Global Information Assurance Certification Paper

SANS 2000, San Jose
Practical Exam
Kim Tissue
June 15,2000

The following 10 traces were gathered from CheckPoint Firewall-1 logs from May to June 2000.

Detect 1

12-May-00 13:51:33 hme0 FWInt log drop 212.11.164.180 60000 192.168.60.70 2140 udp 38 len 30
12-May-00 13:51:33 hme0 FWInt log drop 212.11.164.180 60000 192.168.60.74 2140 udp 38 len 30

1. Source of Trace
    a. Company network
2. Detect was generated by:
    a. CheckPoint Firewall-1 Logs
    b. Explanation of fields:

6May2000 [Date] **1:12:26** [Time] **hme0** [Interface] **FWInt** [origin –which firewall] **log** [type] **drop** [action] **dhcp132.check.k-state.net** [source address] **65535** [source port] **198.162.60.70** [destination address] **53** [Service –destination port] **tcp** [transport protocol] **38** [rule] **len 40** [Info]

3. Probability the source address was spoofed.
    a. Low – this attacker's client needs to receive a response back from a server if found.
    b. This IP 212.11.164.180 is from an ISP in Saudia Arabia.
4. Description of Attack
    a. Attack against UDP port 2140 from client outbound port 60000, this is Deep Throat.
5. Attack Mechanism
    a. Deep Throat is a "Remote Administration" trojan horse program. The client, called "Deep Throat Remote Control", is run on a remote computer to gain access to any computer connected to a TCP/IP network or the Internet. An executable server program is required to be installed on the victim's computer to permit the attacker remote site access.
    b. The attacker using outbound source port 60000, sends UDP to port 2140 in search of a Deep Throat server (compromised box). Then using ports 2140 and 3150, the Deep Throat client initiates a back door, Back Orifice-like remote session. Once successfully activated, DT will negotiate a

connection with http://www.mirabilis.com (ICQ) and notifies its maker via HTTP post.

6. Correlations:
    a. This attack is discussed on several websites: SANS at http://www.sans.org/y2k/DT.htm ; F-Secure Corp at http://www.datafellows.com/v-descs/dthroat.htm ; and Privacy Software Corp at http://www.nsclean.com/psc-dt.htm
7. Evidence of active targeting
    a. This attack was a general scan of our network.
8. Severity
    a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
    b. (5+5) – (5+4) = 1
9. Defensive recommendations
    a. Defenses are good. CheckPoint FW-1 Rules blocked the attack.
    b. Because this attack was rapid- timestamp is the same and we have more than 2 servers review log configuration to ensure that data is not dropping out. Could also be an aborted scan attempt and therefore only 2 entries showed up in the logs.
10. Multiple Choice Question
    a. Attack can be best described as an attempted:
        A) Portmapper exploit
        B) DNS Zone Transfer scan
        C) Netbios scan
        D) Deep Throat exploit

Answer D)

Detect 2

14-May-00 12:55:54 hme2 FWInt log drop 210.216.154.135 1122 192.168.60.70 143 tcp 38 len 60
14-May-00 12:56:02 hme0 FW2int log drop 210.216.154.135 1119 192.168.60.73 143 tcp 38 len 60
14-May-00 12:56:02 hme0 FW2int log drop 210.216.154.135 1120 192.168.60.72 143 tcp 38 len 60

1. Source of Trace
    a. Company network
2. Detect was generated by
    a. CheckPoint Firewall-1 Logs
    b. Explanation of fields

6May2000 [Date] **1:12:26** [Time] **hme0** [Interface] **FWInt** [origin –which firewall] **log** [type] **drop** [action] **dhcp132.check.k-state.net** [source address] **65535** [source port] **198.162.60.70** [destination address] **53** [Service –destination port] **tcp** [transport protocol] **38** [rule] **len 40** [Info]

3. Probability the source address was spoofed
    a. Low- this attack needs to receive the response from the server.
    b. This IP 210.216.154.135 is from a range of addresses owned by the National Computerization Agency in Korea.
4. Description of Attack
    a. Attacker is probing for IMAP servers on port 143
    b. This is a reconnaissance attack.
    c. There are known vulnerabilities with unpatched IMAP servers and this attacker is looking for IMAP servers.
5. Attack Mechanism
    a. Attacker sends TCP to port 143 in hopes of receiving a response from the server indicating that it is an IMAP server.
    b. The attacker is looking for IMAP servers to exploit. According to CERT Summary CS-97.09 "In the implementation of both protocols on a UNIX system, the server must run with root privileges so it can access mail folders and undertake some file manipulation on behalf of the user logging in. After login, these privileges are discarded. However, in at least the University of Washington's implementation vulnerability exists in the way the login transaction is handled. This vulnerability can be exploited to gain privileged access on the server. By preparing carefully crafted text to a system running a vulnerable version of these servers, remote users may be able to cause a buffer overflow and execute arbitrary instructions with root privileges."
    c. From CERT Summary CS-97.04 Special Edition "On one machine where large-scale scans were launched, the intruders installed a Trojan Horse identd server. This Trojan identd allowed intruders to connect to the identd server and obtain root access.
6. Correlations
    a. Information about this vulnerability has been widely distributed for some time.
    b. IMAP attacks were discussed in Stephen Northcutt's SANS2000 class, Network Intrusion Analysis.
    c. CERT Summary CS-97.04 Special Edition http://www.cert.org/summaries/CS-97.04.html
    d. CERT Summary CS-97.09 http://www.cert.org/advisories/CA-97.09.imap_pop.html
7. Evidence of Active Targeting
    a. This attack was a general scan of our network.
8. Severity
    a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
    b. (5+5) – (5+4) = 1
9. Defensive recommendation
    a. Defenses are fine. CheckPoint FW-1 Rules blocked the attack.
10. Multiple Choice Question:

This intent of this attack is:

A) Buffer Overflow
B) Virus Launch
C) IMAP scan
D) Denial of Service

Answer C)

Detect 3

12-May-00 21:27:25 hme0 FWInt log drop 203.66.195.84 4800 192.168.60.70 111 tcp 38 len 60
12-May-00 21:27:25 hme0 FWInt log drop 203.66.195.84 4799 192.168.60.74 111 tcp 38 len 60
21-May-00 18:30:20 hme2 log drop 63.70.25.58 111 192.168.60.70 111 tcp len 40
21-May-00 18:30:29 hme0 FW2int log drop 63.70.25.58 111 192.168.60.73 111 tcp 38 len 40
21-May-00 18:30:29 hme0 FW2int log drop 63.70.25.58 111 192.168.60.72 111 tcp 38 len 40
4-Jun-00 16:40:00 hme0 FWInt log drop 203.253.182.98 918 192.168.60.74 111 tcp 39 len 60
4-Jun-00 16:40:01 hme0 FWInt log drop 203.253.182.98 919 192.168.60.70 111 tcp 39 len 60
4-Jun-00 16:40:02 hme0 FWInt log drop 203.253.182.98 920 192.168.60.75 111 tcp 39 len 60

1. Source of Trace
    a. Company network
2. Detect was generated by:
    a. CheckPoint Firewall-1 Logs
    b. Explanation of fields

6May2000 [Date] **1:12:26** [Time] **hme0** [Interface] **FWInt** [origin –which firewall] **log** [type] **drop** [action] **dhcp132.check.k-state.net** [source address] **65535** [source port] **198.162.60.70** [destination address] **53** [Service –destination port] **tcp** [transport protocol] **38** [rule] **len 40** [Info]

3. Probability the Source address was spoofed:
    a. Low – the attacker requires receipt of the response from the server to be successful.
    b. The IP 203.66.195.84 is registered to Chunhwa Telecom Co Ltd in Taiwan, the IP 63.70.25.58 is registered to Sattech Ltd a subnet from UUNet technologies and the 203.253.182.98 is in a range of addresses registered to the National Computerization Agency in Korea (also seen in Detect #2)
4. Description of attack
    a. Attempt to access portmapper. Attackers are scanning TCP port 111 in an attempt to identify our hosts operating systems. If successful then

they can pair appropriate exploits to particular operating systems found.
   b. 3 scans from 3 different networks IP's on different days.
5. Attack Mechanism
   a. Attackers may have used a program, such as nmap, since the individual attack incidents' timestamps are close together.
   b. Nmap is a current scanning tool that can attempt to remotely identify a host's o/s. Nmap sends unexpected stimuli to identify a host's o/s based on the replies. In our logs were cannot see the details of the packet such as tcp flags to determine just what stimuli was sent.
   c. Once the attacker receives a response from a host he/she can then match up an exploit to that particular o/s.
   d. Additional detail from SANS http://www.sans.org/topten.htm "Remote procedure calls (RPC) allow programs on one computer to execute programs on a second computer. They are widely-used to access network services such as shared files in NFS. "
6. Correlations
   a. This attack was discussed at SANS2000 San Jose in both Hal Pomeranz's TCP/IP for Intrusion Detection and Perimeter Defense class, and Stephen Northcutt's Network-Based Intrusion Detection Analysis class.
   b. An excerpt from SANS website http://www.sans.org/topten.htm "Multiple vulnerabilities caused by flaws in RPC, are being actively exploited. There is compelling evidence that the vast majority of the distributed denial of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized because they had the RPC vulnerabilities. The broadly successful attack on U.S. military systems during the Solar Sunrise incident also exploited an RPC flaw found on hundreds of Department of Defense systems."
   c. Security Portal at http://www.securityportal.com/list-archive/bugtraq/1999/Sep/0113.html There have been many reports of exploitations involving RPC vulnerabilities. Such exploitations can lead to root compromise on systems that implement these RPC services.
   d. In 1994 CERT had an advisory CA-95.15 which denoted an increasing number of reports of root compromises caused by intruders using tools to exploit a number of NFS (Network File System) vulnerabilities. See http://www.cert.org/advisories/CA-94.15.NFS.Vulnerabilities.html
7. Evidence of active Targeting
   a. This attack was a general scan of our network.
8. Severity
   a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
   b. (5+4) – (5+4) = 0
9. Defensive Recommendations
   a. Defenses are good. CheckPoint FW-1 Rules blocked attack

b. Set up a system running tcpdump in order to review the packet details.

10. Multiple Choice Question

What does the attacker hope to gain from the above attack:

A) DNS version Scan
B)OS fingerprinting
C)Telnet session
D)FTP access

Answer B)

Detect 4

5-May-00 19:36:49 hme2 FWInt log drop 210.95.255.65 4530 192.168.60.70 98 tcp 38 len 60
5-May-00 19:36:59 hme0 FW2int log drop 210.95.255.65 4533 192.168.60.73 98 tcp 38 len 60
5-May-00 19:36:59 hme0 FW2int log drop 210.95.255.65 4532 192.168.60.72 98 tcp 38 len 60
9-May-00 22:06:02 hme0 FWInt log drop 203.74.210.206 4820 192.168.60.70 98 tcp 38 len 60
9-May-00 22:06:02 hme0 FWInt log drop 203.74.210.206 4819 192.168.60.74 98 tcp 38 len 60
23-May-00 20:45:45 hme2 FWInt log drop 193.129.252.129 4366 192.168.60.70 98 tcp 38 len 60
23-May-00 20:45:53 hme0 FW2int log drop 193.129.252.129 4369 192.168.60.73 98 tcp 38 len 60
23-May-00 20:45:56 hme0 FW2int log drop 193.129.252.129 4368 192.168.60.72 98 tcp 38 len 60

1. Source of Trace
    a. Company network
2. Detect was generated by:
    a. CheckPoint Firewall –1 logs
    b. Explanation of fields:

6May2000 [Date] **1:12:26** [Time] **hme0** [Interface] **FWInt** [origin –which firewall] **log** [type] **drop** [action] **dhcp132.check.k-state.net** [source address] **65535** [source port] **198.162.60.70** [destination address] **53** [Service –destination port] **tcp** [transport protocol] **38** [rule] **len 40** [Info]

3. Probability the source address was spoofed
    a. Low – the attacker requires receipt of the response from the server to be successful.
    b. The IP 210.95.255.65 is registered to the National Computerization Agency in Korea (also seen in Detect #2 &3); IP 203.74.210.206 is registered to Chunhwa Telecom Co Ltd in Tawian (also seen in Detect #3)

; IP 193.129.252.129 is registered to Broadcasters Audience Research Board Ltd in Great Britain.

