Global Information Assurance Certification Paper

Detect: 1

May 7 23:31:21 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.31.212.213:4790 to 24.3.21.199 on unserved port 27374
May 8 00:41:59 cc1014244-a kernel: securityalert: udp if=ef0 from 24.129.16.16:1030 to 24.3.21.199 on unserved port 9200
May 8 02:36:36 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.161.94.8:1572 to 24.3.21.199 on unserved port 1243
May 8 02:36:41 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.161.94.8:1826 to 24.3.21.199 on unserved port 5400
May 8 02:36:46 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.161.94.8:2080 to 24.3.21.199 on unserved port 6400
May 8 06:27:19 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.17.13.101:3128 to 24.3.21.199 on unserved port 27374
May 8 10:34:25 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.112.132.178:1073 to 24.3.21.199 on unserved port 27374
May 8 11:58:37 cc1014244-a kernel: securityalert: udp if=ef0 from 208.147.89.119:22852 to 24.3.21.199 on unserved port 6970
May 8 13:21:59 cc1014244-a kernel: securityalert: udp if=ef0 from 207.188.7.102:30324 to 24.3.21.199 on unserved port 6970
May 8 13:30:38 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.1.50.85:4809 to 24.3.21.199 on unserved port 1234
May 8 13:30:40 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.1.50.85:4809 to 24.3.21.199 on unserved port 1234
May 8 13:32:51 cc1014244-a kernel: securityalert: udp if=ef0 from 205.219.198.204:1493 to 24.3.21.199 on unserved port 4436
May 8 17:15:29 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.8.178.161:2170 to 24.3.21.199 on unserved port 1243

1. **Source of Trace :** http://www.sans.org/y2k/051400.htm

2. **Detect Generated by:** The detect was probably generated by a UNIX firewall or proxy as indicated by the reference to a kernel. It should be noted that the trace does not go into detail as to any flags set in the TCP packets. The fields of importance are Timestamp, kernel, action, protocol, rule causing the action, source IP/Port, destination IP/Port.

3. **Probability Source Address was Spoofed:** In the majority of cases shown above the TCP packets were generated from *HOME.COM* and the UDP packets were generated from *REAL.COM*. Since the addresses were widespread throughout the domains it is a good possibility that the addresses are being spoofed and that any return packets may be redirected to the attacker's true address.

4. **Description of Attack:** This is a scan for various trojans on one specific host. All activity is generated on one day at various times. This seems to be a trace of two separate attacks looking for various trojans on this target system. Trojans looked for on this day included 1243/27347 – sub 7 , 5400 – Blade runner/Back Construction, 6400 – The Thing, 6970 – Gate Crasher, and 1234 Ultors. I found a very nice reference list of trojan ports at **www.zipworld.com.au/~michael_h/trojans01c.htm**.

5. **Attack Mechanism:** The packets are intended to elicit a response from a compromised system which would then inform the attacker that the given trojan exists on the system.

6. **Correlations:** This event drew my attention before I had consulted the example detects provided by SANS after my course. Timothy Trow analysed a similar scan from Binette, which

was published on 3/28 in GIAC. From Stephen's comments this attacker has been trying to look at this particular system for a long period of time. It is also possible that the attacker is using this particular target as a constant test case for various script modifications to ensure that the script will run as well as the faint hope that the target will have one loophole open. A reasonable question might also be; What about this particular system is so interesting to the attacker that he keeps coming back? Is it possible that this target is also being used in attempts to establish trojan connections and that the detects are the attacker looking for confirmation of success?

7. Evidence of Active Targeting: Over both cited days and other posts to GIAC only the exact same host has been targeted albeit with many ports.

8. Severity: Criticality = 3 [Trace does not indicate if target is anything more than a workstation]

Severity = 5 [If any trojans were successful the root access and possibly the entire network could be compromised]

System Countermeasures = 3 [detailed log indicates an alert system admin so I assume system is relativly up to date]

Network Countermeasures = 5 [Firewall is blocking packets]

Severity evaluation = [3 +5 – 3 – 5] = 0

9. Defensive Recommendation: Defenses are fine. I believe no responses were sent back to the attackers. Suggested fire wall rule would be to block SYN packets from the network and to block incoming UDP packets from known trojan source ports which are not used by the network

10. Sample Test Question: Examining the attack above, Which of the following statements is true?

A: a single attacker probably generated the event.

B: The event was recorded by SNORT.

C: The attack was targeting known trojan ports.

D: The traces were certainly a result of a wide based hacker network.

Answer: C

Detect: 2

Name: canopus.ucsd.edu
Address: 132.239.114.243
Apr 23 09:54:28 132.239.114.243:14049 -> xxx.xxx.xxx.001:5556 SYN **S*****
Apr 23 09:54:28 132.239.114.243:14052 -> xxx.xxx.xxx.005:5556 SYN **S*****
Apr 23 09:54:28 132.239.114.243:14051 -> xxx.xxx.xxx.003:5556 SYN **S*****
Apr 23 09:54:28 132.239.114.243:14050 -> xxx.xxx.xxx.002:5556 SYN **S*****
Apr 23 09:54:34 132.239.114.243:14051 -> xxx.xxx.xxx.004:5556 SYN **S*****
Apr 23 09:54:34 132.239.114.243:14052 -> xxx.xxx.xxx.005:5556 SYN **S*****

Apr 23 11:45:37 EDT: Blocked inbound TCP SYN from
132.239.114.243 port 27705 to x.x.67.62 port 5556

Apr 23 11:45:37 EDT: Blocked inbound TCP SYN from
132.239.114.243 port 27706 to x.x.67.65 port 5556

Apr 23 11:45:37 EDT: Blocked inbound TCP SYN
from 132.239.114.243 port 27707 to x.x.67.77 port 5556

1. **Source of Trace:** top trace: http://www.sans.org/y2k/042600.htm
bottom trace: http://www.sans.org/y2k/042900.htm

2. **Detect Generated by:** Top trace is a sniffer trace showing timestamp, source system:port, destination system:port and TCP flag. The bottom trace is a firewall or proxy log showing timestamp, action taken [which indicates the rule that caused the action], source ID:port, and destination ID:port.

3. **Probability Source Address was Spoofed:** No, The attacking system was one traced to canopus.ucsd.edu. However the poster of the lower scan contacted the owner of the source system who replied to him that the system had been pulled from the network for investigation. I would be curious to know if the source system had been compromised from an external source and was being used as an intermediary for the event or if the attack was programmed from the machine alone.

4. **Description of Attack:** Network scan for a specific trojan. This is an attempt to discover any hosts compromised with the BO Facil trojan.

5. **Attack Mechanism:** Attacking system sends SYN packets in an attempt to elicit a response from a compromised system infected with BO-Facil. Note that all packets are sent at the same time and that the source ports increment.

6. **Correlations:** I included the second trace to show what seems to be a modification of the first scan. In the top scan all hosts on the class C network were scanned. Two hours later the second trace only targeted systems running port 80 webservers. An interesting question would be "Are all the systems in the top scan port 80 webservers or has the attack been modified in the two hour time span to only look at previously discovered systems?"

7. **Evidence of Active Targeting:** The top scan seemingly targeted all systems on the network. The bottom scan targeted only specific systems. The bottom scan was very much targeted by what would seem to be prior knowledge.

8. Severity: Criticality = 3 [web server targeted]

Severity = 3 [if trojan found system could be compromised and used for unintended purposes]

System Countermeasures = 0 [unknown state of host]

Network Countermeasures = 5 [firewall blocked traffic]

Severity = 3 + 3 – 0 – 5 = 1

9. Defensive Recommendation: Defenses were correct. Firewall/proxy blocked packets. The firewall/proxy is defending the network against this attack properly. Suggested firewall rules are to block incoming SYN packets.

10. Sample Test Question

A: The event was blocked by a firewall rule.

B: TCP wrappers blocked The event.

C: The event was blocked by host configuration.

D: None of the above.

Answer: A

Detect: 3

```
Mar 19 21:50:37 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.11:53
Mar 19 21:50:37 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.12:53
Mar 19 21:50:37 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.20:53
Mar 19 21:50:37 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.32:53
Mar 19 21:50:37 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.34:53
Mar 19 21:50:38 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.61:53
Mar 19 21:50:38 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.73:53
Mar 19 21:50:38 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.80:53
Mar 19 21:50:38 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.82:53
Mar 19 21:50:38 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.84:53
Mar 19 21:50:38 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.98:53
Mar 19 21:50:38 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.100:53
Mar 19 21:50:39 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.157:53
Mar 19 21:50:40 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.181:53
Mar 19 21:50:40 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.187:53
Mar 19 21:50:41 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.217:53
Mar 19 21:50:41 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.222:53
Mar 19 21:50:41 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.224:53
Mar 19 21:50:41 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.225:53
Mar 19 21:50:41 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.237:53
Mar 19 21:50:41 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.239:53
Mar 19 21:50:41 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.240:53
Mar 19 21:50:41 hostk snort[4656]: SCAN-SYNFIN: 198.146.83.191:53 -> a.b.d.243:53

[**] SCAN-SYNFIN [**]
        03/19-21:50:36.832284 198.146.83.191:53 -> a.b.d.11:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......

        [**] SCAN-SYNFIN [**]
        03/19-21:50:36.853107 198.146.83.191:53 -> a.b.d.12:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......

        [**] SCAN-SYNFIN [**]
        03/19-21:50:37.010846 198.146.83.191:53 -> a.b.d.20:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......

        [**] SCAN-SYNFIN [**]
        03/19-21:50:37.245273 198.146.83.191:53 -> a.b.d.32:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......

        [**] SCAN-SYNFIN [**]
        03/19-21:50:37.279695 198.146.83.191:53 -> a.b.d.34:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......
```

```
[**] SCAN-SYNFIN [**]
        03/19-21:50:36.832284 198.146.83.191:53 -> a.b.d.11:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......

        [**] SCAN-SYNFIN [**]
        03/19-21:50:36.853107 198.146.83.191:53 -> a.b.d.12:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......

        [**] SCAN-SYNFIN [**]
        03/19-21:50:37.010846 198.146.83.191:53 -> a.b.d.20:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......

        [**] SCAN-SYNFIN [**]
        03/19-21:50:37.245273 198.146.83.191:53 -> a.b.d.32:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......

        [**] SCAN-SYNFIN [**]
        03/19-21:50:37.279695 198.146.83.191:53 -> a.b.d.34:53
        TCP TTL:31 TOS:0x0 ID:39426
        **SF**** Seq: 0x2D7B753B Ack: 0x76E8EFD7 Win: 0x404
        00 00 00 00 00 00 ......
```

1. **Source of Trace:** http://www.sans.org/y2k/032000.htm

2. **Detect Generated by:** Snort Intrusion Detection System.

3. **Probability Source Address was Spoofed:** Not likely. Information from scan would have to be received by the source. It is possible that the source could have a redirect instruction built in for the return information but it is not likely.

4. **Description of Attack:** This is a scan for servers listening on port 53[DNS] on the target network.

5. **Attack Mechanism:** Constructed packets are broadcast to hosts on the network with the intention of finding an internal network DNS host. The impossible flag combination of SYN-FIN could be designed to evaded a firewall set to refuse SYN packets. As is stated in the *Intrusion Detection and Packet filtering Course Manual* [pp. 114] this could also be a search for a server running the Linux operation system which will respond to this scan with a SYN-FIN-ACK packet. This was probably done by a scripted attack as is evidenced by 1] the source port being 53. 2] all packets have the same packet identifier [39426] and 3] the rapid sending of the packets.

6. Correlations: SYN-FIN scans are well documented throughout the GIAC. This scan may be a variant of the SYN-FIN-Source 0 scan documented in Bugtraq\1998_3/014.html. That this scan is set to source port on the DNS port using TCP protocol makes it slightly unusual and it could be the beginning of a zone transfer intelligence gathering exploit.

7. Evidence of Active Targeting: The fact that the exploit was made up of manufactured packets and quite possibly scripted proves active targeting.

8. Severity:

Criticality = 5 [DNS servers targeted]

Lethality = 3 [If host table capture is effected attacker has knowledge of the network]

System Countermeasures = 0 [no knowledge of the target systems is available]

Network Countermeasures = 5 [I assume SNORT blocked the packets]

Severity = [5 + 3 – 0 – 5] = 3

9. Defensive Recommendation: Defense was fine, Firewall blocked attack. Suggested firewall rules would be to block any impossible TCP flag combinations.

10. Sample Test Question

A: The attack is a zone transfer

B: The attack is a DNS version scan

C: The attack is an information probe scan

D: All of the above

Answer C:

Detect: 4

02:26:31.574847 209.216.2.200 > morannon.kdi.com: (frag 30041:48@2960)
02:26:31.583572 209.216.2.200 > morannon.kdi.com: icmp: echo request (frag 30041:1480@0+)
02:26:31.583582 209.216.2.200 > morannon.kdi.com: (frag 30044:48@2960)
02:26:31.591760 209.216.2.200 > morannon.kdi.com: icmp: echo request (frag 30044:1480@0+)
02:26:31.591768 209.216.2.200 > morannon.kdi.com: (frag 30046:48@2960)
02:26:31.600166 209.216.2.200 > morannon.kdi.com: icmp: echo request (frag 30046:1480@0+)
02:26:31.600173 209.216.2.200 > morannon.kdi.com: (frag 30048:48@2960)
02:26:31.609754 209.216.2.200 > morannon.kdi.com: icmp: echo request (frag 30048:1480@0+)
02:26:31.609785 209.216.2.200 > morannon.kdi.com: (frag 30050:48@2960)
02:26:31.618328 209.216.2.200 > morannon.kdi.com: icmp: echo request (frag 30050:1480@0+)
02:26:31.618354 209.216.2.200 > morannon.kdi.com: (frag 30052:48@2960)
02:26:31.626650 209.216.2.200 > morannon.kdi.com: icmp: echo request (frag 30052:1480@0+)
02:26:31.626656 209.216.2.200 > morannon.kdi.com: (frag 30054:48@2960)
02:26:31.635248 209.216.2.200 > morannon.kdi.com: icmp: echo request (frag 30054:1480@0+)

1. **Source of Trace:** http://www.sans.org/y2k/032900.htm

2. **Detect Generated by:** Windump capture of network traffic. The fields are timestamp, packet id, source ID , target id, protocol, fragment identifier, fragment size, and offset.

3. **Probability Source Address was Spoofed:** Unlikely. The source address resolves to a valid organization. The poster of the trace noted that the owners of the system were contacted.

4. **Description of Attack:** This is a Denial of Service attack combining the "fragmented ICMP attack" and the "un-named fragmentation attack" .

5. **Attack Mechanism:** Attacker crafts fragmented ICMP packets having non-contiguous starting points. When the host attempts to re-assemble the packets the intent is to cause the operating system to hang up or re-boot. This particular trace shows normal packet size with only the middle 1480 size packet missing. The crafter of this attack may be using the fragments to evade a network rule dis-allowing ICMP echo requests from entering the network.

6. **Correlations:** The "un-named fragmentation attack is documented *in TCP/IP for Intrusion Detection and Perimeter Defense* [PP 3-25/26] and the fragmented ICMP attack is documented in *Network Based Intrusion Detection Analysis* [P- 255].

7. **Evidence of Active Targeting:** The packets were all aimed at one host system.

8. **Severity:**

   Criticality = 2 [no identity of the attacked system was given]

   Lethality = 1 [only certain operating systems are subject to this attack, no information was given if any reconnaissance had occurred previously]

   System Countermeasures = 0 [no information available]

   Network Countermeasures = 5 [the poster of the trace did not suggest that the packets cause any problem so I can only assume that no damage was done]

   Severity = [2 + 1 – 0 – 5] = -2

8. Defensive Recommendation: The host system defenses seemed to be adequate. A firewall or packet filter rule blocking ICMP echo requests should defeat this attack. Keeping operating systems current with all recommended patches should also contribute to avoiding this type of attack.

9. Sample Test Question

A: The packet's missing fragments could not have ever existed.

B: ICMP packets cannot contain fragments.

C: It is necessary to allow all types of ICMP traffic into a network.

D: All of the above are incorrect.

Answer: = D

Detect: 5

Feb 25 21:14:38 134.161.1.101 21043: %SEC-6-IPACCESSLOGP:
list ingress denied udp 38.29.63.57(4419) -> 134.161.67.71(34555),
1 packet
Feb 25 21:14:51 134.161.1.101 21044: %SEC-6-IPACCESSLOGP:
list ingress denied udp 38.29.63.57(4420) -> 134.161.67.71(34555),
1 packet
Feb 25 21:14:57 134.161.1.101 21045: %SEC-6-IPACCESSLOGP:
list ingress denied udp 38.29.63.57(4421) -> 134.161.67.71(34555),
1 packet
Feb 25 21:15:00 134.161.1.101 21046: %SEC-6-IPACCESSLOGP:
list ingress denied udp 38.29.63.57(4422) -> 134.161.67.71(34555),
1 packet
Feb 26 00:35:40 134.161.1.101 22024: %SEC-6-IPACCESSLOGP:
list ingress denied udp 38.29.63.57(4523) -> 134.161.67.71(34555),
1 packet
Feb 26 11:01:56 134.161.1.101 24967: %SEC-6-IPACCESSLOGP:
list ingress denied udp 38.29.63.170(4531) -> 134.161.67.71(34555),
1 packet
Feb 26 11:09:24 134.161.1.101 25007: %SEC-6-IPACCESSLOGP:
list ingress denied udp 38.29.63.170(4541) -> 134.161.67.71(34555),
1 packet
Feb 26 11:09:26 134.161.1.101 25008: %SEC-6-IPACCESSLOGP:
list ingress denied udp 38.29.63.170(4542) -> 134.161.67.71(34555),
1 packet

1. **Source of Trace:** http://www.sans.org/y2k/030100.htm

2. **Detect Generated by:** Cisco router log: The relevant fields are : Timestamp, router address, Access list identifier, action taken, protocol, source IP & port, destination IP & port.

3. **Probability Source Address was Spoofed:** Medium Address resolves back to an Internet service provider. It would take the cooperation of the ISP to trace the actual user and determine if the account was being misappropriated by someone other than the account owner.

4. **Description of Attack:** This trace was generated after the system administrator discovered a system on his network [the destination system] had been compromised with both Back Orifice and a Windows version of the Trinoo client. Named Winoo this trojan caused the compromised system to listen on port 34555. The trace is either a master system or a daemon at a higher tier in the network attempting to communicate with the previously compromised target system. Setting router Access Control Lists [ACL] to block packets going to this system generated the trace from which may be deduced that the DDOS to communicates with its client machines by UDP.

5. **Attack Mechanism:** Winoo Master Host [the true attacker] sends commands out to compromised clients directing them to perform actions ranging from compromising other systems in the network to conducting Distributed Denial of Service [DdoS] on a given target.

6. **Correlations:** On GIAC lists for both 3/2/00 and 3/4/00 systems listening on this port were reported. All compromised networks were found to be .EDU networks. The 3/4/00 post included a search of previously captured network traffic, which showed the source address from this trace as well as other addresses from the source network creating traffic to this particular port.

7. Evidence of Active Targeting: Obviously prior to discovery by the system administrator, the compromised system had reported its presence back to the Master [Attacker] system. The Master system had no way of knowing that the compromised system had been taken off line and was targeting communication at the compromised system.

8. Severity:

Criticality = 4 [Compromised system could infect others in the Network]

Lethality = 4 [Attacker could own the network but considering that the compromise was to put a client host in place the system itself would not be shut down but would be used to attack other networks]

System Countermeasures = 0 unknown . [The compromise was allowed to happen but it was discover by other means.]

Network countermeasures = 5 [router ACL set to block traffic to the compromise port]

Severity = [3 + 4 – 0 – 5] = 2

9. Defensive Recommendation: The current counter measures worked adequately. The knowledge gained should be used to inspect the network for other hosts, which may have been compromised. Any traffic coming from the source network should be captured and examined with an eye towards a "script Kiddie" merely modifying the listening port or the protocol used by the trojan.

10. Sample Test Question

A: The packets were a result of an automated script.

B: The source address was spoofed.

C: The packets were 34555 bytes in size.

D: This is attempted Master-Daemon communication.

Answer D:

Detect: 6

Feb 29 08:21:19 dns2 /usr/local/bin/snort[8374]:
RPC - portmap-request-mountd: 192.117.186.53:918 -> x.x.x.x:111
Feb 29 08:21:19 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:24 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:29 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:34 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:39 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)
Feb 29 08:21:44 dns2 rpcbind: refused connect
from 192.117.186.53 to getport(mountd)

1. **Source of Trace:** http://www.sans.org/y2k/030100.htm

2. **Detect Generated by:** Snort Intruder Detection. The fields are Timestamp, destination host, RPC service, source host, port attacked.

3. **Probability Source Address was Spoofed:** Medium The source resolves back to the Israeli Network Information Center.

4. **Description of Attack:** This is an attempt to gain root access to a host via use of mountd. The daemon is subject to buffer overflow against a LINUX system [CVE 199-002] or against Solaris [CVE 1999-212] could be mounted and the attacker could gain root access or knowledge of files on the target. Another GIAC analyst pointed out that the source port of 53 could be an attempt to get past firewall rules blocking such traffic. Also note that the target is a DNS server, if compromised this could lead to all sorts of mischief.

5. **Attack Mechanism:** The attack begins with an attempt to gain information from portmapper and subsequently attempts to gain a response from the mountd daemon directly by name.

6. **Correlations:** The similar traces shown throughout the month of February 2000 are mostly aimed at .EDU sights. However the source ports are not always 53. It is likely an exploit was published on one of the "hacker sites" and has been slightly modified by various users. The even 5-second interval between packets would also lead to a suspicion of a script being run.

7. **Evidence of Active Targeting:** The scan was aimed at one target only.

8. **Severity:**

Criticality = 5 [Target is a NS server]

Lethality = 5[Depending on operating system of target the subsequent attack could lead to Root access or total network knowledge – see Section 4.]

System Countermeasures = 3 [basically unknown Server protection – however since the vulnerabilities of the OS attacks date from 1999 I am presuming that patches would be applied]

Network countermeasures = 5 [Snort rule blocks RPC calls]

Severity = [5 + 5 –3 –5] =2

9. Defensive Recommendation: Network rebuffed the attack. Host systems should be maintained as to current patches against discovered vulnerabilities and configured with no extraneous services. Firewalls, routers and packet filters should have rules and/or access lists upgraded regularly as new attack patterns are discovered.

10. Sample Test Question

A: This is a buffer overflow attack.

B: This is a system log scan.

C: This is a zone transfer attack.

D: The source port is an attempt to bypass system ingress rules.

Answer D:

Detect: 7

Mar 4 20:07:41.498701 134.76.242.31,23 -> 10.0.0.3,23 PR tcp len 20 40 -A
Mar 4 20:07:41.514052 134.76.242.31,25 -> 10.0.0.3,25 PR tcp len 20 40 -A
Mar 4 20:07:41.526642 134.76.242.31,143 -> 10.0.0.3,143 PR tcp len 20 40 -A
Mar 4 20:07:41.540043 134.76.242.31,110 -> 10.0.0.3,110 PR tcp len 20 40 -A
Mar 4 20:07:44.512896 134.76.242.31,23 -> 10.0.0.8,23 PR tcp len 20 40 -A
Mar 4 20:07:44.546208 134.76.242.31,25 -> 10.0.0.8,25 PR tcp len 20 40 -A
Mar 4 20:07:44.579704 134.76.242.31,143 -> 10.0.0.8,143 PR tcp len 20 40 -A
Mar 4 20:07:44.593504 134.76.242.31,110 -> 10.0.0.8,110 PR tcp len 20 40 –A

1. Source of Trace: http://www.sans.org/y2k/030600.htm

2: Detect Generated by: tcpdump of sniffed network traffic. The fields of interest are Timestamp, Source IP/Port, Destination IP/Port, protocol, header length, Flag set.

3: Probability Source Address was Spoofed: Low: The attacker is looking for responses from active systems. The source address resolves to a network in Germany.

4: Description of Attack: Information gathering attack looking for live hosts on the network. Probably a scripted tool, possibly a modification of ACK.COM, judging from the source port an destination port being the same as well as the rapid sequence of scans on each host. In normal traffic the source port would probably be an ephemeral port above 1023.

5: Attack Mechanism: Since no outgoing packets have requested responses, the attacker is expecting a reached system to respond with a RESET flag packet. The attacking packets are sent with an ACK flag set to persuade a packet filtering device to allow the packet into the network. To make the traffic seem more "normal" the attacker is targeting the ports for common services, i.e. telnet, sendmail, IMAP, and POP 3.

6: Correlations: This attack is defined in *Intrusion Detection Analysis – Shadow Style* Pp – 178.

7: Evidence of Active Targeting: Yes, note four separate packets to each host. A longer trace might have shown a pattern to the selection of the fourth octet.

8: Severity:

Criticality = 2 [at this point the attacker would not be able to ascertain anything more than a system exists]
Lethality = 1 [systems would not be harmed by this first information gathering, but further probes would follow]

System Countermeasures = 0 [systems would reply to packet]

Network Countermeasures = 3 [No return traffic shown]

Severity = [2 + 1 – 0 – 1] = 2

9: Defensive Recommendation: This specific attack could be blocked by a filtering rule stating that packets having only the ACK flag and having identical source and destination ports should be dropped. Such a combination would probably not occur in normal traffic.

10: Sample Test Question

A: This attack is an attempt to shut down common ports.

B: The attacker is using an inverse scan for hosts.

C: This attack is attempting to by-pass packet filtering rules.

D: None of the above.

Answer C:

Detect: 8

Jan 30 13:43:40.686098 208.220.132.41,137 -> 10.0.0.32,137 PR udp len 20 78
Jan 30 13:43:42.183425 208.220.132.41,137 -> 10.0.0.32,137 PR udp len 20 78
Jan 30 13:43:51.447650 208.220.132.41,137 -> 10.0.0.33,137 PR udp len 20 78
Jan 30 13:44:12.652868 208.220.132.41,137 -> 10.0.0.35,137 PR udp len 20 78

[.. and so on ..]

Jan 30 13:58:32.859186 208.220.132.41,137 -> 10.0.0.126,137 PR udp len 20 78
Jan 30 13:58:38.988800 208.220.132.41,137 -> 10.0.0.127,137 PR udp len 20 78
Jan 30 13:58:40.460850 208.220.132.41,137 -> 10.0.0.127,137 PR udp len 20 78
Jan 30 13:58:41.968551 208.220.132.41,137 -> 10.0.0.127,137 PR udp len 20 78

1: Source of Trace: http://www.sans.org/y2k/020200.htm

2: Detect Generated by: tcpdump The fields are TimeStamp, Source IP/Port, Destination IP/Port, Protocol, packet length.

3: Probability Source Address was Spoofed: low The attacker is looking for systems with NetBIOS services. The source system resolves to an ISP.

4: Description of Attack: This is a methodical information gathering scan of a network looking for Windows or NT based hosts running this service. If any hosts respond the attacker would possible attempt to gain access to the host to run NBSTAT and gain network information or to gain access to the host's file system.

5: Attack Mechanism: The attacker sends packets to hosts within the network hoping to find NetBIOS in use. If a host responds a connection may be attempted. With a connection made the attacker may attempt use a Null Session to run NBSTAT to gain further information about the network, gain access to files on the host, gain access to registry keys and mount an attack to obtain system passwords. Certain viruses, such as the 911 Worm operate using file shares.

6: Correlations: This type of scan and its possible consequences are discussed in the SANS course manual 2.4/2.5 *INTRUSION DETECTION ANALYSIS* PP 292-295. The NetBIOS attack is also declared one of the ten most critical Internet security threats by the Expert's Consensus V 1.15.

7: Evidence of Active Targeting: The entire class C network of the target is being scanned host by host.

8: Severity:

Criticality = 4 [If the service is found a means of access to major network components may be found]

Lethality = 5 [The entire network may be accessed with information discovered by gaining NetBIOS access]

System Countermeasures = 0 [no information given]

Network Countermeasures = 5 [no return traffic shown]

Severity = [4 + 5 – 0 –5] = 4

9: Defensive Recommendation: As of this trace system defenses seem to be adequate. Proper steps would be to restrict file sharing as much as possible – best case would be to never enable NetBIOS on all hosts. Block inbound connections to NetBIOS Session Service from the network router or from the NT hosts running the service.

Sample Test Question

A. This attack is would succeed because all Windows/NT systems need to have the NetBIOS service in operation.

B: This attack will shut down all file sharing services on the network.

C: This attack is launched from a spoofed source address.

D. Access to NetBIOS can reveal large amounts of information about the network and its users.

Answer: D

Detect: 9

```
 Mar 3 00:04:56 dns3 portsentry[301]: attackalert:
Connect from host: max3-240.max3.hou.infohwy.com/207.90.225.240
to TCP port: 79
Mar 3 00:05:00 dns3 portsentry[301]: attackalert:
Connect from host: max3-240.max3.hou.infohwy.com/207.90.225.240
to TCP port: 143
Mar 3 00:07:09 dns3 portsentry[301]: attackalert:
Connect from host: max3-240.max3.hou.infohwy.com/207.90.225.240
to TCP port: 79
Mar 3 00:07:11 dns3 in.telnetd[11055]:
refused connect from max3-240.max3.hou.infohwy.com
Mar 3 00:07:17 dns3 portsentry[301]: attackalert:
Connect from host: max3-240.max3.hou.infohwy.com/207.90.225.240
to TCP port: 143
Mar 3 00:07:25 dns3 in.telnetd[11131]:
refused connect from max3-240.max3.hou.infohwy.com
Mar 3 00:08:55 dns3 portsentry[301]: attackalert:
Connect from host: max3-240.max3.hou.infohwy.com/207.90.225.240
to TCP port: 79
Mar 3 00:08:56 dns3 in.telnetd[11133]:
refused connect from max3-240.max3.hou.infohwy.com
Mar 3 00:09:02 dns3 portsentry[301]: attackalert:
Connect from host: max3-240.max3.hou.infohwy.com/207.90.225.240
to TCP port: 143
Mar 3 00:09:09 dns3 in.telnetd[11134]:
refused connect from max3-240.max3.hou.infohwy.com
```

1. **Source of Trace:** http://www.sans.org/y2k/030400.htm

2. **Detect Generated by:** Port Sentry. Fields are Timestamp, Destination IP, action, attempted Source IP name resolution, Source IP, Destination Port

3. **Probability Source Address was Spoofed:** Low Source IP resolves to an ISP. The attack is depending on getting information returned from the target.

4. **Description of Attack:** The attacker is attempting an intrusion on the target system. He verifies that finger, IMAP and telnet are available on the system. He then attempts access to the host via telnet. He gets information on users from finger, information on services from IMAP and then may attempt to obtain passwords in order to gain access to the system.

5. **Attack Mechanism:** By attempting connection over various services the attacker may determine which destination ports the network rules will allow him to connect with this host.

6. **Correlations:** The targeted services are all subject to various types of attacks as documented in the CVE. They share a commonality of all being subject to some type of buffer overflow attack. Many of the attacks can result in root access to the target. The list of *Ten Most Critical Internet Security Threats* also lists IMAP as a severely vulnerable service. I am not sure that the attacker knew his target was a DNS host as no probe was mounted against port 53.

7. Evidence of Active Targeting: All attempts were made on the same host.

8. Severity:

Criticality = 5 [target was a DNS server, even if the attacker was not aware of the fact]

Lethality = 4 [possibility of denial of service or root access]

System Countermeasures = 3 [host based IDS system running]

Network Countermeasures = 5 [portmapper blocked or alerted on connections]

Severity = [5 + 4 – 3 –5] = 1

9. Defensive Recommendation: The system withstood the attack at this time. A needs analysis of the host should be undertaken to see if it is necessary for the host's function to have these services running and if they are not necessary they should be removed.

10. Sample Test Question

A: The ports under attack can be used to obtain root access.

B: Success of this attack will not lead to a large amount of information about the host being discovered.

C: This is a zone transfer attack.

D: Port Sentry is a network based IDS.

ANSWER: A

Detect: 10

```
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2496 dst xxx.xxx.xxx.0/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2497 dst xxx.xxx.xxx.1/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2498 dst xxx.xxx.xxx.2/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2499 dst xxx.xxx.xxx.3/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2500 dst xxx.xxx.xxx.4/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2501 dst xxx.xxx.xxx.5/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2502 dst xxx.xxx.xxx.6/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2503 dst xxx.xxx.xxx.7/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2504 dst xxx.xxx.xxx.8/111
May 12 14:48:58 : Deny inbound tcp src
  210.104.234.5/2505 dst xxx.xxx.xxx.9/111
May 12 14:48:59 : Deny inbound tcp src
  210.104.234.5/2506 dst xxx.xxx.xxx.10/111
May 12 14:48:59 : Deny inbound tcp src
  210.104.234.5/2507 dst xxx.xxx.xxx.11/111
May 12 14:48:59 : Deny inbound tcp src
  210.104.234.5/2508 dst xxx.xxx.xxx.12/111
```

1. **Source of Trace:** http://www.sans.org/y2k/060100.htm

2. **Detect Generated by:** Filtering Router or firewall. The fields are Timestamp, action, protocol, source IP/Port, Destination IP/Port.

3. **Probability Source Address was Spoofed:** Low. Information gathering scan from Ilsan Information Industrial High School, Korea.

4. **Description of Attack:** Attacker is scanning entire Class C network looking for SUNRPC/PORTMAPPER . Access to port 111 allows attacker to port locations running various RPC services to be used for future attacks.

5. **Attack Mechanism:** Probability of a scripted/automated attack. Attacker is hoping to gain knowledge of which hosts are running portmapper via getting a response from that host via normal TCP handshake. The trace exhibits several signature characteristics. The destination IP is incremented one by one, simultaneously likewise is the source port. The rapid transmission of packets leads me to believe that this is an automated scan.

6. **Correlations:** GIAC reports through the early months of 2000 show many instances of attacks against RPC services and attempts to gain information about those services via access to PORTMAPPER. Direct users of PORTMAPPER can include use of the service as a proxy [CVE 1999 –168] and DoS attacks [CAN 1999 –0195]. *The Ten Most Critical Internet Security Threats* lists vulnerability of this service as high and recommends that portmapper be disabled if at all possible.

7. Evidence of Active Targeting: The entire class C network was methodically scanned.

8. Severity:

Criticality = 4 [Attacker gains knowledge of addresses of vulnerable hosts – further attacks will be much more critical]

Lethality = 2 [This exploit in itself is not lethal, but if successful will lead to a much larger compromise]

System Countermeasures = 0 [No information about hosts given in scan]

Network Countermeasures = 5 [the firewall or router has a rule blocking external TCP contact with this port]

Severity = [4 + 2 – 0 – 5] = 1

9. Defensive Recommendation: The defenses are working properly. There is always the possibility of entrance into the network through an unknown back door so the network hosts should be configured not to enable this port if at all possible.

10. Sample Test Question

A: The network hosts are dropping the packets.

B: This exploit is successful against Windows\NT hosts.

C: This exploit will overload a firewall.

D: Rules or Access Control Lists prevented this scan.

Answer D: