Global Information Assurance Certification Paper

Additional Course Work - Multiple choice questions:

Day 1

1. How would the IP datagram identify that it contained a TCP segment?

   a) The 16 bit destination port in the IP header would contain a value of 23.
   b) The 4 bit header length field in the IP header would contain a value of 6.
   c) The 10th byte Protocol field in the IP header would contain a value of 17.
   d) The 9th byte in the IP header would contain 0000 0110.

2. How do TCP and UDP protocols differ?

   a) TCP is faster than UDP, which waits for a reply before it sends another packet.
   b) TCP is connection oriented and therefore is more reliable than UDP.
   c) UDP will always be slower than TCP because it is connectionless.
   d) UDP is internet optimized for long haul communication.

3. One of the attributes of the Windows Internet Naming Service (WINS) is:
   a) Naming collisions are prevented since a user can register any name with a WINS server and it will be accepted.
   b) The naming convention used by Microsoft allows names up to 50 characters in length.
   c) On boot the client broadcasts its NetBIOS name and information between 5 and 10 times to ensure it is received by every other client.
   d) Since the NetBIOS names are verified when the WINS database replicates, entries are quickly deleted when a host goes offline.

4. Which of the following is not a feature of tcpdump?
   a) By default, it will collect all traffic passing on the network.
   b) TCP output records will show the flags and sequence numbers.
   c) Each UDP record will be expressly labeled "udp".
   d) Command line options allow for altering the type of records collected as well as the data output.

5. In a tcpdump hexadecimal output, what is the meaning of a value of 45 in the 0th byte?
   a) The TCP segment is 45 bytes long.
   b) The IP datagram is 45 bytes long.
   c) The IP Protocol version is 4 and the header is 5 bytes long.
   d) The IP Protocol version is 4 and the header is 20 bytes long.

6. TCP ports which are numbered greater than 1023 are generally:
   a) Client ports known as ephemeral ports.
   b) Are selected for only a particular connection.
   c) Differ from one connection to the next.
   d) All of the above.

7. During a graceful termination of a TCP session,
   a) One host sends a FIN and the other responds with a RESET.
   b) Each host initiates a FIN and the other responds with an ACK.
   c) One host sends the other a RESET.
   d) Since the communication is unidirectional, only one FIN and ACK are necessary.

8. During normal fragmentation of an ICMP echo request,
   a) Each fragment will contain the ICMP message pseudo-header.
   b) The last fragment will have the Last Fragment bit set in the IP header.
   c) Each fragment will have a number cloned from the IP identification number.

d) All fragments will have a data payload of equal length.

9. Internet Control Message Protocol (ICMP) messages are
   a) Used as a common mapping technique.
   b) Similar to UDP and TCP because they require port numbers.
   c) Similar to TCP because they can support broadcast traffic.
   d) Often used to deliver an error about another ICMP message.

10. When a host receives an ICMP "time exceeded in-transit" it means,
    a) The receiving host's timer ran out as it waited for the IP datagram to arrive.
    b) The number of seconds in the time to live value was too short for the datagram to reach the receiving host.
    c) The time to live value was decremented to zero by a router somewhere along its path and the IP datagram was discarded.
    d) All of the fragmented datagrams did not reach the destination host in time to be reassembled by the receiving host.

Day 2

1. Which of the following is inherently true about IP itself?
   a) All TCP, UDP, and ICMP data gets transmitted encapsulated within IP datagrams.
   b) IP datagram delivery is reliable.
   c) IP is designed to be network hardware dependent.
   d) All of the above.

2. Which of the following information is contained in the tcpdump format for fragmented packets?
   a) The fragment size including the IP header.
   b) The fragment's offset in bytes in the original IP datagram.
   c) The "+" sign to indicate the last fragment has been sent.
   d) All of the above.

3. Which of the following is <u>not</u> generally true of a router packet filter?
   a) **It is used to consider each packet with regard to the packets it inspected before**.
   b) It is used to provide inexpensive firewall capability for networks.
   c) It is used to permit or deny network traffic based on information in the network headers.
   d) It is used to block all packets destined for certain well-known ports.

4. Which of the following tcpdump filters would detect a Land Attack?
   a) tcp[0:4] = tcp[4:4]
   b) ip[0:4] = ip[4:4]
   c) tcp[12:4] = tcp[16:4]
   d) ip[12:4] = ip [16:4]

5. Along with the control information in the 40 byte options field of the IP header, the maximum number of router IP addresses specified in source routing is:
   a) 9
   b) 19
   c) 29
   d) 39

6. The Ping o' Death Attack differs from the Smurf Attack in that
   a) The Ping o' Death does not utilize the ICMP echo request.
   b) The Ping o' Death is not a denial of service.
   c) The Ping o' Death utilizes generated impossible packets.
   d) The Ping o' Death requires intermediary hosts to amplify ICMP traffic.

7. Loki is a form of
   a) Denial of service utilizing ICMP.
   b) Network mapping utilizing ICMP.
   c) Information tunneling utilizing UDP.
   d) Backdoor vulnerability resulting from an "insider" attack.

8. Tcpdump patters of Loki and Back Orifice are similar in that:
   a) A single packet from a client causes several response packets.
   b) UDP is used by both attacks to transfer packets.
   c) Port 31337 is used by both as the default port.
   d) Neither can be installed easily without an administrator's knowledge.

9. When a attacker's TCP Portscanning program sends a crafted SYN packet and receives a SYN-ACK in response, the operating system on the attackers machine will then:
   a) Reply with an ACK to complete the three-way handshake.
   b) Reply with a SYN-FIN to close the connection.
   c) Reply with a FIN-ACK to start to close the connection.
   d) Reply with a RESET because it did not initiate the three-way handshake.

10. Through what type of filter at the Shadow Analysis Station should the logs collected by the sniffer be run?
   a) Protocol based filter .
   b) Anomaly detection filter.
   c) Scan-finding filter.
   d) All of the above.

Day 3

1. What is Shadow not?
   a) Freeware available from www.nswc.navy.mil.
   b) A Unix based intrusion detection system.
   c) Able to perform payload analysis in real time.
   d) Pull based architecture which views events of interest via a web browser.

2. What would the filter be to find if the Don't Fragment bit was set?
   a) ip[6] & 0x40 != 0
   b) ip[6] & 0x4f != 0
   c) ip[6] & 0x20 != 0
   d) ip[6] & 0x40 = 0

3. What tcpdump option would one use to print the records in hexadecimal?
   a) -s
   b) -vv
   c) -w
   d) -x

4. Which of the following is not commonly part of the default analysis host hourly filters?
   a) badhost.filter
   b) tcp.filter
   c) icmp.filter
   d) ip.filter

5. What is not true about the IP Header Identification?
   a) 8 bit (1 byte) number found in the IP header.
   b) Value typically incremented by 1 for each datagram sent.

c) Uniquely identifies every datagram sent by a host.
d) Also known as the fragment ID used to reassemble fragmented packets.

6. Which of the following is true about the Time to Live Value
   a) It is a 16 bit value in the IP header.
   b) It is set by the host sending the datagram.
   c) It is incremented by 1 by each router in its path.
   d) Its initial value is not operating system related.

7. What conditions is not a requirement for the WinNuke attack to work?
   a) The urgent flag bit must be on.
   b) The target must have an unpatched and vulnerable Windows operating system.
   c) The attack must be directed to a port on which the vulnerable system is not listening.
   d) The urgent value must be set to 3.

8. Which of the following is important to remember when using tcpshow?
   a) The default shapshot length set by most sites allows the entire datagram to be interpreted.
   b) It was written with built-in intelligence about attack and exploit signatures.
   c) It will not attempt to interpret payload data.
   d) It will not properly translate a payload that is not ASCII-based.

9. What determines the number of bytes displayed in the tcpdump hex output?
   a) The -s value.
   b) The -vv value.
   c) The -w value.
   d) The -x value.

10. What is a possible result if snaplen is increased?
    a) Time to process packets is decreased.
    b) Amount of packet buffering effectively increased.
    c) IP header data could be lost from received packets.
    d) IP packets may be lost.

Days 4 / 5

1. What does the following log show?
   Dec 12 12:25:36 ucsb.edu 45670: 8w5d∧l: %SEC-6-IPACCESSLOGP: list 190 denied tcp 201.160.111.189(2040) -> 172.21.27.224(3128), 1 packet
   a) A Cisco router allowed one packet passed to reach a SQUID Proxy.
   b) A SonicWall firewall detected this incursion to a SQUID Proxy.
   c) A Soho firewall blocked an attempted incursion to an HTTP port.
   d) Access list 190 caused a Cisco router to block an attempted incursion.

2. It is important to remember that firewalls have some limitations in intrusion detection because:
   a) Generally, their logs present all traffic on the network to which they are connected, even that traffic not destined for the network they are protecting.
   b) Generally, their logs only present the traffic they allowed to pass through, and not what was blocked.
   c) Generally, their logs only present the exceptions, which were blocked.
   d) Generally, their logs do not indicate the direction of the traffic.

3. What address pairing generally indicates an attempt to reach PC Anywhere?
   a) TCP 80 and 1080
   b) UDP 1243 and 27374
   c) UDP 22 and 5632
   d) TCP 20 and 21

4. Why is it generally not a good idea to have both the sensor and the analysis software on the same box?
   a) Response time to intrusion detects is hindered since they would have to be processed through the firewall.
   b) Transfer of sensor logs would hinder the systems ability to continue logging detects.
   c) If an intrusion detection system is compromised, it might divulge too much about the site from its rule set.
   d) In this configuration, the firewall will not be able to effectively block hostile incursion attempts.

5. Most Intrusion Detection Systems and Virus Detection Programs operate similarly in that:
   a) They utilize site policy for detection.
   b) **They utilize signatures of known attacks for detection**.
   c) They provide alerts in real time.
   d) They are optimized to detect encrypted attacks.

6. Among the strengths of the NID software is that:
   a) It cannot be overwhelmed by a busy network.
   b) With typical configurations, it is not easily blindsided by new exploits.
   c) Regardless of the mode in which it is running, it will capture all content.
   d) It can created detailed records of the event of interest for later analysis.

7. Pull based event generators will:
   a) Respond in real time.
   b) Generate alerts when an attack occurs.
   c) Produce a Generalized Intrusion Detection Object when an event is detected.
   d) Require a query for data by the analyst.

8. What flag(s) would be set if the TCP header flags value was 32?
   a) **ACK**
   b) SYN / ACK
   c) SYN
   d) FIN

9. What is a basic characteristic of a SYN flood?
   a) The attacker sends SYNs to a server and saturates it by completing a series of 3 way handshakes.
   b) The attacker keeps track of the SYN/ACK replies to determine when the attacked server is saturated.
   c) The attacker uses a host network to flood the server under attack with SYNs from multiple sources.
   d) The attacker uses a spoofed IP address and after saturating the server under attack is able to keep it saturated with only a few periodic SYNs.

10. How is the Severity of an attack calculated?
    a) It is equal to the criticality of the system being attacked.
    b) It is equal to countermeasures in place subtracted from the sum of criticality and lethality.
    c) It is equal to the sum of criticality and lethality.
    d) It is equal to the sum of the replacement of the data lost and time to restore operation.

11. Which of the following is <u>not</u> part of the reality of Low Sensor Coverage?
    a) Improved software allows for pattern matching scaled in internet backbone speeds.
    b) It is possible to build a network that is virtually impossible to monitor.
    c) Content sensors top out below 100Mbs.
    d) Sensors are often tuned to only monitor certain services.

12. When correlating detection log data it is important not to:
    a) Correlate observations from similar sensors.
    b) Fuse observations from multiple types of sensors.
    c) Only trust the output of one well understood sensor.
    d) Locate secondary sources of data at your facility.

13. In traffic analysis, the primary dimensions include all except:
    a) To
    b) From
    c) Protocol
    d) Service

14. A 0 source port and the SYN/FIN flags appearing together has been a common signature of:
    a) NMAP
    b) Loki
    c) IMAP
    d) SYN Flood

15. Which of the following is <u>not</u> a feature common to Shadow:
    a) It uses tcpdump to record traffic.
    b) It is concerned with packet contents rather than header information.
    c) Files are filtered for attack patterns at the analysis station.
    d) Each line in the record represents a packet observed by the sensor.

16. Blocking outgoing TCP Port 6667 would be used to:
    a) Prevent unauthorized ftp.
    b) Prevent unauthorized use of internet games.
    c) **Prevent unauthorized use of web-chat**.
    d) Prevent common hacker exploits.

17. Why is it advisable to block TCP and UDP ports 7, 13, and 19 from the outside.?
    a) Prevent external control of system via use of telnet.
    b) Prevent self-sustaining denial of service using ftp to ftp data transfer.
    c) Prevent self-sustaining denial of service using echo, daytime, and chargen.
    d) Prevent external NFS file theft via use of DNS.

18. To prevent network mapping by ICMP echo requests, these should be blocked:
    a) External to internal at the filtering router or firewall.
    b) Both external to internal and internal to external at the filtering router and firewall.
    c) At every system connected to the network.
    d) At all of the routers inside the filtering router.

19. Zone transfer will allow an attacker to:
    a) Download files from your mail servers.
    b) Download a host table from your site.
    c) Download a list of systems with the FTP ports open.
    d) Download the current configuration of your sites filtering router.

20. It is a very good idea to block access to port 137 because:
    a) Attackers can own your system by running DNS on this port.
    b) Attackers can gather a lot of information about your system from NetBIOS.
    c) Attackers can execute programs remotely using NetBIOS session service on this port.
    d) Attackers can transfer files from privileged directories via this port.

Additional Course Work - Multiple choice answers:

Day 1

1. d
2. b
3. c

4. c
5. d
6. d
7. b
8. c
9. a
10. c

Day 2

1. a
2. b
3. a
4. d
5. a
6. c
7. d
8. a
9. d
10. d

Day 3

1. c
2. a
3. d
4. a
5. a
6. b
7. c
8. d
9. d
10. d

Days 4 / 5

1. d
2. c
3. c
4. c
5. b
6. d
7. d
8. a
9. d
10. b
11. a
12. c
13. c
14. c
15. b
16. c
17. c
18. a
19. b
20. b

Intrusion Detect # 1 - WinGate Scan

Uonumanet Ltd, Niigata, JP

Jun 7 17:52:10 hostm /kernel:
Connection attempt to TCP z.y.x.14:**8080** from 202.235.50.12:**65535**

Jun 7 17:59:25 dns1 snort[266909]: MISC-WinGate-8080-Attempt:
202.235.50.12:**65535** -> z.y.w.34:**8080**

Jun 7 17:59:26 dns2 snort[8668]: MISC-WinGate-8080-Attempt:
202.235.50.12:**65535** -> z.y.w.66:**8080**

Jun 7 17:59:27 dns3 snort[1813]: MISC-WinGate-8080-Attempt:
202.235.50.12:**65535** -> z.y.w.98:**8080**

[**] MISC-WinGate-8080-Attempt [**]

06/07-17:59:25.458320 202.235.50.12:**65535** -> z.y.w.34:**8080** TCP
TTL:**240** TOS:0x0 **ID:15990** **S***** Seq: **0x3E760000** Ack: 0x0 Win:
0x200 00 00 00 00 00 00 .....

[**] MISC-WinGate-8080-Attempt [**]
06/07-17:59:26.099813 202.235.50.12:**65535** -> z.y.w.66:**8080** TCP
TTL:**240** TOS:0x0 **ID:15990** **S***** Seq: **0x3E760000** Ack: 0x0 Win:
0x200 16 90 49 32 1D E1 ..I2..

[**] MISC-WinGate-8080-Attempt [**]
06/07-17:59:26.734588 202.235.50.12:**65535** -> z.y.w.98:**8080** TCP
TTL:**240** TOS:0x0 **ID:15990** **S***** Seq: **0x3E760000** Ack: 0x0 Win:
0x200 00 00 00 00 00 00 .....

1. Source of trace:
http://www.sans.org/y2k/061000.htm

2. Source generated by:

Source appears to have been generated by Snort

Fields of Interest:

Source address and source port - 202.235.50.12:**65535**
Destination address and destination port - z.y.x.14:**8080** to z.y.w.98:**8080**
Sequence Number - **0x3E760000**
Time to Live - **240**
Flags Set - **S***** and Ack
Type of service - TOS:0x0
IP ID: **15990**

3. Possibility that the source address was spoofed.

Since the attack appears to be a scan of ports for active WinGate (or possibly Web) services, it seems that a spoofed address is unlikely because the attacker is attempting to get a reply. The possibility of the attacker working through a proxy is not known.

4. Description of attack:

Attack against TCP port 8080, this is most probably a probe for WinGate services (or less likely Web services on this port.)

5. Attack mechanism:

The attacker appears to be using a program to generate a scan of ports on the 202.235.50.xxx addresses for the existence of vulnerable web services.
The Syn and Ack flags being set may indicate an apparent attempt to penetrate any firewall defenses. This second part of the TCP three-way handshake is commonly not blocked by firewalls since many do not keep track of outgoing Syn's, which are the start of the three-way handshake.
The program in use generates a fixed sequence number - **0x3E760000,** a fixed 'ephemeral' port - **65535,** and a high value for TTL - (something initially larger than 240)
The attack appears to be methodical in that the sequence of addresses probed are almost exactly evenly spaced.
The IP address range 202.232.0.0 - 202.235.255.255 (JPNIC-NET-JP) is owned by Japan Network Information Center

6. Correlations:

June 11, 2000 -	Bill Stewart Lone scan to 202.235.50.12.65535 > Subnet2.189.8080
June 3, 2000 -	Paul Zimski - Site Scan from 202.235.50.12
June 1, 2000 1000	Daragh Carter - Two scans 202.235.50.12.65535 > us.us.us.33.8080 and us.us.us.40.8080
June 1, 2000 1400 -	Klaus Steding-Jessen - DNS probe from 202.235.50.12
June 3, 2000 -	Paul Zimski - Site Scan from 202.235.50.12
May 30, 2000 1100 -	Stephan Odak - Network Scan from 202.235.50.12

The following, although from a different source address appear to be using the same program / settings to generate their scan.

May 30, 2000 0900 -	R. Jesus Garcia - WinGate 8080 scan - src: 207.78.247.50:65535 through 6 host
May 29, 2000 -	Taurfish Technology Services 207.78.247.50:65535->8080
May 28, 2000 1100 -	Thom Dyson Director of Information Services Sybex, Inc. - Scan of 6 addresses from 207.78.247.50: 65535->8080
May 28, 2000 1030 -	Earle Lane - Scan of 5 addresses from 207.78.247.50:65535->8080
May 26, 2000 1000 -	Laurie - Scan of 12 addresses from 207.78.247.50:65535 ->8080
May 25, 2000 -	Phillip - Scan of 5 addresses from 207.78.247.50:65535->8080 Terry Wells - Scan of 5 addresses from 207.78.247.50:65535->8080
May 23, 2000 0800 -	Arrigo Scan of 4 addresses from 207.78.247.50:65535->8080

7. Evidence of active targeting:

a) Characteristics of packets are inconsistent with normal TCP/IP behavior since:
   - Sequence numbers do not change, are fixed at **0x3E760000**
   - Source port for all 'responses' to various addresses is always the same: 65536

- TTL value is the same high number, which is higher than any that typical of any system OSs other than Solaris 2.x
- IP ID numbers never change, indicating crafted packets

b) The last three addresses under attack are exactly x.x.x.32 apart. (The difference between the first and the second is very close to that value at x.x.x.30.) This could be an indicator of a planned and not very random attack.

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

Critical - Attack appears to be in search of WinGate services, which, if found, could be utilized to launch a Denial of Service Attack
Assigned value - 4

Lethal - If WinGate was found on targeted machine, the buffer space could be easily consumed.
(Ref :www.hopper.dynip.com/SilentEarth/htm/wingate_out_of_buffer_dos.htm)
Assigned value - 4

Countermeasures -

System - Unknown
Assigned value - 3

Network - Tools being used to gather and analyze intrusion detection indicates an active interest in the process of intrusion detection. Although this suggests that this site actively looks after the details of their network operation it is not uncommon that while one side of network support is vigilant other individuals are not. This quantity is also unknown from the information provided.
Assigned value - 3

Severity = (4 + 4) - (3 + 3) = +2

9. Defensive recommendation:

This vulnerability appears in all versions of Wingate. If this service is not used, blocking TCP 8080 would be one option. If Wingate is being used, only trusted ip addresses should be allowed access to the service.

10. Multiple choice question:

This trace is most probably a probe to attack,

a) Domain Name Server services
b) Post Office Protocol Services
c) Windows Name Services
d) Alternate HTTP Services

Answer - d.

