Global Information Assurance Certification Paper

These analyses were developed by George McKee for the practical examination following the IDIC course curriculum attended at SANS SNAP 2000, San Jose.

Detect 1

Jun 11 02:22:49.199 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (210.206.72.130->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4661->110)

Jun 11 02:22:49.200 inet01 firelogd[111]: 226 IP packet dropped (210.206.72.130->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4661->110): Restricted Port: Protocol=TCP[SYN] Port 4661->110 (received on interface xxx.xxx.xxx.253)

Jun 10 19:41:42.656 inet02 firelogd[273]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.112 (210.206.72.130->xxx.xxx.xxx.112: Protocol=TCP[SYN] Port 2111->110)

Jun 11 02:14:02.781 inet02 firelogd[273]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.112 (210.206.72.130->xxx.xxx.xxx.112: Protocol=TCP[SYN] Port 4619->110)

Jun 11 02:14:02.785 inet02 firelogd[273]: 226 IP packet dropped (210.206.72.130->xxx.xxx.xxx.112: Protocol=TCP[SYN] Port 4619->110): Restricted Port: Protocol=TCP[SYN] Port 4619->110 (received on interface xxx.xxx.xxx.112)

No DNS.
Port 110 = POP3

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Axent Raptor Firewall
3. Probability the source route was spoofed
    a. Probably not. The address is allocated by the APNIC to a Korean organization. Korea is a known source of state-sponsored hacking.

    inetnum: 210.206.72.128-210.206.72.191
    netname: KRVELRYUESSET-YG
    descr: Korea Value Asset
    descr: 198 Uljiro2-Ga Joong-Gu
    descr: SEOUL
    country: KR.

    b. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for POP3 servers
    b. Script kiddy probably got a new application
    c. Information is obtained if the server responds with a SYN/ACK to the attacker
5. Attack Mechanism
    a. Attacker tries to locate POP3 servers in order to run exploits against them
    b. This works on a TCP 3-way handshake. Attacker sends SYN to victim to port 110. Victim responds with a SYN/ACK a POP3 server is installed.
6. Correlations
    a. This scan was detected on two different firewalls (inet01 and inet02 in the traces) on June 10 and June 11
7. Evidence of Active Targeting

    a. Unlikely. The June 11 traces show probes 140 addresses apart separated by 8 minutes, suggesting a systematic address-by-address scan.
8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. What will attacker learn from this attempt:
        a) Host is listening for Telnet
        b) Host is a router
        c) Host is a NT server
        d) None of the above.

Answer d)

Detect 2

From a log extending from midnight to 4pm on June 11
6 pings at 0:18, 0:45, 1:13, 1:40, 2:07, 2:34, 3:02, 3:29, 3:57, 4:24, 5:12, 5:46, 6:13, 7:36, 8:04, 8:32, 9:28, 9:55, 10:23, 10:51, 11:20, 12:15, 12:43, 13:11, 13:38, 14:06, 14:34, 15:02, 15:31

Jun 11 07:36:31.953 inet02 firelogd[273]: 226 IP packet dropped (4.4.106.15->xxx.xxx.xxx.120: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)
Jun 11 07:36:33.937 inet02 firelogd[273]: 226 IP packet dropped (4.4.106.15->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)
Jun 11 07:36:55.968 inet02 firelogd[273]: 226 IP packet dropped (4.4.106.15->xxx.xxx.xxx.120: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 07:36:57.984 inet02 firelogd[273]: 226 IP packet dropped (4.4.106.15->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)
Jun 11 07:36:57.984 inet02 firelogd[273]: 226 IP packet dropped (4.4.106.15->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 07:37:20.015 inet02 firelogd[273]: 226 IP packet dropped (4.4.106.15->xxx.xxx.xxx.120: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 07:37:22.015 inet02 firelogd[273]: 226 IP packet dropped (4.4.106.15->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

DNS Name: PPPa82-ResaleJacksonMs1-5R7052.saturn.bbn.com
Address: 4.4.106.15

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Axent Raptor Firewall
3. Probability the source route was spoofed.

    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for active hosts
    b. Information is obtained if the server responds with a ECHO REPLY to the attacker
    c. This is clearly an automated scan.
5. Attack Mechanism
    a. Attacker tries to locate active hosts in order to run more targeted exploits against them later
    b. Because net 4.0.0.0 belongs to MIT, this might be a research project. However, the DNS name suggests a dialup connection from one of a range of subnets leased by MIT to GTE Internet Services (formerly BBN). It could be a GTE research project…
6. Correlations
    a. This scan was detected on two different IP addresses served by the same multi-homed firewall over a period of 15 hours.
7. Evidence of Active Targeting
    a. Unlikely. Two addresses, 5 apart, within 2 seconds of each other.
    b. Unlikely. Repeated for 15 hours even with no responses.
8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. What will attacker NOT learn from this attempt:
        i. What addresses respond to pings.
        ii. Changes in network performance hour-by-hour
        iii. What services are vulnerable
        iv. Changes in network performance second-by-second

Answer iii.)

Detect 3

Jun 11 12:03:30.984 inet02 firelogd[273]: 226 IP packet dropped (24.30.243.42->xxx.xxx.xxx.120: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 12:03:32.171 inet02 firelogd[273]: 226 IP packet dropped (24.30.243.42->xxx.xxx.xxx.120: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 12:03:44.781 inet02 firelogd[273]: 226 IP packet dropped (24.30.243.42->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 12:03:46.203 inet02 firelogd[273]: 226 IP packet dropped (24.30.243.42->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 12:03:47.218 inet02 firelogd[273]: 226 IP packet dropped (24.30.243.42->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 12:03:48.718 inet02 firelogd[273]: 226 IP packet dropped (24.30.243.42->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 12:03:47.218 inet02 firelogd[273]: 226 IP packet dropped (24.30.243.42->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

Jun 11 12:03:48.718 inet02 firelogd[273]: 226 IP packet dropped (24.30.243.42->xxx.xxx.xxx.125: Protocol=ICMP[Echo request]): Transparent Access Prohibited: Protocol=ICMP[Echo request] (received on interface xxx.xxx.xxx.112)

DNS Name: va-24-30-243-42.va.mediaone.net
Address: 24.30.243.42
Occurred only once.

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Axent Raptor Firewall
3. Probability the source route was spoofed.
    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for active hosts
    b. Information is obtained if the server responds with a ECHO REPLY to the attacker
5. Attack Mechanism
    a. Attacker tries to locate active hosts in order to run more targeted exploits against them later
6. Correlations
    a. Net 24 is known to be allocated to cable modem providers. This is confirmed by the DNS name, a well-known cable modem ISP.
7. Evidence of Active Targeting
    a. Unlikely. Two addresses, 5 apart, within 15 seconds of each other.
8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. “Transparent access prohibited” means:
        i. The LAN is based on FDDI-over-copper
        ii. The access was blocked by a firewall rule
        iii. Firewalls cannot be routers
        iv. Both ii and iii.

Answer ii.)

Detect 4

Jun 01 14:16:43.840 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (207.234.170.177->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 3722->524)
Jun 01 14:16:43.841 inet01 firelogd[111]: 226 IP packet dropped (207.234.170.177->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 3722->524): Restricted Port: Protocol=TCP[SYN] Port 3722->524 (received on interface xxx.xxx.xxx.253)

Repeated 12 times between 12:22:07 and 12:22:12

Jun 01 12:22:10.145 inet02 firelogd[273]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.112 (207.234.170.177->xxx.xxx.xxx.112: Protocol=TCP[SYN] Port 2252->524)

Repeated 14 times between 14:16:43 and 14:16:50

No DNS
207.234.170.0 is assigned to isco (NETBLK-NETRUNNER-ISCO)
3363 w.commercial blvd suite 202
ftlauderdale, FL 33309
USA
Port 524 is Novell's Netware Core Protocol (NCP)

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Axent Raptor Firewall
3. Probability the source route was spoofed.
    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for Novell Netware servers
    b. Information is obtained if the server responds with a SYN/ACK to the attacker
5. Attack Mechanism
    a. Attacker tries to locate active hosts in order to run more targeted exploits against them later. Unprotected Netware servers are likely to provide large filesystems that may contain interesting software or data.
6. Correlations
    a. Port 524 is a frequent target of port scanners. Port 524 is Novell's Netware Core Protocol (NCP), see http://www.nwconnection.com/jun.97/tcpip67/index.html for details.
    b. ***Note**: please update the "Frequently Probed Ports" page at http://www.sans.org/y2k/ports.htm with this information. Thanks.*
7. Evidence of Active Targeting
    a. Unlikely. Two addresses, 140 apart, probed two hours apart, suggests a simple address-by-address scan.
8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. "IP packet dropped" means:
        i. a SYN Flood is in progress
        ii. The access was blocked by a firewall rule

iii. The packet was delivered to a lower level in the protocol stack
iv. The data field was empty.

Answer ii)

Detect 5

Jun 02 15:28:49.338 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (207.193.15.197->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4412->1)

Jun 02 15:28:49.341 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (207.193.15.197->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4413->7)

Jun 02 15:28:49.343 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (207.193.15.197->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4414->9)

Jun 02 15:28:49.349 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (207.193.15.197->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4415->11)

Jun 02 15:28:49.388 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (207.193.15.197->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4416->13)

Jun 02 15:28:49.401 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (207.193.15.197->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4418->15)

Jun 02 15:28:49.402 inet01 firelogd[111]: 347 Possible Port Scan detected on Interface xxx.xxx.xxx.253 (207.193.15.197->xxx.xxx.xxx.253: Protocol=TCP[SYN] Port 4419->19)

Continued until 16:02

Name: ppp-207-193-15-197.hstntx.swbell.net
Address: 207.193.15.197

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Axent Raptor Firewall
3. Probability the source route was spoofed.
    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Sequential scan of well-known ports. This is a classic port scan.
    b. Information is obtained if the server responds with a SYN/ACK to the attacker
5. Attack Mechanism
    a. Attacker tries to locate active ports in order to run more targeted exploits against them later.
6. Correlations
    a. Research within our organization identified this as a benign “Tiger Team” vulnerability assessment.
7. Evidence of Active Targeting
    a. Unlikely. Data not shown indicated a similar scan on the other firewall during the same period
    b. Actually, the scan ***was*** targeted to a restricted range of addresses spanning those used by the firewalls. This is of course the major sociopolitical problem

with intrusion detection. Traffic needs to be monitored by ISPs at the ingress points of the attacks, rather than by the victims at the egress points. ISPs have no economic motivation to do this yet; they haven't figured out that customers will pay for this service.

8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. Even-numbered ports were not probed because:
        i. There is a bug in the attacker's software
        ii. Source ports are even, destination ports are odd
        iii. The usual services on those ports are rarely implemented
        iv. The scanner uses multiple passes with interleaved addresses to avoid suspicion

Answer iii)

Detect 6

59, 2000-06-15 05:13:04, 2003103, NetBus port probe, 24.160.54.3, sc-24-160-54-3.socal.rr.com, 24.160.67.224, , port=12345&name=NetBus, 5

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Network Ice BlackIce Defender
    b. Detect format is described at http://www.networkice.com/Advice/Support/KB/q000018/
3. Probability the source route was spoofed.
    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for NetBus trojan
    b. Information is obtained if the server responds with a SYN/ACK to the attacker
11. Attack Mechanism
    a. Attacker is too lazy to do his own primary hacking, and is attempting to springboard off the work of other hackers
    c. This works on a TCP 3-way handshake. Attacker sends SYN to victim to port 12345. Victim responds with a SYN/ACK if the Trojan is installed in the typical way
5. Correlations
    a. NetBus is a popular trojan. Probes for it have occurred 8 times in the past two days, all from different sources
6. Evidence of Active Targeting
    a. Unlikely. The attacker would be ***using*** Netbus instead of probing for it in a targeted attack..
7. Severity
    a. –3
8. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
9. Multiple choice question
    a. The DNS name of sc-24-160-54-3.socal.rr.com
        i. The attacker is using a cable modem

ii. The attacker is a aware of being a social misfit, but doesn't know how to spell
iii. The attacker likes railroads
iv. The attacker is located in South Carolina

10. Answer i)

Detect 7

59, 2000-06-14 02:16:47, 2003105, SubSeven port probe, 24.66.110.126, CS387435-A, 24.160.67.224, , port=27374&name=Sub_7_2, 1

IP: 24.66.110.126
Node: CS387435-A
Group: SHAW@HOME
MAC: 0080C876C31C
DNS: 24.66.110.126.on.wave.home.com

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Network Ice BlackIce Defender
    b. Detect format is described at http://www.networkice.com/Advice/Support/KB/q000018/
3. Probability the source route was spoofed.
    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for SubSeven trojan
    b. Information is obtained if the server responds with a SYN/ACK to the attacker
5. Attack Mechanism
    a. Attacker is too lazy to do his own primary hacking, and is attempting to springboard off the work of other hackers
    b. This works on a TCP 3-way handshake. Attacker sends SYN to victim to port 27374. Victim responds with a SYN/ACK if SubSeven Trojan is installed in the usual way
6. Correlations
    a. SubSeven is a popular trojan. Probes for it have "only" occurred 4 times in the past two weeks. Three of the four originated at cable modem ISPs.
7. Evidence of Active Targeting
    a. Unlikely. In a targeted attack, the attacker would be ***using*** SubSeven instead of probing for it.
8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. The detection of the "group" name of the attacker indicates
        i. The attacker is using a cable modem
        ii. The attacker is using a Windows PC
        iii. The attacker is using a group of zombie computers

iv. The attacker is part of an organized team of hackers

Answer ii)

Detect 8

19, 2000-06-10 13:02:25, 2001507, PCAnywhere ping, 24.160.67.3, MH2, 24.160.67.224, , port=22, 1

IP: 24.160.67.3
Node: MH2
DNS: cs16067-3.houston.rr.com
Group: MARKHALA
NetBIOS: <0102>__MSBROWSE__<02>
MAC: 0050BA8446EE

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Network Ice BlackIce Defender
    b. Detect format is described at http://www.networkice.com/Advice/Support/KB/q000018/
3. Probability the source route was spoofed.
    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for a Pcanywhere server
    b. Information is obtained if the server responds t to the attacker with a SYN/ACK and further characteristic traffic.
5. Attack Mechanism
    a. If an attack, the attacker is looking for a badly configured Pcanywhere installation.
    b. However, this may also be the result of a badly configured Pcanywhere client, which scans its “Class C” subnet in order to compile a convenient “network neighborhood” icon display.
6. Correlations
    a. Carbon Copy is known to have similar “mapping” behavior.
7. Evidence of Active Targeting
    a. Unlikely. The attacker would be targeting a nonexistent service, since the target computer does not run PCanywhere. Also, see “Attack Mechanism”, comment b.
8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. The “neighborhood” discovered by this PCanywhere mapping activity consists of
        i. Streets within 1000 meters of the detecting PC
        ii. Any RoadRunner customer in Houston
        iii. Any computer with an IP addresss between 24.160.0.1 and 24.160.255.254
        iv. Any computer with an IP addresss between 24.160.67.1 and 24.160.67.254

Answer iv)

Detect 9

59, 2000-06-12 14:10:38, 2001506, Back Orifice ping, 63.39.89.14, OEMCOMPUTER, 24.160.67.224, , type=PING(1)&passwd=0x7A69&length=19&xid=0x2&iport=0x7A69&vport=0x7A69, 2

IP: 63.39.89.14
DNS: 1Cust14.tnt10.tco2.da.uu.net
Node: OEMCOMPUTER
Group: OEMWORKGROUP
MAC: 444553540000

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Network Ice BlackIce Defender
    b. Detect format is described at http://www.networkice.com/Advice/Support/KB/q000018/
3. Probability the source route was spoofed.
    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for a BackOrifice server
    b. Information is obtained if the server responds to the attacker with a SYN/ACK and further characteristic traffic.
5. Attack Mechanism
    b. Attacker is too lazy to do his own primary hacking, and is attempting to springboard off the work of other hackers
    a. This works on a TCP 3-way handshake. Attacker sends SYN to victim to port 31337. Victim responds with a SYN/ACK if SubSeven Trojan is installed in the usual way.
6. Correlations
    a. This is the fourth most frequent type of probe recorded in three weeks of monitoring.
7. Evidence of Active Targeting
    a. Unlikely. The attacker is using the BackOrifice "ping" command to determine whether the Trojan is alive or not.
8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. The port 0x7A69 listed in this detect indicates
        i. The attacker is using a specially modified version of BackOrifice
        ii. The attacker has used a version of BackOrifice in which sophisticated software has converted the Trojan to machine language
        iii. The detector software has printed its output in hexadecimal instead of decimal numeric notation.
        iv. Both ii and iii.

Answer iv) Note: the conversion program used is a "compiler".

Detect 10

39, 2000-06-10 05:42:10, 2003011, DNS port probe, 212.120.124.119, CP11159-a.TILBU1.NB.NL.HOME.COM, 24.160.67.224, , port=53, 1

1. Source of trace
    a. My network
2. Detect was generated by:
    a. Network Ice BlackIce Defender
    b. Detect format is described at http://www.networkice.com/Advice/Support/KB/q000018/
3. Probability the source route was spoofed.
    a. Probably not. The attack relies on the ability to get information back from the target. With a spoofed address, the information would go somewhere else.
4. Description of Attack
    a. Attempted scan for a domain nameserver on its TCP port
    b. Information is obtained if the server responds to the attacker with SYN/ACK and characteristic follow-on traffic.
5. Attack Mechanism
    a. This might be a somewhat intelligent hacker, possibly attempting to find nameservers that respond on the port normally used for zone transfers. If a zone transfer is successfully obtained, it will provide a list of managed systems, thus enabling a more efficient search for targets.
6. Correlations
    a. 212.120.64.0/18 is assigned to @Home Benelux. A SubSeven probe originated from another subnet allocated to the same ISP in the Netherlands two days earlier. If this were a dialup ISP, it would be suggestive of a single hacker, but because @home is a cable modem provider, addresses do not typically change significantly from day to day. The probes are probably uncorrelated.
7. Evidence of Active Targeting
    a. Unlikely. The attacker should know better than to think that a cable modem subscriber would have any reason to run their own nameserver.
8. Severity
    a. –3
9. Defensive Recommendation
    a. Defenses are fine. Firewall blocked attack
10. Multiple choice question
    a. The six-level domain name CP11159-a.TILBU1.NB.NL.HOME.COM in this detect indicates
        i. Home.com is a multinational company
        ii. The capacity limits of the Domain Name System are nearing exhaustion
        iii. @Home uses its DNS naming conventions to indicate architectural features of its network.
        iv. Both i and iii.

Answer iv)

Last Updated: May 22nd, 2017

Upcoming Training

Mentor Session - SEC503	Oceanside, CA	May 29, 2017 - Jun 29, 2017	Mentor
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced