Global Information Assurance Certification Paper

Joseph Andersen

Detect 1

Trace:
10:36:31.299665 195.221.122.44.111 > 192.168.2.2.111: SF 815187402:815187402(0) win 1028
10:36:31.332942 195.221.122.44.111 > 192.168.1.3.111: SF 815187402:81518 7402(0) win 1028
10:36:31.334991 195.221.122.44.111 > 192.168.1.4.111: SF 815187402:815187402(0) win 1028
10:36:31.364464 195.221.122.44.111 > 192.168.1.5.111: SF 815187402:815187402(0) win 1028

1. Source of Trace
   My network
2. Detect was generated by:
   tcpdump as part of the shadow system
   Fields:
   [timestamp] [Source ip address.port] > [destination ip address.port]:[IP flags] [sequence number] [window size]
3. Probability the source address was spoofed
   Low. I don't think this one was spoofed. It looks like reconnaissance and they would need to get the information back.
4. Description of attack:
   This looks like they are looking for machines that are using the sunrpc port (111) This is typically on Sun OS machines.
5. Attack Mechanism:
   They are just using a port scanner with the Syn and Fin flags set and targeting only port 111. You can see that they are just walking through the ip addresses. The Syn and Fin flag combination are the give away for this type of scan.
6. Correlations:
   Stephen Northcut t talked about this in the SNAP 2000 conference. See Manual 2.5 page 269.
7. Evidence of active targeting:
   This is just a generic scan looking for specific types of machines. Namely Sun machines.
8. Severity:
   (Critical + Lethal) - (System + Net Counter measures) = Severity
   (5+1) - (4+2) = -1
9. Defensive Recommendations
   Watch for more activity from this IP address area to see if they have found any weak machines.
10. Multiple Choice Question
    This trace is an attempt to:
    A) Cause a buffer overflow on port 111
    B) Scan for Portmapper
    C) Cause a Denial of Service to these hosts
    D) This is normal activity

Answer: B

Detect 2:

Trace:
04:53:39.811935 203.238.3.7.3928 > xx.xx.xx.2.domain: S 4080638659:4080638659(0) win 32120 (DF)
04:53:39.812469 x x.xx.xx.2.domain > 203.238.3.7.3928: S 4090339595:4090339595(0) ack 4080638660 win 8576
04:53:39.827408 203.238.3.7.3929 > xx.xx.xx.3.domain: S 4071792438:4071792438(0) win 32120 (DF)
04:53:39.827848 xx.xx.xx.3.domain > 203.238.3.7.3929: S 1692627500:169 2627500(0) ack 4071792439 win 10136 (DF)
04:53:39.840375 203.238.3.7.3932 > xx.xx.xx.6.domain: S 4080697577:4080697577(0) win 32120 (DF)
04:53:39.842370 xx.xx.xx.6.domain > 203.238.3.7.3932: S 945734420:945734420(0) ack 4080697578 win 32120 (DF)
04:53:40.118269 203.238.3.7.3928 > xx.xx.xx.2.domain: . ack 4090339596 win 32120 (DF)
04:53:40.130531 203.238.3.7.3929 > xx.xx.xx.3.domain: . ack 1692627501 win 32120 (DF)
04:53:40.144605 203.238.3.7.3932 > xx.xx.xx.6.domain: . ack 945734421 win 32120 (DF)
04:53:40.186367 203.238.3.7.3928 > xx.xx.xx.2.domain: F 4080638660:4080638660(0) ack 4090339596 win 32488 (DF)
04:53:40.186660 xx.xx.xx.2.domain > 203.238.3.7.3928: . ack 4080638661 win 8576
04:53:40.186878 xx.xx.xx.2.domain > 203.238.3.7.3928: F 4090339596 :4090339596(0) ack 4080638661 win 8576
04:53:40.493553 203.238.3.7.3928 > xx.xx.xx.2.domain: . ack 4090339597 win 32488 (DF)
04:53:41.283107 203.238.3.7.3241 > xx.xx.xx.2.domain: 62760 inv_q+ [b2&3=0x980] A? . (27)
04:53:41.283757 xx.xx.xx.2.domain > 203 .238.3.7.3241: 62760 inv_q Refused [0q] 1/0/0 (27)

1. Source of Trace
   My Network
2. Detect was generated by:
   Shadow system using tcpdump
3. Probability the source address was spoofed
   Low. They are trying to get the information back to their own machine so they can see it.
4. Description of attack
   Scanning for DNS servers and then attempting inverse queries.
5. Attack mechanism
   They first start scanning through the network looking for any servers that respond to port 53 which is the DNS port. After t hey get an answer back they try and do an inverse DNS query to see if it would be eligible for some older exploits.
6. Correlations
   Hal Pomeranz talked about this in his class during the SNAP 2000 conference in San Jose. See Manual 2.1 Pages 4 -25 to 4-27
7. Evidence of Active Targeting
   This attack is doing a general scan first then getting specific.
8. Severity

(Critical + Lethal) - (System + Net Countermeasures) = Severity
(5+1) - (4+2) = 0

9. Defensive recommendation:
   The defenses are fine, the Inver se query failed
10. Multiple choice question
    This trace is an example of what?
    A. Syn/Fin Scan
    B. Normal Activity, no malicious intent
    C. DNS Inverse Query
    D. DNS zone transfer to a secondary DNS server.
    Answer: C

Detect 3:

Trace:
May 20 10:06:00 icestorm portsentry[10121]: attackalert: SYN/Normal scan from host: 203.69.218.98/203.69.218.98 to TCP port: 98
May 20 10:06:00 icestorm portsentry[10121]: attackalert: Host 203.69.218.98 has been blocked via wrappers with string: "ALL: 203.69.218. 98"
May 20 10:06:00 icestorm portsentry[10121]: attackalert: Host 203.69.218.98 has been blocked via dropped route using command: "/sbin/ipchains -I input -s 203.69.218.98 -j DENY -l"

1. Source of Trace:
   http://www.sans.org/y2k/052400 -1300.htm
2. Detect was genereated by:
   A security program called icestorm portsentry.
   Description of fields
   [timestamp][which program is reporting]:[type of attack]:[from host] to [port]
   The remaining entries are rep orting that the host is being blocked out.
3. Probability the source address was spoofed:
   Low. The person is doing reconnaissance and would like to get the information back.
4. Description of attack:
   Attempting to see if the machine is a Linux machine a nd if linuxconf is running.
5. Attack Mechanism:
   They were trying to do a simple connection to port 98 which is the linuxconf port. Linuxconf is one of the configuration tools that RedHat linux and derivatives thereof use. If it is a poorly protected sy stem then they can use linuxconf to gain root access.
6. Correlations:
   Stephen Northcutt talked about this in the SNAP 2000 conference in San Jose. See manual 2.4 page 159.
7. Evidence of Active Targeting:
   Hard to tell from this small snippet, if there was further activity to other machines then we would know for sure. Based on this trace though it seems very specific.
8. Severity:
   (Critical + Lethal) - (System + Net Countermeasures) = Severity
   (5+5) - (5+5) = 0
9. Defensive recommendation:
   It looks like the portsentry took care of the problem before it even got started.
10. Multiple choice test question:

Port 98 is usually equated with what application?

A) Pop 3
B) IMAP
C) LinuxConf
D) NNTP (usenet news)

Answer: C

Detect 4:

Trace:

```
May 28 09:35:33 zion snort[27540]: spp_portscan: PORTSCAN DETECTED from
206.176.81.2
May 28 09:35:33 206.176.81.2:4074  -> x.y.z.102:110 SYN **S*****
May 28 09:35:36 206.176.81.2:4072  -> x.y.z.100:110 SYN **S*****
May 28 09:35:33 206.176.81.2:4077  -> x.y.z.104:110 SYN **S*****
May 28 09:35:33 206.176.81.2:4086  -> x.y.z.110:110 SYN **S*****
May 28 09:35:36 zion snort[27540]: spp_portscan: portscan status from 206.176.81.2: 9
connections across 9 hosts: TCP(9), UDP(0)
May 28 09:35:36 206.176.81.2:4074  -> x.y.z.102:110 SYN **S*****
May 28 09:35:36 206.176.81.2:4077  -> x.y.z.104:110 SYN **S*****
May 28 09:35:36 206.176.81.2:4086  -> x.y.z.110:110 SYN **S*****
May 28 09:35:36 206.176.81.2:4111  -> x.y.z.125:110 SYN **S*****
May 28 09:36:12 zion snort[27540]: sp p_portscan: portscan status  from 206.176.81.2: 8
connections across 8 hosts: TCP(8), UDP(0)
May 28 09:37:13 zion snort[27540]: spp_portscan: End of portscan from 206.176.81.2
```

1. Source of trace:
   http://www.sans.org/y2k/060100 -1400.htm
2. Detect was generated by:
   Snort intrustion detection system.
   Description of fields:
   [timestamp] [source ip address:port] -> [destination ip address:port] [tcp flags that are set]
3. Probability the source address was spoofed
   Low. This looks like reconnaissance and they would need to somehow get the information back.
4. Description of attack:
   This is a scan for pop3 mail servers on this network
5. Attack mechanism:
   They are not trying to be sneaky at all, they are doing blatant attempts to start communication with the pop3 mail server. If any of these machines answer back the attacker will know that pop3 is running. Then they can start guessing usernames and passwords to get into the corporate email.

   This could be also this "hacker's" sneaky way of doing a host scan. They may think that their scan will be covered up by all of the other corporate pop3 activity. This would show the person some likely targets.
6. Correlations:
   Stephen Northcutt talked about scann ing in depth in the SNAP 2000 in San Jose. See Manual 2.5 page 277.

7. Evidence of active targeting:
   This is general targeting right now. The more specific stuff will come later.
8. Severity:
   (Critical + Lethal) - (System + Net Countermeasures) = Seve rity
   (4+3) - (5+2) = 0
9. Defensive recommendation:
   Double check that all of the servers are up to date on patches and versions of pop3, and then watch for more specific traffic from this address.
10. Multiple Choice Question
    This trace is an example of what?
    A) DNS lookup
    B) Pop2 email scan
    C) Pop3 email scan
    D) Pop4 email scan
    Answer: C

Detect 5:

Trace:
209.67.123.169 > xx.xx.xx.2
02:56:11.658829 www.rivalcom.net.2100 > xx.xx.xx.2.domain: S 141013878:141013942(64) win 2048
02:56:11.659357 xx.xx.xx.2.domain > www.rivalcom.net.2100: S 2745286788:2745286788(0) ack 141013879 win 8192
02:56:11.659482 www.rivalcom.net.2101 > xx.xx.xx.2.domain: S 1331985529:1331985593(64) win 2048
02:56:11.659907 xx.xx.xx.2.domain > www.rivalcom.net.2101: S 2745341647:2745341647(0) ack 1331985530 win 8192
02:56:11.660057 www.rivalcom.net.2102 > xx.xx.xx.2.domain: S 1125271579:1125271643(64) win 2048
02:56:11.660482 xx.xx.xx.2.domain > www.rivalcom.net.2102: S 2745397344:2745397344(0) ack 1125271580 win 8192
02:56:11.709723 www.rivalcom.net.2101 > xx.xx.xx.2.domain: R 1331985530:1331985530(0) win 0
02:56:11.710194 www.rivalcom.net.2100 > xx.xx.xx.2.domain: R 141013879:141013879(0) win 0
02:56:11.710517 www.rivalcom.net.2102 > xx.xx.xx.2.domain: R 1125271580:112527 1580(0) win 0
02:56:11.714511 www.rivalcom.net.2101 > xx.xx.xx.2.domain: R 1331985530:1331985530(0) ack 2745341648 win 2048
02:56:11.714963 www.rivalcom.net.2100 > xx.xx.xx.2.domain: R 141013879:141013879(0) ack 2745286789 win 2048
02:56:11.715411 www.riva lcom.net.2102 > xx.xx.xx.2.domain: R 1125271580:1125271580(0) ack 2745397345 win 2048
1. Source of trace
   My Network
2. Detect was generated by:
   This is taken from the Shadow Intrusion Detection System.
   Fields:
   [timestamp] [Source ip address.port] > [de stination ip address.port]:[IP flags]

[sequence number] [window size]

3. Probability the source address was spoofed
   Low. The communication actually starts to take place.
4. Description of attack:
   I don't think you could really call this an attack. It l ooks more like load balancing to me.
5. Attack Mechanism:
   This same pattern of events happened approximately every 45 minutes for at least a week. This just seems to be an attempt by rivalcom.net to do load balancing to our site. They want to provide th e fastest connection during different parts of the day.
6. Correlations:
   Stephen Northcutt did talk about some ISP's doing load balancing efforts in class. There is a little bit mentioned in manual 2.5 on page 322.
7. Evidence of Active Targeting:
   This is very specific since it only hits the DNS server.
8. Severity:
   (Critical + Lethal) - (System + Net Countermeasures) = Severity
   (5 + 1) - (4 + 2) = 0
9. Defensive recommendation:
   I think this is one of those instances where you just have to live with it until they decide they have done enough load balancing and stop. I did write to them asking what they were doing, but have heard nothing back.
10. Multiple choice question:
    If this trace happened consistently it could be an example of what?
    A) A buffer overflow on the DNS server
    B) A failed DNS zone transfer
    C) DNS load balancing
    D) A scan for DNS servers
    Answer: C

Detect 6:

Trace:

```
18:47:42.833004 attacker.somewhere.net.56498 > target.somewhere.com.echo: S
3714019486:3714019486(0) win 4096
18:47:42.833385 target.somewhere.com.echo > attacker.somewhere.net.56498: S
3449196742:3449196742(0) ack 3714019487 win 8855 (DF)
18:47:42.894483 attacker.somewhere.net.56500 > target.somewhere.com.echo: SFP
3714019486:3714019486(0) win 4096 urg 0
18:47:42.954265 attacker.somewhere.net.56502 > target.somewhere.com.tcpmux: S
3714019486:3714019486(0) win 4096
18:47:42.954502 target.somewhere.com.tcpmux > attacker.somewhere.net.56502: R 0:0(0)
ack 3714019487 win 0 (DF)
18:47:46.325531 target.somewhere.com .echo > attacker.somewhere.net.56498: S
3449196742:3449196742(0) ack 3714019487 win 8855 (DF)
18:47:52.326171 target.somewhere.com.echo > attacker.somewhere.net.56498: S
3449196742:3449196742(0) ack 3714019487 win 8855 (DF)
18:47:52.417523 attacker.somew here.net.56498 > target.somewhere.com.echo: S
3714019486:3714019486(0) win 4096
18:47:52.417957 target.somewhere.com.echo > attacker.somewhere.net.56498: . ack
```

3714019487 win 8855 (DF)
18:47:52.440906 attacker.somewhere.net.56500 > target.somewhere.com.e cho: SFP
3714019486:3714019486(0) win 4096 urg 0
18:47:52.462459 attacker.somewhere.net.56502 > target.somewhere.com.tcpmux: S
3714019486:3714019486(0) win 4096
18:47:52.462731 target.somewhere.com.tcpmux > attacker.somewhere.net.56502: R 0:0(0)
ack 3714019487 win 0 (DF)
18:48:04.327287 target.somewhere.com.echo > attacker.somewhere.net.56498: S
3449196742:3449196742(0) ack 3714019487 win 8855 (DF)
18:48:15.228844 gatekeeper.uccu.com.ftp > attacker.somewhere.net.56498: S
4248573367:4248573367(0) ack 3364 554775 win 8215
18:48:28.329612 target.somewhere.com.echo > attacker.somewhere.net.56498: S
3449196742:3449196742(0) ack 3714019487 win 8855 (DF)
18:49:16.335018 target.somewhere.com.echo > attacker.somewhere.net.56498: S
3449196742:3449196742(0) ack 371 4019487 win 8855 (DF)

1. Source of Trace:
   My network test area
2. Detect was generated by:
   Shadow Intrusion Detection System using tcpdump
   Fields:
   [timestamp] [Source ip address.port] > [destination ip address.port]:[IP flags] [sequence number] [window size]
3. Probability the source address was spoofed:
   Low. This is reconnaissance and the information needs to get back to the attacker.
4. Description of attack:
   This is nmap doing a scan for hosts with os fingerprinting.
5. Attack mechanism:
   I wanted to see what the "normal" traffic for nmap was when it had the os fingerprinting option set. This is nmap version 2.53 with the -sS and -O options in the command line. This will scan for hosts in a range and then try and find out what their operating system is. I ran this against our live systems and nmap was about 90% correct with its guesses. That gives a lot of information to an attacker.
6. Correlations:
   Hal Pomeranz talked about nmap in his class at SNAP 2000 in San Jose. See manual 2.2 pages 172 - 176.
7. Evidence of active targeting:
   Since this was general reconnaissance it was looking at network mapping and not a one specific host.
8. Severity:
   (Critical + Lethal) - (System + Net Countermeasures) = Severity
   (5 + 1) - (4 + 2) = 0
9. Defensive recommendation:
   There isn't much that you can do to stop network scanning, just make sure you have the latest patches to your OS and software.
10. Multiple choice test question:
    nmap is used for which purpose:
    A) Port scanning a specific host
    B) Doing a general network scan for hosts
    C) Mapping out a network

D) All of the above

Answer: D

Detect 7:

Trace:

14:53:26.966897 216.133.4.7.4711 > xx.xx.xx.2.domain: S 1461821194:1461821194(0) win 32120 (DF)
14:53:26.967497 xx.xx.xx.2.domain > 21 6.133.4.7.4711: S 2131701393:2131701393(0) ack 1461821195 win 8576
14:53:26.968521 216.133.4.7.4712 > xx.xx.xx.3.domain: S 1458779852:1458779852(0) win 32120 (DF)
14:53:26.968930 xx.xx.xx.3.domain > 216.133.4.7.4712: S 1324069908:1324069908(0) ack 1458779853 win 10136 (DF)
14:53:26.970535 216.133.4.7.4715 > xx.xx.xx.6.domain: S 1448710281:1448710281(0) win 32120 (DF)
14:53:29.851518 216.133.4.7.4714 > xx.xx.xx.5.domain: S 1460896640:1460896640(0) win 32120 (DF)

1. Source of Trace:
   My network
2. Detect was generated by:
   Shadow Intrusion Detection System using tcpdump
   Fields:
   [timestamp] [Source ip address.port] > [destination ip address.port]:[IP flags] [sequence number] [window size]
3. Probability the source address was spoofed:
   Low. It looks like they are doing reconnaissance so they will want their findings back.
4. Description of attack:
   Scanning for DNS servers
5. Attack Mechanism:
   They are sending the start of the 3 -way handshake and waiting for a response from the servers that are listening on port 53.
6. Correlations:
   Scanning was talked about in the SNAP 2000 conference in San Jose by Vicki Irwin. See Manual 2.2 pages 110 - 123. This section deals with different types of scans.
7. Evidences of Active targeting:
   This is a general scan and is not looking at one specific host, but at all DNS servers in general.
8. Severity
   (Critical + Lethal) - (System + Net Countermeasures) = Severity
   (5 + 1) - (5 + 2) = -1
9. Defensive recommendations:
   You could block all traffic for your internal DNS server at the router. On the outside you pretty much have to have that opened for people to use your internet servers.
10. Multiple choice question:
    This trace is an example of
    A) A scan for DNS servers
    B) Scanning for Web Servers
    C) Scanning for Mail servers

D) A zone transfer

Answer: A

Detect 8:

Trace:

09:56:20.703287 63.226.100.102.17036 > xx.xx.xx.2.31337: S 134106359:134106359(0) win 8192 (DF)
09:56:20.703797 xx.xx.xx.2.31337 > 63.226.100.102.17036: R 0:0(0) ack 134106360 win 0
09:56:21.302879 63.226.100.102.17036 > xx.xx.xx.2.31337: S 134106359:134106359(0) win 8192 (DF)
09:56:21.303381 xx.xx.xx.2.31337 > 63.226.100.102.17036: R 0:0(0) ack 134106360 win 0
09:56:21.902189 63.226.100.102.17036 > xx.xx.xx.2.31337: S 134106359:134106 359(0) win 8192 (DF)
09:56:21.902711 xx.xx.xx.2.31337 > 63.226.100.102.17036: R 0:0(0) ack 134106360 win 0
09:56:22.502404 63.226.100.102.17036 > xx.xx.xx.2.31337: S 134106359:134106359(0) win 8192 (DF)
09:56:22.502926 xx.xx.xx.2.31337 > 63.226.100.102.1 7036: R 0:0(0) ack 134106360 win 0

1. Source of the trace
   My network
2. Detect was generated by:
   Shadow Intrusion Detection System using tcpdump
   Fields:
   [timestamp] [Source ip address.port] > [destination ip address.port]:[IP flags] [sequence number] [window size]
3. Probability the source address was spoofed:
   Medium. It is possible that this was coming from somewhere else, but I would think that it is more along the reconnaissance line and that they would want the information back.
4. Description of attack:
   It looks like they are probing for a Trojan or Back Orifice 2000.
5. Attack mechanism:
   They are starting the handshake to port 31337 which is usually tied to Back Orifice. The problem is that the older version of Back Orifice used UDP and not TCP. This could be someone who is using Bo2k and just liked that port number. The host responds with a reset because it is not listening on that port.
6. Correlations:
   Back Orifice is talked about in Manual 2.2 pages 100 -104 of the SNAP2000 conference in San Jose.
7. Evidence of Active targeting:
   This is definitely active targeting. They are only focusing on one host.
8. Severity:
   (Critical + Lethal) - (System + Net Countermeasures) = Severity
   (5 + 1) - (3 + 5) = -2
9. Defensive recommendations:
   This attack failed, so the defenses are adequate.
10. Multiple Choice question
    The original Back Orifice program used which protocol?

A) TCP
B) ICMP
C) UDP
D) None of the above

Answer: C

Detect 9:

Trace:
May 20 07:51:34 cc1014244 -a kernel: securityalert: udp if=ef0 from 24.2.228.223:137 to 24.3.21.199 on unserved port 137
May 20 11:09:52 cc1014244 -a kernel: securityalert: tcp if=ef0 from 24.3.246.148:3132 to 24.3.21.199 on unserved port 27374
May 20 12:34:55 cc1014244 -a kernel: securityalert: tc p if=ef0 from 63.20.64.221:2570 to 24.3.21.199 on unserved port 27374
May 20 15:11:51 cc1014244 -a kernel: securityalert: udp if=ef0 from 24.9.224.123:137 to 24.3.21.199 on unserved port 137

1. Source of Trace:
   http://www.sans.org/y2k/052400 -1300.htm
2. Detect was generated by:
   It looks like this detect was made by a firewall. It resembles a Gauntlet firewall log readout.
   Fields:
   [Timestamp] [reporting program]:[type of alert]:[protocol]if=[Network interface] from [source ip address:port] to [destination address] on unserved port [destination port number]
3. Probability the source address was spoofed:
   Low. This is another form of reconnaissance and the attacker will want the information back.
4. Description of attack:
   Trying to attach to port 137 to see if the host is a windows machine.
5. Attack mechanism:
   Basically you attach to the port and if it does allow you then you know it is most likely a windows type machine. Then you can see if there a re any shares available on the machine to exploit, or, you can try a number of different ways to compromise the machine.
6. Correlations:
   Stephen Northcutt talked about NetBios in the SNAP2000 conference in San Jose. See Manual 2.5 page 210.
7. Evidence of Active targeting:
   This looks like they are trying this specific machine.
8. Severity:
   (Critical + Lethal) - (System + Net Countermeasures) = Severity
   (5 + 1) - (5 + 5) = -4
9. Defensive recommendations:
   None, the Defenses held up just fine.
10. Multiple choice question:
    Netbios is usually equated with which operating system?
    A) Windows 95

B) Windows NT workstation
C) Windows NT Server
D) All of the above

Answer: D

Detect 10:

Trace:
03:58:15.235672 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:15.239141 phwww.netcast.nl.2356 > 204.x.x.0.echo: udp 1024
03:58:15.368527 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:15.371826 phwww.netcast.nl.41056 > 204.17.222.255.echo: udp 1024
03:58:17.902494 phwww.netcast.nl > 20 4.x.x.0: icmp: echo request
03:58:17.906341 phwww.netcast.nl.3471 > 204.x.x.0.echo: udp 1024
03:58:18.035617 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:18.039447 phwww.netcast.nl.2933 > 204.17.222.255.echo: udp 1024
03:58:19.870268 phwww.n etcast.nl > 204.x.x.0: icmp: echo request
03:58:19.874172 phwww.netcast.nl.42557 > 204.x.x.0.echo: udp 1024
03:58:20.003372 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:20.007210 phwww.netcast.nl.21668 > 204.17.222.255.echo: udp 1024
03:58:21.896327 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:22.028786 phwww.netcast.nl.11873 > 204.x.x.0.echo: udp 1024
03:58:22.030896 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:22.162075 phwww.netcast.nl.54301 > 204.17.222.255.echo: udp 1024
03:58:23.432190 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:23.435480 phwww.netcast.nl.23701 > 204.x.x.0.echo: udp 1024
03:58:23.608424 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:23.611678 phwww.netcast.nl.11568 > 204.1 7.222.255.echo: udp 1024
03:58:24.833797 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:24.837642 phwww.netcast.nl.7792 > 204.x.x.0.echo: udp 1024
03:58:24.966905 phwww.netcast.nl > 204.x.x.255: icmp: echo request

1. Source of Trace:
   http://www.sans.org/y2k/052000.htm
2. Detect was generated by:
   Probably tcpdump
   Fields:
   [timestamp] [Source ip address.port] > [destination ip address.port]:[IP flags] [sequence number] [window size]
3. Probability the source address was spoofed:
   High. Usually with DOS attacks they don't want to be linked with the packet in any way.
4. Description of attack:
   Send a lot of ping traffic to the host and it will overwhelm it and shut it down.
5. Attack Mechanism:
   It looks like this attacker is just hoping that by sending these packets that these two machines will get in an echo war. Whatever one machine sends it will send back to the other machine. Since it is probably a spoofed address the two machines will just keep sending it back and forth. This will suck up the CPU and network bandwidth

and effectively shut everything down.

6. Correlation:
   This attack looks like it is a spin off of one that was discussed in the SNAP2000 conference. Page 257 of the 2.5 manual.
7. Evidence of Active targeting:
   This is very specific. Both machines had to have been picked out by the attacker.
8. Severity:
   (Critical + Lethal) - (System + Net Countermeasures) = Severity
   (5 + 4) - (5 + 2) = 2
9. Defensive recommendations:
   There is no real use for the echo or the chargen ports. The traffic to them should be blocked out at the router.
10. Multiple choice question:
    This trace is an example of what?
    A) Ping request and reply
    B) Back Orifice in action
    C) DOS attack
    D) None of the above
    Answer: C