Intrusion Detect # 2 - SNMP Scan

p156_52.kyungpook.ac.kr

May 15 17:37:12 : Deny inbound udp src 209.86.13.111/1027 dst x.x.x.229/161
May 15 17:37:12 : Deny inbound udp src 209.86.13.111/1027 dst x.x.x.228/161

May 15 17:37:12 : Deny inbound udp src 209.86.13.111/1027 dst x.x.x.227/161

1. Source of trace:

   http://www.sans.org/y2k/052100.htm

2. Source generated by:

   Source type unknown, possibly a firewall or filtering router.

   Fields of Interest:

Date Time:	May 15 17:37:12
Action taken:	Deny inbound
Type of Packet:	UDP
Source Address:	209.86.13.111, EarthLink, Inc. (NET-EARTHLINK2000-E)
Source Port:	1027
Destination Address:	x.x.x.229 decrementing to x.x.x.227
Destination Port:	161

3. Possibility that the source address was spoofed.

   Since the attack appears to be a scan of ports for active SNMP services, it seems that a spoofed address is unlikely because the attacker is attempting to get a reply. The possibility of the attacker working through a proxy is not known.

4. Description of Attack:

   Attack is against UDP port 161, this is a scan for active Simple Network Management Services (SNMP).

5. Attack mechanism:

   This attack is a scan attempt (or a portion of one) to find open SNMP services on a descending series of network addresses.
   If these services are found available, the attacker can potentially utilize this mechanism to learn the configuration of the attacked network and / or launch a denial of service attack.

6. Correlations:

   No other activity from this address has been found reported to Global Incident Analysis Center since January 2000. Other attacks against port 161 have been noted including:

   May 12, 2000 - Bryce Alexander
   April 26, 2000 - David Hoelzer
   March 22, 2000 - 1700 Laurie
   March 20, 2000 - Erik Fichtner

7. Evidence of active targeting:

   The attack originates from an external address and is destined for an decrementing series of addresses. While requests a management host to discover what else is on its network have "leaked" onto the internet, it doesn't seem likely here. It has also been seen that laptop computers looking for a HP JetDirect printer have caused similar traffic, which also appears unlikely in this case.

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

Critical - Attack appears to be in search of SNMP services, which, if found, could be utilized to discover network configuration on a victims network and to launch a Denial of Service Attack. Possibility of being effective against a router.
Assigned value - 5

Lethal - Could cause a denial of service.
Assigned value - 4

Countermeasures -

System - Unknown
Assigned value - 3

Network - This intrusion was effectively blocked by the device, which provided this trace, in that UDP traffic was denied to port 161. Other means of possible connection to the network, however, are not known.
Assigned value - 4

Severity = (5 + 4) - (3 + 7) = +2

9. Defensive recommendation:

Ensure that all devices which allow connectivity into the network block all SNMP traffic.

10. Multiple choice question:

This trace is most probably an attack against,

a) Domain Name Server services
b) Post Office Protocol Services
c) Windows Name Services
d) Simple Network Management Protocol

Answer - d.

Intrusion Detect # 3 - RingZero Trojan Variant with Socks (Network Mapping by another name)

14:28:15 drop 172.20.20.136 192.168.16.1 tcp 3128
14:28:15 drop 172.20.20.136 192.168.16.1 tcp http-proxy
14:28:15 drop 172.20.20.136 192.168.16.2 tcp http-proxy
14:28:15 drop 172.20.20.136 192.168.16.1 tcp 1080
14:28:15 drop 172.20.20.136 192.168.16.3 tcp 3128
14:28:15 drop 172.20.20.136 192.168.16.2 tcp 3128
14:28:15 drop 172.20.20.136 192.168.16.2 tcp 1080
14:28:15 drop 172.20.20.136 192.168.16.3 tcp http-proxy
14:28:15 drop 172.20.20.136 192.168.16.3 tcp 1080
14:28:15 drop 172.20.20.136 192.168.16.4 tcp 3128
(incidentally, this scan ends up scanning 1080 twice, then by the end of the .17 network, 3 times!)

1. Source of trace:

http://www.sans.org/y2k/010700-1215.htm

2. Source generated by:

   Source unknown: firewall or filter router perhaps

   Fields of Interest:

Time:	14:28:15
Action taken:	drop
Source address:	172.20.20.136
Destination address:	192.168.16.4
Type of packet:	TCP
Port / type of service:	1080 / http-proxy / 3128

3. Possibility that the source address was spoofed.

   Since the attack appears to be an attempt to map a sequence of network ports, it seems that a spoofed address is unlikely because the attacker is attempting to get a reply. The possibility of the attacker working through a proxy is not known.

4. Description of Attack:

   This attack works by attempting to make a TCP connection and to identify an open port to the services available on the ports shown.

5. Attack mechanism:

   Initially, this attack looks like yet another variant of the common and boring RingZero scan. What is worthy of note, however, is that the scan is stepping through a series of ports. Thus it could be that an attempt is being made to hide a mapping attack inside what appears to be a RingZero Scan. The attacker is somewhat randomizing his attack in that the scan is not sequential, but for each address, the doors to each of the three ports (1080, 3128, and http-proxy) are rattled.

6. Correlations:

   No other activity from this address has been found reported to Global Incident Analysis Center since January 2000.

   A typical RingZero attack is represented by:

   January 21, 2000 - Chris

   Another representation of a RingZero attack with the Socks variant is represented by:

   April 28, 2000 - David Nolan

   Discussion regarding RingZero mapping (Ignorance Detector) by Stephen Northcutt is available at:

   http://www.sans.org/y2k/050300-1100.htm

7. Evidence of active targeting:

   First, since there is no common service associated with the 'well known' address of 3128, this indicates that something other than normal network activity is occurring. The semi-sequential but thorough scan of three different service ports for each address indicates that the attacker is deliberately after available open ports on each of the addresses in these two segments (192.168.16.x and 192.168.17.x).

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

Critical - Attack appears to be in search of open ports on anything which is attached to any of the addresses scanned, and is not specifically targeted at servers, routers or other significant assets.
Assigned value - 3

Lethal - This attack in itself will not do any damage but it is likely to be followed by an attack targeted at a specific address or addresses.
Assigned value - 2

Countermeasures -

System - Unknown whether any system countermeasures are in place to stop this attack other than the device which dropped the incoming packet
Assigned value - 4

Network - It is not known whether this attack would be stopped by any other device on the network nor whether any assets on this address range on the network have any of these ports open.
Assigned value - 3

Severity = (3 + 2) - (4 + 3) = -2

9. Defensive recommendation:

It would be wise to assure that these three ports are only open on the systems, which require the service associated with them. Port 3128 should not be open on any. The filtering device, which dropped these packets, seems to be doing what is required from that entry point to deny this connectivity. It would be prudent to keep watch for future activity from this source address, though a resulting attack may be launched from anywhere.

10. Multiple choice question:

This attack involving tcp ports 1080, 3128, and http-proxy is

a) An attempt to flood the ports as part of a denial of service attack.
b) An indicator of a trivial RingZero scan.
c) A scan for available web services.
d) A device to conceal a more sinister mapping attack.

Answer - d.

Intrusion Detect # 4 POP II Scan

keiei001.business.ube-k.ac.jp.

```
05/22 10:52:35.392671 202.18.185.11.0 > 10.2.8.1.109:
  SF 386203648:386203648(0) win 512 (ttl 225, id 24579)
05/22 10:52:40.491957 202.18.185.11.0 > 10.2.9.1.109:
  SF 386203648:386203648(0) win 512 (ttl 225, id 4867)
05/22 10:52:50.695775 202.18.185.11.0 > 10.2.11.1.109:
  SF 386203648:386203648(0) win 512 (ttl 225, id 28417)
05/22 11:14:15.933964 202.18.185.11.0 > 10.2.8.2.109:
  SF 386203648:386203648(0) win 512 (ttl 225, id 9988)
05/22 11:14:21.031330 202.18.185.11.0 > 10.2.9.2.109:
  SF 386203648:386203648(0) win 512 (ttl 225, id 2050)
```

```
05/22 11:14:31.243858 202.18.185.11.0 > 10.2.11.2.109:
  SF 386203648:386203648(0) win 512 (ttl 225, id 4097)
05/22 11:57:53.509343 202.18.185.11.0 > 10.2.11.4.109:
  SF 386203648:386203648(0) win 512 (ttl 225, id 47108)
```

1. Source of trace:

   http://www.sans.org/y2k/052800-1130.htm

2. Source generated by:

   tcpdump

   Fields of interest:

   Fields of Interest:

Time:	Start -	10:52:35
	End -	11:57:53
Duration:		5 Min. 18 Sec. (Low and Slow)
Service Type:		TCP
Total Number of Detects:		7
Source of Attack:		202.18.185.11 JPNIC-NET-JP Japan Network Information Center
Destination:		10.2.11.4
Destination Port:		109 - Post Office Protocol - Version 2
Sequence Number:		386203648 (Static)
TTL:		225
IP ID:		Non Sequential
Flags Set:		Syn and Fin

3. Possibility that the source address was spoofed.

   This could only be a denial of service attack if the simultaneous SF flag settings is intended to lockup the victim target. It is more probable that the attacker is probing with the intent of finding an open port so a non-spoofed source address would be required.

4. Description of Attack:

   The purpose of POP 2 scans has been to find services left open on Port 109 for this rarely used protocol. Because of the low and slow nature of this attack, it may be an attempt by the attacker to do mapping of the victim's network.

5. Attack mechanism:

   This attacker appears to be attempting to penetrate firewall defenses by having the Syn Fin flags set, since some firewalls do not block packets with the Fin flag set, which improves the possibility of a response, and since the Fin signals the termination of a signal connection, some logging devices may not report it. The penetration is slow and random and may be a part of a long term mapping project.

6. Correlations:

   No other activity from this address has been found reported to Global Incident Analysis Center since January 2000.

   Examples of typical POP 2 attacks are represented by:
   May 27, 2000 2000 - Lloyd

7. Evidence of active targeting:

   Since Syn and Fin flags do not occur 'naturally' as part of a TCP three way handshake process, these packets have to have been crafted and directed against the target address. The flags setting, the source port equal to 0, and the static Sequence number have been observed in many attacks which use the program which generated this traffic. The large TTL value is also another probable indicator of crafted packet activity, but is rather overwhelmed by the preponderance of other indicators.

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

   Critical - This attack appears to be directed at POP 2 services, which are rarely used at this time. This would probably be on an older Unix computer. However, it may also be part of a larger mapping effort.
   Assigned value - 3

   Lethal - This attack in itself will not do any damage but if it is actually a mapping attempt, it could be followed by an attack targeted at a specific address or addresses.
   Assigned value - 1

   Countermeasures -

   System - Since few systems make use of this service, it can be expected that few will have this port open
   Assigned value - 4

   Network - It is not known whether this attack was stopped by the perimeter network devices.
   Assigned value - 2

   Severity = (3 + 1) - (4 + 2) = -2

9. Defensive recommendation:

   The perimeter network filtering devices should block all access to this obsolete port, and all systems should have this service port disabled.

10. Multiple choice question:

    What indicators in this trace are certain indicators that these packets have been generated artificially?

    a) Source address and IP ID.
    b) IP ID and TTL value.
    c) Win size and TTL value.
    d) Sequence number and Source Port.

    Answer - d.

Intrusion Detect # 5 Portscan

May 16 21:20:24 dns1 snort[51901]: spp_portscan:
PORTSCAN DETECTED from 24.65.93.104
May 16 21:20:30 dns1 snort[51901]: spp_portscan:
portscan status from 24.65.93.104: 6 connections across 1 hosts:
TCP(6), UDP(0)
May 16 21:20:36 dns1 snort[51901]: spp_portscan:
End of portscan from 24.65.93.104

May 16 21:20:23 24.65.93.104:2830 -> z.y.w.34:79 SYN **S*****
May 16 21:20:24 24.65.93.104:2841 -> z.y.w.34:23 SYN **S*****
May 16 21:20:23 24.65.93.104:2833 -> z.y.w.34:80 SYN **S*****
May 16 21:20:24 24.65.93.104:2834 -> z.y.w.34:143 SYN **S*****
May 16 21:20:24 24.65.93.104:2836 -> z.y.w.34:53 SYN **S*****
May 16 21:20:24 24.65.93.104:2838 -> z.y.w.34:110 SYN **S*****

1. Source of trace:

   http://www.sans.org/y2k/052000.htm

2. Source generated by:

   Snort

   Fields of interest:

Date / Time:	May 16 21:20:24	
Source Address:	24.65.93.104	
Source Port:	2830 incrementing to 2838	
Destination Address:	z.y.w.34	
Type of Service:	TCP	
Destination Ports:	23	Telnet
	53	Domain Name Server
	79	Finger
	80	World Wide Web - HTTP
	110	Post Office Protocol - Version 3
	143	Internet Message Access Protocol
Flags Set:	Syn	

3. Possibility that the source address was spoofed.

   This scan would not be effective unless the reply information is returned to the attacking host. The source address may be a proxy but other than that possible hopping point, the address is real.

4. Description of Attack:

   This attack is a quick and dirty attempt to determine the availability of the most vulnerable and most interesting ports on the target device. Access to them could give the attacker root privileges at worst or at least allow them manipulative access to the system.

5. Attack mechanism:

   The attacker sent Syn requests to the ports of interest. They have been sent quickly and only once. And they have all been sent to only one network address. With the reply the attacker will know which vulnerabilities can be exploited against this device.

6. Correlations:

   The attacker made the following Portscan the following day. Although the address being attacked is different, the order in which the ports are being scanned is identical to the previous day's scan.