4. Description of attack
    a. Attackers are probing for Linuxconf on TCP port 98.
    b. According to SANS this attack was dubbed Hack of the Month in November 1999.
5. Attack Mechanism
    a. Attack is reconnaissance. Attackers are searching for a response to scans on TCP port 98 in order to locate systems that have Linuxconf installed. Linuxconf is a sophisticated administration system for the Linux operating system. If these were poorly protected systems and because Linuxconf runs as root, once found the system would be compromised.
    b. For more information on the product http://www.solucorp.qc.ca/linuxconf/
6. Correlations
    a. This attack has been seen since November 1999 and was discussed at SANS2000 San Jose in Stephen Northcutt's Network-Based Intrusion Detection Analysis class. Also see page 159 in workbook 2.4/2.5
    b. A recent posting (June 3, 2000) on the GIAC pages of SANS' website regarding Linuxconf: http://www.sans.org/y2k/060300.htm
    c. Back in Nov 99 scanning port 98 was discussed in the Linux Mailing list archives: http://www.linuxsa.org.au/mailing-list/1999-11/554.html
7. Evidence of Active Targeting
    a. This attack was a general scan of our network.
8. Severity
    a. (critical + Lethal) – (System + Net Countermeasures) = Severity
    b. (5+5) – (5+4) = 1
9. Defensive Recommendations
    a. Defenses are fine. CheckPoint FW-1 Rules blocked attack.
10. Multiple Choice Question

Attacker was scanning for:

A) Back Orifice
B) ICQ
C) Quake
D) Linuxconf

Answer D)

Detect 5

3-Jun-00 5:10:50 hme0 FWInt log drop 207.134.254.4 109 192.168.60.74 109 tcp 39 len 40
3-Jun-00 5:10:50 hme0 FWInt log drop 207.134.254.4 109 192.168.60.70 109 tcp 39 len 40

3-Jun-00 5:10:50 hme0 FWInt log drop 207.134.254.4 109 192.168.60.75 109 tcp 39 len 40
5-Jun-00 10:31:17 hme0 FWInt log drop 12.21.137.195 3835 192.168.60.74 109 tcp 39 len 60
5-Jun-00 10:31:17 hme0 FWInt log drop 12.21.137.195 3836 192.168.60.70 109 tcp 39 len 60
5-Jun-00 10:31:17 hme0 FWInt log drop 12.21.137.195 3837 192.168.60.75 109 tcp 39 len 60

1. Source of Trace
    a. Company network
2. Detect was generated by:
    a. CheckPoint Firewall-1 Logs
    b. Explanation of fields:

6May2000 [Date] **1:12:26** [Time] **hme0** [Interface] **FWInt** [origin –which firewall] **log** [type] **drop** [action] **dhcp132.check.k-state.net** [source address] **65535** [source port] **198.162.60.70** [destination address] **53** [Service –destination port] **tcp** [transport protocol] **38** [rule] **len 40** [Info]

3. Probability the Source address was spoofed
    a. Low- the attacker requires receipt of the response from the server in order to be successful
    b. IP 207.134.254.4 is registered to iSTAR Internet Inc ISP in Ottawa Canada (interesting that it is Canada again); IP 12.21.137.195 is registered to Information Management Associates out of Atlanta Georgia, which is sub netted from AT & T.
4. Description of Attack
    a. Attackers are scanning TCP port 109 on our network. This is pop-2's port.
5. Attack Mechanism
    a. Attackers are scanning hosts on TCP port 109 looking for responses indicating that it is a pop-2 server.
    b. POP is one of the popular remote access mail protocols, which allows users to access their e-mail accounts from internal and external networks. POP is especially vulnerable to exploitation because openings are frequently left in firewalls to allow for external e-mail access. Attackers who exploit flaws in IMAP or POP often gain instant root-level control.
    c. Example of exploit for POP-2: CVE –1999-0920 Buffer overflow in the pop-2d POP daemon in the IMAP package allows remote attackers to gain privileges via the FOLD command.
6. Correlations
    a. This reconnaissance attack was described in Stephen Northcutt's SANS2000 class, Network Intrusion Analysis
    b. Reference to the POP vulnerability is listed in the resource "How To Eliminate The Ten Most Critical Internet Security Threats The Experts' Consensus" on SANS at http://www.sans.org/topten.htm

7. Evidence of Active Targeting
    a. This attack was a general scan of our network.
8. Severity
    a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
    b. (5+5) – (5 +4) = 1
9. Defensive Recommendation
    a. Defenses are fine. CheckPoint FW-1 Rule blocked attack.
10. Multiple choice question
    The following is true of this attack
        A) It is a denial of service attack
        B) Attack is a POP 2 scan
        C) An unprotected host could be compromised
        D) B and C

Answer D)

Detect 6

6-May-00 4:55:01 hme0 FWInt log drop cr49202-a.surrey1.bc.wave.home.com 1864 192.168.60.74 1080 tcp len 48
6-May-00 4:55:01 hme0 FWInt log drop cr49202-a.surrey1.bc.wave.home.com 1865 192.168.60.70 1080 tcp 38 len 48
19-May-00 3:17:43 hme0 FWInt log drop portup364.portup.com 2264 192.168.60.74 1080 tcp 38 len 48
19-May-00 3:17:43 hme0 FWInt log drop portup364.portup.com 2265 192.168.60.70 1080 tcp 38 len 48
30-May-00 3:34:03 hme0 FWInt log drop adsl-63-199-202-192.dsl.lsan03.pacbell.net 2723 192.168.60.74 1080 tcp 38 len 48
30-May-00 3:34:03 hme0 FWInt log drop adsl-63-199-202-192.dsl.lsan03.pacbell.net 2724 192.168.60.70 1080 tcp 38 len 48
5-Jun-00 1:05:57 hme0 FWInt log drop secureplanet.net 2931 192.168.60.74 1080 tcp 39 len 44
5-Jun-00 1:05:57 hme0 FWInt log drop secureplanet.net 2932 192.168.60.70 1080 tcp 39 len 44
5-Jun-00 1:05:57 hme0 FWInt log drop secureplanet.net 2933 192.168.60.75 1080 tcp 39 len 44
7-Jun-00 17:50:50 hme0 FWInt log drop 213.45.12.214 4748 192.168.60.74 1080 tcp 38 len 48
7-Jun-00 17:50:50 hme0 FWInt log drop 213.45.12.214 4753 192.168.60.70 1080 tcp 38 len 48
7-Jun-00 17:50:50 hme0 FWInt log drop 213.45.12.214 4762 192.168.60.75 1080 tcp 38 len 48

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

   a. CheckPoint Firewall-1 Logs
3. Probability the source address was spoofed
   a. Low - the attacker requires receipt of the response from the server in order to be successful
   b. All IP's are registered to ISP's @Home, pacbell.net, portup.net, secureplanet.net (Milano, Italy) and Telcom Italia Net (Italy).
4. Description of Attack
   a. Attackers were scanning our hosts on TCP port 1080. This is the socks port. SOCKS is designed to allow a host outside of a firewall to connect transparently and securely through the firewall. As a consequence, some sites may have port 1080 opened for incoming connections to a system running a socks daemon.
5. Attack Mechanism
   a. Attacker scans on port 1080 looking for a SOCKS proxy response. If found attacker may be attempting to connect to a telnet redirector such as Wingate. If there was a machine running Wingate inside the firewall the system could be used to redirect telnet connections to other servers inside the firewall.
   b. The attacker could also be looking for other services besides Wingate proxied through SOCKS. For example prxtools 'fizzbounce' maps a tcp connection from a local port over a remote http proxy server that does http-relay to a remote host. See http://packetstorm.securify.com
6. Correlations
   a. The SOCKS attack was described in Stephen Northcutt's SANS2000 class, Network-Based Intrusion Detection Analysis.
   b. Christopher Misra wrote up a Special notice on SANS regarding socks attacks. http://www.sans.org/y2k/socks.htm
   c. 6/9/1999 socks check exploit script written and posted on rootshell.com The scripts takes a list of IPs and scans them for insecure Socks proxy servers. http://rootshell.com/archive-j457nxiqi3gq59dv/199906/sockcheck.c.html
7. Evidence of Active Targeting
   a. This attack was a general scan of our network.
8. Severity
   a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
   b. (5+ 4) – (5 +4) = 0
9. Defensive Recommendations
   a. Defenses are fine. CheckPoint FW-1 Rules blocked attack
10. Multiple choice question:
    This trace is best described as:
    a) Buffer Overflow
    b) Scan for Zone Transfer
    c) Port Scan
    d) Socks Scan

Answer is D)

Detect 7

5-May-00 16:56:56 hme1 FW2int log drop dhcp132.check.k-state.net 65535 255.255.255.255 53 tcp 38 len 40
5-May-00 16:56:56 hme1 FW2int log drop dhcp132.check.k-state.net 65535 fw2-exodus-ext 53 tcp 38 len 40
6-May-00 1:12:26 hme0 FWInt log drop dhcp132.check.k-state.net 65535 192.168.60.70 53 tcp 38 len 40
6-May-00 1:12:26 hme0 FWInt log drop dhcp132.check.k-state.net 65535 192.168.60.75 53 tcp 38 len 40

1. Source of Trace
    a. Company network
2. Detect was generated by:
    a. CheckPoint Firewall-1 Logs
3. Probability the source address was spoofed.
    a. Low - the attacker requires receipt of the response from the server in order to be successful
    b. The attack host address dhcp132.check.k-state.net is registered to Kansas State University
4. Description of Attack
    a. Attacker using high numbered outbound port 65535 to inbound TCP port 53 which is DNS.
5. Attack Mechanism
    a. Attacker uses the high numbered port of 65535 to evade firewalls. Early revisions of CheckPoint Firewall-1 could not block source port 0 or 65535. Thus if an attacker wanted to attempt to access TCP port 53 (DNS) which is normally blocked, he/she might try using source port 0 or 65535.
    b. Most likely it is a script kiddie with a compiler. The May 5th traces were scanning at the ISP Exodus.net- a broadcast and an external firewall (fw2-exodus-ext). Then the next morning it got to our network.
6. Correlations
    a. Discussed at SANS 2000 in Stephen Northcutt's SANS2000 class, Network-Based Intrusion Detection Analysis (page 201 in workbook 2.4/2.5)
7. Evidence of active Targeting
    a. The attack was a general scan of our network.
8. Severity
    a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
    b. (5+5) – (5 +4) = 1
9. Defensive recommendation
    a. Defenses are fine. CheckPoint FW-1 Rules blocked attack
10. Multiple Choice Question
    Attacker was scanning for:

A) DNS
B) FTP
C) SMTP
D) SOCKS

Answer A)

Detect 8

2-May-00 18:41:37 hme0 FWInt log drop proxy.zcomm.com 1535 192.168.60.70 21 tcp 38 len 44
10-May-00 16:23:21 hme2 FWInt log drop cr414186-a.ktchnr1.on.wave.home.com 3188 192.168.60.70 21 tcp 38 len 64
10-May-00 16:23:28 hme0 FW2int log drop cr414186-a.ktchnr1.on.wave.home.com 3191 192.168.60.73 21 tcp 38 len 64
14-May-00 18:41:45 hme2 FWInt log drop ia-piex-gw01-e0-1-1-cr178.videotron.net 4602 192.168.60.70 ftp tcp 38 len 60
14-May-00 18:41:53 hme0 FW2int log drop ia-piex-gw01-e0-1-1-cr178.videotron.net 4605 192.168.60.73 21 tcp 38 len 60
14-May-00 18:41:53 hme0 FW2int log drop ia-piex-gw01-e0-1-1-cr178.videotron.net 4604 192.168.60.72 21 tcp 38 len 60

