Intrusion Detection In Depth

GCIA Practical Assignment

Version 2.9

Janice Y. Slocumb

SANS Baltimore 2001

May 13 – May 20, 2001
Table of Contents

Assignment 1 – Detects ...........................................................................................................................................3
    Analysis 1 – SYN Flood Denial Of Service Attack ................................................................. 3
    Analysis 2 – Anomalous Traffic .............................................................................................10
    Analysis 3 - Attempted Intrusion of Mail Server ...............................................................15
    Analysis 4 – ICQ Webfront Denial of Service .................................................................20
    Analysis 5 - Buffer Overflow ............................................................................................24
Assignment 2 – White Paper .........................................................................................................................28
Assignment 3 – Analyze This ......................................................................................................................35
    Executive Summary ..................................................................................................................35
    Detailed Analysis ....................................................................................................................36
Assignment 4 – Analysis Process ...........................................................................................................101
References ..................................................................................................................................................103
Assignment 1 -- Detects

Network Trace Analysis Section

Analysis # 1: SYN Flood Denial Of Service Attack

This data was captured on March 20, 2001 and covers the entire 24-hour period. This traffic is the result of a third-party effect. The data was run through TCPDUMP filtering the data to select only traffic involving host victim.host.cn. I have removed several of the records for the sake of brevity. Also, the source and destination IP addresses have been sanitized to protect the identity of the networks involved. The TCPDUMP data used for this analysis was generated by TCPDUMP version 3.4 with LIBPCAP version 0.4.

```
[hostname]# gunzip –c raw.tcpdump.file.gz |tcpdump –r -nv host victim.host.cn
```

```
00:00:05.325495 victim.host.cn.19713 > CCC.DDD.66.50.26477: R 0:0(0) ack 357306772 win 0
00:00:05.851129 victim.host.cn.62401 > CCC.DDD.92.61.25897: R 0:0(0) ack 1586197602 win 0
00:00:13.862514 victim.host.cn.18688 > AAA.BBB.178.112.10721: R 0:0(0) ack 282119840 win 0
00:00:15.734722 victim.host.cn.26716 > AAA.BBB.239.62.59408: R 0:0(0) ack 1922412476 win 0
…………..
00:00:05.325495 victim.host.cn.19713 > CCC.DDD.66.50.26477: R 0:0(0) ack 357306772 win 0
00:00:05.851129 victim.host.cn.62401 > CCC.DDD.92.61.25897: R 0:0(0) ack 1586197602 win 0
00:00:13.862514 victim.host.cn.18688 > AAA.BBB.178.112.10721: R 0:0(0) ack 282119840 win 0
00:00:15.734722 victim.host.cn.26716 > AAA.BBB.239.62.59408: R 0:0(0) ack 1922412476 win 0
…………..
00:01:00.753200 victim.host.cn.60548 > AAA.BBB.116.116.36724: R 0:0(0) ack 1253424384 win 0
00:01:05.021322 victim.host.cn.19214 > EEE.FFF.244.228.22705: R 0:0(0) ack 626599357 win 0
00:01:08.388103 victim.host.cn.62401 > CCC.DDD.156.189.27305: R 0:0(0) ack 287514210 win 0
…………..
00:02:05.619106 victim.host.cn.26774 > CCC.DDD.183.250.30085: R 0:0(0) ack 829011917 win 0
00:02:14.554244 victim.host.cn.42214 > AAA.BBB.84.195.45931: R 0:0(0) ack 1073833603 win 0
…………..
00:03:00.357609 victim.host.cn.25697 > AAA.BBB.51.7.40504: R 0:0(0) ack 1727698954 win 0
00:03:01.407003 victim.host.cn.50006 > AAA.BBB.183.188.9594: R 0:0(0) ack 1 win 0
00:03:07.953575 victim.host.cn.37952 > AAA.BBB.149.149.48845: R 0:0(0) ack 108292992 win 0
…………..
00:04:02.411061 victim.host.cn.41772 > AAA.BBB.104.139.41364: R 0:0(0) ack 1273292517 win 0
00:04:08.837816 victim.host.cn.36687 > CCC.DDD.195.115.28655: R 0:0(0) ack 963576653 win 0
…………..
00:05:10.972132 victim.host.cn.30827 > CCC.DDD.23.66.23019: R 0:0(0) ack 1407766767 win 0
00:05:13.053044 victim.host.cn.46217 > AAA.BBB.109.39.47773: R 0:0(0) ack 1392838048 win 0
…………..
01:00:00.356280 victim.host.cn.56930 > AAA.BBB.76.25.63384: R 0:0(0) ack 899064475 win 0
01:00:00.426227 victim.host.cn.57983 > GGG.HHH.111.222.53302: R 0:0(0) ack 752413067 win 0
01:00:04.174352 victim.host.cn.44080 > CCC.DDD.248.11.54382: R 0:0(0) ack 99130774 win 0
01:00:06.455800 victim.host.cn.13335 > CCC.DDD.178.98.58355: R 0:0(0) ack 1817842886 win 0
01:02:13.263338 victim.host.cn.51975 > CCC.DDD.237.81.57875: R 0:0(0) ack 1750046609 win 0
01:02:26.444701 victim.host.cn.16972 > AAA.BBB.116.166.62904: R 0:0(0) ack 1893948423 win 0
01:02:26.816313 victim.host.cn.3510 > AAA.BBB.3.242.40891: R 0:0(0) ack 1524783358 win 0
01:02:27.904057 victim.host.cn.15962 > AAA.BBB.86.247.27588: R 0:0(0) ack 1817261562 win 0
01:04:59.593073 victim.host.cn.10464 > AAA.BBB.123.21.4205: R 0:0(0) ack 832170616 win 0
01:04:59.880870 victim.host.cn.50406 > AAA.BBB.236.172.17585: R 0:0(0) ack 240691700 win 0
01:04:59.914503 victim.host.cn.61732 > AAA.BBB.82.119.29422: R 0:0(0) ack 1867708312 win 0
01:04:59.994769 victim.host.cn.11127 > CCC.DDD.84.29.64269: R 0:0(0) ack 1018786354 win 0
01:04:59.913332 victim.host.cn.11851 > CCC.DDD.84.29.64269: R 0:0(0) ack 1589928351 win 0
01:06:26.289329 victim.host.cn.46188 > CCC.DDD.152.108.35864: R 0:0(0) ack 1482632657 win 0
01:06:30.229635 victim.host.cn.2189 > CCC.DDD.113.174.33753: R 0:0(0) ack 1909867999 win 0
01:06:31.468289 victim.host.cn.50609 > AAA.BBB.163.224.43036: R 0:0(0) ack 147706525 win 0
01:06:32.785544 victim.host.cn.50178 > CCC.DDD.33.17.45895: R 0:0(0) ack 439205749 win 0
01:06:40.545441 victim.host.cn.39504 > AAA.BBB.173.207.39593: R 0:0(0) ack 657203863 win 0
03:12:06.598617 victim.host.cn.50178 > CCC.DDD.33.81.33671: R 0:0(0) ack 930100661 win 0
03:12:09.372545 victim.host.cn.8992 > AAA.BBB.179.231.39733: R 0:0(0) ack 643403437 win 0
03:12:09.480322 victim.host.cn.51858 > AAA.BBB.4.128.16154: R 0:0(0) ack 1536003191 win 0
04:13:46.066229 victim.host.cn.10908 > AAA.BBB.201.112.1963: R 0:0(0) ack 2339268937 win 0
04:13:47.286671 victim.host.cn.5191 > AAA.BBB.173.132.7113: R 0:0(0) ack 1030938308 win 0
04:13:50.136495 victim.host.cn.57372 > CCC.DDD.132.6.31033: R 0:0(0) ack 17499983189 win 0
04:13:51.719852 victim.host.cn.19545 > CCC.DDD.249.6.62800: R 0:0(0) ack 1987999831 win 0
04:13:56.880441 victim.host.cn.39098 > CCC.DDD.112.109.28158: R 0:0(0) ack 1486823943 win 0
08:12:10.997507 victim.host.cn.7019 > AAA.BBB.92.254.17658: R 0:0(0) ack 1415199347 win 0
08:12:13.733272 victim.host.cn.3041 > AAA.BBB.80.116.35758: R 0:0(0) ack 183031388 win 0
Janice Y. Slocumb

GCIA Practical Assignment Version 2.9

08:12:14.254762 victim.host.cn.10617 > CCC.DDD.50.63.33879: R 0:0(0) ack 77120912 win 0

………………

22:56:35.643333 victim.host.cn.30388 > CCC.DDD.119.68.36761: R 0:0(0) ack 1813517330 win 0
22:56:35.734460 victim.host.cn.35200 > CCC.DDD.50.124.11161: R 0:0(0) ack 1773167938 win 0
22:56:36.102244 victim.host.cn.7019 > AAA.BBB.220.126.50554: R 0:0(0) ack 395057139 win 0
22:56:38.557208 victim.host.cn.44643 > AAA.BBB.222.190.39866: R 0:0(0) ack 1 win 0
22:56:39.242390 victim.host.cn.63269 > CCC.DDD.177.39.4137: R 0:0(0) ack 1947117272 win 0

………..

23:00:08.357919 victim.host.cn.2350 > CCC.DDD.73.217.31491: R 0:0(0) ack 724731909 win 0
23:00:11.232469 victim.host.cn.45214 > CCC.DDD.188.226.10278: R 0:0(0) ack 329880662 win 0
23:00:12.866921 victim.host.cn.43964 > AAA.BBB.195.106.3481: R 0:0(0) ack 207366747 win 0

………..

23:58:26.186701 victim.host.cn.10464 > AAA.BBB.123.21.2157: R 0:0(0) ack 1623541880 win 0
23:58:26.642481 victim.host.cn.29263 > CCC.DDD.109.131.44953: R 0:0(0) ack 1588985544 win 0
23:58:27.323237 victim.host.cn.31090 > CCC.DDD.18.109.17148: R 0:0(0) ack 1244601211 win 0

………..

23:59:54.506025 victim.host.cn.60373 > CCC.DDD.192.184.43161: R 0:0(0) ack 733593374 win 0

1. Source of Trace:
This trace data came from a network that I monitor as a part of my professional duties as a Network Security Analyst.

2. Detect was generated by:
The attack was detected using Shadow, the IDS system written by the Naval Surface Warfare Center (NSWC). It can be downloaded at no cost from http://nswc.navy.mil/ISSEC/CID. This detect was triggered because victim.host.cn sent several hundred packets to multiple hosts in our network within a 1 hour period. Shadow has been configured to list all hosts with IP addresses outside of our security domain which make excessive one-to-many connections during 1 hour. The TCPDUMP utility with a specific host filter was used against 24 hours of data captured by Shadow to gather additional information.

3. Probability the source address was spoofed:
The probability that the source address shown in this trace is spoofed is very unlikely. However, keep in mind this is the address of the victim of the attack not the perpetrator. The reset packets directed at our network are coming from the victim to us. The fact that the inbound traffic are RST-ACK packets further verifies that our addresses were spoofed in the original attack.

4. Description of the Attack
The data in this trace indicates a SYN flood denial of service (DoS) attack was launched against victim.host.cn using spoofed address from several of our networks. Each of our spoofed addresses was used to send several packets to the victim. This raises the issue that the hostile party has done some prior reconnaissance of our address space and collected a list of valid IP addresses which he is now using to attack another host. The traffic was dispersed such that the resulting reset packets had no negative impact on the hosts on our network; however this does suggest that our addresses were interleaved with addresses from other networks to launch the attack against victim.com.cn.

The use of spoofed addresses in this type of attack is common because the perpetrator is not interested in receiving the packet responses. DoS attacks are used to adversely affect system availability by abusing network resources such as bandwidth and system resources such as memory and processing cycles sometimes leading to system crashes. Disruptions of this type can cause major problems to organizations that rely on the availability of their systems to support mission critical processes.

5. Attack mechanism:
The goal of DoS attacks are to deny something from users or other machines/processes. This type of attack can be accomplished several ways. In this particular instance, SYN packets were directed at the victim looking for high numbered TCP ports. The destination ports were not available on the victim host; thus causing the generation of thousands of RST-ACK packets. TCP is a connection oriented protocol. It uses a mechanism called the 3-way handshake to establish sessions between hosts. During normal session establishment a SYN packet flows from the client to the server. The source port of the client is an ephemeral port and the destination port on the server is one of the well known TCP/IP service ports that is “listening” on the server machine. The server then places the connection in SYN_RECV state and sends a SYN/ACK packet back to the client. The client responds with an ACK packet and the connection is established (see diagram1).

SYN floods are used to prevent the victim from responding to legitimate session requests by overwhelming it with large volumes of mutant packets. Since TCP is a stateful protocol, system memory is required to track the status of each connection. When the victim is flooded with incomplete connections its memory is depleted leaving none for handling other processes.¹ There are several ways to interrupt the normal connection establishment data flow. The method used in this attack was as follows. The hostile host originating the attack crafted several thousand SYN packets with spoofed source IP addresses and directed them to high numbered TCP ports that were not “listening” on victim.host.cn. The victim machine responded with reset packets directed at the spoofed IP addresses (see diagram 2). The source of the stimulus is unknown and was not captured in the trace.

The SYN flood attack has been around for a long time, in fact it was one of the exploits Kevin Mitnick used in his famous Mitnick Attack. (A very good explanation of his attack is included in “Network Intrusion Detection An Analyst’s Handbook 2nd Edition”).

¹ Intrusion Signatures and Analysis
A very good write-up describing SYN flooding can be found on the Internet at http://www.niksula.cs.hut.fi/~dforsber/synflood/result.html.

6. Correlations:
This traffic was not captured by any other tool because it consisted of single reset packets directed at valid IP addresses and the source host was not filtered at the network perimeter by the router ACL. An informative explanation of DoS attacks is documented in chapter 11 of “Hacking Exposed Network Security Secrets and Solutions” by Stuart McClure, Joel Scambray, and George Kurtz.

7. Evidence of active targeting:
This was a targeted attack; however it was not targeted at us. The intended target was victim.host.cn. The traffic we saw on our network was the result of the spoofing of our IP addresses.

8. Severity:
(Criticality + Lethality) – (System Countermeasure + Network Countermeasures)
(1 +1) – (1+1) = 0
Criticality = 1 (No critical systems in our network were affected by the attack)
Lethality = 1 (There was no adverse effect on the hosts owning the spoofed addresses)
System Countermeasure = 1 (No host countermeasures were in place to prevent this type of attack)
Network Countermeasure = 1 (No network filters were in place to block this activity from entering our network)

9. Defensive recommendations:
Our network:
• If the volume of traffic is such that it has the potential to negatively impact our network block inbound traffic from victim.host.cn
Victim network:
• Adjust the timeout value for the maximum number of incomplete connections on the firewall. (This may not have helped in this case because the stream of traffic was constant for 24 hours.)
Victim host:
• Depending on which venders IP stack is used, consider increasing the size of the connection queue allowing the system administrator more time to respond to an attack by blocking the flow of inbound traffic at the network perimeter. This approach will affect the system performance; however, it may prevent a total system lockout.
• Disable all unnecessary services.
• Ensure all patches are current.

10. Multiple choice test question:
How can you identify the originating IP of a SYN flood attack when spoofed source addresses are used?
A. View router logs for the perimeter gateway looking for incoming traffic.
B. Use TCPDUMP output filtering for the source IP.
C. The originating IP cannot be determined.

The correct answer is C. The IP of the hostile machine that originated the attack can’t be determined because the IP header has been crafted replacing the actual source IP with a spoofed address in the packets directed at the victim and the source IP address in the resulting reset packets are that of the victim.
SYN Flood Attack

Diagram 2
Analysis 2 – Anomalous Traffic

I received this log of interesting traffic from an outside source requesting any insight I might have on what’s happening. Here is the story, about once a month he sees numerous IP addresses that do SYN packets. The source and destination ports are normally high. They hit one IP address and leave. The activity usually only lasts one hour. If the source addresses are spoofed IP’s, sending one packet to different systems does not accomplish anything. To many to be ‘wrong addresses’. The IP addresses are foreign and domestic and some IANA Reserve. Can't be network mapping because any returns would go to the real IP address holder.

