Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering "Intrusion Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia
Assignment #1 – Five Network Scans

Detect #1 (named iquery attempt)

[**] DNS named iquery attempt [**]
UDP TTL:45 TOS:0x0 ID:1794 IpLen:20 DgmLen:493
Len: 473
25 15 09 80 00 00 01 00 00 00 00 3E 41 41 41 %...........>AAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA>
BEEE
BEEE
BEEE
BEEE
BEEE
25 15 09 80 00 00 01 00 00 00 00 3E 41 41 41 %...........>AAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA>
BEEE
BEEE
BEEE
BEEE
BEEE
25 15 09 80 00 00 01 00 00 00 00 3E 41 41 41 %...........>AAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAA>
BEEE
BEEE
BEEE
BEEE
BEEE

The Log Format:

<table>
<thead>
<tr>
<th>Meaning</th>
<th>Snort information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snort signature</td>
<td>[<strong>] DNS named iquery attempt [</strong>]</td>
</tr>
<tr>
<td>Date/Time group</td>
<td>03/14-22:16:11.061618</td>
</tr>
<tr>
<td>Source Address and port (2693)</td>
<td>seeker.net:2693</td>
</tr>
<tr>
<td>Direction operator</td>
<td>-&gt;</td>
</tr>
<tr>
<td>Destination Address and port (53)</td>
<td>my.dns.com:53</td>
</tr>
<tr>
<td>Protocol and Time to Live (TTL)</td>
<td>UDP TTL:45</td>
</tr>
<tr>
<td>Type of Service (TOS)</td>
<td>TOS:0x0</td>
</tr>
<tr>
<td>Packet ID in binary</td>
<td>ID:1794</td>
</tr>
<tr>
<td>IP header length</td>
<td>IpLen:20</td>
</tr>
<tr>
<td>Total length</td>
<td>DgmLen:493</td>
</tr>
<tr>
<td>UDP length</td>
<td>Len: 473</td>
</tr>
</tbody>
</table>

1. **Source of trace.**

My network.

2. **Detect was generated by:**

Detect was generated by Snort Intrusion Detection System, Version 1.7.

Snort rule:

explain the log format

3. **Probability the source address was spoofed:**

Probably not spoofed. Spoofing the address would be defeating the purpose to see response.

4. **Description of attack:**

The attacker is trying to determine if a name server supports IQUERY (Inverse Query).

5. **Attack Mechanism:**

IP address seeker.net is trying to determine if the name server, my.dns.com, supports IQUERY.
This signature often indicates a pre-attack probe used to locate vulnerable servers running named. With Inverse Query Buffer Overrun in BIND 4.9 and BIND 8 Releases attacker can gain root-level access to name server.

6. Correlation:

The following links have additional information:
http://www.whitehats.com/info/IDS277
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0009
http://www.securityfocus.com/ids/277
http://www.insecure.org/sploits/bind.multiple.vuln.html

7. Evidence of active targeting:

The source IP address iquery.net targeted IP address my.dns.com

8. Severity:

(System Criticality + Attack Lethality) – (System Countermeasures + Network Countermeasures) = Severity

(5 + 3) - (5+2) = 1

System Criticality: 5 - DNS server
Attack Lethality: 3 - Pre-attack probe
System Countermeasures: 5 - Modern operating system, all patches
Network Countermeasures: 2 - Firewall in place, but traffic is allowed to target

9. Defensive recommendation:

"Upgrading to the latest version of bind, available at: http://www.isc.org/bind.html will eliminate this vulnerability.

CERT advisory CA-98.05.bind_problems.html details individual vendor responses. It also provides information about specific vendor patches." (http://www.securityfocus.com/ids/277).

10. Multiple choice test question:

Which service is on port 53?

A SMTP  
B WWW  
C FTP  
D DNS
Answer D

Detect #2 (SMTP relaying denied) – (Back)

[**] SMTP relaying denied [**]
03/20-20:06:08.358631 my.smtp.com:25 -> seeker.relaying.net:2407
TCP TTL:253 TOS:0x0 ID:424 IpLen:20 DgmLen:91 DF
***AP*** Seq: 0xBAD1876C Ack: 0x3CDEBA59 Win: 0x2530 TcpLen: 20
35 35 30 20 35 2E 37 2E 31 20 3C 61 77 73 75 6D 550 5.7.1 <awsum
34 75 40 65 78 63 69 74 65 2E 63 6F 6E 69 65 69 66 66 6E 69 65 4u@excite.com>..
2E 20 52 65 6C 61 79 73 75 6D 67 20 64 65 6F 70 72 69 65 76 65 69 550 5.7.1
Relaying denied
64 0D 0A
d..

[**] SMTP relaying denied [**]
03/20-20:06:17.951379 my.smtp.com:25 -> seeker.relaying.net:2422
TCP TTL:253 TOS:0x0 ID:64682 IpLen:20 DgmLen:91 DF
***AP*** Seq: 0x671C7308 Ack: 0x3CFC1DB3 Win: 0x2530 TcpLen: 20
35 35 30 20 35 2E 37 2E 31 20 3C 61 77 73 75 6D 550 5.7.1 <awsum
34 75 40 65 78 63 69 74 65 2E 63 6F 6E 69 65 69 66 66 6E 69 65 4u@excite.com>..
2E 20 52 65 6C 61 79 73 75 6D 67 20 64 65 6F 70 72 69 65 76 65 69 550 5.7.1
Relaying denied
64 0D 0A
d..

1. Source of trace.

My network.

2. Detect was generated by:

Detect was generated by Snort Intrusion Detection System, Version 1.7.
Snort rule:
alert tcp $HOME_NET 25 -> $EXTERNAL_NET any (msg:"SMTP relaying denied";
flags: A+; content: "5.7.1"; depth:70; reference:arachnids,249;)

3. Probability the source address was spoofed:

Probably spoofed.

4. Description of attack:

"Mail relay is enabled, allowing abuse by spammers." (CAN-1999-0512)

5. Attack Mechanism:
On the Internet, there are mail servers that are miss-configured and are an open relay. This means that unscrupulous people can send bulk unsolicited junk e-mail through those relays and bombard other sites.

6. **Correlation:**

   http://www.whitehats.com/info/IDS249  
   http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0512

7. **Evidence of active targeting:**

   The seeker.relaying.net targeted my.smtp.com and packets, from the dump, are responses from my.smtp.com.

8. **Severity:**

   \[(\text{System Criticality} + \text{Attack Lethality}) - (\text{System Countermeasures} + \text{Network Countermeasures}) = \text{Severity}\]

   \[(4 + 1) - (5 + 2) = -2\]

   System Criticality: 4 - SMTP server  
   Attack Lethality: 1 - Attack is unlikely to succeed  
   System Countermeasures: 5 - Modern operating system, all patches  
   Network Countermeasures: 2 - Firewall in place, but traffic is allowed to target

9. **Defensive recommendation:**

   "This behavior indicates the successful blocking of an attempt at relaying email through an internal email server." (ids249)

10. **Multiple choice test question:**

    What is signature of the "SMTP relaying denied"

    A FLAGS SYN, PSH  
    B CONTENT "550"  
    C FLAGS ACK, PSH CONTENT "5.7.1", DEPTH "70"  
    D DEPTH "7"

    **Answer C**

**Detect #3 (False Positive - transmitting data via HTTP)** - (Back)
SANS Intrusion Detection & Analysis Certification
New Orleans January 28 - February 2, 2001

44 20 43 4F 4C 53 50 41 4E 3D 22 33 22 20 41 4C 4D COLSPAN="3" AL
49 47 4E 3D 22 43 45 4E 54 45 52 22 3E 0D 0A 09
09 09 3C 68 22 3E 0D 0A 09 09 3C 2F 74 64 3E 0D 0A 09 3C 2F
74 72 3E 0D 0A

[**] DDOS shaft client to handler [**]
TCP TTL:111 TOS:0x0 ID:34892 IpLen:20 DgmLen:292 DF
***AP*** Seq: 0x4093E4A0 Ack: 0xA1454F2 Win: 0x40B0 TcpLen: 20
48 54 50 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D
0A 53 65 72 76 65 72 3A 20 4D 69 64 76 65 72 6F 73 6F
66 74 2D 49 49 53 2F 35 2E 30
65 63 74 69 6F 6E 3A 20 6B 65 64 77 61 72 74 75 61 72 74 3A
76 65 0D 0A 44 61 74 65 3A 20 57 65 64 2C 20 31
34 20 4D 61 72 20 32 30 30 30 20 3A 35 39 20 47 4D 54 3A
3A 35 39 20 47 4D 54 0D 0A 43 6F 6E 74 65 66 74 65 70 2D 61 6C 69 67 68 74 20 3A
4D 54 79 70 65 3A 20 69 66 64 77 61 72 74 75 61 72 74 3A
67 0D 0A 41 63 63 68 3A 20 57 65 64 2C 20 31
3A 20 62 79 74 65 73 0D 0A 4C 61 73 74 72 2D 4D 6F
64 69 66 69 6D 64 3A 20 54 75 65 2C 20 30 33 20
4F 63 74 20 32 30 30 30 20 32 30 33 3A 30 36 3A 30 32
32 20 47 4D 54 0D 0A 45 54 61 67 3A 20 22 61 61
62 35 66 35 36 37 35 32 64 63 30 31 3A 30 36 3A 38 61
37 22 0D 0A 43 6F 6E 74 65 66 74 2D 4C 65 66 67
74 68 3A 20 32 34 36 39 0D 0A 0D 0A

HTTP/1.1 200 OK.
.Server: Microsof
ft-IIS/5.0..Conn
ection: keep-al
..Date: Wed, 1
Mar 2001 10:57
Marified: Tue, 03
Oct 2000 20:06:2
2 GMT..ETag: "aa
b5f566752de01:8a
7".Content-Length
th: 2469....
The Log Format:

<table>
<thead>
<tr>
<th>Meaning</th>
<th>Snort information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snort signature</td>
<td>[<strong>] DDOS mstream client to handler [</strong>]</td>
</tr>
<tr>
<td>Date/Time group</td>
<td>03/14-13:51:25.235058</td>
</tr>
<tr>
<td>Source Address and port (80)</td>
<td><a href="http://www.server.net:80">www.server.net:80</a></td>
</tr>
<tr>
<td>Direction operator</td>
<td>-&gt;</td>
</tr>
<tr>
<td>Destination Address and port (12754)</td>
<td>my.ws.com:12754</td>
</tr>
<tr>
<td>Protocol and Time to Live (TTL)</td>
<td>TCP TTL:117</td>
</tr>
<tr>
<td>Type of Service (TOS)</td>
<td>TOS:0x0</td>
</tr>
<tr>
<td>Packet ID in binary</td>
<td>ID:1009</td>
</tr>
<tr>
<td>IP header length</td>
<td>IpLen:20</td>
</tr>
<tr>
<td>Total length</td>
<td>DgmLen:141</td>
</tr>
<tr>
<td>Don't Fragment Flag</td>
<td>DF</td>
</tr>
<tr>
<td>TCP flags set</td>
<td><em><strong>AP</strong></em></td>
</tr>
<tr>
<td>Sequence # in Hex</td>
<td>Seq: 0xE70F58F</td>
</tr>
<tr>
<td>Acknowledgement # in Hex</td>
<td>Ack: 0x1645CAEE</td>
</tr>
<tr>
<td>Windows size in Hex</td>
<td>Win: 0x2058</td>
</tr>
<tr>
<td>TCP header length</td>
<td>TcpLen: 20</td>
</tr>
</tbody>
</table>

1. **Source of trace.**

My network

2. **Detect was generated by:**

Detect was generated by Snort Intrusion Detection System, Version 1.7.
Snort rule:
alert tcp $EXTERNAL_NET any -> $HOME_NET 12754 (msg:"DDOS mstream client to handler"; content: ">"; flags: A+; reference:cve,CAN-2000-0138;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 20432 (msg:"DDOS shaft client to handler"; flags: A+; reference:arachnids,254;)

3. **Probability the source address was spoofed:**

Probably not spoofed.

4. **Description of attack:**

N/A

5. **Attack Mechanism:**

N/A
6. Correlation:

The following links have additional information about Distributed Denial of Service (DDOS) attacks "mstream client to handler" and " shaft client to handler":
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0138
http://xforce.iss.net/alerts/advice48.php
http://marc.theaimsgroup.com/?l=bugtraq&m=95715370208598&w=2
http://marc.theaimsgroup.com/?l=bugtraq&m=95722093124322&w=2
http://www.whitehats.com/info/IDS254
http://www.securiteam.com/windowsntfocus/Microsoft_IIS_shtml_exe_path_disclosure_vulnerability.html

7. Evidence of active targeting:

N/A

8. Severity:

(System Criticality + Attack Lethality) – (System Countermeasures + Network Countermeasures) = Severity

(x + x) - (x + x) = x

System Criticality:
Attack Lethality:
System Countermeasures:
Network Countermeasures:

9. Defensive recommendation:

N/A

10. Multiple choice question:

This log was generated by which IDS:

A Shadow
B Snort
C Real Secure
D Net Ranger

Answer B

Detect #4 (WEB-FRONTPAGE shtml.exe ) - (Back)

[[**] WEB-FRONTPAGE shtml.exe [**]]
03/20-11:52:34.076724 192.168.100.101:57426 -> my.web.com:80
TCP TTL:246 TOS:0x0 ID:60524 IpLen:20 DgmLen:363

***AP*** Seq: 0x8E3E61C9  Ack: 0xFD006BC0
47 45 54 20 2F 5F 76 74 69 5F 62 69 6E 2F 73 68
74 6D 6C 2E 65 78 65 2F .. .. .. .. .. .. .. ..

1. **Source of trace.**

My network

2. **Detect was generated by:**

Detect was generated by Snort Intrusion Detection System, Version 1.7.
Snort rule:

3. **Probability the source address was source:**

Probably not spoofed, if attacker determines the physical path of HTML, HTM, ASP, and SHTML files.

Probably spoofed if attacker want to cause denial of service.

4. **Description of attack:**

This attack has two references, which describe attacks:
- "The shtml.exe program in the FrontPage extensions package of IIS 4.0 and 5.0 allows remote attackers to determine the physical path of HTML, HTM, ASP, and SHTML files by requesting a file that does not exist, which generates an error message that reveals the path." (CAN-2000-0413)
- "The shtml.exe component of Microsoft FrontPage 2000 Server Extensions 1.1 allows remote attackers to cause a denial of service in some components by requesting a URL whose name includes a standard DOS device name." (CAN-2000-0709)

5. **Attack Mechanism:**

The IP address 192.168.100.101 sends a packet, which contains "/_vti_bin/shtml.exe" and a path to a non-existing file to my.web.com. "Passing a path to a non-existent file to the shtml.exe or shtml.dll (depending on platform) program will display an error message stating that the file cannot be found accompanied by the full local path to the web root. For example, performing a request for http://target/_vti_bin/shtml.dll/non_existant_file.html will produce an error message stating "Cannot open "C:\localpath\non_existant_file.html": no such file or folder"." (bid 1174) Expose information of the real path, an attacker can later use for future attacks.
6. **Correlation:**

The following links have additional information:
- [http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0413](http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0413)
- [http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0709](http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0709)

7. **Evidence of active targeting:**

The source IP address **192.168.100.101** targeted **my.web.com**.

8. **Severity:**

(System Criticality + Attack Lethality) – (System Countermeasures + Network Countermeasures) = Severity

\[(4 + 2) - (2 + 2) = 2\]

- **System Criticality:** 4 - Web server
- **Attack Lethality:** 2 - Pre attack probe
- **System Countermeasures:** 2 - Target is not patched
- **Network Countermeasures:** 2 - Firewall in place, but traffic is allowed to target

9. **Defensive recommendation:**

"Microsoft will be addressing this issue with version 1.2 of Frontpage Server Extensions 2000." (bid 1174)

10. **Multiple choice test question:**

Which item is a signature of a "WEB-FRONTPAGE shtml.exe" attack:

A /_vti_/html.exe  
B /_vti_bin/shtml.exe  
C /_vti_bin/http.exe  
D /_bin/shttp.exe

**Answer B**

**Detect #5** (False Positive - miss-configured Tivoli/IBM TME 10 agent) - (Back)
SANS Intrusion Detection & Analysis Certification  
New Orleans January 28 - February 2, 2001

Mar 11 20:58:04 192.168.100.100:13991 -> 17.32.16.228:13991 UDP
Mar 11 20:58:05 192.168.100.100:13991 -> 17.32.156.4:13991 UDP
Mar 11 20:58:06 192.168.100.100:13991 -> 17.32.229.4:13991 UDP

alert
[*] spp_portscan: portscan status from 192.168.6.202: 7 connections across 7 hosts:
TCP(0), UDP(7) [*]
03/11-20:58:08.684813

Cisco Secure PIX firewall
106011: Deny inbound (No xlate) udp src xxx: 192.168.100.100/13991 dst xxx:17.32.115.196/13991
106011: Deny inbound (No xlate) udp src xxx: 192.168.100.100/13991 dst xxx:17.32.157.196/13991

The log format:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/pix55em/pixemsgs.htm#40403

1. **Source of trace.**

My network.

2. **Detect was generated by:**

Detect was generated by Snort Intrusion Detection System, Version 1.7. Cisco Secure PIX firewall. (explain the format)

3. **Probability the source address was spoofed:**

Probably not spoofed

4. **Description of attack:**

IP address 192.168.100.100 scanned IP addresses on port 13991.

5. **Attack Mechanism:**

N/A

6. **Correlation:**

The following correlating data is included (from Sniffer Pro), providing a complete UDP packet.

DLC: ----- DLC Header -----
DLC:
DLC: Frame 1 arrived at 14:45:32.0000; frame size is 60 (003C hex) bytes.
DLC: Destination = Station Cisco107AC10
DLC: Source = Station 00105AE795F6
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header ----- 
IP: 
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine 
IP: ...0 .... = normal delay 
IP: .... 0... = normal throughput 
IP: ....0.. = normal reliability 
IP: Total length = 31 bytes 
IP: Identification = 21878
IP: Flags = 0X
IP: .0. .... = may fragment 
IP: ..0. .... = last fragment 
IP: Fragment offset = 0 bytes 
IP: Time to live = 64 seconds/hops 
IP: Protocol = 17 (UDP)
IP: Header checksum = 5B01 (correct)
IP: Source address = [192.168.100.100]
IP: Destination address = [17.32.241.196]
IP: No options 
IP: 
UDP: ----- UDP Header ----- 
UDP: 
UDP: Source port = 13991
UDP: Destination port = 13991
UDP: Length = 11
UDP: Checksum = 4732 (correct) 
UDP: [3 byte(s) of data]
UDP: 
ADDR HEX ASCII
0000: 00 00 0c 07 ac 10 00 10 5a e7 95 f6 08 00 45 00 | ..........!Xn6....
0010: 00 1f 55 76 00 00 40 11 5b 01 xx xx xx xx xx | ..... .$.{y....
0020: xx xx 36 a7 36 a7 00 0b 47 32 81 00 00 00 00 | 1D.x.x....a.....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ............

7. Evidence of active targeting:
N/A

8. Severity:
(System Criticality + Attack Lethality) – (System Countermeasures + Network Countermeasures) = Severity

(x + x) - (x + x) = x

System Criticality:
Attack Lethality:
System Countermeasures:
Network Countermeasures:

9. **Defensive recommendation:**

Do right configuration.

10. **Multiple choice question:**

106011: Deny inbound (No xlate) udp src xxx:192.168.100.100/13991 dst xxx:17.32.115.196/13991

This log was generated by:

A Check Point FW1
B Cisco Secure PIX firewall
C Cisco Secure IDS
D Shadow

**Answer B**
1. Source of the Attack - thong.pl - automated multi dos attack tool


According to the (1), "Thong-th-thong-th-thong.pl AKA thong.pl is a PERL script which automates several attacks against various Cisco products.

To be specific:

12-13-00 - Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
11-28-00 - Cisco 675 Web Administration Denial of Service Vulnerability
10-26-00 - Cisco Catalyst 3500 XL Remote Arbitrary Command
10-25-00 - Cisco IOS Software HTTP Request DoS Vulnerability"

2. Description of Attack

2.1 Exploits Details

Name: Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
CVE: CAN-2001-0080 (under review) (2)
Operating System: Cisco Catalyst 6000, 5000, or 4000 switches
Brief Description: Cisco switches allow remote attackers to cause a denial of service by connecting to the SSH service with a non-SSH client, which generates a protocol mismatch error.

Name: Cisco 675 Web Administration Denial of Service Vulnerability
BUGTRAQ id: 2012
Operating System: Cisco DSL Router 677.0, Cisco DSL Router 675.0
Brief Description: "If the Cisco 675 DSL Router has the Web Administration Interface enabled, a remote attacker could telnet to the router and issue a simple malformed HTTP GET request. Once connected via telnet to the Web Administration Interface, issuing the command GET ?\n\nwill crash the telnet session as well as the router, requiring it be power cycled before resuming normal operation." (3)

Name: Cisco Catalyst 3500 XL Remote Arbitrary Command
CVE: CAN-2000-0945 (under review) (4)
Operating System: Cisco Catalyst 3500 XL switches
Brief Description: Web configuration interface for Catalyst 3500 XL switches allows remote attackers to execute arbitrary commands without authentication via URL containing the /exec/ directory.

Name: Cisco IOS Software HTTP Request DoS Vulnerability
CVE: CVE-2000-0984 (5)
Operating System: Cisco IOS 12.0 through 12.1

Brief Description: HTTP server in Cisco IOS 12.0 through 12.1 allows local users to cause a denial of service (crash and reload) via URL containing a "?/" string.

2.2 How to use the exploit

To start PERL script, the following command can be used:
# ./thong.pl -h <host>

Then, you can choose one of the next options:

DATE            VULNERABILITY
1. 12-13-00 - Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
2. 11-28-00 - Cisco 675 Web Administration Denial of Service Vulnerability
3. 10-26-00 - Cisco Catalyst 3500 XL Remote Arbitrary Command
4. 10-25-00 - Cisco IOS Software HTTP Request DoS Vulnerability

Enter Option:

2.3 Source code

The source code can be found at (1) and the lines below come from thong.pl:

sub computeOption
{
  if  ($menu_opt == "1"){$PORT = 22; $STRING = "this ain't SSH";} 
  elsif ($menu_opt == "2"){$PORT = 80; $STRING = "GET / HTTP/1.0\n";} 
  elsif ($menu_opt == "3"){$PORT = 80; three();} 
  elsif ($menu_opt == "4"){$PORT = 80; $STRING = "GET /error?/ HTTP/1.0\n";} 
  else  {print "Select a real option!\n"; menu();}
}

sub three
{
  print "Enter file to read or enter D for default (/show/config/cr): ";
  $key = <STDIN>;
  chomp ($key);
  print "\nGetting $key...";

  if (($key eq "D")||($key eq "d"))
  {
    print "\nGetting /show/config/cr...\n";
    $STRING = "GET /exec/show/config/cr HTTP/1.0\n";
  }
  else
  {
    print "\nGetting $key...\n";
    $STRING = "GET /exec$key HTTP/1.0\n";
  }
3. Trace of the Attack

I used Sniffer Pro from Network Associates and I have done trace for Cisco IOS Software HTTP Request DoS Vulnerability.

First the three way handshake, SYN, SYN-ACK, ACK:
1 [attacker] [http-server] 74 TCP: D=80 S=1130 SYN SEQ=3676262050 LEN=0 WIN=32120
2 [http-server] [attacker] 60 TCP: D=1130 S=80 SYN ACK=3676262051
   SEQ=3588378044 LEN=0 WIN=4128
3 [attacker] [http-server] 60 TCP: D=80 S=1130 ACK=3588378045 WIN=32120

Attacker sends a HTTP request:

TCP: ----- TCP header -----
   TCP: Source port = 1130
   TCP: Destination port = 80 (WWW-HTTP)
   TCP: Sequence number = 3676262051
   TCP: Next expected Seq number= 3676262074
   TCP: Acknowledgment number = 3588378045
   TCP: Data offset = 20 bytes
   TCP: Flags = 18
      .0. .... = (No urgent pointer)
      ..1 ... = Acknowledgment
      .... 1... = Push
      .... .0.. = (No reset)
      .... ...0 = (No SYN)
      .... ...0 = (No FIN)
   TCP: Window = 32120
   TCP: Checksum = 45D2 (correct)
   TCP: No TCP options
   TCP: [23 Bytes of data]
TCP: ----- Hypertext Transfer Protocol -----
HTTP: Line 1: GET /error?/ HTTP/1.0
HTTP: Line 2:
HTTP:

Detecting the attack

I wrote the Snort rule:
alert tcp any any -> http-server 80 (msg:"Cisco IOS HTTP Request Vulnerability CVE-2000-0984";flags: AP; content:"?/"; nocase;)

That means alert on any source IP address sends a TCP traffic to destination host http-server with destination port of 80 and with PUSH and ACK flags and content ?/ giving a message of "Cisco IOS HTTP Request Vulnerability CVE-2000-0984".

Snort file alert shows next lines:
[**] Cisco IOS HTTP Request Vulnerability CVE-2000-0984 [**]
TCP TTL:64 TOS:0x0 ID:38022 IpLen:20 DgmLen:63 DF
***AP*** Seq: 0xFF5E4053 Ack: 0xA2774234 Win: 0x7D78 TcpLen: 20

Snort file TCP:1174-80 shows next lines:
TCP TTL:64 TOS:0x0 ID:38022 IpLen:20 DgmLen:63 DF
***AP*** Seq: 0xFF5E4053 Ack: 0xA2774234 Win: 0x7D78 TcpLen: 20
47 45 54 20 65 72 72 6F 72 3F 2F 20 48 54 50 2F 31 2E 30 0A 0A
P/1.0..

Resources and References
(1) http://www.hack.co.za/exploits/os/hardware/routers/cisco/thong.pl
(2) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0080
(3) http://securityfocus.net/frames/?content=/vdb/bottom.html%3Fvid%3D2012
(4) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0945
(5) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0984
Assignment #3 – Analyze This Scenario – (Back)

1. Scenario

"Your organization has been asked to provide a bid for security services to GIAC Enterprises, an e-business startup that sells electronic fortune cookie sayings. You have been provided with one month’s worth of data from a Snort system with a fairly standard rulebase. From time to time, the power has failed or the disk was full so you do not have data for all days. Your task is to analyze the data. Be especially alert for signs of compromised systems or network problems and produce an analysis report." (1)

2. Snort Snarf output of the alert files

<table>
<thead>
<tr>
<th>Signature</th>
<th># Alerts</th>
<th># Sources</th>
<th># Destinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>site exec - Possible wu-ftpd exploit - GIAC000623</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SITE EXEC - Possible wu-ftpd exploit - GIAC000623</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>STATDX UDP attack</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Happy 99 Virus</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Probably NMAP fingerprint attempt</td>
<td>8</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>External RPC call</td>
<td>59</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td>Back Orifice</td>
<td>63</td>
<td>9</td>
<td>60</td>
</tr>
<tr>
<td>TCP SMTP source Port traffic</td>
<td>100</td>
<td>5</td>
<td>88</td>
</tr>
<tr>
<td>Broadcast Ping to subnet 70</td>
<td>151</td>
<td>23</td>
<td>1</td>
</tr>
<tr>
<td>connect to 515 from inside</td>
<td>159</td>
<td>10</td>
<td>98</td>
</tr>
<tr>
<td>SUNRPC highport access</td>
<td>204</td>
<td>25</td>
<td>19</td>
</tr>
<tr>
<td>SMB Name Wildcard</td>
<td>515</td>
<td>93</td>
<td>171</td>
</tr>
<tr>
<td>Russia Dynamo - SANS Flash 28-jul-00</td>
<td>546</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>NMAP TCP ping!</td>
<td>558</td>
<td>47</td>
<td>156</td>
</tr>
<tr>
<td>SNMP public access</td>
<td>591</td>
<td>20</td>
<td>7</td>
</tr>
<tr>
<td>Queso fingerprint</td>
<td>710</td>
<td>52</td>
<td>72</td>
</tr>
<tr>
<td>Null scan!</td>
<td>824</td>
<td>525</td>
<td>171</td>
</tr>
<tr>
<td>Attempt Sun RPC high port access</td>
<td>2041</td>
<td>16</td>
<td>22</td>
</tr>
<tr>
<td>Win Gate 1080 Attempt</td>
<td>2202</td>
<td>466</td>
<td>565</td>
</tr>
<tr>
<td>Watch list 000222 NET - NCFC</td>
<td>2401</td>
<td>31</td>
<td>19</td>
</tr>
<tr>
<td>Connect to 515 from outside</td>
<td>4237</td>
<td>9</td>
<td>2876</td>
</tr>
<tr>
<td>Tiny Fragments - Possible Hostile Activity</td>
<td>5339</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>DNS udp DoS attack described on unisog</td>
<td>16146</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>SYN - FIN scan!</td>
<td>51192</td>
<td>37</td>
<td>27067</td>
</tr>
<tr>
<td>Watchlist 000220 IL - ISDNNET-990517</td>
<td>104507</td>
<td>46</td>
<td>100</td>
</tr>
</tbody>
</table>

Table 1
3. Top 5 alert signatures of 25 identified signatures

3.1 Watchlist 000220 IL - ISDNNET-990517

<table>
<thead>
<tr>
<th>#</th>
<th>Sources</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>212.179.79.2</td>
<td>48786</td>
<td>48786</td>
<td>41</td>
<td>41</td>
</tr>
<tr>
<td>2</td>
<td>212.179.27.111</td>
<td>37604</td>
<td>37604</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>212.179.95.5</td>
<td>4563</td>
<td>4563</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>212.179.77.20</td>
<td>2353</td>
<td>2353</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>212.179.44.105</td>
<td>1517</td>
<td>1517</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Top Destination Hosts

<table>
<thead>
<tr>
<th>#</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>1</td>
<td>MY.NET.201.222</td>
<td>37604</td>
<td>37609</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>MY.NET.220.126</td>
<td>25182</td>
<td>25183</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>MY.NET.225.234</td>
<td>9309</td>
<td>9314</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>MY.NET.202.94</td>
<td>5181</td>
<td>5253</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>MY.NET.229.114</td>
<td>5080</td>
<td>5082</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

Detailed analysis of the summary field (SnortSnarf) shows that only one signature is present for all five Top Source Hosts and it is Watchlist 000220 IL - ISDNNET-990517 and all 46 source hosts traffic comes from Israel. For example IP address 212.179.79.2 has the next information from RIPE Whois Database:

- **Inetnum:** 212.179.79.0 - 212.179.79.63
- **netname:** CREOSCITEX
- **descr:** CREOSCITEX-SIFRA
- **country:** IL
- **admin-c:** ZV140-RIPE
- **tech-c:** NP469-RIPE
- **status:** ASSIGNED PA
- **notify:** hostmaster@isdn.net.il
- **changed:** hostmaster@isdn.net.il 20001109
- **source:** RIPE

Top Destination Hosts shows most targeted hosts on MY.NET, for this attack, and all of them have at least one scanning signature, for example "SYN-FIN scan!". The lines below come from Snort. "Null scan!", in the first line, indicates the scanning of the port 6699 on MY.NET.201.222. After scanning came traffic to MY.NET.201.22 on the same port.
I have found the report of similar traffic on (2) and comment was: "In this case, a large portion of it looks like gnutella related activity." "Gnutella is the protocol that allows those with a Gnutella client to distribute files." (3) For more information on Gnutella, take a look at (3) or (4). There are some security risks to use gnutella, for example:
- no restrictions possible on unauthorized sharing of files,
- not anonymous,
- ability to see what other people are searching for on the network,
- distributed nature of servant makes it difficult to block access to GnutellaNet, '
- ability to change the port you use makes it difficult to block access to GnutellaNet,
- ability to define your own internal network with a single exit point to the rest of the internet makes it difficult to block access to GnutellaNet

7 different signatures are present for IP address MY.NET.202.94 as a destination:
- 2 instances of Null scan!,
- 3 instances of SYN-FIN scan!,
- 3 instances of BackOrifice,
- 4 instances of Attempt Sun RPC high port access,
- 6 instances of SUNRPC highport access,
- 54 instances of WinGate 1080 Attempt,
- 5181 instances of Watchlist 000220 IL - ISDNNET-990517.

Lines above show many strange actions on the IP address MY.NET.202.94 and it will require further review.

### 3.2 SYN - FIN scan!

Event description: "A TCP probe was sent with the SYN+FIN flags set in the header. This traffic does not occur naturally and indicates an intentional probe, likely as a part of single-packet OS detection." (6)
Top Source Hosts

<table>
<thead>
<tr>
<th>#</th>
<th>Sources</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>211.34.40.1</td>
<td>17604</td>
<td>17604</td>
<td>17604</td>
<td>17604</td>
</tr>
<tr>
<td>2</td>
<td>195.56.182.206</td>
<td>9878</td>
<td>9878</td>
<td>9878</td>
<td>9878</td>
</tr>
<tr>
<td>3</td>
<td>194.234.48.26</td>
<td>8565</td>
<td>8565</td>
<td>8565</td>
<td>8565</td>
</tr>
<tr>
<td>4</td>
<td>147.8.182.157</td>
<td>4096</td>
<td>4096</td>
<td>4096</td>
<td>4096</td>
</tr>
<tr>
<td>5</td>
<td>194.204.334.131</td>
<td>3052</td>
<td>3052</td>
<td>3052</td>
<td>3052</td>
</tr>
</tbody>
</table>

Top Destination Hosts

<table>
<thead>
<tr>
<th>#</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>1</td>
<td>MY.NET.253.11</td>
<td>19</td>
<td>294</td>
<td>17</td>
<td>24</td>
</tr>
<tr>
<td>2</td>
<td>MY.NET.21.15</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>MY.NET.5.125</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>MY.NET.11.212</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>MY.NET.223.255</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

Snort rule:

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN SYN FIN";flags:SF; reference:arachnids,198;)

The number of 27067 destinations shows that MY.NET has been seriously scanned. Most scanned ports were 21, 109 and 53. The lines below show one example of SYN-FIN scan on port 21.

12/12-06:11:20.503923  [**] SYN-FIN scan! [**] 132.68.37.141:21 -> MY.NET.4.249:21
12/12-06:11:20.763860  [**] SYN-FIN scan! [**] 132.68.37.141:21 -> MY.NET.5.7:21
12/12-06:11:20.784158  [**] SYN-FIN scan! [**] 132.68.37.141:21 -> MY.NET.5.8:21
12/12-06:11:20.864150  [**] SYN-FIN scan! [**] 132.68.37.141:21 -> MY.NET.5.12:21
12/12-06:11:20.884078  [**] SYN-FIN scan! [**] 132.68.37.141:21 -> MY.NET.5.13:21

3.3 DNS udp DoS attack described on unisog

DNS udp DoS attack described on unisog  8 sources   16 destinations

Top Source Hosts

<table>
<thead>
<tr>
<th>#</th>
<th>Sources</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>209.67.50.203</td>
<td>16132</td>
<td>16132</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>209.67.50.253</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>209.67.50.85</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>209.67.50.209</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>209.67.50.241</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Top Destination Hosts

<table>
<thead>
<tr>
<th></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>1</td>
<td>MY.NET.1.3</td>
<td>5411</td>
<td>5452</td>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>MY.NET.1.4</td>
<td>5390</td>
<td>5408</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>MY.NET.1.5</td>
<td>5331</td>
<td>5352</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>MY.NET.1.8</td>
<td>6</td>
<td>3219</td>
<td>4</td>
<td>31</td>
</tr>
<tr>
<td>5</td>
<td>MY.NET.1.10</td>
<td>6</td>
<td>1279</td>
<td>3</td>
<td>22</td>
</tr>
</tbody>
</table>

IP address 209.67.50.203 attacks DNS servers (MY.NET.1.3, MY.NET.1.4, MY.NET.1.5) with udp packets (rate of 60 per second). The lines below show some of the Snort records:

- 01/06-18:31:00.300393 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:15835 -> MY.NET.1.4:53
- 01/06-18:31:01.544243 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:16097 -> MY.NET.1.3:53
- 01/06-18:31:02.539097 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:10054 -> MY.NET.1.4:53
- 01/06-18:31:02.586111 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:4890 -> MY.NET.1.3:53
- 01/06-18:31:02.686219 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:3638 -> MY.NET.1.4:53

I have found the rapport of DNS udp on (6) and DNS udp packets repeated only 2 per second.

**3.4 Tiny Fragments - Possible Hostile Activity**

Event description: "With many IP implementations it is possible to impose an unusually small fragment size on outgoing packets. If the fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it didn't hit a match in the filter." (7) The tiny fragment attack is designed to fool the IDS.

Tiny Fragments - Possible Hostile Activity       26 sources         12 destinations

Top Source Hosts

<table>
<thead>
<tr>
<th></th>
<th>Sources</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>65.4.87.43</td>
<td>733</td>
<td>733</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>202.205.5.10</td>
<td>521</td>
<td>521</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>202.101.43.122</td>
<td>460</td>
<td>460</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>61.134.9.133</td>
<td>458</td>
<td>458</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>61.140.75.3</td>
<td>415</td>
<td>415</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
### Top Destination Hosts

<table>
<thead>
<tr>
<th></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>1</td>
<td>MY.NET.1.8</td>
<td>3148</td>
<td>3219</td>
<td>17</td>
<td>31</td>
</tr>
<tr>
<td>2</td>
<td>MY.NET.1.10</td>
<td>1264</td>
<td>1279</td>
<td>14</td>
<td>22</td>
</tr>
<tr>
<td>3</td>
<td>MY.NET.217.162</td>
<td>727</td>
<td>733</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>MY.NET.60.11</td>
<td>168</td>
<td>1456</td>
<td>2</td>
<td>140</td>
</tr>
<tr>
<td>5</td>
<td>MY.NET.1.9</td>
<td>8</td>
<td>16</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

I'll point that some of the Tiny Fragments - Possible Hostile Activity took place at same time as DNS udp DoS attack and it shows the lines below.
01/06-19:14:50.459957  **[**] DNS udp DoS attack described on unisog [**] 209.67.50.203:8660 -> MY.NET.1.3:53
01/06-19:14:50.511252  **[**] DNS udp DoS attack described on unisog [**] 209.67.50.203:5889 -> MY.NET.1.3:53
01/06-19:14:50.672602  **[**] Tiny Fragments - Possible Hostile Activity [**] 202.205.5.10 -> MY.NET.1.8
01/06-19:14:50.672647  **[**] Tiny Fragments - Possible Hostile Activity [**] 202.205.5.10 -> MY.NET.1.8
01/06-19:14:50.702372  **[**] DNS udp DoS attack described on unisog [**] 209.67.50.203:29297 -> MY.NET.1.4:53
01/06-19:14:51.027301  **[**] DNS udp DoS attack described on unisog [**] 209.67.50.203:13164 -> MY.NET.1.4:53
It will require further review.

### 3.5 Connect to 515 from outside

Port 515/tcp uses to access to printer service ports and printing service is called LPRng. According to CVE-2000-0917 "Format string vulnerability in use_syslog() function in LPRng 3.6.24 allows remote attackers to execute arbitrary commands."

| Connect to 515 from outside | 9 sources | 2876 destinations |

### Top Source Hosts

<table>
<thead>
<tr>
<th></th>
<th>Sources</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>141.211.176.99</td>
<td>2236</td>
<td>2236</td>
<td>2195</td>
<td>2195</td>
</tr>
<tr>
<td>2</td>
<td>216.119.15.88</td>
<td>1273</td>
<td>1273</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>209.217.166.69</td>
<td>713</td>
<td>713</td>
<td>710</td>
<td>710</td>
</tr>
<tr>
<td>4</td>
<td>192.118.36.9</td>
<td>7</td>
<td>7</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>64.46.70.175</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Top Destination Hosts

<table>
<thead>
<tr>
<th>#</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>1</td>
<td>MY.NET.100.209</td>
<td>405</td>
<td>405</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>MY.NET.99.104</td>
<td>403</td>
<td>406</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>MY.NET.130.86</td>
<td>259</td>
<td>260</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>MY.NET.214.166</td>
<td>209</td>
<td>211</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>MY.NET.20.1</td>
<td>7</td>
<td>10</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

The number of 2876 destinations shows that MY.NET has been scanned on port 515 and the first four destinations IP addresses, from table above, require further investigation.

Snort rules, which can detect LPRng exploits:
alert tcp $EXTERNAL_NET any -> $HOME_NET 515 (msg:"EXPLOIT LPRng overflow"; flags: A+; content:"/43 07 89 5B 08 8D 4B 08 89 43 0C B0 0B CD 80 31 C0 FE C0 CD 80 E8 94 FF FF FF 2F 62 69 6E 2F 73 68 0A/"; reference:bugtraq,1712;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 515 (msg:"EXPLOIT redhat 7.0 lprd overflow"; flags: A+; content:"[58 58 58 58 25 2E 31 37 32 75 25 33 30 30 24 6E]";)

Snort records:
[**] connect to 515 from outside [**] 141.211.176.99:4683 -> MY.NET.71.56:515
[**] connect to 515 from outside [**] 141.211.176.99:4719 -> MY.NET.71.90:515
[**] connect to 515 from outside [**] 141.211.176.99:4732 -> MY.NET.71.103:515
[**] connect to 515 from outside [**] 141.211.176.99:4873 -> MY.NET.71.244:515
[**] connect to 515 from outside [**] 141.211.176.99:1714 -> MY.NET.75.35:515

4. Other Alerts of Interest

4.1 SNMP public access

The Simple Network Management Protocol (SNMP) is used for monitoring routers, switches and other network elements (UDP port 161). For authentication, SNMP is using community strings. Default SNMP community strings, set to "public" and "private", are frequently used. SNMP public access is one of the Top Ten Internet Security Threats. (8)
Top Destination Hosts

<table>
<thead>
<tr>
<th>#</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>1</td>
<td>MY.NET.101.192</td>
<td>316</td>
<td>374</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>MY.NET.100.99</td>
<td>104</td>
<td>106</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>MY.NET.50.154</td>
<td>94</td>
<td>94</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>MY.NET.100.143</td>
<td>36</td>
<td>37</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>MY.NET.100.206</td>
<td>21</td>
<td>22</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Snort rule:
alert udp any any -> $HOME_NET 161 (msg: "SNMP public access"; content:"public");

IP address targeted three computers on MY.NET (MY.NET.100.99, MY.NET.100.143 and MY.NET.100.206) and the next lines shows some Snort records.

01/12-09:56:42.477347 [**] SNMP public access [**] 128.46.156.231:2159 -> MY.NET.100.206:161
01/12-09:56:43.001464 [**] SNMP public access [**] 128.46.156.231:2163 -> MY.NET.100.143:161
01/12-09:56:48.423324 [**] SNMP public access [**] 128.46.156.231:2168 -> MY.NET.100.99:161
01/12-09:56:50.337560 [**] SNMP public access [**] 128.46.156.231:2171 -> MY.NET.100.99:161
01/12-09:56:53.542213 [**] SNMP public access [**] 128.46.156.231:2173 -> MY.NET.100.99:161

For this alert, there are 20 sources and 7 destinations and it's something odd. It must be opposite, i.e. more destinations than sources and it means there are always more network elements than network management stations.

It will require further investigation.

4.2 Russia Dynamo - SANS Flash 28-jul-00

The SANS Institute wrote:
"SANS Flash Report: Trojans Sending More Data To Russia
July 28, 2000, 6:20 pm, EDT

This is preliminary information. The GIAC (Global Incident Analysis Center) has received several submissions showing large amounts of data being sent, illegitimately, from Windows 98 machines to a Russian IP address (194.87.6.X). The cause is most probably a Trojan, but whatever it is, it is moving fast."
SANS Intrusion Detection & Analysis Certification  
New Orleans January 28 - February 2, 2001

Top Source Hosts

<table>
<thead>
<tr>
<th># Sources</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 MY.NET.205.138</td>
<td>442</td>
<td>442</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2 194.87.6.38</td>
<td>104</td>
<td>104</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Top Destination Hosts

<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>1 194.87.6.38</td>
<td>442</td>
<td>442</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2 MY.NET.205.138</td>
<td>104</td>
<td>108</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

The lines below come from Snort and we can see traffic in both directions.

...  
12/08-16:08:54.086006 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 -> MY.NET.205.138:6699  
12/08-16:08:56.777675 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:08:57.590220 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:08:59.189855 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 -> MY.NET.205.138:6699  
12/08-16:08:59.672791 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:09:00.315359 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 -> MY.NET.205.138:6699  
12/08-16:09:01.419429 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:09:01.419771 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:09:01.900908 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:09:01.901472 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:09:02.217496 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 -> MY.NET.205.138:6699  
12/08-16:09:03.692655 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:09:05.164572 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:09:14.532328 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 -> MY.NET.205.138:6699  
12/08-16:09:18.221557 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478  
12/08-16:09:20.714259 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]  
MY.NET.205.138:6699 -> 194.87.6.38:2478
It is an evidence that computer MY.NET.205.138 was probably infected with Trojan.

4.3 Broadcast Ping to subnet 70

Event description: "ICMP messages to broadcast addresses are allowed, allowing for a Smurf attack that can cause a denial of service." (9)

Top Source Hosts

<table>
<thead>
<tr>
<th>#</th>
<th>Sources</th>
<th># Alerts (sig)</th>
<th># Alerts (total)</th>
<th># Srcs (sig)</th>
<th># Srcs (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>213.154.131.131</td>
<td>52</td>
<td>52</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>194.102.93.101</td>
<td>26</td>
<td>26</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>193.231.220.91</td>
<td>17</td>
<td>17</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>193.231.220.137</td>
<td>12</td>
<td>12</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>193.231.220.238</td>
<td>8</td>
<td>8</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Top Destination Hosts

<table>
<thead>
<tr>
<th>#</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>1</td>
<td>MY.NET.70.255</td>
<td>151</td>
<td>153</td>
<td>23</td>
<td>25</td>
</tr>
</tbody>
</table>

Detailed analyze of the summary field (SnortSnarf) shows that 2 different signatures are present for MY.NET.70.255 as a destination:
- 2 instances of SYN-FIN scan!
- 151 instances of Broadcast Ping to subnet 70.

I don't know addressing scheme and all net masks on MY.NET. If MY.NET.70.255 is a broadcast address, this net possibly would be used as a smurf amplifier. If not, MY.NET.70.255 requires further investigation. For example, Loki traffic, which is using for covering the tracks, looks like ICMP traffic.

4.4 Back Orifice

Back orifice is well known backdoor, with many versions. Old Back Orifice port was UDP 31337, but today Back Orifice hasn't default port.

All alerts under this headline require further investigation.

4.5 Attempt Sun RPC high port access, SUNRPC highport access and External RPC call

"Sun's Remote Procedure Call (RPC) protocol [Sun Microsystems, 1988, 1990] underlies many of the new services. Unfortunately, many of these services represent potential security problems " (10)
Remote Procedure Calls is, also, one of the Top Ten Internet Security Threats. (8)

All alerts under this headline require further investigation.

**Conclusion**

From the Table 1, we can see many signatures and they can cover one attack scenario, i.e. reconnaissance, penetration and denial of service.

MY.NET scanned heavily and the most popular scan was "SYN - FIN scan".

There are many signs that traffic on MY.NET was probably gnutella related.

On MY.NET, there are many examples of strange traffic, like Tiny Fragments, Connect to 515 from outside and inside, SNMP public access, RPC traffic. It will require further investigation.

Russia Dynamo - SANS Flash 28-jul-00 is one example that MY.NET has computer infected probably with "Trojans Sending More Data To Russia".

"DNS udp DoS attack described on unisog" and "Broadcast Ping to subnet 70" are examples of Denial of Service attacks on MY.NET.

**Resources and References**

1. [http://www.sans.org/giactc/GCIA_assignment.htm#7](http://www.sans.org/giactc/GCIA_assignment.htm#7)
2. [http://www.sans.org/y2k/052000.htm](http://www.sans.org/y2k/052000.htm)
3. [http://www.gnutella.co.uk/about/](http://www.gnutella.co.uk/about/)
4. [http://gnutella.nerdherd.net/tutorial.htm](http://gnutella.nerdherd.net/tutorial.htm)
8. [http://www.sans.org/topten.htm](http://www.sans.org/topten.htm)
10. (Firewalls and Internet Security, Repelling the Wily Hacker, William R. Cheswick, Steven M. Belovin, Addison - Wesley Publishing Company)
## Upcoming Training

<table>
<thead>
<tr>
<th>Training Event</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Rocky Mountain 2019</td>
<td>Denver, CO</td>
<td>Jul 15, 2019 - Jul 20, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Summer 2019</td>
<td>Boston, MA</td>
<td>Jul 29, 2019 - Aug 03, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Chicago 2019</td>
<td>Chicago, IL</td>
<td>Aug 19, 2019 - Aug 24, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Seattle SEC503</td>
<td>Seattle, WA</td>
<td>Aug 19, 2019 - Aug 24, 2019</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Canberra Spring 2019</td>
<td>Canberra, Australia</td>
<td>Sep 02, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2019</td>
<td>Las Vegas, NV</td>
<td>Sep 09, 2019 - Sep 16, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Oslo September 2019</td>
<td>Oslo, Norway</td>
<td>Sep 09, 2019 - Sep 14, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2019</td>
<td>London, United Kingdom</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2019</td>
<td>Dallas, TX</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cairo October 2019</td>
<td>Cairo, Egypt</td>
<td>Oct 19, 2019 - Oct 24, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Santa Monica 2019</td>
<td>Santa Monica, CA</td>
<td>Oct 21, 2019 - Oct 26, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Toronto SEC503</td>
<td>Toronto, ON</td>
<td>Nov 04, 2019 - Nov 09, 2019</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Frankfurt December 2019</td>
<td>Frankfurt, Germany</td>
<td>Dec 09, 2019 - Dec 14, 2019</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>