1. Source of trace
    a. Company network
2. Detect was generated by:
    a. CheckPoint Firewall-1 Logs
3. Probability the source route was spoofed
    a. Low - the attacker requires receipt of the response from the FTP server in order to be successful
    b. All attacking hosts are from domains (zcomm.com, home.com and videotron.net) that are ISP's.
4. Description of Attack
    a. Attackers are scanning for FTP servers on TCP port 21.
5. Attack Mechanism
    a. Attackers attempting to connect to TCP port 21, which is FTP.
    b. If a server responded to a port 21 scan then the attacker could run exploits, or even just try to guess usernames and passwords. An attacker may even find a guest account (with password guest) and be able to log onto the server. As an authenticated user (guest) he/she could attempt to upload executables and run them among other things. For example remote buffer overflows in various FTP servers leads to potential root compromise
    c. In addition any user with a local account on a system offering FTP services with vulnerable configurations (see cert below) may gain root access. Support for anonymous FTP is not required to exploit this vulnerability.
6. Correlations

a. FTP server exploits have been around for some time. CERT Advisory CA-95.16 talks about wu-ftpd misconfiguration vulnerability and the consequences. http://www.cert.org/advisories/CA-95.16.wuftpd.vul.html
b. FTP server exploits have been around for some time. On 2/9/99 a general public advisory regarding a remote buffer overflow exploit of ftp was posted to Rootshell.com http://rootshell.com/archive-j457nxiqi3gq59dv/199902/ftpd.txt.html They point out that Intruders who are able to exploit this vulnerability can ultimately gain interactive access to the remote ftp server with root privilege.

7. Evidence of Active Targeting
   a. This attack was a general scan of our network.
8. Severity
   a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
   b. (5 + 5) – (5+4) = 1
9. Defensive Recommendation
   a. Defenses are good. CheckPoint FW-1 Rules blocked attack
10. Multiple choice question

What is attacker looking for from this attempt:

a) Telnet server
b) FTP server
c) IIS server
d) SMTP server

Answer b)

Detect 9

```
13-May-00 16:27:36 hme0 FWInt log drop ppp-206-170-25-208.sntc01.pacbell.net
1025 192.168.60.74 22 udp 38 len 30
13-May-00 16:27:36 hme0 FWInt log drop ppp-206-170-25-208.sntc01.pacbell.net
1025 192.168.60.70 22 udp 38 len 30
13-May-00 16:30:31 hme0 FWInt log drop ppp-206-170-25-208.sntc01.pacbell.net
1026 192.168.60.74 22 udp 38 len 30
13-May-00 16:30:31 hme0 FWInt log drop ppp-206-170-25-208.sntc01.pacbell.net
1026 192.168.60.70 22 udp 38 len 30
25-May-00 3:53:58 hme1 FW2int log drop cj42229-a.alex1.va.home.com 44952
fw2-exodus-ext 22 tcp 38 len 40
25-May-00 3:53:59 hme1 FW2int log drop cj42229-a.alex1.va.home.com 44953
fw2-exodus-ext 22 tcp 38 len 40
25-May-00 3:54:00 hme1 FW2int log drop cj42229-a.alex1.va.home.com 44960
fw2-exodus-ext 22 tcp 38 len 60
25-May-00 3:54:00 hme1 FW2int log drop cj42229-a.alex1.va.home.com 44962
fw2-exodus-ext 22 tcp 38 len 60
```