```
14:33:15.249635 3.148.231.60.42711 > CCC.DDD.166.62.64656: S 1526567552:1
526567552(0) win 1024
14:32:11.080174 7.14.211.44.29428 > XXX.YY.62.37.35462: S 204837356:204837356(0) win 1024
14:35:33.213144 22.30.155.83.28283 > XXX.YY.101.8.6913: S 1095217197:1095217197(0) win 1024
14:32:56.010195 16.59.125.32.59249 > XXX.YY.37.28.55377: S 1861900171:1861900171(0) win 1024
14:34:13.934264 8.190.221.14.16226 > AAA.BBB.90.49.57588: S 256851244:256851244(0) win 1024
14:35:27.896478 32.73.129.10.773 > AAA.BBB.175.19.9735: S 161589680:161589680(0) win 1024
14:33:46.922766 38.106.51.20.13027 > XXX.YY.67.109.41670: S 1371042277:1371042277(0) win 1024
14:33:07.819816 41.119.199.23.29727 > XXX.YY.94.83.59235: S 1317679216:1317679216(0) win 1024
14:34:21.570973 35.147.238.7.47388 > XXX.YY.61.113.16841: S 1575498373:1575498373(0) win 1024
14:33:44.417406 34.168.52.11.18309 > XXX.YY.175.70.4707: S 1151188750:1151188750(0) win 1024
14:34:40.727891 49.125.4.53.33872 > XXX.YY.237.92.53910: S 1460596383:1460596383(0) win 1024
```

© SANS Institute 2000 - 2002, Author retains full rights.

Janice Y. Slocumb
GCIA Practical Assignment Version 2.9
When he viewed the trace into hex here is what he found. He was concerned because there appeared to be 6 bytes of data included in the datagram.

Packet 1

IP Header

Version: 4
Header Length: 20 bytes
Service Type: 0x00

Datagram Length: 40 bytes
Identification: 0x3825
Flags: MF=off, DF=off
Fragment Offset: 0
TTL: 59
Encapsulated Protocol: TCP
Header Checksum: 0x8B1A
Source IP Address: 7.14.211.44
Destination IP Address: XXX.YY.62.37

TCP Header

Source Port: 29428 (<unknown>)
Destination Port: 35462 (<unknown>)
Sequence Number: 0204837356
Acknowledgement Number: 1249317570
Header Length: 20 bytes (data=0)
Flags: URG=off, ACK=off, PSH=off, RST=off, SYN=on, FIN=off
Window Advertisement: 1024 bytes
Checksum: 0xF67B
Urgent Pointer: 0

TCP Data
<No data>

I decoded the packet using a TCP header layout template to see what was happening.

14:32:11.080174 0:e0:fe:7c:30:a0 0:10:7:17:38:c0 0800 60: 7.14.211.44.29428 >
XXX.YY.62.37.35462: S 204837356:204837356(0) win 1024
4500 0028 3825 0000 3b06 8b1a 070e d32c
a431 3e25 72f4 8a86 0c35 91ec 4a77 12c2
5002 0400 f67b 0000 0011 0000 0600
TCP Header:

<table>
<thead>
<tr>
<th>Src port</th>
<th>Dst port</th>
<th>Seq. #</th>
<th>Ack #</th>
<th>Hdr Len</th>
<th>Flags</th>
<th>Window size</th>
<th>Checksum</th>
<th>Urg Ptr</th>
<th>Options</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>72F4</td>
<td>8A86</td>
<td>0C35</td>
<td>4A77</td>
<td>5</td>
<td>00</td>
<td>0400</td>
<td>F67B</td>
<td>0000</td>
<td>0011</td>
<td>0000 0600</td>
</tr>
</tbody>
</table>

1. **Source of Trace:**
   This trace data was provided to me by an analyst of a network outside of my organization.

2. **Detect was generated by:**
   The detect was done using TCPDUMP. The detailed breakdown of the packet was done using a packet analyzer such as Net-Xray to dump the content of the packet including the payload that was captured.

3. **Probability the source address was spoofed:**
   I agree with my analyst friend, it is highly unlikely that the source addresses are spoofed. If they are sending one packet to different systems on different subnets does not accomplish anything.

4. **Description of the Attack:**
   There is no clear indication that this data represents an attack. The desired mission of this analysis is to determine if an attack is occurring.

5. **Attack mechanism:**
   It appears that data has been included in the initial SYN packet though it is not indicated in the TCPDUMP output. Detailed analysis of the hexadecimal breakdown of one of the packets raises some questions.

   - The datagram length field in the IP header denotes a total datagram length of 40 bytes indicating that no data is present. In actuality the datagram is 46 bytes long. What are the extra 6 bytes intended for?

   - Could they be garbled TCP options? 
     No, the TCP header length is 0x5 which is 20 bytes the default TCP header length.

   - Could this be data destined for an application? If so, what does it mean? 
     The TCP header analysis indicates that there is no data included.

       ASCII conversion of extra 6 bytes:
       NUL VT NUL NUL ACK NUL
       00 11 00 00 06 00
6. Correlations:
I began looking at the Ethernet header for clues as to what was going on. The type field contains 0800 indicating that the traffic is IP over Ethemet. Ethernet frames over IP have a minimum size restriction of 46 bytes. When necessary, the data field should be padded (with octets of zero) to meet the IEEE 802 minimum frame size requirements. This padding is not part of the IP datagram and is not included in the total length field of the IP header.2

This explains the extra 6 bytes of data not accounted for in the total length field; however, it does not explain why the extra 6 bytes are not all zeros. This could be the result of a flaw in building of the IP datagram at the source host. Of course, the truly paranoid might think this is an attempt to use a covert channel to the destination host.

7. Evidence of active targeting:
I imported the TCPDUMP output into Microsoft Excel and sorted it by source and destination IPs and there was no pattern to the packets. The traffic doesn’t appear to be targeted at any particular host or network.

8. Severity:
(Criticality + Lethality) – (System Countermeasure + Network Countermeasures) 
(1 +1) – (1+1) = 0
Criticality = 1 (No critical systems in our network were affected by the attack) 
Lethality = 1 (There was no adverse affect on the destination hosts)
System Countermeasure = 1 (No host countermeasures were in place to prevent this type of attack)
Network Countermeasure = 1 ( No network filters were in place to block this activity from entering our network)

9. Defensive recommendations:
• Disable all unnecessary services on host in the network.
• Ensure all patches are current.

10. Multiple choice test question:
Under what circumstances is it allowable to send data in an initial SYN packet?

A. When using T/TCP for client/server applications.
B. When the ACK flag is set to 0.
C. When the FIN flag is on.
D. Never

The correct answer is B. Data can be sent with an initial SYN packet as long as the ACK flag is not set. Setting the ACK flag would indicate that prior packets had been received. The data is saved at the receiving host and forwarded to the application at the completion of the 3-way handshake.

2 TCP/IP Illustrated Vol 1
Analysis 3 - Attempted Intrusion of Mail Server

A intruder attempted to gain unauthorized access to a mission critical server via a telnet session. The server involved was the organizations mail server. Unauthorized access to this server has the potential of taking down mail service to hundreds, if not thousands of users.

NID Connection Log Entries:

```
<table>
<thead>
<tr>
<th>telnet</th>
<th>index</th>
<th>warning</th>
<th>destination</th>
<th>source</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------</td>
<td>-----</td>
<td>-------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>1618</td>
<td>8.722</td>
<td>smtp.host.com</td>
<td>intruder.host.pl</td>
</tr>
<tr>
<td></td>
<td>1565</td>
<td>8.722</td>
<td>smtp.host.com</td>
<td>intruder.host.pl</td>
</tr>
</tbody>
</table>
```

TCPDUMP output:

```
13:54:32.080000 intruder.host.pl.1282 > smtp.host.com.23: S 2635135109:2635135109(0) win 8760 <mss 1460,nop,nop,sackOK> (DF) (ttl 112, id 7466) 
13:54:32.080000 smtp.host.com.23 > intruder.host.pl.1282: S 102400000:102400000(0) ack 2635135110 win 32768 <mss 1460> (DF) (ttl 62, id 50593) 
13:54:34.080000 smtp.host.com.23 > intruder.host.pl.1282: P 4:7(3) ack 4 win 32768 (DF) (ttl 62, id 50597) 
13:54:35.580000 smtp.host.com.23 > intruder.host.pl.1282: P 4:7(3) ack 4 win 32768 (DF) (ttl 62, id 50599) 
13:54:36.040000 smtp.host.com.23 > intruder.host.pl.1282: P 7:16(9) ack 10 win 32768 (DF) (ttl 62, id 50601) 
13:54:42.860000 smtp.host.com.23 > intruder.host.pl.1282: P 32:35(3) ack 32 win 32768 (DF) (ttl 62, id 50616) 
```
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:54:42.880000</td>
<td>smtp.host.com.23 &gt; intruder.host.pl.1282: P 529:734(205) ack 35 win 32768 (DF) (ttl 62, id 50619)</td>
</tr>
<tr>
<td>13:54:44.680000</td>
<td>intruder.host.pl.1282 &gt; smtp.host.com.23: P 35:38(3) ack 741 win 8020 (DF) (ttl 112, id 7479)</td>
</tr>
<tr>
<td>13:54:45.140000</td>
<td>smtp.host.com.23 &gt; intruder.host.pl.1282: P 741:744(3) ack 50 win 32765 (DF) (ttl 62, id 50630)</td>
</tr>
<tr>
<td>13:54:46.130000</td>
<td>intruder.host.pl.1282 &gt; smtp.host.com.23: P 53:56(3) ack 750 win 8011 (DF) (ttl 112, id 7483)</td>
</tr>
</tbody>
</table>
Janice Y. Slocumb  

GCIA Practical Assignment Version 2.9

1. Source of Trace:
This trace data came from a remote network monitored by our CERT team.

2. Detect was generated by:
The original detect was generated by **NID - Network Intrusion Detector v 2.2.1** which is developed and supported by Lawrence Livermore National Laboratory. You can find them on the web at http://www.llnl.gov.

- **NID** is made up of a suite of tools that collect, detect, and analyze network traffic
- Data is detected and collected based on criteria you specify in customization files.
  - Strings
  - TCP protocols (ports)
  - UDP protocols (ports)
  - Exceptions (traffic to ignore)
  - Trusted and untrusted hosts/servers
- **NID** is a passive detector so network users are unaware of its presence
- It requires no modification to the hosts that its monitoring
- As data is detected that matches the criteria you specified it's given assigned a "warning level" based on the protocol's capability and authentication required.
- For example telnet has a lot of capabilities but it also requires user authentication (password) to use.
- In contrast TFTP has high capability but the required authentication level is low.
- The mode of operation used to analyze this detect is call retrospective analysis.

**ANALYSIS TOOLS**

- **STREAM** - reads the raw data files and assembles all the packets associated with the session.
- **PLAYBACK** - displays the session streams.
- **Init side**
- **Dest side**
- **PACKET PRINT** - displays a portion of the packets displayed in the stream along with decoding the header information. ( -e and -ip options)

TCPDUMP was used to filter out the header packets associated with the source and destination machines and provide a synopsis of the dataflow between the two systems.
3. **Probability the source address was spoofed:**
The probability that the source address was spoofed is slim to nil because the hostile must receive the response packets to successfully carry out the attack.

4. **Description of the attack:**
Hostile attempted login using telnet service (23/tcp) on two separate attempts.

5. **Attack mechanism:**
The intruder probed a single host for the TCP telnet service (port 23). The victim responded and the 3-way handshake was complete. The intruder than attempted to gain unauthorized access to the target host using default userids.

6. **Correlations:**
The initial detect was triggered in NID. Further investigation using TCPDUMP and the appropriate filters confirmed the connections and the passage of data between the hostile machine and the victim.

   The telnet service is a common target of intruders because successful exploitation of this service can give the intruder root level authority on the target. At that point the target is susceptible to a wide variety of exploits, rootkits can be installed with trojanized processes, denial of service (DoS) attacks can be launched, and distributed denial of service tools (DdoS) installed for use in attacking other systems. There are literally hundreds of articles available on the Internet documenting the damage that can be done via a successful telnet exploit.

7. **Evidence of active targeting:**
This was a targeted attack. The hostile directed the activity only at smtp.host.com. This was the only traffic from the hostile machine for the day. This leads me to believe that prior reconnaissance had taken place.

8. **Severity:**
(Criticality + Lethality) – (System Countermeasure + Network Countermeasures)

   (5 + 2) – (3 + 1) = 3

   Criticality = 5 (A critical system in the network was targeted for the attack)
   Lethality = 2 (The attack was unsuccessful)
   System Countermeasure = 3 (Default accounts were not left vulnerable to prevent this type of attack)
   Network Countermeasure = 1 (No network filters were in place to block this activity from entering our network)

9. **Defensive recommendations:**
   - Institute a block at the perimeter gateway for the offending IP.
   - Disable all unnecessary services on smtp.host.com
   - Ensure all applicable current patches are installed on smtp.host.com
10. **Multiple choice question:**
What TCPDUMP option will display the time to live, packet id, and options field from the TCP header?

A. `–n`
B. `–e`
C. `–x`
D. `–vv`

The correct answer is D. the `–vv` (verbose) option will display these additional fields. The `–n` option will prevent the IP to hostname conversion; `–e` displays the link-level header on each dump line; `–x` dumps each packet, minus the link level header, in hex.
Analysis 4 – ICQ Webfront Denial of Service

ICQ ("I Seek You") is a user-friendly Internet program that notifies you when your friends and associates are online and enables you to contact them. With ICQ, you can chat, send messages and files, exchange Web page addresses, play games, etc. This is an analysis of DoS attack against the ICQ Webfront service which allows users to create homepages.

Snort Rule (1.6 Ruleset):
`alert tcp any any -> any 80 (msg:"MISC - ICQ Webfront HTTP DoS"; flags:PA; content:"??????????");`  

Snort Alert
[*] MISC - ICQ Webfront HTTP DoS [*]
03/27-00:11:00.071491 0:0:C:36:6F:AB -> 0:10:2F:A9:78:80 type:0x800 len:0x382
my.net.229.36:4954->victim.net.42.214:80 TCP TTL:126 TOS:0x0 ID:1684 DF
***AP*** Seq: 0x1738E59B Ack: 0xB3189E0D Win: 0x2058 [Snort log]

Snort Log Content
[*] MISC - ICQ Webfront HTTP DoS [*]
03/27-00:11:00.071532 0:0:C:36:6F:AB -> 0:10:2F:A9:78:80 type:0x800 len:0x382
my.net.229.36:4954->victim.net.42.214:80 TCP TTL:126 TOS:0x0 ID:1684 DF
***AP*** Seq: 0x1738E59B Ack: 0xB3189E0D Win: 0x2058
47 45 54 20 2F 73 63 72 69 70 74 73 2F 63 6D 73  GE
2F 43 4D 53 2E 41 53 50 3F 49 44 3D 35 38 39 30  /CMS.ASP?ID=5890
39 33 33 26 44 32 3D 61 62 4F 41 43 53 4B 73 3F 933&D2=abOACSKs?
3F 3F 3F 5F 40 3F 3F 2F 64 41 57 3D 31 36 37 26 4C  ???_??&AW=167&L
56 3D 32 34 35 26 4D 55 3D 39 38 35 36 35 32 V=2045&MU=985652
37 34 31 26 4C 43 3D 32 30 31 30 33 32 36 3A 741&LC=20010326:
31 26 43 46 3D 31 30 26 4E 50 3D 31 26 47 41 30 1&CF=10&NP=1&GA0
3D 30 26 48 41 30 3D 31 34 30 26 47 4E 36 3D =0&HA0=1400&GN6=
39 33 35 35 36 32 37 34 31 26 48 53 30 3D 3F 98562741&HS0=??
3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F  ????????????????
3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F  ?????C?????????????
3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F  ????????????????
3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F  ????????????????
1. Source of Trace
This trace data was captured from a network I monitor as part of my professional duties as a Network Security Analyst.

2. Detect was generated by:
This detect was generated by Snort using ruleset 1.6. Snort is a freely available lightweight network IDS written by Mr. Marty Roesch with contributions and enhancements contributed from many sources. Snort uses libpcap, a publicly available framework for capturing network traffic. It will run anywhere libpcap is installed.3

3. Probability the source address was spoofed:

3 http://www.snort.org
The possibility that the source IP was spoofed by another host inside your network is possible though very unlikely. To verify that the IP was not spoofed, I used TCPDUMP with the –e option to view the link level (Ethernet) header in other legitimate traffic to the source IP. I used this data to compare MAC addresses with those in this trace. They were the same. Had this been spoofed traffic the MAC addresses would not match.

4. Description of the attack:
The ICQ Web Front DoS causes the mini httpd that comes with current ICQ clients, or sometimes the entire ICQ client, to crash by appending a “?” character to the URL. This attack works on Windows 95/98 systems. The exploit and Discovery By: Charles Chear

5. Attack mechanism
The attack sends a stimulus, the trailing “??” appended to the URL to the recipient to react by crashing the mini http daemon bringing down the users homepage.

6. Correlation:
This traffic was initially captured by the Snort Alert facility. The specific rule that was triggered was alert tcp any any -> any 80 (msg:"MISC - ICQ Webfront HTTP DoS"; flags:PA; content:"??????????");. This rule looks specifically for tcp traffic from any source IP (internal or external) using any source port that goes to any IP destination address with a destination port of 80 (HTTP). The packet must have the push and acknowledgement flags set. In addition, the packet payload must contain a string of question marks. Adding the flag settings and payload content values to the rule reduces the occurrences of false positives.

The more in-depth supporting data containing the packet payload content was logged in the Snort log which confirms the validity of the alert.

There are several entries in Bugtraq@securityfocus.com that discuss this vulnerability.

7. Evidence of targeting:
This was a targeted attack. The source host directed its attack at a single web server.

8. Severity:
(Criticality + Lethality) – (System Countermeasure + Network Countermeasures)
(5 +5) – (1 + 1) = 8
Criticality = 5 (Access to the user’s homepage is interrupted, which could result in major inconveniences)
Lethality = 5 (The attack will bring down the httpd and in some cases the entire ICQ client)
System Countermeasure = 1 (No patch available to prevent the attack)
Network Countermeasure = 1 (No network filters were in place to block this activity from entering our network)

http://www.shmoo.com/mail/bugtraq/sep00/msg00598.shtml
9. **Defensive recommendations:**
   - Implement the flexible response feature of Snort to reset sessions that trigger this alert. This would prevent the attacks from originating inside or entering into our network. This approach would be a more effective approach than implementing egress/ingress filters at the perimeter gateway because Snort can examine payload content and gateways and firewalls cannot. Careful consideration must be taken before implementing the flexible response feature however; because it could result in you launching a DoS attack against yourself. Also, if you are sniffing your network in stealth mode this feature will not work.5
   - Ensure all system patches are current.
   - Implement a security policy on the allowance of ICQ traffic.

10. **Multiple choice test question:**
    What option does Snort 1.8 other than would allow you to gather additional information on this session?
    
    A. Rst_snd
    B. Icmp_host
    C. Tag

    The correct answer is C. The Tag option allows you to tag sessions that trigger a rule and log all traffic involving the perpetrator for a specified period of time.

---

5 Intrusion Detection- Snort Style, by Marty Roesch, SANS Institute
**Analysis 5: Buffer Overflow**

Buffer overflow attacks violate system memory by overwriting storage boundaries with rogue machine code that will get executed when the violated area is accessed and give the attacker root level access.

**NID Connection Log Entry**

```
<table>
<thead>
<tr>
<th>protocol</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>telnet</td>
<td>10 8.722 hacker.guy.bg</td>
<td>victim.host.org</td>
</tr>
</tbody>
</table>
```

**Example Log Entry**

```
Source = BAD.NET.1.75 -- hacker.guy.bg
Destination = MY.NET.10.233 -- victim.host.org
Start time = Sun Jun 3 12:04:04 2001
Protocols = [32879 23] (6)
Stream = conn.010603:12.10.stream.init
```

