Global Information Assurance Certification Paper

David Hed
GIAC/GCIA Certification Practical

SANS 2001 Baltimore (International Attendee)

(picture blatantly stolen from the panorama view of Baltimore from their Touristpage in hope of showing that Baltimore was a beautiful city)

Information/Disclaimer

Some IP's are left unsanitised, no ip has been altered if unobfuscated. MY.NET has in some cases been changed to 10.0. Sometimes the attacker is named "he" that is somewhat intentional based on the probability of gender. No electrons where harm ed in the capture of the packets. There is a separate appendix with the information of the top alert hosts.

Assignment 1

Detect 1

BIND Exploits still popular to search for

1. Source of Trace.

Corporate network. Outside of the firewalls.

2. Detect was generated by:

Snort IDS with ACID, with portscan logging

Below you can see the logfile with snort alerts. After the "from" you will see from what IP the connections came. You also see the number of connections and if they where TCP or UPD (icmp doesnt have any ports although ping sweeps is a sort of scanning.

Portscan Summary:

```
[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 209.207.190.234 (THRESHOLD 4 connections
exceeded in 0 seconds) [**]
[**] [100:2:1] spp_portscan: portscan status from 209.207.190.234: 222 connections across 220
hosts: TCP(220), UDP(2) [**]
[**] [100:2:1] spp_portscan: portscan status from 209.207.190.234: 411 connections across 411
hosts: TCP(410), UDP(1) [**]
[**] [100:2:1] spp_portscan: portscan status from 209.207.190.234: 590 connections across 590
hosts: TCP(590), UDP(0) [**]
[**] [100:2:1] spp_portscan: portscan status from 209.207.190.234: 407 connections across 407
hosts: TCP(407), UDP(0) [**]
[**] [100:2:1] spp_portscan: portscan status from 209.207.190.234: 29 connections across 29
hosts: TCP(29), UDP(0) [**]
[**] [100:3:1] spp_portscan: End of portscan from 209.207.190.234: TOTAL time(18s) hosts(1653)
TCP(1656) UDP(3) [**]
```

He sweeps through big parts of our nets here.

Intreresting parts:

```
[…]

Jul 18 18:01: 52 209.207.190.234:2488  -> 192.168.43.0:53 SYN ******S*
Jul 18 18:01:49 209.207.190.234:2490   -> 192.168.43.2:53 SYN ******S*
Jul 18 18:01:49 209.207.190.234:3876   -> 192.168.43.2:53 UDP
Jul 18 18:01:52 209.207.190.234:2492   -> 192.168.43.4:53 SYN ******S *
Jul 18 18:01:52 209.207.190.234:2494   -> 192.168.43.6:53 SYN ******S*
Jul 18 18:01:52 209.207.190.234:2496   -> 192.168.43.8:53 SYN ******S*
[…]

Jul 18 18:01:52 209.207.190.234:2692   -> 192.168.43.184:53 SYN ******S*
Jul 18 18:01:52 209.207.190.234:2694   -> 192.168.43.186:53 SYN ******S*
Jul 18 18:01:52 209.207.190.234:2489   -> 192.168.43.1:53 SYN ******S*
Jul 18 18:01:52 209.207.190.234:2491   -> 192.168.43.3:53 SYN ******S*
```

```
Jul 18 18:01:52 209.207.190.234:3876   -> 192.168.43.3:53 UDP
Jul 18 18:01:52 20 9.207.190.234:2493  -> 192.168.43.5:53 SYN ******S*
Jul 18 18:01:52 209.207.190.234:2495   -> 192.168.43.7:53 SYN ******S*
Jul 18 18:01:52 209.207.190.234:2497   -> 192.168.43.9:53 SYN ******S*
[…]

Jul 18 18:01:53 209.207.190.234:2718   -> 192.168.43.209:53 S YN ******S*
Jul 18 18:01:53 209.207.190.234:2712   -> 192.168.43.204:53 SYN ******S*
Jul 18 18:01:53 209.207.190.234:2715   -> 192.168.43.206:53 SYN ******S*
Jul 18 18:01:53 209.207.190.234:2717   -> 192.168.43.208:53 SYN ******S*
Jul 18 18:01:53 209.207.190 .234:2719  -> 192.168.43.210:53 SYN ******S*
Jul 18 18:01:53 209.207.190.234:3876   -> 192.168.43.3:53 UDP
Jul 18 18:01:56 209.207.190.234:3142   -> 192.168.43.220:53 SYN ******S*
Jul 18 18:01:56 209.207.190.234:3143   -> 192.168.43.221:53 SYN ******S*
Jul 1 8 18:01:56 209.207.190.234:3144  -> 192.168.43.222:53 SYN ******S*
Jul 18 18:01:55 209.207.190.234:2720   -> 192.168.43.211:53 SYN ******S*

[…]
```

And he goes further:

The alertlog from snort reveals some further information gathering.

```
#0-(1-376701) DNS  named iquery attempt 2001 -07-18 18:01:53
209.207.190.234:3876  192.168.43.3:53  UDP

#1-(1-376700) DNS named version attempt 2001  -07-18 18:01:52
209.207.190.234:3876  192.168.43.3:53  UDP

#2-(1-376699) DNS named iquery attempt 2001  -07-18 18:01:49
209.207.190.234:3876  192.168.43.2:53  UDP

#3-(1-376698) DNS named version attempt 2001  -07-18 18:01:49
209.207.190.234:3876  192.168.43.2:53  UDP
```

In my snort configuration used at this time i did not have complete dumps of the complete traffic. I do not see the need for it for these scanning attempts.

3. Probability the source address was spoofed:

HIGHLY UNLIKELY, he took action (although it seems automated) from the response he got from the portscanning. But it is likely that the source could be a compromised system.

4. Description of attack:

The attacker tried to check for Inverse Query support and the version of the DNS software.

5. Attack mechanism:

This is a typical information gathering attack. If #defining INVQ isnt commented out from the bind configuration the attacker could gather information about our domain structure. Ancient nslookup can however crash if INVQ is commented out. (source: http://www.cert.org/advisorie s/CA-1998-05.html)

The following can be read at: http://packetderm.cotse.com/CIE/RFC/1035/59.htm

The contents of inverse queries and responses

Inverse queries reverse the mappings performed by standard query operations; while a standard query maps a domain name to a resource, an inverse query maps a resource to a domain name. For example, a standard query might bind a domain name to a host address; the corresponding inverse query binds the host address to a domain name.
Inverse queries take the form of a single RR in the answer section of the message, with an empty question section. The owner name of the query RR and its TTL are not significant. The response carries questions in the question section which identify all names possessing the query RR WHICH THE NAME SERVER KNOWS. Since no name server knows about all of the domain name space, the response can never be assumed to be complete. Thus inverse queries are primarily useful for database management and debugging activities. Inverse queries are NOT an acceptable method of mapping host addresses to host names; use the IN-ADDR.ARPA domain instead.
Where possible, name servers should provide case-insensitive comparisons for inverse queries. Thus an inverse query asking for an MX RR of "Venera.isi.edu" should get the same response as a query for "VENERA.ISI.EDU"; an inverse query for HINFO RR "IBM-PC UNIX" should produce the same result as an inverse query for "IBM-pc unix". However, this cannot be guaranteed because name servers may possess RRs that contain character strings but the name server does not know that the data is character.
When a name server processes an inverse query, it either returns:

1. zero, one, or multiple domain names for the specified resource as QNAMEs in the question section
2. an error code indicating that the name server doesn't support inverse mapping of the specified resource type.

When the response to an inverse query contains one or more QNAMEs, the owner name and TTL of the RR in the answer section which defines the inverse query is modified to exactly match an RR found at the first QNAME.
RRs returned in the inverse queries cannot be cached using the same mechanism as is used for the replies to standard queries. One reason for this is that a name might have multiple RRs of the same type, and only one would appear. For example, an inverse query for a single address of a multiply homed host might create the impression that only one address existed.

6. Correlations :

We have had previous portscans and events for our DNS servers. On the www.incidents.org archives you can see this IP-number scan port 111 only a few days before. (source http://www.incidents.org/archives/intrusions/msg01071.html)

7. Evidence of active targeting:

Probably not, he could have gotten the IP's for our DNS servers in a more easy way. The scans where probably part of a bigger sweep.

8. Severity:

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

Criticality: **5**
These servers are the main dns servers. A compromise on them (without knowing) would be disastrous. So the potential of damage was high.

Lethality: **2**

Information gathering about the systems. Nothing to much to worry about. [there was bugs/exploits for BIND8]

System Countermeasures: **5**
Systems patched and updated.

Network Countermeasures: **1**
This is normal traffic, nothin g will stop this. No additional logging is made except on the server itself.

Severity: (5+3)-(6) = 2

9. Defensive recommendation:

Continued logging and use of IDS for inventory logging of these kinds of events.

10. Multiple choice test question:

iquery is a

a) inverse query towards the DNS

b) incomplete query towards the DNS.

c) internet query for domains.

d) important query towards the DNS

Correct answer is A

Additional Info:

In a attempt to track down who this was I saw that this must be some spooky happenings

http://www.samspade.org/t/lookat.cgi?address=209.207.190.234&whois=on&clueless=no

Official name: *chembid.com*
Addresses: *209.207.190.234*
Error checking for DNS forgery

Whois for chembid.com
[…]
whois -h whois.crsnic.net chembid.com
Crsnic redirect failed
Whois Server Version 1.3

[…]

No match for dom ain "CHEMBID.COM".

>>> Last update of whois database: Sat, 21 Jul 2001 01:56:18 EDT <<<

[…]

HE IS GONE!!! The DNS dont resolve

I tried manually from another network

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

No match for "CHEMBID.COM".

>>> Last update of whois database: Sat, 21 Jul 2001 01:56:18 EDT <<<

The Registry database contains ONLY .COM, . NET, .ORG, .EDU domains and
Registrars.

machine# ping www.chembid.com
ping: cannot resolve www.chembid.com: Unknown host
machine# ping 209.207.190.234
PING 209.207.190.234 (209.207.190.234): 56 data bytes
^C
--- 209.207.190.234 ping statistics ---
7 packets transmitted, 0 packets received, 100% packet loss

Looking for the owner of the network at WWW.ARIN.NETi find:
Verio, Inc. (NET-VRIO-209-207-128) 8005 South Chester Street Englewood, CO 80112 US

Netname: VRIO -209-207-128 Netblock: 209.207.128.0 - 209.207.255.255 Maintainer: VRIO Coordinator: Verio, Inc. (VIA4 -ORG-ARIN) vipar@verio.net 303.645.1900

Not giving up I also try

machine# whois -m 209.207.190.234
route: 209.207.128.0/17
descr: digitalNATION, Inc.
origin: AS7019
notify: noc@dn.net
mnt-by: MAINT -AS7019
changed: bradd@dn.net 19991229
source: VERIO

Looking at http://www.dn.net i get redirected to http://home.verio.com/products/dedicated/index.cfm so my guess is that this individual was thrown out of their hosting services… oh well, case closed.
Atleast hegot as far as poking around alittle on our systems.

The above tracing is the only one inclu ded in the detects! (the ones in analyze this is in the appendix)

Detect 2

Frontpage exploitables, not served here…

1. Source of Trace.

Educational network
Apache webbserver loggfiles and correlated with another networks Snort/tcpdump

2. Detect was generated by:

Apache webbserver loggfiles and correlated with another network

The logfiles are placing in the following order:

Who did:	10.xxx.6.xx - -
when did it happen:	[10/Jun/2001:21:10:36 +0200]
what happened:	GET /_vti_inf.html HTTP/1.1" 404 302
additional details of the event:	Mozilla/2.0 (compatible; MS FrontPage 4.0)"

Step 1:

```
Accesslog
10.xxx.6.xx - - [10/Jun/2001:21:10:36 +0200] "GET /_vti_inf.html HTTP/1.1" 404 302 "-"
"Mozilla/2.0 (compatible; MS FrontPage 4.0)"
```

Step 2:

```
Accesslog
10.xxx.6.xx - - [10/Jun/2001:21:10:36 +0200] "POST /_vti_bin/shtml.exe/_vti_rpc HTTP/1.1" 404 316
"-" "MSFrontPage/4.0"
```

3. Probability the source address was spoofed:

Unlikely, he was looking for response not disrupting service.

4. Description of attac k:

The attacker tried by remote to exploit Front Page extensions on the http service. I have seen this kind of behavior from **searchbots** before looking for file inventory. But this IP was **internal**! Which had me interested.

5. Attack mechanism:

Looking further online for an explanation:
Get _vti_inf.html could be a probe for frontpage extensions

(http://www.insecure.org/sploits/Microsoft.frontpage.insecurities.html)

Post shtml.exe could be a try to find the webserver path
(http://www.securiteam.com/windowsntfocus/5NP0J0U1FO.html)

Looking at Technet you see that shtml.exe is the Server Extensions b rowse-time stub program _vti_inf.html is the FrontPage information file.
(http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/office/reskit/fp98serk/appendixes/A_UNPERM.asp)

This bug/exploit is reported at:
(http://www.securityfocus.com/bid/1174)

Although this could just be a functionality test for frontpage extensions from Office2000 as described by Richard Bejtlich.
(http://www.sans.org/y2k/062000.htm)

6. Correlations:

Since I got access to some other networks I am using the same detect here for correlation

```
Packet 9715
TIME:   10:56:58.340165 (1.649911)
LINK:   03:33:8E:33:33:00 -> 94:21:73:12:9C:30 type=IP
  IP:   h107n1fls3o804 -> yyycacheeyyy hlen=20 TOS=00 dgramlen=299 id=5510
        MF/DF=0/1 frag=0 TTL=117 proto=TCP cksum=E23E
 TCP:   port 1351 -> www seq=3060279280 ack=2014254625
        hlen=20 (data=259) UAPRSF=011000 wnd=17520 cksum=A7B7 urg=0
DATA:   GET /_vti_inf.html HTTP/1.1.
        Date: Mon, 16 Jun 2001 08:56:41 GMT.
        MIME-Version: 1.0.
        Accept: */*.
        User-Agent: Mozilla/2.0 (compatible; MS FrontPage 4.0).
        Host: www.yyy.se.
        Accept: auth/sicily.
        Content-Length: 0.
        Connection: Keep-Alive.
        Cookie: visited=true.
        .

-------------------------------------------------------------------------------
Packet xxxxxx
TIME:   10:56:58.620071 (0.279906)
LINK:   03:33:8E:33:33:00 -> 94:21:73:12:9C:30 type=IP
  IP:   h107n1fls3o804 -> yyycacheeyyy hlen=20 TOS=00 dgramlen=404 id=551A
        MF/DF=0/1 frag=0 TTL=117 proto=TCP cksum=E1CB
 TCP:   port 1352 -> www seq=3060500022 ack=2495324808
        hlen=20 (data=364) UAPRSF=011000 wnd=17520 cksum=F149 urg=0
DATA:   POST /_vti_bin/shtml.exe/_vti_rpc HTTP/1.1.
        Date: Mon, 16 Jun 2001 08:56:41 GMT.
        MIME-Version: 1.0.
```

```
User-Agent: MSFrontPage/4.0.
Host: www.yyy.se.
Accept: auth/sicily.
Content-Length: 41.
Content-Type: application/x-www-form-urlencoded.
X-Vermeer-Content-Type: application/x-www-form-urlencoded.
Connection: Keep-Alive.
.
method=server+version%3a4%2e0%2e2%2e2611
.
```

Packet xxxxxxx+1

7. Evidence of active targeting:

What we are dealing with here are bored CS students staying at campus over the summer. I know for a fact that the IP number next to this server is a unpatched IIS server, although this host that got attacked we removed the FrontPage extensions and functionality a while back.

8. Severity:

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

Criticality: **5**
This server is the m ain dns, smtp -relay and http/ftp server for the student network! If it went down or got compromised hundreds of PFY's would lose their internet connectivity/activity.

Lethality: **3**
If we where running IIS or still having the FrontPage extensions availabl e harm could have been done. Or serious information gathering about the system could have been made.

System Countermeasures: **5**
The FrontPage extensions had been removed for some time , besides this is a FreeBSD server running apache, not IIS on Windows.

Network Countermeasures: **1**
This is normal traffic, nothing will stop this. No additional logging is made except on the server itself.

Severity: (5+3) -(6) = 2, although i would go even higher then 5 on System Countermeasures if i could. Since the only att ack it made was filling up the logfile in /var

9. Defensive recommendation:

Talk to the admins running IIS on the other segment that they really should consider changing operating system and http-server. Or atleast firewall it for their internal use.

10. Multiple choice test question:

For FrontPage support the /_vti_inf.html is the

a) Frontpage Virtual Transmission Interface page.

b) FrontPage information file

c) valuable transaction integrity checker for IIS servers.

d) Frontpage exploit collec tor

Correct answer is B

Additional Info:

I did trace the guy down the other day and asked him about this, he denied anything of everything, although he seemed to know his ways with computers. Oh well no harm done here but its good to know thee enemy.

[Added 2001-07-24: I did some tests with the server with Office 2000 and confirms that it is Word/Office looking for Frontpage extensions! The server itself lacks frontpage extensions]

Resources on the web:

http://www.insecure.org/sploits/Microsoft.frontpage.insecurities.html

http://www.securiteam.com/windowsntfocus/5NP0J0U1FO.html

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/office/reskit/fp98serk/appendixes/A_UNPERM.asp

http://www.securityfocus.com/bid/1174

http://www.sans.org/y2k/062000.htm

Detect 3

Worms in the house (this detect replaces a previous ida ISAPI Overflow)

1. Source of Trace.

Corporate network. Snort Sensor

2. Detect was generated by:

Snort IDS connected to MySQL/ACID management representation

IP	source addr	dest addr	Ver	Hdr Len	TOS	Length	ID	Flags	Offset	TTL	chksum
	204.210.243.191	Our.iis.server	4	5	0	1500	2134	0	0	110	13336
	FQDN	Source Name					Dest. Name				
		Wvl243191.columbus.rr.com					www.hostname.xyz				
	Options	*none*									

TCP	source port	Dest port	R1	R0	URG	ACK	PSH	RST	SYN	FIN	seq #	Ack	offset	Res	Window	urp	chksum
	4614	80				X	X				1868438840	1440451	5	0	17520	0	1931
	Options	*none*															

Payload	Length = 1460 000 : 2F 64 65 66 61 75 6C 74 2E 69 64 61 3F 4E 4E 4E / **default.ida?** NNN 010 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 020 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 030 : 4E 4E 4E 4E 4E 4 E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 040 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 050 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 060 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNN NNNNNNNNNNNN 070 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 080 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 090 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 0a0 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 0b0 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 0c0 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNNNNNNNNNN 0d0 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E NNNN NNNNNNNNNNN 0e0 : 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 25 75 39 NNNNNNNNNNNN%u9 0f0 : 30 39 30 25 75 36 38 35 38 25 75 63 62 64 33 25 090%u6858%ucbd3% 100 : 75 37 38 30 31 25 75 39 30 39 30 25 75 36 38 35 u7801%u9090%u685 110 : 38 25 75 63 62 64 33 25 75 37 38 30 31 25 75 39 8%ucbd3%u7801%u9 120 : 30 39 30 25 75 36 38 35 38 25 75 63 62 64 33 25 090%u6858%ucbd3% 130 : 75 37 38 30 31 25 75 39 30 39 30 25 75 39 30 39 u7801%u9090%u909 140 : 30 25 75 38 31 39 30 25 75 30 30 63 33 25 75 30 0%u81 90%u00c3%u0 150 : 30 30 33 25 75 38 62 30 30 25 75 35 33 31 62 25 003%u8b00%u531b% 160 : 75 35 33 66 66 25 75 30 30 37 38 25 75 30 30 30 u53ff%u0078%u000 170 : 30 25 75 30 30 3D 61 20 20 48 54 54 50 2F 31 2E 0%u00=a HTTP/1. 180 : 30 0D 0A 43 6F 6E 7 4 65 6E 74 2D 74 79 70 65 3A 0..Content -type: 190 : 20 74 65 78 74 2F 78 6D 6C 0A 48 4F 53 54 3A 77 text/xml.HOST:w 1a0 : 77 77 2E 77 6F 72 6D 2E 63 6F 6D 0A 20 41 63 63 ww.worm.com. Acc 1b0 : 65 70 74 3A 20 2A 2F 2A 0A 43 6F 6E 74 65 6E 74 ept: * /*.Content 1c0 : 2D 6C 65 6E 67 74 68 3A 20 33 35 36 39 20 0D 0A -length: 3569 .. 1d0 : 0D 0A 55 8B EC 81 EC 18 02 00 00 53 56 57 8D BD ..U.....SVW.. 1e0 : E8 FD FF FF B9 86 00 00 00 B8 CC CC CC CC F3 AB .... 1f0 : C7 85 70 FE FF FF 00 00 00 00 E9 0A 0B 00 00 8F ..p..... 200 : 85 68 FE FF FF 8D BD F0 FE FF FF 64 A1 00 00 00 .h.....d.... 210 : 00 89 47 08 64 89 3D 00 00 00 00 E9 6F 0A 00 00

3. Probability the source address was spoofed:

Unlikely, this is an a utomated attack that isn't known to spoof itself in anyway.

4. Description of attack:

Automated Worm attack, towards IIS servers (indexing service). Pretty famous at the time of writing.

The signature that spooted the detect was:
alert tcp $EXTERNAL_NE T any -> $HTTP_SERVERS 80 (msg: "ida ISAPI Overflow";content: ".ida?"; dsize: >239; flags: A+; nocase;)

This was on the 20:th of July so it this is a Code Red version CRv1
I caught in the IDS. (this assumpsion is based on the information provided at http://www.incidents.org/react/code_red.php that the worm tried to deface the page with the www.worm.com text)

5. Attack mechanism:

From the CERT advisory (http://www.cert.org/advisories/CA-2001-19.html) you can read the following:

The "Code Red" worm attack proceeds as follows:

3. The "Code Red" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service described in CERT advisory CA-2001-13
4. The same exploit (HTTP GET request) is sent to each of the randomly chosen hosts due to the self-propagating nature of the worm. However, depending on the configuration of the host which receives this request, there are varied consequences.

- **IIS 4.0 and 5.0 servers with Indexing service enabled** will be compromised by the "Code Red" Worm
- **Unpatched Cisco 600-series DSL routers** will process the HTTP request thereby triggering an unrelated vulnerability which causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
- **Systems not running IIS, but with an HTTP server listening on TCP port 80** will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log.

5. If the exploit is successful, the worm begins executing on the victim host. In the earlier variant of the worm, victim hosts with a default language of English experienced the following defacement on all pages requested from the server:

   ```
   HELLO! Welcome to http://www.worm.com! Hacked By Chinese!
   ```

   Servers configured with a language that is not English and those infected with the later variant will not experience any change in the served content.

6. Correlations:

This attack hits all over the internet more or less, we even had some false alarms in the previous week, but i choose to take a “real” one towards a WinNT system.

Looking at the statistics from the www.incidents.com/diary/
07/20 09:00 EDT updated Code Red summary from cas.org's IDS:

Date	# Worm Probes	# Unique Source Addr's Probing (For the Day)	# Unique Source Addr's Probing (Cumulative)	# Unique Dest Addr's being Probed (Day)
07/12	3	1	1	1
07/13	611	27	28	19
07/14	36273	1076	1080	659
07/15	215020	3498	3642	1845
07/16	316828	6137	7147	2705
07/17	316359	7097	10213	2717
07/18	294345	8247	13867	3131
07/19	4080321	272052	279912	64768
07/20	**74954**	**3485**	**280443**	**20611**
07/21 *	7588 *	641 *	280405 *	2506 *

So it looks like we got hit at the end of the first wave. None of our systems where affected and I shared the tools avaible for letting other associates battle this problem.

7. Evidence of active targeting:

Nah… Well active targeting against the WinNT plattform. Not against us.

8. Severity:

Calculated Severity = (Criticality+Lethality) -(System Cou ntermeasures+Network Countermeasures)

Criticality: **5**
The systems attacked has alot of "pr -value" for my company, they are running WinNT and are somewhat of the black sheep's in the webserver farm.

Lethality: **5**
Defacing the site and potentially doing DoS-attacks towards a foreign goverment, NOT good for public relations with our NATO -friends (we say we are neutral here in Sweden).

System Countermeasures: **5**
I almost started laughing during the pre -post-mortem analysis. Indexing Service is turned off an d the server is running with Swedish language settings so it wasnt defaced. And these WinNT servers are the only Windows boxes exposed to the internet. I almost looked forward for my first real Incidenthandling and post-mortem analysis. Oh well better luck next time =)

Network Countermeasures: **2**
Couldnt stop it. We detected it in the IDS, analysed it.

Severity: (5+5) -(7) = 3, This could have been dangerous, although no traces of a successful attack was made.

9. Defensive recommendation:

Continue to ke ep these servers on a separate DMZ and take them down after migration of the web applications to Solaris. [also recommended and did a security scanning over other Windows servers for the vulnerability with the tool from eeye availble from http://www.eeye.com/html/Research/Tools/CodeRedScanner.exe] [added 2001 -10-08 The servers are still running with appropriate patches, but at a boardmeeting this incident lead to a new project: migrating away from IIS]. These systems should be observed if new patches will be needed before the migration can take place.

10. Multiple choice test question:

The reason Code Red Worm did not successfully **deface** the majority of IIS sites was:

a) Because Mi crosoft makes software secure by default(© to OpenBSD).

b) Because one patch is enough to solve all problems.

c) Because Open Source Software is Communism.

d) Because America isn't the center of the world (i.e. have English/American language set by def ault).

Correct answer is D, and hopefully the crax0rs dont read this so they make exploits work with other language settings then English/American…

[This is hopefully considered as a joke by egocentric Americans, so no offense :-]

Additional Info:

Resources on the web:
http://www.incidents.org/diary/diary.php
http://archives.neohapsis.com/archives/bugtraq/2001 -07/0396.html

http://www.cert.org/advisories/CA_-2001-19.html
http://www.incidents.org/react/code_red.php

Detect 4

They shut our faul m outh?

1. Source of Trace.

Corporate network. Snort (production sensor number4 towards internet)

2. Detect was generated by:

Snort IDS connected to MySQL/ACID management representation

Meta	ID #	Time	Triggered Signature	
	1 - 438362	2001-07-21 17:33:12	ICMP Destination Unreachable (Communication with Destination Network is Administratively Prohibited)	
	Sensor	Name	Interface	Filter
		snort4	fxp0	*None*
	Alert Group	*none*		

IP	source addr	Dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
	217.5.127.49	192.168.43.233	4	5	0	56	19029	0	0	52	57593
	FQDN	Source Name				Dest. Name					
		Unable to resolve address				*Unable to resolve address*					
	Options	*None*									

ICMP	type	Code	Checksum	id	seq #
	Destination Unreachable	Network ANO	25811		

Payload
length = 32 000 : 00 00 00 00 4 5 00 00 28 F9 E9 00 00 1D 06 46 1D ....E..(.....F. 010 : C2 47 40 92 D9 50 81 9F 07 42 00 71 28 37 68 39 .G@..P...B.q(7h9
[that a nice feature in word… makes an e -mail link…]

3. Probability the source address was spoofed:

Unlikely, although it is a chance that that the initial attacker spoofed us making us the destination adress.

4. Description of attack:

It is more of a detect towards our system then a attack on us. [I have tried to contact the sou rce ip owners without any response].

5. Attack mechanism:

A wild guess here is the attacker was abusing the senders service and that the other (source adress) network has closed down communication. Strange though that this was the only detect to/from this network.

ICMP CODES:

RFC 1700 contains the possible values for each ICMP type and code:

Type	Name	Code(s)
0	Echo reply	0 – none
1	Unassigned	
2	Unassigned	
3	Destination unreachable	0 - Net unreachable 1 - Host unreachable 2 - Protocol unreachable 3 - Port unreachable 4 – Fragmentation needed and DF bit set 5 - Source route failed 6 - Destination network unknown 7 - Destination host unknown 8 - Source host isolated 9 – Communication with destination network is administratively prohibited 10 – Communication with destination host is administratively prohibited 11 - Destination network unreachable for TOS 12 - Destination host unreachable for TOS
4	Source quench	0 – none
5	Redirect	0 - Redirect datagram for the network 1 - Redirect datagram for the host 2 - Redirect datagram for the TOS and network 3 - Redirect datagram for the TOS and host
6	Alternate host address	0 - Alternate address for host
7	Unassigned	
8	Echo	0 – None
9	Router advertis ement	0 – None
10	Router selection	0 – None
11	Time Exceeded	0 - Time to live exceeded in transit 1 - Fragment reassembly time exceeded
12	Parameter problem	0 - Pointer indicates the error 1 - Missing a required option 2 - Bad length
13	Timestamp	0 – None
14	Timestamp reply	0 – None
15	Information request	0 – None
16	Information reply	0 – None
17	Address mask request	0 – None
18	Address mask reply	0 – None
19	Reserved (for security)	
20-	Reserved (for robustness	

29 experiment)
30 Traceroute
31 Datagram conversion error
32 Mobile host redirect
33 IPv6 where-are-you
34 IPv6 I-am-here
35 Mobile registration request
36 Mobile registration reply
37-255 Reserved

Source: http://www.onlamp.com/pub/a/bsd/2001/04/04/FreeBSD_Basics_.html

6. Correlations:

none, I have tried mailing the network admins for both networks without any good response. Oh well it was back in 1995 or so when you could actually get a reply quickly from a NOC -engineer…. ;-)

7. Evidence of active targeting:

Higly Unlikely that he was. My suggestion as above is that we just got a detect from the crossfire, a ricochet if you would like ballistics terms.

8. Severity:

Calculated Severity = (Criticality+Lethality) -(System Countermeasures+Network Countermeasu res)

Criticality: **1**
We dont have a host at this IP, we just got a detect in the crossfire.

Lethality: **1**
Information gathering about other systems. Nothing to much to worry about.

System Countermeasures: **5**
Systems patched and updated. Not our rule -set being sent out… : -)

Network Countermeasures: **5**
It got logged, it got dropped in the firewalls. We logged it, analysed it.

Severity: (1+1) -(10) = -8, this was the only " Communication with destination host is administratively prohibited " detected so far. Although I dont see a problem with it since it must have been a spoofed transmission in the communication **before** it reached our network.

9. Defensive recommendation:

Continued logging for more strange ICMP messages, they are getting more and more interesting. Also recommending myself and others around me to read up on the excellent paper by Ofir Arkin (listed in the resources).

10. Multiple choice test question:

ICMP is:

a) Only useful for ping and traceroute in some cases.

b) An obsolete protocol that should be dropped at the firewalls

c) A protocol rightfully getting more and more attention from the IDS -community

d) Never used for covert channels or fingerprinting of operating systems.

Correct answer is C

Additional Info:

Resources on the web:

http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf

Detect 5

Detection of scan towards unknown host with crafted packet

1. Source of Trace.

Perimiter of own network. (outside the firewalls)

2. Detect was generated by:

Snort intrusion detection system 1.8, portscanner configuration.

```
Portscan log:
Jul 19 06:59:58 194.65.57.182:0 -> 192.168.43.134:0 NULL ********
```

Snort intrusion detection s ystem 1.8, inventory configuration

ID	≤ Signature ≥	≤ TimeStamp ≥	≤ Source Address ≥	≤ Dest. Address ≥	≤ Layer 4 Proto ≥
#0-(1-378147)	[arachNIDS] SCAN NULL	2001-06-19 06:59:58	194.65.57.182:0	192.168.43.134:0	TCP
#1-(1-378145)	[arachNIDS] SCAN NULL	2001-06-19 06:59:56	194.65.57.182:0	192.168.43.134:0	TCP
#2-(1-350473)	[arachNIDS] SCAN NULL	2001-06-18 06:04:19	194.65.57.182:0	192.168.43.228:0	TCP
#3-(1-350474)	[arachNIDS] SCAN NULL	2001-06-18 06:04:21	194.65.57.182:0	192.168.43.228:0	TCP

My configurations on the outside is to log portscans locally and more important events in a database:
One snort process picks up portscans and logs them locally on the sensor
The second reports other alerts to a MySQL database (ACID as representation)

3. Probability the source address was spoofed:

Probably not, well it could be if the attacker/scanner wasn't interested in the results.

4. Description of attack:

Null SCAN, Setting both payload flags and port to 0
Possibly probing our network.

IP	source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
	194.65.57.182	192.168.43.1	4	5	0	20	24773	0	0	108	50723
	FQDN	Source Name				Dest. Name					
		Unable to resolve address				*Unable to resolve address*					
	Options	*None*									

TCP	source port	dest port	R1	R0	URG	ACK	PSH	RST	SYN	FIN	seq #	ack	Offset	res	window	urp	chksum
	0	0									0	0	0	0	0	0	0

What had me worried here was that he probed a network of ours that wasnt registered at the DNS I wasn't that familiar with the adresspace. It turns out however that the c lass-C network he was probing **isn't in use yet. So he is shooting blindly** .

The Signature in snort that picked it up was

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN NULL";flags:0; seq:0; ack:0; reference:arachnids,4; classtype:attempted -recon; sid:623; rev:1;)

5. Attack mechanism:

The scan is made by setting sequence number and control bits to zero, no SYN, FIN or anything. [in this case even the portnumbers where 0] This is a pretty basic surveillance scan and is low risk compared to other mo re sophisticated scans.

6. Correlations:

None, haven't even seen this guy in any alert before on any network I have sensors.
[off the record: a friend did some test on the "31337h4x0r" and it seems like it was infected by some trojans!, so perhaps the box did someone else's bidding at the time]

7. Evidence of active targeting:

Not really, it seems like an automated scan with wrong number, this network hasn't been alive for at least 6years (= never). What made me look into the event was that it intrig ued me since i didn't recognize the target of the scan.

8. Severity:

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

Criticality: 1

This whole segment that he scans over these two days isn't active.

Lethality: 1

This scan is the equivalent to ping, using TCP. The attack was a disaster from his perspective.

System Countermeasures: N/A

He was shooting blindly, I got worried at first that it was a system i was unaware of.

Network Countermeasures: 5

Firewalls isnt passing anything to this network.

Severity: (1+1) -(5) = -3, or less

9. Defensive recommendation:

Continued logging of events and a followup if this IP had any further traffic to us.

10. Multiple choice test question:

A SCAN NULL type of scan se ts the following crafted package:

a) source adress to all zeros, causing a massive ping -DoS attack on all older BSD -server all over the internet.

b) sets the sequence number equal to the checksum, which fools the TCP/IP stack to resend the same package fro m a arbitrary open port in the operating system.

c) sets the sequence number to zero as well as the controlbits.

d) sets defrag to 0 causing the loopback interface to keep send 0 -bit packages, usually eating up all resources and eventually stops the Kernel from Context Switching.

Correct answer is B, just kidding its C

Additional Info:

The alerts show:

```
[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 194.65.57.182 (STEALTH)
[**]
06/19-06:59:56.258452 194.65.57.182:0  -> 192.168.43.134:0
06/19-06:59:58.929306 194.65.57.182:0  -> 192.168.43.134:0

[**] [100:2:1] spp_portscan: portscan status from 194.65.57.182: 1
connections across 1 hosts: TCP(1), UDP(0) STEALTH [**]
[**] [100:3:1] spp_portscan: End of portscan from 194.65.57.182: TOTAL
time(2s) hosts(1)  TCP(1) UDP(0) STEALTH [**]
```

Resources on the web:
http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids4
http://advice.networkice.com/Advice/Intrusions/2000309/default.htm

Assignment 2(new)

Assignment 2 - State of Intrusion Detection

Implementing IDS; get ting yet another tool, or how to get a capable automated security officer and the hardware to assist the process. (Recomendations from my experience)

This text is a summary of some design and technical issues common for IDS projects. I have tried to focus on technical and architectural issues with new insights not mentioned elsewhere. But also giving room for theories about the state of Intrusion Detection considering the firms and solutions that exist. Bare in mind that my spelling grammar maybe somewhat terrible since English isnt my primary language. I have tried to write so certain parts can be used/integrated for some form of FAQ.

The goal audience is those who are in the process of investing in hardware for Intrusion Detection. A little disclaimer o n the products mentioned, I am in no way related to any of the products or companies. I do see the serious problem with IDS being a immature productline today and there are alot of consultants that wants your money. My path of choice has been to try to fix things independently and with collaboration with my coworkers using the best hardware performance vs. price ratio with Open Source products. I have tested alot of the commercial products and lets be fair, they are all terrible more or less today and Snort is the only one worth its price/time (it is free for those who are not familiar with Snort). I am not going into details in configurations/deployment here since its not the time or place. I am just trying to mention the implementation of products that are pretty of the shelf but not that "vendorized" to be IDS - equipment. Perhaps their sales offices will catch on in time…

Inside or outside the firewall

The design issue that always seem to come up in every IDS -project is "outside or inside the firewall?". In my opinion the answer is both. Just as the question on the hen and the egg, it was the cock that was there first. You must have an open mind thinking out of the boundaries to get the implementation you need/want. IDS is not a product you get from the sh elf it is a process, more on this later.

Promises, Promises, Promises…

As IDS is a somewhat new and immature securityproduct if you relate to firewalls. There are alot of consultants and firms that will promise you gold and green forests without performi ng those when you get them in the lab environment. "We will have that in the next version" is a term im beginning to hate more and more. The biggest problem with going your own path is that i dont have any vendor to call when i/someone fsck up. I see my co llegues when they experience problems with Microsoft servers or SUN servers, they always have a ace up their sleeve for these situations "Vendor X has been notified and we are working on the problem". So perhaps im in for a rough journey using Open Source products on Intel hardware with a free UNIX operating system. I dont get support from any of the camps since i betray them both in some way. Well now the situation isnt that bad, you can/will get allies in other camps and Quislings among the others. Open Source is here to stay and gaining ground for special purposes. I am glad i have a

manager that trusts my judgement, well actually its more at stake then his trust… Oh well dont get scared of going your own way it will be rewarding!

Do not do it in your " sparetime"

For a successful implementation i do recommend making the implementation and pilot a project with set timedates. Both for your sake as a future intrusion analyst, but also for your company. We need to get the show on the road, the scriptkiddies and 31337h4x0rz are out there ready to battle, at least you can open your eyes to get an inventory of the weapons they use quickly.

Get the managers to grasp on what IDS really is

The first obstacle you have to win over is budget/resource allocation, ho w do i get management to understand the importance of IDS. In my case it was the revelation of the use of firewalls. They dont stop attackers, they act as a traffic controller. Sure they stop some of the attackers but not those in disguise and with nasty p ayload. You could see the firewall as a castlewall with some openings. If this were a castle the IDS would be a security officer looking down on the carriages load. The firewall/guards look at the coachman and asks where he is from and where he plans to go and if there are more carriages that will follow. The IDS will give you a more in depth view of what is going on in the network. Not just "who from?", "where to?", hopefully the IDS will give you additional information of what happened. This gives the chi ef of operations the ability to ask what happened before you start speculating on how it could happen if something goes wrong.

But we got our loyal firewalls that should be enough!

One big advantage with ID Sensors is that they will be the ability to veri fy the integrity/configuration of a firewall. Especially if you place your sensors both inside and outside of the firewall. If i may go back to my castle you can see this as keeping track of the log for what is said to have come pass the guards and what yo ur automated security officer have seen get passed.

Outsourcing this IDS thingie?

Outsourcing IDS is not an option for most big enterprises because my belief is that one will always get what one pays for. Consider you having your own IT -security personnel they know much more about your environment then any other company will ever do. If you pay less for others to watch over your network, my opinion is that you would be better of with a trafficdumper and a simple IDS that you check on from time to time, if you wish to save your money. A price offer from a consultantfirm was equal to three fulltime analysts in -house so in our case it wasn't even cheaper! I could spend a whole paper on discussing around the clock availability and the issues with that, but i f eel that is very different for other organizations. I would rather invest in a huge fileserver just to keep evidence on what passed to/from your network (complete payload) in case something happens. My opinion is that if your taking IT - security seriously y ou should dedicate the time and resources for a complete infrastructure. Feel free to read Charles Hutsons work about outsourcing to get both sides of the story:
http://www.sans.org/y2_k/practical/Charles_Hutson_GCIA.doc

Trafficdumping with a Redundant Array of INEXPENSIVE Disks

If you dont want to go on expensive SCSI -drives or using a storage array network (SAN) you can go pretty cheap on a system that can hold 16 ATA100 drives, yo u can then have over 1TB of traffic storage for roughly a third of its SCSI equivalent. It is a shame that at the time of writing the 3ware Escalade controllers are disappearing from the market. Apparently they where too good to be on the market, 3ware wis h to sell their integrated solutions.

Example of case for ATA100 RAID trafficdumper

One problem with the trafficdumper is that it will not alarm on any intrusion attempts, you have to check on the traffic. You could however use Shado w for going through these logs but this system is more of a evidencecollector then a IDS. There exist a product based on FreeBSD and TCPDUMP called NetVCR from NIKSUN. But i prefer to build the solution myself if i where to get this. You will get good perf ormance and notice on dropped packets with FreeBSD (you can replay the dumps into another IDS like snort aswell). Of course you can not IDEdisks on the equipment if your internetline is huge, then you have to sort traffic. Filter out e -mail and http traffic. I can recommend having reverse proxies (loadbalancers) combined with antivirus to handle the serious security issues with protocols involved. My philosophy is that you let the right thing be in the right place and IDS should detect not react. But do no t leave contentscanning/blocking left out just because you have a IDS.

Use your spare storage if availble

In my environment we will possibly use the spare storage on a SAN for temporary fullcapture logs. If you have that ability this is a good option! I h ave no idea why we have so much diskspace available but if its still free i can go back to see every packet from every host in more then 11 months that has come/left our networks. One month should be enough for the "highquality data" and keeping 2+years of the "lowfidelity datatransfer logs", I know I cant use that space forever.

Dual Interface Adapters

When it comes to the interfaces that pick up data on a FastEthernet environment the Intel Pro dual server adapter is a single PCI slot for two interfaces. It is good for expanding. In my lab we have plans to test this adapter for redundancyoverlaps of the firewalls as well as statefull

inspection with passive taps. Regretfully I have not any completed analysis of this at the time of writing and i have not y et seen much information about it on the internet. This will be covered in the next version of this document ; -) [see above with vendor promises. Seriously I will publish my result in some forum/mailinglist when this brainchild verified of working]

Getting five times more interfaces for IDS on one RackUnit

One good thing with it is that you can with a 1U rackserver monitor with five interfaces and keep one for management net (connection to database/logging). The rackserver i mention above is the DELL350. It has good performance (PIII 850MHz) for less then $2k with two additional dual interfaces (this includes taking out the monitor adapter, using OpenSSH for "direct interaction").

Picture of a 1U DELL350

Of course other vendors as SUN and HP has solutions aswell, both with SCSI and IDE so my choice of DELL was more a hint i got that OpenBSD runs excellent on these DELL350 machines (and NFR has support for the interfaces mentioned, and it is a OpenBSD based appliance). The re are other NIC's aswell, for example 3com982 (but it is out of stock at the moment). But i will leave it up to you and your company to sort things out, i can only say what worked for me. DISCLAIMER: Bare in mind that it takes alot of CPU resources if yo u place such sensors on heavy networks. Only use such sensors on slow connections or segments with limited traffic without bursts that isnt critical at all **. Dedicated sensors are always best** , this is just a way to please your manager of segment coverage… I Hope he doesnt read this…

Spotting misconfigurations

Everything a IDS picks up isnt evil hacking attempts, its sometimes misconfigurations or equipment failing. Communications equipment are good examples. When calibrating the IDS it's a good thing that this "service" is included. There are plenty of examples of this in submitted works and conversations on the internet.

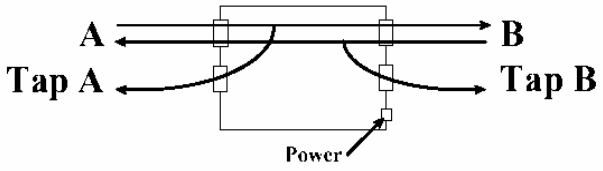
When spanning/hubbing is not an option/preferable

In a switched enviroment you sometimes cannot monitor the traffic you wish. Or perhap s for performance reasons you cannot SPAN out another port. Another possibility is that you wish to QUICKLY setup a sensor on a segment/line/interface without any possibilities/credentials other then physical access (no i do not try to give Black Hats new ideas, they already know). Actually i think that if you take money out of the equation hubbing is never a good option. You then place a SPF (single point of failure) infront of your fancy shining *insert favorite vendor* server.

The solution could be pas sive taps, again i do not have any relation with any companies mentioned, but Shomiti are world leading when it comes to this. These taps are completely passive and works with FULL DUPLEX when it comes to hubs and spanned ports you are limited to only a to tal of the combined traffic. I cant tell you how many people i have been forced into this discussion. But trust me, you can at some point have use of passive taps for fullduplex monitoring when resources do not permit it in other ways. I have seen solution s that you can connect interfaces into boxes to make them passive (more or less cutting out the send wires (logical and physical) this aint pretty sight!).

How the tap looks in physical form

One good thing that i have verified with this product is that you can actually remove the power or change around the tap-cables without disrupting the production environment. You can place 3 of these passive taps on a 1U rack.



How it works in logic

Shomiti/Finisar also has a 12port product that lets you switch between the systems you wish to monitor/tap. I had plans to use it in a lab-environment but could not find it that usefull in my enviroment. Just wanted to mention it.

For a more detailed information on how to use this with CISCO Switches you can visit the Metases site mentioned in the sources.

Where should sensors be placed?

Now when we got some potential hardware extras you can implement, lets get back to the softside of IDS deployment. What about WHAT/WHERE/HOW we should monitor, should we proctect us from the internet or the internet from us. Tough question, but most computer crimes are internal (i belive that most networkintrusion attempts are external, but most successfull are from people that know your organisation). Can we spot them on these sensors? Yes sure you can but thats usually more anomaly detection then stringbased. Dont forget your external connections like VPN and modems/RAS. Of cource your milage may vary, some perhaps only needs a single sensor at the web-dmz because it is the only face out. With many sensors be sure to use an implementation that will support centralized management. Another thing that ALOT of people seem to miss while speaking about IDS is timestamps, the use of NTP is crucial. Dont miss out on it! Another tip if using Snort is to go with OpenBSD on the sensors. For management and databases you can use pretty much "anything" but i do want to know if we are losing packets aswell as having a secure installation on the sensor by default. Linux does not have this ability.

Rutines and guidelines of usage

It is important that you do not forget to document how the systems shall be implemented and educating the users and surveillance team. Depending on size of the company i cannot give specific recommendations on how much you should delegate of the process. In smaller companies you have to do it all by your self. You have to sleep some times and the more you can automate the better of you are in a tight human resource situation. For excellent coverage on the usage of systems and further education i recommend you going the GCIA certification track and read Stephen Northcutts books (or maybe you already are taking the track). One thing to really keep in mind is that IDS is not a product it is a process, you will need time to constantly update and maintain this imporant part of your infrastructure.

Sources / Resources for information used and additional information:

Internet

http://www.shmoo.com/mail/ids/nov_99/msg00047.html (archived discussion about hardware/ids)
http://www.metases.com/files/Shomiti.pdf (document on Shomiti taps with Cisco2900)
http://www.finisar -systems.com/products/index.html (Ethernet and Fiberchannel taps)
http://www.niksun.com/products/netvcr.html (if you dont want to build your trafficdumper by yourself)
http://www.sans.org/y2k/practical/Charles_Hutson_GCIA.doc (assignment2 is about outsourcing)
http://www.tcpdump.org/ (TCPDUMP)
http://www.snort.org/ (Snort IDS) *no its not spelled Snorth, Mr.Consult -know-it-all*
http://www.nswc.navy.mil/ISSEC/CID/ (Shadow IDS)
http://www.cert.org/kb/acid/ (Analyst Console for Intrusion Databases)
http://www.freebsd.org (Highperformance and stable Operating System)
http://www.openbsd.org (Highly secured and stable Operating System)

Books & other info

Network Intrusion Detection: An Analyst's Handbook: Stephen Northcutt, Judy Novak, Don ald McLachlan (2000)
Manpages from the BSD distibutions can learn you alot! Also be sure to check out TCPDUMP

Assignment2old

Update of Trojans and worms, correlated with known ports

(replaced by Assignment2new on October 25:th 2001)

Background

This update has used Joakim von Brauns list as a base, with modifications and corrections. Updates have been gathered from my lab and from the sources listed below.

Overview

Although times are changing and trojanports can be modified the list below can still be us ed to see potential trojan traffic. The pageformat here restricted me from correlating the ports with the wellknown/regular services. **Please also look in the separate file** included in my submitted work there should be a text file with tabbed separation and a preformatted excelfile. For the known ports the FreeBSD servicelist was used (IANA).

Port	Protocol	Alternative Servicename/Trojan/Activity
	ICMP	Skydance (used to run on TCP 4000)
2	TCP	Death
20	TCP	Senna Spy FTP server
21	TCP	Back Construc tion, Blade Runner, Doly Trojan, Fore, Freddy, Invisible FTP, Juggernaut 42 , Larva, MotIv FTP, Net Administrator, Senna Spy FTP server, Traitor 21, WebEx, WinCrash
22	TCP	Shaft
23	TCP	Fire HacKer, Tiny Telnet Server - TTS, Truva Atl
25	TCP	Ajan, Antigen, BSE Trojan, Email Password Sender - EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Tapiras, Terminator, WinPC, W inSp
31	TCP	Agent 31, Hackers Paradise, Masters Paradise
39	TCP	SubSARI
41	TCP	Deep Throat, Foreplay or Reduced Foreplay
44	TCP	Artic
48	TCP	DRAT
50	TCP	DRAT
58	TCP	DMSetup
59	TCP	DMSetup
79	TCP	CDK, Firehotcker
80	TCP	AckCmd, Ba ck End, CGI Backdoor, Executor, Hooker, RingZero
81	TCP	RemoConChubo
99	TCP	Hidden
110	TCP	ProMail trojan
113	TCP	Invisible Identd Deamon, Kazimas
119	TCP	Happy99
121	TCP	JammerKillah
123	TCP	Net Controller
133	TCP	Farnaz
142	TCP	NetTaxi
146	TCP	Infector
146	UDP	Infector
170	TCP	A-trojan

334	TCP	Backage
420	TCP	Breach
421	TCP	TCP Wrappers trojan
456	TCP	Hackers Paradise
513	TCP	Grlogin
514	TCP	RPC Backdoor
531	TCP	Rasmin
555	TCP	Ini-Killer , Net Ad ministrator, Phase Zero, Phase -0, Stealth Spy
605	TCP	Secret Service
666	TCP	Attack FTP, Back Construction, Cain & Abel, NokNok, Satans Back Door - SBD, ServU, Shadow Phyre
667	TCP	SniperNet
669	TCP	DP trojan
692	TCP	GayOL
777	TCP	AimSpy, Undetected
808	TCP	WinHole
911	UDP	Dark Shadow
911	TCP	Dark Shadow
999	TCP	Deep Throat, Foreplay or Reduced Foreplay, WinSatan
1000	TCP	Der Späher / Der Spaeher
1001	TCP	Data Theef, Der Späher / Der Spaeher, Le Guardien, Silencer, WebEx
1010	TCP	Doly Trojan v1.35
1011	TCP	Doly Trojan
1012	TCP	Doly Trojan
1015	TCP	Doly Trojan
1016	TCP	Doly Trojan v1.5
1020	TCP	Vampire
1024	TCP	NetSpy, Latinus
1031	TCP	Xanadu
1042	TCP	BLA trojan
1045	TCP	Rasmin
1049	TCP	/sbin/initd
1050	TCP	MiniCommand
1054	TCP	AckCmd
1080	TCP	WinHole
1081	TCP	WinHole
1082	TCP	WinHole
1083	TCP	WinHole
1090	TCP	Xtreme
1095	TCP	Remote Administration Tool - RAT
1097	TCP	Remote Administration Tool - RAT
1098	TCP	Remote Administration Tool - RAT
1099	TCP	Blood Fest Evolution, Remote Administration Tool - RAT
1170	TCP	Psyber Stream Server - PSS, Streaming Audio Server, Voice
1200	UDP	NoBackO
1201	UDP	NoBackO
1207	TCP	SoftWAR
1212	TCP	Kaos, Stealth Proxy [I] (hidden Socks4/5 Proxy server)
1234	TCP	Ultors Trojan
1243	TCP	BackDoor-G, SubSeven , SubSeven Apocalypse, Tiles
1245	TCP	VooDoo Doll, NetBus, GabanBus
1255	TCP	Scarab
1256	TCP	Project nEXT
1269	TCP	Matrix
1313	TCP	NETrojan
1338	TCP	Millenium Worm
1349	TCP	Bo dll

1386	TCP	Dagger
1492	TCP	FTP99CMP
1509	TCP	Psyber Streaming Server
1524	TCP	Trin00
1600	TCP	Shivka-Burka
1777	TCP	Scarab
1807	TCP	SpySender
1966	TCP	Fake FTP
1969	TCP	OpC BO
1981	TCP	Bowl, Shockrave
1999	TCP	Back Door, TransScout
2000	TCP	Der Späher / Der Spaeher, Insane Network
2001	TCP	Der Späher / Der Spaeher, TrojanCow
2023	TCP	Ripper Pro
2080	TCP	WinHole
2115	TCP	Bugs
2140	TCP	The Invasor
2140	UDP	Deep Throat, Fore play or Reduced Foreplay
2155	TCP	Illusion Mailer
2255	TCP	Nirvana
2283	TCP	HVL RAT5
2300	TCP	Xplorer
2339	TCP	Voice Spy (Contact)
2339	UDP	Voice Spy
2345	TCP	Doly Trojan
2565	TCP	Striker trojan
2583	TCP	WinCrash
2589	TCP	Dagger
2600	TCP	Digital RootBeer
2716	TCP	The Prayer
2773	TCP	SubSeven , SubSeven 2.1 Gold
2801	TCP	Phineas Phucker
2989	UDP	Remote Administration Tool - RAT
3000	TCP	Remote Shut
3024	TCP	WinCrash
3128	TCP	RingZero
3129	TCP	Masters Par adise
3131	TCP	SubSARI
3150	TCP	The Invasor
3150	UDP	Deep Throat, Foreplay or Reduced Foreplay
3456	TCP	Terror trojan
3459	TCP	Eclipse 2000, Sanctuary
3700	TCP	Portal of Doom - POD
3791	TCP	Total Solar Eclypse
3801	TCP	Total Solar Ec lypse
4000	TCP	Skydance (newer versions run ICMP)
4092	TCP	WinCrash
4201	TCP	War Trojan
4242	TCP	Virtual Hacking Machine - VHM
4321	TCP	BoBo
4444	TCP	Prosiak, Swift Remote
4567	TCP	File Nail
4590	TCP	ICQ Trojan
4950	TCP	ICQ Trogen (Lm)
5000	TCP	Back Door Setup, Blazer5, Bubbel, ICKiller, Sockets des Troie, BioNet (lite 1.0)
5001	TCP	Back Door Setup, Sockets des Troie
5002	TCP	cd00r, Shaft

5010	TCP	Solo
5011	TCP	One of the Last Trojans - OOTLT, One of the Last Trojans - OOTLT, modified
5025	TCP	WM Remote KeyLogger
5031	TCP	Net Metropolitan
5032	TCP	Net Metropolitan
5321	TCP	Firehotcker
5343	TCP	WCrat - WC Remote Administration Tool
5400	TCP	Back Construction, Blade Runner
5401	TCP	Back Construction, B lade Runner 1
5402	TCP	Back Construction, Blade Runner 2
5512	TCP	Illusion Mailer
5550	TCP	Xtcp
5555	TCP	ServeMe
5556	TCP	BO Facil
5557	TCP	BO Facil
5569	TCP	Robo-Hack
5637	TCP	PC Crasher
5638	TCP	PC Crasher
5742	TCP	WinCrash
5760	TCP	Portmap Remote Root Linux Exploit
5882	UDP	Y3K RAT
5888	TCP	Y3K RAT
6000	TCP	The Thing
6006	TCP	Bad Blood
6272	TCP	Secret Service
6400	TCP	The Thing
6666	TCP	Dark Connection Inside, NetBus worm
6667	TCP	ScheduleAgent, Trin ity, WinSatan
6669	TCP	Host Control, Vampire
6670	TCP	BackWeb Server, Deep Throat, Foreplay or Reduced Foreplay, WinNuke eXtreame
6711	TCP	BackDoor-G, SubSeven , VP Killer, SubSARI
6712	TCP	Funny trojan, SubSeven
6713	TCP	SubSeven
6723	TCP	Mstream
6771	TCP	Deep Throat, Foreplay or Reduced Foreplay
6776	TCP	2000 Cracks, BackDoor -G, SubSeven , VP Killer
6838	UDP	Mstream
6883	TCP	Delta Source DarkStar (??)
6912	TCP	Shit Heep
6939	TCP	Indoctrination
6969	TCP	GateCrasher, IR C 3, Net Controller, Priority
6970	TCP	GateCrasher
7000	TCP	Exploit Translation Server, Kazimas, Remote Grab, SubSeven 2.1 Gold
7001	TCP	Freak88
7215	TCP	SubSeven , SubSeven 2.1 Gold
7300	TCP	NetMonitor
7301	TCP	NetMonitor 1
7306	TCP	NetMonitor
7307	TCP	NetMonitor 3
7308	TCP	NetMonitor 4
7424	TCP	Host Control
7424	UDP	Host Control
7597	TCP	Qaz
7626	TCP	Glacier Backdoor
7777	TCP	Tini
7789	TCP	Back Door Setup, ICKiller
7983	TCP	Mstream

8080	TCP	Brown Orifice , Re moConChubo, RingZero
8787	TCP	Back Orifice 2000
8988	TCP	BacHack
8989	TCP	Rcon, Recon, Xcon
9000	TCP	Netministrator
9325	UDP	Mstream
9400	TCP	InCommand
9872	TCP	Portal of Doom - POD
9873	TCP	Portal of Doom - POD 1
9874	TCP	Portal of Doom - POD 2
9875	TCP	Portal of Doom - POD 3
9876	TCP	Cyber Attacker, Rux
9878	TCP	TransScout
9989	TCP	Ini-Killer
9999	TCP	The Prayer
10067	UDP	Portal of Doom - POD 4
10085	TCP	Syphillis
10086	TCP	Syphillis
10100	TCP	Gift
10101	TCP	BrainSpy
10167	UDP	Portal of Doom - POD 5
10520	TCP	Acid Shivers
10528	TCP	Host Control
10607	TCP	Coma
10666	UDP	Ambush
11000	TCP	Senna Spy Trojan Generator
11050	TCP	Host Control
11051	TCP	Host Control
11223	TCP	Progenic troj an, Secret Agent
12076	TCP	Gjamer
12223	TCP	Hack´99 KeyLogger
12310	TCP	Precursor
12345	TCP	Cron / crontab, Fat Bitch trojan, GabanBus, icmp_pipe.c, Mypic , NetBus , NetBus Toy, NetBus worm, Pie Bill Gates, VaLV -N.E.t, Whack Job, X -bill
12346	TCP	Fat Bitch trojan, GabanBus, NetBus , X -bill
12349	TCP	BioNet
12361	TCP	Whack-a-mole
12362	TCP	Whack-a-mole
12623	UDP	DUN Control
12624	TCP	ButtMan
12631	TCP	Whack Job
12754	TCP	Mstream
13000	TCP	Senna Spy Trojan Generator
13010	TCP	Hacker Brasil - HBR
14500	TCP	PC Invader
15092	TCP	Host Control
15104	TCP	Mstream
15382	TCP	Sub7 (old beta)
15858	TCP	CDK
16484	TCP	Mosucker
16660	TCP	Stacheldraht
16772	TCP	ICQ Revenge
16969	TCP	Priority
17166	TCP	Mosaic
17300	TCP	Kuang2 the virus
17449	TCP	Kid Terror
17499	TCP	CrazzyNet

17777	TCP	Nephron
18753	UDP	Shaft
19864	TCP	ICQ Revenge
20000	TCP	Millenium
20001	TCP	Millenium, Millenium (Lm)
20002	TCP	AcidkoR
20005	TCP	MoSucker
20023	TCP	VP Killer
20034	TCP	NetBus 2.0 Pro, NetRex, Whack Job
20331	TCP	BLA trojan
20432	TCP	Shaft
20433	UDP	Shaft
21544	TCP	GirlFriend, Kid Terror
21554	TCP	Exploiter, Kid Terror, Schwindler, Winsp00fer, Exploiter, Freddy
22222	TCP	Donald Dick, Prosiak
23005	TCP	NetTrash
23023	TCP	Logged
23032	TCP	Amanda
23432	TCP	Asylum
23456	TCP	Evil FTP, Ugly FTP, Whack Job
23476	TCP	Donald Dick
23476	UDP	Donald Dick
23477	TCP	Donald Dick
26274	UDP	Delta Source
26681	TCP	Voice Spy - OBS!!! namnen har bytt plats
27374	TCP	Bad Blood, DefCon 8, Lion Worm (no trojan it's a worm), Ramen Worm (no trojan it's a worm) Sub7 , Sub7 2.1 Gold, Sub7 2.1.4, Sub7 2.2
27444	UDP	Trin00 master to deamon communication
27573	TCP	SubSeven
27665	TCP	Trin00 attacker to master
29104	TCP	NetTrojan
29891	TCP	The Unexplained
30001	TCP	ErrOr32
30003	TCP	Lamers Death
30029	TCP	AOL trojan
30100	TCP	NetSphere
30101	TCP	NetSphere
30102	TCP	NetSphere
30103	TCP	NetSphere
30103	UDP	NetSphere
30129	TCP	Masters Paradise
30133	TCP	NetSphere
30303	TCP	Sockets des Troie , Socket23
30700	TCP	Mantis by Shaban
30947	TCP	Intruse
30999	TCP	Kuang2
31335	UDP	Trin00 deamon communication to master
31336	TCP	Bo Whack , Butt Funnel
31337	TCP	Back Fire, Back Orifice (Lm), Back Orifice russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, cron / crontab, Freak88, icmp_pipe.c, Sockdmini
31337	UDP	Back Orifice, Deep BO
31338	TCP	Back Orifice, Butt F unnel, DK NetSpy
31338	UDP	Deep BO, DK NetSpy
31339	TCP	DK NetSpy
31339	UDP	DK NetSpy
31557	TCP	Xanadu
31666	TCP	BOWhack
31785	TCP	Hack´a´Tack

31788	TCP	Hack´a´Tack
31789	UDP	Hack´a´Tack
31790	TCP	Hack´a´Tack
31791	UDP	Hack´a´Tack
31792	TCP	Hack´a´Tack
32001	TCP	Donald Dick
32100	TCP	Peanut Brittle, Project nEXT
32418	TCP	Acid Battery
33270	TCP	Trinity v.3
33333	TCP	Blakharaz, Prosiak
33567	TCP	Lion Worm backdoor Root Shell
33568	TCP	Lion Worm trojan SSH daem on
33577	TCP	PsychWard
33777	TCP	PsychWard
33911	TCP	Spirit 2000, Spirit 2001
34324	TCP	Big Gluck, TN , Tiny Telnet Server
34444	TCP	Donald Dick
34555	UDP	Trin00 (for Windows)
35555	UDP	Trin00 (for Windows)
37651	TCP	Yet Another Troja n - YAT
39168	TCP	Trinity v.3
40412	TCP	The Spy
40421	TCP	Agent 40421, Masters Paradise
40422	TCP	Masters Paradise 1
40423	TCP	Masters Paradise 2
40426	TCP	Masters Paradise 3
41666	TCP	Remote Boot Tool - RBT, Remote Boot Tool - RBT
44444	TCP	Prosiak
47262	UDP	Delta Source
50000	TCP	SubSARI
50505	TCP	Sockets des Troie
50766	TCP	Fore, Schwindler
51966	TCP	Cafeini
52317	TCP	Acid Battery 2000
53001	TCP	Remote Windows Shutdown - RWS
54283	TCP	SubSeven , SubSeven 2.1 Gol d
54320	TCP	Back Orifice 2000
54321	TCP	Back Orifice 2000, School Bus
55555	TCP	B02k, Eurocalculator
55850	TCP	MyServer DDoS Agent
57341	TCP	NetRaider
58339	TCP	Butt Funnel
60000	TCP	Deep Throat, Foreplay or Reduced Foreplay, Sockets des Troie
60008	TCP	Lion Worm Root Shell (t0rn rootkit)
60068	TCP	Xzip 6000068
60411	TCP	Connection
61348	TCP	Bunker-Hill
61466	TCP	TeleCommando
61603	TCP	Bunker-Hill
63485	TCP	Bunker-Hill
64101	TCP	Taskman / Task Manager
65000	TCP	Devil, Sockets des Troie, Stacheldraht
65432	TCP	The Traitor (= th3tr41t0r)
65432	UDP	The Traitor (= th3tr41t0r)
65534	TCP	/sbin/initd
65535	TCP	RC1 trojan (Remote Control)

Second reminder: The full Correlation and comparation with well known ports/services is included in the zip file and perhaps edited for webformat at the sans website(?).

Sources:
http://www.sys -security.com/html/papers/trojan_list.html
http://www.sans.org/newlook/resources/IDFAQ/oddports.htm
http://www.simovits.com/trojan s/
http://dark -e.com/archive/trojans/
http://www.certcc.or.kr/advisory/
http://www.dark -e.com/cgi -bin/quiz.cgi
http://www.zonelabs.com/knowledgebase/trojanports.html
http://www.multimania.com/cdc/trojanh.htm

One link that seems to hold additional correlat ion with other ports is
http://www.lost.net.au/~ben/ports
the deadline and me being out of office/labs couldnt make me include any trojans listed there.

Assignment 3

Analyse This

[I am assuming this is a un iversity network]

Executive Summary:

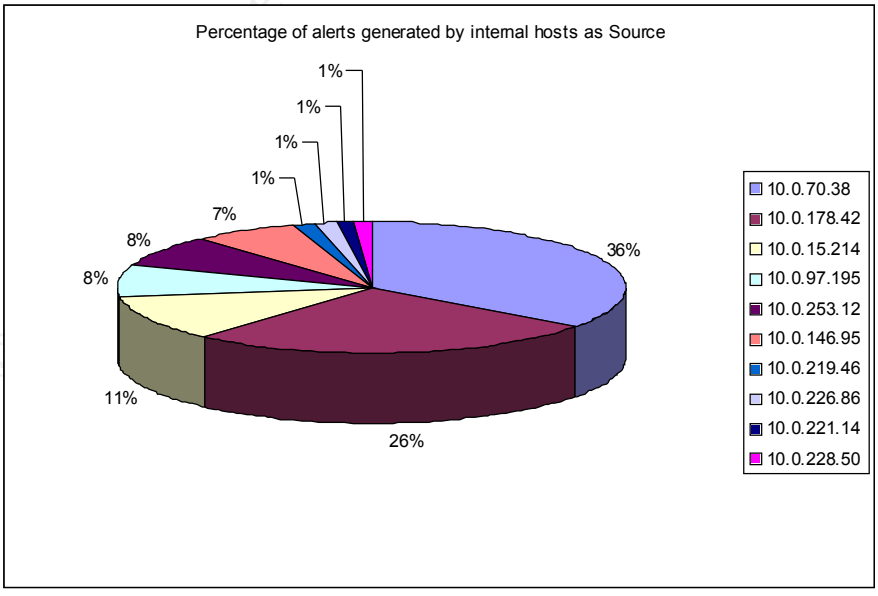
What you are dealing with here is massive problems and a very open network. The point that is most interesting is the spread of attacks on various networks. Perhaps some institutions still have their own support perso nal and in some cases there are dorms running wild during times where there are not finals coming up. I have seen this before and at the end you will find some projects recommended. The projects should be **considered** doing already this budget year. Most of the tools needed can be provided with no installation/license costs if Freeware/Open Source is used, other then the time needed.

But before assigning personnel and resources on those projects let me summarize the technical details listed below.

Likely you have been hacked by people from the outside.
Likely your policies are failing in some institutions where malicious activity is originating from.
We have various malicious activity inside ranging from Portscanning to Trojans.

Trojans can be used by stu dents to steal/plagiarize other students work and worse!

At the end of the report you will find diagrams and statistics that can be useful for knowing where to start the work. I will include one diagram here for easy viewing of internal hosts as the source of alert.



Analyze this, findings

Working with a security audit for a university is always a challenge since there is often loose rulesets on the eventual firewalls compared to my own environment. Several of the log files where available for me but not the architecture and layout of the site. However i the previous work on the net did help me out.

The analysis process i used was to combine the strength of UNIX in its places (sorting and getting humanreadable data), while using Microsoft Office for t he representation of it. As a attempt to get to know what kind of arena we where talking about here i used the excellent perlscripts by Chris Kuethe (his work is linked from the GCIA Analysts page http://www.sans.org/y2k/practical/chris_kuethe_gcia.html).

Alerts from 2001 -03-01-> 2001-07-13 (redid this procedure on 2001 -07-15 for updated analysis)

```
bash-2.05# perl -s /home/my_nick/prog/alertcount.pl -t /home/gcia/alert.*
>./total && sort -nr ./total > ./sorted2
```

Produced this data:
(please also look in t he diagram section which has exluded the outside network)

3495193	UDP SRC and DST outside network	83,47365%
229542	Watchlist 000220 IL -ISDNNET -990517	5,48202%
160686	Possible trojan server activity	3,83757%
46046	SYN-FIN scan!	1,09969%
37030	WinGate 1 080 Attempt	0,88437%
33057	High port 65535 udp - possible Red Worm – traffic	0,78948%
32004	Attempted Sun RPC high port access	0,76433%
31224	Russia Dynamo - SANS Flash 28 -jul-00	0,74570%
27723	External RPC call	0,66209%
17407	High port 65535 tcp - possible Red Worm – traffic	0,41572%
17144	SMB Name Wildcard	0,40944%
11956	Possible RAMEN server activity	0,28554%
10967	Connect to 515 from outside	0,26192%
9564	Port 55850 tcp - Possible myserver activity - ref. 010313 -1	0,22841%
7425	Tiny Fragments - Possible Hostile Activity	0,17733%
6617	Queso fingerprint	0,15803%
4864	Watchlist 000222 NET -NCFC	0,11616%
3029	SUNRPC highport access!	0,07234%
2033	TCP SRC and DST outside network	0,04855%
1696	Back Orifice	0,04050%
920	Null scan!	0,02197%
614	NMAP TCP ping!	0,01466%
196	ICMP SRC and DST outside network	0,00468%
133	Connect to 515 from inside	0,00318%
54	SNMP public access	0,00129%
21	Probable NMAP fingerprint attempt	0,00050%
13	STATDX UDP attack	0,00031%
11	TCP SMTP Source Port traffic	0,00026%
8	SITE EXEC - Possible wu -ftpd exploit - GIAC000623	0,00019%
2	Broadcast Ping to subnet 70	0,00005%
1	hax0r boy 010615	0,00002%
1	Happy 99 Virus	0,00002%

As i saw it was a limited inventory of unique kinds of events. My first priority was to a nalyze the trojans and virus attacks. I did that judgement based on that "we got hackers" possibly inside the network already. That one event of "hax0r boy 010615" got me particularly interested on what it was, its not in the snort rule set.

I made a big logfile of alertfile then substituted My.NET to 192.168 with sed ("cat bigfile | sed s/MY.NET/10.0/g") Redid this to 10.0 after realizing that 192.168.*** .*** was in use from another internal network.

I tried Snortsnarf on the files for further simpli fied analysis but could not get all days into the same statistics due to snortsnarfs heavy memory usage. I did however get them in one by one in a browsable directory.

WinGate 1080 Attempt

A search/connection attempt for WinGate (usually runs on port 1080). If a cracker where to use this, in the victims log the Wingate machine would show up not revealing the crackers true [read: previous] IP-Address.

High port 65535 udp possible Red Worm - traffic

Red Worm could compromise Linux hosts installing back door access, but this port is also used by Remote Control (RC Trojan).

During April there seems to be alot of traffic being generated from 10.0.253.12 examples below

```
04/04-09:22:26.908922  [**] High port 65535 tcp - possible Red Worm - traffic [**]
10.0.253.12:47193 -> 10.0.59.131:65535
04/04-09:22:30.818622  [**] High port 65535 tcp - possible Red Worm - traffic [**]
10.0.253.12:47196 -> 10.0.59.132:65535
[note that the capture above is TCP based, it could be internal scans for the worm]
```

Russia Dynamo

Although alittle undocumented this seems to be a trojan/virus with the ability to "phone home".

194.87.6.33 has valid reverse DNS of 33.6.87.194.dynamic.dol.ru

194.87.6.189 has valid reverse DNS of 189.6.87.194.dynamic.dol.ru

194.87.6.21 has valid reverse DNS of 21.6.87.194.dynamic.dol.ru

Using some different ports 1596, 1598, 316, 317 2226 2233, 2234 (and others) but
316-317 seems to be sending/receiving port at the hacked side
It seems somewhat "crafted"… 10.0.178.42 responds to 194.87.6.21

Example of different ports:

```
04/09-00:22:47.392083  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:2227
04/09-00:22:51.390345  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:317 ->
194.87.6.106:2222
```

```
04/09-00:22:51.418620  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:2229
04/09-00:22:55.980801  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:2231
04/09-00:22:56.518739  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:317 ->
194.87.6.106:2222
04/09-00:23:01.228070  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:2233
04/09-00:23:01.566307  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:2233
04/09-00:23:01.566593  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:2233
04/09-00:23:03.774136  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:317 ->
194.87.6.106:2222
04/09-00:23:05.840195  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:2234
```

The attacker stops at an earlier point

```
04/06-18:41:08.075705  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1094
04/06-18:41:09.807090  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1094
04/06-18:41:09.809037  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1094
04/06-18:41:09.809247  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1094
04/06-18:41:12.029163  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1094
04/06-18:41:12.029405  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1094
04/06-18:41:12.029694  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1094
04/06-18:41:12.476418  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1094
```

And resumes again

```
04/06-20:07:58.026064  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1256
04/06-20:07:58.441197  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1256
04/06-20:07:58.441700  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1256
04/06-20:08:00.361982  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.106:1256 ->
10.0.178.42:316
04/06-20:08:01.515631  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1256
04/06-20:08:05.246483  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1256
04/06-20:08:07.950065  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.106:1256 ->
10.0.178.42:316
04/06-20:08:10.065797  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.106:1256 ->
10.0.178.42:316
04/06-20:08:10.339432  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1256
04/06-20:08:12.273942  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.106:1256 ->
10.0.178.42:316
04/06-20:08:14.837635  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1256
04/06-20:08:15.812275  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.106:1256 ->
10.0.178.42:316
04/06-20:08:15.815564  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:316 ->
194.87.6.106:1256
```

There is a stop over some time aswell

```
04/28-09:01:24.401167  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.144:2074 ->
10.0.218.86:6700
04/28-09:01:32.992812  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.144:2074 ->
10.0.218.86:6700
04/28-09:01:32.992858  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.144:2074 ->
10.0.218.86:6700
```

```
04/28-09:01:32.992904  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.144:2074 ->
10.0.218.86:6700
04/28-09:01:32.992948  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.144:2074 ->
10.0.218.86:6700
04/28-09:01:32.992993  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.144:2074 ->
10.0.218.86:6700
05/16-20:16:08.430781  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:317 ->
194.87.6.45:1551
05/16-20:16:39.746815  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:317 ->
194.87.6.45:1563
05/16-20:16:40.933776  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:317 ->
194.87.6.45:1564
05/16-20:16:44.105137  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 10.0.178.42:317 ->
194.87.6.45:1565
```

Alot of the activity was under April but i still recommend looking into the above host for furt her analysis.

External RPC call

Programs using RPC (Remote Procedure Calls has had a troublesome history and usually they are blocked at firewalls. These connections are not to be taken lightly, because alot of exploit code exist for various platforms. Also see the note about Sun RPC high port access.

SMB Name Wildcard

On port 137 Windows machines in a network communication is interchanged about machinenames and users. A wildcard could potentially give out everyhost/user on the network in question. This is for recon not intrusion. Not that high risk.

Possible RAMEN server activity

Ramen is a Worm infecting Red Hat 6.2 and 7.0. It is using vulnerabilities in LPRng, rpc statd and wu-ftp. It leaves a server running on port 27374 distributing itself furt her.
More information available on www.sans.org/y2k/ramen.htm

Connect to 515 from outside

Port 515, a well-known port LPRng for printing services, could be used for intruders to exploit this service for information leaks and various denial of service at tacks (removing printques for example). If there exist any holes in this service a rootshell could be dropped to the attacker.

There is some strange activity here though that I would advise you to drop at a previous router

```
05/17-14:21:37.151619  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.137.92:515
05/25-00:22:48.795281  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.133.109:515
05/26-22:40:40.877276  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.137.175:515
05/27-06:01:33.056576  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.132.129:515
05/27-11:43:09.224530  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.135.77:515
05/29-05:25:41.292060  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.132.62:515
05/30-11:49:59.466081  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.137.204:515
05/31-02:13:05.254837  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.132.180:515
06/01-03:15:40.778816  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.137.60:515
```

```
06/01-22:48:22.674710  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.132.117:515
06/02-09:03:16.407159  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.137.123:515
06/02-20:45:09.154901  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.132.197:515
06/03-14:36:30.623742  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.132.32:515
06/04-09:56:22.301178  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.132.51:515
06/07-11:08:36.127132  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.137.19:515
06/10-12:15:47.342416  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.133.82:515
06/10-14:38:46.978955  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.133.216:515
06/11-17:34:16.983125  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.133.42:515
```

255.255.255.255 is **NOT** a valid IP adress, although scriptkiddies sometimes thinks it would make a huge ping for the whole internet. (this isnt the case). This is a crafted packet

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

Could be a backdoor for Linux systems, shutting down some services and replacing 'ls' and 'ps' with its own versions. Im honestly not that familiar with it, it is listed in my trojan list on this port. I recommend further reading on the following UR L

http://lists.insecure.org/incidents/2000/Oct/0141.html

Its purpose should be "a Trinoo -style tool called MyServer on their linux box"
Information from
http://www.google.com/search?q=cache:d9xVEpq0_pc:www.sans.org/y2k/082200.htm++myserver+55850&hl=sv

Tiny Fragments - Possible Hostile Activity

Many tiny fragments can cause denial of service on some Microsoft Window machines. These small fragments may also be used to "fooled" to let it pass through firewalls since thier length could be below minimum fragments size for certain filters.

Queso fingerprint

A program used for fingerprinting networked machines without the 3 -way handshake.

Attempted Sun RPC high port access

This is a scan for ephemeral ports using the direct port instead of via the portmapper to find out the port number(portmapper usually runs on port 111). Although SUN themself have not released the full information about thi s issue ("any day now" since a while back). I belive that these ports arre primarily used for internal usage. Firewalling them would be recommended.

Back Orifice

Port 31337 is always kind of interesting to look and search for, it is Elite for these crack ers to use this port and in several cases I have seen this port being used for various services. In the Snort logs we can see various scans for this port. Back to the subject: Back Orifice much like NetBus

are trojans that can be used for remote administra tion. It was a popular backdoor in 1998 but nowadays I havent seen much BO activity. Sub7 is the trojan that gets most attention now. BO is however very potentially dangerous!!! But most Antiviral software can deal with it pretty easily.

Some correlation can however be made….

```
03/13-22:24:56.749614  [**] connect to 515 from outside [**] 209.112.47.7:31337 ->
10.0.135.120:515
04/14-09:31:24.834984  [**] connect to 515 from outside [**] 210.61.82.20:31337 ->
10.0.133.194:515
04/23-09:29:14.420358  [**] connect to 515 from outside [**] 255.255.255.255:31337 ->
10.0.137.174:515
04/27-03:55:03.830585  [**] connect to 515 from outside [**] 207.18.175.10:31337 ->
10.0.134.71:515
```

My question… is it 31337 with print spoolers? the paperless society isnt already here ???

Null Scan

These are scans (maybe from nmap) with no TCP flags set. See in the detects for a similar practical example. These packages should never exist in the normal communication so they are crafted in someway.

NMAP TCP ping

Sort of like a ping but using TCP with a ack instead of ICMP Echo. A recon scans for open services. As an example we can see this search for ftp sites:

```
04/03-07:56:46.541493  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.144:21
04/03-07:58:12.029339  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.149:21
04/03-07:58:17.742633  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.149:21
04/03-08:00:25.709372  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.156:21
04/03-08:02:17.099803  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.169:21
04/03-08:03:12.754353  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.172:21
04/03-08:04:01.048707  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.175:21
04/03-08:04:07.628942  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.175:21
04/03-08:05:57.237796  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.181:21
04/03-08:06:42.223664  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.183:21
04/03-08:07:18.570074  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.185:21
04/03-08:07:25.919783  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.185:21
04/03-08:08:01.014153  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.188:21
04/03-08:08:50.611628  [**] NMAP TCP ping! [**] 217.3.182.110:43186 -> 10.0.53.191:21
```

Speaking of scans I have not placed that much energy in the portscans but 211.240.28.66 seems to have scanned quite a bit in beginning of June.

SNMP public access

Scans against Simple Network Ma nagement Protocol (SNMP), UDP port 161. SNMP is a protocol that is used to pass information about network equipment such as routers switches. An intruder can use this information to gather valuable information about networks, which could be used in an attack at a later date. These should definitely be blocked at a firewall.

Probable NMAP fingerprint attemtp

Nmap as mentioned above can be used as a networkfinger printing program. However, snort can be used as a "nmap fingerprinter program" from its partic ular habits in scanning. So the 21 detects here are highly likely to have been using nmap as there scanning device.

Just making one example here from internal hosts

```
06/09-17:43:32.486337  [**] Probable NMAP fingerprint attempt [**] 10.0.100.65:62178 ->
10.0.101.141:7
```

STATDX UDP attack

STATDX exploits rpc.statd, statd itself is demanded to get a functioning NFS session and the connections are usually made via the portmapper.

```
04/07-08:34:23.517421  [**] STATDX UDP attack [**] 212.131.172.130:669 -> 10.0.6.15:32776
04/10-02:44:07.761846  [**] STATDX UDP attack [**] 24.43.176.96:2099 -> 10.0.6.15:32776
05/13-17:25:23.747462  [**] STATDX UDP attack [**] 24.12.85.103:1016 -> 10.0.6.15:32776
05/25-13:26:13.548623  [**] STATDX UDP attack [**] 213.66.5.79:707 -> 10.0.6.15:32776
05/25-21:34:55.164114  [**] STATDX UDP attack [**] 209.247.88.12:859 -> 10.0.6.15:32776
06/12-19:32:18.546477  [**] STATDX UDP attack [**] 129.49.65.82:1014 -> 10.0.6.15:32776
06/21-13:00:24.763749  [**] STATDX UDP attack [**] 139.142.135.118:717 -> 10.0.6.15:32776
06/22-23:44:51.058551  [**] STATDX UDP attack [**] 210.107.198.164:973 -> 10.0.6.15:32776
06/25-22:53:16.464836  [**] STATDX UDP attack [**] 212.209.79.162:717 -> 10.0.6.15:32776
06/26-05:14:35.459849  [**] STATDX UDP attack [**] 212.209.79.162:620 -> 10.0.6.15:32776
06/30-12:17:02.869023  [**] STATDX UDP attack [**] 210.90.168.5:836 -> 10.0.6.15:32776
07/01-09:00:37.454441  [**] STATDX UDP attack [**] 211.23.6.234:835 -> 10.0.6.15:32776
07/13-03:50:33.248147  [**] STATDX UDP attack [**] 210.223.52.151:741 -> 10.0.6.15:32776
```

Looking further from attacks from 24.43.176.96 you see him in some portmapper scannings aswell, example:

```
04/09-16:39:00.095674  [**] External RPC call [**] 24.43.176.96:3438 -> 10.0.134.210:111
04/09-16:39:00.118155  [**] External RPC call [**] 24.43.176.96:3441 -> 10.0.134.213:111
04/09-16:39:00.826378  [**] External RPC call [**] 24.43.176.96:3540 -> 10.0.135.56:111
04/09-16:39:00.883688  [**] External RPC call [**] 24.43.176.96:3548 -> 10.0.135.64:111
```

And some portscans aswell

```
04/09-16:53:48.211369  [**] spp_portscan: portscan status from 24.43.176.96: 15 connections
across 15 hosts: TCP(15), UDP(0) [**]
04/09-16:53:50.734537  [**] spp_portscan: End of portscan from 24.43.176.96 (TOTAL HOSTS:54
TCP:56 UDP:0) [**]
```

I assume that 24.12.85.103 is in some way relating to this individual and look at alerts from this host. He has a similar “trackrecord” the following month

```
05/13-17:26:57.596230  [**] External RPC call [**] 24.12.85.103:2932 -> 10.0.132.22:111
05/13-17:26:57.650085  [**] External RPC call [**] 24.12.85.103:2941 -> 10.0.132.31:111
05/13-17:26:57.878334  [**] External RPC call [**] 24.12.85.103:2977 -> 10.0.132.67:111
05/13-17:26:57.985854  [**] External RPC call [**] 24.12.85.103:3103 -> 10.0.132.193:111
05/13-17:26:57.997435  [**] External RPC call [**] 24.12.85.103:3105 -> 10.0.132.195:111
05/13-17:26:58.368244  [**] External RPC call [**] 24.12.85.103:3293 -> 10.0.133.128:111
05/13-17:26:58.781355  [**] External RPC call [**] 24.12.85.103:3406 -> 10.0.133.241:111
05/13-17:41:11.447819  [**] spp_portscan: PORTSCAN DETECTED from 24.12.85.103 (THRESHOLD 7
connections in 2 seconds) [**]
05/13-17:26:58.893185  [**] External RPC call [**] 24.12.85.103:3426 -> 10.0.134.6:111
05/13-17:26:58.928998  [**] External RPC call [**] 24.12.85.103:3432 -> 10.0.134.12:111
05/13-17:26:59.406011  [**] External RPC call [**] 24.12.85.103:3633 -> 10.0.134.213:111
05/13-17:26:59.467621  [**] External RPC call [**] 24.12.85.103:3643 -> 10.0.134.223:111
05/13-17:26:59.856202  [**] External RPC call [**] 24.12.85.103:3836 -> 10.0.135.161:111
05/13-17:26:59.867819  [**] External RPC call [**] 24.12.85.103:3838 -> 10.0.135.163:111
05/13-17:27:00.083553  [**] External RPC call [**] 24.12.85.103:3873 -> 10.0.135.198:111
05/13-17:27:00.268393  [**] External RPC call [**] 24.12.85.103:3879 -> 10.0.135.204:111
05/13-17:27:00.558761  [**] External RPC call [**] 24.12.85.103:3925 -> 10.0.135.250:111
05/13-17:41:13.373415  [**] spp_portscan: portscan status from 24.12.85.103: 16 connections
across 16 hosts: TCP(16), UDP(0) [**]
05/13-17:27:01.692126  [**] External RPC call [**] 24.12.85.103:4352 -> 10.0.137.167:111
05/13-17:27:01.728228  [**] External RPC call [**] 24.12.85.103:4358 -> 10.0.137.173:111
05/13-17:27:01.756704  [**] External RPC call [**] 24.12.85.103:4362 -> 10.0.137.177:111
05/13-17:27:01.940867  [**] External RPC call [**] 24.12.85.103:4392 -> 10.0.137.207:111
05/13-17:27:01.958587  [**] External RPC call [**] 24.12.85.103:4394 -> 10.0.137.209:111
05/13-17:27:01.981864  [**] External RPC call [**] 24.12.85.103:4398 -> 10.0.137.213:111
05/13-17:41:15.668962  [**] spp_portscan: portscan status from 24.12.85.103: 6 connections across
6 hosts: TCP(6), UDP(0) [**]
```

```
05/13-17:41:18.196608  [**] spp_portscan: End of portscan from 24.12.85.103 (TOTAL HOSTS:21
TCP:22 UDP:0) [**]
```

I also assumed that patterns are alike for the other attackers. But here is something interesting!

```
05/25-13:26:13.003934  [**] External RPC call [**] 213.66.5.79:2402 -> 10.0.6.15:111
05/25-13:26:13.548623  [**] STATDX UDP attack [**] 213.66.5.79:707 -> 10.0.6.15:32776
05/25-13:26:14.095402  [**] External RPC call [**] 213.66.5.79:2402 -> 10.0.6.15:111

05/25-21:34:55.064589  [**] External RPC call [**] 209.247.88.12:2857 -> 10.0.6.15:111
05/25-21:34:55.164114  [**] STATDX UDP attack [**] 209.247.88.12:859 -> 10.0.6.15:32776
```

I highly recommend analyzing this host: 10.0.6.15, also see in the Link Diagram for more information.

TCP SMTP Source Port traffic

```
03/20-18:35:12.740918  [**] TCP SMTP Source Port traffic [**] 207.175.141.6:25 -> 10.0.207.28:522
04/19-10:48:40.446704  [**] TCP SMTP Source Port traffic [**] 204.214.6.215:25 ->
10.0.201.32:1004
04/20-02:12:43.373137  [**] TCP SMTP Source Port traffic [**] 204.214.6.215:25 ->
10.0.75.134:1018
04/20-04:05:19.987554  [**] TCP SMTP Source Port traffic [**] 204.214.6.215:25 ->
10.0.138.120:1003
04/20-05:30:11.331118  [**] TCP SMTP Source Port traffic [**] 204.214.6.215:25 ->
10.0.152.179:1014
04/25-14:44:09.628978  [**] TCP SMTP Source Port traffic [**] 195.40.27.50:25 ->
10.0.161.125:1011
05/14-04:25:50.665911  [**] TCP SMTP Source Port traffic [**] 63.218.225.88:25 ->
10.0.139.54:1007
05/18-10:59:47.340244  [**] TCP SMTP Source Port traffic [**] 129.43.100.100:25 ->
10.0.253.53:281
07/03-11:16:43.255384  [**] TCP SMTP Source Port traffic [**] 207.88.135.158:25 -> 10.0.5.73:807
07/05-08:45:43.767416  [**] TCP SMTP Source Port traffic [**] 129.43.100.100:25 ->
10.0.253.52:583
07/05-08:47:04.770142  [**] TCP SMTP Source Port traffic [**] 129.43.100.100:25 ->
10.0.253.52:583
```

Perhaps I missed the boat [Swedish saying] but i dont understand why this rule alerts on external hosts. However question is why these ports connects to so many different hosts. I would recommend centralizing the smtp mail access points .

