Global Information Assurance Certification Paper

Intrusion Detection in Depth

GCIA Practical Assignment (v 2.7a)

by

MICHAEL LASTOR

MAY 2001

ASSIGNMENT # 1

5 Network Detects

Detect # 1

```
010422 01:01:19  211.123.22.130:3748   1   6   MY.NET.230.0 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3749   1   6   MY.NET.230.1 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3750   1   6   MY.NET.230.2 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3751   1   6   MY.NET.230.3 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3752   1   6   MY.NET.230.4 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3753   1   6   MY.NET.230.5 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3754   1   6   MY.NET.230.6 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3755   1   6   MY.NET.230.7 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3756   1   6   MY.NET.230.8 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3758   1   6   MY.NET.230.9 :111     0     1   0.04
010422 01:01:19  211.123.22.130:3760   1   6   MY.NET.230.10:111     0     1   0.04
010422 01:01:19  211.123.22.130:3762   1   6   MY.NET.230.11:111     0     1   0.04
010422 01:01:19  211.123.22.130:3764   1   6   MY.NET.230.12:111     0     1   0.04
010422 01:01:19  211.123.22.130:3766   1   6   MY.NET.230.13:111     0     1   0.04
010422 01:01:19  211.123.22.130:3768   1   6   MY.NET.230.14:111     0     1   0.04
010422 01:01:19  211.123.22.130:3769   1   6   MY.NET.226.14:111     0     1   0.04
010422 01:01:19  211.123.22.130:3770   1   6   MY.NET.230.15:111     0     1   0.04
010422 01:01:19  211.123.22.130:3771   1   6   MY.NET.230.16:111     0     1   0.04
010422 01:01:19  211.123.22.130:3772   1   6   MY.NET.230.17:111     0     1   0.04
010422 01:01:19  211.123.22.130:3773   1   6   MY.NET.230.18:111     0     1   0.04
010422 01:01:19  211.123.22.130:3774   1   6   MY.NET.230.19:111     0     1   0.04
010422 01:01:19  211.123.22.130:3775   1   6   MY.NET.230.20:111     0     1   0.04
```

Cut to save space

```
010422 01:01:19  211.123.22.130:3988   1   6   MY.NET.237.240:111    0     1   0.04
010422 01:01:19  211.123.22.130:3989   1   6   MY.NET.237.241:111    0     1   0.04
010422 01:01:19  211.123.22.130:3990   1   6   MY.NET.237.242:111    0     1   0.04
010422 01:01:19  211.123.22.130:3991   1   6   MY.NET.237.243:111    0     1   0.04
010422 01:01:19  211.123.22.130:3992   1   6   MY.NET.237.244:111    0     1   0.04
010422 01:01:19  211.123.22.130:3993   1   6   MY.NET.237.245:111    0     1   0.04
010422 01:01:19  211.123.22.130:3994   1   6   MY.NET.237.246:111    0     1   0.04
010422 01:01:19  211.123.22.130:3995   1   6   MY.NET.237.247:111    0     1   0.04
010422 01:01:19  211.123.22.130:3996   1   6   MY.NET.237.248:111    0     1   0.04
010422 01:01:19  211.123.22.130:3997   1   6   MY.NET.237.249:111    0     1   0.04
010422 01:01:19  211.123.22.130:3998   1   6   MY.NET.237.250:111    0     1   0.04
010422 01:01:19  211.123.22.130:3999   1   6   MY.NET.237.251:111    0     1   0.04
010422 01:01:19  211.123.22.130:4000   1   6   MY.NET.237.252:111    0     1   0.04
010422 01:01:19  211.123.22.130:4001   1   6   MY.NET.237.253:111    0     1   0.04
010422 01:01:19  211.123.22.130:4002   1   6   MY.NET.237.254:111    0     1   0.04
010422 01:01:19  211.123.22.130:4003   1   6   MY.NET.237.255:111    0     1   0.04
010422 01:01:19  211.123.22.130:4004   1   6   MY.NET.237.256:111    0     1   0.04
```

1. Source of Trace:

This trace is from one of the networks we monitor.

2. Detect was generated by:

A custom written script that parses the raw survey data from the Network Intrusion Detection (NID) sensor on the networks we monitor to produce the format below:

Date	Time	Source IP:Port		Protocol	Destination IP:Port		Total #	Size
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.0 :111	0	1	0.04
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.1 :111	0	1	0.04
		# of Packets Sent by Source			**# of Packets Sent by Dest. (Response)**			

(Size is in Kbytes) Protocol: 6=TCP, 17=UDP, 1=ICMP.

3. Probability the source address was spoofed:

This is considered information gathering, to see if any of the hosts have port 111 open and listening. This information needs to get back to the originator, so I would say the source address is NOT spoofed. However, it may be a compromised host, or a "jump point," for the actual attacker.

4. Description of attack:

This is a scan looking for an open and listening port of 111 on a Unix machine. If a machine is found to be listening on port 111, then one of many buffer overflow attacks can be used to compromise the machine.

5. Attack mechanism:

Scanning port 111 is the first step in this attack. The hacker is looking for computers listening on port 111. In my trace, the hacker sent one packet to each IP address in a Class 'C' block to see if he gets any responses. If the hacker receives a "port unreachable" or no response at all, he will assume there is no computer or it is not running the services requested. If he does get a response, then the hacker will attempt an RPC portmapper dump. This will give him a list of all RPC programs running on the target machine. From there, he can make the determination if anything can be exploited. There are numerous exploits that can be used, such as the *rpcbind* vulnerability, the rpc.cmsd overflow exploit, just to name a few. The *rpcbind* vulnerability, if successful, will give the hacker root level access to the target machine.

6. Correlations:

Although I cannot find the actual IP attacking anyone else, the port targeted happens to be the # 2 port of interest according to Incidents.org on April 30, 2001 (http://www.incidents.org/cid/query/top_10port_7.php) and another good paper about rpc was written by David P. Reece and is located at http://www.sans.org/newlook/resources/IDFAQ/blocking.htm. There are over 11 official and 7

Candidate CVE's about this subject – CVE-1999-0320, CVE-1999-0189, and CVE-1999-0190 are just a few of them.

7. Evidence of active targeting:

This does not seem to be active targeting, or targeting at all. The hacker started with a Class "C" address block and just incremented the fourth octet by one for each scan, looking for anyone listening on port 111.

8. Severity:

Direction	Category	Value	Reasons
Attack	Critical	3	Mixture of hosts, error toward caution.
	Lethality	5	If successful, hacker may gain ROOT access.
Response	System	3	Too many hosts – Unsure of the status of patches.
	Network	5	No replies, blocked by the firewall.
Severity = (3 + 5) – (3 + 5) = 0			

9. Defensive recommendation:

If you do not need RPC to be used on your system, disable it and block port 111 at the firewall. However, it is possible (default by some manufactures) to have RPC listening on other, higher ports, such as 37340. The best thing is to ensure only authorized users / hosts have permissions to connect to port 111 or whatever the default is. For Windows users, this is not serious at all. The hacker is just scanning computers looking for a UNIX system they can exploit.

10. Multiple choice test question:

From the trace above, the attacker is looking for port 111, why?

a) To see if the mail server is up and running
b) To see if RPC is running and listening on a Unix machine
c) To see what version of Windows the machine is running
d) To do a remote system back-up

Answer: (b)

Detect # 2

010418	12:02:21	211.239.90.198:3457	1	6	MY.NET.36.31:98	0	1	0.04
010418	12:02:21	211.239.90.198:3465	1	6	MY.NET.36.39:98	0	1	0.04
010418	12:02:21	211.239.90.198:3468	2	6	MY.NET.36.42:98	0	2	0.08
010418	12:02:21	211.239.90.198:3469	2	6	MY.NET.36.43:98	0	2	0.08
010418	12:02:21	211.239.90.198:3470	1	6	MY.NET.36.44:98	0	1	0.04
010418	12:02:22	211.239.90.198:3471	2	6	MY.NET.36.45:98	0	2	0.08
010418	12:02:22	211.239.90.198:3472	2	6	MY.NET.36.46:98	0	2	0.08
010418	12:02:22	211.239.90.198:3473	2	6	MY.NET.36.47:98	0	2	0.08
010418	12:02:22	211.239.90.198:3474	2	6	MY.NET.36.48:98	0	2	0.08
010418	12:02:22	211.239.90.198:3475	2	6	MY.NET.36.49:98	0	2	0.08
010418	12:02:22	211.239.90.198:3476	2	6	MY.NET.36.50:98	0	2	0.08
010418	12:02:22	211.239.90.198:3477	2	6	MY.NET.36.51:98	0	2	0.08
010418	12:02:22	211.239.90.198:3478	2	6	MY.NET.36.52:98	0	2	0.08
010418	12:02:22	211.239.90.198:3479	2	6	MY.NET.36.53:98	0	2	0.08
010418	12:02:25	211.239.90.198:3480	1	6	MY.NET.36.54:98	0	1	0.04
010418	12:02:25	211.239.90.198:3481	1	6	MY.NET.36.55:98	0	1	0.04
010418	12:02:25	211.239.90.198:3482	1	6	MY.NET.36.56:98	0	1	0.04
010418	12:02:22	211.239.90.198:3486	1	6	MY.NET.36.60:98	0	1	0.04
010418	12:02:25	211.239.90.198:3488	1	6	MY.NET.36.62:98	0	1	0.04
010418	12:02:22	211.239.90.198:3495	1	6	MY.NET.36.69:98	0	1	0.04
010418	12:02:22	211.239.90.198:3502	1	6	MY.NET.36.76:98	0	1	0.04
010418	12:02:22	211.239.90.198:3513	1	6	MY.NET.36.87:98	0	1	0.04
010418	12:02:25	211.239.90.198:3519	1	6	MY.NET.36.93:98	0	1	0.04
010418	12:02:22	211.239.90.198:3523	1	6	MY.NET.36.97:98	0	1	0.04
010418	12:02:22	211.239.90.198:3535	1	6	MY.NET.36.109:98	0	1	0.04
010418	12:02:25	211.239.90.198:3536	1	6	MY.NET.36.110:98	0	1	0.04
010418	12:02:25	211.239.90.198:3537	1	6	MY.NET.36.111:98	0	1	0.04
010418	12:02:22	211.239.90.198:3538	2	6	MY.NET.36.112:98	0	2	0.08
010418	12:02:25	211.239.90.198:3539	1	6	MY.NET.36.113:98	0	1	0.04
010418	12:02:25	211.239.90.198:3540	1	6	MY.NET.36.114:98	0	1	0.04
010418	12:02:25	211.239.90.198:3544	1	6	MY.NET.36.118:98	0	1	0.04
010418	12:02:25	211.239.90.198:3549	1	6	MY.NET.36.123:98	0	1	0.04
010418	12:02:22	211.239.90.198:3558	1	6	MY.NET.36.132:98	0	1	0.04
010418	12:02:25	211.239.90.198:3562	1	6	MY.NET.36.135:98	0	1	0.04
010418	12:02:22	211.239.90.198:3572	1	6	MY.NET.36.145:98	0	1	0.04
010418	12:02:25	211.239.90.198:3582	1	6	MY.NET.36.154:98	0	1	0.04
010418	12:02:22	211.239.90.198:3583	1	6	MY.NET.36.155:98	0	1	0.04
010418	12:02:22	211.239.90.198:3587	1	6	MY.NET.36.159:98	0	1	0.04
010418	12:02:22	211.239.90.198:3596	1	6	MY.NET.36.168:98	0	1	0.04
010418	12:02:22	211.239.90.198:3604	1	6	MY.NET.36.176:98	0	1	0.04
010418	12:02:22	211.239.90.198:3613	1	6	MY.NET.36.185:98	0	1	0.04
010418	12:02:22	211.239.90.198:3622	1	6	MY.NET.36.194:98	0	1	0.04
010418	12:02:22	211.239.90.198:3629	1	6	MY.NET.36.201:98	0	1	0.04
010418	12:02:25	211.239.90.198:3637	1	6	MY.NET.36.209:98	0	1	0.04
010418	12:02:22	211.239.90.198:3643	1	6	MY.NET.36.215:98	0	1	0.04
010418	12:02:22	211.239.90.198:3656	1	6	MY.NET.36.228:98	0	1	0.04
010418	12:02:25	211.239.90.198:3661	1	6	MY.NET.36.233:98	0	1	0.04

010418 12:02:22 211.239.90.198:3672 1 6 MY.NET.36.244:98 0 1 0.04

1. Source of Trace:

This trace is from one of the networks we monitor.

2. Detect was generated by:

A custom written script that parses the raw survey data from the Network Intrusion Detection (NID) sensor on the networks we monitor to produce the format below:

Date	Time	Source IP:Port		Protocol	Destination IP:Port		Total #	Size
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.0 :111	0	1	0.04
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.1 :111	0	1	0.04

# of Packets Sent by Source **# of Packets Sent by Dest. (Response)**

(Size is in Kbytes) Protocol: 6=TCP, 17=UDP, 1=ICMP.

3. Probability the source address was spoofed:

This would be considered information gathering to see if any of the hosts have port 98 open and listening. This information needs to get back to the originator, so I would say the source address is NOT spoofed. However, it may be a compromised host, or a "jump point," for the actual attacker.

4. Description of attack:

If the hacker initiates a Buffer overflow to a Linux box with the linuxconf package, this would allow the attacker to gain root privileges.

5. Attack mechanism:

Note (a little background on the subject) From the website of the developers of linuxconf (http://www.solucorp.qc.ca/linuxconf/),
"To connect using the web interface to a linuxconf box (not a demo), you connect to port 98, using a URL like this one:

http://your_linux_box:98/

By default, this service is disabled. To enable it, visit the networking menu in linuxconf, at the end, select the entry "linuxconf network access." Read the help there :-)
You don't have to install an httpd server to get this feature. Linuxconf handles the http protocol itself and is started from the inetd server."

As you can imagine, this could be a problem. The attacker would start by probing port 98 looking for some type of response. If the hacker received "port unreachable" or no answer at all, this would tell him that, either there is no box at that IP (turned off or something like that) or that box is not a Linux box running linuxconf. If, however, he got a 'positive' response from the box, then he would initiate a buffer overflow. This buffer overflow, if executed properly, would give the hacker access to the system at the root level. (This buffer overflow can be easily obtained at http://linux.opennet.ru/base/linux/252.txt.html.)

6. Correlations:

During a search through the search engine 'google', I came across many message boards with posts concerning scans to port 98. According to Security Alert For Enterprise Resources' (SAFER) website, http://www.safermag.com/html/safer34/alerts/45.html,

"An attacker supplying excess data to the USER_AGENT field in vulnerable versions of Linuxconf. This data can overflow the relevant buffer, creating a stack overflow and, properly exploited, allowing remote execution of arbitrary code as root." This was released on February 12, 2001. Their website also gives the reference of http://www.securityfocus.com/bid/2352 with, basically, the same information, but Securityfocus gives it a Bugtraq ID# of 2352.
The only CVE that pertains to this vulnerability is a Candidate CVE: CAN-2000-0017.
Stephen Northcutt covered this particular port during the Aloha II Intrusion Detection Immersion Curriculum, which is also on page 354 in the book provided to us by the SANS Institute. This port of interest has also been seen by other SANS followers through the submission of traces to the sans.org website, http://www.sans.org/y2K/042500-2300.htm.

7. Evidence of active targeting:

This does not seem to be active targeting, or targeting at all. Looks like the hacker had an automated script that randomly scans address within a given Class "C" address block. The hacker could have actually scanned all of the address in the address block, but due to sensor location and network topology, we did not detect scans to the other address.

8. Severity:

Direction	Category	Value	Reasons
Attack	Critical	3	Mixture of hosts, error toward caution.
	Lethality	5	If successful, hacker may gain ROOT access.
Response	System	3	Too many hosts – Unsure of running services.
	Network	5	No replies from hosts or blocked by the firewall.
Severity = (3 + 5) – (3 + 5) = 0			

9. Defensive recommendation:

The defenses of this network are good, no replies were sent to the hacker. Either the firewall stopped the packets or the boxes did not reply. To error on the side of caution, if any of the hosts in this network is running Linux, the linuxconf service should be disabled, which it is by default. If this service is disabled, there is no threat from this vulnerability.

