Global Information Assurance Certification Paper

Joshua Senzer San Jose 2000

Detect 1
2000/06/01 8:27:17 PM GMT -0400: 3Com Fast EtherLi..[0000][No matching rule] Blocking incoming TCP: src=209.73.241.114, dst=homebox.dsl.net, sport=814, dport=111.
2000/06/01 8:27:20 PM GMT -0400: 3Com Fast EtherLi..[0000][No matching rule] Blocking incoming TCP: src=209.73.241.114, dst=homebox.dsl.net, sport=814, dport=111.
2000/06/01 8:39:40 PM GMT -0400: 3Com Fast EtherLi..[0000][No matching rule] Blocking incoming TCP: src=209.73.241.104, dst=homebox.dsl.net, sport=617, dport=111.
2000/06/01 8:39:43 PM GMT -0400: 3Com Fast EtherLi..[0000][No matching rule] Blocking incoming TCP: src=209.73.241.104, dst=homebox.dsl.net, sport=617, dport=111.

1.Source of Trace: Home DSL connect
2.generated by :
a.ConSeal Signal9 (host-based `firewall`)
b. Field summary
2000/06/01-date 8:39:43 PM GMT –0400-time: 3Com Fast EtherLi..-adapter name[0000]-adapter number[No matching rule]-rule number (if any) Blocking incoming TCP:-action src=209.73.241.104,-source ip dst=homebox.dsl.net,-destination ip sport=617-source port, dport=111 –dest port
3.Probability addresses were spoofed:
Low, Ips resolve and trace back to SCGNYC.com which I believe to be a hosting company. Addresses were registered to Globix (a nationwide tier 2 ISP).
4.Discription of attack:
a. Attacker is "turning doorknobs" looking for active Sun Remote procedure Calls.
b. This is a prime example of a "needle in a haystack" attack looking for improperly configured Sun boxes that might be sitting unattended on a DSL network.
5.Attack Mechanism: Attacker appears to be trying to be `stealthy` in his attempt at OS fingerprinting, This can be seen by the time difference in the logs trying one host from the source ip block, and than another 12 minutes later.
Attacker is looking specifically for SunOS boxes most logically to exploit(see CVE 1999-189,1999-190).
6. Correlations:
a. After contacting Globix I learned that I was not the only person that day reporting such activity regarding said hosts.
b. see CVE 1999-189,1999-190
7. Evidence of active targeting:
a. None. the target host is non SunOS on a large DSL subnet with no mail or name services running.
8.Severity [(critical + Lethal) – (System + Net Countermeasures) = Severity]
(2+1)-(4+4)= -5
9. Defensive Recommendations
a. none. The one host of mine on this link is not running SunOS nor will it respond to RPCs. Firewall caught and blocked traffic
10 . Multiple Choice
This Trace shows

A. port scanning
B. CGI buffer overflow
C. OS Fingerprinting
D. Trojan trolling

answer C.

Detect 2.
Time: 6-Jun-2000 01:48:19
NFR: feral
Source IP: 61.141.205.107 (WANG)
Hosts Contacted: [XXX.XXX.106.44,XXX.XXX.106.50,XXX.XXX.106.
51,XXX.XXX.106.49,XXX.XXX.106.56,XXX.XXX.106.55,XXX.XXX.106.59,
XXX.XXX.106.42,XXX.XXX.106.58,XXX.XXX.106.47,XXX.XXX.106.60,160.
79.106.62,XXX.XXX.106.65,XXX.XXX.106.66,XXX.XXX.106.61,XXX.XXX.
106.63,XXX.XXX.106.68,XXX.XXX.106.71,XXX.XXX.106.73,XXX.XXX.106.
76,XXX.XXX.106.77,XXX.XXX.106.78,XXX.XXX.106.81,XXX.XXX.106.82,
XXX.XXX.106.69,XXX.XXX.106.67,XXX.XXX.106.83,XXX.XXX.106.84,160.
79.106.90,XXX.XXX.106.92,XXX.XXX.106.93,XXX.XXX.106.95,XXX.XXX.
106.97,XXX.XXX.106.99,XXX.XXX.106.100,XXX.XXX.106.101,XXX.XXX.
106.102,XXX.XXX.106.103,XXX.XXX.106.104,XXX.XXX.106.109,XXX.XXX.
106.107,XXX.XXX.106.105]

Time: 6-Jun-2000 01:50:04
NFR: feral
Source IP: 61.141.205.107 (WANG)
Hosts Contacted: [XXX.XXX.108.1,XXX.XXX.108.15,XXX.XXX.108.
17,XXX.XXX.108.25,XXX.XXX.108.26,XXX.XXX.108.29,XXX.XXX.108.18,
XXX.XXX.108.20,XXX.XXX.108.16,XXX.XXX.108.32,XXX.XXX.108.34,160.
79.108.33,XXX.XXX.108.24,XXX.XXX.108.30,XXX.XXX.108.42,XXX.XXX.
108.46,XXX.XXX.108.43,XXX.XXX.108.44,XXX.XXX.108.31,XXX.XXX.108.
47,XXX.XXX.108.48,XXX.XXX.108.37,XXX.XXX.108.35,XXX.XXX.108.38,
XXX.XXX.108.40,XXX.XXX.108.52,XXX.XXX.108.53,XXX.XXX.108.55,160.
79.108.57,XXX.XXX.108.49,XXX.XXX.108.60,XXX.XXX.108.61,XXX.XXX.
108.63,XXX.XXX.108.51]