```
[*** 40 second idle time reduced to 10 seconds. ***]
grep -v '#' /etc/inetd.conf;
last -20;
```

```
[*** 37 second idle time reduced to 10 seconds. ***]
tail -20 /etc/inetd.conf;
```

```
[*** 62 second idle time reduced to 10 seconds. ***]
echo tcpmux stream tcp nowait root /usr/bin/tcpmux tcpmux >> /etc/inetd.conf;
ls ; /usr/sbin/inetd ; ls -l /usr/sbin/inetd;
which inetd;
find / -name inetd;
```
Janice Y. Slocumb

GCIA Practical Assignment Version 2.9

[*** 99 second idle time reduced to 10 seconds. ***]
cat /etc/passwd;
/usr/etc/inetd;

[*** 68 second idle time reduced to 10 seconds. ***]

cp /bin/sh /bin/trsh; chmod 7755 root:RCtHJd1B6QD1I:0:0:Super-User:/bin/tcsh

[**** End of stream ****]

1. Source of trace
This trace was captured on a network monitored as a part of my duties as an network analyst.

2. Detect was generated by
The original detect was generated by **NID - Network Intrusion Detector v 2.2.1** which is developed and supported by Lawrence Livermore National Laboratory. You can find them on the web at http://www.llnl.gov.

- NID is made up of a suite of tools that collect, detect, and analyze network traffic
- Data is detected and collected based on criteria you specify in customization files.
  - Strings
  - TCP protocols (ports)
  - UDP protocols (ports)
  - Exceptions (traffic to ignore)
  - Trusted and untrusted hosts/servers
- NID is a passive detector so network users are unaware of its presence
- It requires no modification to the hosts that its monitoring
- As data is detected that matches the criteria you specified it's given assigned a "warning level" based on the protocol's capability and authentication required.
- For example telnet has a lot of capabilities but it also requires user authentication (password) to use.
- In contrast TFTP has high capability but the required authentication level is low.
- The mode of operation used to analyze this detect is call retrospective analysis.
ANALYSIS TOOLS

- **STREAM** - reads the raw data files and assembles all the packets associated with the session.
- **PLAYBACK** - displays the session streams.
- **Init** side
- **Dest** side
- **PACKET PRINT** - displays a portion of the packets displayed in the stream along with decoding the header information. (**-e and -ip** options)

3. **Probability that the source address was spoofed**
The source I was not spoofed. For this attack to be successful the attacker must receive the response packets.

4. **Description of the attack**
"There exists a vulnerability in the telnetd service and its code portion incorrectly handling user supplied data as format strings in the sprintf() and syslog() functions. If successfully exploited, arbitrary commands can be executed on a vulnerable system with the root user privileges"  

5. **Attack mechanism**
The attacker exploited the vulnerability in the telnetd daemon to cause a buffer overflow and gain root access on an SGI system.

6. **Correlations**
   - [http://msgs.securepoint.com/cgi-bin/get/bugtraq0008/152.html](http://msgs.securepoint.com/cgi-bin/get/bugtraq0008/152.html)

7. **Evidence of targeting**
This was a targeted attack directed at a SGI host. This indicates prior reconnaissance activity to identify vulnerable hosts.

8. **Severity: (Criticality + Lethality) – (System Countermeasure + Network Countermeasures)**
   - (5 + 5) – (1 + 1) = 8
   - Criticality = 5
   - Lethality = 5 (The attack was successful)
   - System Countermeasure = 1 (Available patch not installed to prevent the attack)
   - Network Countermeasure = 1 (No network filters were in place to block this activity from entering our network)

---

[6](http://lsd-pl.net/files/get?IRIX/irx_telnetd)
9. **Defensive Recommendations**
Install appropriate patches to SGI host
Block the hostile IP address at the perimeter gateway
Disable all unnecessary services

10. **Multiple choice question**
What pattern string should you include in your string based IDS to detect this type of attack.
   
   A. telnet  
   B. /bin/sh  
   C. passwd  

The correct answer is B. The attacker passes /bin/sh in the packet payload to invoke a shell.
Assignment 2 - White Paper

Security In the World of E-Commerce

At the closing of the Clinton administration, President Clinton made the following statement:

“During my Administration, America's economy and society has been transformed by new information and communications technologies. The information technology sector has accounted for almost one-third of U.S. economic growth, and has helped spark an increase in U.S. productivity and global competitiveness.”

The Internet provides a service that is highly accessible. Over three hundred million people now use the Internet, compared to three million in 1994. They can access more than one billion web pages, with an estimated three million new pages added every day. In 2000, Internet usage worldwide was up almost 80% from 1999.

This explosion in Internet usage has fueled the growth and popularity of e-commerce. In the spring of 2000, the Census Bureau released the first official measure of an important subset of business-to-consumer e-commerce, "e-retail." In the fourth quarter of 1999, online sales by retail establishments totaled $5.3 billion, or 0.64 percent of all retail sales. Consumers spent US$3.9 billion online in May 2001. Though this was a 9 percent decrease from the $4.3 billion racked up in Internet sales in April, this is an astounding statistic. People increasingly use the Internet not only to make purchases, but also to arrange financing, take delivery of digital products, and get follow-up service.

The Internet is providing a way for small business to participate in business-to-business e-commerce. In the past, larger companies used private networks to carry out electronic commerce, but high costs kept the resulting efficiencies out of reach for most small businesses. The Internet has changed this by making it easier and cheaper for all businesses to transact business and exchange information.

Electronic commerce (e-commerce) is defined as any transaction that involves the exchange of something of value over a communications network. E-commerce involves selling directly to the customer via the Internet whereas e-business involves sharing information and/or streamlining interactions with business partners. The very nature of the technology poses some difficult security problems because it actively encourages outsiders to access merchant’s systems.

---

7 http://www.ecommerce.gov/ecomnews/01-16-POTUS-STATEMENT.html
8 http://www.esa.doc.gov/de2k.htm
9 http://www.ecommercetimes.com/perl/story/11308.html
As early as July 1999, a study conducted by Information Security Magazine indicated that e-commerce operations are 57 percent more likely to experience a security breach than other online sites. Additionally, e-commerce sites were 24 percent more likely to be the target of a hacker/cracker attack.\(^{10}\)

There are several types of security threats looming on the Internet. Eavesdropping involves intercepting and reading messages. Masquerading refers to the sending and receiving data using someone else’s identity. Message tampering is the altering of messages. Replaying involves using previously sent messages to gain unauthorized privileges. Infiltration is the abuse of authority to run hostile or malicious code. Traffic analysis is really the unauthorized sniffing traffic from the network. Denial of service attacks prevents authorized access to resources.

There are 2 basic approaches to secure electronic commerce. The first focuses on securing servers and network sites to protect resources via perimeter security for example using firewalls. Unfortunately firewalls cannot protect against attacks that do not go through the firewall.

The second approach focuses on transaction security. This addresses prevention of 'sniffers', authentication of all parties involved in the transaction, message integrity to prevent message tampering, and a nonrepudiable record of the transaction. Prevention of 'sniffers' means that transaction details such as credit card details transferred during online transactions use channel and document based security, to prevent eavesdropping.

In global Internet commerce, the parties involved may not know each other, therefore it is necessary to validate authentication of both parties. Certificate authorities (CA) which are financial institutions like VeriSign or FirstVirtual systems, act as third parties for the transactions. The CA authenticates clients by issuing them with certificates that are digitally authorized by the CA and which contains a secure digital signature. The client can then use this signature in online transactions.

Another major thing that needs to be done to protect consumers is the enactment of laws against cyber crime. This is a critical step if e-commerce is to reach its full potential. A study conducted by McConnell International, a Washington consulting company in December of 2000 reported that most nations laws don’t deter cyber crime. Thirty-three of the 52 nations participating in the survey didn’t have criminal codes to deal with computer crime.\(^{11}\)

The data involved in e-commerce transactions is critical and sensitive pertaining to customers and business partners. In some cases attackers have tools such as "packet

\(^{10}\) E-Commerce Times, July 26, 1999
sniffers" to monitor a computer network, accessing confidential e-mails, account names, passwords and credit card information.

E-commerce merchants must focus on web servers and their associated databases management systems to provide secure environments. Many businesses use freely available software in the implementation of their e-commerce solutions. Although this reduces the overhead costs involved in providing the service, it certainly increases the security risks. On June 19th, Newsbytes magazine reported that several small online shops were exposing their customer order data, including credit card numbers, because of improperly installed online shopping cart software. A free online shopping cart program called DCShop, from Boston-based DC Business Solutions, caused the exposure. Thousands of copies of DCShop have been downloaded from the company's site.12

On June 13, DCBS posted an advisory at its site warning DCShop operators of the vulnerability. The advisory states that if the program is improperly installed unauthorized Internet users would be able to retrieve sensitive customer information including names, mailing addresses, e-mails and credit card numbers with expiration dates. The DCShop security advisory is available here: http://www.dcscripts.com/dcforum/dcshop/44.html

Protecting against financial fraud is another major challenge. In a study conducted by The Worldwide E-Commerce Fraud Prevention Network in April of this year found that nearly half of e-tailers surveyed said online fraud is a "significant problem."

"The survey, which was conducted over the week of March 5 on the Network's Web site, found that 50 percent of those surveyed reported online losses from fraud of between $1,000 and $10,000. Nineteen percent said they had lost more than $100,000."13

Merchants categorized the most effective tools for fraud prevention this way. Those with address verification ranked highest at 68 percent of those surveyed, real-time authorization at 52 percent, card verification codes at 49 percent, and customized rules at 42 percent.

After taking a look at the current security posture of e-commerce, the natural question that came to mind was, how do you address the challenges? There are some basic security services defined by the International Organization for Standardization 14

- Authentication ensures that the identity or data origin is genuine.
- Access control ensures that only authorized users/processes gain access to protected data.

13 http://www.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/hn/xml/01/04/05/010405hnfraud.xml&dctag=ecommerce
Janice Y. Slocumb

Data confidentiality ensures that only authorized user/processes understand the protected data.

Data integrity protects data against unauthorized modification.

Nonrepudiation ensures that users/processes are not denied the required access to resources.

What tools are available to help overcome the security challenges? My research yielded several tools available on the market today. This is in no way an exhaustive list. I must add a disclaimer here; I am in no way recommending or advocating the use of any of these tools. I cannot, and do not speak for the effectiveness of them. My intent is just to take a look at some of the available options.

At a presentation conducted by the Department of Defense in May of last year several multi-platform products were highlighted.

**Usage: Single Web Server Access and transaction control**
**Platform: NT, HP-UX, Solaris**

*Praesidium Domainguard Access and Domainguard Rules,*

Web authorization managers that combine powerful Web security with ease of use. The products, Praesidium Domainguard Access and Domainguard Rules, make it easy for organizations to create and manage a secure Web environment within which customers, business partners and employees can perform transactions and share sensitive information.

**Usage: Portal Access and Transaction Control**
**Platform NT, HP-UX, Solaris**

*DomainGuard Enterprise*

DomainGuard Enterprise is a user access solution for Microsoft-based (NT/IIS) environments providing a centralized point of control for all access to Web objects. It interfaces with existing user definitions and access groups by plugging into the LDAP directory, and managers and administrators can control and assign access to individual Web objects.

Features of the authentication interface include single sign-on, meaning that a user need only login once and replication, which allows user and policy data to be instantly replicated across multiple servers.¹⁵

**Usage: Application Protection**
**Platform: HP-UX**

*VirtualVault*

---

Virtualvault is a secure Web transaction server that is designed to safely connect enterprise applications and databases to clients on the Internet. On April 25, 2001 - Hewlett-Packard was awarded Best General Security product in the Reader's Trust category for HP Virtualvault. This is the second year running that Virtualvault has received this award.

**Usage: Windows Server Protection**
**Platform:** NT/IS, W2000

**WebEnforcer**

Webenforcer automatically uncovers hundreds of vulnerabilities, eliminates them, and continuously monitors and enforces security.

**Usage: Web Queue & Service management**
**Platform:** HP-UX, NT, Solaris, Linux

**WebQoS**

HP webqos is a multi-platform server-based used to control web site performance and resources. Webqos receives and looks at all HTTP request and data packets before passing them on to the web server. No data is passed to via a HTTP connection request to the web server unless there is legitimate data associated with the request. Therefore, the web server will not be affected by a HTTP denial of service.

**Usage: Network Traffic security**
**Platform:** NT, HP-UX, Solaris

**E-Firewall**

E-Firewall uses a robust set of application proxies to examine the entire data stream of every connection attempted through the firewall. Traffic is filtered according to explicit order-independent rules.

**Extranet Security**
**Platform:** NT, HP-UX, Solaris

**Extranet VPN**

Extranet VPN secures communications between third-party users and a company's internal network, with user-based authentication and strong encryption of information sent over the Internet.

---

20 [http://www.erpworld.org/vendor/prod/f175.html](http://www.erpworld.org/vendor/prod/f175.html)
Accelerates SSL connection on Web Servers  
Platform: HP-UX  
SpeedCard

HP Speedcard improves the performance of applications running on HP servers whenever user authentication protocols such as the Secure Sockets Layer (SSL) bundled into Netscape Enterprise Server are implemented. It offloads cryptographic computations from web server.  

E-commerce security is a work in progress. There is no “silver bullet” solution to the security problems associated with e-commerce. The problem is a global one and it will require input and cooperation from nations around the world to meet the challenge.

22 http://www.hp.com/security/products/speedcard/
Additional References:
http://www.securityfocus.com/focus/ids/articles/marcmyers.html
Assignment 3 – Analyze This

Executive Summary:

Thank you for the opportunity to review and assess the security posture of your organization’s network. This report provides an initial assessment of your network based on a sampling of your network traffic. It includes recommendations that will improve security practices in your organization.

Observations/Recommendations:

Establish and enforce policies on appropriate network use. There is a considerable amount of traffic generated by tools such as Gnutella and ICQ; 67% of the scan activity originated inside your network. High volumes of this type of traffic take away resources that could be used to support the organization.

Consider the placement of your sensor. Seven percent of the total detects where involving private network addresses. Six percent of the detects were generated by host 10.0.0.1 which is generating bootp traffic to the network broadcast address 10.255.255.255 which could be normal traffic if it is a diskless workstation or it could be an indication of a misconfigured machine. The other 1% of the detects were generated by netbios name service traffic (UDP port 137) from host 192.168.0.2

There was evidence of possible the presence of compromised hosts in the network. Those hosts are specified in the detailed section of the report. Verification, containment, and eradication must be done on the effected systems. Known Trojan ports should be blocked at the perimeter gateway.

Ingress and regress filtering should be implemented to prevent packets with source IP addresses outside of your address range from leaving your network. This will prevent attackers from using your network as a launch pad for distributed denial of service attacks.
Detailed Analysis based upon the following data:

### Alerts

<table>
<thead>
<tr>
<th>File Name:</th>
<th>Begin Date/Time:</th>
<th>End Date/Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert-01-Apr</td>
<td>Mar 31 00:16:24</td>
<td>Apr  1 00:03:54</td>
</tr>
<tr>
<td>Alert-03-Apr</td>
<td>Apr  2 00:16:13</td>
<td>Apr  2 23:48:12</td>
</tr>
<tr>
<td>Alert-23-Mar</td>
<td>Mar 22 00:19:45</td>
<td>Mar 23 00:05:39</td>
</tr>
<tr>
<td>Alert-26-Mar</td>
<td>Mar 25 00:16:50</td>
<td>Mar 26 00:05:58</td>
</tr>
<tr>
<td>Alert-27-Mar</td>
<td>Mar 26 00:24:49</td>
<td>Mar 26-23:50:03</td>
</tr>
</tbody>
</table>

### Scans

<table>
<thead>
<tr>
<th>File Name:</th>
<th>Begin Date/Time:</th>
<th>End Date/Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnortScan-01-Apr</td>
<td>Mar 31 00:00:16</td>
<td>Mar 31 23:58:36</td>
</tr>
<tr>
<td>SnortScan-03-Apr</td>
<td>Apr  2 00:00:09</td>
<td>Apr  2 23:56:58</td>
</tr>
<tr>
<td>SnortScan-23-Mar</td>
<td>Mar 22 00:04:49</td>
<td>Mar 22 23:50:49</td>
</tr>
<tr>
<td>SnortScan-26-Mar</td>
<td>Mar 25 00:00:32</td>
<td>Mar 25 23:56:16</td>
</tr>
<tr>
<td>SnortScan-27-Mar</td>
<td>Mar 26 00:10:42</td>
<td>Mar 26 23:57:00</td>
</tr>
</tbody>
</table>

### Out of Spec

<table>
<thead>
<tr>
<th>File Name:</th>
<th>Begin Date/Time:</th>
<th>End Date/Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOS-Apr-02</td>
<td>Apr  2 00:04:39</td>
<td>Apr  2 23:47:52</td>
</tr>
</tbody>
</table>
### Alert Listing

**Duration:** Earliest alert at **00:04:49**.047251 on 03/22/2001  
Latest alert at **23:48:12**.158179 on 04/02/2001

<table>
<thead>
<tr>
<th>Total</th>
<th>Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>10906</td>
<td>Watchlist 000220 IL-ISDNNET-990517</td>
</tr>
<tr>
<td>10833</td>
<td>Attempted Sun RPC high port access</td>
</tr>
<tr>
<td>3175</td>
<td>UDP SRC and DST outside network</td>
</tr>
<tr>
<td>2494</td>
<td>SYN-FIN scan!</td>
</tr>
<tr>
<td>431</td>
<td>External RPC call</td>
</tr>
<tr>
<td>307</td>
<td>connect to 515 from outside</td>
</tr>
<tr>
<td>296</td>
<td>Possible RAMEN server activity</td>
</tr>
<tr>
<td>243</td>
<td>SMB Name Wildcard</td>
</tr>
<tr>
<td>139</td>
<td>Queso fingerprint</td>
</tr>
<tr>
<td>136</td>
<td>Watchlist 000222 NET-NCFC</td>
</tr>
<tr>
<td>117</td>
<td>WinGate 1080 Attempt</td>
</tr>
<tr>
<td>109</td>
<td>Back Orifice</td>
</tr>
<tr>
<td>96</td>
<td>TCP SRC and DST outside network</td>
</tr>
<tr>
<td>49</td>
<td>Russia Dynamo – SANS Flash 28-jul-00</td>
</tr>
<tr>
<td>38</td>
<td>Null scan!</td>
</tr>
<tr>
<td>29</td>
<td>Port 55850 tcp - Possible myserver activity - ref. 010313-1</td>
</tr>
<tr>
<td>24</td>
<td>NMAP TCP ping!</td>
</tr>
<tr>
<td>20</td>
<td>Tiny Fragments - Possible Hostile Activity</td>
</tr>
<tr>
<td>10</td>
<td>SUNRPC highport access!</td>
</tr>
<tr>
<td>8</td>
<td>ICMP SRC and DST outside network</td>
</tr>
<tr>
<td>2</td>
<td>connect to 515 from inside</td>
</tr>
</tbody>
</table>

Total: 29462
Detects Prioritized by Number of Occurrences in Descending Order

**Detect #1:** Watchlist 000220 IL-ISDNNET-990517

**SnortSnarf signature page**
Watchlist 000220 IL-ISDNNET-990517
SnortSnarf v052301.1

10906 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Duration: Earliest such alert at **04:07:26.296525 on 03/22/2001**
Latest such alert at **23:07:48.661953 on 04/02/2001**

Watchlist 000220 IL-ISDNNET-990517 26 sources 25 destinations

<table>
<thead>
<tr>
<th>Top 5 Sources triggering this attack signature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
</tr>
<tr>
<td>212.179.4.50</td>
</tr>
<tr>
<td>212.179.127.41</td>
</tr>
<tr>
<td>212.179.72.226</td>
</tr>
<tr>
<td>212.179.28.66</td>
</tr>
<tr>
<td>212.179.27.6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Top 5 Destinations receiving this attack signature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destinations</strong></td>
</tr>
<tr>
<td>999.999.222.154</td>
</tr>
<tr>
<td>999.999.156.55</td>
</tr>
<tr>
<td>999.999.201.238</td>
</tr>
<tr>
<td>999.999.219.14</td>
</tr>
<tr>
<td>999.999.219.38</td>
</tr>
</tbody>
</table>

**Threat/Vulnerabilities:** Gnutella allows the sharing of files through firewalls:
gnutella-svc  6346/tcp  gnutella-svc
gnutella-svc  6346/udp  gnutella-svc
gnutella-rtr  6347/tcp  gnutella-rtr
gnutella-trt  6347/udp  gnutella-rtr

The source host are registered to Israeli address.

**Correlations:**  [http://www.sans.org/y2k/051900.htm](http://www.sans.org/y2k/051900.htm)

**Reference:**
[http://www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers)
Detect #2: Attempted Sun RPC high port access

**SnortSnarf signature page**
Attempted Sun RPC high port access  
**SnortSnarf** v052301.1

10833 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Duration: Earliest such alert at 19:42:24.114048 on 03/26/2001  
Latest such alert at 22:40:51.585106 on 04/02/2001

<table>
<thead>
<tr>
<th>Sources triggering this attack signature</th>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>63.121.232.185</td>
<td>10379</td>
<td>10379</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>209.150.227.153</td>
<td>452</td>
<td>452</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>205.188.153.101</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>205.188.153.97</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destinations receiving this attack signature</th>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>999.999.221.198</td>
<td>8926</td>
<td>8926</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>999.999.224.2</td>
<td>1905</td>
<td>1905</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>999.999.224.58</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>999.999.228.90</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities:

| Rpc bind32 Check                          | The Rpcbind service normally only listens on port 111. Under Solaris the Rpcbind service will also listen under port 32771, this sometimes allows attackers to bypass packet filtering firewalls. |
CVE-1999-0189
Solaris rpcbind listens on a high numbered UDP port, which may not be filtered since the standard port number is 111.

**Rule:** alert udp any any -> $HOME_NET 32771 (msg: "Attempted Sun RPC high port access");
http://www.clark.net/~roesch/misc-lib

**Correlation:**
http://www.sans.org/y2k/021500.htm
http://www.sans.org/y2k/051900.htm
http://www.cpmc.columbia.edu/misc/docs/iss/html/ch_2.html
http://cve.mitre.org/cve/refs/refmap/source-SUN.html
**Detect #3:** UDP SRC and DST outside network

![SnortSnarf signature page](image)

SnortSnarf signature page
UDP SRC and DST outside network
SnortSnarf v052301.1

**3175 alerts** with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Duration: Earliest such alert at **00:30:45.656617 on 03/22/2001**
Latest such alert at **23:48:12.158179 on 04/02/2001**

| UDP SRC and DST outside network | 65 sources | 268 destinations |

**Top 5 Sources triggering this attack signature**

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>1502</td>
<td>1502</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>129.2.225.92</td>
<td>502</td>
<td>502</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.2</td>
<td>384</td>
<td>384</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>169.254.67.123</td>
<td>246</td>
<td>246</td>
<td>212</td>
<td>212</td>
</tr>
<tr>
<td>192.168.0.13</td>
<td>101</td>
<td>101</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Top 5 Destinations receiving this attack signature**

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srs (sig)</th>
<th># Srs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.255.255</td>
<td>1502</td>
<td>1502</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>128.183.7.7</td>
<td>502</td>
<td>502</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.255</td>
<td>383</td>
<td>383</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>235.80.68.83</td>
<td>167</td>
<td>167</td>
<td>33</td>
<td>33</td>
</tr>
<tr>
<td>169.254.255.255</td>
<td>58</td>
<td>58</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**Threat/Vulnerabilities:** Neither side of the connection was within your network. This traffic could be an indication of IP address forgery, or that your network is being used to launch an attack on some other network. I should not see this type of traffic normally.

**Correlations:** [http://www.cs.wright.edu/~pmateti/Courses/499/IPexploits/](http://www.cs.wright.edu/~pmateti/Courses/499/IPexploits/)
Detect #4: SYN-FIN scan!

2494 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalert.txt

Duration: Earliest such alert at 00:00:52.899361 on 03/31/2001
  Latest such alert at 23:48:17.240683 on 03/31/2001

SYN-FIN scan!  2 sources  1950 destinations

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>211.178.63.4</td>
<td>2493</td>
<td>2493</td>
<td>1949</td>
<td>1949</td>
</tr>
<tr>
<td>24.17.64.12</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Top 5 Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.218.49</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.2.49</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.144.83</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.18.61</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.5.92</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: SYN/FIN scans are often used to avert firewalls and scan for open ports. This is a well known reconnaissance tactic used by hackers. It can also be used as a way to fingerprint the target operating system. The primary source of this attack is registered to a Korean network address.

Rule: alert TCP SEXTERNAL any -> $INTERNAL any (msg: "SYN-FIN Scan!"; flags:SF);

Correlations: [http://www.whitehats.com/cgi/arachNIDS/Show? id=ids198&view=event](http://www.whitehats.com/cgi/arachNIDS/Show? id=ids198&view=event)
**Detect #5:** External RPC call

**SnortSnarf signature page**

**External RPC call**

**SnortSnarf v052301.1**

---

**431 alerts** with this signature using input module SnortFileInput, with sources:

- D://GIAC/massalrt.txt

Duration: Earliest such alert at **16:26:56.292779 on 03/25/2001**
Latest such alert at **23:18:23.558962 on 04/02/2001**

<table>
<thead>
<tr>
<th>External RPC call</th>
<th>7 sources</th>
<th>344 destinations</th>
</tr>
</thead>
</table>

**Top 5 Sources triggering this attack signature**

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>209.217.53.190</td>
<td>130</td>
<td>130</td>
<td>130</td>
<td>130</td>
</tr>
<tr>
<td>61.129.39.161</td>
<td>81</td>
<td>81</td>
<td>65</td>
<td>65</td>
</tr>
<tr>
<td>24.91.102.156</td>
<td>69</td>
<td>69</td>
<td>69</td>
<td>69</td>
</tr>
<tr>
<td>209.189.124.214</td>
<td>52</td>
<td>52</td>
<td>52</td>
<td>52</td>
</tr>
<tr>
<td>209.70.72.22</td>
<td>44</td>
<td>44</td>
<td>44</td>
<td>44</td>
</tr>
</tbody>
</table>

**Top 5 Destinations receiving this attack signature**

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.135.210</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>999.999.132.110</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>999.999.132.138</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>999.999.132.114</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>999.999.132.208</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**Threat/Vulnerabilities:** RPC implements a logical client-to-server communications system designed specifically for the support of network applications.

**Rule:**

**Correlations:** [http://www.sans.org/y2k/010300-0900.htm](http://www.sans.org/y2k/010300-0900.htm)

**Reference:** [http://nscp.upenn.edu/aix4.3html/aixprggd/progcom/ch8_rpc.htm](http://nscp.upenn.edu/aix4.3html/aixprggd/progcom/ch8_rpc.htm)
Detect #6: connect to 515 from outside

SnortSnarf signature page
connect to 515 from outside
SnortSnarf v052301.1

307 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Duration: Earliest such alert at 10:03:20.841926 on 03/22/2001
Latest such alert at 18:07:49.638079 on 04/02/2001

**Top 5 Sources triggering this attack signature**

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>216.162.44.140</td>
<td>188</td>
<td>188</td>
<td>143</td>
<td>143</td>
</tr>
<tr>
<td>63.123.106.6</td>
<td>37</td>
<td>37</td>
<td>37</td>
<td>37</td>
</tr>
<tr>
<td>207.124.229.123</td>
<td>33</td>
<td>33</td>
<td>31</td>
<td>31</td>
</tr>
<tr>
<td>212.125.177.199</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>205.238.235.88</td>
<td>17</td>
<td>17</td>
<td>16</td>
<td>16</td>
</tr>
</tbody>
</table>

**Top 5 Destinations receiving this attack signature**

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.133.216</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>999.999.133.208</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>999.999.134.81</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>999.999.134.31</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>999.999.134.54</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

**Threat/Vulnerabilities:** Adore scans the Internet checking Linux hosts to determine whether they are vulnerable to any of the following well-known exploits: LPRng, rpc-statd, wu-ftp and BIND. LPRng is installed by default on Red Hat 7.0 systems. From the
reports so far, Adore appears to have started its spread on April 1. (http://www.sans.org/y2k/adore.htm)
TCP port 515 (LPD) can also be used for remote OS detection - not a root exploit.
Correlations: http://www.sans.org/y2k/122100-1200.htm
http://packetstorm.securify.com/advisories/l0pht/l0pht.00-01-08.lpd

There are several CVE entries involving TCP port 515:
CVE-1999-0299 - Buffer overflow in FreeBSD lpd through long DNS hostnames.
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0299
CVE-2000-0534 - The apsfilter software in the FreeBSD ports package does not properly read user filter configurations, which allows local users to execute commands as the lpd user.
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0534
CAN-1999-0061 ** CANDIDATE (under review) ** File creation and deletion, and remote execution, in the BSD line printer daemon (lpd).
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0061
CAN-2000-0839 ** CANDIDATE (under review) ** WinCOM LPD 1.00.90 allows remote attackers to cause a denial of service by sending a large number of LPD options to the LPD port (515).
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0839
CAN-2000-0879 ** CANDIDATE (under review) ** LPPlus programs dccsched, decldser, dccbkst, dcshut, decldpsht, and dccbkstshut are installed setuid root and world executable, which allows arbitrary local users to start and stop various LPD services.
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0879
CAN-2000-1064 ** CANDIDATE (under review) ** Buffer overflow in the LPD service in HP JetDirect printer card Firmware x.08.20 and earlier allows remote attackers to cause a denial of service.
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-1064
Detect #7: Possible RAMEN server activity

SnortSnarf signature page
Possible RAMEN server activity
SnortSnarf v052301.1

296 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalert.txt

Duration: Earliest such alert at 01:24:02.231341 on 03/22/2001
Latest such alert at 19:57:08.989338 on 04/02/2001

Possible RAMEN server activity
92 sources
120 destinations

Top 5 Sources triggering this attack signature

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>203.199.88.59</td>
<td>65</td>
<td>65</td>
<td>31</td>
<td>31</td>
</tr>
<tr>
<td>63.10.42.245</td>
<td>15</td>
<td>15</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.209.86</td>
<td>13</td>
<td>13</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.221.26</td>
<td>10</td>
<td>10</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>999.999.98.171</td>
<td>9</td>
<td>9</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Top 5 Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>63.10.40.155</td>
<td>17</td>
<td>17</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>24.180.160.210</td>
<td>16</td>
<td>16</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>999.999.210.2</td>
<td>15</td>
<td>15</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.221.26</td>
<td>10</td>
<td>10</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>203.199.88.59</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: Ramen is a self-propagating worm that exploits vulnerabilities in Red Hat versions of Linux. It is spread using port 27374. Hosts 999.999.209.86, 999.999.221.26, and 999.999.98.171 show indication of compromise.

Correlations: http://www.linuxsecurity.com/articles/network_security_article-2335.html
http://www.internetnews.com/wd-news/article/0,,10_563141,00.html
Detect #8: SMB Name Wildcard

**signature page**

SMB Name Wildcard

*SnortSnarf* v052301.1

---

243 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Duration: Earliest such alert at **00:11:57.626793 on 03/22/2001**

Latest such alert at **23:35:23.810694 on 04/02/2001**

Top 5 Sources triggering this attack signature

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.41.3.11</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>211.118.86.11</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>217.1.75.169</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>61.113.69.107</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>62.47.50.129</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Top 5 Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.132.36</td>
<td>20</td>
<td>22</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>999.999.133.32</td>
<td>15</td>
<td>15</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>999.999.135.45</td>
<td>11</td>
<td>12</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>999.999.133.245</td>
<td>11</td>
<td>13</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>999.999.135.25</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: replacing the name in standard Netbios "nbstat" frames with an "*" followed by blanks, attackers can gain valuable Netbios naming information and node status information from Netbios and SAMBA clients. Taking advantage of the inability of SMB to parse correctly when the wildcard is used. The response contains a listing of any Netbios names known to that node.

Correlations: [http://www.sans.org/y2k/051300.htm](http://www.sans.org/y2k/051300.htm)

[http://www.sans.org/y2k/practical/Loras_Evan_GCIA.doc](http://www.sans.org/y2k/practical/Loras_Evan_GCIA.doc)
Detect #9: Queso fingerprint

139 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalert.txt

Duration: Earliest such alert at 00:59:01.795512 on 03/22/2001
Latest such alert at 15:30:33.434439 on 04/02/2001

| Queso fingerprint | 14 sources | 20 destinations |

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>129.206.170.20</td>
<td>101</td>
<td>101</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>158.75.57.4</td>
<td>13</td>
<td>13</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>24.50.80.131</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>213.64.149.61</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>130.233.26.197</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srons (sig)</th>
<th># Srons (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.202.54</td>
<td>98</td>
<td>99</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>999.999.219.14</td>
<td>8</td>
<td>840</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>999.999.229.38</td>
<td>7</td>
<td>20</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>999.999.219.134</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.218.142</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: Queso is a tool used to attempt to determine what operating system a host is running. This could be potentially dangerous as attackers could use this information to launch targeted attacks.

Correlations: [http://www.securityfocus.com/frames?focus=ids&content=/focus/ids/articles/portscan.html](http://www.securityfocus.com/frames?focus=ids&content=/focus/ids/articles/portscan.html)
Detect #10: Watchlist 000222 NET-NCFC

**SnortSnarf signature page**

Watchlist 000222 NET-NCFC

**SnortSnarf** v052301.1

**136 alerts** with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalert.txt

Duration: Earliest such alert at **06:02:56.754894 on 03/22/2001**
  Latest such alert at **21:37:37.636498 on 04/02/2001**

Watchlist 000222 NET-NCFC 10 sources 9 destinations

---

**Top 5 Sources triggering this attack signature**

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>159.226.92.9</td>
<td>94</td>
<td>94</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>159.226.41.166</td>
<td>22</td>
<td>22</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>159.226.6.6</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>159.226.158.188</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>159.226.47.217</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Top 5 Destinations receiving this attack signature**

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.144.54</td>
<td>94</td>
<td>95</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>999.999.100.81</td>
<td>22</td>
<td>23</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>999.999.253.43</td>
<td>6</td>
<td>7</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>999.999.6.47</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>999.999.140.236</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Threat/Vulnerabilities:** This alert was generated because the source addresses involved are associated with the Computer Network Center Chinese Academy of Sciences and they are attempting to access a mail server in your network. This could indicate that some malicious activity will follow.

**Correlations:** http://www.zeltser.com/sans/practical/
Detect #11: WinGate 1080 Attempt

SnortSnarf signature page
WinGate 1080 Attempt
SnortSnarf v052301.1

117 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Earliest such alert at 00:44:14.910522 on 03/22/2001
Latest such alert at 22:20:11.600061 on 04/02/2001
WinGate 1080 Attempt 53 sources 64 destinations

Top 5 Sources triggering this attack signature

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>204.117.70.5</td>
<td>8</td>
<td>8</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>195.66.170.8</td>
<td>8</td>
<td>8</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>217.10.143.59</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>63.102.227.48</td>
<td>6</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>216.54.223.198</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Top 5 Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.60.11</td>
<td>6</td>
<td>8</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>999.999.204.102</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>999.999.202.58</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>999.999.156.55</td>
<td>4</td>
<td>2166</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>999.999.254.10</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: Wingate allows multiple hosts to share a single internet connection. Attackers use this to hide while launching attacks.
Detect #12:  Back Orifice

SnortSnarf signature page

Back Orifice

SnortSnarf v052301.1

109 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Duration: Earliest such alert at 14:37:58.116356 on 03/26/2001
Latest such alert at 14:38:45.807857 on 03/26/2001

**Sources triggering this attack signature**

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.162.245.198</td>
<td>109</td>
<td>109</td>
<td>109</td>
<td>109</td>
</tr>
</tbody>
</table>

**Top 5 Destinations receiving this attack signature**

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srgs (sig)</th>
<th># Srgs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.7.53</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.20.130</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.7.57</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.20.6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.2.105</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Threat/Vulnerabilities:** Back Orifice allows remote users to gain access to your computer and potentially run malicious code. The source of these alerts are registered to ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-5)

13241 Woodland Park Road  Herndon, VA 20171  US

**Correlations:**

http://www.symantec.com/avcenter/warn/backorifice.html
http://www.zdnet.com/zdmn/stories/zdnn_smgraph_display/0,3441,2124585,00.html
**Detect #13:** TCP SRC and DST outside network

**SnortSnarf signature page**

TCP SRC and DST outside network

SnortSnarf v052301.1

---

**96 alerts** with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Duration: Earliest such alert at **08:10:56.202450 on 03/22/2001**

Latest such alert at **22:24:19.069127 on 04/02/2001**

**TCP SRC and DST outside network** 22 sources 35 destinations

---

**Sources triggering this attack signature**

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>65.9.246.190</td>
<td>42</td>
<td>44</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>169.254.101.152</td>
<td>19</td>
<td>19</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>172.140.196.73</td>
<td>12</td>
<td>12</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>206.196.177.82</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>192.168.0.5</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Destinations receiving this attack signature**

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.173.102.93</td>
<td>40</td>
<td>40</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12.77.186.67</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>205.188.49.19</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>205.188.49.16</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>205.188.45.241</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Threat/Vulnerabilities:** Neither side of the connection was within your network. This traffic could be an indication of IP address forgery, or that your network is being used to launch an attack on some other network. I should not see this type of traffic normally.

**Correlations:**
- [http://www.all.net/journal/netsec/9606.html](http://www.all.net/journal/netsec/9606.html)
Detect #14: Russia Dynamo - SANS Flash 28-jul-00

SnortSnarf signature page
Russia Dynamo - SANS Flash 28-jul-00
SnortSnarf v052301.1

49 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalert.txt

Duration: Earliest such alert at 09:55:13.472191 on 03/22/2001
   Latest such alert at 19:02:52.309207 on 04/02/2001

Russia Dynamo - SANS Flash 28-jul-00 4 sources 3 destinations

Sources triggering this attack signature

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>194.87.6.189</td>
<td>43</td>
<td>43</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.178.42</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>194.87.6.164</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>194.87.6.21</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.178.42</td>
<td>44</td>
<td>46</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>194.87.6.21</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>999.999.219.14</td>
<td>1</td>
<td>840</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: The 194.87.6.x network is registered to a Russian address. This could be an indication of compromised hosts in your network. I recommend that the 999.999.178.42 and 999.999.219.14 hosts be checked for any indication of a Trojan.

CORRELATIONS:
HTTP://ARCHIVES.NEOHAPSIS.COM/ARCHIVES/SANS/2000/0068.HTML
HTTP://WWW.SANS.ORG/Y2K/072818.HTM

HTTP://WWW.SANS.ORG/Y2K/PRACTICAL/MIIKA_TURKIA_GCIA.HTML
Detect #15: Null scan!

Snort Snarf signature page
Null scan!
Snort Snarf v052301.1

38 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalert.txt

Duration: Earliest such alert at 00:04:49.047251 on 03/22/2001
Latest such alert at 04:38:08.108174 on 04/02/2001

Null scan! 26 sources 19 destinations

Top 5 Sources triggering this attack signature

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.108.215.109</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>24.43.241.223</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>24.17.64.12</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>24.141.54.29</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>24.201.95.135</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Top 5 Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.209.30</td>
<td>9</td>
<td>10</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>999.999.220.38</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>999.999.229.38</td>
<td>5</td>
<td>20</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>999.999.226.82</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>999.999.209.154</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: Null scans are used by attackers for reconnaissance gathering about open port on target hosts.

CORRELATIONS: HTTP://WWW.NCMAG.COM/2001_03/CYBERCRIME/
HTTP://WWW.NETWORKICE.COM/ADVICE/INTRUSIONS/2000309/DEFAULT.H
Detect #16: Port 55850 tcp - Possible myserver activity - ref. 010313-1

SnortSnarf signature page
Port 55850 tcp - Possible myserver activity - ref. 010313-1
SnortSnarf v052301.1

29 alerts with this signature using input module SnortFileInput, with sources:

- D:\GIAC\massalert.txt

Duration: Earliest such alert at 03:30:35.045398 on 03/22/2001
Latest such alert at 16:47:04.593439 on 03/31/2001

Port 55850 tcp - Possible myserver activity - ref. 010313-1 9 sources 10 destinations

**Sources triggering this attack signature**

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.218.86</td>
<td>16</td>
<td>16</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>199.20.66.1</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>198.81.129.194</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.60.38</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>212.158.113.194</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Top 5 Destinations receiving this attack signature**

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.154.1.109</td>
<td>14</td>
<td>14</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.229.38</td>
<td>4</td>
<td>20</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>999.999.253.112</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>213.44.175.50</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>63.97.226.2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Threat/Vulnerabilities:** MyServer is a DDoS tool. The agent uses port 55850. Hosts 999.999.218.86 and 999.999.60.38 should be checked for indication of compromise.

**Correlations:** [http://www.sans.org/y2k/082200.htm](http://www.sans.org/y2k/082200.htm)
Detect #17: NMAP TCP ping!

SnortSnarf signature page
NMAP TCP ping!
SnortSnarf v052301.1

24 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalert.txt

Duration:
Earliest such alert at 00:23:38.294659 on 03/22/2001
Latest such alert at 20:32:54.095143 on 04/02/2001

| NMAP TCP ping! | 8 sources | 12 destinations |

Top 5 Sources triggering this attack signature

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.102.197.234</td>
<td>11</td>
<td>11</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>199.197.130.21</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>202.187.24.3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>63.119.91.2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>194.133.58.2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Top 5 Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.1.8</td>
<td>8</td>
<td>8</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.1.10</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.100.165</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>999.999.60.14</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>999.999.1.3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: This event indicates that a remote user has used the NMAP portscanning tool to probe the server. An NMAP TCP ping was sent to determine if a host is reachable. pcAnywhere 8.x and 9.x allows remote attackers to cause a denial of service via a TCP SYN scan, e.g. by nmap.

Correlations: [http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0324](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0324)
Detect #18: Tiny Fragments - Possible Hostile Activity

SnortSnarf signature page
Tiny Fragments - Possible Hostile Activity
SnortSnarf v052301.1

20 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalrt.txt

Duration: Earliest such alert at 17:44:11.884673 on 03/25/2001
Latest such alert at 16:48:11.374219 on 04/02/2001

| Tiny Fragments - Possible Hostile Activity | 2 sources | 14 destinations |

Sources triggering this attack signature

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>202.39.78.125</td>
<td>18</td>
<td>18</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>202.39.78.124</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Top 5 Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Spcs (sig)</th>
<th># Spcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.203.150</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>999.999.203.50</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.230.42</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.208.142</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>999.999.204.218</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: Attackers sometimes use tools to craft packets containing tiny fragments to prevent detection by intrusion detection systems. By fragmenting packets and spreading the signature over multiple packets hostile traffic can often get by pattern matching IDS systems. Fragmentation can sometimes occur in normal traffic; however it can cause problems when reassembly is not handled correctly. There are several known exploits that utilize fragmentation such as teardrop, jolt2, etc.

Detect #19: SUNRPC highport access!

SnortSnarf signature page
SUNRPC highport access!
SnortSnarf v052301.1

10 alerts with this signature using input module SnortFileInput, with sources:
- D:/GIAC/massalert.txt

Duration: Earliest such alert at 14:58:28.952796 on 03/25/2001
Latest such alert at 14:58:29.585974 on 03/25/2001

| SUNRPC highport access! | 1 sources | 1 destinations |

Sources triggering this attack signature

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>216.136.171.195</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Destinations receiving this attack signature

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.100.225</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: This alert was generated as a result of a lone host being targeted and probed for SUNRPC services. The source of this attack is of special interest because it is registered to an address in the Netherlands.

Correlations: CVE-1999-0189
Solaris rcbind listens on a high numbered UDP port, which may not be filtered since the standard port number is 111.
Detect #20: ICMP SRC and DST outside network

SnortSnarf signature page

ICMP SRC and DST outside network
SnortSnarf v052301.1

8 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/mausalrt.txt

Duration: Earliest such alert at 08:11:09.556945 on 03/22/2001
Latest such alert at 18:49:26.972974 on 04/02/2001

ICMP SRC and DST outside network | 4 sources | 5 destinations

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.168.100.123</td>
<td>3</td>
<td>6</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>65.9.246.190</td>
<td>2</td>
<td>44</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>172.167.9.216</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>172.128.30.236</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srgcs (sig)</th>
<th># Srgcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>217.32.140.237</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>216.101.207.124</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>172.164.87.212</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>207.91.16.230</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>24.162.140.146</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: Neither side of the connection was within your network. This traffic could be an indication of IP address forgery, or that your network is being used to launch an attack on some other network. I should not see this type of traffic normally. Additionally, the TCP packets source and destination port numbers are unusual. The source port is 137 (Netbios name service) and the destination port is 53 (DNS).

Detect #21: connect to 515 from inside

2 alerts with this signature using input module SnortFileInput, with sources:

- D:/GIAC/massalert.txt

Earliest such alert at 10:43:50.894426 on 03/22/2001
Latest such alert at 10:59:47.384457 on 03/22/2001

<table>
<thead>
<tr>
<th>Source</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Dsts (sig)</th>
<th># Dsts (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>999.999.179.78</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destinations</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srs (sig)</th>
<th># Srs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.13.123.8</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Threat/Vulnerabilities: A host inside your network is accessing the spooler port of a host outside of your network; though this could be normal it could also be an indication of an unauthorized transfer to data or the presence of a tool such as Netcat.

Correlations: [http://www.sans.org/y2k/practical/Loras_Evan_GCIA.doc](http://www.sans.org/y2k/practical/Loras_Evan_GCIA.doc)
top ten talkers involved in Detects

**Total Connections = 23,764**

<table>
<thead>
<tr>
<th>#Connections</th>
<th>Src IP</th>
<th>Dst IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>8926</td>
<td>63.121.232.185</td>
<td>999.999.221.198</td>
</tr>
<tr>
<td>6473</td>
<td>212.179.4.50</td>
<td>999.999.222.154</td>
</tr>
<tr>
<td>2160</td>
<td>212.179.127.41</td>
<td>999.999.156.55</td>
</tr>
<tr>
<td>*1502</td>
<td>10.0.0.1</td>
<td>10.255.255.255</td>
</tr>
<tr>
<td>1453</td>
<td>63.121.232.185</td>
<td>999.999.224.2</td>
</tr>
<tr>
<td>1082</td>
<td>212.179.72.226</td>
<td>999.999.201.238</td>
</tr>
<tr>
<td>831</td>
<td>212.179.28.66</td>
<td>999.999.219.14</td>
</tr>
<tr>
<td>502</td>
<td>129.2.225.92</td>
<td>128.183.7.7</td>
</tr>
<tr>
<td>452</td>
<td>209.150.227.153</td>
<td>999.999.224.2</td>
</tr>
<tr>
<td>*383</td>
<td>192.168.0.2</td>
<td>192.168.0.255</td>
</tr>
</tbody>
</table>

* These are internal private network addresses. They are generating bootp traffic.
81% of the total detects were generated by these top 10 hosts.

Top ten talkers involved in Scans

<table>
<thead>
<tr>
<th>Total Scans</th>
<th>Src IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>22269</td>
<td>193.251.27.118</td>
</tr>
<tr>
<td>19589</td>
<td>212.144.16.169</td>
</tr>
<tr>
<td>16860</td>
<td>999.999.220.42</td>
</tr>
<tr>
<td>14683</td>
<td>200.51.8.209</td>
</tr>
<tr>
<td>13326</td>
<td>999.999.221.198</td>
</tr>
<tr>
<td>10071</td>
<td>999.999.227.206</td>
</tr>
<tr>
<td>9978</td>
<td>999.999.224.2</td>
</tr>
<tr>
<td>7573</td>
<td>202.112.209.30</td>
</tr>
<tr>
<td>6374</td>
<td>999.999.218.86</td>
</tr>
<tr>
<td>5409</td>
<td>999.999.224.130</td>
</tr>
</tbody>
</table>

67% of the total scans originated from inside
33% of the total scans originated from outside
Whois info for 10 External Source Address

I selected these hosts because 8 of them were prime talkers involved in detects and the remaining 2 were primary participants in scanning activity.

<table>
<thead>
<tr>
<th>External IP Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>193.251,27.118*</td>
</tr>
<tr>
<td>212.144.16.169*</td>
</tr>
<tr>
<td>63.121.232.185</td>
</tr>
<tr>
<td>212.179.4.50</td>
</tr>
<tr>
<td>212.179.127.41</td>
</tr>
<tr>
<td>63.121.232.185</td>
</tr>
<tr>
<td>212.179.72.226</td>
</tr>
<tr>
<td>212.179.28.66</td>
</tr>
<tr>
<td>129.2.225.92</td>
</tr>
<tr>
<td>209.150.227.153</td>
</tr>
</tbody>
</table>
Whois: 193.251.27.118
inetnum: 193.251.0.0 - 193.251.95.255
netname: IP2000-ADSL-BAS
descr: France Telecom IP2000 ADSL BAS
descr: BAS for services FTI-1 and FTI-2
country: FR
admin-c: WITR1-RIPE
tech-c: WITR1-RIPE
status: ASSIGNED PA
remarks: for hacking, spamming or security problems send mail to
remarks: postmaster@wanadoo.fr AND abuse@wanadoo.fr
remarks: for ANY problem send mail to gestionip.ft@francetelecom.com
notify: gestionip.ft@francetelecom.com
mnt-by: FT-BRX
changed: gestionip.ft@francetelecom.fr 20000525
changed: gestionip.ft@francetelecom.fr 20001010
changed: gestionip.ft@francetelecom.com 20010510
source: RIPE

route: 193.251.0.0/18
descr: France Telecom
descr: RAIN-TRANSPAC
origin: AS3215
mnt-by: FT-BRX
changed: gestionip.ft@francetelecom.fr 20001026
source: RIPE

role: Wanadoo Interactive Technical Role
address: France Telecom Wanadoo Interactive
address: 41, rue Camille Desmoulins
address: 92442 ISSY LES MOULINEAUX Cedex
address: FR
phone: +33 1 41 33 39 00
fax-no: +33 1 41 33 39 01
e-mail: abuse@wanadoo.fr
e-mail: postmaster@wanadoo.fr
admin-c: FTI-RIPE
tech-c: TEFS1-RIPE
nic-hdl: WITR1-RIPE
notify: gestionip.ft@francetelecom.com
mnt-by: FT-BRX
changed: gestionip.ft@francetelecom.com 20010504
source: RIPE
**Whois: 212.144.16.169**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>inetnum</td>
<td>212.144.16.0 - 212.144.17.255</td>
</tr>
<tr>
<td>netname</td>
<td>O-TEL-O-IPBB</td>
</tr>
<tr>
<td>descr</td>
<td>o.tel.o GmbH</td>
</tr>
<tr>
<td>countrystatus</td>
<td>DE</td>
</tr>
<tr>
<td>country</td>
<td>DE</td>
</tr>
<tr>
<td>admin-c</td>
<td>RH10371-RIPE</td>
</tr>
<tr>
<td>tech-c</td>
<td>TW39-RIPE</td>
</tr>
<tr>
<td>status</td>
<td>ASSIGNED PA</td>
</tr>
<tr>
<td>notify</td>
<td><a href="mailto:hostmaster@o-tel-o.de">hostmaster@o-tel-o.de</a></td>
</tr>
<tr>
<td>mnt-by</td>
<td>OTELO-MNT</td>
</tr>
<tr>
<td>changed</td>
<td><a href="mailto:hostmaster@o-tel-o.de">hostmaster@o-tel-o.de</a> 20001107</td>
</tr>
<tr>
<td>changed</td>
<td><a href="mailto:hostmaster@o-tel-o.de">hostmaster@o-tel-o.de</a> 20010522</td>
</tr>
<tr>
<td>source</td>
<td>RIPE</td>
</tr>
<tr>
<td>route</td>
<td>212.144.0.0/16</td>
</tr>
<tr>
<td>descr</td>
<td>Mannesmann o.tel.o GmbH &amp; Co</td>
</tr>
<tr>
<td>descr</td>
<td>Germany</td>
</tr>
<tr>
<td>origin</td>
<td>AS3209</td>
</tr>
<tr>
<td>notify</td>
<td><a href="mailto:ip-registry@arcor.net">ip-registry@arcor.net</a></td>
</tr>
<tr>
<td>mnt-by</td>
<td>ARCOR-MNT</td>
</tr>
<tr>
<td>changed</td>
<td><a href="mailto:ip-registry@arcor.net">ip-registry@arcor.net</a> 20000103</td>
</tr>
<tr>
<td>source</td>
<td>RIPE</td>
</tr>
<tr>
<td>person</td>
<td>Ralf Haupt</td>
</tr>
<tr>
<td>address</td>
<td>o.tel.o GmbH</td>
</tr>
<tr>
<td>address</td>
<td>Deutz-Muehlheimer-Strasse 111</td>
</tr>
<tr>
<td>address</td>
<td>D-51063 Koeln</td>
</tr>
<tr>
<td>address</td>
<td>Germany</td>
</tr>
<tr>
<td>phone</td>
<td>+49 221 808 8682</td>
</tr>
<tr>
<td>fax-no</td>
<td>+49 221 808 7530</td>
</tr>
<tr>
<td>e-mail</td>
<td><a href="mailto:hostmaster@o-tel-o.de">hostmaster@o-tel-o.de</a></td>
</tr>
<tr>
<td>nic-hdl</td>
<td>RH10371-RIPE</td>
</tr>
<tr>
<td>notify</td>
<td><a href="mailto:hostmaster@o-tel-o.de">hostmaster@o-tel-o.de</a></td>
</tr>
<tr>
<td>mnt-by</td>
<td>OTELO-MNT</td>
</tr>
<tr>
<td>changed</td>
<td><a href="mailto:hostmaster@o-tel-o.de">hostmaster@o-tel-o.de</a> 20010424</td>
</tr>
<tr>
<td>source</td>
<td>RIPE</td>
</tr>
<tr>
<td>person</td>
<td>Thomas Weigel</td>
</tr>
<tr>
<td>address</td>
<td>Mannesmann o.tel.o GmbH</td>
</tr>
<tr>
<td>address</td>
<td>Deutz-Muehlheimer-Str. 111</td>
</tr>
<tr>
<td>address</td>
<td>D-51063 Koeln</td>
</tr>
<tr>
<td>address</td>
<td>Germany</td>
</tr>
<tr>
<td>phone</td>
<td>+49 221 808 8735</td>
</tr>
<tr>
<td>fax-no</td>
<td>+49 221 808 7984</td>
</tr>
<tr>
<td>e-mail</td>
<td><a href="mailto:thomas.weigel@o-tel-o.de">thomas.weigel@o-tel-o.de</a></td>
</tr>
<tr>
<td>nic-hdl</td>
<td>TW39-RIPE</td>
</tr>
<tr>
<td>notify</td>
<td><a href="mailto:guardian@xlink.net">guardian@xlink.net</a></td>
</tr>
<tr>
<td>mnt-by</td>
<td>XLINK-MNT</td>
</tr>
</tbody>
</table>
changed: nipper@xlink.net 19951206
changed: guardian@xlink.net 19960226
changed: guardian@xlink.net 19961108
changed: hostmaster@o-tel-o.de 19970512
changed: hostmaster@o-tel-o.de 19970804
changed: mlelstv@xlink.net 19980618
changed: guardian@xlink.net 20000111
changed: maier@xlink.net 20000529
source: RIPE
Whois: 63.121.232.185
UUNET Technologies, Inc. (NETBLK-UUNET63)
3060 Williams Drive, Suite 601
Fairfax, Virginia 22031
US
Netname: UUNET63
Netblock: 63.64.0.0 - 63.127.255.255
Maintainer: UU
Coordinator:
  UUNET, Technical Support (OA12-ARIN) help@uu.net
  (800) 900-0241
Domain System inverse mapping provided by:
AUTH03.NS.UU.NET 198.6.1.83
AUTH00.NS.UU.NET 198.6.1.65
ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

----------
Sigecom (NETBLK-UU-63-121-232)
6045 Wedeking Avenue
Evansville, IN 47715
US
Netname: UU-63-121-232
Netblock: 63.121.232.0 - 63.121.239.255
Maintainer: SIGE
Coordinator:
  Wilkison, Chris (CW471-ARIN) cwilkison@sigecom.net
  812-437-0530
Whois: 212.179.4.50
inetnum: 212.179.4.48 - 212.179.4.63
netname: SCP-SYSTEMS-LTD
descr: SCP-SYSTEMS-LAN
country: IL
admin-c: ES4966-RIPE
tech-c: NP469-RIPE
status: ASSIGNED PA
notify: hostmaster@isdn.net.il
mnt-by: RIPE-NCC-NONE-MNT
changed: hostmaster@isdn.net.il 20000628
source: RIPE

derect: 212.179.0.0/17
descr: ISDN Net Ltd.
origin: AS8551
notify: hostmaster@isdn.net.il
mnt-by: AS8551-MNT
changed: hostmaster@isdn.net.il 19990610
source: RIPE

person: Eran Shchori
address: BEZEQ INTERNATIONAL
address: 40 Hashacham Street
address: Petach-Tikva 49170 Israel
phone: +972 3 9257710
fax-no: +972 3 9257726
e-mail: hostmaster@bezeqint.net
nic-hdl: ES4966-RIPE
changed: registrar@ns.il 20000309
source: RIPE

person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: NP469-RIPE
changed: registrar@ns.il 19990902
source: RIPE
Whois: 212.179.127.41
inetnum: 212.179.127.0 - 212.179.127.127
netname: ARAVA-DEVELOPMENT-COMPANY-LTD
descr: ARAVA-DEVELOPMENT-LAN
country: IL
admin-c: ES4966-RIPE
tech-c: NP469-RIPE
status: ASSIGNED PA
notify: hostmaster@isdn.net.il
mnt-by: RIPE-NCC-NONE-MNT
changed: hostmaster@isdn.net.il 20000525
source: RIPE

route: 212.179.0.0/17
descr: ISDN Net Ltd.
origin: AS8551
notify: hostmaster@isdn.net.il
mnt-by: AS8551-MNT
changed: hostmaster@isdn.net.il 19990610
source: RIPE

do a person: Eran Shchori
address: BEZEQ INTERNATIONAL
address: 40 Hashacham Street
address: Petach-Tikva 49170 Israel
phone: +972 3 9257710
fax-no: +972 3 9257726
e-mail: hostmaster@bezeqint.net
nic-hdl: ES4966-RIPE
changed: registrar@ns.il 20000309
source: RIPE

do a person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: NP469-RIPE
changed: registrar@ns.il 19990902
source: RIPE
**Whois: 63.121.232.185**
UUNET Technologies, Inc. (NETBLK-UUNET63)
3060 Williams Drive, Suite 601
Fairfax, Virginia 22031
US
Netname: UUNET63
Netblock: 63.64.0.0 - 63.127.255.255
Maintainer: UU
Coordinator:
   UUNET, Technical Support (OA12-ARIN) help@uu.net
   (800) 900-0241

Domain System inverse mapping provided by:

   AUTH03.NS.UU.NET   198.6.1.83
   AUTH00.NS.UU.NET   198.6.1.65

**ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE**
-----------
Sigecom (NETBLK-UU-63-121-232)
6045 Wedeking Avenue
Evansville, IN 47715
US

Netname: UU-63-121-232
Netblock: 63.121.232.0 - 63.121.239.255
Maintainer: SIGE

Coordinator:
   Wilkison, Chris (CW471-ARIN) cwilkison@sigecom.net
   812-437-0530
Whois: 212.179.72.226
inetnum: 212.179.72.224 - 212.179.72.239
netname: KESHET
descr: KESHET-LAN
country: IL
admin-c: ES4966-RIPE
tech-c: NP469-RIPE
status: ASSIGNED PA
notify: hostmaster@isdn.net.il
mnt-by: RIPE-NCC-NONE-MNT
changed: hostmaster@isdn.net.il 20000320
source: RIPE

route: 212.179.0.0/17
descr: ISDN Net Ltd.
origin: AS8551
notify: hostmaster@isdn.net.il
mnt-by: AS8551-MNT
changed: hostmaster@isdn.net.il 19990610
source: RIPE

person: Eran Shchori
address: BEZEQ INTERNATIONAL
address: 40 Hashacham Street
address: Petach-Tikva 49170 Israel
phone: +972 3 9257710
fax-no: +972 3 9257726
e-mail: hostmaster@bezeqint.net
nic-hdl: ES4966-RIPE
changed: registrar@ns.il 20000309
source: RIPE

person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: NP469-RIPE
changed: registrar@ns.il 19990902
source: RIPE
Whois: 212.179.28.66
inetnum: 212.179.28.64 - 212.179.28.127
netname: VSOFT
descr: VSOFT-LAN
country: IL
admin-c: NP469-RIPE
tech-c: NP469-RIPE
status: ASSIGNED PA
notify: hostmaster@isdn.net.il
mnt-by: RIPE-NCC-NONE-MNT
changed: hostmaster@isdn.net.il 20000106
source: RIPE

route: 212.179.0.0/17
descr: ISDN Net Ltd.
origin: AS8551
notify: hostmaster@isdn.net.il
mnt-by: AS8551-MNT
changed: hostmaster@isdn.net.il 19990610
source: RIPE

person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: NP469-RIPE
changed: registrar@ns.il 19990902
source: RIPE
Whois: 129.2.225.92
University of Maryland (NET-UMD-BOGON-NET)
  Network Operations Center Bldg 224, Room 1301
  College Park, MD 20742
  US
  Netname: UMD-BOGON-NET
  Netblock: 129.2.0.0 - 129.2.255.255
  Coordinator:
   University of Maryland DNS Administration  (UM-ORG-ARIN)
   dnsadmin@NOC.UMD.EDU
   (301) 405-3003
  Domain System inverse mapping provided by:

  NOC.UMD.EDU       128.8.5.2
  NS1.UMD.EDU       128.8.74.2
  NS2.UMD.EDU       128.8.76.2
**Whois: 209.150.227.153**
Clarity Connect Inc (NETBLK-CCI-NETWORK)
  200 Pleasant Grove Road
  Ithaca, NY 14850
  US

Netname: CCI-NETWORK
Netblock: 209.150.224.0 - 209.150.255.255
Maintainer: CLCO

Coordinator:
  Lalley, Joseph (JL583-ARIN) lalley@CLARITYCONNECT.COM
  607-257-8596

Domain System inverse mapping provided by:

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS1.CLARITYCONNECT.COM</td>
<td>206.64.143.2</td>
</tr>
<tr>
<td>NS2.CLARITYCONNECT.COM</td>
<td>206.64.143.10</td>
</tr>
</tbody>
</table>
Scan Activity Analysis

- The biggest offender from inside your network was host 999.999.220.42 with 16,860 connections. Further investigation of the combined scans file using MS-Excel revealed that on March 22nd between the hours of 20:00 and 22:00 host 999.999.220.42 was scanning a lot of hosts. I also noticed that the source port was unchanging (port 9737). The destination ports ranged from 9017 – 9897. This could be an indication that some automated scanning tool such as Nessus was running.
- 67% of the scan activity originated from inside your network.
- 3% of the scan activity originated from outside your network.
- There was a high volume of scanning activity on March 31st. That was a Saturday and it is obvious that the attackers took advantage of the fact that most CERT teams operate at a reduced staffing level on weekends.
- March 31st beginning at midnight, host 195.22.0.154 started a telnet scan to multiple hosts in your network on subnets 206 – 214, 218 – 222, and 224 – 230.
- These are crafted packets scanning for FTP, HTTP, POP2, DNS, SUNRPC services. Attackers often set both the SYN and FIN flags in an attempt to get through firewalls.

Mar 31 00:05:54 211.178.63.4:21 -> 999.999.132.34:21 SYNFIN **SF****
Mar 31 00:06:07 211.178.63.4:8080 -> 999.999.130.34:8080 SYNFIN **SF****
Mar 31 00:06:50 211.178.63.4:21 -> 999.999.143.34:21 SYNFIN **SF****
Mar 31 00:08:42 211.178.63.4:21 -> 999.999.165.34:21 SYNFIN **SF****
Mar 31 00:08:58 211.178.63.4:109 -> 999.999.170.34:109 SYNFIN **SF****
Mar 31 00:10:09 211.178.63.4:21 -> 999.999.182.34:21 SYNFIN **SF****
Mar 31 00:11:47 211.178.63.4:109 -> 999.999.203.34:109 SYNFIN **SF****
Mar 31 00:12:41 211.178.63.4:53 -> 999.999.210.34:53 SYNFIN **SF****
Mar 31 00:14:34 211.178.63.4:53 -> 999.999.232.34:53 SYNFIN **SF****
Mar 31 00:21:27 211.178.63.4:21 -> 999.999.60.35:21 SYNFIN **SF****
Mar 31 00:27:44 211.178.63.4:111 -> 999.999.133.35:111 SYNFIN **SF****
Mar 31 00:29:42 211.178.63.4:21 -> 999.999.157.35:21 SYNFIN **SF****
Mar 31 00:30:25 211.178.63.4:8080 -> 999.999.161.35:8080 SYNFIN **SF****

- The hostile was conducting reconnaissance the entire class “B” network searching for DNS servers possibly for later targeting with an exploit. **This source IP is registered to a Denmark address.**

Mar 31 00:39:37 195.41.102.2:2073 -> 999.999.1.52:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2120 -> 999.999.1.99:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2125 -> 999.999.1.104:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2137 -> 999.999.1.116:53 SYN **S*****
Janice Y. Slocumb  GCIA Practical Assignment Version 2.9

Mar 31 00:39:38 195.41.102.2:2140 -> 999.999.1.119:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2141 -> 999.999.1.120:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2146 -> 999.999.1.125:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2154 -> 999.999.1.133:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2176 -> 999.999.1.155:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2178 -> 999.999.1.157:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2184 -> 999.999.1.163:53 SYN **S*****
Mar 31 00:39:38 195.41.102.2:2190 -> 999.999.1.169:53 SYN **S*****

Mar 31 00:56:06 195.41.102.2:1548 -> 999.999.154.247:53 SYN **S*****
Mar 31 00:56:06 195.41.102.2:1550 -> 999.999.154.249:53 SYN **S*****
Mar 31 00:56:07 195.41.102.2:1576 -> 999.999.155.20:53 SYN **S*****
Mar 31 00:56:07 195.41.102.2:1580 -> 999.999.155.24:53 SYN **S*****
Mar 31 00:56:07 195.41.102.2:1650 -> 999.999.155.94:53 SYN **S*****
Mar 31 00:56:07 195.41.102.2:1654 -> 999.999.155.98:53 SYN **S*****
Mar 31 00:56:07 195.41.102.2:1658 -> 999.999.155.102:53 SYN **S*****
Mar 31 00:56:07 195.41.102.2:1690 -> 999.999.155.134:53 SYN **S*****
Mar 31 00:56:07 195.41.102.2:1701 -> 999.999.155.145:53 SYN **S*****

• Continuing reconnaissance for DNS service.

Mar 31 01:19:51 209.116.250.194:2380 -> 999.999.1.17:53 SYN **S*****
Mar 31 01:19:52 209.116.250.194:2403 -> 999.999.1.40:53 SYN **S*****
Mar 31 01:19:52 209.116.250.194:2409 -> 999.999.1.46:53 SYN **S*****
Mar 31 01:19:52 209.116.250.194:2414 -> 999.999.1.51:53 SYN **S*****
Mar 31 01:19:52 209.116.250.194:2413 -> 999.999.1.50:53 SYN **S*****
Mar 31 01:19:52 209.116.250.194:2416 -> 999.999.1.53:53 SYN **S*****
Mar 31 01:19:52 209.116.250.194:2472 -> 999.999.1.109:53 SYN **S*****
Mar 31 01:19:52 209.116.250.194:2479 -> 999.999.1.116:53 SYN **S*****
Mar 31 01:19:53 209.116.250.194:2552 -> 999.999.1.189:53 SYN **S*****
Mar 31 01:19:53 209.116.250.194:2551 -> 999.999.1.188:53 SYN **S*****
Mar 31 01:19:53 209.116.250.194:2554 -> 999.999.1.191:53 SYN **S*****
Mar 31 01:19:53 209.116.250.194:2556 -> 999.999.1.193:53 SYN **S*****
Mar 31 01:19:54 209.116.250.194:2370 -> 999.999.1.7:53 SYN **S*****
Mar 31 01:19:55 209.116.250.194:2390 -> 999.999.1.27:53 SYN **S*****
Mar 31 01:19:55 209.116.250.194:2400 -> 999.999.1.37:53 SYN **S*****
Mar 31 01:19:55 209.116.250.194:2484 -> 999.999.1.121:53 SYN **S*****

• A host inside your network was scanning for **DMSsetup Trojan**. This activity continued until 19:56:06.

Mar 31 01:47:44 999.999.221.26:60148 -> 217.68.101.100:59 SYN **S*****
Mar 31 01:47:44 999.999.221.26:60272 -> 24.108.111.232:59 SYN **S*****
Mar 31 01:47:46 999.999.221.26:8150 -> 24.66.132.216:59 SYN **S*****
Mar 31 01:47:46 999.999.221.26:17909 -> 12.21.214.85:59 SYN **S*****
Hostile searching for Unix boxes running SUNRPC services.

Continuing reconnaissance for DNS service. The source IP is registered to a Chinese address.
Janice Y. Slocumb  
GCIA Practical Assignment Version 2.9

- Host inside looking for MP3 services (Gnutella port 6346, Kazaa prot 1214)

Mar 31 07:20:03 999.999.227.130:3147 -> 199.8.9.49:6346 SYN **S*****
Mar 31 07:20:03 999.999.227.130:3149 -> 24.16.148.124:6346 SYN **S*****
Mar 31 07:20:03 999.999.227.130:3151 -> 213.213.36.7:6346 SYN **S*****
Mar 31 07:20:03 999.999.227.130:3150 -> 130.132.70.123:6346 SYN **S*****
Mar 31 07:20:03 999.999.227.130:3152 -> 24.170.100.47:6346 SYN **S*****
Mar 31 07:20:03 999.999.227.130:3153 -> 172.173.44.248:6346 SYN **S*****
Mar 31 07:20:03 999.999.227.130:3156 -> 63.202.80.2:6346 SYN **S*****
Mar 31 07:20:03 999.999.227.130:3158 -> 63.173.98.100:6347 SYN **S*****

Mar 31 13:20:11 999.999.215.18:1599 -> 63.88.159.93:1214 SYN **S*****
Mar 31 13:20:11 999.999.215.18:1655 -> 62.46.98.110:1214 SYN **S*****
Mar 31 13:20:12 999.999.215.18:1660 -> 138.234.87.69:1214 SYN **S*****
Mar 31 13:20:12 999.999.215.18:1605 -> 138.234.185.51:1214 SYN **S*****

Mar 31 23:11:55 999.999.209.50:3569 -> 194.95.170.157:1214 SYN **S*****
Mar 31 23:11:55 999.999.209.50:3585 -> 193.40.254.184:1214 SYN **S*****
Mar 31 23:11:55 999.999.209.50:3542 -> 59.183.220.47:11024 SYN **S*****
Mar 31 23:11:55 999.999.209.50:3591 -> 62.178.117.106:6347 SYN **S*****
Mar 31 23:11:57 999.999.209.50:3595 -> 169.237.58.33:1214 SYN **S*****

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.
Janice Y. Slocumb

Mar 31 23:11:57 999.999.209.50:3578 -> 136.165.138.205:1214 SYN **S*****
Mar 31 23:11:57 999.999.209.50:3584 -> 138.234.67.208:1214 SYN **S*****
Mar 31 23:11:59 999.999.209.50:3599 -> 137.48.135.8:1214 SYN **S*****

......

Mar 26 02:29:34 999.999.209.30:4191 -> 167.206.191.134:6346 SYN **S*****
Mar 26 02:29:34 999.999.209.30:4189 -> 216.93.96.188:6346 SYN **S*****
Mar 26 02:29:37 999.999.209.30:4197 -> 64.230.85.231:6346 SYN **S*****
Mar 26 02:29:34 999.999.209.30:4198 -> 64.230.0.138:6346 SYN **S*****

• Hostile scanning for spooler services possibly looking for exploitable spooler services.

Mar 31 19:02:30 999.999.205.162:3139 -> 146.186.232.166:1214 SYN **S*****
Mar 31 19:02:30 999.999.205.162:3059 -> 138.234.67.207:1214 SYN **S*****
Mar 31 19:02:31 999.999.205.162:3153 -> 129.74.170.114:1214 SYN **S*****
Mar 31 19:02:32 999.999.205.162:3168 -> 24.88.154.189:1214 SYN **S*****
Mar 31 19:02:33 999.999.205.162:3175 -> 24.130.188.80:1214 SYN **S*****
Mar 31 19:02:33 999.999.205.162:3087 -> 24.201.72.177:1214 SYN **S*****
Mar 31 19:02:34 999.999.205.162:3090 -> 213.44.202.199:1214 SYN **S*****
Mar 31 19:02:34 999.999.205.162:3179 -> 24.115.162.148:1214 SYN **S*****
Mar 31 19:02:34 999.999.205.162:3180 -> 138.234.146.35:1214 SYN **S*****

• Hostile scanning for SubSeven, SubSeven Apocalypse, or BackDoor-G

Mar 31 13:35:50 207.124.229.123:3636 -> 999.999.132.251:515 SYN **S*****
Mar 31 13:35:51 207.124.229.123:3575 -> 999.999.132.190:515 SYN **S*****
Mar 31 13:35:52 207.124.229.123:3600 -> 999.999.132.215:515 SYN **S*****
Mar 31 13:35:52 207.124.229.123:3604 -> 999.999.132.219:515 SYN **S*****
Mar 31 13:35:52 207.124.229.123:4121 -> 999.999.134.226:515 SYN **S*****
Mar 31 13:35:52 207.124.229.123:4123 -> 999.999.134.228:515 SYN **S*****
Mar 31 13:35:52 207.124.229.123:4127 -> 999.999.134.232:515 SYN **S*****
Mar 31 13:35:52 207.124.229.123:4133 -> 999.999.134.238:515 SYN **S*****
Mar 31 13:35:52 207.124.229.123:4135 -> 999.999.134.240:515 SYN **S*****

© SANS Institute 2000 - 2002
As part of GIAC practical repository.
Author retains full rights.
Automated multi-port scan of lone host. The source IP is registered to an address in the Netherlands.

Hostile performing scan of the class “B” network via crafted packets, note the source and destination ports are the same and both the SYN and FIN flags are set. This was a low and slow scan that continued until 23:58:36.
Mar 31 00:10:09 211.178.63.4:21 -> 999.999.182.34:21 SYNFN **SF****
Mar 31 00:11:47 211.178.63.4:109 -> 999.999.203.34:109 SYNFN **SF****
Mar 31 00:12:41 211.178.63.4:53 -> 999.999.210.34:53 SYNFN **SF****
Mar 31 00:14:34 211.178.63.4:53 -> 999.999.232.34:53 SYNFN **SF****
Mar 31 00:21:27 211.178.63.4:21 -> 999.999.60.35:21 SYNFN **SF****
Mar 31 00:27:44 211.178.63.4:109 -> 999.999.133.35:109 SYNFN **SF****
Mar 31 00:29:42 211.178.63.4:53 -> 999.999.157.35:53 SYNFN **SF****

• Hostile scanning for FTP servers. The source IP is registered to a German address. This activity could be a precursor to further hostile activity.

Mar 31 14:31:10 217.85.227.219:4536 -> 999.999.1.72:21 SYN **S*****
Mar 31 14:31:10 217.85.227.219:4539 -> 999.999.1.75:21 SYN **S*****
Mar 31 14:31:12 217.85.227.219:4490 -> 999.999.1.26:21 SYN *********
Mar 31 14:31:12 217.85.227.219:4522 -> 999.999.1.58:21 SYN *********
Mar 31 14:31:12 217.85.227.219:4532 -> 999.999.1.68:21 SYN *********
Mar 31 14:31:12 217.85.227.219:4500 -> 999.999.1.36:21 SYN *********

• Host on your network scanning for TransScout, Insane Network 4, Millennium

Mar 31 17:00:49 999.999.227.162:37770 -> 24.31.244.33:2000 SYN **S*****
Mar 31 17:00:49 999.999.227.162:39520 -> 172.136.52.24:2000 SYN **S*****
Mar 31 17:00:49 999.999.227.162:44770 -> 24.17.187.55:2000 SYN **S*****
Mar 31 17:00:49 999.999.227.162:46330 -> 24.214.101.119:2000 SYN **S*****
Mar 31 17:00:49 999.999.227.162:53430 -> 24.22.218.4:2000 SYN **S*****
Mar 31 17:00:50 999.999.227.162:41680 -> 65.80.14.120:2000 SYN **S*****
Mar 31 17:00:51 999.999.227.162:35660 -> 172.155.192.4:2000 SYN *********
Mar 31 17:00:51 999.999.227.162:51230 -> 64.231.82.228:2000 SYN **S*****
Mar 31 17:00:52 999.999.227.162:47620 -> 172.150.137.69:2000 SYN **S*****
Mar 31 17:00:52 999.999.227.162:48740 -> 64.228.91.64:2000 SYN **S*****
Mar 31 17:00:52 999.999.227.162:47550 -> 209.233.30.67:2000 SYN **S*****
Mar 31 17:00:58 999.999.227.162:32650 -> 172.155.174.151:2000 SYN **S*****
• Hostile scan for DNS servers originating from a host registered to a Polish address.

Mar 31 18:56:42 212.87.234.136:3548 -> 999.999.1.25:53 SYN **S*****
Mar 31 18:56:42 212.87.234.136:3549 -> 999.999.1.26:53 SYN **S*****
Mar 31 18:56:42 212.87.234.136:3550 -> 999.999.1.27:53 SYN **S*****
Mar 31 18:56:42 212.87.234.136:3558 -> 999.999.1.35:53 SYN **S*****
Mar 31 18:56:43 212.87.234.136:3583 -> 999.999.1.4:53 SYN **S****
Mar 31 18:56:43 212.87.234.136:3585 -> 999.999.1.9:53 SYN **S*****
Mar 31 18:56:45 212.87.234.136:3543 -> 999.999.1.20:53 SYN **S*****
Mar 31 18:56:45 212.87.234.136:3544 -> 999.999.1.21:53 SYN **S*****
Mar 31 18:56:49 212.87.234.136:3592 -> 999.999.1.64:53 SYN **S*****
Mar 31 18:56:49 212.87.234.136:3592 -> 999.999.1.127:53 SYN **S*****

• Hostile scanning for Telnet servers. This is possibly a precursor to further hostile activity. The source IP is registered to a Portuguese address.

Mar 31 20:08:04 195.22.0.154:4334 -> 999.999.53.13:23 SYN **S*****
Mar 31 20:08:04 195.22.0.154:1038 -> 999.999.53.23:23 SYN **S*****
Mar 31 20:08:04 195.22.0.154:1045 -> 999.999.53.59:23 SYN **S*****
Mar 31 20:08:04 195.22.0.154:1047 -> 999.999.53.63:23 SYN **S*****
Mar 31 20:08:04 195.22.0.154:1049 -> 999.999.53.61:23 SYN **S*****
Mar 31 20:08:05 195.22.0.154:1066 -> 999.999.53.79:23 SYN **S*****
Mar 31 20:08:06 195.22.0.154:1090 -> 999.999.53.96:23 SYN **S*****
Mar 31 20:08:06 195.22.0.154:1104 -> 999.999.53.108:23 SYN **S*****
Mar 31 20:08:06 195.22.0.154:1107 -> 999.999.53.110:23 SYN **S*****
Mar 31 20:08:10 195.22.0.154:1109 -> 999.999.53.112:23 SYN **S*****
Mar 31 20:08:10 195.22.0.154:1799 -> 999.999.53.156:23 SYN **S*****
Mar 31 20:08:11 195.22.0.154:1826 -> 999.999.53.176:23 SYN **S*****
Mar 31 20:08:11 195.22.0.154:1127 -> 999.999.53.126:23 SYN **S*****
Mar 31 20:08:11 195.22.0.154:1849 -> 999.999.53.194:23 SYN **S*****
Mar 31 20:08:12 195.22.0.154:1852 -> 999.999.53.196:23 SYN **S*****
Mar 31 20:08:12 195.22.0.154:1857 -> 999.999.53.201:23 SYN **S*****
Mar 31 20:08:12 195.22.0.154:1862 - 999.999.53.205:23 SYN **S*****
Mar 31 20:08:12 195.22.0.154:1879 - 999.999.53.219:23 SYN **S*****
Mar 31 20:08:13 195.22.0.154:1809 - 999.999.53.161:23 SYN **S*****

- Inside hosts scanning for NewsEDGE server TCP (TCP 1), Unreal Admin Webserver, Ultima Online, mIRC, or NewsEDGE server TCP (TCP 1) / external shell (test).

Mar 31 20:51:11 999.999.204.26:4134 - 63.196.54.13:8888 SYN **S*****
Mar 31 20:51:12 999.999.204.26:4138 - 63.196.54.18:8888 SYN **S*****
Mar 31 20:51:12 999.999.204.26:4139 - 63.196.54.4:8888 SYN **S*****
Mar 31 20:51:12 999.999.204.26:4144 - 63.196.54.35:8888 SYN **S*****
Mar 31 20:51:12 999.999.204.26:4145 - 63.196.54.38:8888 SYN **S*****
Mar 31 20:51:12 999.999.204.26:4151 - 63.196.54.23:8888 SYN **S*****
Mar 31 20:51:13 999.999.204.26:4154 - 63.196.54.22:8888 SYN **S*****
Mar 31 20:51:13 999.999.204.26:4156 - 217.3.91.95:8888 SYN **S*****

- Automated multi-port scan of lone host. The source IP is registered to an address in the Philippians.

Mar 31 22:01:11 210.23.241.119:4371 - 999.999.97.77:12345 SYN **S*****
Mar 31 22:01:11 210.23.241.119:4376 - 999.999.97.77:20034 SYN **S*****
Mar 31 22:01:11 210.23.241.119:4377 - 999.999.97.77:5400 SYN **S*****
Mar 31 22:01:11 210.23.241.119:4381 - 999.999.97.77:9872 SYN **S*****
Mar 31 22:01:11 210.23.241.119:4382 - 999.999.97.77:20000 SYN **S*****
Mar 31 22:01:11 210.23.241.119:4384 - 999.999.97.77:7307 SYN **S*****

- Hostile searching for Unix boxes running SUNRPC services.

Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.110:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.116:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.138:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.142:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.144:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.146:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.148:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.150:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.156:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.170:111 SYN **S*****
Mar 31 23:17:26 209.217.53.190:111 - 999.999.132.172:111 SYN **S*****

- Hostile scanning for SMTP servers. This could be a precursor to an exploit attempt. The source IP is registered to an Australian address. This activity continued until 02:05.
Janice Y. Slocumb

GCIA Practical Assignment Version 2.9

Mar 26 00:38:53 203.89.246.250:2977 -> 999.999.1.106:25 SYN **S*****
Mar 26 00:38:53 203.89.246.250:2973 -> 999.999.1.102:25 SYN **S*****
Mar 26 00:38:53 203.89.246.250:2945 -> 999.999.1.74:25 SYN **S*****
Mar 26 00:38:53 203.89.246.250:2933 -> 999.999.1.62:25 SYN **S*****
Mar 26 00:38:53 203.89.246.250:2931 -> 999.999.1.60:25 SYN **S*****
Mar 26 00:38:53 203.89.246.250:2927 -> 999.999.1.56:25 SYN **S*****
Mar 26 00:38:53 203.89.246.250:2925 -> 999.999.1.54:25 SYN **S*****
Mar 26 00:38:53 203.89.246.250:2921 -> 999.999.1.50:25 SYN **S*****

......

Mar 26 02:05:29 203.89.246.250:1344 -> 999.999.254.225:25 SYN **S*****
Mar 26 02:05:29 203.89.246.250:1346 -> 999.999.254.227:25 SYN **S*****
Mar 26 02:05:29 203.89.246.250:1348 -> 999.999.254.229:25 SYN **S*****
Mar 26 02:05:29 203.89.246.250:1350 -> 999.999.254.231:25 SYN **S*****
Mar 26 02:05:29 203.89.246.250:1352 -> 999.999.254.233:25 SYN **S*****
Mar 26 02:05:29 203.89.246.250:1368 -> 999.999.254.249:25 SYN **S*****

• Host from the Philippians looking for NetBus 2 Pro **inside host may be compromised**
Mar 31 22:01:11 210.23.241.119:4377 -> 999.999.97.77:20034 SYN **S*****

• Scanning for NetBus 2 Pro on a host in registered to a Netherland address.
Mar 26 03:00:56 999.999.204.26:4520 -> 212.204.216.51:20034 SYN **S*****
Mar 26 03:35:43 999.999.204.26:1228 -> 212.204.216.51:20034 SYN **S*****
Mar 26 04:00:38 999.999.204.26:1671 -> 212.204.216.51:20034 SYN **S*****
Mar 26 06:26:07 999.999.204.26:4589 -> 212.204.216.51:20034 SYN **S*****

• Inside host scanning for most likely a web server.
Mar 26 03:00:58 999.999.204.26:4522 -> 63.161.255.184:8888 SYN **S*****
Mar 26 03:00:58 999.999.204.26:4524 -> 65.33.65.240:8888 SYN **S*****
Mar 26 03:01:01 999.999.204.26:4524 -> 65.33.65.240:8888 SYN **S*****
Mar 26 03:30:32 999.999.204.26:1101 -> 63.196.54.11:8888 SYN **S*****
Mar 26 03:30:33 999.999.204.26:1103 -> 63.196.54.20:8888 SYN **S*****
Mar 26 03:30:33 999.999.204.26:1105 -> 63.196.54.19:8888 SYN **S*****
Mar 26 03:30:33 999.999.204.26:1106 -> 63.196.54.4:8888 SYN **S*****
Mar 26 03:30:33 999.999.204.26:1108 -> 63.196.54.15:8888 SYN **S*****
Mar 26 03:30:33 999.999.204.26:1113 -> 63.196.54.17:8888 SYN **S*****
Mar 26 03:30:33 999.999.204.26:1114 -> 63.196.54.34:8888 SYN **S*****
Mar 26 03:30:34 999.999.204.26:1124 -> 63.196.54.28:8888 SYN **S*****
Mar 26 03:35:41 999.999.204.26:1202 -> 63.196.54.19:8888 SYN **S*****
Mar 26 03:35:42 999.999.204.26:1203 -> 63.196.54.4:8888 SYN **S*****
Mar 26 03:35:43 999.999.204.26:1225 -> 63.196.54.21:8888 SYN **S*****
Mar 26 03:35:43 999.999.204.26:1226 -> 216.138.208.138:8888 SYN **S*****
Mar 26 03:35:43 999.999.204.26:1228 -> 212.204.216.51:20034 SYN **S*****
Mar 26 04:00:37 999.999.204.26:1651 -> 63.196.54.14:8888 SYN **S*****

- Inside host scanning for Diablo 2 (game)

Mar 26 04:59:14 999.999.253.24:34825 -> 204.127.134.16:25 SYN **S*****
Mar 26 04:59:15 999.999.253.24:34829 -> 204.127.134.18:25 SYN **S*****
Mar 26 04:59:15 999.999.253.24:34832 -> 192.28.4.11:25 SYN **S*****
Mar 26 04:59:15 999.999.253.24:34833 -> 206.46.170.43:25 SYN **S*****
Mar 26 04:59:15 999.999.253.24:34835 -> 131.96.5.77:25 SYN **S*****
Mar 26 04:59:16 999.999.253.24:34837 -> 32.97.166.40:25 SYN **S*****
Mar 26 04:59:16 999.999.253.24:34810 -> 208.200.190.6:25 SYN **S*****
Mar 26 04:59:17 999.999.253.24:34832 -> 194.75.152.225:25 SYN **S*****
Mar 26 04:59:17 999.999.253.24:34845 -> 64.12.136.57:25 SYN **S*****

- Inside host scanning for SMTP servers.

Mar 26 06:26:42 61.129.39.161:1408 -> 999.999.132.20:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1405 -> 999.999.132.17:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1406 -> 999.999.132.18:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1416 -> 999.999.132.28:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1419 -> 999.999.132.31:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1410 -> 999.999.132.22:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1414 -> 999.999.132.26:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1426 -> 999.999.132.38:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1431 -> 999.999.132.43:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1430 -> 999.999.132.42:111 SYN **S*****
Mar 26 06:26:42 61.129.39.161:1429 -> 999.999.132.41:111 SYN **S*****
Mar 26 06:26:43 61.129.39.161:1466 -> 999.999.132.78:111 SYN **S*****
Mar 26 06:26:43 61.129.39.161:1468 -> 999.999.132.80:111 SYN **S*****
Mar 26 06:26:43 61.129.39.161:1477 -> 999.999.132.89:111 SYN **S*****
Mar 26 06:26:43 61.129.39.161:1489 -> 999.999.132.101:111 SYN **S*****
Mar 26 06:26:43 61.129.39.161:1490 -> 999.999.132.102:111 SYN **S*****

- Hostile scanning for SUNRPC service. The source IP is registered to a Chinese address.

Mar 26 02:00:37 999.999.204.26:1651 -> 63.196.54.14:8888 SYN **S*****
• Inside host doing multi-port scan with attack ports intermingled. Often attackers use this method to hide their presence. (sadmind)


http://www.sans.org/infosecFAQ/malicious/cmsd.htm. This is very likely a compromised host.

Worm
Mar 26 19:26:11 999.999.5.54:3240 -> 65.9.248.100:282 SYN **S*****
Mar 26 19:26:11 999.999.5.54:3240 -> 65.9.248.100:755 SYN **S*****
Mar 26 19:26:11 999.999.5.54:3252 -> 65.9.248.100:262 SYN **S*****
Mar 26 19:26:11 999.999.5.54:3253 -> 65.9.248.100:575 SYN **S*****
Mar 26 19:26:12 999.999.5.54:3341 -> 65.9.248.100:1008 SYN **S***** Lion

Trojan Horse
Mar 26 19:28:55 999.999.5.54:1143 -> 65.9.248.100:693 SYN **S*****
Mar 26 19:28:55 999.999.5.54:1145 -> 65.9.248.100:27665 SYN **S***** Trin00

slave port
Mar 26 19:28:55 999.999.5.54:1164 -> 65.9.248.100:920 SYN **S*****

- Internal host looking for Trin00 slave. This may be a trin00 master, **compromised host**.

Mar 22 10:43:52 999.999.179.78:3607 -> 24.13.2766:27665 SYN **S*****

- Internal host appears to be offering an NFS services to foreign hosts in places like Germany, the Netherlands, Great Britain coupled with the fact that this activity is occurring on a Saturday. This is very likely a **compromised host**.

Mar 31 14:23:32 999.999.204.202:2000 -> 212.137.72.48:7858 UDP
Mar 31 14:24:13 999.999.204.202:2000 -> 12.47.50.159:7778 UDP
Mar 31 14:24:18 999.999.204.202:2000 -> 130.236.146.82:14001 UDP
Mar 31 14:24:29 999.999.204.202:2000 -> 203.164.3.201:20341 UDP
Mar 31 14:24:34 999.999.204.202:2000 -> 207.98.129.241:7778 UDP
Mar 31 14:24:36 999.999.204.202:2000 -> 128.2.22.21:7778 UDP
Mar 31 14:24:54 999.999.204.202:2000 -> 209.61.204.11:7798 UDP
Mar 31 14:24:54 999.999.204.202:2000 -> 152.2.217.245:7778 UDP
Mar 31 14:42:01 217.85.227.219:2000 -> 999.999.53.36:21 SYN **S*****

.....

Mar 31 19:29 999.999.206.2:2000 -> 249.5.227.74:7778 UDP

.....

Mar 31 19:34:53 999.999.209.82:2000 -> 194.185.88.48:8601 UDP
Mar 31 19:35:01 999.999.209.82:2000 -> 208.185.73.201:7778 UDP

.....

- ICQ traffic originating from within your network.

Mar 26 12:17:47 999.999.227.26:1580 -> 212.137.72.20:40000 UDP
Janice Y. Slocumb

Mar 26 14:36:05 999.999.209.14:3924 -> 193.45.237.247:4000 UDP
Mar 26 15:00:22 999.999.209.14:3056 -> 134.102.123.7:4000 UDP

• Internal host scanning for DNS and SMTP servers.

Mar 31 13:13:05 999.999.100.230:32782 -> 194.79.69.129:53 UDP
Mar 31 13:13:05 999.999.100.230:32782 -> 143.89.41.155:53 UDP
Mar 31 13:13:05 999.999.100.230:32782 -> 204.134.124.2:53 UDP
Mar 31 13:13:06 999.999.100.230:32782 -> 192.5.5.241:53 UDP
Mar 31 13:13:06 999.999.100.230:32782 -> 146.230.192.5:53 UDP

• Scan for SUNRPC service via crafted packets; note the source and destination ports are the same.

Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.1:111 SYN **S*****
Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.18:111 SYN **S*****
Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.22:111 SYN **S*****
Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.28:111 SYN **S*****
Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.30:111 SYN **S*****
Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.32:111 SYN **S*****
Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.42:111 SYN **S*****
Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.54:111 SYN **S*****
Apr  2 11:36:43 209.217.53.190:111 -> 999.999.132.56:111 SYN **S*****
Scan for FTP servers from a host registered to a Netherlands address. This is likely reconnaissance for a future exploit attempt.
• Scan for FTP servers from a host registered to a German address. This is likely reconnaissance for a future exploit attempt.

Apr  2 23:12:42 217.1.32.130:3238 -> 999.999.1.28:21 SYN **S*****
Apr  2 23:12:42 217.1.32.130:3250 -> 999.999.1.40:21 SYN **S*****
Apr  2 23:12:42 217.1.32.130:3256 -> 999.999.1.46:21 SYN **S*****
Apr  2 23:12:42 217.1.32.130:3262 -> 999.999.1.52:21 SYN **S*****
Apr  2 23:12:42 217.1.32.130:3260 -> 999.999.1.50:21 SYN **S*****
Apr  2 23:12:42 217.1.32.130:3268 -> 999.999.1.58:21 SYN **S*****
Apr  2 23:12:44 217.1.32.130:3466 -> 999.999.2.2:21 SYN **S*****
Apr  2 23:12:44 217.1.32.130:3468 -> 999.999.2.4:21 SYN **S*****
Apr  2 23:12:44 217.1.32.130:3472 -> 999.999.2.8:21 SYN **S*****
Apr  2 23:12:44 217.1.32.130:3476 -> 999.999.2.12:21 SYN **S*****
Apr  2 23:12:44 217.1.32.130:3480 -> 999.999.2.16:21 SYN **S*****

• Scan for DNS servers from a host registered to an address in the Netherlands. This is likely reconnaissance for a future exploit attempt.

Apr  2 23:56:41 128.148.184.75:1356 -> 999.999.2.4:53 SYN **S*****
Apr  2 23:56:41 128.148.184.75:1358 -> 999.999.2.6:53 SYN **S*****
Apr  2 23:56:41 128.148.184.75:1359 -> 999.999.2.7:53 SYN **S*****
Apr  2 23:56:41 128.148.184.75:1360 -> 999.999.2.8:53 SYN **S*****
Apr  2 23:56:41 128.148.184.75:1362 -> 999.999.2.10:53 SYN **S*****
Apr  2 23:56:41 128.148.184.75:1376 -> 999.999.2.24:53 SYN **S*****
Apr  2 23:56:41 128.148.184.75:1386 -> 999.999.2.34:53 SYN **S*****
Apr  2 23:56:41 128.148.184.75:1408 -> 999.999.2.56:53 SYN **S*****
Apr  2 23:56:50 128.148.184.75:4906 -> 999.999.4.22:53 SYN **S*****
Apr  2 23:56:50 128.148.184.75:4907 -> 999.999.4.23:53 SYN **S*****
Apr  2 23:56:50 128.148.184.75:4908 -> 999.999.4.24:53 SYN **S*****
Apr  2 23:56:50 128.148.184.75:4910 -> 999.999.4.26:53 SYN **S*****
Apr  2 23:56:50 128.148.184.75:4911 -> 999.999.4.27:53 SYN **S*****
Out Of Spec Analysis

Top 10 Out of Specs culprits

<table>
<thead>
<tr>
<th># of Conns</th>
<th>Src Ips</th>
<th>Dst IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>63.100.208.92</td>
<td>999.999.253.125</td>
</tr>
<tr>
<td>9</td>
<td>128.46.156.117</td>
<td>999.999.60.38</td>
</tr>
<tr>
<td>9</td>
<td>130.233.26.197</td>
<td>999.999.219.134</td>
</tr>
<tr>
<td>9</td>
<td>24.108.146.141</td>
<td>999.999.207.218</td>
</tr>
<tr>
<td>8</td>
<td>24.22.21.90</td>
<td>999.999.100.165</td>
</tr>
<tr>
<td>7</td>
<td>213.51.144.129</td>
<td>999.999.217.42</td>
</tr>
<tr>
<td>7</td>
<td>999.999.208.226</td>
<td>129.2.249.90</td>
</tr>
<tr>
<td>6</td>
<td>213.45.5.54</td>
<td>999.999.229.38</td>
</tr>
<tr>
<td>6</td>
<td>24.169.64.7</td>
<td>999.999.211.74</td>
</tr>
<tr>
<td>5</td>
<td>158.75.57.4</td>
<td>999.999.215.62</td>
</tr>
</tbody>
</table>

Port 0 is a reserved port and should not appear in normal traffic. This is one-way traffic from inside your network out. Judging by the sequence numbers the source host is not a busy host.
Link Diagram:
Janice Y. Slocumb  GCIA Practical Assignment Version 2.9

03/23-17:12:16.782480 63.100.208.92:2323 -> 999.999.253.125:80
TCP TTL:47  TOs:0x0  ID:0  DF
**21S**  Seq: 0x9452B87A  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1962109 0  EOL  EOL  EOL  EOL

03/23-17:12:16.885806 63.100.208.92:2325 -> 999.999.253.125:80
TCP TTL:47  TOs:0x0  ID:0  DF
**21S**  Seq: 0x942D6234  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1962119 0  EOL  EOL  EOL  EOL

03/23-17:12:16.906894 63.100.208.92:2326 -> 999.999.253.125:80
TCP TTL:47  TOs:0x0  ID:0  DF
**21S**  Seq: 0x9488C70E  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1963052 0  EOL  EOL  EOL  EOL

03/23-17:12:16.906894 63.100.208.92:2326 -> 999.999.253.125:80
TCP TTL:47  TOs:0x0  ID:0  DF
**21S**  Seq: 0x9488C70E  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1963052 0  EOL  EOL  EOL  EOL

03/23-17:12:36.771631 63.100.208.92:2340 -> 999.999.253.125:80
TCP TTL:47  TOs:0x0  ID:0  DF
**21S**  Seq: 0x95AD3075  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1964108 0  EOL  EOL  EOL  EOL

03/23-17:13:56.303137 63.100.208.92:2388 -> 999.999.253.125:80
TCP TTL:47  TOs:0x0  ID:0  DF
**21S**  Seq: 0x9A70CA2B  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1972061 0  EOL  EOL  EOL  EOL

03/23-17:13:58.224986 63.100.208.92:2389 -> 999.999.253.125:80
TCP TTL:47  TOs:0x0  ID:0  DF
**21S**  Seq: 0x9B58DBF4  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1972253 0  EOL  EOL  EOL  EOL

03/23-17:13:58.288327 63.100.208.92:2391 -> 999.999.253.125:80
TCP TTL:47  TOs:0x0  ID:0  DF
**21S**  Seq: 0x9B27D3AE  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1972256 0  EOL  EOL  EOL  EOL
Janice Y. Slocumb  

**GCIA Practical Assignment Version 2.9**

```
21S***** Seq: 0x9B45013E  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1972260 0 EOL EOL EOL EOL

03/23-17:13:58.329155 63.100.208.92:2392 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF

21S***** Seq: 0x9AA59910  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1972263 0 EOL EOL EOL EOL

03/23-17:14:11.103018 63.100.208.92:2401 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF

21S***** Seq: 0x9C29C474  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1974087 0 EOL EOL EOL EOL

03/23-17:14:30.044847 63.100.208.92:2411 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF

21S***** Seq: 0x9D0C474B  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1975436 0 EOL EOL EOL EOL

03/23-17:16:19.356373 63.100.208.92:2507 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF

21S***** Seq: 0xA2F1AACE  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1986365 0 EOL EOL EOL EOL

03/23-17:16:19.397451 63.100.208.92:2508 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF

21S***** Seq: 0xA3478A73  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK  TS: 1986381 0 EOL EOL EOL EOL
```
Janice Y. Slocumb  GCIA Practical Assignment Version 2.9

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Janice Y. Slocumb  GCIA Practical Assignment Version 2.9

03/23-17:16:33.208213 63.100.208.92:2519 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF
21S**** Seq: 0xA491FD8  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK TS: 1987749 0 EOL EOL EOL EOL

03/23-17:16:33.978147 63.100.208.92:2522 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF
21S**** Seq: 0xA3CA5C7B  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK TS: 1987826 0 EOL EOL EOL EOL

03/23-17:17:06.373781 63.100.208.92:2549 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF
21S**** Seq: 0xA6807632  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK TS: 1991064 0 EOL EOL EOL EOL

03/23-17:17:26.395956 63.100.208.92:2555 -> 999.999.253.125:80
TCP TTL:47  TO:0x0  ID:0  DF
21S**** Seq: 0xA76CB964  Ack: 0x0  Win: 0x16D0
TCP Options => MSS: 1460  SackOK TS: 1993068 0 EOL EOL EOL EOL
This traffic represents a targeted probe that was likely generated by an automated scanning tool such as NMAP or Netcat to probe a lone host inside your network for web services. Note the neatly incrementing source port numbers and the setting of the reserved TCP flag bits. This method is often used to bypass IDS systems that only trigger on SYN flags. The setting of the reserved bits is also a method of OS detection.
These packets have all the TCP flag bits set and this is not normal. Packets of this type are not used in normal communication and should not be seen. Packet generating tools such as Hping, Queso, and NMAP can be used to generate these invalid packets for the purpose of network mapping and OS detection. With that in mind I found it interesting that two of the host that were involved all had European address; 152.66.225.153 – Hungray, and 195.249.200.155 – Denmark.
Assignment 4 - Analysis Process

I conducted my analysis on a HP Pavilion 9870 running Windows/ME. This was my first challenge since most of the tools used in prior practicals were Unix based. I’d like to extend my thanks to Loras Even for her insight. Reviewing her practical was a big help.

I had to do quite a bit of up-front preparation before I could begin to analyze the data. I’ve listed here the steps I performed to complete my analysis.

1. I installed several tools on my box. I’ve listed them here:
   - WIN32 versions of unix tools such as grep, and sed
   - WIN32Perl
   - Apache Web Server for viewing SnortSnarf HTML output

2. After installing the tools, I selected the subset of data that I would analyze and saved them in .txt files.
   Data Used

   Alerts:
   April 1,2,3 (content data is for Mar 31, Apr 1, and Apr 2 respectively)
   Mar 23,26,27 (content data is for Mar 22, Mar25, and Mar26 respectively)

   Scans:
   April 1,2,3 (content data is for Mar 31, Apr 1, and Apr 2 respectively)
   Mar 23,26,27 (content data is for Mar 22, Mar25, and Mar26 respectively)

   Out Of Spec Data:
   April 2 (content data is for Apr 1)
   Mar 23,26,27,28 (content data is for Mar 22, Mar 25, Mar 26, and Mar 27 respectively)

3. All of the Alert*.txt files were combined into one file using the dos COPY command. After combining the files I used sed to replace all instances of MY.NET with 999.999 and redirected the output to a new file. I had to do this because I got the following error attempting to run SnortScan files through snortsnaf with “MY.NET” string. To resolve this I changed MY.NET to 999.999.

   Use of uninitialized value in numeric comparison (\=\=\=\=) at \\
   :/usr/local/lib/MemTimeBase.pm line 69, <ifh000> line 3329.
   Use of uninitialized value in numeric^C comparison (\=\=\=\=) at \\
   C:/usr/local/lib/MemTimeBase.pm line 69, <ifh000> line 3329
4. I downloaded snortsnarf.pl from www.silicondefense.com/software/snortsnarf and processed the output from step 3. This allowed me to use my web browser to view the data in html format.

5. Next I processed each day’s scan file through snortsnarf individually. I could not combine them because the volume of data caused memory shortage errors.

6. I pulled out critical data for analysis using perl scripts from Mike Bell’s practical. (Many thanks to Mike) I modified them replacing MY.NET with 999.999

7. I used Mike’s perl script to create a listing of the total number of alerts by type and imported the resulting file into MS-Excel for sorting since I don’t have the sort utility.

8. Big Talkers – the top 10 talkers (ran the script top_talkers.pl and imported the resulting file into MS-Excel for sorting since I don’t have the sort utility) input file = massalrt.txt (combined alerts file) output file= Top Ten Big_talkers

9. To get the total number of connections (29,434) I used the Excel SUM function to total the connection count column from the Big-Talkers file.

10. To get the list of source IP addresses and the number of associated scans I used Mike’s snort_source.pl script. I saved the output as a text file using WORDPAD. I imported the text file into Excel and sorted it by total connections. input file = allscans.txt (combined alerts file) output file= Scanner SourceIPs

11. To get the list of the source/destination pairs for the top Out of Spec talkers is used Mike’s top_talkers_oos.pl input file = ooSpec.txt output file=D:\SANS\top oos talkers (ran the script top_talkers.pl and imported the resulting file into MS-Excel for sorting since I don’t have the sort utility) This was the data I used to my link graph.

12. I used grep to analyze the combined scans file because the file was too large to load into MS-Excel.

Performing this analysis in a windows platform was challenging at best; however it has shown me that network traffic analysis can be done outside of the Unix arena.
References:


Northcutt, Stephen; Cooper, Mark; Fearnow, Matt; Fredrick, Karen Intrusion Signatures and Analysis New Riders, 2001


McClure, Stuart, Scambray, Joel, and Kurtz, George. Hacking Exposed Network Security Secrets and Solutions

Roesch, Marty. Intrusion Detection- Snort Style, SANS Institute

Stoev, Philip.”ICQ WebFront HTTPd DoS”
http://www.shmoo.com/mail/bugtraq/sep00/msg00598.shtml

http://www.sans.org/y2k/analysts.htm
1. Paul Asadoorian #0337
2. Loras Even #325
3. Mike Bell (Perl scripts)
# Upcoming Training

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Blue Team and Purple Team 2020</td>
<td>United Arab Emirates</td>
<td>Jul 13, 2020 - Jul 18, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Rocky Mountain Summer 2020</td>
<td>CO</td>
<td>Jul 20, 2020 - Jul 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - SEC503: Intrusion Detection In-Depth</td>
<td>United Arab Emirates</td>
<td>Jul 29, 2020 - Sep 04, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 3 ET</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS vLive - SEC503: Intrusion Detection In-Depth</td>
<td>SEC503 - 202008</td>
<td>Aug 10, 2020 - Sep 16, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Essentials Live Online 2020</td>
<td>Australia</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020 - Live Online</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2020 - Live Online</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020</td>
<td>Dallas, TX</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020 - Live Online</td>
<td>Dallas, TX</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London November 2020</td>
<td>London, United Kingdom</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>