10. Multiple choice test question:

The linuxconf service is disabled by default, why should you ***not*** enable it?

a) The system will become completely unstable

b) The password file will over-write itself with 0's
c) This will open port 98 to a listen state
d) Will set up the web server and the default web page

Answer (c)

Detect # 3

010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.29:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.30:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.31:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.32:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.33:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.45:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.46:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.47:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.48:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.49:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.50:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.51:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.52:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.53:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.60:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.61:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.62:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.63:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11558	1	17	MY.NET.60.65:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.109:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.110:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.111:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.112:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.113:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.114:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.116:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.117:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.126:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.127:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.128:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.129:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.130:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.131:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.132:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.133:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.156:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.171:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.172:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.173:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.174:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.177:31789	0	1	0.009

010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.178:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.180:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.187:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.188:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.190:31789	0	1	0.009
010425 18:13:20	212.217.115.79:11559	1	17	MY.NET.60.191:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.192:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.195:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.196:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.203:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.205:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.206:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.208:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.209:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.249:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.250:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.251:31789	0	1	0.009
010425 18:13:21	212.217.115.79:11559	1	17	MY.NET.60.253:31789	0	1	0.009

1. Source of Trace:

This trace is from one of the networks we monitor.

2. Detect was generated by:

A custom written script that parses the raw survey data from the Network Intrusion Detection (NID) sensor on the networks we monitor to produce the format below:

Date	Time	Source IP:Port		Protocol	Destination IP:Port		Total #	Size
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.0 :111	0	1	0.04
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.1 :111	0	1	0.04

# of Packets Sent by Source **# of Packets Sent by Dest. (Response)**

(Size is in Kbytes) Protocol: 6=TCP, 17=UDP, 1=ICMP.

3. Probability the source address was spoofed:

This would be considered a reconnaissance effort. The hacker is looking for a Trojan, and in order for anything useful to happen, the hacker must talk to it. I would say the source address is NOT spoofed.

4. Description of attack:

The hacker locates an infected or "trojanized" host, connects his client software with the server software on the infected host, takes over the infected host, and literally controls everything on that host.

5. Attack mechanism:

The best ways to explain the attack mechanism is by letting the creator of the product or Trojan explain it. From the *Official Hack 'a' Tack Homepage*, Copyright 1999-2000 by DaNcE-eViL, Inc. (http://www.crokket.de/hat/index1.html)
"Hack'a'Tack is a RAT (Remote Administration Tool) or Trojan like Back Orifice or SubSeven. It uses an exploit in Windows 9x to gain access to a remote computer through the Internet using the target computer's IP address and a small server program which must be installed on the remote box."

Once at their website, if you click on the Information link and then select the "tips and tricks" you will get their *'Tutorial on infecting people with Hack'a'Tack*.' With this tutorial, you will find out about the ways to establish a connection with an infected host. As stated above, the server.exe program must be installed on the target machine. This can be done via email attachments or something of the like. Once the program is installed and listening to port 31789, all the hacker needs to do is to connect his computer (using the client.exe program) to the target. There are essentially three ways to locate an infected machine that you can connect to. The easiest and laziest way is to click the Transmit IP button. This will go out to the Hack 'a' Tack FTP server and pull down the IP's and names of infected computers. You just have to wait for a few seconds in order to find out how many infected computers are in the list. The second way is to do the actual scanning for infected hosts. Just enter the Start-IP into the input field and click on the scan button to start scanning (This is what this trace shows). As the scanner finds an infected machine, the name will be displayed in the list also. The third way to locate a victim or establish a connection would only be used if you want to access a special computer. If you have the IP address of an infected machine, just enter the IP address into the IP-Address field and click on 'connect'. Once you have found an infected computer and have connected to it, you literally control the box. You can do anything you want to, even shutdown, log off user, etc.

6. Correlations:

From Xploiter.com (http://www.xploiter.com/security/hackattack.html), they give us the technical information on the Trojan:

Name: Hack 'a' Tack
Version: Version No. not known
File Sizes: See Above
Affected Operating Systems: **Win95 & 98 - possibly NT**
Listen ports (default): TCP - 31785, 31787, 31789 & 31791 - **UDP - 31789** & 31791
Startup Routine: Registry
Written in: Delphi
Severity: Medium Risk

There are tons of message boards that have material concerning this Trojan; one of the most interesting ones was http://lists.gnac.net/firewalls/mhonarc/firewalls.199907/msg00772.html. This one gives a brief list of the ports associated with the Hack 'a' Tack Trojan;

The ports used by this Trojan include the following:
TCP ports 31785 and 31787
UDP ports 31789 and 31791

In addition, Onctek has a list of ports that are used by known Trojans, which also listed this

Trojan using port 31789 UDP (http://www.onctek.com/trojanports.html).
Jeff Stutzman, an analyst with SANS, listed port 31789 as being seen on his daily report (http://www.sans.org/y2k/0102stutzman.htm). There are no CVE associated with this attack since is does not deal with an operating system or service fault. Trojans, I believe, are not covered in CVE's.

7. Evidence of active targeting:

This does not seem to be active targeting, or targeting at all. Looks like the hacker pressed the 'scan' button and let the client application do its thing. The hacker or the application could have actually scanned all of the address in the address block, but due to sensor location and network topology, we did not detect scans to the other address.

8. Severity:

Direction	Category	Value	Reasons
Attack	Critical	3	Mixture of hosts, error toward caution.
	Lethality	5	If infected, attacker owns your box.
Response	System	5	Antiviral patterns up-to-date.
	Network	5	No replies from hosts, blocked by the firewall.
Severity = (3 + 5) – (5 + 5) = -2			

9. Defensive recommendation:

The defenses of this network are good, no replies were sent to the hacker. Either the firewall stopped the packets or the boxes are not infected. The sites should ensure that their virus patterns are always the most current one, and scan the systems regularly. If this type of probe continues for a long period, the site may want to block the IP address (if it is always the same) or block the port at the firewall.

10. Multiple choice test question:

When you open an attachment with the Hack 'a' Tack Trojan in it, what happens next?

a) The server.exe application installs itself and starts to listen on port 31789.
b) The hard drive is completely erased.
c) Sends a message to the infected hosts' user stating, "I own you!"
d) Sends an e-mail message to everyone in your address book.

Answer (a)

Detect # 4

010406 06:06:15	64.165.54.89:2522	2	6	MY.NET.221.0:80	0	2	0.056
010406 06:06:15	64.165.54.89:2523	3	6	MY.NET.221.0:8080	0	3	0.084
010406 06:06:15	64.165.54.89:2524	3	6	MY.NET.221.0:3128	0	3	0.084
010406 06:06:15	64.165.54.89:2525	3	6	MY.NET.221.0:1080	0	3	0.084
010406 06:06:15	64.165.54.89:2526	3	6	MY.NET.221.0:8000	0	3	0.084
010406 06:06:15	64.165.54.89:2527	3	6	MY.NET.221.0:8081	0	3	0.084
010406 06:06:15	64.165.54.89:2528	3	6	MY.NET.221.0:23	0	3	0.084
010406 06:06:15	64.165.54.89:2529	3	6	MY.NET.221.0:2301	0	3	0.084
010406 06:06:15	64.165.54.89:2530	3	6	MY.NET.221.1:80	0	3	0.084
010406 06:06:15	64.165.54.89:2531	3	6	MY.NET.221.1:8080	0	3	0.084
010406 06:06:15	64.165.54.89:2532	3	6	MY.NET.221.1:3128	0	3	0.084
010406 06:06:15	64.165.54.89:2533	5	6	MY.NET.221.1:1080	0	5	0.140
010406 06:06:15	64.165.54.89:2534	3	6	MY.NET.221.1:8000	0	3	0.084
010406 06:06:15	64.165.54.89:2535	3	6	MY.NET.221.1:8081	0	3	0.084
010406 06:06:15	64.165.54.89:2536	2	6	MY.NET.221.1:23	0	2	0.056
010406 06:06:15	64.165.54.89:2537	3	6	MY.NET.221.1:2301	0	3	0.084
010406 06:06:16	64.165.54.89:2538	3	6	MY.NET.221.2:80	0	3	0.084
010406 06:06:16	64.165.54.89:2539	3	6	MY.NET.221.2:8080	0	3	0.084
010406 06:06:16	64.165.54.89:2540	3	6	MY.NET.221.2:3128	0	3	0.084
010406 06:06:16	64.165.54.89:2541	3	6	MY.NET.221.2:1080	0	3	0.084
010406 06:06:16	64.165.54.89:2542	3	6	MY.NET.221.2:8000	0	3	0.084
010406 06:06:16	64.165.54.89:2543	3	6	MY.NET.221.2:8081	0	3	0.084
010406 06:06:16	64.165.54.89:2544	4	6	MY.NET.221.2:23	0	4	0.112
010406 06:06:16	64.165.54.89:2545	2	6	MY.NET.221.2:2301	0	2	0.056
010406 06:06:18	64.165.54.89:2546	3	6	MY.NET.221.3:80	0	3	0.084
010406 06:06:18	64.165.54.89:2547	3	6	MY.NET.221.3:8080	0	3	0.084
010406 06:06:18	64.165.54.89:2548	3	6	MY.NET.221.3:3128	0	3	0.084
010406 06:06:18	64.165.54.89:2549	2	6	MY.NET.221.3:1080	0	2	0.056
010406 06:06:18	64.165.54.89:2550	3	6	MY.NET.221.3:8000	0	3	0.084
010406 06:06:18	64.165.54.89:2551	3	6	MY.NET.221.3:8081	0	3	0.084
010406 06:06:18	64.165.54.89:2552	3	6	MY.NET.221.3:23	0	3	0.084
010406 06:06:18	64.165.54.89:2553	3	6	MY.NET.221.3:2301	0	3	0.084
010406 06:06:22	64.165.54.89:2554	3	6	MY.NET.221.4:80	0	3	0.084
010406 06:06:22	64.165.54.89:2555	3	6	MY.NET.221.4:8080	0	3	0.084
010406 06:06:22	64.165.54.89:2556	3	6	MY.NET.221.4:3128	0	3	0.084
010406 06:06:22	64.165.54.89:2557	3	6	MY.NET.221.4:1080	0	3	0.084
010406 06:06:22	64.165.54.89:2558	3	6	MY.NET.221.4:8000	0	3	0.084
010406 06:06:22	64.165.54.89:2559	3	6	MY.NET.221.4:8081	0	3	0.084
010406 06:06:22	64.165.54.89:2560	3	6	MY.NET.221.4:23	0	3	0.084
010406 06:06:22	64.165.54.89:2561	2	6	MY.NET.221.4:2301	0	2	0.056
010406 06:06:23	64.165.54.89:2562	2	6	MY.NET.221.5:80	0	2	0.056
010406 06:06:23	64.165.54.89:2563	3	6	MY.NET.221.5:8080	0	3	0.084
010406 06:06:23	64.165.54.89:2564	3	6	MY.NET.221.5:3128	0	3	0.084

010406	06:06:23	64.165.54.89:2565	3	6	MY.NET.221.5:1080	0	3	0.084
010406	06:06:23	64.165.54.89:2566	2	6	MY.NET.221.5:8000	0	2	0.056
010406	06:06:23	64.165.54.89:2567	3	6	MY.NET.221.5:8081	0	3	0.084
010406	06:06:23	64.165.54.89:2568	3	6	MY.NET.221.5:23	0	3	0.084
010406	06:06:23	64.165.54.89:2569	3	6	MY.NET.221.5:2301	0	3	0.084

Cut to save space

010406	06:08:09	64.165.54.89:4523	3	6	MY.NET.221.250:80	0	3	0.084
010406	06:08:09	64.165.54.89:4524	3	6	MY.NET.221.250:8080	0	3	0.084
010406	06:08:09	64.165.54.89:4525	3	6	MY.NET.221.250:3128	0	3	0.084
010406	06:08:09	64.165.54.89:4526	3	6	MY.NET.221.250:1080	0	3	0.084
010406	06:08:09	64.165.54.89:4527	3	6	MY.NET.221.250:8000	0	3	0.084
010406	06:08:09	64.165.54.89:4528	3	6	MY.NET.221.250:8081	0	3	0.084
010406	06:08:09	64.165.54.89:4529	3	6	MY.NET.221.250:23	0	3	0.084
010406	06:08:09	64.165.54.89:4530	3	6	MY.NET.221.250:2301	0	3	0.084
010406	06:08:09	64.165.54.89:4531	2	6	MY.NET.221.251:80	0	2	0.056
010406	06:08:09	64.165.54.89:4532	3	6	MY.NET.221.251:8080	0	3	0.084
010406	06:08:09	64.165.54.89:4533	3	6	MY.NET.221.251:3128	0	3	0.084
010406	06:08:09	64.165.54.89:4534	3	6	MY.NET.221.251:1080	0	3	0.084
010406	06:08:09	64.165.54.89:4535	3	6	MY.NET.221.251:8000	0	3	0.084
010406	06:08:09	64.165.54.89:4536	3	6	MY.NET.221.251:8081	0	3	0.084
010406	06:08:09	64.165.54.89:4537	3	6	MY.NET.221.251:23	0	3	0.084
010406	06:08:09	64.165.54.89:4538	3	6	MY.NET.221.251:2301	0	3	0.084
010406	06:08:09	64.165.54.89:4539	3	6	MY.NET.221.252:80	0	3	0.084
010406	06:08:09	64.165.54.89:4540	3	6	MY.NET.221.252:8080	0	3	0.084
010406	06:08:09	64.165.54.89:4541	3	6	MY.NET.221.252:3128	0	3	0.084
010406	06:08:09	64.165.54.89:4542	3	6	MY.NET.221.252:1080	0	3	0.084
010406	06:08:09	64.165.54.89:4543	3	6	MY.NET.221.252:8000	0	3	0.084
010406	06:08:09	64.165.54.89:4544	3	6	MY.NET.221.252:8081	0	3	0.084
010406	06:08:09	64.165.54.89:4545	3	6	MY.NET.221.252:23	0	3	0.084
010406	06:08:09	64.165.54.89:4546	3	6	MY.NET.221.252:2301	0	3	0.084
010406	06:08:09	64.165.54.89:4547	3	6	MY.NET.221.253:80	0	3	0.084
010406	06:08:09	64.165.54.89:4548	3	6	MY.NET.221.253:8080	0	3	0.084
010406	06:08:09	64.165.54.89:4549	3	6	MY.NET.221.253:3128	0	3	0.084
010406	06:08:09	64.165.54.89:4550	3	6	MY.NET.221.253:1080	0	3	0.084
010406	06:08:09	64.165.54.89:4551	4	6	MY.NET.221.253:8000	0	4	0.112
010406	06:08:09	64.165.54.89:4552	3	6	MY.NET.221.253:8081	0	3	0.084
010406	06:08:09	64.165.54.89:4553	3	6	MY.NET.221.253:23	0	3	0.084
010406	06:08:09	64.165.54.89:4554	3	6	MY.NET.221.253:2301	0	3	0.084
010406	06:08:09	64.165.54.89:4555	3	6	MY.NET.221.254:80	0	3	0.084
010406	06:08:09	64.165.54.89:4556	3	6	MY.NET.221.254:8080	0	3	0.084
010406	06:08:09	64.165.54.89:4557	3	6	MY.NET.221.254:3128	0	3	0.084
010406	06:08:09	64.165.54.89:4558	3	6	MY.NET.221.254:1080	0	3	0.084
010406	06:08:09	64.165.54.89:4559	3	6	MY.NET.221.254:8000	0	3	0.084
010406	06:08:09	64.165.54.89:4560	3	6	MY.NET.221.254:8081	0	3	0.084
010406	06:08:09	64.165.54.89:4561	3	6	MY.NET.221.254:23	0	3	0.084
010406	06:08:09	64.165.54.89:4562	3	6	MY.NET.221.254:2301	0	3	0.084

1. Source of Trace:

This trace is from one of the networks we monitor.

2. Detect was generated by:

A custom written script that parses the raw survey data from the Network Intrusion Detection (NID) sensor on the networks we monitor to produce the format below:

Date	Time	Source IP:Port		Protocol	Destination IP:Port		Total #	Size
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.0 :111	0	1	0.04
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.1 :111	0	1	0.04

# of Packets Sent by Source **# of Packets Sent by Dest. (Response)**

(Size is in Kbytes) Protocol: 6=TCP, 17=UDP, 1=ICMP.

3. Probability the source address was spoofed:

The source address was NOT spoofed. The source will scan for other machines and must get a response back.

4. Description of attack:

Locates web servers and web proxy servers and sends the data to a local site, presumably so that the hacker can go to the machine of interest later for the attack. Using multiple infected machines can also use this as a Denial of Service attack.

5. Attack mechanism:

NOTE (From the website http://www.cknow.com/cknewsletter/0311.htm#ringzero "The name of this beast is taken from the name of the most basic level of operation for an operating system. Programs that run at ring zero generally have unrestricted access to the entire machine." Just a little background on the name)

From the website http://www.cknow.com/cknewsletter/0311.htm#ringzero, and http://www.symantec.com/avcenter/venc/data/ringzero.trojan.html gives the best overall picture of what RingZero does and how it does it.

First, the program is packed in a 'host program'. When you run the host program, the Trojan is installed on the computer. RingZero hides its process by registering itself as a Windows service, so it is not displayed in the Windows task manager. The Trojan then installs a VxD file (RING0.VXD) and two executable files (ITS.EXE and PST.EXE) when the program initially runs. The Trojan then sets the system up so that the executables will run each time the system starts. ITS.EXE creates the file ITS.DAT (reason unknown at this time). PST.EXE scans IP addresses looking for ports 80, 8080, and 3128. These ports are commonly used for HTTP, HTTPS/Proxy, and Squid Proxy respectively. If a target host answers on one of the ports that was scanned, then a CGI script at the site www.rusftpsearch.net is run and appears to record the proxy's IP address.

According to SANS web page, http://www.sans.org/newlook/resources/IDFAQ/ring_zero.htm,

"SANS' participants from around the world are reporting scans on port 80 (common port for world wide web), 8080 (common location for proxy), 3128 (squid proxy) and occasionally other 8000 series ports."
It looks as if this is that variant of the RingZero Trojan, because of the ports that were scanned. The other three ports scanned were port 23 (Telnet), 1080 (Wingate Proxy) and port 2301 (from what I can find on the Internet, tcp port 2301 is Compaq's Insight Managers' http interface or it may be a management port on some Cisco routers). Overall, it is still looking for proxy servers, with the exception of port 23. Referring back to http://www.cknow.com/cknewsletter/0311.htm#ringzero, collecting information appears to be the sole purpose of this Trojan. However, as cited by NSWC's John Green, "this activity reflects a significant advance in distributed attack technology because of Ring Zero's transmission rate; dynamic configuration options (may be able to go from scanning to attacking); and automated result consolidation." That excerpt was taken from, http://www.attrition.org/security/advisory/nipc/nipc-024.ringzero_trojan. This means the Trojan can be used for a Denial of Service (DoS) against a specified victim, and if multiple infected machines were used for the DoS, the results would be devastating.

6. Correlations:

According to SANS website located at, http://www.sans.org/newlook/resources/IDFAQ/ring_zero.htm, "SANS' participants from around the world are reporting scans on port 80 (common port for world wide web), 8080 (common location for proxy), 3128 (squid proxy) and occasionally other 8000 series ports." One of the many traces was posted at http://www.sans.org/y2k/021301.htm by Sid Faber, with Matt Fearnow as the Handler on Duty.
Stephen Northcutt covered this particular port during the Aloha II Intrusion Detection Immersion Curriculum, which is also on page 169 in the book provided to us by the SANS Institute. In addition, Bill Royds, a current GIAC Certified Intrusion Analyst (GCIA), submitted his assignment paper with RingZero as one of his detects.

7. Evidence of active targeting:

This does not seem to be active targeting, or targeting at all. Looks like the an infected machine (assuming) is 'doing its job' and scanning an entire Class 'C' address block looking for any proxy servers that will respond to it.

8. Severity:

Direction	Category	Value	Reasons
Attack	Critical	4	Looking for specific machines, Proxy servers.
	Lethality	3	Possibly acquire password lists from infected hosts
Response	System	5	Antiviral patterns up-to-date.
	Network	5	No replies from hosts, blocked by the firewall.
Severity = (4 + 3) – (5 + 5) = -3			

9. Defensive recommendation:

The defenses of this network are good, no replies were sent to the source host. Either the firewall stopped the packets or the boxes are not running the requested services. The sites should ensure that their virus patterns are always the most current one, and scan the systems regularly. The site administrator should monitor outbound traffic to see if their site is scanning other sites for the above-mentioned ports, if they are scanning other hosts, then this is a good indication that they are infected and need to clean their machines.

10. Multiple choice test question:

In a 'classic' RingZero scan, what types of servers or services is the source host looking for?

a) SMTP servers
b) IRC servers
c) FTP servers
d) Proxy servers

Answer (d)

Detect # 5

010406 04:12:57	65.112.196.156:4065	10	6	MY.NET.228.0:515	0	10	0.3
010406 04:12:57	65.112.196.156:4066	10	6	MY.NET.228.0:53	0	10	0.3
010406 04:12:57	65.112.196.156:4067	6	6	MY.NET.228.1:515	0	6	0.18
010406 04:12:57	65.112.196.156:4068	6	6	MY.NET.228.1:53	0	6	0.18
010406 04:12:57	65.112.196.156:4069	10	6	MY.NET.228.2:515	0	10	0.3
010406 04:12:57	65.112.196.156:4070	10	6	MY.NET.228.2:53	0	10	0.3
010406 04:12:57	65.112.196.156:4071	11	6	MY.NET.228.3:515	0	11	0.33
010406 04:12:57	65.112.196.156:4072	11	6	MY.NET.228.3:53	0	11	0.33
010406 04:12:57	65.112.196.156:4073	10	6	MY.NET.228.4:515	0	10	0.3
010406 04:12:57	65.112.196.156:4074	10	6	MY.NET.228.4:53	0	10	0.3
010406 04:12:57	65.112.196.156:4075	4	6	MY.NET.228.5:515	0	4	0.12
010406 04:12:57	65.112.196.156:4076	4	6	MY.NET.228.5:53	0	4	0.12
010406 04:12:57	65.112.196.156:4077	5	6	MY.NET.228.6:515	0	5	0.15
010406 04:12:57	65.112.196.156:4078	5	6	MY.NET.228.6:53	0	5	0.15
010406 04:12:57	65.112.196.156:4079	10	6	MY.NET.228.7:515	0	10	0.3
010406 04:12:57	65.112.196.156:4080	10	6	MY.NET.228.7:53	0	10	0.3
010406 04:12:57	65.112.196.156:4081	6	6	MY.NET.228.8:515	0	6	0.18
010406 04:12:57	65.112.196.156:4082	6	6	MY.NET.228.8:53	0	6	0.18
010406 04:12:57	65.112.196.156:4083	10	6	MY.NET.228.9:515	0	10	0.3
010406 04:12:57	65.112.196.156:4084	10	6	MY.NET.228.9:53	0	10	0.3
010406 04:12:57	65.112.196.156:4085	10	6	MY.NET.228.10:515	0	10	0.3
010406 04:12:57	65.112.196.156:4086	10	6	MY.NET.228.10:53	0	10	0.3

Cut to save space

010406 04:12:59	65.112.196.156:4555	6	6	MY.NET.228.245:515	0	6	0.18
010406 04:12:59	65.112.196.156:4556	6	6	MY.NET.228.245:53	0	6	0.18
010406 04:12:59	65.112.196.156:4557	5	6	MY.NET.228.246:515	0	5	0.15
010406 04:12:59	65.112.196.156:4558	5	6	MY.NET.228.246:53	0	5	0.15
010406 04:12:59	65.112.196.156:4559	5	6	MY.NET.228.247:515	0	5	0.15
010406 04:12:59	65.112.196.156:4560	5	6	MY.NET.228.247:53	0	5	0.15
010406 04:12:59	65.112.196.156:4561	5	6	MY.NET.228.248:515	0	5	0.15
010406 04:12:59	65.112.196.156:4562	5	6	MY.NET.228.248:53	0	5	0.15
010406 04:12:59	65.112.196.156:4563	5	6	MY.NET.228.249:515	0	5	0.15
010406 04:12:59	65.112.196.156:4564	5	6	MY.NET.228.249:53	0	5	0.15
010406 04:12:59	65.112.196.156:4565	5	6	MY.NET.228.250:515	0	5	0.15
010406 04:12:59	65.112.196.156:4566	5	6	MY.NET.228.250:53	0	5	0.15
010406 04:12:59	65.112.196.156:4567	7	6	MY.NET.228.251:515	0	7	0.21
010406 04:12:59	65.112.196.156:4568	7	6	MY.NET.228.251:53	0	7	0.21
010406 04:12:59	65.112.196.156:4569	6	6	MY.NET.228.252:515	0	6	0.18
010406 04:12:59	65.112.196.156:4570	6	6	MY.NET.228.252:53	0	6	0.18
010406 04:12:59	65.112.196.156:4571	5	6	MY.NET.228.253:515	0	5	0.15
010406 04:12:59	65.112.196.156:4572	5	6	MY.NET.228.253:53	0	5	0.15
010406 04:12:59	65.112.196.156:4573	5	6	MY.NET.228.254:515	0	5	0.15
010406 04:12:59	65.112.196.156:4574	5	6	MY.NET.228.254:53	0	5	0.15

1. Source of Trace:

This trace is from one of the networks we monitor.

2. Detect was generated by:

A custom written script that parses the raw survey data from the Network Intrusion Detection (NID) sensor on the networks we monitor to produce the format below:

Date	Time	Source IP:Port		Protocol	Destination IP:Port		Total #	Size
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.0 :111	0	1	0.04
010422	01:01:19	211.123.22.130:3748	1	6	MY.NET.230.1 :111	0	1	0.04

# of Packets Sent by Source **# of Packets Sent by Dest. (Response)**

(Size is in Kbytes) Protocol: 6=TCP, 17=UDP, 1=ICMP.

3. Probability the source address was spoofed:

The source address was NOT spoofed. The source will scan for other machines and must get a response back.

4. Description of attack:

The Linux worm, called the Adore Worm, tries to exploit the overflow vulnerability of lpd port 515 and may exploit TCP ports 53 (DNS) and 111 (RPC) on Linux hosts. Once the worm has infected a host, it will start scanning the Internet in an attempt to propagate itself.

5. Attack mechanism:

There seems to be varying versions of this worm, due to the fact that the source code is readily available and can be modified to suite the hackers taste. I will cover the "worst case" variant of this worm. The Adore Worm, no relation to the Adore rootkit, will scan the Internet looking for hosts with ports 53, 111 and/or 515 open and listening. Once a target is found, the worm will then launch an attack at the noted vulnerability until it has compromised the host. If it detected port 53 open and vulnerable, it will use that attack to gain access. On the other hand, if it found port 515 vulnerable, it would launch a buffer overflow attack against the lpd port. Either way, the worm will gain access to the target host. Once the source has compromised the target, it will establish a connection to port 3879. Data is transferred (unknown what that is –commands?) between the source and target. Then the target will set up an HTTP session and (appears) downloads C source code, which is compiled and executed. The worm will then gather some system information and send out two emails with this information in them to a mailbox in China. The Adore Worm then adds the users "*ftp*" and "*anonymous*" to the */etc/ftpusers* file. The worm will then block the vulnerability that was exploited and will kill the *rpc.statd, rpc.rstatd*, and *lpd* processes, which will prevent these vulnerabilities from being exploited by others. Next, the worm will replace the *klogd* (kernel message logger) with a backdoor program. This backdoor will allow root shell access. Finally, the worm looks for new systems to compromise. The worm will generate random Class "B" IP addresses, scan them and check to see if there are any hosts that are vulnerable to the *rpc.statd, rpc.rstatd*, *lprng,* and/or *bind* vulnerabilities. If the worm

finds a host vulnerable, the worm will launch an attack against the known vulnerability to gain access to the system. Then the cycle will repeat itself.

6. Correlations:

Linux has several vulnerabilities that are concerned with ports 53 and 515. According to the CVE database, there are over 19 entries for the bind vulnerability alone. The *lprng* vulnerability (the only one currently) is a candidate CVE, CAN-2000-0917. The *bind* vulnerability has 19 entries, some of which are candidate CVEs. A few of the relevant CVE's are CAN-2001-0010, CVE-1999-0009, and CVE-1999-0833. Symantec also has a good write-up on the subject of the Adore Worm, along with one from SANS. Cliff Yago submitted the most informative bit of information I came across to SANS GIAC, with Matt Fearnow as the Handler on Duty. This is the best "article" (for lack of a better term) I have read concerning this worm. On May 04, 2001, www.Incidents.org listed port 53 as the #1 port of interest, with port 111 listed as #3 and port 515 being #4.

7. Evidence of active targeting:

This does not seem to be active targeting. Looks like the infected machine is 'doing its job' and scanning its randomly generated address block looking for any vulnerable hosts that will respond to it.

8. Severity:

Direction	Category	Value	Reasons
Attack	Critical	4	Looking for Linux machines (DNS, Print servers.)
	Lethality	5	Gains Root access and Possibly acquire password lists from infected hosts
Response	System	3	Numerous Hosts – unsure of system patches.
	Network	5	No replies from hosts or blocked by the firewall.
Severity = (4 + 5) – (3 + 5) = 1			

9. Defensive recommendation:

The defenses of this network seem to be good because no replies were sent to the source host. Either the firewall stopped the packets or the boxes are not running the requested services. The sites should ensure that they have the latest patches installed. If the site does not require any of the above-mentioned services, (RPC, DNS, or Printer support) these services should be disabled. In addition, the site administrator should monitor outbound traffic to see if their site is scanning other sites for the above-mentioned ports, if they are scanning other hosts, then this is a good indication that they are infected and need to clean their machines.

10. Multiple choice test question:

The Adore Worm attempts to propagate itself by what means?

a) As an attachment in e-mail

b) FTP'ing itself to other FTP servers
c) Scanning the Internet looking for hosts with known exploits
d) It doesn't – It's dormant

Answer (c)

ASSIGNMENT # 2

Describe the State of Intrusion Detection
A white paper on an Intrusion Detection Technology

Network Fuzzy Logic Attack Recognition Engine (NET-FLARE)

Today's Information Warrior has many tools designed to assist in the detection of unwanted personnel into the computer systems they are responsible for. The only drawback is that none of the tools currently available will alert the Information Warrior in real time. All of the tools provide excellent information; it is just that the information would be reviewed the day after it is produced, if that early. In addition, to compound the situation even worse, if you are responsible for multiple sensors, downloading and trying to correlate the information can take many man-hours. Thankfully, there is a tool that can be used, which will eliminate these problems, called "NET – FLARE."

NET – FLARE stands for Network Fuzzy Logic Attack Recognition Engine and was developed by the U.S. Air Force Research Laboratory under contract F30602-C-00-0044 to WetStone Technologies, Inc. The ultimate goal of NET – FLARE is to provide the Information Warrior the ability to process large and varied sources of information, provide flexible viewing and analyzing of the data that will result in efficient reporting of information to those who need it. NET-FLARE is still under development and is currently being tested in the field at Defense Information Systems Agency – Pacific Region (DISA-PAC), which monitors Department of Defense networks in the Pacific Region. For the purpose of this paper, DISA-PAC will be referred to as ' the testing facility'.

NET – FLARE achieves its goal by receiving streams of data from multiple sensors. NET – FLARE is designed and equipped to support data streams from various types of sensors, such as NIDS, JIDS, ASIM, or Real Secure, just to name a few. This will allow you to use your current combination of sensors and have the data fed directly into NET – FLARE for processing. The data is received via Secure Shell connections to ensure data integrity. Once NET– FLARE receives the data, the decision engine will check it against the user created rule set, or policy, to see if any alarms should be "sounded." The rules or policy that will be used can be created "on the fly" by the user. This is necessary because new threats appear daily, and the Information Warrior needs to be able to combat these new threats. If multiple sensors are used, NET – FLARE is able to take all incoming data and correlate any events between sensors to give the Information Warrior the "complete picture" of their network.

There are three separate component applications that makeup NET – FLARE. These components, designed to work together to achieve the overall goal, are the NET – FLARE Policy Editor, the NET – FLARE Decision Engine, and the NET – FLARE Visualization / Correlation Engine.

In the latest release of NET – FLARE, the NET – FLARE Policy Editor provides for the creation, editing, deletion, and exportation of situation and mission based decision policies. The NET – FLARE Decision Engine provides for the reading and processing of sensor data. The NET – FLARE Visualization / Correlation Engine provides for the viewing and analyzing of this data. Since NET – FLARE is still under development these capabilities will be further advanced and generalized to support even greater flexibility on the part the Information Warrior.

Figure (1-1) shows the relationship of the different components of the NET – FLARE system.

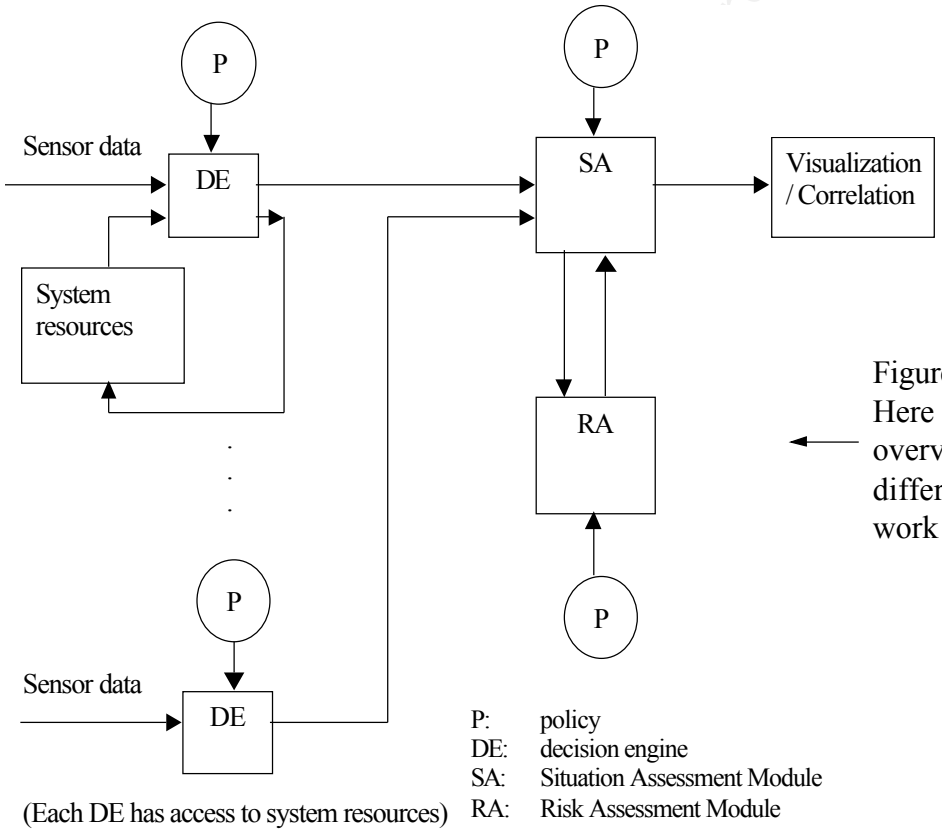

Figure (1-1)
Here is a basic overview of how the different components work together.

Figure (1-2) NET – FLARE Policy Editor

Figure (1-2) shows the initial screenshot of NET – FLARE's Policy Editor. The Policy Editor is not directly used in the operation of NET – FLARE, but it is needed and used to create, delete, edit, and export Policy files. There are no default settings associated with the Policy Editor, but currently, there are four policies that are contained within the Policy Editor. For ASIM compatibility, the policies are DEFAULT and THREATCON ALPHA. For JIDS compatibility, they are THREATCON JIDS and REDALERT-JIDS. Other default policies can be added in order to provide compatibility with other sensors.

The custom configuration of the policies via the Policy Editor is one of NET – FLARE's greatest strengths. This feature allows for complete customization for a specific task or problem at hand. Since the Information Warrior has the ability to have multiple policies with multiple rules, the creation of policies should be well thought out and examined before a policy is put into place.

In order to explain the Policy Editor, each section, by button, will be explained.

Edit Policy button is used after the policy that you would like to edit is selected, by using the drop down menu in the center of the Policy Editor window. Once you have selected the policy, click the Edit Policy button.

Delete Policy button is self-explanatory. To delete a policy, simply select the policy in the drop down menu and click "Delete Policy." Since this is a Windows based application, you will be prompted to confirm the selection.

Add Policy button is used to add a new policy. When you click the "Add Policy" button, you will be prompted to enter in a name for the new policy. Use the drop down box to select any default values from preexisting policies. If you choose to select a default value from a preexisting policy, the fields in the Edit section will be pre-populated with that policy's rules and classifications.

Export Policy button is used to export a policy to be used by the Decision Engine. In order for a policy to be used by the Decision Engine, the user must export that policy. This is accomplished in two easy steps, which are: (1) select a policy via the drop down box in the center of the Policy Editor window. (2) Once the correct policy is selected, click the "Export Policy" button. This will export the policy to the default location (C:\Program Files\WetStone Technologies\NET-FLARE\ nmarules\ammo.txt). This file is replaced every time a new policy or

an edited policy is exported. Keep in mind that only one policy exists in this folder at a time.

Exit button, another self-explaining title, is used to exit the Policy Editor.

Policies define both the decision rules as well as the interconnectivity of sensors and detectors. Remotely placed host and network based intrusion detection sensors, firewalls, and boundary devices feed real-time data to the NET-FLARE Decision Engine. The NET-FLARE Decision Engine supports multiple simultaneous sensor inputs from a variety of sensor types such as host, network, and border devices. Individual policies can also be defined for each sensor input. This is a major advantage for the Information Warrior that has to manage multiple sensors, especially if you want one sensor to look for one particular event and another one to look for something completely different.

Having the ability to create policies "on the fly" has proven to be invaluable to the testing facility. This feature has given us the ability to increase our response time ten-fold for new threats. From the time our site hears of a new threat that we should be looking for, to the time we have a new rule or policy in place looking for this threat, is within two minutes. In addition, because all of the sensors are feeding one central location, essentially all of the sensors would be updated simultaneously.

The next component that we will discuss is the Decision Engine. Figure (1-3) is a sample screen shot of the Decision Engine.

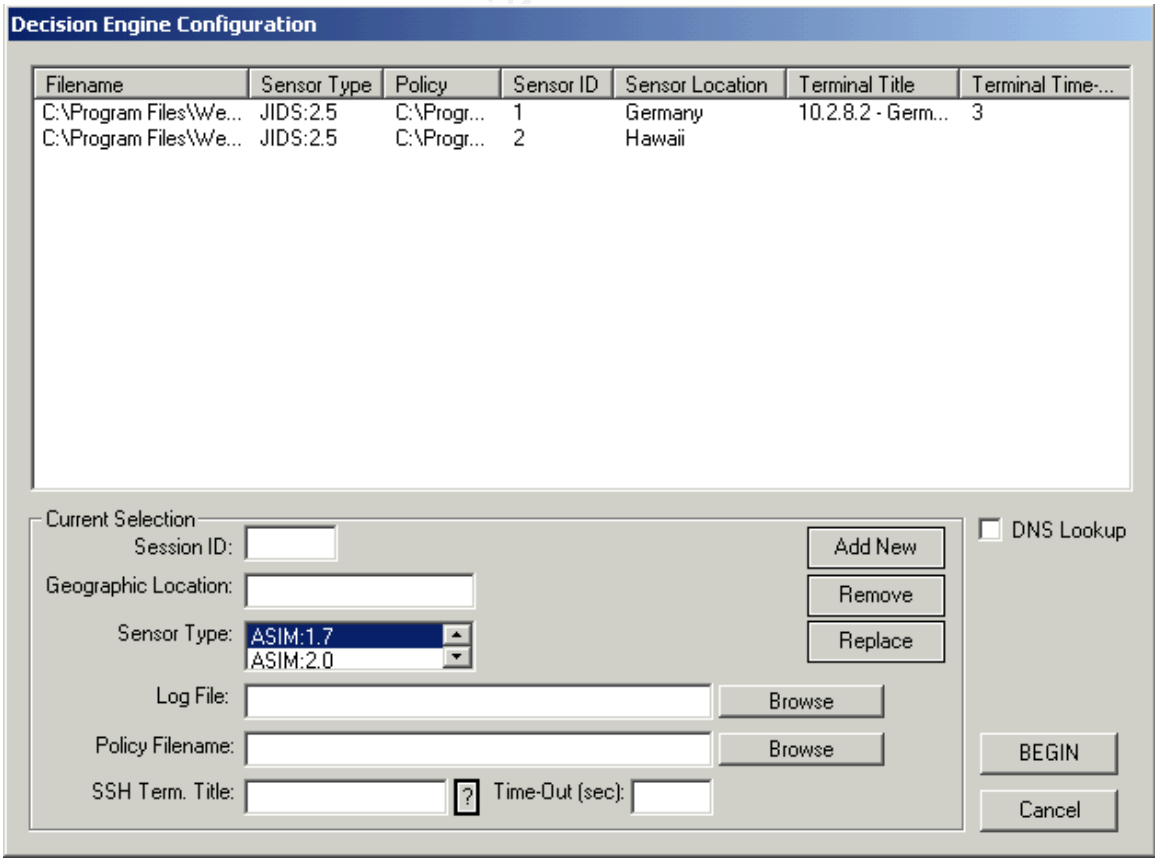

Figure (1-3) NET – FLARE's Decision Engine screen shot

The Decision Engine normalizes the data into a set of fuzzy values, which are compared against the policy, the appropriate rule or rules are fired, and the results are then transferred to the Visualization Engine. As you can see in the figure above, there is a block titled "SSH Term. Title." This is so that you can configure the SSH Terminal type for each individual sensor in order for NET – FLARE to monitor the "health" of the connection. If you are responsible for multiple sensors, this will prove to be invaluable. It will give the Information Warrior the ability to examine the "health" of all of his/her sensors with one look at the screen. If one of the connections is down, the Information Warrior will be able to restore the connection immediately.

The SSH Terminal Title feature was added at the request of the testing facility. This is due to remote sensors closing the secure shell connection after '*x*' minutes of inactivity. Since NET-FLARE receives it data from secure shell, the connection must remain open. This allows us the ability to monitor the status of the connection and reconnect if connection is lost. With the next release of NET-FLARE, there will be a button that the operator can push to re-establish the connection.

The NET-FLARE Decision Engine scales to support up to 64 real-time sensor feeds (single Pentium III ® 850 MHz processor). However, the Visualization Engine, which is covered next, can support up to 256 real-time Decision Engine feeds. Multi-processor system configurations are fully supported.

With the policy having been added and / or edited, and the data stream from the sensors are flowing into the Decision Engine, we now turn our attention to the Visualization / Correlation Engine. The data display has a highly user configurable interface allowing a user to view all alarms with selected data or a single alarm with all data. Analysis tools allow graphic configuration of events, the ability to produce reports and graphs, as well as storing and retrieving data for future analysis. This makes the perfect tool to use for real time detections and for further analysis of an event at a later date. Figure (1-4) is a screen shot of the Visualization / Correlation Engine (VCE) configuration window.

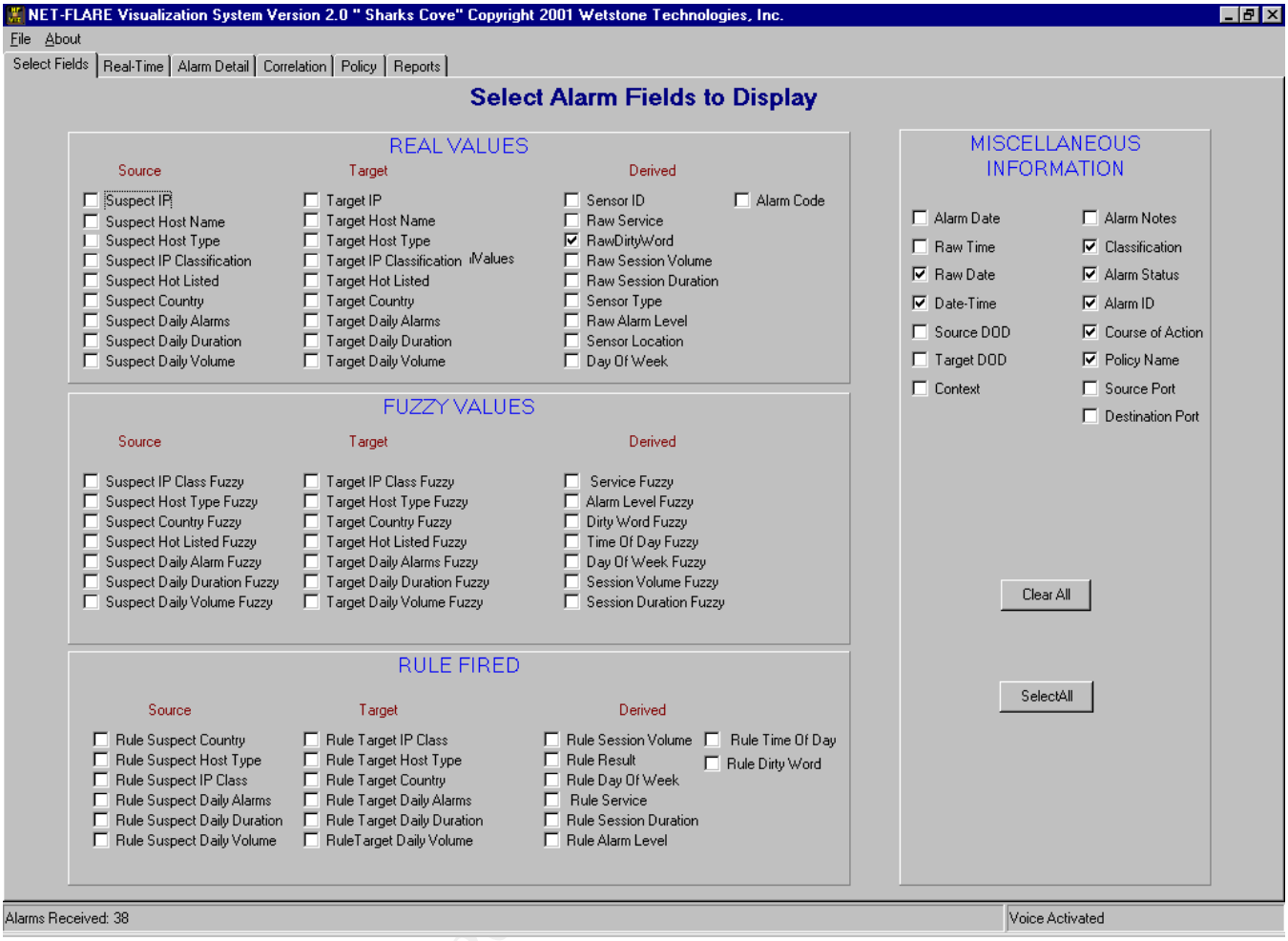

Figure (1-4) NET – FLARE Visualization System *Select Fields* Tab

As you can see from the screen shot above, the user can select what fields they would like to have displayed upon receiving a detect or alarm from a sensor. You will notice the selections of "Suspect Country…" and "Target Country…" because NET-FLARE includes several internal multi-dimensional matrices that convert IP address to Country name and will allow you to automatically track hot-listed and local IP activity.

Being able to look for "suspect countries" or "target countries" is another feature that was requested by the testing facility. This allows us to look for specific threat countries trying to connect to our networks. As an example: shortly after the incident with a US submarine and the Japanese fishing boat, and the US spy-plane and the Chinese fighter plane, we had to set rules or policies to look for these countries – knowing that someone would try to retaliate for these accidents.

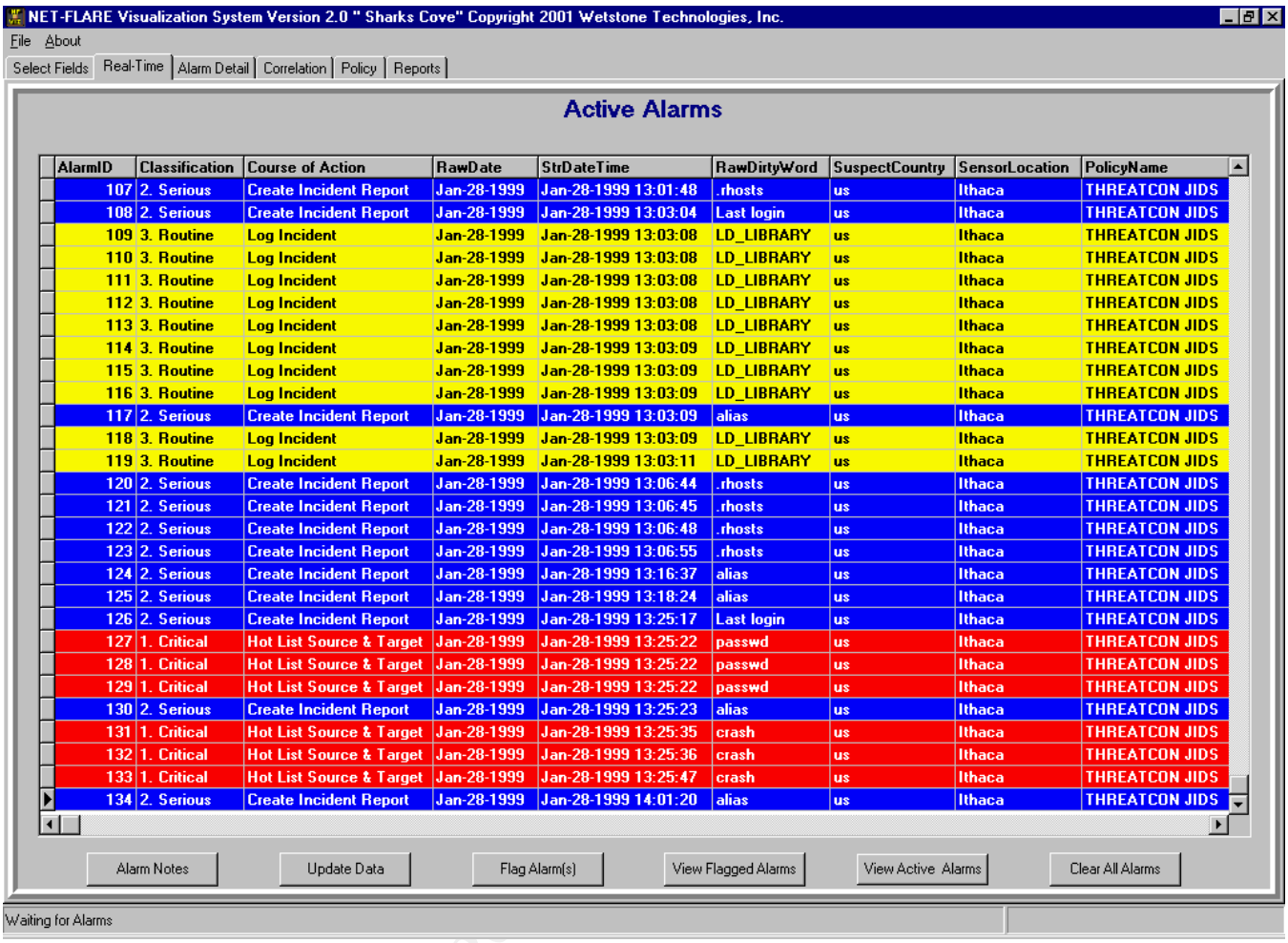

Figure (1-5) NET – FLARE Visualization System *Real-Time* Tab

The next tab to discuss is the "Real – Time" tab. The *Active Alarms* grid has been given the flexibility to be an effective analysis tool for each analyst's specific needs and tasks. Fields selected on the previous tab are displayed for each alarm. Alarms are displayed by *Alarm ID* and in ascending order by default. Alarms can be displayed in ascending order based on any field simply by clicking on that column's heading while holding down the Ctrl key, or descending order using the Shift key. Figure (1-5) shows what the "Real – Time" Tab looks like.

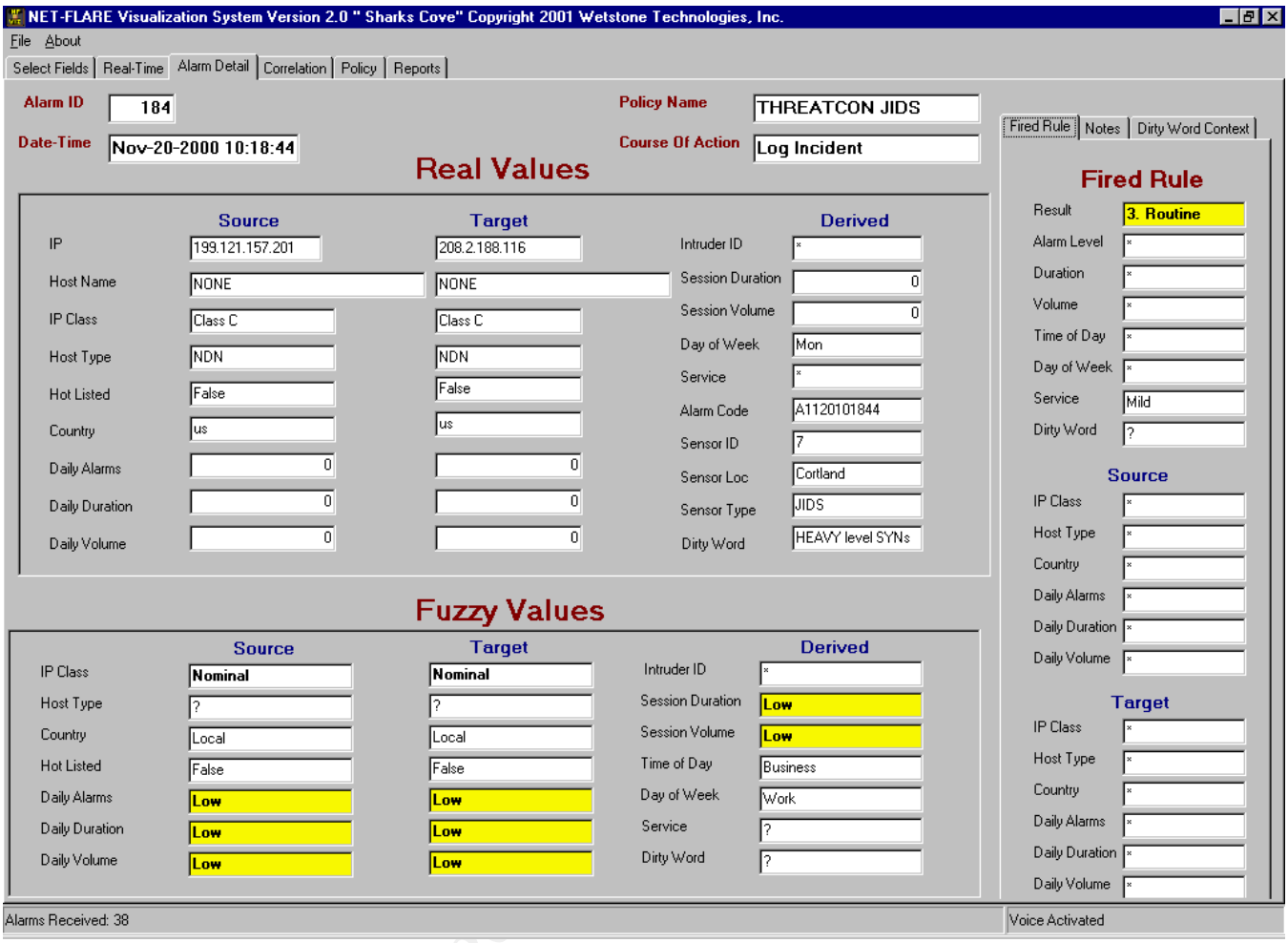

Figure (1-6) NET – FLARE Visualization System *Alarm Detail* Tab

The Alarm Detail tab, as shown in Figure (1-6), displays all information for the selected alarm. The data is organized similarly to the *Select Fields* tab by categories: *Real Values*, *Fuzzy Values*, and *Fired Rule*. The *Alarm Notes* information for the specific alarm is viewable from the *Notes* tab and editable by using the *Edit Notes* button. The full context of the eighty-character string is also available from the *Dirty Word Context* tab.

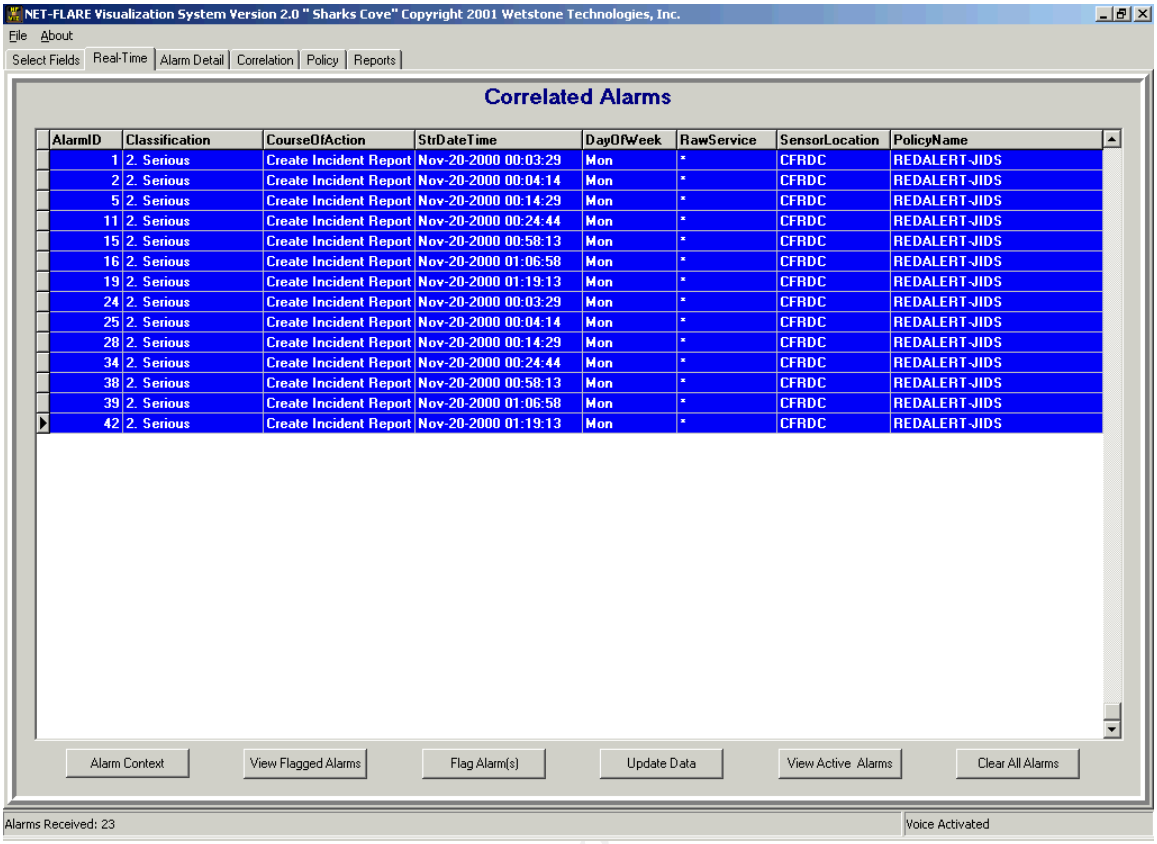

Figure (1-7) NET – FLARE Visualization System Correlated Alarms Tab

Correlation between sensors or events can be configured according to Service, or Port, in addition to Source, Target, and Source Country for analysis by selecting the appropriate tab. When alarms are correlated based upon a field - they can also be viewed as an isolated group when returning to the Real-Time tab.

Since the testing facility monitors multiple sensors over a large geographical region, the correlation feature of NET-FLARE has come in quite handy. This allows us to get a nice graphical display of related events instead of using shell commands and trying to parse through megabits of data each day. This gives us insight to potential problems, such as what is being targeted and by whom.

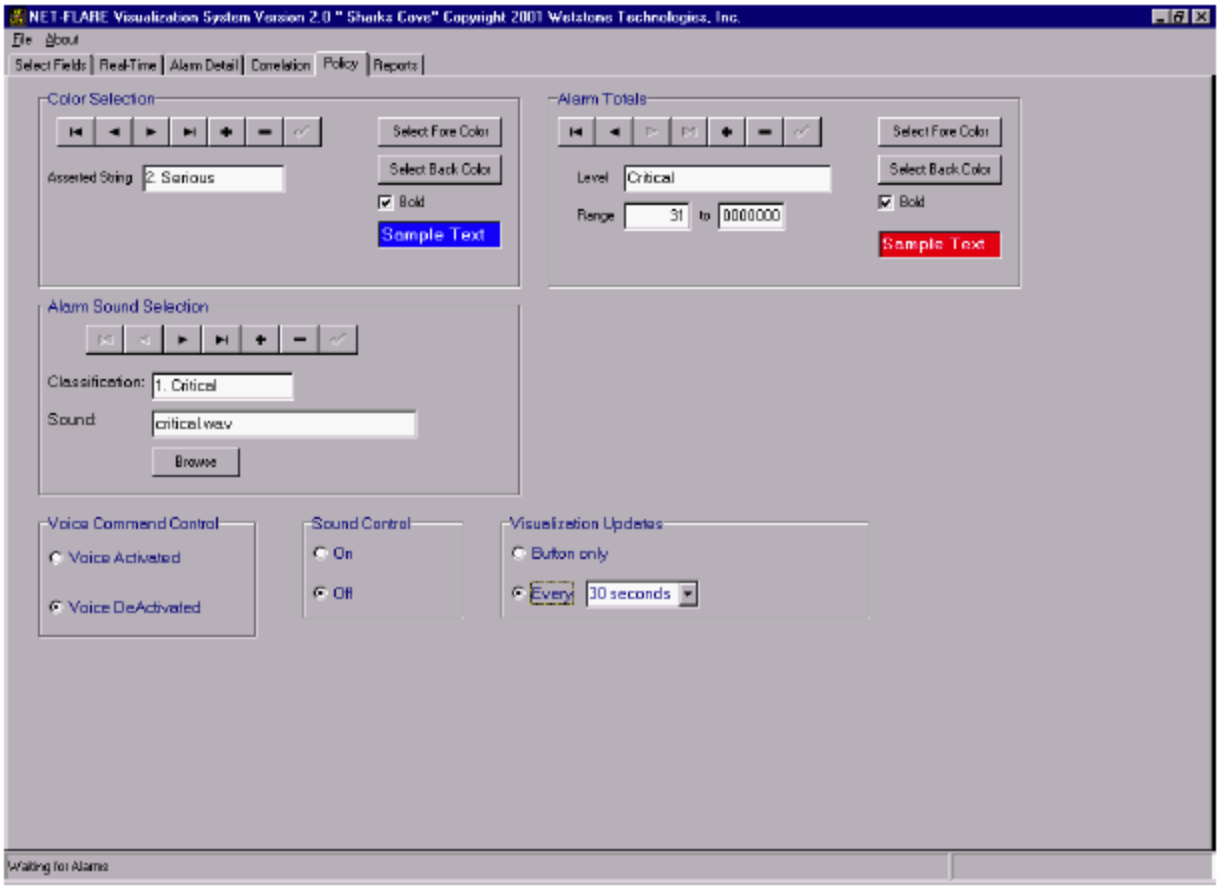

Figure (1-8) NET-FLARE Visualization System *Policy* Tab

This tab is where the user can configure and set various settings, such as: Voice Command Control, Sound Control and Visualization Updates. The Policy tab also contains format style information as well as the user preference controls. From this tab, you can configure the graphic features of the Visualization System. Alarm Color, Alarm Totals, and Alarm Sound Selection can be set or modified in this window also.

This allows the testing facility to tailor the visual display to our preferences. NET-FLARE also has the capability to us voice activation or Voice Command Control, to allow for keyboard less entry of tasks. This feature, however, is not implemented at the testing facility due to higher than normal levels of background noise and the lack of physical resources to support this feature.

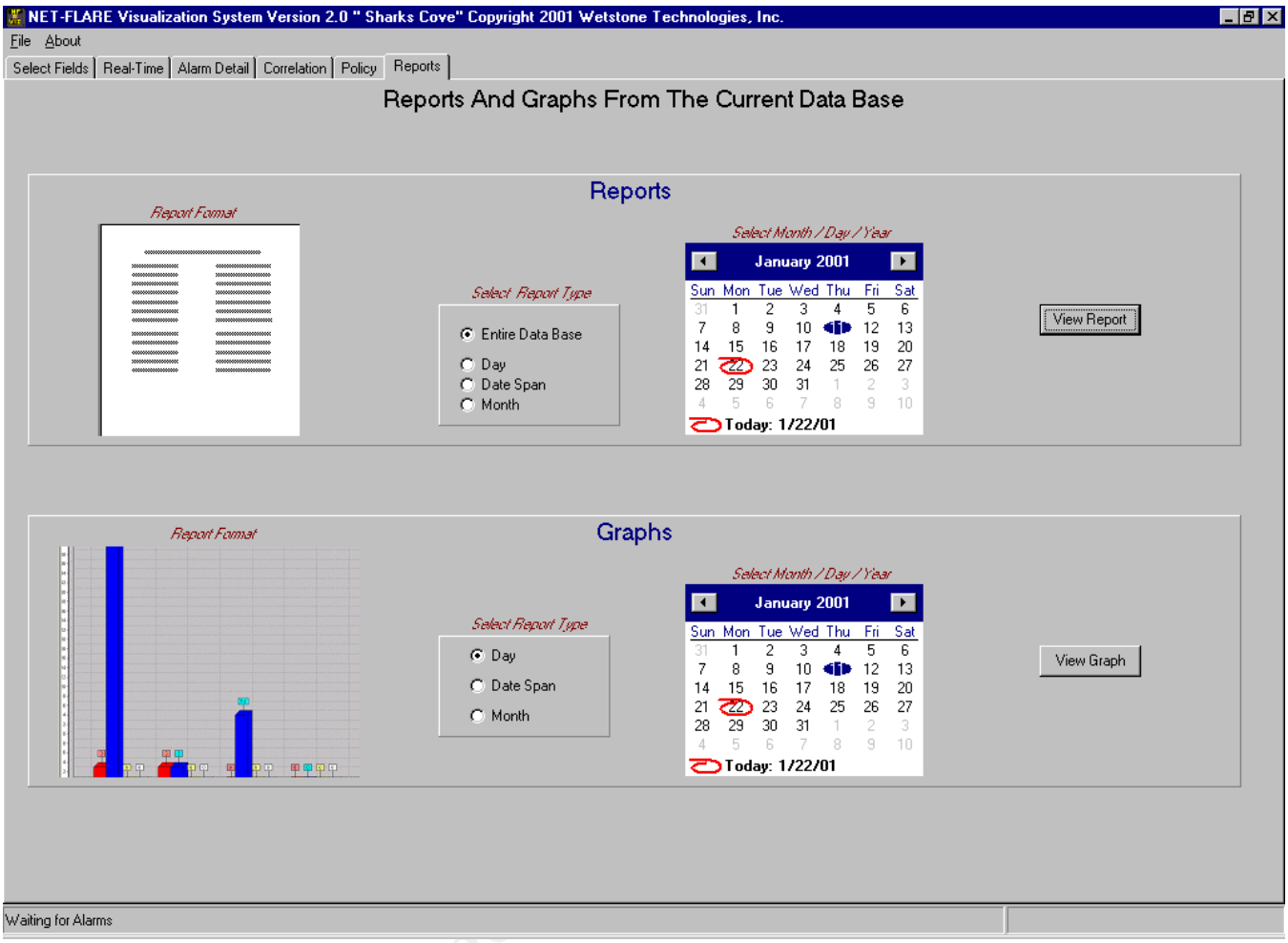

Figure (1-9) NET – FLARE Visualization System *Reports* Tab

Reports and graphs can be generated based upon the Entire Database, Day, Date Span, or Month. Graphs represent the alarms in a clustered column format by Classification: Critical, Serious, Routine or Clear. There are also options to print and save specific reports or graphs.

Figure (1-9) shows the configuration tab for the reports that NET – FLARE can produce while Figure (1-10) and Figure (1-11) show two sample output reports that can be produced by NET – FLARE.

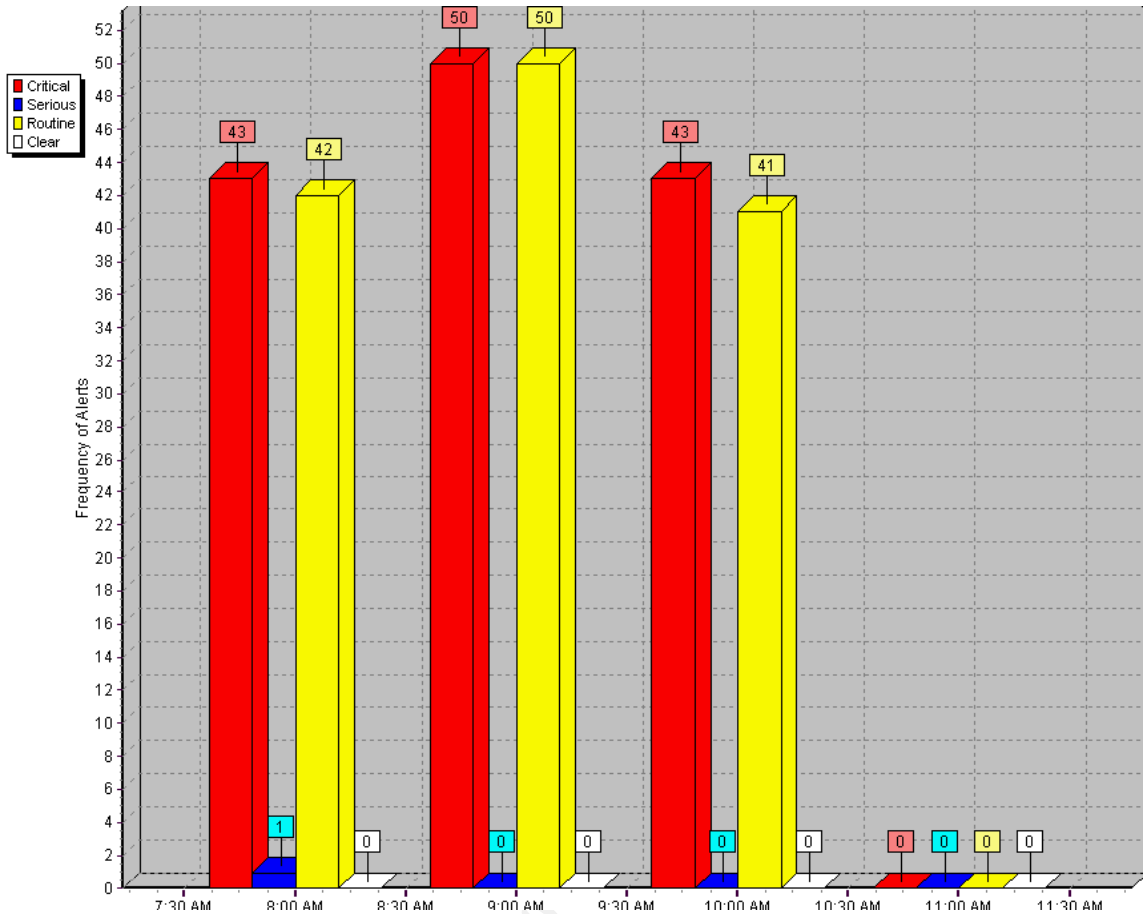

Figure (1-10) NET – FLARE sample report output – Day Graph

NET FLARE Report

Data Base Summary

Alarm Time	Classification	Course of Action	Policy Name	SENSOR ID	SENSOR Location	SENSOR Type	SUSPECT/TARGET	SUSPECT/TARGET IP Address	SUSPECT/TARGET Hot Listed	SUSPECT/TARGET Country
Nov-20-2000 00:03:29	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	199.121.159.150	False	us
							TARGET	209.10.169.58	False	us
Nov-20-2000 00:03:29	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	199.121.159.150	False	us
							TARGET	209.10.169.58	False	us
Nov-20-2000 00:04:14	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	199.121.159.150	False	us
							TARGET	209.10.78.210	False	us
Nov-20-2000 00:04:14	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	199.121.159.150	False	us
							TARGET	209.10.78.210	False	us
Nov-20-2000 00:09:14	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	163.251.13.91	False	us
							TARGET	206.39.68.135	False	us
Nov-20-2000 00:09:14	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	163.251.13.91	False	us
							TARGET	206.39.68.135	False	us
Nov-20-2000 00:09:44	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	204.34.2.89	False	us
							TARGET	207.14.58.228	False	us
Nov-20-2000 00:09:44	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	204.34.2.89	False	us
							TARGET	207.14.58.228	False	us
Nov-20-2000 00:14:29	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	199.121.159.150	False	us
							TARGET	159.120.51.25	False	us
Nov-20-2000 00:14:29	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	199.121.159.150	False	us
							TARGET	159.120.51.25	False	us
Nov-20-2000 00:15:14	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	204.34.141.2	False	us
							TARGET	192.215.32.111	False	us
Nov-20-2000 00:15:14	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	204.34.141.2	False	us
							TARGET	192.215.32.111	False	us
Nov-20-2000 00:17:44	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	204.34.2.89	False	us
							TARGET	207.14.58.228	False	us
Nov-20-2000 00:17:44	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	204.34.2.89	False	us
							TARGET	207.14.58.228	False	us
Nov-20-2000 00:20:59	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	204.34.141.2	False	us
							TARGET	205.188.132.67	False	Unknown
Nov-20-2000 00:20:59	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	204.34.141.2	False	us
							TARGET	205.188.132.67	False	Unknown
Nov-20-2000 00:22:29	1. Critical	Hot List Source	THREATCON JIDS	1	Germany	JIDS	SUSPECT	165.247.131.243	False	us
							TARGET	204.34.141.2	False	us
Nov-20-2000 00:22:29	2. Serious	Create Incident Report	REDALERT1-JIDS	2	Hawaii	JIDS	SUSPECT	165.247.131.243	False	us
							TARGET	204.34.141.2	False	us

Figure (1-11) NET – FLARE sample report output – Data Base Report

The next release of NET-FLARE will provide even better post-analysis of data. What this means is that we will be able to run past data through NET-FLARE to check for new threats. When the Information Warrior hears of a new threat or vulnerability, chances are it has been "in the wild" for months before the public hears about it. It is most likely that the networks we monitor have already been subjected to this new attack – months ago. However, since we did not know what to look for with this new threat, our networks were not 'protected' by the IDS.

We can now create rules for the new threat, take past data, and run it through NET-FLARE again looking for this new threat to see if an attack was launched. If one is detected, we could then go to the sensor or host itself to check if the attack was successful or not. This feature will allow us to verify the integrity of our networks and see if any hosts were compromised. If any hosts were, we will know exactly when the compromise took place.

Third-party plug-in support or tool integration is another outstanding quality of NET – FLARE. One of the key features designed into NET-FLARE is its flexibility and modular design. This design allows WetStone Technologies, Inc or other developers to integrate new features and functionality without modifying the core program. Additional flexibility has been added to NET-FLARE through the use of sensor plug-ins. This plug-in flexibility will enable NET – FLARE to provide support for many of the commercial and open source IDS sensors on the market today.

During the last few months, research was performed to determine the feasibility of integrating two new IDS sensor types into NET-FLARE's decision engine. The two sensors that were studied are: SNORT – which is an Open Source IDS system and SMART Watch – which is developed by WetStone Technologies, Inc. The results of the research for the two new IDS sensor plug-ins for NET – FLARE is very positive and integration into NET-FLARE should be a relatively simple process.

The following statement and technical requirements from WetStone Technologies, Inc.'s NET – FLARE Datasheet.

NET-FLARE provides a powerful set of tools for management and correlation of connected IA sensors. - Secure SSH connectivity - Continuous health monitoring - Built-in backup and management of IA data - Alarm flagging for expert analysis and control - Interactive notes recording for each alarm event - Simple sharing of IA sensor data with other analysts - Dynamic upgrade and sharing of decision policies - CD or network installation	NET-FLARE is supported on Windows 2000 ® and NT ® Recommended hardware configuration: - Windows 2000 or NT 4.x - 512 MB of memory - 60-120 GB of disk space - 1024 x 768 32 bit or higher resolution video - 19lo monitor (Visualization Engine) - Appropriate NIC interface - CDR (for backup and data sharing)

As a summary, NET – FLARE seems to be the only true "real time" intrusion detection tool on the market today. NET – FLARE has given the Information Warrior the ability to correlate the information from multiple sensors, even if they are different types of sensors. The ability to update the application is extremely easy due to the modular design. We have received updates via e-mail, replaced the two or three files and the new features were installed and working properly, all within thirty minutes. From the time of our initial request for new or improved features, to the time we received the e-mail with the files to replace, encompassed approximately one week. NET – FLARE will be one of the most relied upon tools in the Information Warriors arsenal against hackers and unwanted activity.

ASSIGNMENT # 3

"Analyze This" Scenario

GAIC Enterprises,

I would like to thank you for the continuing opportunity to provide your organization with information regarding your network security needs. As you are aware, my two associates, Lenny Zeltser and Marc Bayerkohler, have completed the security analysis of your network over the past six months. Their analysis is based on the Snort Data sets, which your staff provides to us.

I have taken the liberty to review their reports, and use them to build from, in order to provide you with an "as-complete-as-possible" picture of your network security posture. To paraphrase Marc Bayerkohler, the most recent analyst to review your network, 'looking at past data from your network will assist to better understand the present.'

The received data set contains three different formats (SnortS, SnortA, OOScheck), which is the output of alerts generated by the Snort IDS during this monitoring period. This period covers dates between November 24 thru January 19. Although this period is actually 57 days in length, only 52 days worth of data was collected. The lack of data being collected for certain days is attributed to events such as power failures and disc space problems. Therefore, our analysis of your network cannot be 100% complete, but it will give you a very good indication of the security posture of your network is at this time.

Since the data was provided in different formats, the analysis will be given on each format. We will start with previous data and then give current data. This will allow you to see how effective your corrective measures were, from previous recommendations.

Top Alert Destination Hosts

Hosts	*Previous # of Alerts*	*Current # of Alerts*	*Status*
MY.NET.253.105	47	8	Resolved
MY.NET.217.2	6	2	Resolved
MY.NET.253.41	4,387	296	Continue Monitoring
MY.NET.100.230	749	803	Continue Monitoring
MY.NET.201.222	N / A	37,609	Increase Monitoring
MY.NET.220.126	N / A	25,183	Increase Monitoring
MY.NET.225.234	N / A	9,314	Investigate Host
MY.NET.1.3	N / A	5,452	Increase Monitoring
MY.NET.1.4	N / A	5,408	Increase Monitoring

MY.NET.1.5	N / A	5,352	Increase Monitoring

Updates to Previous Alert Destination Hosts:

MY.NET.253.105: This host seems to be losing its popularity among the scanning sources. This period it only saw 8 scans against it. All of which look like "normal standard" scanning. Ports 0, 21, and 53 were the ports that were probed and are very common ports to look for. The only interesting probe seen was from 139.130.61.206 looking for port 109, which is used for POP2 mail. Unless you have a POP2 server running on this host, I would not worry about this.

MY.NET.217.2: This host is also losing its popularity among scanning sources. This monitoring period it only saw two scans against it. Port 21 and 53 were the target ports. As stated earlier, these are common ports to look for, and at this time, there is no cause for alarm.

MY.NET.253.41: This host seems to be continuing to act as a mail server with 279 of the 296 total alerts going to port 25 (SMTP mail). Of the 18 different sources going to this host, eight of them were tagged by the Watchlist 000222 NET-NCFC alert because they belong to The Computer Network Center Chinese Academy of Sciences (NET-NCFC). These sources belong to the 159.226.x.x network and have been noted in the last two reports. Since this traffic was reported earlier and is still continuing, I would have to assume that this is normal traffic and should be regarded as a false positive.

MY.NET.100.230: During this monitoring period, this host had 803 alerts with 748 of them targeting port 25 (SMTP mail) and 53 going to port 113 (Authentication). Over 98 % of alerts to port 25 and port 113 were generated by Watchlist 000222 NET-NCFC alert because they belong to the 159.226.x.x network, which is owned by The Computer Network Center Chinese Academy of Sciences (NET-NCFC). The amount of traffic to this host remained relatively constant, and appears to be one of the mail servers. These alerts can be regarded as false positives.

***NOTE: MY.NET.253.41** and **MY.NET.100.230** both seem to be mail servers with authorized clients in China. Since these hosts have been detected previously as mail servers and are still acting as mail servers, I can only assume that this is normal traffic and should be disregarded. However, with the increased tensions between USA and China (due to the US aircraft and China aircraft collision - April 01, 2001) I would recommend continuing to monitor these hosts for "questionable" activity. If one of your authorized mail clients in China becomes compromised, that client may be able to take advantage of the 'trust relationship' between your server and that client.*

New Alert Destination Hosts:

MY.NET.201.222: This was the # 1 destination host during this monitoring period. It had

37,609 alerts with 37,604 generating from 212.179.27.111, which is also the # 2 Alert Source. This IP is registered to Bezeq International, located in Israel, which is why it triggered the Watchlist 000220 IL-ISDNNET-990517 rule. Between the hours of 0200 and 0600 on January 04, is when these detects occurred. The source targeted only port 6688, which is most commonly used for MP3 music or Napster. MY.NET.201.222 seems to be acting as an MP3 or Napster Server. If this is common practice or normal operations, I would recommend that this host be moved to a non-productive leg of your network. Because the amount of bandwidth required while the MP3 is being streamed for listening, or during MP3 transfers, is relatively high, this will severely degrade your network performance. If this host is moved to a non-productive leg of the network, then the operational network performance will not be affected and you will still be able to provide this service. However, if this is not common practice or normal operations, then I would look into the possibilities that (1) a user within the network has set up a Napster server without proper permissions, or (2) this host may have been compromised and the individual responsible is using your host as a Napster Server. Your security personnel need to investigate this matter further.

MY.NET.220.126: This host had 25,183 alerts, of which 25,182 were triggered by the Watchlist 000220 IL-ISDNNET-990517 rule. The IP, 212.179.79.2, belongs to CREOSCITEX-SIFRA in Israel and was the source for these alerts. This source was targeting port 6699, which is also used for Napster, like port 6688 as mentioned above. Refer to the write-up for MY.NET.201.222 for recommendations concerning this activity.

MY.NET.225.234: This host had 9,314 alerts, of which, 9,309 were triggered by the Watchlist 000220 IL-ISDNNET-990517 rule with 212.179.79.2 being the culprit. This source, also belonging to CREOSCITEX-SIFRA in Israel, was noted using port 38318 and probing MY.NET.225.234's port 4967 for 43 minutes. At the time of this writing, port 4967 and 38318 are listed as unassigned by IANA (Internet Assigned Numbers Authority) and we are currently trying to determine the significance of these ports and what services or vulnerabilities may be associated with them. In the Alert log, the source port remained constant during the 43-minute event, which could mean one of two things. (1) An actual connection was made, in which case since the services are unknown, may or may not be normal traffic. (2) No connection was made just a lot of attempts, but with the source port remaining the same during the whole event may be an indication that the packets were crafted. Crafted packets means that the source IP is "up to no good" and should be watched carefully. We would recommend that you increase your monitoring of this host to look for malicious activity and / or possible compromise. Once these ports and the services or vulnerabilities have been identified, we will contact you with this information.

MY.NET.1.3: MY.NET.1.3 seems to be, due to the large number of hosts trying to connect to port 53, a DNS server. This host saw 13 different sources, and all but two were targeting port 53, the other two made one attempt each at port 21. The most significant alert came from 209.67.50.203, which belongs to *register.com*. This source accounted for 5,411 of the 5,452 alerts for this host. This source happens to be our #4 Alert Source and this event will be covered in the next section, *'Top Alert Source Hosts'*. The other scans directed at this host seem to be

your 'standard scans' and can be ignored.

MY.NET.1.4 & MY.NET.1.5: Both of these hosts seem to be DNS servers like MY.NET.1.3. MY.NET.1.4 had 5,408 alerts while MY.NET.1.5 had 5,352. Both hosts were probed by the same source, which is why they are grouped together. Like MY.NET.1.3, the most significant alerts for these hosts came from 209.67.50.203. This source accounted for 5,390 of the 5,408 alerts for MY.NET.1.4 and 5,331 of the 5,352 alerts for MY.NET.1.5. This source happens to be our #4 Alert Source and these events will be covered in the next section, *'Top Alert Source Hosts'*. The only other interesting probes to these hosts were targeting port 109, which is used for POP2 mail. Unless your mail service software has not been updated in the last few years, this is nothing to worry about. All mail servers should be running POP3 mail, which uses port 110.

Top Alert Source Hosts

Hosts	*Previous # of Alerts*	*Current # of Alerts*	*Status*
202.38.128.188	0	0	Resolved
MY.NET.253.12	0	4	Resolved
204.60.176.2	0	0	Resolved
159.226.45.3	1,558	69	Resolved - Verify
142.150.225.137	0	0	Resolved
212.179.79.2	N / A	48,786	Increase Monitoring
212.179.27.111	N / A	39,015	Continue Monitoring
211.34.40.1	N / A	17,604	Low Threat - Verify
209.67.50.203	N / A	16,123	Block Address
195.56.182.206	N / A	9,878	Continue Monitoring

Updates to Previous Alert Source Hosts:

202.38.128.18: Noted no further activity from this address.

MY.NET.253.12: This monitoring period showed only 4 alerts; three of them were this host connecting to port 515 (printer port) to a host outside the network. If this is allowed, there is no cause for alarm, however, if printing to an outside printer is not standard operating procedures, I would have your System Administrator look into this matter.

204.60.176.2: Noted no further activity from this address.

159.226.45.3: This was another monitoring period that has seen the amount of alerts decrease. This source seems to be using MY.NET.253.41 and MY.NET.253.42 as mail servers and using MY.NET.6.7 for authentication. This IP should be looked at to make sure it is allowed to access

these mail servers. If it is then this can be considered normal traffic and disregarded, however, if this IP is not allowed to access these mail servers then appropriate measures need to be taken (i.e., blocking IP).

142.150.225.137: Noted no further activity from this address.

New Alert Source Hosts:

212.179.79.2: This source had 48,786 alerts and belongs to CREOSCITEX-SIFRA in Israel, which looks like it may be an ISP. This source hit a total of 44 hosts in the MY.NET network. MY.NET.220.126 was hit the most by this source and accounted for 25,181 of the alerts. The source was targeting port 6699 on MY.NET.220.126, which would indicate that MY.NET.220.126 is acting like a Napster Server. As stated above, if this is common practice or normal operations, I would recommend that this host be moved to a non-productive leg of your network. Because the amount of bandwidth required while the MP3 is being streamed for listening, or during MP3 transfers, is relatively high, this will severely degrade your network performance. If this host is moved to a non-productive leg of the network, then the operational network performance will not be affected and you will still be able to provide this service. However, if this were not common practice or normal operations, then I would look into the possibilities that (1) a user within the network has set up a Napster server without proper permissions, or (2) this host may have been compromised and the individual responsible is using your host as a Napster Server. Your security personnel need to investigate this matter further.
MY.NET.225.234 accounted for 9,309 alerts from this source, which was triggered by the Watchlist 000220 IL-ISDNNET-990517 rule. As stated above, the source port of 38318 and destination port of 4967 are unassigned and currently no known services or vulnerabilities are associated with either. We will continue to research this matter and provide you with this information as it becomes available.
Port 4876 on MY.NET.228.214 and MY.NET.229.114 were probed 4,445 and 5,080 times respectively. This source used three different ports to conduct this probe, 31012, 31835 and 40227, all of which are listed as 'unassigned' by IANA. Since this source is using unassigned ports and initiating large scale scans or probes toward your network, I would increase the monitoring of this source. Everything may turn out to be normal traffic, but until that can be verified, I would error on the side of caution and increase monitoring of this source.

212.179.27.111: This source had 39,015 alerts with 37,604 going to MY.NET.201.222. Like MY.NET.220.126, this host looks like a Napster Server, which is why this source was going to port 6688 on it. As discussed above, you need to respond appropriately if in fact this is a Napster Server. The other host this source targeted was MY.NET.217.138. This host had port 41033 and port 41038 targeted. Both of these ports are listed as 'unassigned' by IANA and we are currently researching the services and / or vulnerabilities associated with each. We would recommend continuing to monitor this source until the intent of this traffic can be verified.

211.34.40.1: This was the #3 Alert source with 17,604 alerts credited to it. During its 21-minute scan on January 7, it targeted 17,604 different hosts. All hosts were probed on port 53 and with a source port of 53. This would lead me to believe that this source was actively looking for DNS servers on the MY.NET network. I would recommend that your staff make sure all of your DNS servers are up-to-date with the latest patches to protect against any known DNS vulnerabilities, and I would continue to monitor this IP for any further activity.

209.67.50.203: This source is the most disturbing and needs to be dealt with immediately. This source had 16,123 alerts and only targeted three hosts on the MY.NET network. They were MY.NET.1.3 (5,411 alerts), MY.NET.1.4 (5,390 alerts), and MY.NET.1.5 (5,331 alerts). All three hosts were targeted on port 53 and had a Denial of Service (DoS) launched against them. While researching this matter, we found a thread on one of the message boards with information concerning this host and this type of attack. To summarize the thread, it is recommended that a block be placed for this IP. More specifically, you should institute an ACL with udp packets from 209.67.50.203 be blocked and not allowed into the network. Information on how to go about setting this up is given on the message board (http://theorygroup.com/Archive/Unisog/2001/msg0058.html).

195.56.182.206: This source triggered the "SYN-FIN scan!" rule 9,878 times. During the 22-minute scan on January 10, this source scanned 9,878 different hosts on the MY.NET network. The source was targeting port 21 (ftp) and using port 21 as its source port. This activity is indicative of a source that is looking for an active FTP server and/or can be used to determine the host operating system. Since I do not have information indicating what this source received from this scan (his results of this reconnaissance scan), I can only recommend that you verify with your staff that all of your FTP servers have the latest patches installed. I would also recommend that you not allow anonymous ftp connections, if you currently do. Your staff should continue to monitor for this IP address, if this source obtained information about your network and what hosts are in fact FTP servers and/or their operating systems, this source may come back for a focused, targeted attack to those hosts.

Top Scan Destination Hosts

Hosts	*Previous # of Alerts*	*Current # of Alerts*	*Status*
MY.NET.101.89	253	165	All False Positives
MY.NET.70.234	52	11	Minor Target
MY.NET.179.78	461	5	Minor Target
MY.NET.97.73	6	11	Minor Target
MY.NET.223.86	N / A	48,288	Continue Monitoring
MY.NET.201.78	N / A	26,405	Continue Monitoring
MY.NET.202.94	N / A	9,302	False Positives
MY.NET.98.182	N / A	9,273	Continue Monitoring

MY.NET.203.98	N / A	7,148	Continue Monitoring

Updates to Previous Scan Destination Hosts:

MY.NET.101.89: This monitoring period only saw 165 alerts for this host, with the majority of them coming from MY.NET.1.3 and MY.NET.1.4. All of the alerts for this host seem to be normal DNS traffic. This host was also "scanned" by MY.NET.1.5 using port 123 (ntp) which would indicate that MY.NET.101.89 is also acting a time server.

MY.NET.70.234: During this monitoring period, MY.NET.70.234 was scanned a mere 11 times from 8 different sources. Of the 11 scans, 8 of them were targeted toward port 21, which would indicate that MY.NET.70.234 is running an ftp server, or some people think it is. If MY.NET.70.234 is in fact running an ftp server, your staff should ensure that the proper patches are in place. If you are not running an ftp server on this host, this can be considered as a false positive. The other scans were to port 109 (POP2) looking for a POP2 mail server, and one scan was looking for port 27374 which is known for the SubSeven Trojan.

MY.NET.179.78: This host was scanned 5 times by five different sources. The scans were rather typical, to port 21 (ftp) and to port 27374 (SubSeven Trojan). The interesting one to this host was coming from 131.161.49.140 attempting to go to port 22, which is used for Secure Shell connections. The unusual thing about it was the packet that was sent. The packet that was sent had certain "flags" that were set which would indicate that this packet was crafted. You should insure that only required hosts are allowed to connect to this host or disable this service all together if it is not needed.

MY.NET.97.73: 11 total scans were directed at this host with nine different sources. Eight of the scans were a typical scan of port 21 while two scans were going for port 27374 looking for a SubSeven Trojan. Unless this host is acting as an ftp server, I would not worry too much about these scans. If it is an ftp server, make sure the proper patches and security measures are in place.

New Scan Destination Hosts:

MY.NET.223.86: This host is our new # 1 scan destination host this monitoring period. This host had 48,288 scans from 10 different sources. 24.4.196.167 and 24.29.40.11 accounted for 99.96 % of the alerts to this host. Source 24.4.196.167 registered 29,528 alerts or scans to this host. This source is registered to the *@HOME Network* with an official name of "cc32281-a.etntwn1.nj.home.com." MY.NET.223.86 had ports targeted that ranged between port 4 and port 65,534 and seemed to choose the ports at random. The other major scanner of this host was 24.29.40.11, which registered a total of 18,744 probes or scans toward this host. This source belongs to the *EXCALIBUR Group* with an official name of "cm-24-29-40-11.nycap.rr.com." This source, like 24.4.196.167, seemed to be doing a major probe or scan of your network. Both of these sources should be monitored to see if they return to follow up on their reconnaissance.

MY.NET.201.78: This host had two interesting events associated with it. The first was a scan from 24.180.134.156, belonging to the *@HOME network* with the official name of "cc349491-a.hwrd1.md.home.com." This source had 26,368 scans toward MY.NET.201.78. Like other noted scans, this started out with port 3 and worked its way up to 65,526 using random ports along the way. This IP should be placed on the list of IPs to monitor. Depending on the reconnaissance efforts of this source, this IP may be back. The second event is quite disturbing, for a production network. This deals with the utility called, Gnotella. A description from the Gnotella web site explains what Gnotella can do,

> " Gnotella is a distributed real time search and file sharing program. Gnotella and other compatible programs form a peer-to-peer network over which you can share files you specify, search for, and download files that others in the network (referred to as the Gnutella Network) are sharing. Due to the nature of the network, the number of users, files, and size of the files available can vary dramatically and rapidly. Gnotella lets you share ANY type of file."

As you can see, this could be very dangerous if an unauthorized person was to gain access to your network via Gnotella and had access to ANY file. This host, MY.NET.201.78 tried to connect to 220 other hosts to see if they were listening on port 6346, which is the default port for Gnotella. MY.NET.201.78 had seven other sources trying to contact it on port 6346. This would lead me to believe that this host, MY.NET.201.78 is in fact set up as a Gnotella server. This should be looked into immediately due to the potential serious security breaches involved. If a user did not set up this service, your staff may want to look for a possible compromise of MY.NET.201.78 and take appropriate actions.

MY.NET.202.94: This host ranked as # 3 Scan destination with 9,302 alerts. Two major events were noted on this host, one in which MY.NET.202.94 was the target and one where it was the source. The first noted event had 216.99.200.242 targeting MY.NET.202.94 on December 30 21:05 thru December 31 01:10. The initial look at this event had me concerned because during the scan, 9,283 ports were scanned - 6,664 used the TCP protocol while the remaining 2,619 used UDP protocol. After investigating the event farther, I learned that 216.99.200.242 belongs to Securedesign.net (www.securedesign.net), which provides security scans for users that request it. The basic scan will only scan the TCP ports and display the results on screen. The 'full' scan will not only scan your TCP ports, but will also scan your UDP ports. The results however, cannot be displayed on screen because they need time to process the results of the scan, so they will e-mail you your results. The scan logs indicate that the user at MY.NET.202.94 requested a full scan be done on the machine. During the next monitoring period, could you please include the results from this scan when you send us the Snort data sets, this will help us correlate questionable events. The second event noted has MY.NET.202.94 as the actual source of the scan. MY.NET.202.94 scanned approximately 8 hosts in the 207.46.204.xxx network. The curious thing about the scan is that the source used port 9000, targeted port 9000 and used UDP protocol. The 'normal' services associated with port 9000 use TCP as the protocol, such as Alta Vista Web Server / Search Engine installed with a default port of 9000 along with IBM Websphere's Administration Server, also set to port 9000 by default. After researching this event further, I have concluded that MY.NET.202.94 is participating in on-line gaming. The IP address of 207.46.204.xxx belongs to Microsoft, which has an on-line game called Asheron's Call, and runs

on port 9000 and 9004. Both of these ports are consistent with the traffic seen. On-line gaming would explain the 2-hour connection times seen during the three days of traffic. As with the Napster Server issue stated earlier in this paper, if this is common practice and allowed – this is a false positive. I would recommend moving this host off the production leg of the network so it will not degrade network performance. If this is not allowed in the work place, a simple solution would be to block the required ports and not allow that traffic in or out of the network. (ports required for this game can be located at http://support.microsoft.com/support/kb/articles/q236/4/30.asp).

MY.NET.98.182: This host ranked # 4 of the Scan hosts with 9,273 alerts. Between 11:34 and 12:08 on December 28, MY.NET.98.182 recorded 9,262 alerts all originating from 66.20.207.21, which is registered to *BellSouth* with the official name of "adsl-20-207-21.mia.bellsouth.net." The source used random ports between port 1 and port 9144. Because of the randomness of the ports scanned and the number of ports that were scanned, seems to lead to the conclusion that this was an automated scan. A likely tool that was used would be Nmap. As John Green, of the US Naval Surface Warfare Center, described the capabilities of Nmap, he concludes, "The intelligence that can be garnered by using Nmap is extensive. It provides all the information that is needed for a well-informed, full-fledged, precisely targeted assault on a network. Such an attack would have a high probability of success, and would likely go unnoticed by organizations that lack intrusion detection capabilities." As you can see, this tool is very useful to the hacker community. This IP should continue to be monitored to see if this source comes back for more reconnaissance efforts or to launch an actual attack. Other traffic to this host consisted of normal scans to port 21 looking for an ftp server and to port 12345 looking for a Netbios Trojan. Security precautions should already be in place to defend against these two types of attack.

MY.NET.203.98: This host saw scans from 11 different sources with 7,148 alerts being triggered. Most of the scans were to port 21 for ftp while one was going to port 109 for the POP2 mail server. The main scan took place on December 6 at 06:32 until 06:42 by 24.180.134.156, (cc349491-a.hwrd1.md.home.com) owned by the *@HOME network*. For the 10 minutes of the scan, the source scanned 7,136 ports ranging from port 15 thru port 65,535 - picking ports at random. As stated above, because of the number of ports scanned and the amount of time it took, indicates this is an automated script or application like Nmap. Continue to monitor this IP for future traffic.

Top Scan Source Hosts

Hosts	*Previous # of Alerts*	*Current # of Alerts*	*Status*
24.2.169.101	0	0	Low Threat
202.235.50.12	0	0	Low Threat
208.220.120.13	0	0	Low Threat

24.13.87.239	0	0	Low Threat
202.38.128.188	0	0	Low Threat
MY.NET.213.186	N / A	50,252	On-Line gaming
MY.NET.100.230	N / A	49,182	False Positives
MY.NET.217.94	N / A	33,734	On-Line gaming
24.180.134.156	N / A	33,502	Increase Monitoring
MY.NET.98.200	N / A	32,406	Possible Compromise

Updates to Previous Scan Source Hosts:

None of the Scan sources from the previous monitoring period showed up in any of the scan logs. This would indicate, as my previous analyst noted, one of two things. Because no further traffic is seen from any of the host that they did not gather any useful information and are looking for other targets, or (2) once they finished the reconnaissance on your network they discarded the compromised host they were using to launch the reconnaissance effort. These hosts can be considered a very low threat.

New Scan Source Hosts:

MY.NET.213.186: Ranked # 1 of our Scan Sources with 50,252 alerts connecting with 3,070 different hosts. This source was using port 28800 UDP for the connections, which as it turns out, is used for the MS Gaming Zone. This means that someone on the network is accessing the MS Game server and playing games. This can seriously degrade your network performance. If this practice is allowed, I would recommend that this machine be moved to a non-production leg of the network so the effects of playing the games will not have any affect on the rest of the network.

MY.NET.100.230: This host received 49,182 alerts during this period. All of which seem to be false positives. This host is acting as a heavily loaded DNS server, a mail server/client and an authentication server/client. MY.NET.100.230 had 41,737 alerts concerning port 53 for DNS queries to 7,071 hosts. The top three DNS hosts that connected with MY.NET.100.230 were 198.41.0.4 (1,235 alerts), 198.41.3.38 (682 alerts) and 198.41.3.101 (514 alerts) which are "*a.root-servers.net*," "*a.gtld-servers.net*," and "*g.gtld-servers.net*" respectively. All three of these, and others noted in the scan logs, are owned by *VeriSign Global Registry Services*. During this period, MY.NET.100.230 connected with 1,116 hosts on port 25, which is used for electronic mail (e-mail). Of the total 6,305 alerts using port 25 with this host, 233 alerts came from 199.75.44.25, which belongs to *SURAnet (Southeastern Universities Research Association Network)*. The other two top alerts were from 165.251.8.79 and 165.251.8.124, both having 98 alerts each. 165.251.8.xxx network belong to *FXnet* with a domain registration of '*mail.com*'.
This looks as if MY.NET.100.230 is acting like a mail server to the MY.NET network and as a mail client to the external servers. MY.NET.100.230 is using 204.160.241.38 as its primary authentication server. This combination had 59 of the 1,130 total alerts on port 113. Again, all traffic to or from this host looks like normal traffic and is no cause for alarm.

MY.NET.217.94: This was the # 3 source host with 33,734 alerts. The two most significant events for this host involve on-line game playing. MY.NET.217.94 was noted as scanning over 2,000 (2,105 to be exact) hosts looking for a reply from port 7778. This port, the server query ping port, is used to ping hosts in order to find hosts that are servers in the MSN Gaming Zone (www.zone.com). Microsoft has a knowledgebase article on these ports located at: http://support.microsoft.com/support/kb/articles/Q159/0/31.ASP. Unreal Tournament and Deathmatch are just two of the many games that are available through MSN Gaming Zone and use port 7778 to query the servers. The other noted event also deals with on-line game servers, this time the servers are located in Italy. The 151.23.31.xxx network had four hosts connecting with MY.NET.217.94 during the days of January 8 and 9, numerous times throughout both days. The host IP's are 151.23.31.21, 22, 23, and 27. The official names of the hosts are: 151.23.31.21= nt2.gamearena.it, 151.23.31.22=nt3.gamearena.it, 151.23.31.23=nt4.gamearena.it, and 151.23.31.27=linux4.gamearena.it. The traffic shows MY.NET.217.94 as both a source of the scans and as a destination with the four above-mentioned IPs. This may be an indication that this host is both a client and a server of on-line games. This activity should be looked into further due to possible degradation of network resources from game play.

24.180.134.156: This host ranked # 4 with 33,502 alerts going to only two hosts in the MY.NET network, MY.NET.201.78 and MY.NET.203.98. MY.NET.201.78 took most of the abuse with 26,368 alerts during three different sessions on December 6. This source scanned 21,257 ports on MY.NET.201.78. The duration was rather quick for the scans and the amount of ports was large and random, which would lead me to believe this was an automated process, possibly like Nmap. The same holds true for MY.NET.203.98; this looks like an automated process. MY.NET.203.98 was only scanned 7,134 times on 7,125 different ports. Since these two hosts were scanned so thoroughly, (MY.NET.201.78 more than MY.NET.203.98) I would have to conclude that this was a more focused, targeted reconnaissance effort. With over 30,000 hosts to choose from, they only picked these two and scanned thousands of ports on each. Looks as if they may have scanned the entire network (or part of it) in the past looking for hosts that were "alive" and now have come back to do a more focused reconnaissance effort to determine exactly what type of host they are dealing with. This source should be watched carefully in the future and these two hosts should be inspected to insure they have the latest security patches installed.

MY.NET.98.200: This host is the last on the list of the top 5 scan sources, but this one is also the most disturbing of them all. This source scanned 10,463 hosts and set off 32,406 alerts during this monitoring period. Two major events caused the alerts for this source; the first deals with port 6112 on both the source and the destination hosts. This is the port that BattleNet and / or Blizzard Games are played on (including Diablo, Warcraft, Starcraft, just to name a few). Only 249 alerts were attributed to this event and involved 175 destination hosts during this one-hour event on December 25. This is non-malicious traffic and would be no cause for alarm. As stated previously, if on-line gaming is allowed on your network, no further action needs to be taken. Network performance should be monitored to insure the gaming is not degrading the system, if it does; your staff needs to take appropriate actions to correct the problem. The second event is both quite large and troublesome. This event involved 10,288 hosts and set off 32,153 alerts during its three sessions on December 28. The port that MY.NET.98.200 used during the whole

event was port 9753 and tried to connect to various ports on the target hosts that ranged from port 9001 thru 9785. The interesting thing is that the ports that MY.NET.98.200 was trying to connect to incremented up by 16 each time (i.e., 9001, 9017, 9033, 9049, up thru 9785). Some of the ports that were targeted do have legitimate uses and services associated with them, but the majority does not. Trying to single out one service as the target service does not make sense in this instance, due to the large number of ports 'unaccounted' for. I am currently investigating this event and will contact you with further information regarding this, as it becomes available. In the meantime, I would increase monitoring, if not remove, this host from the network. Your staff should take a look at this host and see if any unknown services are running on it. This host may have been compromised. The reason for this statement is that all of the IP addresses that this host is trying to reach using port 9753, are located in Korea. Unless you have over 10,000 clients in Korea, I would be suspicious and consider this malicious traffic. In addition, during normal connections, or attempts, the source port should increment up by one. The fact that the source port on MY.NET.98.200 remained the same while contacting over 10,000 hosts just increases my suspicions.

Scan Sources from MY.NET network

During the analysis process, I looked for scans that are coming from hosts within the MY.NET network. There are a few reasons for this type of activity, such as, the host is the security manager's workstations and he/she is performing a routine scan to look for vulnerabilities within the network in order to take appropriate actions. The traffic could be normal, non-malicious traffic or it could indicate that the system has been compromised and being used to scan your network, or others, looking for vulnerabilities. The table below shows the top five hosts in the MY.NET network that were performing such scans.

My.NET Host	*# of Scan Records*
MY.NET.213.186	50,252
MY.NET.100.230	49,182
MY.NET.217.94	33,734
MY.NET.98.200	32,406
MY.NET.253.24	30,567

MY.NET.213.186, MY.NET.100.230, MY.NET.217.94, and **MY.NET.98.200** have all been covered in the previous section, so they will not be covered here. Please refer to the above section for information regarding these hosts.

MY.NET.253.24: This host ranked # 5 as a top-scanning host from the MY.NET network with 30,567 records. All of the traffic noted with this host is using port 25 (SMTP or mail) and a few using port 113 (authentication). A total of 1,260 different hosts were connected with, each averaging 24 connects during this monitoring period. After investigating the destination hosts, I

have concluded that this is normal traffic since the destination hosts all seem to be mail servers, the majority of them belonging to *FXnet*. This seems to be false positives concerning this host.

ASF Servers and Clients

During the last monitoring period, it was noted that your network is using the AFS distributed file system. It is still alarming snort, and you may want to fine-tune the rules in snort to reduce the amount of false positives from this activity. It looks as if you have changed your servers. MY.NET.1.13 was noted as being a vlserver for the network – that host was not seen using ports 7000 - 7007, however, MY.NET.140.21 was noted using port 7001 and set off 11,751 alerts. It looks as if you have configured MY.NET.140.21 as the new vlserver.

Summary

The below table shows the top five hosts / sources that have been mentioned in the preceding paper. These hosts / sources are based on the current snort data that has been provided to us during this monitoring period.

Alert Host	*Alert Source*	*Scan Host*	*Scan Source*	*MY.NET Scan Sources*
MY.NET.201.222	212.179.79.2	MY.NET.223.86	MY.NET.213.186	MY.NET.213.186
MY.NET.220.126	212.179.27.111	MY.NET.201.78	MY.NET.100.230	MY.NET.100.230
MY.NET.225.234	211.34.40.1	MY.NET.202.94	MY.NET.217.94	MY.NET.217.94
MY.NET.1.3	209.67.50.203	MY.NET.98.182	24.180.134.156	MY.NET.98.200
MY.NET.1.4	195.56.182.206	MY.NET.203.98	MY.NET.98.200	MY.NET.253.24

The host that needs immediate attention is MY.NET.98.200. This host is giving indications of a compromise. The odds of it belonging to or being used by someone with 'good intentions' are not high. The other area of concern is the amount of on-line game playing that is going on in your network. With this type of traffic on the network, the network performance is highly degraded. Poor network performance may also be attributed to the fact that you have a few Napster clients / servers and one Gnotella client / server. If these services are allowed on your network, then this is not an issue. I would also recommend that these services be moved to a non-production leg of your network as to not to interfere with actual production work (network performance wise).

Only one source was noted performing large scale scans (covering 1,000's of ports). This IP should be monitored carefully. Since this source targeted only two machines on your network, I would draw the conclusion that this may be step two in the attack process. The first step was to determine what hosts were 'alive' and which ones looked interesting. Once the hosts were determined, then the "major" reconnaissance effort takes place to determine what services and or vulnerabilities that host has (this is what was done here). Then the actual attack takes place, this attack may take place from a different IP since the attacker probably knows you will be looking for his last IP. This is why it is very important that your staff verify all security patches are installed. Although only one major scan was detected this monitoring period, your staff should continue to monitor your network.

ASSIGNMENT # 3a

"Analyze This" Scenario – The Process

Being very new to the Intrusion Detection Analysis world, and having limited Unix/Linux knowledge, this proved to be very challenging for me. The first step was to download the data, and "prep" it for analysis. The first thing I did was to limit the number of files I was working with so I put files together using the 'cat' command (I am working on Linux Red Hat 6.2).
I used " cat SnortA1* >> snort1", "cat SnortA2* >> snort2", …etc. until I was working with only five files. Then I put each of the files into the vi editor to help 'format' the data so that I can use some *grep* and *awk* commands to pull the information out.
The initial line looks something like this:

12/04-01:40:55.943341 [**] WinGate 1080 Attempt [**] 212.62.53.34:1718 -> MY.NET.204.106:1080
12/04-01:42:13.195391 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.33.254:1731 -> MY.NET.223.58:4571

After they come out of the vi editor, they will look something like this:

12/04-01:40:55.943341 **&** WinGate 1080 Attempt **&** 212.62.53.34:1718 **&** MY.NET.204.106:1080
12/04-01:42:13.195391 **&** Watchlist 000220 IL-ISDNNET-990517 **&** 212.179.33.254:1731 **&** MY.NET.223.58:4571

After all five files were 'formatted', I sat down and wrote a little script to help get the foundation of the data needed. This is the script that I used on the Alert files looking for the Alert Hosts:

```
#!/bin/bash
###For use with the Alert Files###

# This will show the source address and the destination port of the
specified target that was attacked or probed.

fgrep -h $1: snort* | awk -F"&" '{print $3, $4}' | awk -F":" '{print $1,
$3}' | grep -v $1 | sort | uniq -c | sort | awk '{printf ("%16s \tto port
%d\t %d times\n", $2, $3, $1)}' >> $1src-prt

cat $1src-prt | awk '{print $1}' | sort | uniq > listofips
echo "   " >> $1src-prt
cat listofips | wc -l | awk '{printf ("Total Sources = %d\n", $1)}' >>
$1src-prt
echo "   " >> $1src-prt
fgrep -h $1: snort* | awk -F"&" '{print $4}' | grep $1: | awk -F":" '{print
$1}' | uniq -c | awk '{printf ("Total alerts for %16s    is %d \n", $2,
```

```
$1)}' >> $1src-prt

LISTOFIPS=`cat listofips`
for IP in $LISTOFIPS
do
##let you know the date and hour, the port used, and how many times that
day/hour
echo "   " >> $1src-prt
echo "    Dates        Port used     How many times from $IP " >> $1src-prt
echo "   " >> $1src-prt

# find what dates the probe or attack took place
fgrep -h $IP: snort* | fgrep $1: | awk -F"&" '{print $1, $4}' | sort | awk -
F":" '{print $1, $4}' | sort | uniq -c | awk '{printf ("%10s \t to port %d
\t %d times\n", $2, $3, $1)}' >> $1src-prt
echo "   " >> $1src-prt
echo "Results of nslookup: " >> $1src-prt
nslookup $IP >> $1src-prt
echo "   " >> $1src-prt
echo "******************************" >> $1src-prt
done
```
rm listofips

The same script was used to find the sources of the Alert files, just had to change the columns that were pulled in the awk commands.
The scan files were handled the same way, sent to the vi editor, reformatted and then the script was run on the files.
This gave me the foundation of the information and then it was just issuing standard 'grep' commands to get more of the details of specific events that I wanted to look at.
Once I had the starting information, I went to the website and looked at previous submissions. I chose Lenny Zeltser and Marc Bayerkohler's papers because they used the same approach that I was thinking about. Both paper received "Honors" so I know they did it right. Marc's paper built upon Lenny's and it seemed to work out and made sense. I just followed suit.

References for Assignments

Previous Submitted Assignments:
http://www.sans.org/y2k/practical/Lenny_Zeltser.htm
http://www.sans.org/y2k/practical/Marc_Bayerkohler_GCIA.html

SANS website and other content from SANS:
http://www.sans.org
http://www.sans.org/y2k/0102stutzman.htm
http://www.sans.org/y2K/042500-2300.htm
http://www.sans.org/newlook/resources/IDFAQ/blocking.htm

Incidents.org Website:
www.incidents.org
http://www.incidents.org/cid/query/top_10port_7.php

Search Engines:
http://www.arin.net
http://www.google.com
http://www.ripe.net
http://cve.mitre.org

Snort Website:
http://www.snort.org

Message Boards:
http://theorygroup.com/Archive/Unisog/2001/msg0058.html
http://lists.gnac.net/firewalls/mhonarc/firewalls.199907/msg00772.html

Miscellaneous Sources on the Web:
Whitehats IDS
http://www.whitehats.com/ids/
Microsoft
http://support.microsoft.com/support/kb/articles/Q159/0/31.ASP
Attrition.org
http://www.attrition.org/security/advisory/nipc/nipc-024.ringzero_trojan
CKnow.com
http://www.cknow.com/cknewsletter/0311.htm#ringzero