1. Source of Trace
    a. Company network
2. Detect was generated by:
    a. CheckPoint Firewall-1 Logs
3. Probability the source address was spoofed
    a. Low - the attacker requires receipt of the response from the server in order to be successful
    b. Both hosts are from ISP's – pacbell.net & home.com
4. Description of Attack
    a. Attacker are scanning hosts on TCP port 22 (secure shell) & UDP port 22 (PC Anywhere)
5. Attack Mechanism
    a. An attacker scans for hosts listening on TCP port 22, which is secure shell, or UDP port 22, which is PC Anywhere. Once found attacker could attempt to login- guessing usernames and passwords such as guest. According to documentation on rootshell.com secure shell 1.2 has a bug such that a user with a non-root account is able to open privileged ports on the local host and redirect them. The implications are a bit scary -- on a machine where telnet or rlogin is normally disabled an ordinary user could set up ssh port redirection of the telnet or rlogin service to a machine under their own control. A user with ordinary privileges could "run" a Web server on a machine not currently running a server bound to port 80 by redirecting port 80 to another host, etc.
    b. An attacker with the client for PC Anywhere could try connecting to servers found responding to UDP port 22. They may find occurrences of easy to guess username and password combinations.
6. Correlations
    a. Secure Shell was discussed at SANS 2000 in Judy Novak's class Intrusion Detection Analysis- Shadow Style. (reference page 295)
    b. Exploits against Secure Shell have been around sine 1997. At Rootshell.com they describe how a non- root user is able to open privileged ports on the local host and redirect them. See url: http://rootshell.com/archive-j457nxiqi3gq59dv/199708/secure_shell.txt.html
    c. On SANS Matt Scarborough wrote a piece regarding PC Anywhere scans http://www.sans.org/y2k/reports.htm
7. Evidence of active Targeting
    a. This attack was a general scan of our network
8. Severity
    a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
    b. (5 +5) – (5 +4) = 1
9. Defensive Recommendations
    a. Defenses are fine. CheckPoint FW-1 Rules blocked attack
10. Multiple Choice Question
    What is the Attacker attempting to do in the above example:
        a) Scan for a Doom server

b) Launch a Land attack
c) Scan for secure shell
d) Download a file via FTP.

Answer C)

Detect 10

13-May-00 22:28:29 hme0 FWInt log drop AC8793BA.ipt.aol.com 2816 192.168.60.70 21 tcp 38 len 4
13-May-00 22:28:29 hme0 FWInt log drop AC8793BA.ipt.aol.com 2815 192.168.60.74 21 tcp 38 len 4
19-May-00 1:22:31 hme0 FWInt log drop gate.ebv.com 64615 192.168.60.70 21 tcp 38 len 6
19-May-00 1:22:54 hme0 FWInt log drop www.ebv.com 2923 192.168.60.70 21 tcp 38 len 6
19-May-00 1:23:01 hme0 FWInt log drop www.ebv.com 2924 192.168.60.70 21 tcp 38 len 6

1. Source of trace
    a. Company network
2. Detect was generated by:
    a. CheckPoint Firewall-1 Logs
3. Probability that the source address was spoofed
    a. Low - the attacker requires receipt of the response from the server in order to be successful
    b. The aol.com address is from an ISP, whereas the ebv.com address is from a company.
4. Description of Attack
    a. Attackers are scanning for Telnet on TCP port 21.
5. Attack Mechanism
    a. Attackers scan the network looking for servers that respond to TCP port 21 (complete the three way handshake) They may be looking for vulnerable systems. If they find telnet servers running on unprotected servers then there are several exploits they may be able to try. For example, there are CVE references to buffer overflows, denial of service and gaining root access.
6. Correlations
    a. CERT Advisory CA-95.14.Telnetd Environment Vulnerability referenced on http://www.infowar.com/iwftp/cert/advisories/CA-95.14.Telnetd_Environment_Vulnerability.html discusses the potential vulnerability of some telnet daemons.
7. Evidence of Active Targeting
    a. The attack on May 13 is a general scan of the network whereas on May 19th the attacker is targeting one host.
8. Severity

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity
b. (5 + 5) – (5 + 4) = 1

9. Defensive Recommendation
    a. Defenses are good. CheckPoint FW-1 Rules blocked attack.
10. Multiple Choice Question

    Attacker was attempting to connect to:

    a) Telnet
    b) DNS
    c) FTP
    d) HTTP

Answer a)

Last Updated: July 26th, 2017

Upcoming Training

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 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 Seattle 2017	Seattle, WA	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 San Diego 2017	San Diego, CA	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