   May 16 22:17:38 24.65.93.104:4397 -> z.y.w.98:79 SYN **S*****
   May 16 22:17:38 24.65.93.104:4408 -> z.y.w.98:23 SYN **S*****
   May 16 22:17:38 24.65.93.104:4401 -> z.y.w.98:80 SYN **S*****
   May 16 22:17:38 24.65.93.104:4402 -> z.y.w.98:143 SYN **S*****
   May 16 22:17:38 24.65.93.104:4404 -> z.y.w.98:53 SYN **S*****
   May 16 22:17:38 24.65.93.104:4406 -> z.y.w.98:110 SYN **S*****

7. Evidence of active targeting:

   This attacker is after the power tools of a system and with his return the following day has demonstrated that he is serious about this probe.

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

   Critical - This attacker appears determined to gain the keys to controlling systems on this network.
   Assigned value - 5

   Lethal - If the attacker is successful in finding and gaining access to these ports, he could 'own' this network with root privileges, or at least make it a very bad day for the system administrator of the z.y.w.x network.
   Assigned value - 5

   Countermeasures -

   System - There is no indication from the traces provided what the current status of system patches to address the vulnerabilities at these ports is. Without the proper patches, filters and denied access, the vulnerability is great.
   Assigned value - 3

   Network - These intrusion attempts were detected by the Intrusion Detection system, and it would be prudent if the firewall or filtering router protecting the network was configured similarly to block them. Unfortunately we have no information that this is the case.
   Assigned value - 2

   Severity = (5 + 5) - (3 + 2) = 5

9. Defensive recommendation:

   Filter all incoming Syn requests at the firewall or filtering router, make certain all available vulnerability patches have been installed, close all of these ports internally which are not necessary for this network's operation.

10. Multiple choice question:

    The services under attack in this port scan include:

    a) FTP, DNS, and TFTP

b) IMAP, TELNET, and FTP
c) HTTP, SMTP, and DNS
d) TELNET, DNS, and IMAP

Answer - d.

Intrusion Detect # 6 IMAP 143/tcp

IMAP 143/tcp

```
May 25 12:52:10 firewall kernel: Packet log: input DENY eth0 PROTO=6
  206.244.48.17:1060 MY.HOST.211:143 L=48 S=0x00 I=19973 F=0x4000 T=120 SYN
  (#11)
May 25 12:52:13 firewall kernel: Packet log: input DENY eth0 PROTO=6
  206.244.48.17:1060 MY.HOST.211:143 L=48 S=0x00 I=20997 F=0x4000 T=120 SYN
  (#11)
May 25 12:52:19 firewall kernel: Packet log: input DENY eth0 PROTO=6
  206.244.48.17:1060 MY.HOST.211:143 L=48 S=0x00 I=25093 F=0x4000 T=120 SYN
  (#11)
May 25 12:52:31 firewall kernel: Packet log: input DENY eth0 PROTO=6
  206.244.48.17:1060 MY.HOST.211:143 L=48 S=0x00 I=35333 F=0x4000 T=120 SYN
  (#11)
```

1. Source of trace:

   http://www.sans.org/y2k/053000-1000.htm

2. Source generated by:

   Source Unknown - Apparently a firewall of some sort.

   Fields of Interest:

Time:	Start -	12:52:10
	End -	12:52:31
Number of Detects:		4
Source of Attack:		206.244.48.17
Source Port:		1060
Destination host:		MY.HOST.211
Destination Port:		143 IMAP
Type of Service:		TCP
IP ID:		19973 incrementing to 35333

3. Possibility that the source address was spoofed.

   This attacker is expecting a response back to determine if IMAP access is available.

4. Description of Attack:

   This is an attempt to determine if Port 143 IMAP is responding on this service.

5. Attack mechanism:

   The attacker's computer makes four attempts to initiate a connection with the Port 143 on the device attached at this address.

6. Correlations:

   No other activity from this address has been found reported to Global Incident Analysis Center since January 2000.

   Other incidents of IMAP attacks are represented by:
   June 6, 2000 - Laurie
   May 18, 2000 - Alex Luetzow

7. Evidence of active targeting:

   Due to the risks associated with IMAP vulnerabilities, any attempt made to connect to this service must be considered hostile.

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

   Critical - Although this is only a probe to determine the availability of IMAP service on the device probed, the vulnerabilities inherent in having an open IMAP port known are great.
   Assigned value - 5

   Lethal - Although this is only a probe to determine the availability of IMAP service, any availability of open access to this service could quickly lead to root privilege available to the attacker - and this is a bad thing.
   Assigned value - 5

   Countermeasures -

   System - It is not shown here whether the IMAP port is open on the device under attack, or if vulnerability patches have been installed to the operating system.
   Assigned value - 3

   Network - The firewall denied this request for access but whether the routers also block this access is unknown.
   Assigned value - 2

   Severity = (5 + 5) - (3 + 2) = 5

9. Defensive recommendation:

   Deny all access to IMAP services, and install all available IMAP vulnerability patches to system OS.

10. Multiple choice question:

    Why is it of interest to the system administrator to block access to the port in the trace above?

    a) Access to this port would initiate IRC chat services.
    b) Access to this port will allow the attacker to send email.
    c) Access to this port could provide proxy services to the attacker.
    d) Access to this port could provide root privileges to the attacker.

    Answer - d.

Intrusion Detect # 7 Syn Flood

[**] spp_portscan: PORTSCAN DETECTED from 194.44.187.30 [**]
06/06-03:43:20.989732
Jun 6 03:43:20 194.44.187.30:0 -> 216.17.46.99:1402 UNKNOWN 21S***A*
RESERVEDBITS
Jun 6 03:43:35 194.44.187.30:1414 -> 216.17.46.99:80 SYN **S*****
Jun 6 03:43:46 194.44.187.30:1416 -> 216.17.46.99:80 SYN **S*****
Jun 6 03:43:55 194.44.187.30:1416 -> 216.17.46.99:80 SYN **S*****
Jun 6 03:44:08 194.44.187.30:1418 -> 216.17.46.99:80 SYN **S*****
Jun 6 03:44:17 194.44.187.30:1418 -> 216.17.46.99:80 SYN **S*****
Jun 6 03:44:25 194.44.187.30:1420 -> 216.17.46.99:80 SYN **S*****
Jun 6 03:44:32 194.44.187.30:1423 -> 216.17.46.99:80 SYN **S*****

1. Source of trace:

   http://www.sans.org/y2k/060700.htm

2. Source generated by:

   Source Unknown

   Fields of Interest:

Time:	Start -	03:43:20
	End -	03:44:32
Duration:		1 Min. 12 Sec.
Service Type:		TCP
Total Number of Detects:		8
Source of Attack:		194.44.187.30 Volynian State University
Source Port:		1414 to 1423 incrementing
Destination:		216.17.46.99
Destination Port:		80 - World Wide Web - HTTP
Flags Set:		Syn

3. Possibility that the source address was spoofed.

   Since this attack represents a burst of Syn requests to the same TCP port without waiting for a response Ack, it is apparent that no response is expected. This attack could very well work with a spoofed source address.

4. Description of Attack:

   This attack is against TCP port 80 HTTP. This is a buffer overflow attack, which is directed at the buffer containing the connection requests waiting to be processed.

5. Attack mechanism:

   This attack initiates a series of TCP connection requests in quick succession, but does not expect or desire a response. The intent is to saturate the buffers so that no legitimate requests for service can be processed. This process is used as part of a hijack of a connection between two hosts in order to silence the host whose identity is stolen.

6. Correlations:

   No other activity from this source address has been found reported to Global Incident Analysis Center since January 2000.

Other incidents of Syn flooding are represented by:
February 8, 2000 2300 - Andy
February 2, 2000 - Erik Fichtner

7. Evidence of active targeting:

   The number of connection attempts made to the same address / port combination in quick succession, as well as the unusual event at the beginning of the sequence, strongly suggest active targeting.

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

   Critical - This event is directed against one system, and not at a critical service (sorry kids.)
   Assigned value - 2

   Lethal - This event is a big annoyance but is not going to kill this system. If it is used to quiet this system while another is being attacked, the other system could be in trouble. But this system will live to surf another day.
   Assigned value - 2

   Countermeasures -

   System - It is unknown what buffer capacity the system being targeted has, or what its time-out setting for connections waiting in cue is.
   Assigned value - 4

   Network - It is not known whether this attack was stopped by the perimeter network devices.
   Assigned value - 2

   Severity = (2 + 2) - (4 + 2) = -2

9. Defensive recommendation:

   Block all incoming Syn requests at the firewall or filtering router.

10. Multiple choice question:

    Why is this trace not typical of a portscan?

    a) Portscans do not utilize incrementing source ports.
    b) Portscans always attack multiple addresses on the same port.
    c) Portscans always attack multiple addresses and multiple ports.
    d) Portscans attack multiple ports on the same address.

    Answer - d.

Intrusion Detect # 8 UDP 137 - NETBIOS Name Service Mapping

10:26:09	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.1	on unserved	port 137
10:26:10	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.1	on unserved	port 137

10:26:13	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.2	on unserved	port 137
10:26:15	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.2	on unserved	port 137
10:26:18	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.3	on unserved	port 137
10:26:21	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.3	on unserved	port 137
10:33:30	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.97	on unserved	port 137
10:33:32	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.97	on unserved	port 137
10:33:36	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.98	on unserved	port 137
10:33:37	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.98	on unserved	port 137
10:33:39	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.99	on unserved	port 137
10:33:42	unix firewall: securityalert	udp from	UUNET:137	to	Unused Segment.99	on unserved	port 137

1. Source of trace:

   Local Office of Major Nationwide Corporate Enterprise

2. Source generated by:

   Unix Firewall

   Fields of Interest:

Time:	Start -	10:26:09
	End -	10:33:42
Duration:		7 Min. 33 Sec.
Total Number of Detects:		171
Service Type:		UDP
Source:		UUNET
Source Ports:		137
Destination:		Unused Address Segment
Destination Port:		137

3. Possibility that the source address was spoofed.

   The attacker against this company is looking for responses to his blatant mapping attempt. While is possible the attacker is working through a proxy or proxies en route to this site, the existence of them is not known and it must for the moment be assumed that he is attacking from UUNET.

4. Description of Attack:

   The attacker sends two UDP packets to map the availability of NETBIOS Name Services. During the process of this trace he mapped addresses of this unused segment from 1 to 99.

5. Attack mechanism:

   The attacker is using UDP, which does not require a three-way handshake, or the establishment of a reliable connection between the attacker and his target. To insure the reliability of his mapping attempt, the attacker has sent two packets to each address in this portion of the subnet.

6. Correlations:

No other activity from this source address has been found reported to Global Incident Analysis Center since January 2000.

A similar attack was launched from LNET but the number of packets sent varied from 1 to 3 for each address, and the addresses were on a different segment.

7. Evidence of active targeting:

   It appears from the time stamp that the attacker was running a script of some sort to produce this mapping scan and because of the consistent number of hits for each address and the blatant sequential nature of the attack, it seems evident that it is active targeting.

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

   Critical - This attack is an annoying mapping attempt on an unused segment. The port to which the attacker is attempting to reach demonstrates a high degree of hostility to a highly sensitive target.
   Assigned value - 4

   Lethal - The target port the attacker is attempting to reach could cause great harm to the network if compromised.
   Assigned value - 4

   Countermeasures -

   System - All system patches for vulnerabilities are in place.
   Assigned value - 4

   Network - This network's firewall blocks all attempts to reach this port and maintains a record of the attempt.
   Assigned value - 4

   Severity = (4 + 4) - (4 + 4) = 0

9. Defensive recommendation:

   Monitor firewall logs to be certain that other mapping attempts using different ports which perhaps are not filtered allow for network incursion.

10. Multiple choice question:

    Which of the following is true about the trace above.

    a) The reason the Syn flag is not shown is because of the output of the firewall used.
    b) The attacker has attempted to map all addresses in the Unused Segment.
    c) The attacker is attempting a denial of service against this network.
    d) The technique in use is not commonly called "low and slow"

    Answer - d.

Intrusion Detect # 9 UDP Denial of Service?

18:08:02	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:08:04	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573

18:08:07	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:08:09	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:08:12	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:08:14	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:14:17	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:14:22	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:14:24	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:14:27	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:14:29	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573
18:14:31	unix firewall: security alert	udp from	FreeI Net:573	to	Unused Server	on unserved	port 573

1. Source of trace:

   Local Office of Major Nationwide Corporate Enterprise

2. Source generated by:

   Unix Firewall

   Fields of Interest:

Time:	Start -	18:08:02
	End -	18:14:31
Duration:		6 Min. 29 Sec.
Total Number of Detects:		141
Source:		FreeI Network ISP
Source Ports:		573
Destination:		Unused Address - Formerly assigned to a server
Destination Port:		573 - Banyan - VIP

3. Possibility that the source address was spoofed.

   This attack is based on the reliable assurance that the source address is an ISP. No address spoofing necessary.

4. Description of Attack:

   This trace appears to be a denial of service attempt using udp. What is actually happening is that in the forgotten past of this organization, at least forgotten by some, the network they ran was Banyan Vines, pre-Novell and pre-NT. The laptops they provided to their "executives" were setup to dial into the mail system, so those on the road could stay in touch with the home office. Well, laptops are hard to get so when the call went out to turn in the laptops for upgrade, those fearful of not getting another one kept the one they had. They can still use the application they had before, and liked and don't want to be forced from using anyway. The only inconvenience is that they cannot connect to the corporate email system. The cure for this is to establish an email account with Yahoo or MSN or HotMail or wherever and have the corporate email forwarded to that account. They can easily reach that account at the home office, and if they establish a FreeI Net account they can reach it on the road with their old laptop too.

5. Attack mechanism:

The problem with the solution above is that these laptops are still configured to attach via the corporate modem to the Banyan server using Banyan Vines Internet Protocol. So, for the duration of their connection to their internet account, the laptop continues to attempt to 'phone home'.

6. Correlations:

   So that FreeI Net does not get all of the free publicity, many of the corporate travelers choose AOL instead with traces which resolve there to prove it.

7. Evidence of active targeting:

   The 'attackers' are not operating within the guidelines of corporate policy, and I'm certain that the traces are annoying, but they are not actively targeting the corporate network.

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

   Critical - Service no longer exists.
   Assigned value - 1

   Lethal - No advantage could be gained if the sevice did exist.
   Assigned value - 1

   Countermeasures -

   System - No vulnerabilities
   Assigned value - 5

   Network - This network's firewall blocks all attempts to reach this port but maintains an annoying record of the attempt.
   Assigned value - 4

   Severity = (1 + 1) - (5 + 4) = 7

9. Defensive recommendation:

   Find the existing laptop computers and remove the Banyan files or reconfigure the firewall filter to ignore incursion attempts to this port and wait until either the executives or their laptops retire. Of the two options, the second is the most probable.

10. Multiple choice question:

    The best method to resolve this problem would include:

    a) Calling FreeI Net to find out why they are not blocking denial of service attacks
    b) Blocking all UDP traffic at the firewall
    c) Reinstallation of the Unused Server to monitor UDP traffic coming into it.
    d) Asking the system administrator what 'well known' UDP port is for.

    Answer - d.

Intrusion Detect # 10 - IRC / Port Mapping

16:49:40	unix firewall: security alert	tcp from	Portugal ISP:1025	to	Temp Office.156	on unserved	port 6667
16:49:41	unix firewall: security alert	tcp from	Portugal ISP:1025	to	Temp Office.156	on unserved	port 6667

16:49:40	unix firewall: security alert	tcp from	Portugal ISP:1026	to	Temp Office.157	on unserved	port 6667
16:49:41	unix firewall: security alert	tcp from	Portugal ISP:1026	to	Temp Office.157	on unserved	port 6667
16:49:41	unix firewall: security alert	tcp from	Portugal ISP:1027	to	Temp Office.158	on unserved	port 6667
16:49:40	unix firewall: security alert	tcp from	Portugal ISP:1027	to	Temp Office.158	on unserved	port 6667
16:49:40	unix firewall: security alert	tcp from	Portugal ISP:1028	to	Temp Office.159	on unserved	port 6667
16:49:42	unix firewall: security alert	tcp from	Portugal ISP:1028	to	Temp Office.159	on unserved	port 6667
16:49:46	unix firewall: security alert	tcp from	Portugal ISP:1122	to	Temp Office.251	on unserved	port 6667
16:49:47	unix firewall: security alert	tcp from	Portugal ISP:1122	to	Temp Office.251	on unserved	port 6667
16:49:48	unix firewall: security alert	tcp from	Portugal ISP:1122	to	Temp Office.251	on unserved	port 6667
16:49:49	unix firewall: security alert	tcp from	Portugal ISP:1122	to	Temp Office.251	on unserved	port 6667
16:49:47	unix firewall: security alert	tcp from	Portugal ISP:1123	to	Temp Office.252	on unserved	port 6667
16:49:48	unix firewall: security alert	tcp from	Portugal ISP:1123	to	Temp Office.252	on unserved	port 6667
16:49:49	unix firewall: security alert	tcp from	Portugal ISP:1123	to	Temp Office.252	on unserved	port 6667
16:49:46	unix firewall: security alert	tcp from	Portugal ISP:1123	to	Temp Office.252	on unserved	port 6667
16:49:49	unix firewall: security alert	tcp from	Portugal ISP:1124	to	Temp Office.253	on unserved	port 6667
16:49:50	unix firewall: security alert	tcp from	Portugal ISP:1124	to	Temp Office.253	on unserved	port 6667
16:49:46	unix firewall: security alert	tcp from	Portugal ISP:1125	to	Temp Office.254	on unserved	port 6667
16:49:47	unix firewall: security alert	tcp from	Portugal ISP:1125	to	Temp Office.254	on unserved	port 6667
16:49:48	unix firewall: security alert	tcp from	Portugal ISP:1125	to	Temp Office.254	on unserved	port 6667

1. Source of trace:

   Local Office of Major Nationwide Corporate Enterprise

2. Source generated by:

   Unix Firewall

   Fields of Interest:

Time:	Start -	16:49:40
	End -	16:49:50
Duration:		10 Seconds
Total Number of Detects:		282
Number of Addresses Mapped:		99
Type of Service		TCP
Source:		Portugal ISP
Source Ports:		1025 to 1125 ascending in groups of 2 to 4
Destination:		Office for Temporary Employees
Destination Port:		6667 - IRC - Internet Relay Chat

3. Possibility that the source address was spoofed.

   The attacker is looking for responses on the IRC port and doing a real thorough job of mapping 99 of the available IP addresses in that segment.

4. Description of Attack:

   The attacker managed in a matter of 10 seconds to deliver a mapping request of 282 packets for a map of 99 addresses by using the somewhat innocuous IRC port.

5. Attack mechanism:

   The attacker has a program available to rapidly dump tcp connection requests to a section of a subnet to find available IRC clients.

6. Correlations:

   Another similar scan was made from this same ISP against another block of addresses on this same subnet.

7. Evidence of active targeting:

   The office in which this subnet lives is used for Temporary Employees who have been known to attempt to use programs which are not approved in the corporate offices or on the corporate network. The corporate policy is to take a dim view of any attempt utilize IRC and views this activity as hostile. At the very least the corporation is not pleased to have their network mapped, but according to their corporate lawyers, mapping is not illegal. (Yet. Editorial comment)

8. Severity: = (Critical + Lethal) - (System + Net Countermeasures)

   Critical - Use of this service in itself, does not necessarily compromise system access, but it would be a method to facilitate future attacks since computer locations are identified by it.
   Assigned value - 3

   Lethal - No access rights or root privileges come with this program although it does raise bandwidth concerns.
   Assigned value - 3

   Countermeasures -

   System - Networked system owned by the local office are configured to prevent the installation of unauthorized software necessary to utilize IRC. Some contracts with temporary employee providers have stipulated that the employees' parent company will provide their computer. The constraints, placed on these computers have been less stringent than those owned by the corporate office. This has cause system operational concern of which this event is an example.
   Assigned value - 3

   Network - This network's firewall blocks all attempts to reach this port and maintains a record of the attempt.
   Assigned value - 4

   Severity = (3 + 3) - (3 + 4) = -1

9. Defensive recommendation:

   Allow only computers owned by the local office to be connected to the network, with appropriate penalties to those who violate the policy, to include dismissal. Unfortunately, the reason the temporary employees are utilized is because the local office does not have the budget to hire permanent employees and provide them with equipment.

10. Multiple choice question:

This detect is not a denial of service attack because:

a) Only one destination port is in use.
b) Multiple source ports are being used.
c) Only one destination address is being targeted.
d) Multiple destination addresses are targeted.

Answer - d.