Time: 6-Jun-2000 01:50:35
NFR: feral
Source IP: 61.141.205.107 (WANG)
Hosts Contacted: [XXX.XXX.108.63,XXX.XXX.108.145,XXX.XXX.
108.147,XXX.XXX.108.149,XXX.XXX.108.144,XXX.XXX.108.151,XXX.XXX.
108.152,XXX.XXX.108.153,XXX.XXX.108.155,XXX.XXX.108.159,XXX.XXX.
108.161,XXX.XXX.108.165,XXX.XXX.108.168,XXX.XXX.108.169,XXX.XXX.
108.171,XXX.XXX.108.173,XXX.XXX.108.160,XXX.XXX.108.175,XXX.XXX.
108.176,XXX.XXX.108.179,XXX.XXX.108.181,XXX.XXX.108.182,XXX.XXX.
108.183,XXX.XXX.108.184,XXX.XXX.108.172,XXX.XXX.108.185,XXX.XXX.
108.187,XXX.XXX.108.188,XXX.XXX.108.190,XXX.XXX.108.191,XXX.XXX.
108.192,XXX.XXX.108.194,XXX.XXX.108.196,XXX.XXX.108.177,XXX.XXX.
108.201,XXX.XXX.108.204,XXX.XXX.108.205,XXX.XXX.108.207,XXX.XXX.
108.195,XXX.XXX.108.210,XXX.XXX.108.197,XXX.XXX.108.212,XXX.XXX.
108.215,XXX.XXX.108.216,XXX.XXX.108.199,XXX.XXX.108.209]

1.Source of detect: My Network
2.Generated by Network Flight Recorder V.4.1.1
2a. In logs "NFR" designates the logical name of the sensor. To conserve on space I have only included logs from one sensor
3.Probability of spoofing: low .. Host is registered to China Telecom and seems to not only be properly routed but relatively secure (icmp disabled)
4. Description of attack: Host mapping, possible reconnaissance for future attacks.
5. Attack mechanism: Attacker used a program or script such as Nmap to scan for live hosts within one of my /16 blocks. Scanning occurred at this rate for approximately 2 hours.
6.Correlation: scans confirmed by additional sensors on the network.
7.Evidence Of targeting: moderate. My internal /16 was targeted but the time in between scan could elude to a much larger scope of the scan.
8.Severtity: (critical + Lethal) – (System + Net Countermeasures) = Severity
(3+2)-(3+4)= -7
9.Defensive recommendations: disable icmp on mission critical segments. Reinforce existing security procedures. Pay close attention to hosts on Chinanet connecting to that /16.
10.Question
From the data presented on these scans what can be gathered?

A. attacker is looking for BO2k clients
B. attacker is attempting to locate the PDC
C. attacker is trying to deny service to many hosts
D .attacker is doing reconnaissance for future susceptible hosts

Answer. D

Detect 3.
Time: 7-Jun-2000 00:21:08
NFR: native
Source IP: 128.223.150.148 (cisco-ts5-line138.uoregon.edu)
Dest IP: XXX.XXX.106.168 (www.nyc..entity.com)
Username: anvovinge\x
Password: dallas22\x
Pass/Fail: fail

Time: 7-Jun-2000 00:19:34
NFR: feral
Source IP: 128.223.150.148 (cisco-ts5-line138.uoregon.edu)
Dest IP: XXX.XXX.106.168 (www.nyc.entity.com)
Username: anovinge\xanovinge\x
Password: dallas22\x
Pass/Fail: fail

Time: 7-Jun-2000 00:20:02
NFR: feral
Source IP: 128.223.150.148 (cisco-ts5-line138 uoregon.edu)
Dest IP: XXX.XXX.106.168 (www.nyc.entity.com)
Username: an\x\x\x\xanovinge\x
Password: dallas22\x
Pass/Fail: fail

1.Source of Detect : My Network
2.Detect Generated by : NFR 4.1.1 –Telnet detection module
3.Probability of spoofed IP :
Low. Rogue traffic originating from a University is common. Reverse lookup shows a hostname that could easily be part of a DHCP pool.
4.Description of attack:
Repeated failed telnet attempts. Though not a traditional "attack", due to the large number of corporate customers which sit downstream on my network, I try to keep tabs on failed telnet attempts(please note: filter is set to grab password on failed attempts only). I like to think of it as `network caller ID`, and I've found that a very little bit of prevention can save grief down the road.
5.Attack mechanism: Attacker appears to have a password for an account on (www.nyc.entity.com), but not the correct username. The attempts are spaced out over time as a possible stealth tactic. Attacker may use a captive host for many unsavory deeds including but not limited to: trojans, ddos clients, sniffers .etc
6. Correlations: This is the only such traffic regarding these hosts. Logging failed login attempts are a great method for tracking unauthorized activity and insecure password schemes.
7. Evidence of active targeting: No other targets were sighted from the source domain. This was a directly targeted attempt.
8. Severity (critical + Lethal) – (System + Net Countermeasures) = Severity
(4+3)-(1+1)=5
9. Defensive recommendation: Alert admin of target host. Change password if account is legitimate. Alert admin. of source host, request logs be provided to ascertain identity/authority of attacker.
10.Multiple Choice:

What are the "red flags" in this detect?

A. source originating from a .edu
B. failed telnet attempts from a Cisco router in a .edu
C. failed attempts staggered over 1.5 hours from .edu in Oregon to a apparently corporate entity in New York.
D. All of the above

Answer D

Detect 4.
******note : I am aware that we were not supposed to use the same type of mechanism for multiple detects. However I feel that both the previous detect and the one following deserve to be recognized as they both reflect legitimate signs of trouble ******* J.S.

Time: 9-Jun-2000 10:28:39
NFR: feral
Source IP: 204.2.10.4
Dest IP: my.net.100.4
Username: root
Password:
Pass/Fail: pass

Time: 7-Jun-2000 11:25:44
NFR: native
Source IP: 204.2.10.4
Dest IP: my.net.100.4
Username: root
Password:
Pass/Fail: pass

Time: 7-Jun-2000 11:18:18
NFR: native
Source IP: 204.2.10.4
Dest IP: my.net.100.4
Username: root
Password:
Pass/Fail: pass

1.Source of trace: My Network
2.Detect generated by : NFR 4.1.1
3.Probability of source spoofed: Moderate. Source ip resolves to a block of 4 class B networks within Rice University, however source host does not respond to outside stimulus.
4. Description of attack: Successful login as "root" via telnet from an non-trusted ip.
5. Attack mechanism: Upon securing root level access on a compromised machine, an unfriendly party may steal/destroy important data, use the compromised host as an attack vehicle on a 3rd party and/or exploit existing trusts the compromised host may have had.
6. Correlations: this detect set precedent for traffic between these two networks. "rooting" machines is the penultimate goal of the hacker, after which achieving it the unfriendly party is free to do what they please.
7. Evidence of targeting: attack was directly targeted. No failed login attempts logged.
8.Severity: (critical + Lethal) – (System + Net Countermeasures) = Severity
(4+5)-(3+1)=5
9.Defensive recommendations: change root password immediately. disable telnet access to root account. Install tcp wrappers. Install ssh.
10. Multiple choice
This detect appears to be: (circle all that apply)
A. normal acceptable traffic
B. sloppy sys admin.
C. telnet overflow
D. a satisfied hacker testing their new root shell
Answer : b,d

Detect 5.
Time: 12-Jun-2000 15:40:00
Source Address: my.net.69.195
Destination Address:152.163.244.17
MAC Source: 00:e0:da:05:7a:00
New Connections: 11

Time: 12-Jun-2000 15:40:00
Source Address: my.net.69.195
Destination Address:152.163.244.16

MAC Source: 00:e0:da:05:7a:00
New Connections: 12

Time: 12-Jun-2000 15:40:00
Source Address: my.net.69.195
Destination Address:152.163.244.15
MAC Source: 00:e0:da:05:7a:00
New Connections: 11

Time: 12-Jun-2000 15:40:00
Source Address: my.net.69.195
Destination Address:152.163.244.14
MAC Source: 00:e0:da:05:7a:00
New Connections: 11

Time: 12-Jun-2000 15:40:00
Source Address: my.net.69.195
Destination Address:152.163.244.11
MAC Source: 00:e0:da:05:7a:00
New Connections: 12

Time: 12-Jun-2000 15:40:00
Source Address: my.net.69.195
Destination Address:152.163.244.12
MAC Source: 00:e0:da:05:7a:00
New Connections: 12

.....
cropped for space

Time: 11-Jun-2000 06:10:00
Source Address: 159.134.235.19 (p19.as1.kilkenny1.
eircom.net)
Destination Address:my.net.57.120
MAC Source: 00:50:50:49:48:00
New Connections: 2

Time: 11-Jun-2000 06:10:00
Source Address: 159.134.235.19 (p19.as1.kilkenny1.
eircom.net)
Destination Address:my.net.57.120
MAC Source: 00:e0:da:05:7a:00
New Connections: 1

.....

Time: 7-Jun-2000 17:55:00
Source Address: 208.16.219.20
Destination Address:my.net.152.130
MAC Source: 00:50:50:49:48:00
New Connections: 1

Time: 6-Jun-2000 15:20:00
Source Address: my.net.69.195
Destination Address:216.34.89.5 (daffy.mydomain.com)
MAC Source: 00:e0:da:05:7a:00
New Connections: 3

Time: 6-Jun-2000 15:15:00
Source Address: my.net.69.195
Destination Address:216.34.89.5 (daffy.mydomain.com)
MAC Source: 00:e0:da:05:7a:00
New Connections: 6
1.Source of trace: My network
2.Detect generated by : NFR 4.1.1
3.Probability Address(s) spoofed : High . Most of the source ips in this detect are not routed. Source hosts on different continents within this detect are showing the same MAC address … while not impossible, seeing this regarding the same destination host is highly improbable. Hosts resolving to the same IP reflecting different MAC addresses.
4.Description of attack: SYN flood. Though usually associated with denial of service, due to the progression through the ip block, this particular activity appears to be more the result of reckless reconnaissance.
5.Attack mechanism: Attacker appears to be attempting to scan for hosts (most likely to use as spoofed addresses) within contiguous ip blocks using SYN packets to look for live hosts as a stealth method of host discovery. Traditional host scanning is usually a lot "noisier" and tends to set off many more common ID alarms.
6.Correlations: This is the first time I have come across a sequential SYN flood, as well I have yet to see it documented.
7.Evidence of active targeting: Low . with the exception of one or two hosts these appear to be general network scans.
8. Severity : (critical + Lethal) – (System + Net Countermeasures) = Severity
(3+4)-(3+3)=1
9.Defensive recommendations: Make sure all unused hosts are either not-routed, or placed in a NAT pool to minimize spoofing
10. Multiple choice
This is probably:
A. stealth host scan
B.SYN flood ddos
C.SYN/FIN attack
D. rlogin attempt
Answer A.

Detect 6.
[**] SCAN-SYN FIN [**]
06/06-23:58:37.557539 194.247.87.235:53 -> z.y.w.98:53 TCP
TTL:27 TOS:0x0 ID:39426 **SF**** Seq: 0x64C2AF11 Ack: 0x4979F54A Win:
0x404 00 00 00 00 00 00 .....
[**] SCAN-SYN FIN [**]
06/06-23:58:47.792897 194.247.87.235:53 -> z.y.w.98:53 TCP
TTL:27 TOS:0x0 ID:39426 **SF**** Seq: 0x5D2F00A4 Ack: 0x4ED983D3 Win:
0x404 00 00 00 00 00 00 .....

[**] SCAN-SYN FIN [**]
06/06-23:58:55.471597 194.247.87.235:53 -> z.y.w.98:53 TCP
TTL:27 TOS:0x0 ID:39426 **SF**** Seq: 0x5EF94849 Ack: 0x4186CC99 Win:
0x404 00 00 00 00 00 00 ......
[**] SCAN-SYN FIN [**]
06/06-23:59:38.689515 194.247.87.235:53 -> z.y.w.98:53 TCP
TTL:27 TOS:0x0 ID:39426 **SF**** Seq: 0x40E6B24A Ack: 0x17BEA20E Win:
0x404 00 00 00 00 00 00 ......

1.Source of detect: Aberdeen Science and Technology Park, Scotland, GB
http://www.sans.org/y2k/061000.htm
2.Detect generated by : Snort ID system
3.Probability of spoofing: High. Having both syn and fin flags toggled show a "impossible packet"
4. Description of attack: upon receipt of syn-fin packets ports which are listening will react differently giving an attacker reconnaissance data for which ports to direct future intrusions towards.
5. Attack mechanism: Attacker is probably utilizing Nmap or a similar utility to scan the ports on the target machine most likely for network mapping reconnaissance info. This can also allow for partial OS fingerprinting, as different operating systems have different responses to "impossible packets".
6.Correlations: This behavior is outlined in RFC 793 and in San Jose Intrusion Detection 2.2 page 138.
7. Evidence of active targeting: Likely. Timestamp puts scans close together suggesting it was actively targeted, or part of a small localized target group.
8.Severity (critical + Lethal) – (System + Net Countermeasures) = Severity
(3+2)-(3+2)= 0
9. Defensive recommendations: Deny all tcp traffic that does not follow RFC at external router/firewall.
10. Multiple Choice: This detect is an example of:
A. crafted packet
B. a host in promiscuous mode
C. session hijacking
D. smurf attack
answer. A.
Detect 7.
NOTE This detect got me REALLY nervous when I first saw it I have included logs of ICMP frags regarding the same hosts as correlation on this attack since it seemed to be unique. I consulted with my personal tcp/ip gurus on this and they had never seen these ICMP types nor did they have any reasonable suggestions for why they might be occurring. After seeing this I called the Admin of the host and asked if he had any incidents occurring at about that time. The domain turned out to be a very recent new customer, apparently at the time these odd packets were delivered there were modifications being done to his upstream routes. My assumption on this is the routing conflict caused the hosts echo replies to my.net.1.228 (a machine in my help desk area) to be mutated. OR a router unknown to me is sending out non-RFC compliant ICMP data.

Time: 12-Jun-2000 16:00:00
NFR: primal
Source IP: my.net.169.130 (LU)
Destination IP: my.net.1.228 (dhcp228-1156.my.net..net)
ICMP Type: 97
ICMP Code: 116
ICMP Description: unknown
Histogram Count Label:1

Time: 12-Jun-2000 16:00:00
NFR: primal
Source IP: my.net.169.130 (LU)
Destination IP: my.net.1.228 (dhcp228-1156.my.net..net)
ICMP Type: 2
ICMP Code: 0
ICMP Description: unknown
Histogram Count Label:1

Time: 12-Jun-2000 16:00:00
NFR: primal
Source IP: my.net.169.130 (LU)
Destination IP: my.net.1.228 (dhcp228-1156.my.net..net)
ICMP Type: 111
ICMP Code: 99
ICMP Description: unknown
Histogram Count Label:2

Time: 12-Jun-2000 16:00:00
NFR: primal
Source IP: my.net.169.130 (LU)
Destination IP: my.net.1.228 (dhcp228-1156.my.net..net)
ICMP Type: 203
ICMP Code: 214
ICMP Description: unknown
Histogram Count Label:1

Time: 12-Jun-2000 16:00:00
NFR: primal
Source IP: my.net.169.130 (LU)
Destination IP: my.net.1.228
ICMP Type: 1
ICMP Code: 0
ICMP Description: unknown
Histogram Count Label:1

Time: 12-Jun-2000 13:00:00
Source IP: my.net.1.228 (dhcp228-1156.my.net..net)

Destination IP: my.net.169.130 (LU)
Count: 18

Time: 12-Jun-2000 16:00:00
Source IP: my.net.1.228 (dhcp228-1156.my.net..net)
Destination IP: my.net.169.130 (LU)
Count: 104

Time: 12-Jun-2000 16:00:00
Source IP: my.net.169.130 (LU)
Destination IP: my.net.1.228 (dhcp228-1156.my.net..net)
Count: 84

1.Source of Detect: my network
2.Detect generated by : NFR 4.1.1 ICMP monitor module
3.Probability of source being spoofed: moderate. Upon seeing this detect I was instantly confused. Detect contains ICMP traffic coming from a downstream client into my internal LAN, these packets however show significant variations from the ICMP standard RFC792. This variation from the standard shows a possibility of spoofing.
4.Description of attack: Attacker sent three unique ICMP packets within milliseconds of one another. Each one of these ICMP packets is classified out of the scope of the RFC and are considered "impossible packets"
5.Attack mechanism: UNKNOWN
6.Correlations: no known existing correlations. Many ICMP frags were recorded at approximately the same time.
7.Evidence of active targeting: Unknown. All three packets had the same time of origin and were localized to one specific host.
8.Severity: (critical + Lethal) – (System + Net Countermeasures) = Severity
(3+1)-(4+2)=-2
9.Defensive Recommendations: contact administrator of attacking host. Block non-RFC compliant ICMP packets at router level. Check router logs for event correlation
10. Multiple Choice
This is an example of :
A.ICMP flooding
B.ICMP Trojan control
C. Trinoo
D. Cant tell from data provided
Answer D.
Detect 8.
Note: ports scanned have been curtailed in the interest of space.
Time: 6-Jun-2000 10:39:47
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2677,2679,2685,2687,2693,2695,2701,
2703,2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,2746,
2747,2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,2781,
2783,2792,2797,2799,2805,2807,2813,2815,2821,2823,2829,2831,
2837,2839,2845,2847,2851,2854,2858,2860,2862,2864,2866,2868,
2870,2872,2874,2876,2878,2880,2882,2884,2894,2898,2902,2904,
2906,2908,2910,2912,2914,2916,2918,2920,2922,2926,2928,2930,
2932,2934,2936,2937,2941,2948,2949,2955,2956,2957,2964,2965,

Time: 6-Jun-2000 10:40:02
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2677,2679,2685,2687,2693,2695,2701,
2703,2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,2746,
2747,2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,2781,
2783,2792,2797,2799,2805,2807,2813,2815,2821,2823,2829,2831,
2837,2839,2845,2847,2851,2854,2858,2860,2862,2864,2866,2868,
2870,2872,2874,2876,2878,2880,2882,2884,2894,2898,2902,2904,
2906,2908,2910,2912,2914,2916,2918,2920,2922,2926,2928,2930,

Time: 6-Jun-2000 10:40:17
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2677,2679,2685,2687,2693,2695,2701,
2703,2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,2746,
2747,2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,2781,
2783,2792,2797,2799,2805,2807,2813,2815,2821,2823,2829,2831,

Time: 6-Jun-2000 10:47:17
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2679,2685,2687,2693,2695,2701,2703,
2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,2746,2747,
2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,2781,2783,
2792,2797,2799,2805,2807,2813,2815,2821,2823,2829,2831,2837,
2839,2845,2847,2851,2854,2858,2860,2862,2864,2866,2868,2870,
2872,2874,2876,2878,2880,2882,2884,2894,2898,2902,2904,2906,

Time: 6-Jun-2000 10:47:07
NFR: native
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [1131,1134,1148,1156,1164,1172,1174,
1177,1180,1183,1189,1197,1205,1213,1221,1228,1229,1230,1238,
1246,1254,1255,1262,1266,1267,1274,1275,1277,1282,1283,1290,
1291,1294,1295,1296,1297,1298,1300,1303]

Time: 6-Jun-2000 10:47:37
NFR: native
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [1310,1311,1312,1313,1315,1317,1321,
1329,1330,1333,1334,1337,1338,1340,1343,1346,1349,1351,1354,
1356,1357,1358,1365,1366,1372,1379,1385,1388,1390,1393,1396,
1398,1399]

Time: 6-Jun-2000 10:47:33
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2679,2685,2687,2693,2695,2701,2703,
2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,2746,2747,
2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,2781,2783,
2792,2797,2799,2805,2807,2813,2815,2821,2823,2829,2831,2837,
2839,2845,2847,2851,2854,2858,2860,2862,2864,2866,2868,2870,

Time: 6-Jun-2000 10:46:32
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2679,2685,2687,2693,2695,2701,2703,
2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,2746,2747,
2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,2781,2783
2839,2845,2847,2851,2854,2858,2860,2862,2864,2866,2868,2870,
2872,2874,2876,2878,2880,2882,2884,2894,2898,2902,2904,2906,
2908,2910,2912,2914,2916,2918,2920,2922,2926,2928,2930,2932,
2934,2936,2937,2941,2948,2949,2955,2956,2957,2964,2965,2972,
2973,2980,2981,2988,2989,2996,2997,3002,3008,3010,3016,3018,
3021,3024,3026,3032,3034,3040,3042,3048,3050,3056,3058,3063,
3064,3066,3067,3072,3074,3075,3080,3082,3088,3090,3096,3098,
3104,3106,3112,3114,3120,3122,3125,3143,3157,3175,3177,3179,

Time: 6-Jun-2000 10:46:16
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2679,2685,2687,2693,2695,2701,2703,
2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,2746,2747,
2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,2781,2783,
2792,2797,2799,2805,2807,2813,2815,2821,2823,2829,2831,2837,
2839,2845,2847,2851,2854,2858,2860,2862,2864,2866,2868,2870,
2872,2874,2876,2878,2880,2882,2884,2894,2898,2902,2904,2906,
2908,2910,2912,2914,2916,2918,2920,2922,2926,2928,2930,2932,
2934,2936,2937,2941,2948,2949,2955,2956,2957,2964,2965,2972,

Time: 6-Jun-2000 10:48:18
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2679,2685,2687,2693,2695,2701,2703,
2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,2746,2747,
2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,2781,2783,
2792,2797,2799,2805,2807,2813,2815,2821,2823,2829,2831,2837,
2839,2845,2847,2851,2854,2858,2860,2862,2864,2866,2868,2870,

Time: 6-Jun-2000 10:20:46
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2355,2363,2368,2369,2376,2377,2383,
2396,2404,2405,2407,2413,2415,2421,2423,2441,2448,2449,2457,
2464,2465,2472,2480,2481,2485,2488,2489,2496,2497,2500,2504,
2505,2512,2513,2520,2521]

Time: 6-Jun-2000 10:21:01
NFR: native
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [80,2338,2340,2347,2352,2353,2354,2357,
2360,2362,2365,2370,2371,2376,2380,2381,2382,2385,2400,2401,
2402,2410,2418,2426,2432,2433,2434,2436,2437,2440,2444,2445,

Time: 6-Jun-2000 10:20:46
NFR: native
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [80,2338,2340,2347,2352,2353,2354,2357,
2360,2362,2365,2370,2371,2376,2380,2381,2382,2385,2400,2401,
2402,2410,2418,2426,2432,2433,2434,2436,2437,2440,2444,2445,
2452,2453,2454,2460,2461,2468,2469,2476,2477,2484,2492,2493,
2501,2508,2509,2516,2517,2524,2525]

Time: 6-Jun-2000 10:24:33
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2533,2535,2541,2549,2551,2557,2559,
2565,2567,2573,2574,2581,2583,2589,2591,2592,2595,2597,2599,
2605,2607,2613,2615,2616,2617,2621,2623,2629,2631,2637,2639,
2645,2647,2653,2655,2661]

Time: 6-Jun-2000 10:34:26
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2671,2677,2679,2685,2687,2693,2695,
2701,2703,2709,2711,2717,2719,2723,2725,2733,2735,2741,2743,
2746,2747,2749,2750,2751,2757,2759,2761,2765,2767,2773,2775,
2781,2783,2792,2797,2799,2805,2807,2813,2815,2821,2823,2829,
2831,2837,2839,2845,2847,2851,2854,2858,2860,2862,2864,2866,
2868,2870,2872,2874,2876,2878,2880,2882,2884,2894,2898,2902,
2904,2906,2908,2910,2912,2914,2916,2918,2920,2922,2926,2928,

Time: 6-Jun-2000 10:33:18
NFR: native
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [3418,3419,3423,3427,3434,3435,3442,
3443,3444,3446,3447,3450,3451,3458,3459,3460,3466,3467,3474,
3475,3479,3482,3483,3490,3491,3498,3499,3506,3507,3508,3514,
3515,3517,3522,3523,3530,3531]

Time: 6-Jun-2000 10:28:26
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2669,2671,2677,2679,2685,2687,2693,
2695,2701,2703,2709,2711,2717,2719,2723,2725,2733,2735,2741,
2743,2746,2747,2749,2750,2751,2757,2759,2761,2765,2767,2773,
2775,2781,2783,2792,2797,2799,2805,2807,2813,2815,2821,2823,
2829,2831,2837,2839,2845,2847,2851,2854,2858,2860,2862,2864,
2866,2868,2870,2872,2874,2876,2878,2880,2882,2884,2894,2898,
2902,2904,2906,2908,2910,2912,2914,2916,2918,2920,2922,2926,
2928,2930,2932,2934,2936,2937,2941,2948,2949,2955,2956,2957,

Time: 6-Jun-2000 10:28:23
NFR: native
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [80,2338,2340,2347,2352,2353,2354,2357,
2360,2362,2365,2370,2371,2376,2380,2381,2382,2385,2400,2401,
2402,2410,2418,2426,2432,2433,2434,2436,2437,2440,2444,2445,
2452,2453,2454,2460,2461,2468,2469,2476,2477,2484,2492,2493,
2501,2508,2509,2516,2517,2524,2525,2529,2530,2538,2546,2554,
2556,2560,2562,2570,2578,2586,2594,2602,2610,2618,2626,2634,
2637,2642,2650,2658,2666,2674,2682,2690,2698,2706,2714,2721,

Time: 6-Jun-2000 10:31:48
NFR: native
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [3180,3188,3195,3197,3203,3210,3211,
3217,3218,3219,3226,3227,3233,3234,3235,3242,3243,3248,3250,
3251,3258,3263,3267,3274,3275,3283,3288,3290,3291,3298,3299,
3306,3307]

Time: 6-Jun-2000 10:32:33
NFR: native
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [3314,3315,3322,3323,3327,3330,3331,
3338,3339,3346,3347,3354,3355,3357,3362,3363,3370,3371,3378,
3379,3386,3387,3391,3394,3395,3402,3403,3410]

Time: 6-Jun-2000 10:31:27
NFR: feral
Source Addr: my.net.85.217
Dest Addr: 209.67.62.14 (JUMBO96B)
Ports: [2669,2671,2677,2679,2685,2687,2693,
2695,2701,2703,2709,2711,2717,2719,2723,2725,2733,2735,2741,
2743,2746,2747,2749,2750,2751,2757,2759,2761,2765,2767,2773,
2775,2781,2783,2792,2797,2799,2805,2807,2813,2815,2821,2823,
2829,2831,2837,2839,2845,2847,2851,2854,2858,2860,2862,2864,
2866,2868,2870,2872,2874,2876,2878,2880,2882,2884,2894,2898,

1.Source of Detect: My network
2. Detect generated by NFR 1.1.4
3. Probability of spoofed host: low . Host is a static routed ip downstream and originating point of much of the troubling traffic on my network.
4.Description of attack: attacker is looking for open ports by way of a port scanner (i.e. Nmap, SATAN) attacker tried to scan the same host a total of 44 times within approximately 20 minutes starting from various ports.
5. Attack mechanism: Attacker is haphazardly scanning the target host, apparently looking for open ports to exploit. The recklessness of this attack (i.e. . no attempt at stealth) in combination with other suspicious activity (host scans, ICMP fragments, many TCP resets)leads me to consider this a "rogue host"
6. Correlations: This host is suspect in a number of other unsavory activities most prominently excessive tcp resets, and ICMP fragmentation.
7.Evidince of active targeting: Target was specifically targeted as shown through the persistence of traffic to the target host, and thoroughness of ports scanned.
8. Severity (critical + Lethal) – (System + Net Countermeasures) = Severity
(3+4)-(3+2)=2
9. Defensive recommendation: request Administrator of source host do an exhaustive security audit. Deny non-essential communications from source host to mission critical systems.
10. Multiple choice question
This detect best shows:
A.OS fingerprinting
B. Trolling for Trojans
C. Reconnaissance
D.DNS buffer overflow attack
Answer C.

Detect 9
Time: 6-Jun-2000 20:16:18
NFR: primal
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 6

Time: 6-Jun-2000 20:18:41
NFR: native
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 6

Time: 7-Jun-2000 11:17:10
NFR: primal
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 7

Time: 7-Jun-2000 16:11:13
NFR: primal
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 2

Time: 7-Jun-2000 16:16:51
NFR: primal
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 3

Time: 7-Jun-2000 20:38:09
NFR: native
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 8

Time: 7-Jun-2000 20:38:11
NFR: native
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 2

Time: 7-Jun-2000 20:38:15
NFR: native
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 4

Time: 7-Jun-2000 20:38:36
NFR: native
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 4

Time: 7-Jun-2000 20:39:44
NFR: native
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 3

Time: 7-Jun-2000 20:44:11
NFR: native
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 9

Time: 8-Jun-2000 14:28:32
NFR: native
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 4

Time: 8-Jun-2000 16:59:48
NFR: feral
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 5

Time: 8-Jun-2000 17:20:01
NFR: primal
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 5

Time: 8-Jun-2000 18:39:26
NFR: primal
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 2

Time: 8-Jun-2000 18:39:28
NFR: primal
Destination IP: my.net.69.3
Number of Packets: 150
Elapsed Time: 2

Time: 9-Jun-2000 18:09:57
NFR: primal
Destination IP: my.net.69.3
Number of Packets: 150

Elapsed Time: 4

1.Source of detect: My network
2.Detect generated by NFR 4.1.1 ping flood reply module. In these detects the "elapsed time" field refers to how many seconds elapsed between the first packet in the group and the last one, in this case reaching the threshold of 150 packets within an elapsed 10 seconds.
3.Probability of IP spoofing: High. No real way to trace back to originating host
4.Description of attack: my.net.69.3 appears to be the victim of a "smurf" denial of service attack.
5.Attack mechanism: In a smurf attack, the attacker would initiate the action by sending multiple icmp (usually echo) requests to a third party with the spoofed address of the victim. The resulting flood of packets can clog and bring to a halt the network of the victim.
6. Correlations. This attack is well documented in the wild .. see CVE1999-0513, and CERT® Advisory CA-98.01 "smurf" IP Denial-of-Service Attacks
7.Evidence of targeting: High. This activity was documented over the course of three days . During this time no other activity of this nature occurred at any other node on the class B
8.Severity: (critical + Lethal) – (System + Net Countermeasures) = Severity
(3+4)-(4+2)=1
9.Defensive recommendations: unfortunately there is not much one can do on the victim side to prevent these attacks. The only way to effectively stop DOS attacks is to not allow any machines under your control to be used as "pawns" to attack other innocent hosts.
10.Multiple Choice
This attack is most commonly known as :
A.) smurf
B.) ping of death
C.) blue screen fever
D.) Loki
Answer A.

Detect 10
please note "i.like.shroo.ms" is the real hostname …. Who knew?

Time: 5-Jun-2000 09:00:16
NFR: feral
Source IP: my.net.56.230 (omi.com)
Destination IP: 63.236.138.196 (i.like.shroo.ms)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:00:24
NFR: feral
Source IP: my.net.56.230 (omi.com)
Destination IP: 63.236.138.196 (i.like.shroo.ms)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:00:33
NFR: feral
Source IP: my.net.56.230 (omi.com)
Destination IP: 63.236.138.196 (i.like.shroo.ms)
Number of Packets: 150

Elapsed Time: 8

Time: 5-Jun-2000 09:00:41
NFR: feral
Source IP: my.net.56.230 (omi.com)
Destination IP: 63.236.138.196 (i.like.shroo.ms)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:04:01
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.cw.net)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:04:09
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.cw.net)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:04:17
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.cw.net)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:04:26
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.cw.net)
Number of Packets: 150
Elapsed Time: 9

Time: 5-Jun-2000 09:04:34
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.cw.net)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:04:42
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.
cw.net)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:04:50
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.
cw.net)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:04:59
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.
cw.net)
Number of Packets: 150
Elapsed Time: 9

Time: 5-Jun-2000 09:05:07
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.
cw.net)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:05:15
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.
cw.net)
Number of Packets: 150
Elapsed Time: 8

Time: 5-Jun-2000 09:05:23
NFR: primal
Source IP: my.net.56.230 (omi.com)
Destination IP: 166.62.74.66 (usr34-dialup2.mix2.Boston.
cw.net)
Number of Packets: 150
Elapsed Time: 8

1.Source of attack: my network
2.Detect generated by: NFR 4.1.1 ping flood module
3.Probability of IP spoofing: Low, OMI is a downstream connection that is a endless source of "interesting" traffic. All of their traffic is scrutinized.
4.Description of attack: Attacker is "ping flooding" the victim by inundating the destination host with many ICMP echo requests in a short amount of time
5.Attack Mechanism: When a host is flooded with echo requests in the quantity and time-frame shown above (150 requests in 8 seconds) , it is possible to overflow the victims available ports causing the tcp stack to panic and/or clog other traffic that might be traveling to or from the victims network on an already utilized link causing router failure.
6.Correlations: This attack is as old as RFC 792. Often this is picked up as a false alarm if people are running a continuous ping as a diagnostic for a host in distress. However due to the destination being an apparent dialup account in Boston, while the source entity is in New York, combined with regularity of "interesting" traffic from this host I like to examine their traffic a little closer.
7.Evidence of targeting: With the over 3 days worth of flooding from the OMI hosts all of the attacks seem to be concise and planned.
8.Severity (critical + Lethal) – (System + Net Countermeasures) = Severity
(2+4)-(3+1)=2
9.Defensive recommendations: Block ICMP requests at the router. A More feasible option set your firewall to drop icmps after they have reached a predefined threshold i.e. 150 requests in 8 seconds.
10.Multiple Choice
When dealing with possible rogue hosts such as OMI it is most important to
A. eliminate the scourge from your network immediately
B. send harassing email to the domain registrant demanding they cease immediately
C. Approach the Admin of the domain in a businesslike manner and try to come to real solutions for issues that they might not be aware of
D. report the host to abuse.net EVERYDAY
Answer C.

Last Updated: July 27th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced