns.com	[attacker2.com]	DNS	C ID=51788 OP=QUERY NAME=800.c
[B]	27	0.000.314	[attacker2.com]	mydns.com	DNS	R ID=51788 STAT=OK NAME=800.com
[B]	28	0.000.013	[attacker2.com]	mydns.com	DNS	R ID=51788 STAT=OK NAME=800.com
[B]	29	3.068.964	mydns.com	[attacker2.com]	DNS	C ID=51788 OP=QUERY NAME=800.c
[B]	30	0.000.006	mydns.com	[attacker2.com]	DNS	C ID=51788 OP=QUERY NAME=800.c
[B]	31	0.000.358	[attacker2.com]	mydns.com	DNS	R ID=51788 STAT=OK NAME=800.com
[B]	32	0.000.013	[attacker2.com]	mydns.com	DNS	R ID=51788 STAT=OK NAME=800.com
[B]	33	3699.160.915	mydns.com	[attacker3.com]	TCP	D=53 S=63949 SYN SEQ=4175137252
[B]	34	0.000.007	mydns.com	[attacker3.com]	TCP	D=53 S=63949 SYN SEQ=4175137252
[B]	35	0.000.190	[attacker3.com]	mydns.com	TCP	D=63949 S=53 SYN ACK=4175137253
[B]	36	0.000.007	[attacker3.com]	mydns.com	TCP	D=63949 S=53 SYN ACK=4175137253
[B]	37	0.114.769	mydns.com	[attacker3.com]	TCP	D=53 S=63949 ACK=950246 WIN=6

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[B]	38	0.000.006	mydns.com	[attacker3.com]	TCP	D=53 S=63949 ACK=950246 WIN=6
[B]	39	0.000.371	mydns.com	[attacker3.com]	TCP	Retransmitted in frame 40; 62 Bytes of
# [B]	40	0.000.009	mydns.com	[attacker3.com]	DNS	C ID=34052 OP=QUERY NAME=223.2
[B]	41	0.000.970	[attacker3.com]	mydns.com	TCP	Retransmitted in frame 42; 138 Bytes of
# [B]	42	0.000.015	[attacker3.com]	mydns.com	DNS	R ID=34052 STAT=OK NAME=223.2.1
[B]	43	0.121.271	mydns.com	[attacker3.com]	TCP	D=53 S=63949 ACK=950364 WIN=6
[B]	44	0.000.007	mydns.com	[attacker3.com]	TCP	D=53 S=63949 ACK=950364 WIN=6
[B]	45	0.000.617	mydns.com	[attacker3.com]	TCP	Retransmitted in frame 46; 62 Bytes of
# [B]	46	0.000.010	mydns.com	[attacker3.com]	DNS	C ID=34053 OP=QUERY NAME=223.2
[B]	47	0.000.460	[attacker3.com]	mydns.com	TCP	Retransmitted in frame 48; 62 Bytes of
# [B]	48	0.000.010	[attacker3.com]	mydns.com	DNS	R ID=34053 STAT=Refused NAME=223
[B]	49	0.122.559	mydns.com	[attacker3.com]	TCP	D=53 S=63949 FIN ACK=950406 SEQ=
[B]	50	0.000.006	mydns.com	[attacker3.com]	TCP	D=53 S=63949 FIN ACK=950406 SEQ=
[B]	51	0.000.210	[attacker3.com]	mydns.com	TCP	D=63949 S=53 ACK=4175137338 W
[B]	52	0.000.007	[attacker3.com]	mydns.com	TCP	D=63949 S=53 ACK=4175137338 W
[B]	53	0.000.266	[attacker3.com]	mydns.com	TCP	D=63949 S=53 FIN ACK=4175137338
[B]	54	0.000.007	[attacker3.com]	mydns.com	TCP	D=63949 S=53 FIN ACK=4175137338
[B]	55	0.115.054	mydns.com	[attacker3.com]	TCP	D=53 S=63949 ACK=950407 WIN=6
[B]	56	0.000.007	mydns.com	[attacker3.com]	TCP	D=53 S=63949 ACK=950407 WIN=6
[B]	57	599.441.631	mydns.com	[attacker4.com]	DNS	C ID=5599 OP=QUERY NAME=223.2.1
[B]	58	0.000.009	mydns.com	[attacker4.com]	DNS	C ID=5599 OP=QUERY NAME=223.2.1
[B]	59	0.000.308	[attacker4.com]	mydns.com	DNS	R ID=5599 STAT=OK NAME=223.2.199
[B]	60	0.000.014	[attacker4.com]	mydns.com	DNS	R ID=5599 STAT=OK NAME=223.2.199

ISS RealSecure Log:

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourcePortName	DestinationPortNa
80730	25-Apr-00	DNS_Zone_High_Port	6	56145	53	56145	DNS-Xfer
84256	26-Apr-00	DNS_Zone_High_Port	6	53358	53	53358	DNS-Xfer
84713	26-Apr-00	DNS_Zone_High_Port	6	61329	53	61329	DNS-Xfer
85220	26-Apr-00	DNS_Zone_High_Port	6	41443	53	41443	DNS-Xfer
85795	26-Apr-00	DNS_Zone_High_Port	6	49642	53	49642	DNS-Xfer
86328	26-Apr-00	DNS_Zone_High_Port	6	62330	53	62330	DNS-Xfer
86702	26-Apr-00	DNS_Zone_High_Port	6	37710	53	37710	DNS-Xfer
87324	26-Apr-00	DNS_Zone_High_Port	6	50534	53	50534	DNS-Xfer
87689	26-Apr-00	DNS_Zone_High_Port	6	58543	53	58543	DNS-Xfer

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

81183	25-Apr-00	DNS_Zone_High_Port	6	64234	53	64234	DNS-Xfer
87874	26-Apr-00	DNS_Zone_High_Port	6	38719	53	38719	DNS-Xfer
87953	26-Apr-00	DNS_Zone_High_Port	6	46890	53	46890	DNS-Xfer
88092	26-Apr-00	DNS_Zone_High_Port	6	60247	53	60247	DNS-Xfer
88178	26-Apr-00	DNS_Zone_High_Port	6	36472	53	36472	DNS-Xfer
88311	26-Apr-00	DNS_Zone_High_Port	6	49372	53	49372	DNS-Xfer
88444	26-Apr-00	DNS_Zone_High_Port	6	57381	53	57381	DNS-Xfer
88696	26-Apr-00	DNS_Zone_High_Port	6	37489	53	37489	DNS-Xfer
88760	26-Apr-00	DNS_Zone_High_Port	6	45577	53	45577	DNS-Xfer
88842	26-Apr-00	DNS_Zone_High_Port	6	58525	53	58525	DNS-Xfer

Cisco Router ACL:

.May 30 12:19:17 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp attackers.com(50169) (Serial1/0 *HDLC*) -> mydns.com(53), 1 packet

.May 31 05:02:13 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp attackers.com(48736) (Serial1/0 *HDLC*) -> mydns.com(53), 1 packet

1. Source of trace:
    a. My Network
2. Detect was generated by:
    a. NAI Sniffer Pro, ISS RealSecure, and Cisco Router ACL
    b. Explanation of fields:

NAI Sniffer Trace:

Flags	Frame	Delta Time	Destination	Source	Protocol	Summary
M [B]	1	0.000.000	mydns.com	[attackers.com]	TCP	D=53 S=55692 SYN SEQ=1657845382

a. Field is pretty self-explanatory here, Source and Destination IP Address and associated ports as well as the protocol

ISS RealSecure Log:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourcePortName	DestinationPortNa
80730	25-Apr-00	DNS_Zone_High_Port	6	56145	53	56145	DNS-Xfer

a. Also, pretty self-explanatory. Source and Destination IP Address and associated ports, as well as an interpreted event description.

Cisco Router ACL:

.May 31 05:02:13 PDT: [timestamp] **%SEC-6-IPACCESSLOGP: list 150** [ACL responsible for action] **denied**[action] **tcp** [transport protocol] **attackers.com(48736)** [source address and port**] (Serial1/0 *HDLC*)** [port blocking action] -> **mydns.com(53)** [destination address and port], **1 packet**

3. Probability the source address was spoofed:

    a. Minimal, Addresses are registered to multiple ISP's

4. Description of attack:

    a. Attackers are attempting and succeeding at Zone Transfers.

5. Attack mechanism:

    a. Attackers are performing DNS Zone transfers to gain knowledge of the network. Basically gaining a complete network map of our site. This is basic pre-attack reconnaissance. P.S. – This was previous to attending SANS. This activity has been resolved through a Cisco ACL.

6. Correlations:

    a. CAN-1999-0532, ** CANDIDATE (under review) ** A DNS server allows zone transfers.
    b. I was able to identify this activity very easily after attending SANS 2000, San Jose, Ca.
    c. ISS RealSecure and Sniffer traces all corroborate this activity, Cisco ACL put in place to deny activity

7. Evidence of active targeting:

    a. These Zone Transfers targeted a specific DNS Server. Information easily gained from InterNIC.

8. Severity:

© SANS Institute 2000 - 2002, Author retains full rights.

a. (Criticality + Lethality) – (System + Countermeasures)
b. (5 + 5) – (5 + 2/5) = 10 – 7/10 = 3/0 I have included both figures for before and after comparison

9. Defense recommendation:

    a. Immediately put Cisco Router ACL in place to deny this activity. As well as blocked specific attacking IP Addresses. Granted, they still have an accurate picture of our network. Fortunately, we are in the middle of a complete network re-design with multiple firewalls and intrusion detection engines. as well as implementing a split-dns scenario.
    b. Defenses now adequate against this activity.

10. Multiple choice test question:

    a. What is the Attacker attempting to acquire from this activity

        a) DNS Zone transfer
        b) Reconnaissance
        c) Pre-attack information
        d) All of the Above

Answer : d)

Detect 2

```
05/19/2000 17:02:43.384 -     UDP packet dropped -
      Source:167.216.187.186, 1248, WAN -
      Destination:homenet.server, 15112, LAN -   -    Rule 0
05/19/2000 17:02:48.752 -     UDP packet dropped -
      Source:167.216.187.186, 1236, WAN -
      Destination:homenet.server, 15112, LAN -   -    Rule 0
05/19/2000 17:02:58.656 -     UDP packet dropped -
      Source:167.216.187.186, 1252, WAN -
      Destination:homenet.server, 15112, LAN -   -    Rule 0
05/19/2000 17:03:10.000 -     UDP packet dropped -
      Source:167.216.187.186, 1249, WAN -
      Destination:homenet.server, 15112, LAN -   -    Rule 0
05/19/2000 17:03:20.432 -     UDP packet dropped -
      Source:167.216.187.186, 1251, WAN -
      Destination:homenet.server, 15112, LAN -   -    Rule 0
05/19/2000 17:09:40.816 -     UDP packet dropped -
      Source:167.216.187.186, 1247, WAN -
      Destination:homenet.server, 15228, LAN -   -    Rule 0
05/19/2000 17:09:43.624 -     UDP packet dropped -
      Source:167.216.187.186, 1235, WAN -
      Destination:homenet.server, 15228, LAN -   -    Rule 0
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
05/19/2000 17:09:48.656 -     UDP packet dropped -
      Source:167.216.187.186, 1248, WAN -
      Destination:homenet.server, 15228, LAN -   -    Rule 0
05/19/2000 17:09:58.464 -     UDP packet dropped -
      Source:167.216.187.186, 1250, WAN -
      Destination:homenet.server, 15228, LAN -   -    Rule 0
05/19/2000 17:10:09.288 -     UDP packet dropped -
      Source:167.216.187.186, 1253, WAN -
      Destination:homenet.server, 15228, LAN -   -    Rule 0
05/19/2000 17:13:26.176 -     UDP packet dropped -
      Source:167.216.187.186, 1246, WAN -
      Destination:homenet.server, 15256, LAN -   -    Rule 0
05/19/2000 17:13:34.480 -     UDP packet dropped -
      Source:167.216.187.186, 1251, WAN -
      Destination:homenet.server, 15256, LAN -   -    Rule 0
05/19/2000 17:13:43.928 -     UDP packet dropped -
      Source:167.216.187.186, 1240, WAN -
      Destination:homenet.server, 15256, LAN -   -    Rule 0
05/19/2000 17:13:54.768 -     UDP packet dropped -
      Source:167.216.187.186, 1243, WAN -
      Destination:homenet.server, 15256, LAN -   -    Rule 0
05/19/2000 17:14:05.688 -     UDP packet dropped -
      Source:167.216.187.186, 1235, WAN -
      Destination:homenet.server, 15256, LAN -   -    Rule 0
05/19/2000 17:19:25.368 -     UDP packet dropped -
      Source:167.216.187.186, 1237, WAN -
      Destination:homenet.server, 15284, LAN -   -    Rule 0
05/19/2000 17:19:27.544 -     UDP packet dropped -
      Source:167.216.187.186, 1239, WAN -
      Destination:homenet.server, 15284, LAN -   -    Rule 0
05/19/2000 17:19:33.032 -     UDP packet dropped -
      Source:167.216.187.186, 1241, WAN -
      Destination:homenet.server, 15284, LAN -   -    Rule 0
05/19/2000 17:19:42.896 -     UDP packet dropped -
      Source:167.216.187.186, 1246, WAN -
      Destination:homenet.server, 15284, LAN -   -    Rule 0
05/19/2000 17:19:53.864 -     UDP packet dropped -
      Source:167.216.187.186, 1248, WAN -
      Destination:homenet.server, 15284, LAN -   -    Rule 0
05/19/2000 17:20:05.160 -     UDP packet dropped -
      Source:167.216.187.186, 1236, WAN -
      Destination:homenet.server, 15284, LAN -   -    Rule 0
05/19/2000 17:32:25.272 -     UDP packet dropped -
      Source:167.216.187.186, 1253, WAN -
      Destination:homenet.server, 15396, LAN -   -    Rule 0
```

1. Source of trace:

    a. My home network, DSL

2. Detect was generated by:

    b. Firewall
    c. Explanation of fields:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
05/19/2000 21:56:16.352 [timestamp] - UDP packet dropped [Action] -
Source:167.216.187.186, 1253, WAN [source address and port]-
Destination:homenet.server, 12116, LAN [destination address and port] -
-     Rule 0 [firewall rule dropping attempt]
```

3. Probability the source address was spoofed:

    a. Minimal, address is registered to digisle.net. Nothing to gain by spoofing.

4. Description of attack:

    a. Attacker is actively targeting specific destination ports from a specific range of source ports. The ISP claims that they are having problems with a Proxy Hunter type program that attempts to discover Web proxy servers throughout the world to enable faster download times. This attack probes for proxy servers in an attempt to map content, when the attacker needs content, his turnaround rate is greatly increased. Could also be used as a type of DoS, as Proxy Hunters can consume significant resources on the target system

5. Attack mechanism:

    a. Attacker scans particular ports looking for a response. If received, attacker will then attempt to exploit or utilize the system with this information. Attacker is scanning in a somewhat stealthy mode, notice timestamps per destination port scanned.

6. Correlations:

    a. This attack is very similar to the Port 7306 discussed in Stephen Northcutt's Network Intrusion analysis class, SANS2000, San Jose. (page 279)
    b. I could not find any related CVE matches.

7. Evidence of active targeting:

    a. High, attacker is hitting my ip address for specific ports.

8. Severity:

    a. $(2 + 2) – (5 + 5) = 4 – 10 = -6$

9. Defense recommendation:

    a. None, Firewall is obviously doing its job.

10. Multiple choice test question:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

b. What is the attacker attempting to gain with this activity

a) Denial of Service
b) Reconnaissance
c) Increased internet performance
d) All of the above

Answer : d)

Detect 3

Cisco Router ACL:

*Jun 4 07:15:03.140 PDT: %SEC-6-IPACCESSLOGDP: list 100 denied icmp attacker.com ((Serial1/0 *HDLC*) -> myrouter.net (8/0), 12 packets

*Jun 4 09:21:16.272 PDT: %SEC-6-IPACCESSLOGP: list 100 denied tcp attacker.com (46261) ((Serial1/0 *HDLC*) -> myrouter.net(23), 1 packet

*Jun 7 10:17:27.244 PDT: %SEC-6-IPACCESSLOGP: list 100 denied tcp attacker.com (46522) ((Serial1/0 *HDLC*) -> myrouter.net(1999), 1 packet

*Jun 7 10:48:31.676 PDT: %SEC-6-IPACCESSLOGP: list 100 denied udp attacker.com (7260) ((Serial1/0 *HDLC*) -> myrouter.net (514), 1 packet
*Jun 7 10:48:35.768 PDT: %SEC-6-IPACCESSLOGP: list 100 denied udp attacker.com (7260) ((Serial1/0 *HDLC*) -> myrouter.net (514), 1 packet

TCPDump:

07:15:42.355034 attacker.com > myrouter.net: icmp: echo request
07:15:42.356314 myrouter.net > attacker.com: icmp: host myrouter.net unreachable - admin prohibited filter
07:15:43.354578 attacker.com > myrouter.net: icmp: echo request
07:15:43.355588 myrouter.net > attacker.com: icmp: host myrouter.net unreachable - admin prohibited filter
07:15:44.355969 attacker.com > myrouter.net: icmp: echo request
07:15:44.357012 myrouter.net > attacker.com: icmp: host myrouter.net unreachable - admin prohibited filter
07:15:45.357559 attacker.com > myrouter.net: icmp: echo request
07:15:45.358579 myrouter.net > attacker.com: icmp: host myrouter.net unreachable - admin prohibited filter
07:15:47.591646 myrouter.net > attacker.com: icmp: host myrouter.net unreachable - admin prohibited filter

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

09:22:47.590452 attacker.com.1677 > myrouter.net.23: S 3497245124:3497245124(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)
09:22:50.554375 attacker.com.1677 > myrouter.net.23: S 3497245124:3497245124(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)
09:22:56.563006 attacker.com.1677 > myrouter.net.23: S 3497245124:3497245124(0) w
in 16384 <mss 1460,nop,nop,sackOK> (DF)

1. Source of trace:
    a. My Network
2. Detect was generated by:
    a. Cisco Router ACL and partial caught with TCPDump
    b. Explanation of fields:

Cisco Router ACL :

***Jun 4 09:21:16.272 PDT**: [Timestamp] **%SEC-6-IPACCESSLOGP: list 100** [ACL Responsible for Action] **denied** [Action] **tcp** [Transport Protocol] **attacker.com** (46261) [Source Address and Port] **((Serial1/0 *HDLC*)** [interface blocking activity] -> **myrouter.net(23)** [Destination Address and Port], **1 packet**

TCPDump:

07:15:47.591646 [timestamp] **myrouter.net** [Source Address] > **attacker.com**: [Destination Address] **icmp**:[transport protocol] **host myrouter.net unreachab le - admin prohibited filter** [Destination action and description]

3. Probability the source address was spoofed:
    a. Minimal, Address is registered to local ISP
4. Description of attack:
    a. Attacker is hunting for Cisco routers and is attempting to abuse some well known vulnerabilities
    b. Reconnaissance and exploitation
5. Attack mechanism:
    a. Attacker is ping local net for viable devices, routers usually live in either the high or low end of an address range. Probably determined through

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

simple nslookup or whois search to find our address space. Attacker then attempted to telnet, not sure why. Next, attacker attempts some well know port specific hacks in an attempt to down the router. Probably found these hacks on some site, and is running through the list

6. Correlations:

    a. CVE-1999-0230, Buffer overflow in Cisco 7xx routers through the telnet service
    b. CVE-1999-0063, Cisco IOS 12.0 and other versions can be crashed by malicious UDP packets to the syslog port.

7. Evidence of active targeting:

    a. This attack was from this specific host and targeted at several of our border routers

8. Severity:

    a. (5 + 2) – (5 + 4) = 7 – 9 = -2

9. Defense recommendation:

    a. Defenses are adequate. Attempt was stopped by router ACL. Potential for further exploits from this user though. Address was specifically blocked in additional ACL statement, and his ISP was notified.

10. Multiple choice test question:

    c. What is the attacker trying to gain with this type of attack scenario ?

        a) Land Attack
        b) Denial of Service
        c) Probe for Trojans
        d) Smurf

Answer : b)

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 4

NAI Sniffer Pro:

Flags	Frame	Delta Time	Destination	Source	Protocol	Summary
M [B]	1	0.000.000	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 2; 55 Bytes of data

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

# [B]	2	0.000.010	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /cgi-bin/webdist.cgi HTTP/1
[B]	3	0.000.586	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 4; 185 Bytes of dat
# [B]	4	0.000.020	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=2917 HTML Data
[B]	5	1.579.500	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 6; 56 Bytes of data
# [B]	6	0.000.009	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /cgi-bin/aglimpse.cgi HTTP/
[B]	7	0.000.586	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 8; 186 Bytes of dat
# [B]	8	0.000.019	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=2925 HTML Data
[B]	9	3.780.301	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 10; 74 Bytes of dat
# [B]	10	0.000.010	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /cgi-bin/campas?%0acat%0
[B]	11	0.000.474	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 12; 204 Bytes of da
# [B]	12	0.000.021	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=2931 HTML Data
[B]	13	3.479.007	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 14; 46 Bytes of dat
# [B]	14	0.000.008	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /cgi-bin/jj HTTP/1.0
[B]	15	0.000.543	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 16; 176 Bytes of da
# [B]	16	0.000.020	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=2939 HTML Data
[B]	17	2.669.602	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 18; 52 Bytes of dat
# [B]	18	0.000.009	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /cgi-bin/formmail HTTP/1.0
[B]	19	0.000.601	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 20; 182 Bytes of da
# [B]	20	0.000.019	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=2942 HTML Data

Flags	Frame	Delta Time	Destination	Source	Protocol	Summary
M [B]	1	0.000.000	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 2; 71 Bytes of data
# [B]	2	0.000.010	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /scripts/samples/search/file
[B]	3	0.000.658	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 4; 201 Bytes of dat
# [B]	4	0.000.020	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3022 HTML Data
[B]	5	1.890.408	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 6; 68 Bytes of data
# [B]	6	0.000.010	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /scripts/samples/search/que
[B]	7	0.000.371	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 8; 198 Bytes of dat
# [B]	8	0.000.020	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3028 HTML Data
[B]	9	4.578.095	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 10; 71 Bytes of dat
# [B]	10	0.000.010	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /scripts/samples/search/que
[B]	11	0.000.983	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 12; 201 Bytes of da
# [B]	12	0.000.021	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3033 HTML Data
[B]	13	2.518.870	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 14; 69 Bytes of dat
# [B]	14	0.000.011	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /scripts/samples/search/sim
[B]	15	0.000.667	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 16; 199 Bytes of da
# [B]	16	0.000.020	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3038 HTML Data
[B]	17	3.039.926	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 18; 71 Bytes of dat
# [B]	18	0.000.011	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /scripts/samples/search/qfu
[B]	19	0.000.666	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 20; 201 Bytes of da
# [B]	20	0.000.021	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3042 HTML Data

Flags	Frame	Delta Time	Destination	Source	Protocol	Summary
M [B]	1	0.000.000	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 2; 56 Bytes of data
[B]	2	0.000.010	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /cgi-bin/windmail.exe HTTP
[B]	3	0.000.667	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 4; 186 Bytes of dat
[B]	4	0.000.020	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3127 HTML Data
[B]	5	0.728.046	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 6; 54 Bytes of data
[B]	6	0.000.009	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /_vti_bin/shtml.dll HTTP/1.0

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[B]	7 0.000.639	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 8; 184 Bytes of dat
[B]	8 0.000.019	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3136 HTML Data
[B]	9 2.171.383	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 10; 45 Bytes of dat
[B]	10 0.000.009	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /.htaccess HTTP/1.0
[B]	11 0.000.597	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 12; 175 Bytes of da
[B]	12 0.000.019	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3140 HTML Data
[B]	13 2.708.750	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 14; 57 Bytes of dat
[B]	14 0.000.009	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /_vti_pvt/doctodep.btr HTTP
[B]	15 0.000.526	[62.125.8.xx]	[mywebsite.com]	TCP	Retransmitted in frame 16; 187 Bytes of da
[B]	16 0.000.019	[62.125.8.xx]	[mywebsite.com]	HTTP	R Port=3145 HTML Data

ISS RealSecure:

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	Des
511346	07-Jun-00	HTTP_Shells	6	2586	80	62.125.8.xx	myw
511351	07-Jun-00	HTTP_Shells	6	2592	80	62.125.8.xx	myw
511362	07-Jun-00	HTTP_Shells	6	2598	80	62.125.8.xx	myw
511399	07-Jun-00	HTTP_Shells	6	2625	80	62.125.8.xx	myw
511415	07-Jun-00	HTTP_IISExAir_DoS	6	2689	80	62.125.8.xx	myw

© SANS Institute 2000 - 2002, Author retains full rights.

511422	07-Jun-00	HTTP_Netscape_PageServices	6	2756	80	62.125.8.xx	myw
511423	07-Jun-00	HTTP_Netscape_SpaceView	6	2766	80	62.125.8.xx	myw
511426	07-Jun-00	HTTP_IE_BAT	6	2806	80	62.125.8.xx	myw
511427	07-Jun-00	HTTP_WebSite_Uploader	6	2814	80	62.125.8.xx	myw
511428	07-Jun-00	HTTP_TestCgi	6	2832	80	62.125.8.xx	myw
511432	07-Jun-00	HTTP_Shells	6	2878	80	62.125.8.xx	myw
511433	07-Jun-00	HTTP_PHF	6	2901	80	62.125.8.xx	myw

© SANS Institute 2000 - 2002, Author retains full rights.

511435	07-Jun-00	HTTP_NphTestCgi	6	2912	80	62.125.8.xx	myw
511436	07-Jun-00	HTTP_Campas	6	2931	80	62.125.8.xx	myw
511437	07-Jun-00	HTTP_Unix_Passwords	6	2931	80	62.125.8.xx	myw
511439	07-Jun-00	HTTP_FaxSurvey	6	2954	80	62.125.8.xx	myw
511440	07-Jun-00	HTTP_Unix_Passwords	6	2954	80	62.125.8.xx	myw

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

511441	07-Jun-00	HTTP_SCO_View-Source	6	2959	80	62.125.8.xx	myw
511442	07-Jun-00	HTTP_Unix_Passwords	6	2959	80	62.125.8.xx	myw
511443	07-Jun-00	HTTP_Unix_Passwords	6	2986	80	62.125.8.xx	myw
511445	07-Jun-00	HTTP_RobotsTxt	6	3057	80	62.125.8.xx	myw
511446	07-Jun-00	HTTP_IE_BAT	6	3062	80	62.125.8.xx	myw

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

511447	07-Jun-00	HTTP_IE_BAT	6	3067	80	62.125.8.xx	myw
511448	07-Jun-00	HTTP_Unix_Passwords	6	3072	80	62.125.8.xx	myw
511449	07-Jun-00	HTTP_Unix_Passwords	6	3076	80	62.125.8.xx	myw
511450	07-Jun-00	HTTP_Unix_Passwords	6	3084	80	62.125.8.xx	myw

© SANS Institute 2000 - 2002, Author retains full rights.

511451	07-Jun-00	HTTP_Unix_Passwords	6	3115	80	62.125.8.xx	myw
511452	07-Jun-00	HTTP_IE_BAT	6	3123	80	62.125.8.xx	myw

1. Source of trace:
    a. My Network
2. Detect was generated by:
    b. ISS and NAI Sniffer Pro
    c. Explanation of fields:

NAI Sniffer Pro:

Flags	Frame	Delta Time	Destination	Source	Protocol	Summary
M [B]	1	0.000.000	[mywebsite.com]	[62.125.8.xx]	TCP	Retransmitted in frame 2; 55 Bytes of data
# [B]	2	0.000.010	[mywebsite.com]	[62.125.8.xx]	HTTP	C Port=0 GET /cgi-bin/webdist.cgi HTTP/1

Pretty self-explanatory, Destination and Source address, Protocol, and payload.

ISS RealSecure:

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddressNa
511346	07-Jun-00	HTTP_Shells	6	2586	80	62.125.8.xx	mywebsite.com

Also pretty self-explanatory, Date, Event Name decode, transport protocol, source and destination ports and addresses, as well as payload.

3. Probability the source address was spoofed:

© SANS Institute 2000 - 2002, Author retains full rights.

a. Minimal, Address is registered to U.K. ISP
b. **inetnum: 62.124.0.0 - 62.126.255.255**
netname: UK-PIPEX-990714
descr: UUNET PIPEX (Formerly PIPEX)
descr: PROVIDER
country: GB
admin-c: SB855-RIPE
admin-c: UPHM1-RIPE
tech-c: UPHM1-RIPE
status: ALLOCATED PA
remarks: Please send abuse notification to abuse@uk.uu.net
notify: routing@uk.uu.net
mnt-by: RIPE-NCC-HM-MNT
changed: hostmaster@ripe.net 19990714
changed: hostmaster@ripe.net 19991004
changed: hostmaster@ripe.net 20000229
source: RIPE

4. Description of attack:

    a. Attacker is running through known CGI and some asp exploits for multiple platforms.

5. Attack mechanism:

    a. Attacker, script kiddie, is probably running some sort of CGI probe script. The timestamps indicate that this is a pre-generated, and not manual attack. When attacker receives a response to any of the CGI vulnerabilities, they can use this information to gain passwords and control of the web server.

6. Correlations:

    a. These are all covered by CVE.

7. Evidence of active targeting:

    a. No question. The attacker is targeting a virtual address of our known web site.

8. Severity:

    a. (4 + 3) – (5 + 4) = 7 – 9 = -2

9. Defense recommendation:

© SANS Institute 2000 - 2002, Author retains full rights.

a. Web servers are not susceptible to these attacks, this directory structure does not exist.
b. Router ACL immediately put in place to block IP address of attacker.
c. ISP notified of questionable activity.

10. Multiple choice test question:

a. What is the attacker attempting to gain with these attack signatures ?

a) Server passwords.
b) Startup permissions
c) Database passwords
d) All of the Above

Answer : d)

Detect 5

```
05/10/2000 23:59:00.128 -     TCP connection dropped -
      Source:209.162.200.64,
63625, WAN -      Destination:homenet.server, 251, LAN -     -    Rule
0
05/10/2000 23:59:00.128 -     TCP connection dropped -
      Source:209.162.200.64,
63626, WAN -      Destination:homenet.server, 540, LAN -    'UUCP' -
      Rule 0
05/10/2000 23:59:00.144 -     TCP connection dropped -
      Source:209.162.200.64,
63627, WAN -      Destination:homenet.server, 1420, LAN -   'Timbuktu'
-     Rule 0
05/10/2000 23:59:00.144 -     TCP connection dropped -
      Source:209.162.200.64,
63628, WAN -      Destination:homenet.server, 79, LAN -     'Finger' -
      Rule 0
05/10/2000 23:59:00.160 -     TCP connection dropped -
      Source:209.162.200.64,
63629, WAN -      Destination:homenet.server, 1385, LAN -    -    Rule
0
05/10/2000 23:59:00.160 -     TCP connection dropped -
      Source:209.162.200.64,
63630, WAN -      Destination:homenet.server, 197, LAN -     -    Rule
0
05/10/2000 23:59:00.176 -     TCP connection dropped -
      Source:209.162.200.64,
63631, WAN -      Destination:homenet.server, 1178, LAN -    -    Rule
0
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
05/10/2000 23:59:00.176 -     TCP connection dropped -
      Source:209.162.200.64,
63632, WAN -      Destination:homenet.server, 40, LAN -      -    Rule
0
05/10/2000 23:59:00.192 -     TCP connection dropped -
      Source:209.162.200.64,
63633, WAN -      Destination:homenet.server, 485, LAN -     -    Rule
0
05/10/2000 23:59:00.192 -     TCP connection dropped -
      Source:209.162.200.64 ,
63634, WAN -      Destination:homenet.server, 421, LAN -     -    Rule
0
05/10/2000 23:59:00.208 -     TCP connection dropped -
      Source:209.162.200.64,
63635, WAN -      Destination:homenet.server, 1662, LAN -    -    Rule
0
05/10/2000 23:59:00.208 -     TCP connection dropped -
      Source:209.162.200.64 ,
63636, WAN -      Destination:homenet.server, 800, LAN -     -    Rule
0
05/10/2000 23:59:00.224 -     TCP connection dropped -
      Source:209.162.200.64,
63637, WAN -      Destination:homenet.server, 1437, LAN -    -    Rule
0
05/10/2000 23:59:00.240 -     TCP connection dropped -
      Source:209.162.200.64,
63638, WAN -      Destination:homenet.server, 1025, LAN -    -    Rule
0
05/10/2000 23:59:00.256 -     TCP connection dropped -
      Source:209.162.200.64,
63639, WAN -      Destination:homenet.server, 808, LAN -     -    Rule
0
05/10/2000 23:59:00.256 -     TCP connection dropped -
      Source:209.162.200.64,
63640, WAN -      Destination:homenet.server, 1010, LAN -    -    Rule
0
05/10/2000 23:59:00.256 -     TCP connection dropped -
      Source:209.162.200.64,
63641, WAN -      Destination:homenet.server, 1524, LAN -    -    Rule
0
```

1. Source of trace:
    a. My home network, DSL
2. Detect was generated by:
    a. WebRamp 700s
    b. Explanation of fields:

05/10/2000 23:59:00.256 [timestamp] - **TCP connection dropped** [Action] - **Source:209.162.200.64,** **63641, WAN** [source address and port]- **Destination:homenet.server,** **1524, LAN** [destination address and port] - - **Rule 0** [firewall rule dropping attempt]

© SANS Institute 2000 - 2002, Author retains full rights.

3. Probability the source address was spoofed:

    a. Minimal, address is registered to EasyStreet Online Services Inc., same ISP.

4. Description of attack:

    a. Attacker is scanning well known ports for back doors, and vulnerabilities. Notice the sequential source ports, and timestamps.

5. Attack mechanism:

    a. Attacker scans particular ports looking for a response. If received, attacker will then attempt to exploit the system with this information.

6. Correlations:

    a. Scanning took place twice during the day

7. Evidence of active targeting:

a. High, attacker is hitting my ip address for random (well known) ports, with sequential source port numbers

8. Severity:

a. (2 + 1) – (5 + 5) = 3 – 10 = -7

9. Defense recommendation:

a. None, Firewall is obviously doing its job

10. Multiple choice test question:

    a. What best describes the methodology of this type of attack

        a) Scan for Trojans
        b) DoS
        c) Teardrop attack
        d) Land Attack

Answer : a)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect 6

ISS Real Secure:

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddress
59463	13-Jun-00	Port_Scan	6	29294	628	attacker.com	router1.com
59464	13-Jun-00	Port_Scan	6	29298	629	attacker.com	Router4.com
ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddress
59480	13-Jun-00	UDP_Port_Scan	17	53	933	router1.com	attacker.com

WINDump:

09:04:52.419494 dwallace.800.com > 199.2.223.252: icmp: echo request
09:04:52.419710 dwallace.800.com > router2.com: icmp: echo request
09:04:52.419868 dwallace.800.com > router1.com: icmp: echo request
09:04:52.420023 dwallace.800.com > router3.com: icmp: echo request
09:04:52.421233 router2.com > dwallace.800.com: icmp: echo reply
09:04:52.421451 router1.com > dwallace.800.com: icmp: echo reply
09:04:52.421871 199.2.223.252 > dwallace.800.com: icmp: echo reply
09:04:52.426287 dwallace.800.com.4606 > router2.com.600: S 484347757:484347757
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.426915 dwallace.800.com.4607 > router1.com.600: S 484398277:484398277
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.427137 router2.com.600 > dwallace.800.com.4606: R 0:0(0) ack 48434775
8 win 0
09:04:52.427580 dwallace.800.com.4608 > 199.2.223.252.600: S 484443545:484443545
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.428144 router1.com.600 > dwallace.800.com.4607: R 0:0(0) ack 48439827
8 win 0
09:04:52.428622 router4.com > dwallace.800.com: icmp: redirect 199.2.223.252 to
host router4.com
09:04:52.500275 router3.com > dwallace.800.com: icmp: echo reply
09:04:52.501549 dwallace.800.com.4609 > router3.com.600: S 484524059:484524059
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.502440 router3.com.600 > dwallace.800.com.4609: R 0:0(0) ack 48452406
0 win 0
09:04:52.627787 dwallace.800.com.4610 > router2.com.601: S 484589077:484589077
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.628660 router2.com.601 > dwallace.800.com.4610: R 0:0(0) ack 48458907
8 win 0
09:04:52.629503 dwallace.800.com.4611 > router1.com.601: S 484641336:484641336
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.630004 dwallace.800.com.4612 > 199.2.223.252.601: S 484683757:484683757
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.630537 router1.com.601 > dwallace.800.com.4611: R 0:0(0) ack 48464133
7 win 0
09:04:52.631047 router4.com > dwallace.800.com: icmp: redirect 199.2.223.252 to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

host router4.com
09:04:52.702833 dwallace.800.com.4613 > router3.com.601: S 484762197:484762197
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.703645 router3.com.601 > dwallace.800.com.4613: R 0:0(0) ack 48476219
8 win 0
09:04:52.829321 dwallace.800.com.4614 > router2.com.602: S 484832046:484832046
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.830201 router2.com.602 > dwallace.800.com.4614: R 0:0(0) ack 48483204
7 win 0
09:04:52.831681 dwallace.800.com.4615 > router1.com.602: S 484873222:484873222
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.832188 dwallace.800.com.4616 > 199.2.223.252.602: S 484919921:484919921
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.832724 router1.com.602 > dwallace.800.com.4615: R 0:0(0) ack 48487322
3 win 0
09:04:52.833237 router4.com > dwallace.800.com: icmp: redirect 199.2.223.252 to
host router4.com
09:04:52.904453 dwallace.800.com.4617 > router3.com.602: S 485006419:485006419
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:52.905168 router3.com.602 > dwallace.800.com.4617: R 0:0(0) ack 48500642
0 win 0
09:04:53.030903 dwallace.800.com.4618 > router2.com.603: S 485095857:485095857
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:53.031772 router2.com.603 > dwallace.800.com.4618: R 0:0(0) ack 48509585
8 win 0
09:04:53.033118 dwallace.800.com.4619 > router1.com.603: S 485150417:485150417
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:53.033942 dwallace.800.com.4620 > 199.2.223.252.603: S 485189935:485189935
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:53.034150 router1.com.603 > dwallace.800.com.4619: R 0:0(0) ack 48515041
8 win 0
09:04:53.035101 router4.com > dwallace.800.com: icmp: redirect 199.2.223.252 to
host router4.com
09:04:53.106082 dwallace.800.com.4621 > router3.com.603: S 485261927:485261927
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:53.106860 router3.com.603 > dwallace.800.com.4621: R 0:0(0) ack 48526192
8 win 0
09:04:53.232506 dwallace.800.com.4622 > router2.com.604: S 485325316:485325316
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:53.233440 router2.com.604 > dwallace.800.com.4622: R 0:0(0) ack 48532531
7 win 0
09:04:53.234495 dwallace.800.com.4623 > router1.com.604: S 485369048:485369048
(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
09:04:53.235394 router1.com.604 > dwallace.800.com.4623: R 0:0(0) ack 48536904
9 win 0

Cisco Router ACL:

*Jun 8 06:19:04.439 PDT: %SEC-6-IPACCESSLOGDP: list 150 denied icmp attacker1.com (ATM1/0 VC 1) -> router1.com (0/0), 1 packet
*Jun 8 06:19:07.315 PDT: %SEC-6-IPACCESSLOGDP: list 150 denied icmp attacker.com (ATM1/0 VC 1) -> router4.com (0/0), 1 packet

1. Source of trace:

© SANS Institute 2000 - 2002, Author retains full rights.

a. My network

2. Detect was generated by:

b. ISS RealSecure and WINDump
c. Explanation of fields:

ISS RealSecure:

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddressNar
59463	13-Jun-00	Port_Scan	6	29294	628	attacker.com	router1.com

Event ID, Event date, Decode of attack signature, protocol ID Source and Destination address and port

WINDump:

09:04:52.426287 [Timestamp] dwallace.800.com.4606 [Source address and port] > router2.com.600: [Destination address and port] S 484347757:484347757(0) [Sequence #] win 16384 [window size] <mss 1460,nop,nop,sackOK> (DF) [options]

Cisco Router ACL:

***Mar 1 20:34:42.968 PST** [Timestamp] : **%SEC-6-IPACCESSLOGDP: list 150** [ACL responsible for action] **denied** [Action] **icmp** [Transport protocol] **Attacker.com** [Source address] **(ATM1/0 VC 1)** [Interface blocking action] -> **router1.com (8/0)** [Destination address], **24 packets**

3. Probability the source address was spoofed:

a. Minimal, address is registered to local ISP

4. Description of attack:

a. Attacker is scanning for devices with ping sweeps, and then performing port scans on these devices.

5. Attack mechanism:

a. Attacker first runs a ping sweep to locate active devices on a network. Basic reconnaissance work. Attacker then determines if there are any potential ports to exploit on these devices via a port scan. Obviously the attacker is using a script or program to perform this sweep judging by the timestamps.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6. Correlations:

    a. Attack was recognized by both ISS and captured with a sniffer.
    b. I see this sort of activity quite often, as do most everyone.

7. Evidence of active targeting:

    a. Attacker has definitely done some previously undetected reconnaissance. Attacker is targeting very specific devices for their scan.

8. Severity:

    a. (5 + 3) – (5 + 4) = 8 – 9 = -1

9. Defense recommendation:

    a. Router ACL has been put in place to hinder this activity.
    b. Specific IP address has been blocked by ACL entry.
    c. ISP has been contacted and made aware of this users activity.

10. Multiple choice test question:

    a. This attack can be characterized as?

        a) Pre-attack reconnaissance
        b) Land Attack
        c) Smurf
        d) Spoof

Answer: a)

Detect 7

EventDate	EventName	ProtocolID	SourcePort	DestinationPort	DestinationPortName	Sourc
5/19/2000 8:37	HTTP_IE_BAT	6	1089	80	HTTP	194.1
5/19/2000 8:37	HTTP_WebSite_Uploader	6	1092	80	HTTP	194.1
5/19/2000 8:37	HTTP_IE_BAT	6	1098	80	HTTP	194.1
5/19/2000 8:37	HTTP_WebSite_Uploader	6	1099	80	HTTP	194.1
5/19/2000 8:38	HTTP_IE_BAT	6	1102	80	HTTP	194.1
5/19/2000 8:38	HTTP_WebSite_Uploader	6	1104	80	HTTP	194.1
5/19/2000 8:38	HTTP_Netscape_SpaceView	6	1106	80	HTTP	194.1
5/19/2000 8:38	HTTP_Netscape_SpaceView	6	1117	80	HTTP	194.1
5/19/2000 8:40	HTTP_Netscape_PageServices	6	1122	80	HTTP	194.1
5/19/2000 8:40	HTTP_Netscape_PageServices	6	1129	80	HTTP	194.1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5/19/2000 8:46	HTTP_IE_BAT	6	1349	80	HTTP	194.1
5/19/2000 8:46	HTTP_WebSite_Uploader	6	1352	80	HTTP	194.1
5/19/2000 8:46	HTTP_IE_BAT	6	1354	80	HTTP	194.1
5/19/2000 8:46	HTTP_WebSite_Uploader	6	1355	80	HTTP	194.1
5/19/2000 8:46	HTTP_IE_BAT	6	1359	80	HTTP	194.1
5/19/2000 8:46	HTTP_WebSite_Uploader	6	1363	80	HTTP	194.1
5/19/2000 8:48	HTTP_Netscape_SpaceView	6	1372	80	HTTP	194.1
5/19/2000 8:48	HTTP_Netscape_SpaceView	6	1377	80	HTTP	194.1
5/19/2000 8:49	HTTP_IIS$DATA	6	1387	80	HTTP	194.1
5/19/2000 8:49	HTTP_IIS$DATA	6	1389	80	HTTP	194.1
5/19/2000 8:49	HTTP_IIS$DATA	6	1392	80	HTTP	194.1
5/19/2000 8:49	HTTP_Netscape_PageServices	6	1393	80	HTTP	194.1
5/19/2000 8:49	HTTP_Netscape_PageServices	6	1396	80	HTTP	194.1
5/19/2000 8:50	HTTP_Netscape_PageServices	6	1399	80	HTTP	194.1
5/19/2000 8:50	HTTP_Netscape_SpaceView	6	1402	80	HTTP	194.1
5/19/2000 8:50	HTTP_FaxSurvey	6	1403	80	HTTP	194.1
5/19/2000 8:50	HTTP_FaxSurvey	6	1405	80	HTTP	194.1
5/19/2000 8:52	HTTP_WebFinger	6	1422	80	HTTP	194.1
5/19/2000 8:52	HTTP_IE_BAT	6	1425	80	HTTP	194.1
5/19/2000 8:52	HTTP_WebFinger	6	1427	80	HTTP	194.1
5/19/2000 8:52	HTTP_IE_BAT	6	1429	80	HTTP	194.1
5/19/2000 8:52	HTTP_WebFinger	6	1431	80	HTTP	194.1
5/19/2000 8:52	HTTP_IE_BAT	6	1433	80	HTTP	194.1
5/19/2000 8:54	HTTP_Unix_Passwords	6	1452	80	HTTP	194.1
5/19/2000 8:54	HTTP_WebFinger	6	1454	80	HTTP	194.1
5/19/2000 8:54	HTTP_Unix_Passwords	6	1457	80	HTTP	194.1
5/19/2000 8:54	HTTP_Novell_Files	6	1460	80	HTTP	194.1
5/19/2000 8:54	HTTP_WebFinger	6	1461	80	HTTP	194.1
5/19/2000 8:54	HTTP_Unix_Passwords	6	1465	80	HTTP	194.1
5/19/2000 8:54	HTTP_Novell_Files	6	1467	80	HTTP	194.1
5/19/2000 8:54	HTTP_WebFinger	6	1468	80	HTTP	194.1
5/19/2000 8:55	HTTP_Novell_Files	6	1473	80	HTTP	194.1
5/19/2000 8:56	HTTP_Netscape_SpaceView	6	1478	80	HTTP	194.1
5/19/2000 8:58	HTTP_Netscape_SpaceView	6	1491	80	HTTP	194.1
5/19/2000 9:04	HTTP_IE_BAT	6	1541	80	HTTP	194.1
5/19/2000 9:04	HTTP_IE_BAT	6	1542	80	HTTP	194.1
5/19/2000 9:04	HTTP_IE_BAT	6	1545	80	HTTP	194.1
5/19/2000 9:06	HTTP_TestCgi	6	1571	80	HTTP	194.1
5/19/2000 9:06	HTTP_TestCgi	6	1595	80	HTTP	194.1
5/19/2000 9:07	HTTP_TestCgi	6	1606	80	HTTP	194.1

1. Source of trace:
    a. My network
2. Detect was generated by:

© SANS Institute 2000 - 2002, Author retains full rights.

a. ISS RealSecure and NAI Sniffer traces
b. Explanation of fields:

ISS database logs pretty self-explanatory, typical date, time, description of attack, port numbers, source and destination addresses, as well as the raw data

3. Probability the source address was spoofed:

    a. Possible, but not likely. Address registered to 194.158.192.0 - 194.158.193.255(BELPAK) Republican Association BELTELECOM; Minsk; Republic of Belarus; BY

4. Description of attack:

    a. Attacker has obviously not done any reconnaissance work as they are running the gamut (Win, IIS, UNIX, Novell, etc.) CGI hacks.

5. Attack mechanism:

    a. This one was right after returning from the conference…Attacker basically just running through the international hacking playbook . Just a script kiddie.

6. Correlations:

    a. Most of these are cataloged at CVE

7. Evidence of active targeting:

    a. Most definitely, attacker is targeting known web server address

8. Severity:

a. $(5 + 2) – (5 + 3/4) = -1/-2$

9. Defense recommendation:

a. Defenses for this attack are fine. None of the attempted hacks were viable for our web server configuration. ACL was generated to block the IP address. We are in the process of automating this procedure.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10. Multiple choice test question:

    a. What is the attacker attempting to exploit ?

        a) POP
        b) CGI
        c) Telnet
        d) Buffer Overflow

Answer: b)

Detect 8

.May 22 11:20:50 PDT: %SEC-6-IPACCESSLOGDP: list 150 denied icmp 172.22.22.81 (Serial1/0 *HDLC*) -> mydns.com (4/0), 1 packet

.May 22 11:27:52 PDT: %SEC-6-IPACCESSLOGDP: list 150 denied icmp 172.22.22.81 (Serial1/0 *HDLC*) -> mydns.com (4/0), 2 packets

1. Source of trace:

    a. My Network

2. Detect was generated by:

    b. Cisco Router ACL
    c. Explanation of fields:

. **May 22 11:27:52 PDT**: [Timestamp] %**SEC-6-IPACCESSLOGDP: list 150** [ACL responsible for action] **denied** [Action] icmp [transport protocol] 172.22.22.81 [Source Address] **(Serial1/0 *HDLC*)** [Interface ACL triggered on] -> **mydns.com (4/0)** [Destination address and action], **2 packets**

3. Probability the source address was spoofed:

    a. Most likely, IANA networks are reserved and therefore, not routed on the Internet.

4. Description of attack:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

a. Attackers are scanning for DNS servers.
b. Most likely reconnaissance work.

5. Attack mechanism:

    a. Attacker is attempting to scan for DNS servers. Attacker then attempts host lookups or zone transfers. Obviously a crafted packet. Not sure what they are gaining with IANA addressing, as they would not receive any response. Possible pre-DoS activity.

6. Correlations:

    a. This attack was discussed in length at SANS 2000, San Jose, Ca.

7. Evidence of active targeting:

    a. Attack is targeting name servers

8. Severity:

    a. (5 + 2) – (5 + 5) = 7 – 10 = -3

9. Defense recommendation:

    a. None, attempt blocked by border router ACL.

10. Multiple choice test question:

    a. What can the trace provide this hacker?

        a) Network Mapping
        b) DNS buffer overflow
        c) Nothing
        d) DNS Zone transfer

Answer: d)

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 9

.May 22 11:17:17 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.0.1.10(3401) (Serial1/0 *HDLC*) -> mywebsite.com(80), 1 packet

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

.May 22 11:18:34 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.0.1.10(3420) (Serial1/0 *HDLC*) -> mywebsite.com(80), 1 packet

.May 22 11:20:34 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.0.1.10(4121) (Serial1/0 *HDLC*) -> mywebsite.com(80), 1 packet

.May 22 11:22:34 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.0.1.10(3598) (Serial1/0 *HDLC*) -> mywebsite.com(80), 1 packet

.May 22 11:24:34 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.0.1.10(3757) (Serial1/0 *HDLC*) -> mywebsite.com(80), 1 packet

.May 22 11:30:34 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.0.1.10(4345) (Serial1/0 *HDLC*) -> mywebsite.com(80), 1 packet

.May 22 11:34:34 PDT: %SEC-6-IPACCESSLOGP: list 150 denied tcp 10.0.1.10(3499) (Serial1/0 *HDLC*) -> mywebsite.com(80), 1 packet

1. Source of trace:

    d. My network

2. Detect was generated by:

    a. Cisco Router ACL
    b. Explanation of fields:

.May 22 11:34:34 PDT: [timestamp] **%SEC-6-IPACCESSLOGP: list 150** [ACL responsible for action] **denied** [action] **tcp** [transport protocol] **10.0.1.10(0)** [source address and port] **(Serial1/0 *HDLC*)** [port blocking action]-> **mywebsite.com0(0)** [destination address and port], **1 packet**

3. Probability the source address was spoofed:

    a. Definitely, 10.0.0.0 networks are reserved and therefore, not routed on the Internet.

4. Description of attack:

© SANS Institute 2000 - 2002, Author retains full rights.

a. Most likely, reconnaissance to determine host, judging by the timestamps. Host is web server. Looking for web servers.
b. Potentially running a script spidering the web site, and collecting URL's. when images are called from image server, it is sending them "nowhere" 10.0.0.X speeding up transfer of website URL's

5. Attack mechanism:

   a. Attacker is attempting to find Web Servers for any number of exploits on them.
   b. Attacker using TCP 3-way handshake to locate servers on port 80

6. Correlations:

   a. This type of scan was covered in depth at the SANS2000, San Jose, Ca.

7. Evidence of active targeting:

   a. This server is an active web server and was the only system, out of many web servers, that was targeted.

8. Severity:

   a. (5 + 1) – (5 + 5) = 6 – 10 = -4

9. Defense recommendation:

   a. None, Router ACL blocking these attempts.

10. Multiple choice test question:

    a. What Cisco Access List statement will block this activity?

       a) access-list 249 deny ip 10.0.0.0 255.255.255.0 any
       b) access-list 150 deny ip 10.0.0.0 255.255.255.0 any
       c) access-list 160 deny ip 10.0.0.0 0.255.255.255 any
       d) access-list 249 deny ip any 10.0.0.0 0.255.255.255

Answer: b)

Detect 10 (Not really an attack, but a potential hole in internal security)

© SANS Institute 2000 - 2002, Author retains full rights.

Cisco router ACL:

.May 22 09:16:41 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.199(2301) (FastEthernet0/0 0008.c7cf.eab8) -> 255.255.255.255(2301), 1 packet
.May 22 09:16:42 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.239(2301) (FastEthernet0/0 0008.c7e6.e49f) -> 255.255.255.255(2301), 1 packet
.May 22 09:16:48 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.193(2301) (FastEthernet0/0 0008.c7b1.5500) -> 255.255.255.255(2301), 1 packet
.May 22 09:16:50 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.248(2301) (FastEthernet0/0 0050.8b6f.7789) -> 255.255.255.255(2301), 1 packet
.May 22 09:16:56 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.241(2301) (FastEthernet0/0 0050.8b6f.46f9) -> 255.255.255.255(2301), 1 packet
.May 22 09:16:59 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.214(2301) (FastEthernet0/0 0008.c7cf.3621) -> 255.255.255.255(2301), 1 packet
.May 22 09:17:02 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.103(2301) (FastEthernet0/0 0008.c7fa.cef4) -> 255.255.255.255(2301), 1 packet
.May 22 09:17:04 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.240(2301) (FastEthernet0/0 0008.c7e6.e4ab) -> 255.255.255.255(2301), 1 packet
.May 22 09:17:10 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.230(2301) (FastEthernet0/0 0080.5f9f.a977) -> 255.255.255.255(2301), 1 packet
.May 22 09:17:13 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.227(2301) (FastEthernet0/0 0008.c7b1.bd8f) -> 255.255.255.255(2301), 1 packet
.May 22 09:17:16 PDT: %SEC-6-IPACCESSLOGP: list 162 denied udp 172.16.0.196(2301) (FastEthernet0/0 0080.5f9f.fb2e) -> 255.255.255.255(2301), 1 packet

NAI Sniffer trace:

Flags	Frame	Delta Time	Destination	Source	Protocol	Summary
[B]	19	0.923.885	[255.255.255.255]	[172.16.0.230]	UDP	D=2301 S=2301 LEN=20
[B]	29	0.641.860	[255.255.255.255]	[172.16.0.188]	UDP	D=2301 S=2301 LEN=20
[B]	37	0.631.021	[255.255.255.255]	[172.16.0.214]	UDP	D=2301 S=2301 LEN=20
[B]	47	0.331.448	[255.255.255.255]	[172.16.0.237]	UDP	D=2301 S=2301 LEN=20
[B]	53	0.061.213	[255.255.255.255]	[172.16.0.196]	UDP	D=2301 S=2301 LEN=20
[B]	69	0.896.923	[255.255.255.255]	[172.16.0.227]	UDP	D=2301 S=2301 LEN=20
[B]	71	0.103.673	[255.255.255.255]	[172.16.0.244]	UDP	D=2301 S=2301 LEN=20
[B]	73	0.441.539	[255.255.255.255]	[172.16.0.242]	UDP	D=2301 S=2301 LEN=20

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[B] 75 0.521.667 [255.255.255.255] [172.16.0.229] UDP D=2301 S=2301 LEN=20

WINDump:

10:51:45.302939 ns.800.com.2301 > 255.255.255.255.2301: udp 212

10:51:45.662812 WWW2.2301 > 255.255.255.255.2301: udp 212

10:51:45.827885 10.0.0.2.2301 > 255.255.255.255.2301: udp 12

10:51:46.458587 10.0.0.2.2301 > 255.255.255.255.2301: udp 12

10:51:48.616047 STAGING.2301 > 255.255.255.255.2301: udp 212

10:51:48.775325 DB4.2301 > 255.255.255.255.2301: udp 212

10:51:49.105957 WWW8.2301 > 255.255.255.255.2301: udp 212

10:51:53.458637 DB5B.2301 > 255.255.255.255.2301: udp 212

10:51:54.274174 DEVDB.2301 > 255.255.255.255.2301: udp 212

10:51:54.408180 NPDB.2301 > 255.255.255.255.2301: udp 212

10:51:54.492789 prestage.800.com.2301 > 255.255.255.255.2301: udp 212

10:51:54.650420 DB2.2301 > 255.255.255.255.2301: udp 212

10:51:54.910051 NP.2301 > 255.255.255.255.2301: udp 212

10:51:56.305589 WWW14.2301 > 255.255.255.255.2301: udp 212

10:51:57.871609 MAIL2.2301 > 255.255.255.255.2301: udp 212

10:51:58.252335 WWW10.2301 > 255.255.255.255.2301: udp 212

10:51:58.977734 wc.800.com.2301 > 255.255.255.255.2301: udp 212

1. Source of trace:
    a. My network
2. Detect was generated by:
    a. Cisco router ACL's, NAI Sniffer Pro, WINDump

© SANS Institute 2000 - 2002, Author retains full rights.

b. Explanation of fields:

Cisco ACL:
.**May 22 09:16:41 PDT**:[timestamp] %**SEC-6-IPACCESSLOGP: list 162**[ACL responsible for action] **denied**[action] **udp**[transport protocol] **172.16.0.199(2301)** [source address and port] **(FastEthernet0/0 0008.c7cf.eab8)** [port blocking action] **-> 255.255.255.255(2301)** [destination address and port], **1 packet**

NAI Sniffer:
Pretty self-explanatory.

WINDump:
Also, pretty self-explanatory.

3. Probability the source address was spoofed:

    a. Low, although initially I suspected they could be.
    b. Addresses were mapped to internally controlled systems.

4. Description of attack:

    a. ACL drops were not understood as these systems reside behind a firewall using NAT to a public address (Yes Stephen, we turned in our un-needed class c's), (possible spoof). Put a sniffer on the network and found these UDP packets were all being sent to UDP:2301, although not enough to implicate any type of DOS. I found that this actually turned out to be a bug with Compaq insite manager. It was residing on these systems and apparently broadcasts out all interfaces of these dual homed systems (systems had NICs internal and external)
    b.

5. Attack mechanism:

    a. These packets should not exist on this network, needed to sniff network , trace source of system and query sys admin for reason of broadcasts and check constant source port UDP:2301

6. Correlations:

    a. I have noticed these packets since introduction of our firewall, and router syslog accounting.
    b. Verified packets with sniffer to get more info on what these packets were. (see above trace)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

c. Also captured with WINDump.
d. CVE-1999-0772: Denial of service in Compaq Management Agents and the Compaq Survey Utility via a long string sent to port 2301.

7. Evidence of active targeting:

   a. Broadcast packet, all systems on subnet seeing this traffic. Need to find out what, if anything it is affecting.

8. Severity:

   a. (Criticality + lethality) – (System + Net Countermeasures)
   b. (5 + 2) – (5 + 5) = 7 – 10 = -3

9. Defense recommendation:

   a. Defenses are fine, compromise is minimal, although internally, this could be used as an exploit to view and potentially change most system information. A bug has been submitted to Compaq to resolve these erroneous broadcasts.

10. Multiple choice test question:

    b. Given the trace, what would your next course of action be?

       a) Contact System Admin
       b) Document activity from as many sources as possible
       c) Lookup port to see if it is well known
       d) All of the above

Answer: d)

© SANS Institute 2000 - 2002 Author retains full rights.