Global Information Assurance Certification Paper

Intrusion Detection In Depth

GCIA Practical Assignment

Version 2.9

Stephen Pedersen

SANS Baltimore

May 2001

Table of contents

Introduction 3
Assignment 1 – Network Detects 5
Detect #1 – 5
Detect #2 – 7
Detect #3 – 10
Detect #4 – 13
Detect #5 – 20
Assignment 2 - Describe the State of Intrusion Detection 23
Introduction 23
CodeRed Worm 24
Leave Worm 25
Conclusion 26
References 27
Assignment 3 – Analyze This 28
Executive Summary 28
Analysis 28
Analysis of Signatures with more than four hundred Alerts 30
Analysis of Signatures with less than four hundred Alerts 46
Top Ten Attacker 52
Top Ten Attacker from my.net 52
Scan log analysis 53
Analysis 53
Top Ten Destination Hosts 54
"Out Of Spec" Packets 55
Defensive Recommendation 56
Analysis process 58
Resources 60

Introduction

Logging Conventions used in this Paper

Snort V1.7 Intrustion Detection System (http://www.snort.org):

Snort packet logs, logged using the text facility are in the following format:

Packet Log format:
[date and time stamps] [source IP:port] [direction of packet] [Destination IP:port] [protocol][time to live] [type of service][IP ID] [IP headerlength] [datagram length] [TCP flags/UDP][sequence no.][Acknowledgement No.] [Window size] [protocol header Length]
[Payload]

Example:
```
[**] FTP - INFO - Anonymous FTP [**]
07/01-08:39:38.497246 64.180.30.249:1291 -> 192.156.136.12:21
TCP TTL:128 TOS:0x0 ID:8467 IpLen:20 DgmLen:56 DF
***AP*** Seq: 0xFF759437  Ack: 0x93CA82E5  Win: 0x440E  TcpLen: 20
55 53 45 52 20 61 6E 6F 6E 79 6D 6F 75 73 0D 0A  USER anonymous..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Snort Alerts can be configure to log to a specific file or it can use the syslog facility. Syslog can be used to configure centralized logging:

Snort alert log has the following format:
```
Mar  5 12:30:01 [MY.SUB.NET.237.2.2] snort[17383]: FTP - INFO - Anonymous FTP:
MY.SUB.NET.51:55558 -> 128.135.252.36:21
```

Snort port scan log:
Log format: [Date] [time] [source IP:port] [Destination IP:port] [TCP flags/UDP].

```
Dec  3 14:35:23 194.139.45.2:21 -> MY.SUB.NET.21:21 SYNFIN **SF****
Dec  3 14:35:23 194.139.45.2:21 -> MY.SUB.NET.22:21 SYNFIN **SF****
Dec  3 14:35:23 194.139.45.2:21 -> MY.SUB.NET.23:21 SYNFIN **SF****
Dec  3 14:35:23 194.139.45.2:21 -> MY.SUB.NET.24:21 SYNFIN **SF****
Dec  3 14:35:23 194.139.45.2:21 -> MY.SUB.NET.25:21 SYNFIN **SF****
Dec  3 14:35:23 194.139.45.2:21 -> MY.SUB.NET.26:21 SYNFIN **SF****
Dec  3 14:35:23 194.139.45.2:21 -> MY.SUB.NET.27:21 SYNFIN **SF****
Dec  3 14:35:23 194.139.45.2:21 -> MY.SUB.NET.28:21 SYNFIN **SF****
```

Lance Spitzner's IDS software using Checkpoint Firewall-1 (http://www.enteract.com/~lspitz/intrusion.html):

Lance has provided a useful script that helps detect suspicious network traffic for Check Point's Firewall-1. He makes use of the userdefined alerts service. A honey-pot rule is defined to drop and trigger the external userdefined alert. The firewall manager passes the log entry to this external alert script. This script can be configured to send alert via email, pager and can dynamically update the firewall rules, using firewall1's sam function. There is logic built into the script, so that you will only get the desired number of alerts. The email will contain the alert number and the original firewall log entry.

Example

```
28May2001  8:56:37 drop   FW1.net >hme0 useralert proto tcp src 216.61.164.172 dst
MY.NET.237 service 54321 s_port 54321 len 40 rule 12

28May2001  8:56:37 drop   FW1.net >hme0 useralert proto tcp src 216.61.164.172 dst
MY.NET.234 service 54321 s_port 54321 len 40 rule 12
```

The format is as follows:

Log format: [Date] [fw-action] [fw-name] [direction & interface] [tracking type] [protocol type] [source address] [destination address] [service/detination port] [source port] [packet length] [rule matched]

ZoneAlarm Personal firewall (http://www.zonezabs.com)

ZoneAlarm is a free personal firewall for home use.

Log format: [FW Direction],[Date],[Time], [source address:source port] [destination address:destination port],[protocol type]

```
FWIN,2001/07/16,07:11:13 -7:00 GMT,209.82.30.76:137,MY.NET.249:137,UDP
```

Information about my network

These detects are collected from two primary sources. The first is a boardband DSL network. This network consist of a Home PC running Windows 2000 with ZoneAlarm firewall installed and a Sun Solaris 8 workstation with snort v1.7 installed. This server also has Sunscreen Lite installed.
The second source is from a corporate boundary network environment. This environment makes use of Check Point firewall1 for Solaris and application gateways.

Assignment 1 – Network Detects
Detect #1 –

Log format: :[Date][Time][Action][Origin][IntDir] [Inteface Name] [Proto][Source][Destination] [Service][Source port][Rule]

```
28May2001  8:56:37 drop   FW1.net >hme0 useralert proto tcp src 216.61.164.172 dst
MY.NET.237 service 54321 s_port 54321 len 40 rule 12

28May2001  8:56:37 drop   FW1.net >hme0 useralert proto tcp src 216.61.164.172 dst
MY.NET.234 service 54321 s_port 54321 len 40 rule 12

28May2001  8:56:37 drop   FW1.net >hme0 useralert proto tcp src 216.61.164.172 dst
MY.NET.235 service 54321 s_port 54321 len 40 rule 12

28May2001  8:56:37 drop   FW1.net >hme0 useralert proto tcp src 216.61.164.172 dst
MY.NET.236 service 54321 s_port 54321 len 40 rule 12
```

Registration Information

whois server: whois.arin.net
Southwestern Bell Internet Services (NETBLK-SBIS-BLK-2) SBIS-BLK-2
216.60.0.0 - 216.63.255.255
Creative Labs (NETBLK-CREATIVE84) CREATIVE84 216.61.164.0 - 216.61.167.255

1. Source of Trace:

This trace is from a CheckPoint firewall1 log deployed at one of our boundary environments.

2. Detect was generated by:

This detect is from a firewall1 log. The rule match triggered a userdefined alert and the log entry is parsed by a shell script, alert.sh (by Lance Spitzner). Alert.sh counts the number of matches and when a threshold is reach an alert is sent via the configured method. See http://www.enteract.com/~lspitz/intrusion.html for more details.

3. Probability the source address was spoofed:

This is a reconnaissance network scan and therefore the attacker needs a response to the stinulus. The source ip address is most likely not spoofed.

4. Description of attack:

The attacker is scanning for the Back Orifice 2000 Trojan listening on tcp port 54321. This attack is under consideration for inclusion is the CVE list (CAN-1999-0660)

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0660

http://xforce.iss.net/alerts/advise31.php
http://advice.networkice.com/advice/intrusions/2003501/default.htm

5. Attack mechanism:

This network scan is looking for a host infected with the BO2K Trojan. BO2K uses a default port of 54321. The attacker is looking for a BO2K server running on TCP port 54321. This Trojan was designed by Sir Dystic of "The CULT OF THE DEAD COW" (cDc). It is a feature rich Windows remote control Trojan and is a very small self contain executable (120Kb server).

This scan is probably crafted as the source port is the same as the destination port and the source port does not increase. It was a noisy scan, many host scanned in a short period of time.

6. Correlations:

Mihnea has also reported this scan on the same day.

http://www.incidents.org/archives/intrusions/msg00469.html

7. Evidence of active targeting:

This scan covered the entire network and the correlation is evidence that the attacker was scanning many different networks. No active targeting.

8. Severity:

(Critical + Lethal) – (System + Network Countermeasures) = Severity

(5+1)-(5+5)=-4

Critical – Servers on this subnet are critical, Hosted DNS, Mail & Web services.
Lethal – Lethal for Window, but not of Unix servers.
System Countermeasures – The are no windows systems within the scanned network.
Network Countermeasures – All servers are behind firewalls.

9. Defensive recommendation:

Defenses are fine; the scan was dropped by the boundary firewall.

10. Multiple choice test question:

Which Trojan is known to use port 54321?

a. Back Orifice
b. SubSeven
c. Back Orifice 2000
d. DeepThroat

Answer: C

Detect #2 –

Log format:[Date][Time][Origin][Action][Int Name][IntDir][Proto][Source][Destination] [Service][Source port][Rule]

```
22Jun20  14:15:53  fw1.net  drop  qfe0  inbound  udp  12.96.169.126  dns.2 ISAKMP
942  55

22Jun20  14:15:56  fw1.net  drop  qfe0  inbound  udp  12.96.169.126  dns.1 ISAKMP
943  55
22Jun20  14:17:00  fw1.net  drop  qfe0  inbound  udp  12.96.169.126  dns.1 ISAKMP
943  55
```

Registration Information
whois server: whois.arin.net
AT&T ITS (NET-ATT) ATT 12.0.0.0 - 12.255.255.255
RELIANT ENERGY (NETBLK-RELIANTENE230-169) RELIANTENE230-169
12.96.169.0 - 12.96.169.255

1. Source of Trace:

This trace is from a CheckPoint firewall1 log deployed at one of our boundary environments

2. Detect was generated by:

This detect was discovered by parsing the firewall logs using an Access database to sort and group by source addresses and services (destination port).

3. Probability the source address was spoofed:

The source ip address is most likely not spoofed as the attacker is in the reconnaissance phase of an attack. If the source address were spoofed, the attacker would not receive the response from his stimulus.

4. Description of attack:

This attacker is searching for IPSEC VPN servers using the IKE protocol. There are weak implementations of IKE, (I.E. SonicWalls 48 byte pre-shared secret or Nortel's CES IKE Phase 1 SA negotiation single DES only), which allow a brute force attack with far less computing power.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0376
http://neworder.box.sk/showme.php3?id=4168

5. Attack mechanism:

Internet **K**ey **E**xchange is used to authenticate and negotiate keys for an IPSEC VPN. The attacker is searching for a server that will respond to his probe. If the attacker receives a response, he will probably try to identify the OS and/or determine the firewall version by using an OS fingerprinting tool like nmap. This information can be used to focus on the appropriate exploit. If the attacker finds a VPN device with a weak IPSEC implementation, his reconnaissance is complete and he can begin the next phase of his attack.

6. Correlations:

The SonicWall vulnerability was reported by Steven Griffin. It has been documented by Bugtraq and ISS's xforce.

http://www.securityfocus.com/archive/1/171929
http://xforce.iss.net/static/6304.php

The Nortel CES Vulnerability was reported anonymously. It is documented at NewOrder
http://neworder.box.sk/showme.php3?id=4168

http://www.incidents.org/archives/y2k/122399.htm

Dec 22 13:14:53 roogna /kernel: ipfw: 64000 Deny UDP 172.20.20.1:500 172.20.20.25:500 in via ed1
Dec 22 13:16:04 roogna /kernel: ipfw: 64000 Deny UDP 172.20.20.1:500 172.20.20.25:500 in via ed1
The following quote is from the above link:"Analysis: This was on the user's "home" firewall which is within a range of cable modem addresses. Since the originator is in the same subnet it could have been an innocent broadcast as a result of "playing" with new software that uses UDP Socket 500 (IPsec/ISAKMP).

The above analysis maybe correct, but it is worth noting that it dates back to Dec 23 1999 and the IKE vulnerabilities are much more resent (both March 2001). This detect could have fallen into the category of a false negative. “

7. Evidence of active targeting:

This was a targeted scan of both of our DNS server. The dns servers are in different address space and no other addresses in these ranges were scanned. Since only my two dns servers were targeted with a specific query this is active targeting.

8. Severity:

(Critical + Lethal) – (System + Network Countermeasures) = Severity

(5+1)-(4+4)=-2

Critical – These servers are our primary and secondary DNS servers.

Lethal – Our DNS server do not run any IPSEC VPN software.

System Countermeasures – These servers are well maintained, the OS is stripped down and only the required services are running.

Network Countermeasures – The score is high as our firewall block the attack.

9. Defensive recommendation:

Primary and secondary DNS server are core to name resolution for our company and domains we host. Although this attack was foiled by our firewalls, an IDS could have flagged this attack for further investigation. By parsing the firewall logs, there is a potential to miss an attack with such a small trace.

10. Multiple choice test question:

What is Internet Key Exchange used for?

a. Enables secure exchanging of public PGP keys
b. Enables Web based e-commerce
c. It is a stream cipher for IPSEC
d. It negotiates security associations for an IPSEC VPN

Answer: D

Detect #3 –

Log format:[DateTime] [SourceIP:Sport][DestinationIP:Dport] [Flags]

Snort Port Scan log
Jul 8 09:31:44 **61.140.73.131:21** -> **Home.net.249:21** SYNFIN ******SF
Jul 8 09:31:44 **61.140.73.131:21** -> **Home.net.250:21** SYNFIN ******SF

Snort v1.7 Rule
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg: "IDS441 - SCAN - Synscan Portscan"; id: 39426; flags: SF;)

[**] IDS441 - SCAN - Synscan Portscan [**]
07/08-09:31:44.503501 **61.140.73.131:21** -> **Home.net.249:21**
TCP TTL:**23** TOS:0x0 ID:**39426** IpLen:20 DgmLen:40
******SF Seq: **0x5BC34829** Ack: **0x498D5239** Win: 0x404 TcpLen: 20

=+=

[**] IDS441 - SCAN - Synscan Portscan [**]
07/08-09:31:44.**523380 61.140.73.131:21 -> Home.net.250:21**
TCP TTL:23 TOS:0x0 ID:**39426** IpLen:20 DgmLen:40
******SF Seq: **0x5BC34829** Ack: **0x498D5239** Win: 0x404 TcpLen: 20

=+=

ZoneAlarm log Correlation
FWIN,2001/07/08, 09:31:44 -7:00 GMT, **61.140.73.131:21**, **Home.net.249:21**,TCP (flags:**SF**)

Registration Information
whois -h whois.apnic.net 61.140.73

% Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
% (whois7.apnic.net)

inetnum: 61.140.0.0 - 61.143.255.255
netname: CHINANET-GD
descr: CHINANET Guangdong province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP

tech-c: WM12-AP
mnt-by: MAINT-CHINANET
mnt-lower: MAINT-CHINANET-GD
changed: hostmaster@ns.chinanet.cn.net 20000601
source: APNIC

1. Source of Trace:

This trace is from a Solaris server at home on a DSL broadband connection.

2. Detect was generated by:

This detect was generated by Snort V1.7 for Solaris.

3. Probability the source address was spoofed:

The source ip address is most likely not spoofed as the attacker is doing a port scan and an OS fingerprint. If the source address were spoofed, the attacker would not receive a response.

4. Description of attack:

This attack is doing an OS fingerprint. Operating Systems respond differently to the illogical SYN/FIN combinations. There are over 90 potential ftp exploits in the CVE database. The attacker would likely focus his attack once he finds an ftp server that is accessible from the Internet.
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ftp

5. Attack mechanism:

This attack tool is most likely some kind of script-kiddie. It allows the attacker to customize the destination port. There are two patterns to note in these packets. The source and destination ports are the same and the IP ID is always 39426. The incidents.org URL in the correlations section confirms this. In my trace the sequence and acknowledgment numbers are identical in both packets. This is odd and is different to the traces from Incidents.org.
.

6. Correlations:

The Zone Alarm log is confirmation of this attack.
There are several very similar detects at incidents.org.

http://www.incidents.org/archives/intrusions/msg00223.html

The above detect is almost identical, dated may 14th 2001 by afletch@xxxxxxxxxxxxxxx. The source/destination ports are the same, the IP ID is 39426 and the Sequence and Acknowledgement numbers are the same for multiple packets.

http://www.incidents.org/archives/y2k/080100.htm
Laurie@.edu also has a trace from August 1st 2000. This trace is using port 53 tcp (dns)

http://www.securityfocus.com/archive/75/189455
Additional confirmation.

http://www.google.com/search?q=61.140.73.131&btnG=Google+Search
... May 29 05:51:08 gate snort[17872]: SCAN SYN FIN [Classification: Attempted Information Leak Priority: 3]: 61.140.73.131:21-> 24.112.17.16:21 ...

This trace was found by search google for the attacker address and I came up with syn fin scan from the same ip and using the same ports. The links from the search were stale so this is all I could get from on the trace.

7. Evidence of active targeting:

This detect was from a DSL network. They hit both of my two servers. This is most likely a scan of the complete DSL address space and therefore no active targeting is evident.

8. Severity:

Address 1
(Critical + Lethal) – (System + Network Countermeasures) = Severity

(5+1)-(4+4)=-2

Critical – Home PC I don't want hacked.

Lethal – No ftp server running.

System Countermeasures – This PC is well maintained, the OS is locked down and only the required services are running.

Network Countermeasures – The score is high as the PC firewall block the attack.

Address 2
(Critical + Lethal) – (System + Network Countermeasures) = Severity

(3+1)-(4+2)=-2

Critical – Lab solaris server not critical .

Lethal – No ftp server running.

System Countermeasures – This servers is well maintained, the OS is locked down and only the required services are running.

Network Countermeasures – The score is low as there is no firewall, but there is the snort IDS running.

9. Defensive recommendation:

I have no recommendations for the PC, but the solaris server could get a firewall. (SunScreen firewall was not install yet.)

10. Multiple choice test question:

Which statement best describes the function of a TCP packet with "SF" flags set?

a. RFC compliant TCP connection handshake
b. FTP denial of service attack
c. TCP handshake running in aggressive mode
d. Operating System fingerprint packet

Answer: D

Detect #4 –

Snort Alerts from syslog

```
Jul 16 02:42:34 pearly snort[311]: [ID 244969 auth.alert] ICMP Destination
Unreachable (Undefined Code!): 157.130.215.21 -> MY.NET.249
Jul 16 09:56:04 pearly snort[311]: [ID 244969 auth.alert] ICMP Destination
Unreachable (Undefined Code!): 157.130.215.21 -> MY.NET.249
Jul 16 11:10:55 pearly snort[311]: [ID 244969 auth.alert] ICMP Destination
Unreachable (Undefined Code!): 157.130.215.21 -> MY.NET.249
Jul 16 15:42:49 pearly snort[311]: [ID 244969 auth.alert] ICMP Destination
Unreachable (Undefined Code!): 157.130.215.21 -> MY.NET.250
Jul 16 13:09:27 pearly snort[311]: [ID 244969 auth.alert] ICMP Destination
Unreachable (Undefined Code!): 157.130.215.21 -> MY.NET.250
Jul 16 19:52:57 pearly snort[311]: [ID 244969 auth.alert] ICMP Destination
Unreachable (Undefined Code!): 157.130.215.21 -> MY.NET.250
```

Snort Packet Logs

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] ICMP Destination Unreachable (Undefined Code!) [**]
07/16-02:42:33.533232 157.130.215.21 -> MY.NET.249
ICMP TTL:246 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3  Code:1  DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
MY.NET.249:1171 -> 216.41.122.35:1200
TCP TTL:122 TOS:0x0 ID:57159 IpLen:20 DgmLen:48
******** Seq: 0x408E6376  Ack: 0x63710E00  Win: 0x6457  TcpLen: 0
** END OF DUMP
00 00 00 00 45 00 00 30 DF 47 40 00 7A 06 6F 86  ....E..0.G@.z.o.
40 B4 1E F9 D8 29 7A 23 04 93 04 B0 40 8E 63 76  @....)z#....@.cv
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] ICMP Destination Unreachable (Undefined Code!) [**]
07/16-09:56:04.056275 157.130.215.21 -> MY.NET.249
ICMP TTL:246 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3  Code:1  DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
MY.NET.249:1086 -> 216.41.122.35:1201
TCP TTL:122 TOS:0x0 ID:32712 IpLen:20 DgmLen:48
******** Seq: 0x6091B48A  Ack: 0x8EA20E00  Win: 0x6457  TcpLen: 0
** END OF DUMP
00 00 00 00 45 00 00 30 7F C8 40 00 7A 06 CF 05  ....E..0..@.z...
40 B4 1E F9 D8 29 7A 23 04 3E 04 B1 60 91 B4 8A  @....)z#.>..`...
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] ICMP Destination Unreachable (Undefined Code!) [**]
07/16-11:10:54.998520 157.130.215.21 -> MY.NET.249
ICMP TTL:246 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3  Code:1  DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
MY.NET.249:1234 -> 216.41.122.35:1090
TCP TTL:122 TOS:0x0 ID:32712 IpLen:20 DgmLen:48
******** Seq: 0x6091B48A  Ack: 0x11140000  Win: 0x3B53  TcpLen: 0
** END OF DUMP
00 00 00 00 45 00 00 30 7F C8 40 00 7A 06 CF 05  ....E..0..@.z...
40 B4 1E F9 D8 29 7A 23 04 D2 04 42 60 91 B4 8A  @....)z#...B`...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Undefined Code!) [**]
07/16-13:09:27.336880 157.130.215.21 -> MY.NET.250
ICMP TTL:246 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3  Code:1  DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
MY.NET.250:1163 -> 216.41.122.35:1255
TCP TTL:122 TOS:0x0 ID:44938 IpLen:20 DgmLen:48
12UAPR*F Seq: 0x501CD06A  Ack: 0xD2897000  Win: 0xC475  TcpLen: 44  UrgPtr: 0xC000
** END OF DUMP
00 00 00 00 45 00 00 30 AF 8A 40 00 7A 06 9F 42  ....E..0..@.z..B
40 B4 1E FA D8 29 7A 23 04 8B 04 E7 50 1C D0 6A  @....)z#....P..j


=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Undefined Code!) [**]
07/16-15:42:49.242369 157.130.215.21 -> MY.NET.250
ICMP TTL:246 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3  Code:1  DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
MY.NET.250:1056 -> 216.41.122.35:1243
TCP TTL:122 TOS:0x0 ID:32712 IpLen:20 DgmLen:48
******** Seq: 0x6091B4A3  Ack: 0xF7110000  Win: 0x3B53  TcpLen: 0
** END OF DUMP
00 00 00 00 45 00 00 30 7F C8 40 00 7A 06 CF 04  ....E..0..@.z...
40 B4 1E FA D8 29 7A 23 04 20 04 DB 60 91 B4 A3  @....)z#. ..`...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] ICMP Destination Unreachable (Undefined Code!) [**]
07/16-19:52:56.748097 157.130.215.21 -> MY.NET.250
ICMP TTL:246 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3  Code:1  DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
MY.NET.250:1228 -> 216.41.122.35:1113
TCP TTL:122 TOS:0x0 ID:65482 IpLen:20 DgmLen:48
*2UA*RSF Seq: 0xE09DF8F4  Ack: 0x9F386E64  Win: 0x2E6F  TcpLen: 24  UrgPtr: 0x65
73
** END OF DUMP
00 00 00 00 45 00 00 30 FF CA 40 00 7A 06 4F 02  ....E..0..@.z.O.
40 B4 1E FA D8 29 7A 23 04 CC 04 59 E0 9D F8 F4  @....)z#...Y....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Log format: [FW Direction],[Date],[Time], [source address:source port] [destination

address:destination port],[protocol type]

Zone Alarm Logs

```
FWIN,2001/07/16,07:11:13 -7:00 GMT,209.82.30.76:137,MY.NET.249:137,UDP
FWIN,2001/07/16,07:22:46 -7:00 GMT,157.130.215.21:0,MY.NET.249:0,ICMP
(type:3/subtype:1)
FWIN,2001/07/16,08:30:41 -7:00 GMT,157.130.215.21:0,MY.NET.249:0,ICMP
(type:3/subtype:1)
FWIN,2001/07/16,10:04:40 -7:00 GMT,157.130.215.21:0,MY.NET.249:0,ICMP
(type:3/subtype:1)
FWIN,2001/07/16,11:19:31 -7:00 GMT,157.130.215.21:0,MY.NET.249:0,ICMP
(type:3/subtype:1)
FWIN,2001/07/16,14:09:25 -7:00 GMT,157.130.215.21:0,MY.NET.249:0,ICMP
(type:3/subtype:1)
FWIN,2001/07/16,15:19:28 -7:00 GMT,157.130.215.21:0,MY.NET.249:0,ICMP
(type:3/subtype:1)
```

Reverse Lookup

500.POS1-1.GW9.PAO1.ALTER.NET.(157.130.215.21)

Registration Information

whois -h whois.arin.net 157.130.215.21
UUNET Technologies, Inc. (NET-UUNETCUSTB40)
3060 Williams Drive
Fairfax, VA 22031
US

Netname: UUNETCUSTB40
Netblock: 157.130.0.0 - 157.130.255.255
Maintainer: UU

Coordinator:
UUNET, Technical Support (OA12-ARIN) help@uu.net
(800) 900-0241

Domain System inverse mapping provided by:

AUTH02.NS.UU.NET 198.6.1.82
AUTH51.NS.UU.NET 198.6.1.162

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 15-Jun-1999.
Database last updated on 21-Jul-2001 23:13:10 EDT.

Reverse Lookup

host35.216.41.122.ma.110.net. A 216.41.122.35

Registration Information
whois -h whois.arin.net 216.41.122.35
Fanch OEM.net, LLC (NET-OEMN-3)
313 Boston Post Road West
Marlboro, MA 01752
US

Netname: OEMN-3
Netblock: 216.41.0.0 - 216.41.127.255
Maintainer: OEMN

Coordinator:
Ennis, Maura (ME8-ARIN) IP-ENG@conversent.com
1 401 384 6000 (FAX) 1 401 384 6015

Domain System inverse mapping provided by:

NS1.OEM.NET	216.41.101.15
NS2.OEM.NET	216.41.101.17

Record last updated on 08-Jun-2001.
Database last updated on 20-Jul-2001 23:08:43 EDT.

1. Source of Trace:

This trace is from a home DSL network.

2. Detect was generated by:

The detect was generated by snort V1.7 for Solaris and my Zone Alarm firewall logs confirmed the traffic.

3. Probability the source address was spoofed:

This source of the ICMP Unreachable packets is not spoofed, but this is a response to a third party, the attacker. This attacker spoofed my IP address.

4. Description of attack:

The traces show unsolicited ICMP Unreachable packets. Analyzing the snort packet logs, you can see the original packets were sent to **157.130.215.21**, but there is no evidence confirming that **my.net.249** sent these packets. Snort would have alerted when **my.net.249** sent these OOS packets and Trojan signatures. It is unclear why the attacker would spoof his source IP if he were doing reconnaissance.

One possible reason could be that he was using **my.net.249** as a silent host with the Hping tool, but this doesn't altogether hold water as the silent host had a firewall installed and so it would not respond.

A second possibility is a bounce denial of service attack against **my.net.249**, using ICMP Unreachable packets

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0214

5. Attack mechanism:

The attacker of the third party system is sending packets to **216.41.122.35** spoofing **my.net.249** as his source IP address. There are various scans, Xmas tree scan, Null flag scan and scans with the reserved bits set. This may be reconnaissance trying to penetrate a packet filtering firewall (no packet state kept), but before the attacker packets could reach the destination, a router is sending ICMP destination unreachable to the source address. This happens to be **my.net.249** and so we the ICMP unreachable packet.

In the Hping senerio the attacker would fine a silent host with an open TCP port. The host is silent because there is no network communication. Therefore the sequence and acknowledgement number are not increasing. When the attacker connects to this open port he will know what sequence and acknowledgement numbers to expect. The attacker then scans the third party host, replacing his source IP with that of the silent host. However, if the attacker connects back to the silent host, he can tell which port is open by examing the sequence number from his connection to the silent host.

In the denial of service senerio, the attacker DOS is directed at **my.net.249.** He sends the original packet to the third party knowing that there will be a ICMP unreachable message. This ICMP packet will be sent back to the source IP, which is **my.net.249**. If we did not have a packet trace or snort IDS, we would not have been able to deduce that the source IP was spoofed and that **my.net.249** did not sent the original crafted packets.

6. Correlations:

Correlation can be seen by examing the detects and firewalls logs from the different systems. The firewall logs from ZoneAlarm confirm this detect and the snort packet trace allow an analyst to explain what was going on.

http://www.incidents.org/archives/intrusions/msg01064.html

7. Evidence of active targeting:

If the Hping senerio was corret then **my.net.249** would not have been the target, but if the ICMP DOS senerio was correct the **my.net.249** was the active target.

8. Severity:

Hping Senario
(Critical + Lethal) – (System + Network Countermeasures) = Severity

(3+1)-(5+5)=-6

Critical – Non Critical home PC
Lethal – not lethal for silent host
System Countermeasures – System has a personal firewall.
Network Countermeasures – Network Intrusion Detection System.

ICMP DOS Senario
(Critical + Lethal) – (System + Network Countermeasures) = Severity

(5+3)-(5+3)=0

Critical – Home PC but I don't what is hacked. It is used extensively.
Lethal – It is potentially Lethal.
System Countermeasures – System has a personal firewall.
Network Countermeasures – Network Intrusion Detection System, the could be a firewall device before **my.net.249**.

9. Defensive recommendation:

Defenses are fine; A perimeter firewall would add defense in depth.

10. Multiple choice test question:

Which of the follow are potential uses of the ICMP protocol?

a. Denial of service attacks
b. Network Mapping
c. Covert channels
d. All of the above

Answer: d

Detect #5 –

ZoneAlarm Log format (See Introduction)

FWIN,2001/07/24,16:01:28 -7:00 GMT, 212.185.240.104:1233,MY.NET.249:1234,TCP (flags:S)

Snort Port Scan log
Jul 24 16:01:26 212.185.240.104:1233 -> MY.NET.249:1243 SYN ******S*
Jul 24 16:01:27 212.185.240.104:1234 -> MY.NET.250:1243 SYN ******S*

1. Source of Trace:

Home DSL network environment

2. Detect was generated by:

This detect was geberated by snort v1.7 from port scan preprocessor.

3. Probability the source address was spoofed:

The source ip address is most likely not spoofed as the attacker is looking Trojans

4. Description of attack:

The attacker is making a standard tcp connect attempt, probably from the client.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0376
http://neworder.box.sk/showme.php3?id=4168

5. Attack mechanism:

Ultors Trojan Horse. Found no other information

Reverse lookup
pD4B9F068.dip.t-dialin.net(212.185.240.104)

Registration Information
Deutsche Telekom Online Service GmbH (T-DIALIN2-DOM)
Waldstrasse 3
Weiterstadt, D-64331
DE

Domain Name: T-DIALIN.NET

Administrative Contact, Technical Contact:
Kaufmann, Daniel (DK162-RIPE) d.kaufmann@T-ONLINE.NET
Deutsche Telekom Online Service GmbH
Julius-Reiber-Str.37
Darmstadt
Germany
D-6429
DE
+49 61 51 680 537 (FAX) +49 61 51 680 519
Billing Contact:
Billing, Domain Name (DN54-RIPE) invoice@TELEKOM.DE
Deutsche Telekom AG, NIC
Gueterstr. 10a
Oldenburg
Germany
26122
DE
+49 441 234 4555 (FAX) +49 441 234 4559

Record last updated on 25-May-2001.
Record expires on 10-Feb-2002.
Record created on 10-Feb-1999.
Database last updated on 26-Jul-2001 06:48:00 EDT.

Domain servers in listed order:

DNS00.SDA.T-ONLINE.DE	195.145.119.62
DNS01.SDA.T-ONLINE.DE	195.145.119.189
DNS00.SUL.T-ONLINE.DE	194.25.2.123
DNS01.SUL.T-ONLINE.DE	194.25.2.124

6. Correlations:

(Peter Sage) http://www.incidents.org/archives/y2k/092300.htm is seeing the same type of connections attempts.

7. Evidence of active targeting:

The attacker is scanning the DSL address space, no active targeting.

8. Severity:

(Critical + Lethal) – (System + Network Countermeasures) = Severity

(4+4)-(5+4)=-1

Critical – Home PC, Don't want it hacked.

Lethal – Windows PC and this is a windows trojan.

System Countermeasures – Firewall on PC.

Network Countermeasures – The score is high as our firewall block the attack and IDS detected it.

9. Defensive recommendation:

All is well.

10. Multiple choice test question:

Which TCP flags are set from a connect scan?

a. Syn Ack
b. Ack
c. Ack Urgent
d. None of the above

Answer: D

Assignment 2 - Describe the State of Intrusion Detection

Signature based IDS

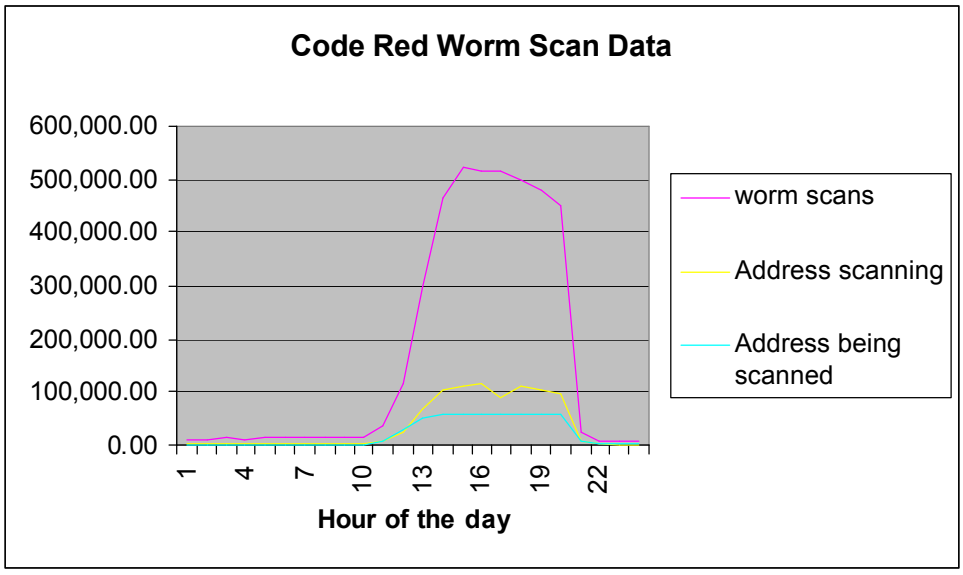
Will it be able to keep up with threat of worms

Introduction

2001 has seen an escalation in the rate at which vulnerabilities are being exploited. We have seen a huge increase in the use of network worms to facilitate the propogation of malicious code. Systems can be compromised at an exponential rate when automated by the use of a worm. Everyone understands the term "compound growth" when used in the context of a financial portfolio. Can you imagine this type of "growth" or systems compromised at "Internet" speed?

I will attempt to show how vulnerable servers on the Internet are. We will examing a few resent worms used to exploit server at an alarming rate. I will relate this to how intrusion detection can help and what can be done to mitigate the risk of a server being compromised. I will discuss some short falls with signature based intrusion detection.

The traditional worm would infect desktops and spread via email or network resources. We are starting to see worms that attack servers by exploiting a vurnerability. Worms of today are not only wreaking havok on the servers they compromise, but may contain denial of service attack code. Worms that can spread at an exponecial rate and launch DOS attacks have a very effective distributed denial of service capability. The CodeRed Worm is an excellent example of this.



Thanks to Ken Eichman of cas.org for posting the data.
You can find the data at http://www.incidents.org/diary/diary.php

The above graph show the rapid increase in scans over a 24 hour period.

There are usually three parts to a worm's code. The exploit used to gain access to a vulnerable system, the propogation of this code and the purpose for the code (I.E. DOS attacks, theft of UIDS/password/credit card #, zombies, etc). We will now look at two examples and briefly discuss the exploits used to gain access to the server, the purpose of the worm and what can be done to defend against the attack.

CodeRed Worm

The CodeRed worm attacks IIS webservers; it gains access by way of the .ida buffer over-flow. The code that allows the IIS server to communicate with the Index Server contains the buffer over-flow. This code is installed by default. The worm finds a vulnerable server and exploits the buffer over-flow, sets itself up in memory and then begins the process over again. One interesting observation to note; the code remain memory resident and therefore file integrity and anti-virus programs will not detect it. Although this worm was crafted as an attack against MS IIS, it is also affecting other device from Cisco and 3Com.

There are two things this worm does as part of it purpose to exist. The first is the defacing of a website. If the language configuration is set to English (US), the website will defaced with the message "Hacked by Chinese!". The second and more destructive of the two, is the denial of service attack against the Whitehouse web site (www.whitehouse.gov) between 20:00 UTC and 23:59 UTC. The worm sends 100Kb of data to port 80. If we consider the graph above that show the potential number of compromised server, you begin to see the how effective this denial of service attack would be.

Why did this worm spread so quickly? This exploit was discovered in mid June and Microsoft released a patch on June 18th. If webmasters and system administrator were up to date with system patch, we would not have seen this rate of infection.
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0500

Signature based IDS's can detect this attack and in conjunction with a firewall maybe able to actively defend your site. The IDS could update the firewall policy to deny access to your webserver from the worm's source IP address. (e.g "fw sam" on firewall1). There has already been a variant of the CodeRed worm released into the wild. This is where signature based IDS shows some short comings. The pattern/signature will have to be updated for each variant. What if the worm contained polymorphic code?

Here are Snort Rules that maybe of some help in your defence against the Code Red Worm.

alert tcp any any <> any 80 (msg: "CodeRed Defacement"; flags: A+; content: "|FF8B8D64 FEFFFF0F BE1185D2 7402EBD3|"; depth:64;)
alert tcp any any <> any 80 (msg: "CodeRed IDA Overflow"; dsize: >239; flags: A+; content:"|2F646566 61756C74 2E696461 3F4E4E4E|";)

The best defence is to patches your servers.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-

033.asp
http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

Leave Worm

Quote from Sans Institute Email: "Given the rate of increase in the Leave worm and its less sophisticated variants, the defensive community could be facing many thousands of zombie agents on compromised Windows platforms that can be instructed to download code and are time synchronized. That represents enough distributed denial of service force to flatten an entire country from an Internet connectivity perspective."

The Leave worm is a little different in that it doesn't actually exploit a vunerability to gain access to a system. It searches the Internet for systems that are already infected with the Subseven Trojan. It enter by using Subseven's default password and instructs Subseven to download f.exe from a site on the Internet. This site has been shutdown. F.exe is execute and proceed to delete C:\WINDOWS\bin.dll, C:\WINDOWS\regsv.exe, and C:\WINDOWS\aci3.dll. It then creates it's own version of regsv.exe and acl3.dll. The registry is also modified.

The Leave worm attempts to resolve some Internet names, to determine if it is connected to the Internet. It uses the daytime function (TCP 13) to synchronise the date and time.

How can you protect your sites? If you keep your anti-virus definitions up to date, you should not have a problem as the Subseven Trojan can be detected and removed by most AV vendors. Personal firewall will help protect your system from both Subseven Trojan and Leave Worm. Signature IDS's can already alert on Subseven scans. Since the Leave Worm makes use of a previously infected server, a Signature IDS will continue to work well.

Snort V1.7 Rule

```
alert TCP $EXTERNAL 27374 -> $INTERNAL any (msg: "IDS279/trojan_trojan-active-subseven21"; flags: SA;)
```

Conclusion

We are seeing a trend in malicious code spreading at alarming rates. This is due to use of network worms to propagate the code. The above examples have demonstrated this fact and to add fuel to the fire, we offen see variants of the worms released shortly after the original worm are detected. One could consider this a slow form of mutation. What if mutation was built in the worm code? How would you detect polymorphic worms? Today IDS vendors are usually behind, when it comes to updating signatures. By the third day, the CodeRed worm had infected over 200 000 IIS server.

Protection against worms or any form of malicious code must be a combined effete. (Defense in Depth) The following will go along way in protecting your servers:

1. Knowledgeable administrators to configure a secure (locked down) server. Only install required Operation System and application components.
2. A Well maintained server with up to date Patches (Automation should be considered)
3. The use of antiviral and file integrity software with up to date signatures.
4. Intrusion Detections systems with up to date signatures and rules

Signature based IDS suffers the same down fall as anti-virus scanners, signatures need to maintained in a timely manner. In large installation this becomes a tedious task. I would like end with an interesting concept. When we build a firewall policy, we construct the policy to explicitly accept the traffic we want and deny everything else. Is it possible to invert the signature based IDS? Write a signature database that matches valid network traffic (RFC compliant). Do not alert on signature matches and alert on traffic that is not recognized. This concept would probably work for packet header, but what can we do about the payload? Voice recognition software usually has a learning phase. IDS could have a learning phase that requires the analysts to confirm traffic that does not match any of the rules. Vendors could provide protocol aware signatures(I.E. protocal syntax checking). For example if you require http traffic, the analyst would add the appropriate rule and the vendor's database would provide the valid syntax checking for the http protocol. When the IDS see's the http packet, it will match a rule and the signature database can perform the content check for protocol syntax. If there is a miss match an alert is generated. Hopefully I have shed some light on the potential of network worms, what can be done to reduce the risk to your server and what role Intrusion Detection Systems have in your security solution. I would like to end by posing a question.
Is signature IDS going to be able to keep up with polymorphic worms or mutating attack code.

References

Eeye IIS .ida exploit: http://www.eeye.com/html/Research/Advisories/AD20010618.html
http://www.eeye.com/html/Research/Advisories/AD20010618.html
Eeye Identify a second strain
http://www.snort.org/codered-tng.htm 21July2001

Snort Rules
http://www.snort.org 21July2001
http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids279&view=signatures

Data from graph and overview
http://www.incidents.org/diary/diary.php 19July2001

Incidents.org article on the Leave Worm
http://www.incidents.org/react/w32leaveworm.php
Sans Email Quote: Subject: Special Alert: Code Red Warning, plus Research Update
Dated 19 July 21, 2001
Authored by Stephen Northcutt

Sans IntrusionDetection Limitations
http://www.sans.org/newlook/resources/IDFAQ/limitations.htm

Symantec
http://www.symantec.com/avcenter/venc/data/w32.leave.worm.html

Polymorphic Viruses By Tarkan Yetiser
http://www.bocklabs.wisc.edu/~janda/polymorf.html

Assignment 3 – Analyze This

Executive Summary

Giac has asked us to analyze the IDS data provider. The data set is from March to June, we have decided to analyze a sub-set of the data because of the volume. We will look at the number of alerts and discuss detects which alert the most frequently. Those detect which occur less frequently, we will provide brief descriptions

This report will provide insight to Giac's current Security Infrastructure. I would like to thank you for the opportunity to help Giac with it's security concerns and look forward working with you in the future.

This report should be considered confidential and distribution should be restricted to authorized individuals.

Analysis

Giac has provided four months of IDS data, included is alert, scan and out of spec packet data. Giac has asked me to analyze at least five days worth of event data. Below is the list of files I chose to analyze.

March 22nd 2001 SnortScan-23-Mar Alert-23-Mar	**March 23rd 2001** SnortScan-24-Mar Alert-24-Mar OOS-Mar-23-2001-packets.de0
March 24th 2001 Scans.010324 alert.010324	**March 25th 2001** SnortScan-26-Mar Alert-26-Mar OOS-Mar-23-2001-packets.de0
March 26th 2001 SnortScan-27-Mar Alert-27-Mar OOS-Mar-23-2001-packets.de0	**March 27th 2001** SnortScan-28-Mar Alert-28-Mar OOS-Mar-23-2001-packets.de0
March 28th 2001 SnortScan-29-Mar Alert-29-Mar OOS-Mar-23-2001-packets.de0	**March 29th 2001** SnortScan-30-Mar Alert-30-Mar OOS-Mar-23-2001-packets.de0
March 30th 2001 Scans.010324 alert.010330 OOS-Mar-23-2001-packets.de0	

There were a total of **63579** alerts between **22th March 2001** and **30th March 2001**

Signature (click for sig info)	**# Alerts**	**# Sources**	**# Destinations**
STATDX UDP attack	1	1	1
ICMP SRC and DST outside network	13	7	8
connect to 515 from inside	13	5	4
SUNRPC highport access!	22	2	2
Tiny Fragments - Possible Hostile Activity	30	2	14
NMAP TCP ping!	40	12	13
Null scan!	44	34	27
Russia Dynamo - SANS Flash 28-jul-00	45	3	3
Port 55850 tcp - Possible myserver activity - ref. 010313-1	68	13	18
TCP SRC and DST outside network	157	32	60
Back Orifice	158	4	158
WinGate 1080 Attempt	185	77	86
Queso fingerprint	192	21	35
External RPC call	265	5	231
SMB Name Wildcard	414	194	142
connect to 515 from outside	487	3	337
Watchlist 000222 NET-NCFC	542	9	9
SYN-FIN scan! :	2185	3	2070
Possible RAMEN server activity	4849	1104	2944
Attempted Sun RPC high port access	8926	1	1
Watchlist 000220 IL-ISDNNET-990517	12732	42	37
UDP SRC and DST outside network:	32211	90	475

Analysis of Signatures with more than four hundred Alerts
(In Descending Order)

UDP SRC and DST outside network

This traffic is originating from your network. This traffic is probably from compromised hosts within my.net. The attacker is crafting the packets with a source address that is outside of your network. (Or using a tool that automate this process.) The best way to trace this traffic is by sniffing network for the mac address and identifing the source ip by mac address. If the source mac address happens to be a router you will need to repeat this on the next segment.

Top 5 Sources

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
206.190.36.120	26704	26704	1	1

10.0.0.1	1502	1502	1	1
129.2.225.92	618	618	1	1
206.190.54.231	410	410	1	1
192.168.0.2	384	384	2	2

I have provided the registration information for this address because it the number one source for the above alert.

206.190.36.120

Yahoo! Broadcast Services, Inc. (NET-NETBLK1-YAHOOBS)
2914 Taylor St.
Dallas, TX 75226
US

Netname: NETBLK1-YAHOOBS
Netblock: 206.190.32.0 - 206.190.63.255
Maintainer: YAHO

Coordinator:
Bonin, Troy (TB501-ARIN) netops@broadcast.com
214.782.4278 ext. 2278

Domain System inverse mapping provided by:

NS.BROADCAST.COM 206.190.32.2
NS2.BROADCAST.COM 206.190.32.3

Record last updated on 29-Jun-2001.
Database last updated on 23-Jul-2001 23:11:01 EDT.

Top 5 Destinations

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
233.28.65.62	26704	26704	1	1
10.255.255.255	1502	1502	1	1
128.183.7.7	618	618	1	1
233.40.70.148	410	410	1	1
192.168.0.255	383	383	1	1

Top 5 Destination Ports

Occurrences	Destination Port	Description
27916	5779	

2212	137	NETBIOS Name Service
1502	67	Dhcp/Bootp
257	38293	Intel RDP-based Alert Messaging broadcast
203	53	Domain name service

Trace of Top Destination

03/24-12:12:34.659853 [**] UDP SRC and DST outside network [**] 206.190.36.120:1034 -> 233.28.65.62:5779

03/24-12:12:34.660520 [**] UDP SRC and DST outside network [**] 206.190.36.120:1034 -> 233.28.65.62:5779

03/24-12:12:34.661192 [**] UDP SRC and DST outside network [**] 206.190.36.120:1034 -> 233.28.65.62:5779

03/24-12:12:34.661876 [**] UDP SRC and DST outside network [**] 206.190.36.120:1034 -> 233.28.65.62:5779

Watchlist 000220 IL-ISDNNET-990517

The detect is specifically configured to detect activity from Israel (ISDN network)

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.179.4.50	6473	6473	1	1
212.179.127.41	2160	2160	1	1
212.179.5.89	963	963	2	2
212.179.28.66	831	831	1	1
212.179.82.220	666	666	1	1

I have provided the registration information for this address because it the number one source for the above alert.

Registration Information for 212.179.4.50:

inetnum	212.179.4.48 - 212.179.4.63
Origin	SCP-SYSTEMS-LTD
descr	SCP-SYSTEMS-LAN
country	IL
Admin. Contact	ES4966-RIPE
Tech. Contact	NP469-RIPE
status	ASSIGNED PA
Notify	hostmaster@isdn.net.il
mnt-by	RIPE-NCC-NONE-MNT
changed	hostmaster@isdn.net.il 20000628
source	RIPE
route	212.179.0.0/17

descr	ISDN Net Ltd.
Origin	AS8551
Notify	hostmaster@isdn.net.il
mnt-by	AS8551-MNT
changed	hostmaster@isdn.net.il 19990610
source	RIPE
person	Eran Shchori
address	BEZEQ INTERNATIONAL
address	40 Hashacham Street
address	Petach-Tikva 49170 Israel
phone	+972 3 9257710
fax-no	+972 3 9257726
e-mail	hostmaster@bezeqint.net
NIC Handle	ES4966-RIPE
changed	registrar@ns.il 20000309
source	RIPE
person	Nati Pinko
address	Bezeq International
address	40 Hashacham St.
address	Petach Tikvah Israel
phone	+972 3 9257761
e-mail	hostmaster@isdn.net.il
NIC Handle	NP469-RIPE
changed	registrar@ns.il 19990902
source	RIPE

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
my.net.222.154	6565	6566	5	6
my.net.156.55	2160	2164	1	4
my.net.219.38	1151	1151	12	12
my.net.219.14	831	840	1	4
my.net.211.10	564	565	1	2

Top 5 Destination Ports

Occurrences	Destination Port	Description
6561	4969	No info found
2177	4772	No info found
1350	6346	No info found
672	4745	No info found
564	4028	No info found

Trace of Top Destination

03/25-02:26:45.860208 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.4.210:57979 -> my.net.222.154:4969
03/25-02:26:46.951506 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.4.210:57979 -> my.net.222.154:4969
03/25-02:26:46.952185 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.4.210:57979 -> my.net.222.154:4969
03/25-02:26:46.957879 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.4.210:57979 -> my.net.222.154:4969

Attempted Sun RPC high port access

Sun RPC is known for a high number of vulnerabilities. RPC is a network socket to application mapping program. It allows application to run on a dynamic high port, which is registered with the RPC application (also known as portmapper)

Top Sources

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
63.121.232.185	8926	8926	1	1

I have provided the registration information for this address because it the number one source for the above alert.

Reverse Lookup

63.121.232.185 newburgh-b-185.sigecom.net

Registration Information for 63.121.232.185:

UUNET Technologies, Inc. (NETBLK-UUNET63) UUNET63 63.64.0.0 - 63.127.255.255
Sigecom (NETBLK-UU-63-121-232) UU-63-121-232 63.121.232.0 - 63.121.239.255

Top 5 Destinations

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
My.net.221.198	8926	8926	1	1

Trace by Top Destination

03/26-19:42:24.114048 [**] Attempted Sun RPC high port access [**] 63.121.232.185:32768 -> my.net.221.198:32771
03/26-19:42:27.178486 [**] Attempted Sun RPC high port access [**] 63.121.232.185:32768 -> my.net.221.198:32771
03/26-19:42:27.602308 [**] Attempted Sun RPC high port access [**] 63.121.232.185:32768 -> my.net.221.198:32771
03/26-19:42:27.671284 [**] Attempted Sun RPC high port access [**] 63.121.232.185:32768 -> my.net.221.198:32771

Possible RAMEN server activity

This detect was triggered by possible Remote Control Trojan activity like SubSeven Trojan.

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
66.30.126.166	341	341	294	294
66.65.84.58	316	316	267	267
164.67.21.63	314	314	284	284
65.24.100.218	308	308	252	252
65.27.22.66	293	293	250	250

I have provided the registration information for this address because it the number one source for the above alert.

Reverse Lookup

66.30.126.166 h000094928d52.ne.mediaone.net

Registration Information for 66.30.126.166

Registrant:
AT&T Broadband (MEDIAONE2-DOM)
183 Inverness Drive West
Suite 160-N
Englewood, CO 80112

Englewood, CO 80112
US

Domain Name: MEDIAONE.NET

Administrative Contact, Technical Contact, Billing Contact:
AT&T Broadband - Legal Demands Center (MA868-ORG) abuse@MEDIAONE.NET
AT&T Broadband

183 Inverness Drive West
ste 100-N
Englewood, CO 80112
USA
800-871-6298
Fax- 720-267-2794

Record last updated on 12-Jun-2001.
Record expires on 07-Jan-2003.
Record created on 06-Jan-1996.
Database last updated on 24-Jul-2001 06:37:00 EDT.

Domain servers in listed order:

NS1.MEDIAONE.NET	24.128.1.80
NS2.MEDIAONE.NET	24.128.1.81
NS1.MW.MEDIAONE.NET	24.131.1.8

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

Netname: ROADRUNNER-NORTHEAST
Netblock: 66.30.0.0 - 66.31.255.255
Maintainer: RRNE

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

Record last updated on 14-Jun-2001.
Database last updated on 23-Jul-2001 23:11:01 EDT.

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
66.30.126.166	408	408	356	356
164.67.21.63	91	91	78	78
152.7.48.9	90	90	79	79
152.7.39.116	86	86	74	74
66.65.84.58	83	83	72	72

Top 5 Destination Ports

Occurrences	Destination Port	Description
3495	27374	SubSeven Trojan
10	1862	techra-server
9	1688	nsjtp-data
8	1318	krb5gatekeeper
6	1786	funk-logger

Trace of Top Destination

03/30-13:05:04.299698 [**] Possible RAMEN server activity [**] my.net.202.93:27374 -> 66.30.126.166:4305
03/30-13:05:05.979807 [**] Possible RAMEN server activity [**] my.net.202.110:27374 -> 66.30.126.166:4322
03/30-13:05:16.141542 [**] Possible RAMEN server activity [**] my.net.202.122:27374 -> 66.30.126.166:4333
03/30-13:05:16.144649 [**] Possible RAMEN server activity [**] my.net.202.126:27374 -> 66.30.126.166:4337

The above trace is showing host my.net.202.93 has responded to SubSeven connections. This host should be investigated further for possible compromise. It maybe infected with the SubSeven Trojan.

SIN/FIN Scan!

This is part of the reconnaissance phase of an attack. The attacker is collecting information such as; Open port on the firewall, OS fingerprinting and open port on hosts

Top Sources

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
61.11.252.117	1432	1432	1432	1432
211.178.63.4	749	749	654	654
24.131.172.251	4	4	4	4

I have provided the registration information for this address because it the number one source for the above alert.

Registration Information for 61.11.252.117:

% Rights restricted by copyright.	//www.apnic.net/db/dbcopyright.html %
See http	(whois6.apnic.net)
inetnum	61.11.249.64 - 61.11.254.255
Origin	HK-IMS-3
descr	Thaicom-IMS, IR
country	TH
Admin. Contact	PB29-AP
Tech. Contact	TU8-AP
mnt-by	MAINT-TH-THAICOM
changed	parkb@thaicom.net 20010405
source	APNIC
person	Park Boonyubol
address	41/103 Ratanathibet Road,
address	Bangkasor, Nonthaburi 11000
country	TH
phone	+66-2-591-0736
fax-no	+66-2-591-0719
e-mail	parkb@thaicom.net
NIC Handle	PB29-AP
mnt-by	MAINT-TH-THAICOM
changed	komsant@cscoms.net 20000818
source	APNIC
person	Taksin Uppalakom
address	41/103 Ratanathibet Road,
address	Bangkasor, Nonthaburi 11000
country	TH
phone	+66-2-591-0736
fax-no	+66-2-591-0719
e-mail	taksinu@thaicom.net

NIC Handle	TU8-AP
mnt-by	MAINT-TH-THAICOM
changed	komsant@cscoms.net 20000818
source	APNIC

Top 5 Destinations

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
my.net.222.4	3	3	1	1
my.net.208.25	3	3	2	2
my.net.21.9	3	3	2	2
my.net.226.30	3	3	2	2
my.net.146.32	3	3	1	1

Top 5 Destination Ports

Occurrences	Destination Port	Description
1616	21	FTP
210	109	Pop-2
181	53	DNS
170	8080	Http proxy
8	111	SUN RPC

Trace of Top Destination

03/30-13:22:53.441652 [**] SYN-FIN scan! [**] 211.178.63.4:109 -> my.net.222.4:109
03/30-13:23:14.294151 [**] SYN-FIN scan! [**] 211.178.63.4:53 -> my.net.222.4:53
03/30-13:23:27.533952 [**] SYN-FIN scan! [**] 211.178.63.4:8080 -> my.net.222.4:8080

These port are known to have root exploits and http proxy can be use for bouce attacks.

Watchlist 000222 NET-NCFC

This detect will alert when traffic is seen from "The Computer Network Center Chinese Academy of Science". Well known source of attacks.

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
159.226.92.9	503	503	1	1
159.226.41.166	22	22	1	1
159.226.6.6	5	5	1	1
159.226.45.3	3	3	3	3
159.226.114.1	3	3	1	1

I have provided the registration information for this address because it the number one source for the above alert.

Reverse Lookup
159.226.92.9 lsec.cc.ac.cn

Registration Information for 159.226.92.9:
The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China
CN

Netname: NCFC
Netblock: 159.226.0.0 - 159.226.255.255

Coordinator:
Qian, Haulin (QH3-ARIN) hlqian@NS.CNC.AC.CN
+86 1 2569960

Domain System inverse mapping provided by:

NS.CNC.AC.CN	159.226.1.1
GINGKO.ICT.AC.CN	159.226.40.1

Record last updated on 25-Jul-1994.
Database last updated on 23-Jul-2001 23:11:01 EDT.

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
my.net.144.54	503	503	1	1
my.net.100.81	22	24	1	2
my.net.253.43	6	7	2	3
my.net.100.230	3	5	2	3
my.net.6.34	3	6	1	3

Top 5 Destination Ports

Occurrences	Destination Port	Description
44	1116	ARDUS Control
31	1034	NT INETINFO.EXE CPU Exploit
23	3383	Enterprise Software Products License Manager
22	38848	No info Found
20	1173	No info Found

Trace of Top Destination

03/22-14:34:25.130123 [**] Watchlist 000222 NET-NCFC [**] 159.226.92.9:21 -> my.net.144.54:1141
03/22-14:34:52.707002 [**] Watchlist 000222 NET-NCFC [**] 159.226.92.9:3037 -> my.net.144.54:113
03/22-14:34:55.725325 [**] Watchlist 000222 NET-NCFC [**] 159.226.92.9:3037 -> my.net.144.54:113
03/22-14:34:59.639951 [**] Watchlist 000222 NET-NCFC [**] 159.226.92.9:21 -> my.net.144.54:1141

Connect to 515 from outside

This alert was detect because an external ip address attempted to connect to the Unix print service, LPRng. It runs of TCP port 515. There are root exploits associated with it.

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
216.191.147.13	283	283	234	234
216.162.44.140	188	188	143	143
64.28.107.215	16	16	16	16

I have provided the registration information for this address because it the number one source for the above alert.

Reverse Lookup

216.191.147.13 www.holodesign.net

Registration Information

Franck GIRARDIN (HOLODESIGN-DOM)
31C Rue des Grands Bas
BESANCON, 25000
FRANCE
Domain Name: HOLODESIGN.COM
Administrative Contact, Billing Contact:
GIRARDIN, Franck (FG1859) fgirardin@HOLODESIGN.COM
HOLO Design
2 Chemin de palente
BESANCON
-
25000
FR
+33381850851 (FAX) +33381850804
Technical Contact:
Guillaume, Maurice (MG8811) mg@SERVEURS-WEB.COM
SC3M SA
2c chemin de palente
BESANCON
FR
25000
FR
33381489458 33381489478

Record last updated on 30-Aug-2000.
Record expires on 26-Sep-2001.
Record created on 26-Sep-1998.
Database last updated on 24-Jul-2001 06:37:00 EDT.

Domain servers in listed order:

NS1.NAMESERVE.NET 207.159.128.3
NS2.NAMESERVE.NET 207.159.128.11

MetroNet Communications Group Inc. (NETBLK-METRONET-CIDR-2)
100 King St. West, Suite 2900
Toronto, Ontario M5X 1B5
CA

Netname: METRONET-CIDR-2
Netblock: 216.191.0.0 - 216.191.255.255
Maintainer: MTCO

Coordinator:
Noc, Metronet Toronto (MTN-ARIN) NOCToronto@METRONET.CA
(416)935-5355

Domain System inverse mapping provided by:

NS1.METRONET.CA	209.82.127.10
NS2.METRONET.CA	216.13.0.10

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 01-Jun-2001.
Database last updated on 23-Jul-2001 23:11:01 EDT.

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
my.net.133.112	4	4	2	2
my.net.132.41	4	6	2	4
my.net.133.76	3	3	2	2
my.net.132.7	3	3	2	2
my.net.134.35	3	3	2	2

Trace of Top Destination

03/22-10:10:48.904645 [**] connect to 515 from outside [**] 216.162.44.140:4765 -> my.net.133.112:515
03/22-10:10:51.899544 [**] connect to 515 from outside [**] 216.162.44.140:4765 -> my.net.133.112:515
03/27-05:34:34.653097 [**] connect to 515 from outside [**] 216.191.147.13:3863 -> my.net.133.112:515
03/27-05:34:37.482376 [**] connect to 515 from outside [**] 216.191.147.13:3863 -> my.net.133.112:515

SMB Name Wildcard

The SMB wild card attack attempts to get netbios names known by the remote system. This will provide the attacker with additional targets.

Top 5 Source Hosts:

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
130.13.64.30	12	12	1	1
211.23.137.66	6	6	1	1
4.41.3.11	6	6	1	1
217.1.75.169	6	6	1	1
24.24.112.126	6	6	1	1

I have provided the registration information for this address because it the number one source for the above alert.

Reverse Lookup

130.13.64.30 vdsl-130-13-64-30.phnx.uswest.net

Regristration Information

Qwest Communications International Inc. (USWEST2-DOM)
600 Stinson Blvd.
Minneapolis, MN 55413
US

Domain Name: USWEST.NET

Administrative Contact, Technical Contact:
Qwest Internet Solutions (HOS48-ORG) dns-info@QWEST.NET
600 Stinson Blvd.
Minneapolis,MN 55413
US
800-672-8520
Fax- 612-664-4770
Billing Contact:
Lundgren, Paul (PL84) abuse@USWEST.NET
U S WEST Interprise Networking
600 Stinson Blvd
Minneapolis, MN 55413
(612) 664-3069 (FAX) (612) 664-4770

Record last updated on 05-Jun-2001.
Record expires on 22-Nov-2001.
Record created on 21-Nov-1994.

Database last updated on 24-Jul-2001 06:37:00 EDT.

Domain servers in listed order:

NS1.USWEST.NET 204.147.80.5
NS2.DNVR.USWEST.NET 206.196.128.1
NS3.MN.USWEST.NET 204.147.80.1

US West Advanced Technologies (NET-USWEST)
4001 Discovery Drive
Boulder, CO 80303
US

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

Record last updated on 28-Mar-2001.
Database last updated on 23-Jul-2001 23:11:01 EDT.

Top 5 Destination Hosts:

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
my.net.132.36	20	21	5	6
my.net.133.32	15	15	3	3
my.net.134.251	12	12	1	1
my.net.133.245	11	14	7	10
my.net.135.45	11	11	3	3

Trace of Top Destination

03/25-09:07:27.876410 [**] SMB Name Wildcard [**] 200.60.46.3:137 -> my.net.132.36:137
03/25-09:07:55.413956 [**] SMB Name Wildcard [**] 4.41.3.11:137 -> my.net.132.36:137
03/25-09:07:57.013419 [**] SMB Name Wildcard [**] 4.41.3.11:137 -> my.net.132.36:137

Correlation For the Above eight attacks
UDP SRC and DST outside network: Andrew Windsor
Watchlist 000220 IL-ISDNNET-990517: Herschel Gelman Crist Clark
Attempted Sun RPC high port access: Mark Evans
Possible RAMEN server activity Michael Semling
SYN-FIN scan! : Paul Asadoorian
Watchlist 000222 NET-NCFC: Mike Bell
connect to 515 from outside: Mark Evans
SMB Name Wildcard : Paul Asadoorian

Analysis of Signatures with less than four hundred Alerts
(In Descending Order)

External RPC call

RPC / Portmapper is traffic with a destination port of UDP/TCP 111. As of July 24th 2001, it was ranked as number three on the Top 10 attacks.
http://www.incidents.org/cid/query/top_10port_7.php

There are many known exploits that use RPC. Information can be gathered from RPC/portmapper about other programs running on that system and the ports they are bound too

Queso fingerprint

Queso is a reconnaissance tool, it allows attackers to perform Operation System finger printing. Once the attacker identifies the OS. The attack can be tailored for that OS and the common application used in that environment.
The top destination is my.net.202.54

Reverse Lookup
129.206.170.20 jupiter.wh.uni-heidelberg.de

Registration Information for 129.206.170.20:
University of Heidelberg (NET-HD-NET)
Im Neuenheimer Feld 293
D-69120 Heidelberg,
DE

Netname: HD-NET
Netblock: 129.206.0.0 - 129.206.255.255

Coordinator:
Hebgen, Michael (MH255-ARIN) michael.hebgen@URZ.UNI-HEIDELBERG.DE
+49 6221 54-4501 (FAX) +49 6221 54-5581

Domain System inverse mapping provided by:

SUN0.URZ.UNI-HEIDELBERG.DE 129.206.100.126
SUN1.URZ.UNI-HEIDELBERG.DE 129.206.100.127
DNS1.BELWUE.DE 129.143.2.1

Record last updated on 14-Dec-1998.
Database last updated on 23-Jul-2001 23:11:01 EDT.

WinGate 1080 Attempt

WinGate is an application proxy usually associated with HTTP proxy, it also support socks. Sock provides generic TCP proxing functionality. An open proxy allows an attacker to bounce off the proxy and attack a third party. The attack would look like it was originating from the system running the WinGate proxy. The Top destinations was my.net.60.11 (http://www.sans.org/newlook/resources/IDFAQ/socks.htm).

Back Orifice

Back Orifice is a remote control Trojan application. It allows a client to remotely use/control a windows system infected with the Back Orifice server. The server usually listens on port 31337. (http://www.sans.org/infosecFAQ/malicious/back_orifice.htm).

I have provided the registration information for this address because it because the attack is a remote control Tojan.

Reverse Lookup

24.162.245.198 rdu162-245-198.nc.rr.com

Registration Information

Road Runner HoldCo, LLC (RR6-DOM)
13241 Woodland Park Rd
Herndon, VA 20171
US

Domain Name: RR.COM

Administrative Contact, Technical Contact, Billing Contact:
Road Runner (NO789-ORG) abuse@RR.COM
Road Runner
13241 Woodland Park Rd
Herndon, VA 20171
US
703-345-3416
Fax- 703-345-2518

Record last updated on 12-Jul-2001.
Record expires on 02-Oct-2010.
Record created on 01-Oct-1996.
Database last updated on 24-Jul-2001 06:37:00 EDT.

Domain servers in listed order:

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

inetnum	0.0.0.0 - 255.255.255.255
Origin	IANA-BLK

descr	The whole IPv4 address space
country	NL
Admin. Contact	IANA1-RIPE
Tech. Contact	IANA1-RIPE
status	ALLOCATED UNSPECIFIED
remarks	The country is really worldwide.
remarks	This address space is assigned at various other places in
remarks	the world and might therefore not be in the RIPE database.
mnt-by	RIPE-NCC-HM-MNT
mnt-lower	RIPE-NCC-HM-MNT
mnt-routes	RIPE-NCC-NONE-MNT
changed	bitbucket@ripe.net 20010529
source	RIPE
role	Internet Assigned Numbers Authority
address	see http://www.iana.org.
e-mail	bitbucket@ripe.net
Admin. Contact	IANA1-RIPE
Tech. Contact	IANA1-RIPE
NIC Handle	IANA1-RIPE
remarks	For more information on IANA services
remarks	go to IANA web site at http://www.iana.org.
mnt-by	RIPE-NCC-MNT
changed	bitbucket@ripe.net 20010411
source	RIPE

TCP SRC and DST outside Network

This traffic is most likely originated from a compromised system.
See "UDP SRC and DST outside network" for more details

Port 55850 tcp – Possible myserver activity – ref. 010313-1

No information available.
http://www.sans.org/082200.htm

Russia Dynamo - SANS Flash 28-jul-00

No information available.

Null scan!

NULL scanning is a crafted TCP packet that has no TCP flags set. The flags indicate the state of the TCP session(Handshake, data flow, session termination). Null Scans are ofter used as decoy traffic. Nmap, a scanning tool, has a decoy feature. (http://www.insecure.org/nmap). This technique is also used to penetrate packet-filtering firewalls and to evade intrusion detection systems

NMAP TCP ping!

The NMAP tcp ping is a tcp packet with the Ack flag set. The destination server will send a Reset packet back. Hence tcp ping. The traces show packets with a source port of 80 and destination port of 53. These port are chosen because DNS and http have a high probability of being open on a firewall and can penetrate non-stateful firewalls. http://www.sans.org/newlook/resources/IDFAQ/What_is_nmap.htm.

Tiny Fragments – Possible Hostile Activity

This attack is used to subvert firewall and evade IDS's. When packet fragments are so small that the payload spans multiple packets, the content match in an IDS will not be triggered. This attack may have been used in conjunction with some other attack. A tool called Frag Router will automatically fragment traffic passing through it. This means any attack could potential make use of Tiny Fragment to evade detection. There were 30 alerts detected using this technique.

SUNRPC highport access!

We covered RPC above; this attack is similar, except the port used is 32771.There are a large number of vulnerabilities associated with RPC. The following link is an excellent reference paper
http://www.sans.org/y2k/trouble_RPCs.htm

Connect to 515 from inside

Port 515 is used by the printing service, LPRng. These detects show connections originating from with MY.NET. There is denial of service attacks associated with LPRng and vulnerabilities, which allow execution of arbitrary code.
More details can be found at http://www.sans.org/newlook/alerts/port515.htm.

ICMP SRC and DST outside network

This alert may indicated a compromised host. The host is sending crafted ICMP packets. Your IDS has detected this because the packets originated from within your network. Some further investigation should be done. This could be part of a denial of service, although the volume is insufficient.

STATDX UDP attack

The Unix rpc.statd daemon is used with Network File Sharing (NFS). The STATDX attack exploits, one of which is a buffer overflow. This will allow root access to the Unix server. There was only one attempt to access port 32776 (rpc.statd)

http://www.sans.org/y2k/practical/Joseph_Rach.html#DETECT2

Top Ten Attacker

Below is a list of the top ten talker that were detected.

Occurrences	Attackers Source IP Addresses
26704	206.190.36.120
8926	63.121.232.185
1502	10.0.0.1
1432	61.11.252.117
749	211.178.63.4
618	129.2.225.92
566	216.191.147.13
410	206.190.54.231
384	192.168.0.2
376	216.162.44.140

In the above table, you will notice to RFC1918 addresses (10.0.0.1, 192.168.0.2). These are obviously spoofed source addresses as they are from non-routable or private address space. You ingress filter should deny these source addresses from entering your network.

Top Ten Attacker from my.net

Below is a list of detects that originated from my.net. These hosts should be investigated further for possible compromises. If investigation reveals a compromised host, it should be removed from the network immediately. Forensic analysis of this host will help you determine how the host was compromised and thereby provided you with the details required to close this security hole and increase your over-all network security.

Occurrences	Attackers Source IP Addresses
21	my.net.221.26
20	my.net.253.24
19	my.net.209.86
16	my.net.218.86
15	my.net.206.118
9	my.net.98.171
9	my.net.97.183
8	my.net.219.178
8	my.net.210.2
6	my.net.60.38

Scan log analysis

The portscan log were used to correlated against the Alerts. I have provided a table of the hosts scanning from within my.net. The traffic categorization is based on the destination port from the scan log entry. The results are shown below:

Top Ten Scanning Hosts from my.net

Occurrences	Source host	Traffic Categorization
18428	my.net.227.42	ENTP traffic (1865), Shockwave 2 traffic(1257)
16860	my.net.220.42	KastenX Pipe (9001)
14394	my.net.228.10	Range of high port, highest TAMS (2726)
13326	my.net.221.198	HackAttack Trojan Horse (32768)
9608	my.net.227.206	Range of high port, highest 21900, No info available
9323	my.net.227.194	27000-27300, No Info available
9040	my.net.218.102	KastenX Pipe (9001)
8719	my.net.221.118	MSN Gaming Zone (28800)
7640	my.net.217.222	KastenX Pipe (9001)
7422	my.net.218.86	GNUtella (6346,6347)

Analysis

Shockwave is a web applet/plug-in that in used by a web browser. Shockwave enabled a web developer to create a multimedia experience for the websurfer. Internet gaming has also shown up. Both of these applications can consume Internet bandwidth. Bandwidth is costly. You should consider whether this type of traffic is required for you business and develop or update your acceptable use policy.
References: Gaming ports can be found at http://www.sans.org/y2k/gaming.htm.

HackAttack is a remote control Trojan and has some very neat features. It is a high security risk and this host should be investigated for compromise.
References: http://www.xploiter.com/security/hackattack.html

Gnutella is an application that enables resource sharing across the Internet. The primary use of gnutella is for sharing MP3 music files. This is also a very high security risk.
References: http://www.incidents.org/detect/gnutella.php

Top Ten Destination Hosts

Occurrences	Destination Address
2092	24.31.216.121
2017	63.162.20.183
1978	24.13.123.8
1978	128.211.223.83
1792	65.9.248.100
1631	24.13.234.24
1625	24.180.11.253
1566	24.9.234.29
1462	172.139.84.34
1424	213.51.207.106

The interesting thing to note about the above data is how it correlates with previous table, Top Ten Scanner from my.net. Many of these destinations are being scan by hosts within your network

Mar 29 15:57:27 my.net.228.10:27888 -> 24.31.216.121:1203 UDP
Mar 29 15:57:29 my.net.228.10:27888 -> 24.31.216.121:1203 UDP
Mar 29 15:57:30 my.net.228.10:0 -> 24.31.216.121:0 UDP
Mar 29 15:57:33 my.net.228.10:0 -> 24.31.216.121:0 UDP
Mar 29 15:57:33 my.net.228.10:27888 -> 24.31.216.121:1203 UDP
Mar 29 15:57:35 my.net.228.10:27888 -> 24.31.216.121:1203 UDP

Reverse Lookup

24.31.216.121 cae31-216-121.sc.rr.com

Registration Information for 24.31.216.121:

ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-1)
13241 Woodland Park Road
Herndon, VA 20171
US
Netname: ROAD-RUNNER-1
Netblock: 24.24.0.0 - 24.31.255.255
Maintainer: SCRR
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

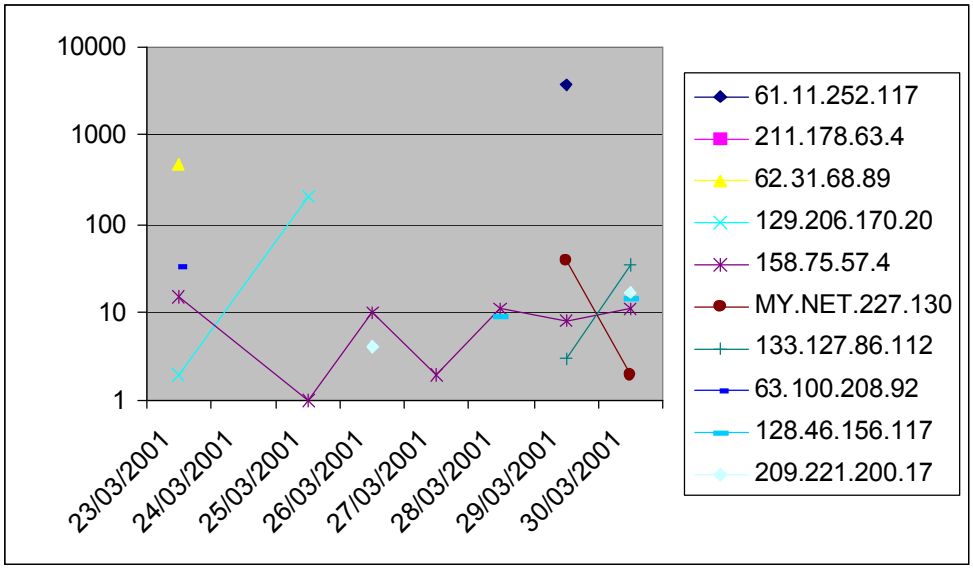
Record last updated on 13-Jun-2001.

Database last updated on 25-Jul-2001 23:06:28 EDT.

"Out Of Spec" Packets

Stephen Northcutt states "Attackers use out-of-spec packets to perform network mapping and to evade some intrusion detection systems and firewalls"[1]. The following section discusses some of the malformed packets seen in the data received from GIAC

Link Graph of Top Ten Out of Spec source addresses from Mar 23rd – Mar 30th and number of occurrences each source show each day.



The table below shows the top ten destinations mal-formed packet ("out of spec") were sent to.

Occurrences	Destination Address
197	MY.NET.202.54
39	MY.NET.253.125
38	MY.NET.213.142
22	MY.NET.100.165
21	MY.NET.219.162

This table shows the top ten sources of mal-formed packet ("out of spec") were sent from.

Occurrences	Source Address
3781	61.11.252.117
2033	211.178.63.4
466	62.31.68.89
199	129.206.170.20
58	158.75.57.4

This table shows the top five different mal-formed TCP flags.

Occurrences	Flags	Description Flags
6291	**SF****	Syn, Fin
448	21S*****	Reserved bits, Syn
8	2*SF**AU	Reserved bits, Syn, Ack, Urgent
8	2*SF****	Reserved bits, Syn, Fin
7	21SF****	Reserved bits, Syn, Fin

Out of spec packet are usually used in reconnaissance. This technique may be able to penetrate packet-filtering firewall and evade Intrusion detection systems, therefore go unnoticed. Some TCP/IP stacks may not handle OOS packets gracefully and therefore be susceptible to a denial of service condition.

Defensive Recommendation

These logs have shown that this network has a fairly open security policy. If there is a firewall at the boundary environment, consider setting the security policy to a default deny and explicitly allow required traffic. (Best Practices) For those servers that require routed Internet access, consider a DMZ stub network off of your firewall. It is recommended that these servers be moved into the DMZ area. The security policy should also implement egress filter as to deny any undesirable out-bound traffic. (i.e. the use of a compromised server to launch other attacks) Host based security products like TCP Wrappers, Tripwire, etc for DMZ server is highly recommended.

PC's, workstation and other internal server should reside inside of a second firewall. An application-based firewall/proxy will provide a higher level of protection (Defense in Depth Strategy). Consider using caching proxies such as iPlanet Proxy or Squid for http and SSL and Socks 5 proxy for other applications. Proxies allow your internal network to be hidden from the Internet.

The continued use of Intrusion Detection sensors at strategic locations through out your network will help your network administrator understand normal and abnormal traffic. IDS is one of the best tools that can provide early warning to malicious traffic.

The best strategy for security is defense in depth; this is more than multiple layers of firewalls. Below are some other recommendations:

- Only Install require Operation System and Application components
- Make sure OS's, firewalls and application servers are at the latest patch level
- Anti-virus software should be deployed on all desktop, with automated signature updates.
- Email gateways should perform virus checking before delivering IN or OUT bound email.
- Change all default passwords
- Servers should be configured to run only required network services.
- Disable file and print sharing all desktops were possible.
- Consider a secure centralized logging facility. This will prove valuable when auditing compromised servers.
- Consider documenting policies as a baseline for administrator to refer to when deploying equipment. (Unix, NT, Firewall, Password, eCommerce, etc)
- Require unique username and password for all users and enforce your password policy.
- Regular network reviews and audits will help maintain a high level of security. Start with a known good baseline and save this for future reference.

Analysis process

I chose to use snortsnarf to analyze the alert data. I spent considerable time getting snortsnarf to work. Some of the problems I experience included:

- alert data source, the (my.net) sanitization
- Running out of memory
- Running out of swap
- Link to addresses 0.0.0.0

I moved the data file I chose to analyze to a 650Mhz Pentium III Linux box with 192Mb of memory. I still experienced swap problem and so I created an additional 512mb swap file.

Data:
I combined all the alerts in to one file and changed the my.net to an address that did not occur in the data set.

Cat alert* >alerts.prac

cat alerts.prac |sed 's/MY.NET/10.10/g' >alerts.prac.clean

Now that I had all the alerts in one data file and clean out the MY.NET, is ran it through snortsnarf.

./snortsnarf –d /var/log/snortsnarf –split=0 –rulesfile /etc/snort/snort.conf \ alerts.prac.clean &

I made use of the following Unix utilities in various combinations to extract the data I wish to see and count: awk, grep , cat, sort, uniq.

I used the following to extract the data for the top five destination ports tables that goes with the top alerts from snortsnarf.

SYN-FIN Example:
Grep "SYN-FIN" alerts.prac.clean > SYN-FIN.tmp
Repeated for all alerts reports by snortsnarf

Cat SYN-FIN.tmp |awk ' {print $7} ' |cut –d ":" –f2 |sort –r |uniq –c |sort –rn |head >top-ten- SYN-FIN -dest-port

This gives me a list of unique destination ports, with the number of occurrences in reverse order.

The top ten attacker:

Cat SYN-FIN.tmp |awk ‘{print $5}’ |cut –d “:” –f1 >>top-attackers

I repeated to all *.tmp file. I had to change the awk command to match the correct field per detect as each detect type log entry was different.

Cat top-attackers |sort –r |uniq –c |sort –rn |head >top-ten-attackers

Scan logs:

Top ten scanner from my.net:

Combined all the scan logs and replaced the my.net with 10.10 using the same technique as with the alert logs.

Grep “10.10” scan.logs |awk ‘{print $4}’ |cut –d “:” –f1 |sort –r |uniq –c |sort –rn |head \
>top-ten-scanners-from-my.net

Extract the ip addresses
Cat top-ten-scanners-from-my.net |cut –d “ “ –f2 > xxx.tmp

For addr in `xxx.tmp`;do
Grep $addr top-ten-scanners-from-my.net |awk ‘{print $6}’ |sort –r |uniq –c |sort –rn \
|head > top-ten-scanners-from-my.net.dest-pair
Done

For the top ten destinations is used a perl script originally from Mike Bell, but Paul Asadoorian modified it to use for destination addresses.

snort_dest.pl

```
#!/usr/bin/perl
#

#   Start mainline code
while (<>) {
#
#  Check for blank line, if so process next line
#
   if ( $_ eq "" )  { next };
#
#  Check for spp_portscan, if it is get the next record
```

```
#
#  Tokenize the string so we can use it
#
   if ($_ =~ m/^\w{3}\s+\d+\s+\d+\:\d+\:\d+\s+([\w\d\.]+)\:(\d+)\s+\-
\>\s+([\d\w\.]+)\:(\d+)\s+UDP/) {

      $saddr =    $1;
      $sport =    $2;
      $daddr =    $3;
      $dport =    $4;
      $dest{$daddr}++;
   }  # end if

   if ($_ =~ m/^\w{3}\s+\d+\s+\d+\:\d+\:\d+\s+([\w\d\.]+)\:(\d+)\s+\-
\>\s+([\d\w\.]+)\:(\d+)\s+([-\w]+)\s+[\*1PUSFAR]+\s+/) {

      $saddr =    $1;
      $sport =    $2;
      $daddr =    $3;
      $dport =    $4;
      $descrp =   $5;
      $dest{$daddr}++;
   }  # end if

}  # while

foreach $num ( sort keys(%dest) ) {
      $strings = $dest{$num};
      foreach $string (split(' ', $strings)) {
            print "$string\t$num\n";
      }
}
```

Resources

http://www.sans.org
http://www.incidents.org
http://packetstormsecurity.org
http://cve.mitre.org
http://xforece.iss.net
http://www.seurityfocus.com
http://www.snort.org