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
Reuben Rubio  
GCIA Practical Assignment Version 2.9  

Table of Contents  

Assignment 1 - Network Detects  

Trace 1 - Bind Inverse Query / Version Query  
Trace 2 - RPCBIND  
Trace 3 - Scan Proxy - 8080/tcp  
Trace 4 - Anonymous FTP  
Trace 5 - Squid Scan - 3128/tcp  

Assignment 2 - A Paper on Intrusion Detection Approach or Strategy  

"Outsourced IDS Monitoring as a Tool"  

Assignment 3 - Analyze this Scenario  

3.1 File Selection  
3.2 List of Detects  
3.3 Top Talkers  
3.4 External IPs with Registration Information  
3.5 Links to OOS Files  
3.6 Possibility of Compromised Systems / Anomalous Activity  
3.7 Defensive Recommendation  
3.8 Analysis Process  

References
1.0 Network Detects

Trace 1 Bind RECON/Attack

1.1 Version Query

Bind is a well-known service that is known for a lot of vulnerabilities. DNS Servers provide hostname to ip address mapping for hosts connected to the Internet. When used correctly, DNS provides attackers precious information about organizations registration information, name servers for the domain, and even the administrative contact for social engineering.

Source of Trace: My administered NETWORK

SNORT

```plaintext
[**] MISC-DNS-version-query [**]
06/26-08:18:27.974657 200.207.120.46:3897-> my.net.work.187:53
UDP TTL:49 TOS:0x0 ID:7070 IpLen:20 DgmLen:58 Len: 38

TCPDUMP
08:18:27.974657 < 200.207.120.46:3897 > my.net.work.187.domain: 4660 [b2&3=0x80] TXT CHAOS?q version.bind. (30) (ttl 49, id 7070)
08:18:27.975803 < my.net.work.129.domain > 200.207.120.46:3897: 4660 ServFail 0/0/0 (30) (DF) (ttl 255, id 52035)
```

Trace 1.2 Inverse Query

Gauntlet Firewall


SNORT

```plaintext
[**] IDS277 - NAMED Iquery Probe [**]
UDP TTL:49 TOS:0x0 ID:32221 IpLen:20 DgmLen:51 Len: 31

[**] IDS277 - NAMED Iquery Probe [**]
UDP TTL:49 TOS:0x0 ID:32223 IpLen:20 DgmLen:51 Len: 31

[**] IDS277 - NAMED Iquery Probe [**]
06/26-13:39:04.807129 210.107.197.183:4540->
```
Probability the Address was spoofed:
Address was probably not spoofed because the attacker needs to see the response of the target system to see the expected result. Once the target is compromised, attacker needs to establish a session with the victim.

Description of Attack: Bind Inverse Query Vulnerability
Trace 1.1 shows that an attacker is querying a particular IP address for the Bind Version that the server is running. By doing so, the attacker is able to determine if there is a possibility of compromising the server by exploiting a particular bind vulnerability like the inverse query vulnerability or the zone transfer vulnerability.

Trace 1.2 shows that the attacker is trying to exploit the inverse query vulnerability by launching it against a range of IP Addresses hoping to actually hit a vulnerable name server.

SecurityFocus defines this vulnerability as "A buffer overflow exists in certain versions of BIND, the nameserver daemon currently maintained by the Internet Software Consortium (ISC). BIND fails to properly bound the data received when processing an inverse query. Upon a memory copy, portions of the program can be overwritten, and arbitrary commands run on the affected host.

1Trace 1.2 also indicates that the impatient attacker does not even need to query bind versions, he just launches the attack anyway hoping to hit a server that is vulnerable.

The CVE reference number for this vulnerability is CVE-1999-0009.

1http://www.securityfocus.com/vdb/bottom.html?section=discussion&vid=134
<table>
<thead>
<tr>
<th>Name</th>
<th>CVE-1999-0009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Inverse query buffer overflow in BIND 4.9 and BIND 8 Releases.</td>
</tr>
</tbody>
</table>

Correlation:
DNS attacks are one of the 10 most popular attacks launched in the Internet today. Candidates taking the Intrusion Detection Practical have time and time again encountered this attack and a lot of information can be found in the posted GCIA practicum's.

Evidence of Active Targeting:
The attacker in both traces seems to indicate that they are simply launching attacks blindly. If they really wanted to attack the server that is running bind, they could have done their homework first by checking the registry database (arin, ripe, or apnic). But then again, it may be an attempt to lead the analyst into thinking that it is a harmless dns probe in order to hide what is really happening in the background.

Severity:
\[
\text{Severity} = (\text{Criticality} + \text{Lethality}) - (\text{System Countermeasures} + \text{Network Countermeasures}) \\
= (5 + 2) - (3 + 5) \\
= -1
\]

Criticality = 5 because DNS Servers provide valuable service and information
Lethality = 2 because attack seems to indicate that it was more of a reconnaissance than an actual attempt against the actual DNS Server
System Countermeasures = 3 because system is not running latest version of bind
Network Countermeasures = 4 because network is protected by a firewall

Defensive Recommendation:
Upgrade to Bind 9.1.3
Enforce ACLs on the border router to limit access to port 53. Since DNS server on the network is just querying, port 53/udp should only be outbound. Port 53/tcp should be blocked.

Multiple Choice Question:
When can port 53/tcp be blocked on the border routers?
- a. Never
- b. DNS Zone Transfers are not required
- c. DNS is a caching server
- d. DNS Server forwarding server

ANSWER: B - Port 53/tcp is only used for Zone Transfers

Trace 2 RPCBIND

Most applications talk to each other via RPC or remote procedure call. RPC uses a program called portmapper to listen and assign ports to running applications. RPCINFO, or it's Windows
counterpart rpcdump, queries port 111 to determine if the target machine is running services that
can be exploited like rpc.cmsd, or rpc.statd, rpc.ttdbserverd.

Source of Trace: MY Administered NETWORK

Detect was generated by:

Gauntlet Firewall

Jun 27 23:48:01 my.network.com unix: securityalert: no match found in local screen: TCP
if=qe3 srcaddr=209.235.8.94 srcport=2188 dstaddr=my.net.work.97 dstport=111
Jun 27 23:48:01 my.network.com unix: securityalert: no match found in local screen: TCP
if=qe3 srcaddr=209.235.8.94 srcport=2188 dstaddr=my.net.work.97 dstport=111

SNORT

Two different sources are included in the table shown below. This table was generated by using
Snortsnarf to process the alert file. This IP Addresses stands out because of the frequency of the
attempts to connect to rpcbind. A closer look at the IP Address reveals that they are coming
from the 209 IP Address belongs to a web hosting facility located in New York,
www.dumbnews.com. The 200.54.185.51 IP Address belongs to a University in Chile,
Universidad Autonoma Del Sur.

<table>
<thead>
<tr>
<th>Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Port</th>
<th>Protocol</th>
<th>Length</th>
<th>TTL</th>
<th>TOS</th>
<th>ID</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/27-06:26:26.128684</td>
<td>200.54.185.51</td>
<td>my.net.work.100</td>
<td>111</td>
<td>UDP</td>
<td>64</td>
<td>48</td>
<td>0x0</td>
<td>25352</td>
<td>872</td>
<td>my.net.work.100</td>
</tr>
<tr>
<td>06/27-06:26:26.340134</td>
<td>200.54.185.51</td>
<td>my.net.work.114</td>
<td>111</td>
<td>UDP</td>
<td>64</td>
<td>48</td>
<td>0x0</td>
<td>25361</td>
<td>873</td>
<td>my.net.work.114</td>
</tr>
<tr>
<td>06/27-06:26:26.551136</td>
<td>200.54.185.51</td>
<td>my.net.work.116</td>
<td>111</td>
<td>UDP</td>
<td>64</td>
<td>48</td>
<td>0x0</td>
<td>25365</td>
<td>874</td>
<td>my.net.work.116</td>
</tr>
<tr>
<td>06/27-06:26:26.762137</td>
<td>200.54.185.51</td>
<td>my.net.work.118</td>
<td>111</td>
<td>UDP</td>
<td>64</td>
<td>48</td>
<td>0x0</td>
<td>25368</td>
<td>875</td>
<td>my.net.work.118</td>
</tr>
<tr>
<td>06/27-06:26:26.973636</td>
<td>200.54.185.51</td>
<td>my.net.work.120</td>
<td>111</td>
<td>UDP</td>
<td>64</td>
<td>48</td>
<td>0x0</td>
<td>25373</td>
<td>876</td>
<td>my.net.work.120</td>
</tr>
</tbody>
</table>
TCPDUMP

At this point, we need to highlight the differences between the Snort Alert and the Gauntlet Alert. The Gauntlet Alert is port 111/tcp, Snort is port 111/udp, both ports are...
used by rpcbind. By using tcpdump to playback the traffic during this time period, we are able to determine that both alerts are correct. Probes to the udp port and the tcp port are indeed happening.

23:48:46.036215 209.235.8.94.2188 > my.net.work.97.sunrpc: S 2191294704:2191294704(0) win 32120 <mss 1460,sackOK,timestamp 51801432 0,nop,wscale 0> (DF)
23:48:46.036807 209.235.8.94.2190 > my.net.work.99.sunrpc: S 2198563057:2198563057(0) win 32120 <mss 1460,sackOK,timestamp 51801432 0,nop,wscale 0> (DF)
23:48:46.037574 my.net.work.99.sunrpc > 209.235.8.94.2190: S 3389103386:3389103386(0) ack 2198563058 win 10136 <nop,nop,timestamp 121974283 51801432,nop,wscale 0,mss 1460> (DF)
... cut for brevity
23:48:46.202672 209.235.8.94.2190 > my.net.work.99.sunrpc: F 1:1(0) ack 1 win 32120 <nop,nop,timestamp 0 121974283> (DF)
23:48:46.203189 my.net.work.99.sunrpc > 209.235.8.94.2190: . ack 1 win 10136 <nop,nop,timestamp 121974299 51801446> (DF)
23:48:49.202513 209.235.8.94.2190 > my.net.work.99.sunrpc: F 1:1(0) ack 1 win 32120 <nop,nop,timestamp 51801751 121974299> (DF)
23:48:49.202887 my.net.work.99.sunrpc > 209.235.8.94.2190: . ack 2 win 10136 <nop,nop,timestamp 121974599 51801751> (DF)
23:48:49.203606 my.net.work.99.sunrpc > 209.235.8.94.2190: F 1:1(0) ack 2 win 10136 <nop,nop,timestamp 121974599 51801751> (DF)
23:48:49.226982 209.235.8.94.2190 > my.net.work.99.sunrpc: . ack 2 win 32120 <nop,nop,timestamp 51801753 121974599> (DF)

Probability the Address was spoofed:
Address is not spoofed because attacker needs to see the reply of the victim machine. What I find interesting though is the ephemeral ports of the two attackers are coming almost from the same range, 870-890. Could they be using the same tool? Could they be the same attacker? Probably. Or could they just be using the same tool? Probably.

Description of Attack:
RPCBIND can reveal a treasure chest of vulnerabilities. From buffer overflows, remote command execution, to actual attacker access that eventually leads to root user compromise.
Listed below are several references to such vulnerabilities related to RPCBIND or Portmapper.
www.cert.org/advisories/CA-1999-05.html
Attack Mechanism:
Attacker queries rpcbind to identify rpc services that are running on target machine. Attacker goes back to exploit vulnerabilities depending on what what revealed by rpcinfo query on the target machine.
Correlation:
RPCBIND is also listed on in the SANS top 10. Please refer to http://www.sans.org/topten.htm for more information.

Evidence of Active Targeting:
There is no evidence of active targeting. However, the attacker is maliciously trying to break-in to machines in the network. These attackers do not care if they know your organization or not, as long as they see that you are vulnerable, my network is a likely target.

Severity:
Severity = ( Criticality + Lethality ) - ( System Countermeasures + Network Countermeasures )

= ( 2 + 4 ) - ( 4 + 4 )

Criticality = 2 because it was more of a sweep than an actual attack to a live server
Lethality = 4 because the exploit can lead to a system compromise.
System Countermeasures = 4 because unnecessary services have been disable. Latest patches are installed on the system.
Network Countermeasures = 4 because hosts are protected by a firewall.

Defensive Recommendation
Block 111 on the border router. Make sure that latest and greatest patches are installed in the system. Replace RPC with secure rpc whenever possible or disable it if the applications on the server does not require rpc.

Multiple Choice Question:
23:48:46.036807 209.235.8.94.2190 > my.net.work.99.sunrpc: S 2198563057:2198563057(0) win 32120 <mss 1460,sackOK,timestamp 51801432 0,nop,wscale 0> (DF)
23:48:46.037574 my.net.work.99.sunrpc > 209.235.8.94.2190: S 3389103386:3389103386(0) ack 2198563058 win 10136 <nop,timestamp 121974283 51801432,nop,wscale 0,mss 1460> (DF)
23:48:46.153526 209.235.8.94.2190 > my.net.work.99.sunrpc: . ack 1 win 32120 <nop,timestamp 51801446 121974283> (DF)
23:48:46.170747 my.net.work.99.sunrpc > 209.235.8.94.2190: S 3389103386:3389103386(0) ack 2198563058 win 10136 <nop,timestamp 121974283> (DF)
23:48:46.202672 209.235.8.94.2190 > my.net.work.99.sunrpc: F 1:1(0) ack 1 win 32120 <nop,timestamp 51801751 121974299> (DF)
23:48:49.202513 209.235.8.94.2190 > my.net.work.99.sunrpc: F 1:1(0) ack 1 win 32120 <nop,timestamp 51801751 121974299> (DF)
23:48:49.202887 my.net.work.99.sunrpc > 209.235.8.94.2190: . ack 2 win 10136 <nop,timestamp 121974599 51801751> (DF)
23:48:49.203606 my.net.work.99.sunrpc > 209.235.8.94.2190: F 1:1(0) ack 2 win 10136 <nop,timestamp 121974599 51801751> (DF)
23:48:49.226982 209.235.8.94.2190 > my.net.work.99.sunrpc: . ack 2 win 32120
<nop,nop,timestamp 51801753 121974599> (DF)

What is wrong in the trace shown above?

a. udp 56
b. ack 2 - no such thing
c. too many Syn's
d. One too many Fin's

ANSWER: D - It normally takes four segments to terminate a tcp connection. A FIN from the server, and ACK from the Client, a FIN from the client, and finally, and ACK from the server. What could cause this session to have one extra FIN? What can this be used for? Or is this just a retransmit?

Trace 3 Scanning for Port 8080 - Proxy Scans

Source of Trace: MY Administered NETWORK
Detect was generated by:
Gauntlet Firewall

This is scary, firewall logs does not indicate any security violation. It's either the Firewall Security Policies were not violated, meaning packet was accepted and delivered to destination or logs were simply not written on /var/log/messages.
Firewall policies reveal that there should have been a security violation. Not sure why logs were not created for this event.

SNORT

[**] SCAN Proxy attempt [**]
06/26-22:19:38.266178 64.20.213.222:1064-> my.net.work.98:8080
TCP TTL:116 TOS:0x0 ID:17666 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1A7F03 Ack: 0x0 Win: 0x16D0 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] SCAN Proxy attempt [**]
06/26-22:19:38.342312 64.20.213.222:1065-> my.net.work.98:8080
TCP TTL:116 TOS:0x0 ID:18178 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1A7F02C Ack: 0x0 Win: 0x16D0 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] SCAN Proxy attempt [**]
06/26-22:19:39.594965 64.20.213.222:1064->
my.net.work.98:8080
TCP TTL:116 TOS:0x0 ID:20482 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1A7F03 Ack: 0x0 Win: 0x16D0 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] SCAN Proxy attempt [**]
06/26-22:19:39.693077 64.20.213.222:1065->
my.net.work.98:8080
TCP TTL:116 TOS:0x0 ID:20738 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1A7F2C Ack: 0x0 Win: 0x16D0 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] SCAN Proxy attempt [**]
06/26-22:19:40.987951 64.20.213.222:1064->
my.net.work.98:8080
TCP TTL:116 TOS:0x0 ID:23554 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1A7F03 Ack: 0x0 Win: 0x16D0 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] SCAN Proxy attempt [**]
06/26-22:19:42.394917 64.20.213.222:1064->
my.net.work.98:8080
TCP TTL:116 TOS:0x0 ID:26114 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1A7F03 Ack: 0x0 Win: 0x16D0 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] SCAN Proxy attempt [**]
06/26-22:19:42.401905 64.20.213.222:1065->
my.net.work.98:8080
TCP TTL:116 TOS:0x0 ID:26370 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1A7F2C Ack: 0x0 Win: 0x16D0 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

TCPDUMP

22:19:38.266178 64.20.213.222.1064 > my.net.work.98.8080: S
1736451:1736451(0) win 5840 <mss 536,nop,nop,sackOK> (DF) (ttl
116, id 17666)
Probability the Address was spoofed:
Zero, attacker needs to see the response in order to determine if the target machine is functioning as a proxy server.

Description of Attack:
This was not an attack, it was more of a reconnaissance effort done by that attacker to see if port 8080 was open. Port 8080 seems to be associated with Proxy Services. It is very likely that the
attacker was looking for open proxies that can be used to anonymize their requests. In doing so, they are hoping to cover their tracks.

Attempts to connect to port 8080 may also be an indication of an attempt to exploit vulnerabilities against the Microsoft Proxy Server, and other proxy servers mentioned below.

Attack Mechanism:

<table>
<thead>
<tr>
<th>Name</th>
<th>CAN-2001-0239 (under review)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Microsoft Internet Security and Acceleration (ISA) Server 2000 Web Proxy allows remote attackers to cause a denial of service, and possibly execute arbitrary commands, via a long web request with a specific type.</td>
</tr>
<tr>
<td>References</td>
<td></td>
</tr>
<tr>
<td>References</td>
<td>BUGTRAQ:20010416 [SX-20010320-2] - Microsoft ISA Server Denial of Service</td>
</tr>
<tr>
<td>References</td>
<td>URL:<a href="http://www.securityfocus.com/archive/1/176912">http://www.securityfocus.com/archive/1/176912</a></td>
</tr>
<tr>
<td>References</td>
<td>BUGTRAQ:20010427 Microsoft ISA Server Vulnerability</td>
</tr>
<tr>
<td>References</td>
<td>URL:<a href="http://www.securityfocus.com/archive/1/179986">http://www.securityfocus.com/archive/1/179986</a></td>
</tr>
<tr>
<td>References</td>
<td>BUGTRAQ:20010417 [SX-20010320-2b] - Followup re. Microsoft ISA Server Denial of Service</td>
</tr>
<tr>
<td>References</td>
<td>URL:<a href="http://www.securityfocus.com/archive/1/177160">http://www.securityfocus.com/archive/1/177160</a></td>
</tr>
<tr>
<td>References</td>
<td>MS:MS01-021</td>
</tr>
<tr>
<td>References</td>
<td>URL:<a href="http://www.microsoft.com/technet/security/bulletin/MS01-021.asp">http://www.microsoft.com/technet/security/bulletin/MS01-021.asp</a></td>
</tr>
<tr>
<td>References</td>
<td>BID:2600</td>
</tr>
<tr>
<td>References</td>
<td>URL:<a href="http://www.securityfocus.com/bid/2600">http://www.securityfocus.com/bid/2600</a></td>
</tr>
<tr>
<td>bugtraq id</td>
<td>2600</td>
</tr>
<tr>
<td>class</td>
<td>Boundary Condition Error</td>
</tr>
<tr>
<td>cve</td>
<td>CAN-2001-0239</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>CVE-2001-0129</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Buffer overflow in Tinyproxy HTTP proxy 1.3.3 and earlier allows remote attackers to cause a denial of service and possibly execute arbitrary commands via a long connect request.</td>
</tr>
</tbody>
</table>
Name | CVE-2000-0416  
---|---  
Description | NTMail 5.0.x allows network users to bypass the NTMail proxy restrictions by redirecting their requests to NTMail's web configuration server.

| Name | CVE-2000-0165  
---|---  
Description | The Delegate application proxy has several buffer overflows which allow a remote attacker to execute commands.

Correlation:

As of July 18, 2001, attacks on Port 8080 is the to 14th attack in www.incidents.org.

Evidence of Active Targeting:

The attacker seemed to know that my.net.work.98 was a proxy server. DNS information shows that the server is an anonymous ftp server hosted by navipath.net. This is definitely active targeting.

Severity:

\[
\text{Severity} = ( \text{Criticality} + \text{Lethality} ) - ( \text{System Countermeasures} + \text{Network Countermeasures} ) \\
= ( 2 + 4 ) - ( 5 + 4 ) \\
= -3
\]

Criticality = 2 because it was more of a sweep than an actual attack to a live server

Lethality = 4 because the exploit can lead to a system compromise.

System Countermeasures = 4 because unnecessary services have been disabled. Latest patches are installed on the system. Port 8080 is only accepting requests from the internal network and is enforcing authentication.

Network Countermeasures = 4 because hosts are protected by a firewall.

Defensive Recommendation

Block 8080 in the border router. Review Firewall configuration to determine why logs were not generated by the possible security violation. Upgrade to the latest and greatest version of the Firewall because we are running three versions behind already,

Multiple Choice Question:

What does 8080/tcp and 3128/tcp have in common?

a. TCP  
b. Used for Proxy Services
c. Can be used as an anonymizer

d. All of the above

e. Nothing

ANSWER: D - 8080 and 3128 are both using the TCP protocol, both are used for http proxy services, and if left open and configured incorrectly, they can be used to anonymize the requests.

Trace 4 Anonymous FTP Attempt

Source of Trace: MY NETWORK
Detect was generated by:
Gauntlet Firewall

Jun 26 22:17:04 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=213.44.212.89 srcport=3022 dstaddr=my.net.work.163 dstport=21
Jun 26 22:17:04 my.network.com ftp-gw[27081]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.161
Jun 26 22:17:04 my.network.com ftp-gw[27082]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:04 my.network.com ftp-gw[27083]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.164
Jun 26 22:17:04 my.network.com ftp-gw[27084]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.162
Jun 26 22:17:05 my.network.com ftp-gw[27085]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.165
Jun 26 22:17:05 my.network.com ftp-gw[27086]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:05 my.network.com ftp-gw[27087]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.163
Jun 26 22:17:05 my.network.com ftp-gw[27088]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.164
Jun 26 22:17:05 my.network.com ftp-gw[27089]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.162
Jun 26 22:17:05 my.network.com ftp-gw[27090]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:05 my.network.com ftp-gw[27091]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.163
Jun 26 22:17:05 my.network.com ftp-gw[27092]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.164
Jun 26 22:17:05 my.network.com ftp-gw[27093]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.162
Jun 26 22:17:05 my.network.com ftp-gw[27094]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:05 my.network.com ftp-gw[27095]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.163
Jun 26 22:17:05 my.network.com ftp-gw[27096]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.164
Jun 26 22:17:05 my.network.com ftp-gw[27097]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.162
Jun 26 22:17:05 my.network.com ftp-gw[27098]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:05 my.network.com ftp-gw[27099]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.163
Jun 26 22:17:05 my.network.com ftp-gw[27100]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.164
Jun 26 22:17:05 my.network.com ftp-gw[27101]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.162
Jun 26 22:17:05 my.network.com ftp-gw[27102]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:05 my.network.com ftp-gw[27103]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.163
Jun 26 22:17:05 my.network.com ftp-gw[27104]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.164
Jun 26 22:17:05 my.network.com ftp-gw[27105]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.162
Jun 26 22:17:05 my.network.com ftp-gw[27106]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:05 my.network.com ftp-gw[27107]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.163
Jun 26 22:17:05 my.network.com ftp-gw[27108]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.164
Jun 26 22:17:05 my.network.com ftp-gw[27109]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.162
Jun 26 22:17:05 my.network.com ftp-gw[27110]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:05 my.network.com ftp-gw[27111]: deny host=nodnsquery/213.44.212.89 connect to my.net.work.189
Jun 26 22:17:07 my.network.com ftp-gw[27088]: deny host=nodnsquery/213.44.212.89 connect to ftp.microsoft.com
Jun 26 22:17:07 my.network.com ftp-gw[27089]: exit host=nodnsquery/213.44.212.89 cmds=1 in=0 out=0 user=unauth duration=2
Jun 26 22:17:07 my.network.com ftp-gw[27090]: deny host=nodnsquery/213.44.212.89 connect to ftp.microsoft.com
Jun 26 22:17:07 my.network.com ftp-gw[27091]: exit host=nodnsquery/213.44.212.89 cmds=1 in=0 out=0 user=unauth duration=2
Jun 26 22:17:07 my.network.com ftp-gw[27092]: deny host=nodnsquery/213.44.212.89 connect to ftp.microsoft.com
Jun 26 22:17:07 my.network.com ftp-gw[27093]: exit host=nodnsquery/213.44.212.89 cmds=1 in=0 out=0 user=unauth duration=2
Jun 26 22:17:07 my.network.com ftp-gw[27094]: deny host=nodnsquery/213.44.212.89 connect to ftp.microsoft.com
Jun 26 22:17:07 my.network.com ftp-gw[27095]: exit host=nodnsquery/213.44.212.89 cmds=1 in=0 out=0 user=unauth duration=2
Jun 26 22:17:07 my.network.com ftp-gw[27096]: deny host=nodnsquery/213.44.212.89 connect to ftp.microsoft.com
Jun 26 22:17:07 my.network.com ftp-gw[27090]: exit
host=nodnsquery/213.44.212.89 cmds=1 in=0 out=0 user=unauth
duration=2
found in local screen: TCP if=ge3 srcaddr=213.44.212.89
srcport=3022 dstaddr=my.net.work.163 dstport=21
Jun 27 00:17:04 my.network.com ftp-gw[27082]: exit
host=nodnsquery/213.44.212.89 cmds=0 in=0 out=0 user=unauth
duration=7200
Jun 27 00:17:05 my.network.com ftp-gw[27110]: exit
host=nodnsquery/213.44.212.89 cmds=0 in=0 out=0 user=unauth
duration=7200

This part of the detect shows that the attacker was trying to scan for servers running ftp. After
exhausting his list, the attacker then tries to use the ftp proxy to connect to ftp.microsoft.com.
Take note of the pid ftp-gw process id 27082. This shows that the attacker tried to connect to the
gateway itself and the session ended after 7200 seconds. The ftp attempt was denied but it still
tied up 1 ftp process.

This could have been successfully used as a denial of service attack against the ftp service
running on my firewall but I guess, that was not the attackers intention. He simply wanted to use
an anonymous ftp server to connect to Microsoft’s site. At least, that is what the logs say.

We have three types of Gauntlet Alerts in this section.
Jun 26 22:17:04 my.network.com unix: securityalert: no match
found in local screen: TCP if=ge3 srcaddr=213.44.212.89
srcport=3022 dstaddr=my.net.work.163 dstport=21

This type of alert is generated by a packet screen violation. This is normally generated by
packets hitting the ip address of one of the interfaces of the firewall.

The other type of alert is generated by the proxies running on the firewall.
Jun 26 22:17:04 my.network.com ftp-gw[27083]: deny
host=nodnsquery/213.44.212.89 connect to my.net.work.164

Accepts were intentionally left out due to security reasons. Suffice it to say that some ftp
attempts were accepted by the proxy but was denied later on when the attacker tried to connect to

Jun 26 22:17:07 my.network.com ftp-gw[27089]: deny
host=nodnsquery/213.44.212.89 connect to ftp.microsoft.com

The number enclosed in brackets is the process identifier for the ftp session.

SNORT

[**] INFO FTP anonymous FTP [**]
06/26-22:17:48.615168 213.44.212.89:3027->
my.net.work.168:21
TCP TTL:112 TOS:0x0 ID:8297 IpLen:20 DgmLen:74
***AP*** Seq: 0x37F9CD9 Ack: 0x82D8E91 Win: 0x7F9B TcpLen: 20

[**] INFO FTP anonymous FTP [**]
06/26-22:17:48.702484 213.44.212.89:3028 -> my.net.work.169:21
TCP TTL:112 TOS:0x0 ID:8553 IpLen:20 DgmLen:74
***AP*** Seq: 0x37F9CDF Ack: 0x82DA446 Win: 0x7F9B TcpLen: 20

[**] INFO FTP anonymous FTP [**]
06/26-22:17:48.803983 213.44.212.89:3029 -> my.net.work.170:21
TCP TTL:112 TOS:0x0 ID:8809 IpLen:20 DgmLen:74
***AP*** Seq: 0x37F9CE1 Ack: 0x82E7560 Win: 0x7F9B TcpLen: 20

[**] INFO FTP anonymous FTP [**]
06/26-22:17:50.030472 213.44.212.89:3041 -> my.net.work.166:21
TCP TTL:112 TOS:0x0 ID:30825 IpLen:20 DgmLen:74
***AP*** Seq: 0x37F9CD7 Ack: 0x82C02AF Win: 0x7F9B TcpLen: 20

TCPDUMP
22:17:45.955582 213.44.212.89.3028 > my.net.work.169.ftp: S
58694876:58694876(0) win 32768 <mss 1460,nop,nop,eol> (ttl 112,
id 35688)
4500 0030 8b68 0000 7006 0e6d d52c d459 | E . 0 h . p . m . , Y
d0c3 36a9 0bd4 0115 037f 9cdc 0000 0000 | . . . 6 . . . . . . . .
7002 8000 a9e9 0000 0204 05b4 0101 0000 | p . . . . . . . . . .
22:17:45.956062 my.net.work.169.ftp > 213.44.212.89.3028: S
137208800:137208800(0) ack 58694877 win 8760 <mss 1460> (DF)
(ttl 255, id 11150)
4500 002c 2b8e 4000 ff06 9f4a d0c3 36a9 | E . , + . @ . . . .
d52c d459 0015 0bd4 082d a3e0 037f 9cdd | . , . Y . . . . . . .
6012 2238 6c98 0000 0204 05b4 0000 ---- | "8 1 . . . . . . . .
22:17:46.296798 213.44.212.89.3028 > my.net.work.169.ftp: . ack
1 win 32768 (ttl 112, id 52328)
4500 0028 cc68 0000 7006 cd74 d52c d459 | E . ( . h . . p . . . .
d0c3 36a9 0bd4 0115 037f 9cdd 082d a3e1 | . . . 6 . . . . . . . .
5010 8000 26bd 0000 0204 05b4 0101 ---- | P . . & . . . . . . . .
22:17:46.525403 my.net.work.169.ftp > 213.44.212.89.3028: P
1:49(48) ack 1 win 8760 (DF) (ttl 255, id 11181)
4500 0058 2bad 4000 ff06 9eff d0c3 36a9 | E . X + . @ . . . .
d52c d459 0015 0bd4 082d a3e1 037f 9cdd | . , . Y . . . . . . .
5018 2238 5952 0000 3530 3120 4e6f 7420 | P . "8 Y R . . 5 0
1 Not
7065 726d 6974 7465 6420 6f6e 6f6e | permitted to con
6e65 6374 2074 6f20 3230 382e 3136 390d0a ---- ---- ---- ---- | work . 1 6 9
\r\n. . . . . . . . 22:17:46.834796 213.44.212.89.3028 >
my.net.work.169.ftp: . ack 49 win 32720 (ttl 112, id 60264)
4500 0028 eb68 0000 7006 ae74 d52c d459 | E . ( . h . . p . . . .
d0c3 36a9 0bd4 0115 037f 9cdd 082d a411 | . . . 6 . . . . . . . .
5010 7fd0 268d 0000 0204 05b4 0101 ---- | P . . & . . . . . . . .
22:17:46.835249 my.net.work.169.ftp > 213.44.212.89.3028: P
49:102(53) ack 1 win 8760 (DF) (ttl 255, id 11201)
4500 005d 2bc1 4000 ff06 9ee6 d0c3 36a9 | E . . ] + . @ . . .
. . . . 6 .
d52c d459 0015 0bd4 082d a411 037f 9cdd | . . . Y . . . . . -
. . . . . . . .
5018 2238 0a97 0000 3232 3020 6e73 6363 | P . " 8 \n . . . 2 2
0 m y .
6677 2e67 7363 632e 636f 6d20 4654 5020 | h o s t . n a m e
. c o m F T P
7072 6f78 7920 2856 6572 7369 6f6e 2056 | p r o x y ( V e r
s i o n V
342e 3229 2072 6561 6479 2e0d 0a 4 . 2 ) r e a d y
. \r \n . . .
22:17:47.145293 213.44.212.89.3028 > my.net.work.169.ftp: . ack
102 win 32667 (ttl 112, id 65384)
4500 0028 ff68 0000 7006 9a74 d52c d459 | E . . ( . h . . p .
. t . , . . Y
d0c3 36a9 0bd4 0015 037f 9cdd 082d a446 | . . 6 . . . . . .
. . . . . . . . - . F
5010 7f9b 268d 0000 0204 05b4 0101 ---- | P . . . & . . . . . .
. . . . . . . . . . . . . .
22:17:48.702484 213.44.212.89.3028 > my.net.work.169.ftp: P
1:35(34) ack 102 win 32667 (ttl 112, id 8553)
4500 004a 2169 0000 7006 7852 d52c d459 | E . . J ! i . . p .
x R . , . Y
d0c3 36a9 0bd4 0015 037f 9cdd 082d a446 | . . 6 . . . . . .
. . . . . . . . - . F
5018 7f9b 67bb 0000 5553 4552 2061 6e6f | P . . g . . . U S
E r a n o
6e79 6d6f 7573 4066 736f 6674 2e63 6f6d 726f | n y m o u s @ f t p
. m i c r o
736f 6674 2e63 6f6d 0d0a ---- ---- ---- | s o f t . c o m
\r \n . . .
22:17:48.703000 my.net.work.169.ftp > 213.44.212.89.3028: . ack
35 win 8760 (DF) (ttl 255, id 11235)
4500 0028 2be3 4000 ff06 9ef9 d0c3 36a9 | E . . ( + . @ . .
. . . . 6 .
d52c d459 0015 0bd4 082d a446 037f 9cff | . . . Y . . . . -
. F . . . .
5010 2238 83ce 0000 0000 0000 0000 ---- | P . " 8 . . . . . .
. . . . . . . . . .
22:17:48.709862 my.net.work.169.ftp > 213.44.212.89.3028: P
102:153(51) ack 35 win 8760 (DF) (ttl 255, id 11236)
4500 005b 2be4 4000 ff06 9ec5 d0c3 36a9 | E . . [ + . @ . .
. . . . 6 .
d52c d459 0015 0bd4 082d a446 037f 9cff | . . . Y . . . . -
. F . . . .
5018 2238 fb32 0000 3530 3120 4e6f 7420 | P . " 8 . . . 5 0
1 Not
7065 726d 6974 7465 6420 746f 2063 6f6e  | permitted
to con
6e65 6374 2074 6f20 6674 702e 6d69 6372 | next to ft
p. mic
6f73 6f66 746e 6d0d 0a
\n. . . . . . . . . . .
22:17:48.717399 my.net.work.169.ftp > 213.44.212.89.3028: F
153:153(0) ack 35 win 8760 (DF) (ttl 255, id 11237)
4500 0028 2be5 4000 ff06 9ef7 d0c3 36a9 | E .. ( + . @ ...
. . . . . . . . . . 
5011 2238 839a 0000 0000 0000 0000 ---- | P. " 8 . . . . .
. . . . . . . . . .
22:17:48.875789 213.44.212.89.3028 > my.net.work.169.ftp: . ack
154 win 32616 (ttl 112, id 9321)
4500 0028 2469 0000 7006 7574 d52c d459 | E .. ( $ i . . p.
. u t . . . . . Y
d0c3 36a9 0bd4 0015 037f 9cff 082d a47a | . . 6 . . . . . . 
. . . . . . . . . .
5010 7f68 266a 0000 0204 05b4 0508 ---- | P . h & j . . . .
. . . . . . . . . .
22:17:53.893319 213.44.212.89.3028 > my.net.work.169.ftp: R
58694911:58694911(0) win 0 (ttl 112, id 32617)
4500 0028 7f69 0000 7006 1a74 d52c d459 | E .. ( . i . . p.
. . t . . . . . Y
d0c3 36a9 0bd4 0015 037f 9cff 082c 02e3 | . . 6 . . . . . . 
. . . . . . . . . .
5004 0000 4777 0000 0204 05b4 0402 ---- | P . . . G w . . . .
. . . . . . . . . .

Probability the Address was spoofed:
Address is definitely not spoofed. FTP will only happen if the FTP client receives the response of the ftp server. A RIPE IP address query reveals that the IP Address belongs to another French Internet service provider.

Description of Attack:
Logs seem to indicate that attacker was attempting to copy something over or pull something from ftp.microsoft.com. The attacker seems to be looking for a repository for binaries, trojans, or what have you's.

Attacker could have cause an FTP denial of service by tying up a limited number of ftp child processes configured to run in the system. However, the attacker does not seem to indicate any interest in creating a DOS, he just wants a ftp relay server.

Attack Mechanism:
The attacker wants to use the ftp server to possibly cover his tracks. His intention may also have been to use the ftp server as a repository for tools, and stolen information.

Correlation:
Anonymous FTP attempts are very common. This was eloquently discussed below.
"The most common attack you will see are hackers/crackers looking for "open anonymous" FTP servers. These are servers with directories that can be written to and read from. Hackers/crackers use these machines as way-points for transferring warez (pirated programs) and pr0n (intentionally misspelled word to avoid search engines classifying this document)."^2

Severity:
Severity = ( Criticality + Lethality ) - ( System Countermeasures + Network Countermeasures )
= ( 2 + 2 ) - ( 4 + 3 )
= -5

Criticality = 2 because it was more of a sweep than an actual attack to a live server
Lethality = 2 because it was more of an attempt to use a service rather than to compromise the server.
System Countermeasures = 4 because unnecessary services have been disabled. FTP is not running on the servers.
Network Countermeasures = 3 because hosts are protected by a firewall but it seems that the firewall is somehow misconfigured because it is accepting ftp sessions initiated from the external interfaces (internet)

Defensive Recommendation
Evaluate firewall rule allowing outsiders (people coming in from external sources) to initiate connections to the Firewall. This could have been an oversight on the part of the firewall admins.

Multiple Choice Question:
Jun 26 22:17:04 my.network.com ftp-gw[27082]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 26 22:17:05 my.network.com ftp-gw[27110]: deny host=nodnsquery/213.44.212.89 connect to 0.0.0.0
Jun 27 00:17:04 my.network.com ftp-gw[27082]: exit host=nodnsquery/213.44.212.89 cmd=0 in=0 out=0 user=unauth duration=7200
Jun 27 00:17:05 my.network.com ftp-gw[27110]: exit host=nodnsquery/213.44.212.89 cmd=0 in=0 out=0 user=unauth duration=7200

In the gauntlet alert above, what triggers the connect to 0.0.0.0

^2http://www.robertgraham.com/pubs/firewall-seen.html
deny message?

a. attacker hits the broadcast address  
b. attacker hits a network address  
c. attacker connects to 0.0.0.0  
d. attacker is unauthorized  

ANS: B - When the attacker accidentally connects to the network address, or start of the subnet, gauntlet sends out an alert message saying the connection to 0.0.0.0 has been denied. Then it times out after two hours. This behavior of the FTP-GW has probably been patched, or recent versions probably do not exhibit this behavior.

Trace 5    Squid Scan
Source of Trace: MY NETWORK
Detect was generated by:

Gauntlet

Jun 27 05:59:14 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=130.92.65.142 srcport=3076 dstaddr=my.net.work.97 dstport=3128
Jun 27 05:59:14 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=130.92.65.142 srcport=3142 dstaddr=my.net.work.163 dstport=3128
Jun 27 05:59:17 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=130.92.65.142 srcport=3076 dstaddr=my.net.work.97 dstport=3128
Jun 27 05:59:17 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=130.92.65.142 srcport=3142 dstaddr=my.net.work.163 dstport=3128
Jun 27 05:59:14 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=130.92.65.142 srcport=3076 dstaddr=my.net.work.97 dstport=3128
Jun 27 05:59:14 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=130.92.65.142 srcport=3142 dstaddr=my.net.work.163 dstport=3128
Jun 27 05:59:14 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=130.92.65.142 srcport=3076 dstaddr=my.net.work.97 dstport=3128
Jun 27 05:59:17 my.network.com unix: securityalert: no match found in local screen: TCP if=qe3 srcaddr=130.92.65.142 srcport=3142 dstaddr=my.net.work.163 dstport=3128

Snort

INFO - Possible Squid Scan
1 sources 65 destinations
### RAW Snort Alerts

[**] INFO - Possible Squid Scan [**]
06/27-05:59:56.803322 130.92.65.142:3075 -> my.net.work.96:3128
TCP TTL:110 TOS:0x0 ID:28035 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C34887D Ack: 0x0 Win: 0x2238 TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] INFO - Possible Squid Scan [**]
06/27-05:59:56.808544 130.92.65.142:3076 -> my.net.work.97:3128
TCP TTL:110 TOS:0x0 ID:28036 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C357ECE Ack: 0x0 Win: 0x2238 TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] INFO - Possible Squid Scan [**]
06/27-05:59:56.812145 130.92.65.142:3077 -> my.net.work.98:3128
TCP TTL:110 TOS:0x0 ID:28037 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C362B89 Ack: 0x0 Win: 0x2238 TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] INFO - Possible Squid Scan [**]
06/27-05:59:56.816328 130.92.65.142:3078 -> my.net.work.99:3128
TCP TTL:109 TOS:0x0 ID:28038 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C36B080 Ack: 0x0 Win: 0x2238 TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] INFO - Possible Squid Scan [**]
06/27-05:59:56.824330 130.92.65.142:3080 -> my.net.work.101:3128
TCP TTL:110 TOS:0x0 ID:28040 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C37F26A Ack: 0x0 Win: 0x2238 TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] INFO - Possible Squid Scan [**]
06/27-05:59:56.830193 130.92.65.142:3081 -> my.net.work.102:3128
TCP TTL:110 TOS:0x0 ID:28041 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C388C9A Ack: 0x0 Win: 0x2238 TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

Cut for Brevity ....

[**] INFO - Possible Squid Scan [**]
06/27-06:00:00.915344 130.92.65.142:3169 -> my.net.work.190:3128
TCP TTL:110 TOs:0x0 ID:29807 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C797633 Ack: 0x0 Win: 0x2238 TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK
[**] INFO - Possible Squid Scan [**]
06/27-06:00:00.915883 130.92.65.142:3170 -> my.net.work.191:3128
TCP TTL:109 TOs:0x0 ID:29814 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C7A5FF5 Ack: 0x0 Win: 0x2238 TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

TCPDUMP

5:59:56.803322 130.92.65.142.3075 > my.net.work.96.3128: S
1278511229:1278511229 (0) win 8760 <mss 1460,nop,wscale
0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) (ttl 110, id 28035)
05:59:56.804154 my.net.work.96.3128 > 130.92.65.142.3075: R
0:0(0) ack 1278511230 win 0 (DF) (ttl 110, id 19403)
05:59:56.804219 my.net.work.96.3128 > 130.92.65.142.3075: R
0:0(0) ack 1 win 0 (DF) (ttl 2, id 19404)
05:59:56.808544 130.92.65.142.3076 > my.net.work.97.3128: S
1278574286:1278574286(0) win 8760 <mss 1460,nop,wscale
0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) (ttl 110, id 28036)
05:59:56.812145 130.92.65.142.3077 > my.net.work.98.3128: S
1278618505:1278618505(0) win 8760 <mss 1460,nop,wscale
0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) (ttl 110, id 28037)
05:59:56.812770 my.net.work.98.3128 > 130.92.65.142.3077: R
0:0(0) ack 1278618506 win 0 (DF) (ttl 110, id 19405)
05:59:56.816328 130.92.65.142.3078 > my.net.work.99.3128: S
1278652544:1278652544(0) win 8760 <mss 1460,nop,wscale
0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) (ttl 110, id 29602)
05:59:56.816706 my.net.work.99.3128 > 130.92.65.142.3078: R
0:0(0) ack 1278652545 win 0 (DF) (ttl 110, id 19406)
Cut for brevity ........
06:00:00.520085 130.92.65.142.3103 > my.net.work.124.3128: S
1279799132:1279799132(0) win 8760 <mss 1460,nop,wscale
0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) (ttl 110, id 29555)
06:00:00.520524 my.net.work.124.3128 > 130.92.65.142.3103: R
0:0(0) ack 1 win 0 (DF) (ttl 110, id 19809)
06:00:00.613756 130.92.65.142.3139 > my.net.work.160.3128: S
1281502725:128150272760 win 0 (DF) (ttl 110, id 29602)
6(0) win 8760 <mss 1460,nop,wscale 0,nop,nop,timestamp 0
0,nop,nop,sackOK> (DF) (ttl 110, id 19810)
Probability the Address was spoofed:

Address is not spoofed because attacker needs to see the response to his probes.

IP Address Lookups reveal the following information:

University of Berne (NET-UNIBE)
Institute of Informatics and Applied Mathematics
Laenggassstrasse 51
CH-3012 Berne
CH
Netname: UNIBE
Netblock: 130.92.0.0 - 130.92.255.255
Coordinator:
Buetikofer, Fritz (FB61-ARIN) btkfr@ID.UNIBE.CH
+41 31 65 3843

Domain System inverse mapping provided by:

ARWEN.UNIBE.CH 130.92.9.52
SWIBE9.UNIBE.CH 130.92.1.1
SCSNMS.SWITCH.CH 130.59.10.30

Record last updated on 17-Feb-1994.
Database last updated on 3-Jul-2001 23:15:43 EDT.

> server arwen.unibe.ch
Default Server: mailhub.unibe.ch
Address: 130.92.9.52
Aliases: arwen.unibe.ch

> 130.92.65.142
Server: mailhub.unibe.ch
Address: 130.92.9.52
Aliases: arwen.unibe.ch

Name: zarkov.unibe.ch
Address: 130.92.65.142

Description of Attack:
Port 3128 is very closely related to port 8080. Both of them are commonly used for http proxy services. 3128 is the default port for Squid. The attacker is looking for open proxies for relaying or anonymizing purposes. He/She may also be looking for squid servers so that he can exploit some vulnerabilities in the future.

Attack Mechanism:
This is more of a reconnaissance effort by the attacker. This was an attempt to identify servers that is running SQUID, not a generic proxy server (Netscape, Micosoft, etc.). Once the target servers are identified, attacker will probably come back for the actual exploit or use the system to attack other servers.

Correlation:
A Bugtraq Security Advisory released on 7-19-2001 also says that Squid, versions TSL 1.01, 1.1, and 1.2, when configured with the httpd_accel_with_proxy off, accepts any requests to the proxy. This allows attacker to use the proxy to scan remote systems, etc. A vulnerability that may also be related to squid is as follows: Bugtraq ID 2059 and CVE Identifier CVE-1999-0710 which is classified as a relay or information gathering attempt.

Severity:
Severity = ( Criticality + Lethality ) - ( System Countermeasures + Network Countermeasures )

= ( 2 + 2 ) - ( 4 + 4 )
= -4

Criticality = 2 because it was more of a sweep than an actual attack to a live server
Lethality = 2 because it was more of an reconnaissance effort rather than an actual attack
System Countermeasures = 4 because unnecessary services have been disabled. Squid is not running on the servers.
Network Countermeasures = 4 because hosts are protected by a firewall and the attempt to connect to 3128 was denied
Defensive Recommendation

Review firewall configuration in an attempt to tighten up the rulebase.
Review Router ACLs and is possible, tighten up ACL config to allow only necessary services to
go in and out of the network.

Multiple Choice Question:

[**] INFO - Possible Squid Scan [**]
06/27-05:59:56.824330 130.92.65.142:3080 -> my.net.work.101:3128
TCP TTL:110 TOS:0x0 ID:28040 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C37F26A  Ack: 0x0  Win: 0x2238  TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] INFO - Possible Squid Scan [**]
06/27-05:59:56.830193 130.92.65.142:3081 -> my.net.work.102:3128
TCP TTL:110 TOS:0x0 ID:28041 IpLen:20 DgmLen:64 DF
******S* Seq: 0x4C388C9A  Ack: 0x0  Win: 0x2238  TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK
2.0 IDS Approach or Strategy

Great! Good Job! Your team has finally convinced upper management to integrate Intrusion Detection in the Corporate Infrastructure. They have approved a budget of $500K to purchase new equipment just for this initial roll out. Your teams role is to build, deploy, monitor and manage the IDS infrastructure.

Then it hits you. Is this a victory or a punishment? Your team of two, you and another admin, is expected to do the following:

1. Deploy IDS in X subnets.
   Deployment is the easy part. Tying the sensors all up and trying to correlate between all the alerts is the tricky part. You realize that you need to do this in phases. You may decide to deploy it, and work out the backend details in Phases. Management requires you to build the infrastructure ASAP.

2. Monitor and Analyze logs generated by the NIDs and HIDs
   Once the Sensors are deployed, you start getting alerts. You now have to analyze those alerts, zero in on a particular alert of interest, and decide whether you want to escalate this to your Organizations CSIRT or not.

   Your team is also responsible for assisting any Investigation required by the CSIRT to determine possible exposures or compromise.

3. Integrate CSIRT Procedures in the Organizational Chart
   OK. Let's face it. Organizations are not created equal. Your team also has to negotiate the challenges of the political environment in your organization; there are certain rules of engagement that you have to follow.

4. Intrusions do not happen on Mondays to Fridays only, management expects 24x7 Coverage.
   This is not possible. Yes your team can program the systems to give you a page or to send you email but that cannot replace trained on-site staff looking at the logs and continuously analyzing data.

   The Company needs to hire and train people. But until then, it's you and your admin buddy.

5. On the Job Training
   Intrusion Detection is a moving target. Sending people to training greatly increases the chance of success but experience is what really counts. Experience can only gained through time and exposure. Therefore, somehow, the feeling of inadequacy is there.

   The "What If?" question haunts you, and somehow, you look for gurus to point you to the right path. It is quite clear; your team is not yet as strong as management expects it to be. And considering that your infrastructure is very critical to your organizations success, you need to beef up you IDS defenses. Your organization is a target. Management hopes that your IDS infrastructure will beef up security.

   So, who are the people you can turn to? How do you handle the situation? Who has the skill,
the infrastructure, and the willingness to do IDS monitoring for you? Outsourced Security Services come in to the picture. What do the bring into the plate? Outsourced Security Service Providers are not created equal. However, the common threads that most OSS Providers seem to offer are:

2. Experienced Staff with the correct skill set focused and dedicated only to Intrusion Detection.
3. Ability to correlate IDS data with other customers thereby establishing trends that enables them to quickly integrate signatures to Managed Sensors.
4. A reporting component that allows the customer to securely view IDS reports and analysis.
5. Incident Response and Forensic capability that integrates with various external Law Enforcement Agencies.
6. Customized Training and Assistance.

At this point, we need to differentiate between Management and Monitoring. Monitoring Services is basically asking the OSSP to look at the logs and to alert you when they see something critical. On top of this, Management Services requires them to make sure that the signatures in the Sensor are current. They may consider adding a service or two depending on what your Company includes in the Service Package. Management Services for Intrusion Detection Sensors range from $2,400-$9,000 per device, per month. Monitoring services is a little bit cheaper ranging from $1,500-$3,200. The management services figures roughly translate to $28,800 per year, per sensor, 24*7*365.

The latest Salary Survey posted in the SANs webpage estimates that an Intrusion Detection Analyst earns approximately 120K per year. If an organization will do 24*7*365, this accumulates to about 4-5 doing 8-12 hour shifts round the clock, 7 days a week. In salaries alone, the organization spends roughly 600K to provide 24*7*365 coverage for IDS alone. Not to mention the recruitment process that seems to always indicate that there is not enough people with the correct experience and background, considering that IDS is relatively a new field that is evolving at light speed.

So, spending $1500, per device, for 24*7*365 is I would say, very reasonable. Why can't we just let them do the IDS for the Organization? ANSWER: Because some organizations want to keep Proprietary Data private. By allowing OSSPs to configure, tweak, and manage your IDS systems, you are giving them access to your network traffic. This can reveal trade secrets, and other proprietary data that your company is trying to protect. By limiting OSSPs to Monitoring Services, you are allowing them to see what you want them to see, just firewall logs and/or IDS Alerts.

**Outsourced Security Services as a Tool**

Just like any hardware and software solutions, IDS monitoring can be used as a tool designed to meet specific goals or targets.

IDS Monitoring helps organizations meet 24*7*365 coverage from day 1 of the implementation cycle. There is no lull time for recruitment and hiring. Most IDS Monitoring vendors claim that their staff is experienced and trained specifically for IDS.
Since my team is new in this field, it is very likely that my team will make rookie mistakes. OSSPs give me a safety net. A room for errors that I hope, in the process of correcting them, will train and transfer knowledge and expertise to me and my team.

OSSPs are not part of the Organization. Therefore, they are immune to the political climate in the organization. They can be very decisive with regards to giving advice and recommendation without fearing any political repercussions.

Most OSSPs have a direct channel to the Law Enforcement. If ever an incident happens, your selected OSSP will have a direct liason with the international community and law enforcement. This gives your organization an added level of coverage if the need to prosecute arises. The organizations CSIRT then gets a chance establish rapport, trust, and confidence with these people before the actual need to escalate or prosecute comes. This option of course, depends on the Contract or the Service Level Agreement with the vendor. There may be some retainer fees involved if this option is included in the SLA.

**In IDS Sensor Placement Is Key**

A successful Intrusion Detection Implementation requires strategic sensor placement. This requires the installation of Sensors all over the infrastructure specially the ingress points of the network. External Networks are monitored for possible attacks coming from the Internet, and Extranet, while Internal Networks are monitored for possible attacks coming from within the organization.

Organizations normally employ a multi-tiered approach in enforcing security. The first level of firewall protects web Servers or application servers, while backend systems are protected by another level of firewalls. This clearly demarks what is considered external and internal by the Organization.

Monitoring Services is a customization of the service offering of Outsource Security Services Providers. As mentioned earlier, this came about due to the need of some organizations to keep their data private.

Sensors that will be monitored by the external entity must be identified right from the very start.

a. which part of the network will most likely be an entry point
b. which part of the network is exposed 7*24
c. which part of the network is considered public
d. which part of the network is the organization most vulnerable

These questions only point to the external part of the network, after the external router, and before the firewall, the segment facing the Internet. A common approach is to have the OSSP monitor the external sensors, and have the in-house staff monitor the internal ones. This is of course, a case-to-case basis and may vary from organization to organization.
Conclusion

For Organizations that consider network data and traffic proprietary, OSSPs can be used as a tool to help meet IDS requirements. Service Level Agreements can be customized to delimit and scope what is going to be monitored and sent to the Provider. Like any tool, the organization should know the strengths of their OSSP. In-House expertise complements the selected OSSP where access to proprietary data becomes an issue. They should work hand in hand in delivering a well developed, well managed, and well-implemented Intrusion Detection Strategy.

The selection of Outsource Security Service Providers can make or break the IDS initiatives of any organization. Very much the like the selection of Hardware and Software solutions, Outsourced Security Service Providers for IDS Monitoring need to be evaluated.

3.0 Analyze This

Five days of scans, OOS files, and alerts were analyzed. I would have preferred having the knowledge of the location of the sensor to make more accurate conclusions about the data set. The intriguing part about the data set is that I could not really identify whether the sensor was in the internal part of the network or whether it was external. If I assumed it was on the internal side of the network, why am I seeing a lot of external addresses? As if the network was not protected at all.

If it was on the external side of the network, why was I seeing a lot of internal addresses? As if there was no restriction. No concept of acceptable use policy or anything like that.

I guess this is probably because I am not at all familiar with the University environment. I am used to having networks delimited by firewalls and ACLs. All servers must conform to the standard build procedure, patched, and scanned for vulnerabilities before it goes online.

3.1 File Selection - April 6-10 2001

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scans</td>
<td>OOS</td>
<td>Alerts</td>
</tr>
<tr>
<td>scans.010406</td>
<td>oos_April.6.2001</td>
<td>alert.010406</td>
</tr>
<tr>
<td>scans.010407</td>
<td>oos_April.7.2001</td>
<td>alert.010407</td>
</tr>
<tr>
<td>scans.010408</td>
<td>oos_April.8.2001</td>
<td>Alert.010408</td>
</tr>
<tr>
<td>scans.010409</td>
<td>oos_April.9.2001</td>
<td>alert.010409</td>
</tr>
<tr>
<td>scans.010410</td>
<td>oos_April.10.2001</td>
<td>alert.010410</td>
</tr>
</tbody>
</table>

3.2 List of Detects

Earliest alert at 00:00:09.156032 on 04/06/2001
Latest alert at 23:31:24.699257 on 04/10/2001
## Signature (click for sig info)

<table>
<thead>
<tr>
<th>Signature</th>
<th># Alerts</th>
<th># Sources</th>
<th># Destinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN-FIN scan!</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>STATDX UDP attack</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>connect to 515 from inside</td>
<td>5</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>ICMP SRC and DST outside network</td>
<td>6</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>NMAP TCP ping!</td>
<td>10</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Back Orifice</td>
<td>16</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>Port 55850 tcp - Possible myserver activity - ref. 010313-1</td>
<td>23</td>
<td>10</td>
<td>13</td>
</tr>
<tr>
<td>High port 65535 udp - possible Red Worm - traffic</td>
<td>29</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>Tiny Fragments - Possible Hostile Activity</td>
<td>31</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Null scan!</td>
<td>52</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>High port 65535 tcp - possible Red Worm - traffic</td>
<td>60</td>
<td>14</td>
<td>16</td>
</tr>
<tr>
<td>SUNRPC highport access!</td>
<td>65</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Queso fingerprint</td>
<td>74</td>
<td>19</td>
<td>25</td>
</tr>
<tr>
<td>TCP SRC and DST outside network</td>
<td>79</td>
<td>13</td>
<td>37</td>
</tr>
<tr>
<td>Watchlist 000222 NET-NCFC</td>
<td>94</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>SMB Name Wildcard</td>
<td>120</td>
<td>79</td>
<td>68</td>
</tr>
<tr>
<td>WinGate 1080 Attempt</td>
<td>134</td>
<td>38</td>
<td>87</td>
</tr>
<tr>
<td>External RPC call</td>
<td>409</td>
<td>9</td>
<td>341</td>
</tr>
<tr>
<td>UDP SRC and DST outside network</td>
<td>483</td>
<td>37</td>
<td>240</td>
</tr>
<tr>
<td>connect to 515 from outside</td>
<td>717</td>
<td>11</td>
<td>523</td>
</tr>
<tr>
<td>Attempted Sun RPC high port access</td>
<td>5177</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Watchlist 000220 IL-ISDNNET-990517</td>
<td>5308</td>
<td>25</td>
<td>30</td>
</tr>
<tr>
<td>Possible trojan server activity</td>
<td>7296</td>
<td>892</td>
<td>4881</td>
</tr>
<tr>
<td>Russia Dynamo - SANS Flash 28-jul-00</td>
<td>23989</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

### 3.3 Top Talkers
### 3.4 External IPs with Registration Info

The following IP Addresses were selected because of the following reasons:

1. Sheer Volume of Alerts
2. Criticality of the Alert

**A. Watchlist 000220 IL-ISDNNET-990517**

What are these Israeli IP Addresses doing in the Universities Network? Why are they generating so much noise? The first three IP addresses seem to have a communication channel on the 37000 range.

<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>212.179.79.2</td>
<td>2204</td>
<td>2204</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>212.179.84.195</td>
<td>614</td>
<td>614</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>212.179.80.232</td>
<td>518</td>
<td>518</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>212.179.80.225</td>
<td>417</td>
<td>417</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>212.179.24.155</td>
<td>395</td>
<td>395</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<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>MY.NET.204.18</td>
<td>21440</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MY.NET.15.214</td>
<td>10114</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MY.NET.217.242</td>
<td>7756</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MY.NET.202.34</td>
<td>6832</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>210.220.73.117</td>
<td>6329</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MY.NET.229.130</td>
<td>6209</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64.229.232.100</td>
<td>3864</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MY.NET.226.190</td>
<td>3814</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MY.NET.227.222</td>
<td>3442</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63.163.94.13</td>
<td>3349</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MY.NET.217.230</td>
<td>3251</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>202.145.57.82</td>
<td>3231</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Prefix</td>
<td>Total</td>
<td>Loop</td>
<td>Port</td>
</tr>
<tr>
<td>-------------</td>
<td>--------</td>
<td>-------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>212.179.5.90</td>
<td>334</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.125.114</td>
<td>291</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>212.179.95.5</td>
<td>274</td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>212.179.40.130</td>
<td>78</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.29.216</td>
<td>47</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.2.185</td>
<td>45</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.80.67</td>
<td>29</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.48.82</td>
<td>23</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>212.179.27.6</td>
<td>15</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>212.179.7.10</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>212.179.67.67</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.72.53</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.25.27</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.81.73</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.82.30</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.80.231</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.76.22</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.84.246</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.81.254</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>212.179.82.31</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**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

**mnt-by:** RIPE-NCC-NONE-MNT

**changed:** hostmaster@isdn.net.il 20001109

**source:** RIPE

**route:** 212.179.0.0/17

**descr:** ISDN Net Ltd.
B. Attempted Sun RPC high port access

Why is this guy doing sun rpc scans from home? Is this guy even aware that his box is doing it? Hostname is ilm26-3-204.ec.rr.com. I think we should consider talking to the service provider and getting to the bottom of it. Somehow, I think, organizations connecting to the Internet should do due diligence by securing the boxes so that it will not be used to generate attacks.

<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>66.26.3.204</td>
<td>5177</td>
<td>5177</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

ROADRUNNER-MIDSOUTH (NETBLK-ROADRUNNER-MIDSOUTH)
13241 Woodland Park Road
Herndon, VA 20171
US

Netname: ROADRUNNER-MIDSOUTH
Maintainer: RRMS

Coordinator:
ServiceCo LLC (ZS30-ARIN) abuse@rr.com
1-703-345-3416

Domain System inverse mapping provided by:

| DNS1.RR.COM | 24.30.200.3 |
| DNS2.RR.COM | 24.30.201.3 |
| DNS3.RR.COM | 24.30.199.7 |
| DNS4.RR.COM | 65.24.0.172 |

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Database last updated on 30-Jun-2001 22:59:10 EDT.

Rogers@Home Cambr (NETBLK-ON-ROG-CMDG-3)
1 Mount Pleasant Road
Toronto, ON M4Y 2Y5
CA

Netname: ON-ROG-CMDG-3

Coordinator:
Network Security, Fraud (AD30-ARIN) abuse@rogers.home.net
(416) 935-4729

Record last updated on 05-Feb-1999.
Database last updated on 30-Jun-2001 22:59:10 EDT.

C. Possible trojan server activity

Just like the previous alert, MY.NET.15.214 is communicating with an IP Addresses that happens to be registered to rr.com. In this instance, it is very likely that MY.NET.15.214 is compromised and is currently configured to hunt down vulnerable systems belonging to the range rr.com, which is a high-speed Internet service provider. The next source, 24.112.202.176 is an IP Address belonging to a Canadian ISP. This attacker seems to be looking for machines that is already running Subseven.

| Possible trojan server activity | 892 sources | 4881 destinations |
### Source

<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>MY.NET.15.214</td>
<td>5176</td>
<td>5176</td>
<td>3880</td>
<td>3880</td>
</tr>
<tr>
<td>24.112.202.176</td>
<td>913</td>
<td>913</td>
<td>858</td>
<td>858</td>
</tr>
<tr>
<td>MY.NET.98.193</td>
<td>59</td>
<td>59</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td>206.132.75.244</td>
<td>13</td>
<td>13</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>24.180.160.210</td>
<td>6</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>MY.NET.219.86</td>
<td>6</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>211.219.138.228</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>211.135.37.98</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>130.205.77.148</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>168.131.99.155</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>MY.NET.97.71</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>MY.NET.181.137</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>24.132.56.141</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>24.132.58.198</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4.41.188.147</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

### Port Number

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocol</th>
<th>Port Name</th>
<th>General Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27374</td>
<td>tcp</td>
<td>ODD Packet - Subseven</td>
<td>ODD Packet - SubSeven</td>
</tr>
<tr>
<td>27374</td>
<td>tcp</td>
<td>trojan / subseven</td>
<td>ImagePump</td>
</tr>
</tbody>
</table>

Global Crossing ([NET-GBLX-9](#))
960 Hamlin Court
Sunnyvale, CA 94089
US

Netname: GBLX-9
Netblock: [206.132.0.0 - 206.132.255.255](#)
Maintainer: GBLX

Coordinator:
Global Crossing ([IA12-ORG-ARIN](#)) ipadmin@gblx.net
+1 800 404-7714

Domain System inverse mapping provided by:
NAME.ROC.GBLX.NET  209.130.187.10
NAME.PHX.GBLX.NET  206.165.6.10

Record last updated on 06-Apr-2001.
Database last updated on 30-Jun-2001 22:59:10 EDT.
Netname: USWEST
Netblock: 130.13.0.0 - 130.13.255.255

Coordinator:
Qwest Communications (ZQ10-ARIN) abuse@tempe-vdoc.com
480-768-4338

Domain System inverse mapping provided by:
NS1.USWEST.NET  204.147.80.5
NS2.DNVR.USWEST.NET  206.196.128.1

Database last updated on 30-Jun-2001 22:59:10 EDT.

@Home Network (NETBLK-BLTMMD1-MD-2)
425 Broadway
Redwood City, CA 94063
US

Netname: BLTMMD1-MD-2

Coordinator:
Operations, Network (HOME-NOC-ARIN) noc-abuse@noc.home.net
(601) 556-5599

Record last updated on 12-Jul-2000.
Database last updated on 30-Jun-2001 22:59:10 EDT.

D. Russia Dynamo - SANS Flash 28-jul-00

This detect is quite old. MY.NET.178.42 is still sending data to the black listed addresses. It could have been overlooked, or it could be a new infection. Regardless, this item really needs to be looked at. This is the top alert from the April 6-10 time period.

<p>| Russia Dynamo - SANS Flash 28-jul-00 | 3 sources | 2 destinations |</p>
<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>MY.NET.178.42</td>
<td>20790</td>
<td>20790</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>194.87.6.106</td>
<td>3071</td>
<td>3071</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>194.87.6.201</td>
<td>128</td>
<td>128</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**inetnum:** 194.87.0.0 - 194.87.255.255  
**netname:** RU-DEMOS-940901  
**descr:** Provider Local Registry  
**country:** RU  
**admin-c:** DNOC-ORG  
**tech-c:** RR-ORG  
**status:** ALLOCATED PA  
**remarks:** changed from SU-DOMES to RU-DEMOS 970415  
**mnt-by:** RIPE-NCC-HM-MNT  
**changed:** auto-dbm@ripe.net 19950424  
**changed:** hostmaster@ripe.net 19960514  
**changed:** hostmaster@ripe.net 19970415  
**changed:** hostmaster@ripe.net 19981102  
**changed:** hostmaster@ripe.net 19981209  
**changed:** hostmaster@ripe.net 20000526  
**source:** RIPE

**route:** 194.87.0.0/19  
**descr:** DEMOS  
**origin:** AS2578  
**notify:** noc@demos.net  
**mnt-by:** AS2578-MNT  
**changed:** noc@demos.net 20000927  
**source:** RIPE

**role:** Demos Internet NOC  
**address:** Demos Company Ltd.  
**address:** 6-1 Ovchinnikovskaya nab.  
**address:** Moscow 113035  
**address:** Russia  
**phone:** +7 095 737 0436  
**phone:** +7 095 737 0400  
**fax-no:** +7 095 956 5042  
**e-mail:** ncc@demos.net  
**admin-c:** KEV6-RIPE  
**admin-c:** RVP18-RIPE  
**admin-c:** GK41-RIPE
E. Connect to 515 from outside

An LPD or spooler vulnerability was released a couple of months back. I would be very surprised if the University allows outsiders from China to send print jobs to the Universities print servers. These are clearly attempts to gain access to the Universities computers.
### connect to 515 from outside

<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>140.122.140.57</td>
<td>165</td>
<td>165</td>
<td>165</td>
<td>165</td>
</tr>
<tr>
<td>63.195.112.230</td>
<td>145</td>
<td>145</td>
<td>141</td>
<td>141</td>
</tr>
<tr>
<td>207.8.203.106</td>
<td>106</td>
<td>106</td>
<td>106</td>
<td>106</td>
</tr>
<tr>
<td>216.130.139.13</td>
<td>87</td>
<td>87</td>
<td>83</td>
<td>83</td>
</tr>
<tr>
<td>207.102.158.10</td>
<td>67</td>
<td>67</td>
<td>57</td>
<td>57</td>
</tr>
<tr>
<td>64.18.0.162</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
</tr>
<tr>
<td>64.14.243.59</td>
<td>44</td>
<td>44</td>
<td>43</td>
<td>43</td>
</tr>
<tr>
<td>199.179.16.236</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>61.142.74.8</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>24.170.117.247</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>65.1.190.220</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Ministry of Education Computer Center (NET-TANET-B88)
12th Fl, 106, Hoping E. Road, Sec 2.
Taiwan Republic of China, R.O.C TW

Netname: TANET-BNET14
Netblock: **140.122.0.0 - 140.122.255.255**

Coordinator:
TANet, Administrator ([AT122-ARIN](mailto:tanetadm@moe.edu.tw))
886-2-27377010-295

Domain System inverse mapping provided by:

- **CC.NTNU.EDU.TW**: 140.122.65.9
- **MOEVAX.EDU.TW**: 140.111.1.2

Record last updated on 14-Apr-1999.
Database last updated on 30-Jun-2001 22:59:10 EDT.
SNFC21 RBACK13 BASIC **63.195.112.0** ([NETBLK-SBCIS39528](mailto:))
303 2nd Street Suite 850N
San Francisco, CA 94107
US
Netname: SBCIS39528
Netblock: 63.195.112.0 - 63.195.119.255

Coordinator:
Pacific Bell Internet (PIA2-ORG-ARIN) ip-admin@PBI.NET
888-212-5411

Record last updated on 08-Sep-1999.
Database last updated on 30-Jun-2001 22:59:10 EDT.

Netname: NETAXS-BLK
Netblock: 207.8.128.0 - 207.8.255.255
Maintainer: NTAC

Coordinator:
Freedman, Avi (AF39-ARIN) freedman@NETAXS.COM
215 576 8669

Domain System inverse mapping provided by:

NS1.NETAXS.COM 207.8.186.1
NS2.NETAXS.COM 207.8.186.2

Record last updated on 04-Jun-1996.
Database last updated on 30-Jun-2001 22:59:10 EDT.

Netname: WEST-GA-NET1
Netblock: 216.130.128.0 - 216.130.159.255
Maintainer: NEWN

Coordinator:
Morrow, Larry (LM435-ARIN) larry@a-plus.net
1 770 683 8324 (FAX) 1 770 252 4230

Domain System inverse mapping provided by:

DNS.NEWNANUTILITIES.ORG 216.130.152.71
DNS2.NEWNANUTILITIES.ORG 216.130.152.72
DNS.A-PLUS.NET  216.130.132.5

Addresses within this block are non-portable

Database last updated on 30-Jun-2001 22:59:10 EDT.
US West Advanced Technologies (NET-USWEST)
4001 Discovery Drive
Boulder, CO 80303
US

3.5 Link Graph of OOS

MY.NET.227.130 is looking for external addresses running the service GNUtella (port 6346/tcp, 6346/udp). This was a very quiet scan that only generated 169 logs when compared to the very loud scans generated by the subseven slaves. An article released last Feb. 27, 2001 talks about a virus, Mandragore\(^3\), that seems to be spreading across Peer-to-Peer file exchange implementations like Gnutella. Another port that seems to be scanned frequently in the OOS files is 6699/tcp, Napster. Both these peer-to-peer file sharing implementations have documented vulnerabilities.

Other ports that were being probed were the usual 110, 80, and 22. Crafted flag combinations were being sent to the mentioned ports to possibly bypass network security measures implemented in the University.

3.6 Anomalous Activity / Possibility of Compromised Systems

Alerts suggest that MY.NET.204.18 and MY.NET.15.214 is a compromised system running subseven. They are both being controlled by the same master, 24.2.52.25. Scan logs also indicate that the servers have different directives. The 15.214 IP Address is looking for other trojans residing on desktops of possibly home users, 15.214 appears to be concentrating on the ISPs like @home, southwestern, and a bbn planet. The 204.18 however, seems to mapping the following networks: 63.88.120.21 - a UUNET block that has been assigned to Amrik Singh, and 129.21.112.10, an IP Address that belongs to Rochester Institute of Technology, NY. These scans could be decoy scans; they are not at all subtle.

Why is MY.NET.217.242 so active? The alert logs and the scan logs show that this server has been communication with the same IP Addresses from 9:41-10:45 on April 9. On this date, IP Address 66.26.3.204, started connection to the rpc port at 7:55 PM, this went on for the next 2 hours, and by 9:53, the internal host was scanning external hosts for rpc vulnerabilities. This is the same vulnerability that was exploited to compromise the system.

3.6 Defensive Recommendation

Fixing this will be a real challenge. There is evidence of compromise, and I do not see any evidence of any security mechanism in place other than the IDS sensors that gathered all the

\(^3\)Http://www.kaspersky.com/news.asp?tnews=0&nview=1&id=162&page=0
data. I think the security posture of the University needs to be evaluated. I also think that there should be some acceptable use policy that limits the students as to what they can, and they cannot do. This way, anything out of the norm will be considered an Intrusion and will therefore be investigated.

The University might want to consider making an example out of one hacker by prosecuting him/her. At this point, I would assume that the University has enough data and forensic evidence to go after the uninvited visitors. If not, I think the University should seriously consider going after some of them. Hopefully, the successful prosecution might scare the other hackers away.

I would recommend containment. The University needs to localize the compromise. Easier said than done right? I do not have the slightest idea as to how I should go about it. A lot of systems show signs of compromise and I do not know where to start. I see a particular attacker having multiple slaves, so if you shut one down, he kills you with the other. The containment or localization issue needs to be addressed ASAP because the longer we wait, the more boxes gets compromised. The University needs to start somewhere until the last compromised system is rebuilt, and made more resistant to break-ins.

Second thing I would do is to prevent or at least make compromises more difficult. This can be done by installing firewalls, router filters, and active IDSs.

I would also like to make the students responsible for the security of their desktops or servers. Hardening documents should be readily available wherever a computer is present. I guess this is more of creating security awareness or consciousness in the University. Something as simple as making the students use stronger passwords, using screen savers, etc. It can also be as technical as having the students harden their servers themselves. I think a lot of mileage can be gained by making the students accountable to the security of their desktop. After all, it is their work that gets lost if a compromise takes place.

3.8 Analysis Process

Data Preparation

I used GAWK, SED, GREP, SORT, and EGREP to format the data in order to extract the top talker and top listener. I had to replace ":" with a white space in order to separate the port number with the source ip address and the destination ip address. I used vi to do this since I only had to process five files and I also did not have enough time to look up the man pages for SED.

The command below counts the number of instances of the source IP address by assigning it to a numeric array named source using the IP Address as the element name or subscript.

gawk -F " " '{ source[$6]++; } END { for (ip in source)  print ip, source[ip] }' apr6 apr7 apr8 apr9 apr10 > toptalker-6-10

The next command counts the number of instances of the source IP address by assigning it to a numeric array named dst.

gawk -F " " '{ dst[$9]++; } END { for (ip in dst)  print ip, dst[ip] }' apr6 apr7 apr8 apr9 apr10 > toplisten-6-10
SED was also used to replace MY.NET with 10.0 so that snortsnarf can execute correctly.

**Data Processing**

As soon as I finished replacing MY.NET with 10.0, I was ready to run snortsnarf against all the alert files. Initially, I ran snortsnarf one file at a time. It was not long until I realized the need to correlate alerts. Since I only had to analyze five days of data, it was simpler for me to merge five days of alert to 1 big file and run snortsnarf against the merged file.

**Data Analysis**

The real challenge for me was to decide which event or particular alert I will pursue and really investigate. This was difficult for me because I cannot really decide which particular host is critical or not. I had to decide based on what I thought was severe based on the volume of alerts, and the lethality of the attack.

The Top Talker List was also compared against the consolidated alert list, and OOS in an effort to establish trends and links. I used utilities like grep and egrep to manually extract data that were relevant to the IP Addresses that I was trying to investigate.
REFERENCES


http://www.securityfocus.com
http://www.whitehats.com
http://www.sans.org
http://www.incidents.org
http://www.arin.net
http://www.ripe.net
http://www.apnic.net
http://www.robertgraham.com
http://www.sans.org/ids/faq
http://cve.mitre.org
http://www.kaspersky.com
http://www.riptech.com
http://www.silicondefense.com
http://www.counterpane.com
http://www.predictive.com
http://www.insecure.org

http://www.securityfocus.com
http://www.whitehats.com
http://www.sans.org
http://www.incidents.org
http://www.arin.net
http://www.ripe.net
http://www.apnic.net
http://www.robertgraham.com
http://www.sans.org/ids/faq
http://cve.mitre.org
http://www.kaspersky.com
http://www.riptech.com
http://www.silicondefense.com
http://www.counterpane.com
http://www.predictive.com
http://www.insecure.org
# Upcoming Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS San Francisco Spring 2020</td>
<td>San Francisco, CA</td>
<td>Mar 16, 2020 - Mar 27, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Mentor Session - SEC503</td>
<td>Houston, TX</td>
<td>Mar 21, 2020 - Apr 25, 2020</td>
<td>Mentor</td>
</tr>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2020 - SEC503: Intrusion Detection In-Depth</td>
<td>Orlando, FL</td>
<td>Apr 05, 2020 - Apr 10, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS London April 2020</td>
<td>London, United Kingdom</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2020</td>
<td>Baltimore, MD</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Columbia SEC503 @ UKI</td>
<td>Columbia, MD</td>
<td>May 04, 2020 - May 09, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Security West 2020</td>
<td>San Diego, CA</td>
<td>May 06, 2020 - May 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam May 2020</td>
<td>Amsterdam, Netherlands</td>
<td>May 11, 2020 - May 18, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio 2020</td>
<td>San Antonio, TX</td>
<td>May 17, 2020 - May 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas Summer 2020</td>
<td>Las Vegas, NV</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich July 2020</td>
<td>Munich, Germany</td>
<td>Jul 06, 2020 - Jul 11, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Rocky Mountain Summer 2020 - SEC503: Intrusion Detection In-Depth</td>
<td>Denver, CO</td>
<td>Jul 20, 2020 - Jul 25, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Columbia 2020</td>
<td>Columbia, MD</td>
<td>Jul 20, 2020 - Jul 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain Summer 2020</td>
<td>Denver, CO</td>
<td>Jul 20, 2020 - Jul 25, 2020</td>
<td>Live Event</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 Amsterdam August 2020</td>
<td>Amsterdam, Netherlands</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2020</td>
<td>Melbourne, Australia</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VA</td>
<td>Aug 24, 2020 - Sep 04, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Summer 2020</td>
<td>New York City, NY</td>
<td>Aug 30, 2020 - Sep 04, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, United Kingdom</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich September 2020</td>
<td>Munich, Germany</td>
<td>Sep 14, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2020</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA - Reston Fall 2020</td>
<td>Reston, VA</td>
<td>Sep 28, 2020 - Oct 03, 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>