SITE EXEC – Possible wu-ftpd exploit – GIAC000623

```
03/06-16:44:02.658052  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
128.61.136.233:4705 -> 10.0.219.22:21
03/20-09:24:48.607882  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
211.120.49.163:1531 -> 10.0.179.78:21
03/20-09:24:55.961621  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
211.120.49.163:1534 -> 10.0.179.81:21
05/13-00:36:42.038299  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
200.255.65.5:4436 -> 10.0.53.10:21
05/14-09:50:25.626651  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
63.196.54.17:4122 -> 10.0.202.218:21
05/14-09:50:27.665472  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
63.196.54.17:4122 -> 10.0.202.218:21
06/10-14:32:43.133301  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
211.235.241.145:1239 -> 10.0.144.59:21
06/10-15:43:44.943254  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
211.235.241.145:1521 -> 10.0.144.59:21
```

There has been some portscans towards these hosts at port 21 I would advice you to look further into any of the above internal hosts.

One example of this came from 128.61.136.233 that shows the following log

```
03/06-16:26:23.340817  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.15:21
03/06-16:26:23.360557  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.16:21
03/06-16:26:23.620733  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.29:21
03/06-16:26:23.681285  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.32:21
03/06-16:26:24.140511  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.55:21
03/06-16:26:24.239503  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.60:21
03/06-16:26:24.281152  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.62:21
03/06-16:26:24.300564  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.63:21
03/06-16:26:24.320510  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.64:21
03/06-16:26:24.480412  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.72:21
03/06-16:26:24.660842  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.81:21
03/06-16:26:24.739300  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.85:21
03/06-16:26:25.179343  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.107:21
03/06-16:26:25.200333  [**] SYN-FIN scan! [**] 128.61.136.233:21 -> 10.0.219.108:21
03/06-16:44:02.658052  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
128.61.136.233:4705 -> 10.0.219.22:21
```

Broadcast Ping to subnet 70

This is a very unstealthy recon attempt towards subnet 70. The attacker is trying to see what hosts

```
03/03-06:19:03.144767  [**] Broadcast Ping to subnet 70 [**] 209.196.35.190 -> 10.0.70.255
03/20-21:03:46.441234  [**] Broadcast Ping to subnet 70 [**] 66.27.184.3 -> 10.0.70.255
```

Happy 99 Virus:

From Alertfile:

```
04/27-18:28:10.815753  [**] Happy 99 Virus [**] 216.49.81.253:2877 -> 10.0.6.35:25
```

Analysis:

Did a grep for more alarms from 216.49.81.253, there was none. A dig for 216.49.81.253 reveals that it seems to be a co ntentscanner for virus from McAfee in Carlifornia. My evidence in this case is that it is sends to port 25 at the network (smtp).

Conclusion:

It seems like the University subscribes to **McAfee antivirus** and that it cleaned an incoming mail, sending a varnin g back to the network in mailformat, [its a theory anyway].

hax0r boy 010615

From Alertfile:

```
06/15-18:52:45.704261  [**] hax0r boy 010615 [**] 10.0.60.11:23 -> 24.19.166.5:3862

24.19.166.5 is cc72678-a.stana1.occa.home.com
```

I search for more events fro m this "individual" since they seem to have marked him up.

```
03/05-07:47:30.621038  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:30.750675  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:36.239362  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:40.417601  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:40.765805  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:42.307651  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:42.717603  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:43.166873  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
```

```
03/05-07:47:47.745743  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:47.996298  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:48.917667  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:49.011850  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
03/05-07:47:49.526872  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.12:35757 ->
10.0.60.11:23
```

It seems like its some sort of shellbox (port 23 is telnet) [it could be a UNIXbox with Fakebo or a compromise d Windowsbox with telnet]

It also runs a myServer DDoS Agent (55850/udp) I read further on: http://www.incidents.org/archives/y2k/082200.htm

cat newbigalert | grep 10.0.60.11 | grep 55850

```
05/09-11:08:49.106525  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
05/09-11:08:49.141924  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
05/09-11:08:49.141982  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
05/09-11:08:49.503345  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
05/09-11:08:51.486648  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
05/09-11:08:56.202690  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
05/09-11:08:57.430746  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
05/09-11:08:58.826008  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
05/09-11:08:58.851851  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:23 -> 148.129.143.2:55850
06/18-13:14:41.825170  [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**]
10.0.60.11:55850 -> 35.10.24.99:31313
```

It seems like a month later the box itself becomes a victim/testbox for myServer. Looking for further trojans

```
03/30-13:15:02.916104  [**] Possible RAMEN server activity [**] 65.27.22.23:2837 ->
10.0.60.11:27374
03/30-13:15:02.916151  [**] Possible RAMEN server activity [**] 10.0.60.11:27374 ->
65.27.22.23:2837
05/19-13:41:22.647703  [**] Possible trojan server activity [**] 24.240.19.143:4348 ->
10.0.60.11:27374
05/19-13:41:22.647796  [**] Possible trojan server activity [**] 10.0.60.11:27374 ->
24.240.19.143:4348
05/19-13:41:24.370135  [**] Possible trojan server activity [**] 24.240.19.143:4348 ->
10.0.60.11:27374
05/19-13:41:24.370178  [**] Possible trojan server activity [**] 10.0.60.11:27374 ->
24.240.19.143:4348
```

Another example is:

```
06/24-19:23:36.904588  [**] Possible trojan server activity [**] 129.170.104.19:1198 ->
10.0.6.15:27374
06/24-19:23:36.904742  [**] Possible trojan server activity [**] 10.0.6.15:27374 ->
129.170.104.19:1198
```

Looking at my updated trojan list I did some random searches for these ports.

Subseven

```
04/23-04:37:57.021740  [**] Possible trojan server activity [**] 10.0.206.242:27374 ->
216.220.164.199:1243
04/23-17:16:26.124770  [**] Possible trojan server activity [**] 198.92.156.150:1243 ->
10.0.213.67:27374
04/24-00:19:03.698484  [**] Possible trojan server activity [**] 216.220.164.133:1243 ->
10.0.216.137:27374
04/24-03:00:23.845762  [**] Possible trojan server activity [**] 216.220.164.133:1243 ->
10.0.213.151:27374
05/16-18:10:41.718440  [**] Possible trojan server activity [**] 65.32.16.253:1243 ->
10.0.130.155:27374
05/16-18:19:16.892280  [**] Possible trojan server activity [**] 65.32.16.253:1243 ->
10.0.1.204:27374
05/18-17:13:06.027822  [**] Possible trojan server activity [**] 24.48.249.61:1243 ->
10.0.140.105:27374
05/19-13:41:44.730765  [**] Possible trojan server activity [**] 205.245.16.35:1243 ->
10.0.5.25:27374
05/19-13:41:45.860168  [**] Possible trojan server activity [**] 205.245.16.35:1243 ->
10.0.5.25:27374
05/24-11:54:11.161796  [**] Possible trojan server activity [**] 202.188.32.234:1243 ->
10.0.98.188:27374
05/24-11:54:11.385010  [**] Possible trojan server activity [**] 10.0.98.188:27374 ->
202.188.32.234:1243
05/24-11:54:14.871506  [**] Possible trojan server activity [**] 202.188.32.234:1243 ->
10.0.98.188:27374
05/24-11:54:15.050804  [**] Possible trojan server activity [**] 10.0.98.188:27374 ->
202.188.32.234:1243
06/27-10:16:47.346579  [**] Possible trojan server activity [**] 10.0.228.245:27374 ->
24.169.119.11:1243
06/27-14:54:58.908832  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.3.16:27374
06/27-15:03:24.026584  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.8.19:27374
06/27-21:00:34.863046  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.29.238:27374
06/27-22:25:00.605279  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.41.74:27374
06/28-01:59:11.015849  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.79.2:27374
06/28-02:26:52.296130  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.82.171:27374
06/28-05:11:44.177184  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.125.132:27374
06/28-06:16:22.074954  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.149.236:27374
06/28-06:42:04.044826  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.170.27:27374
06/28-10:28:21.700608  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.237.82:27374
06/28-10:44:05.862137  [**] Possible trojan server activity [**] 10.0.70.38:1243 ->
10.0.239.75:27374
07/02-19:49:43.330907  [**] Possible trojan server activity [**] 195.84.205.250:1243 ->
10.0.136.244:27374
07/02-19:49:45.934255  [**] Possible trojan server activity [**] 24.203.179.48:1243 ->
10.0.215.210:27374
07/02-19:49:52.324678  [**] Possible trojan server activity [**] 195.84.205.250:1243 ->
10.0.136.244:27374
07/02-19:49:54.543802  [**] Possible trojan server activity [**] 206.74.76.44:1243 ->
10.0.153.102:27374
07/02-19:50:07.872418  [**] Possible trojan server activity [**] 216.86.90.139:1243 ->
10.0.185.98:27374
07/02-19:50:17.155783  [**] Possible trojan server activity [**] 24.191.205.218:1243 ->
10.0.226.244:27374
07/02-19:50:26.143434  [**] Possible trojan server activity [**] 24.191.205.218:1243 ->
10.0.226.244:27374
07/02-19:50:31.306909  [**] Possible trojan server activity [**] 142.176.72.56:1243 ->
10.0.232.151:27374
07/02-19:50:54.724659  [**] Possible trojan server activity [**] 193.153.248.195:1243 ->
10.0.160.0:27374
07/02-19:51:16.004719  [**] Possible trojan server activity [**] 63.10.156.249:1243 ->
10.0.254.83:27374
```

So it seems like there are Sub7 infected machines being exploited from both the inside and outside, noteworthy that there is activity within the network. I also noted some Russian Dynamo activity.

Noteworthy is that communication in some cases is to the inside network aswell to the outside.

I really recommend looking into the alert files again for these possibly afflicted hosts:

One easy way to do this is by just “cat’ing” the log files tog ether and then grep for the specific host or ports intresting. For example 10.0.70.38 is likely to be one to look further into.

Main offender:

The top talker from the alerts is: 212.179.58.200

212.179.58.200 has badly configured reverse DNS.

The reverse DNS for 212.179.58.200 is pvil -200.photonet.com, but pvil -200.photonet.com doesn't resolve to anything.

Port 3697 from this IP is also one of the heavy talkers. Continued watching is recommended. Also feel free to look at the diagrams for further offen ders.

Internal hosts

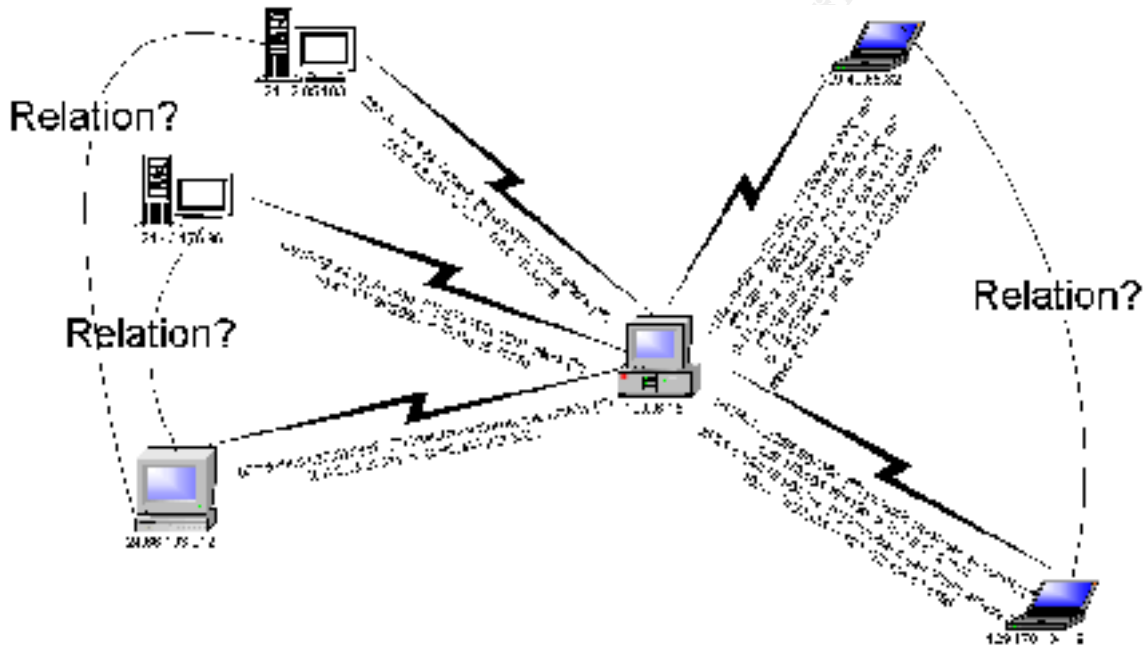
```
This is a quick sorting for some of the problems with the internal network
06/09-17:40:18.996574  [**] SUNRPC highport access! [**] 10.0.100.65:62169 -> 10.0.101.141:32771
06/09-17:40:18.996830  [**] SUNRPC highport access! [**] 10.0.100.65:62169 -> 10.0.101.141:32771
06/09-17:42:08.879148  [**] connect to 515 from inside [**] 10.0.100.65:62169 -> 10.0.101.141:515
06/09-17:42:08.880966  [**] connect to 515 from inside [**] 10.0.100.65:62169 -> 10.0.101.141:515
06/09-17:43:27.608718  [**] Null scan! [**] 10.0.100.65:62177 -> 10.0.101.141:7
06/09-17:43:28.021887  [**] Probable NMAP fingerprint attempt [**] 10.0.100.65:62178 ->
10.0.101.141:7
06/09-17:43:28.436546  [**] NMAP TCP ping! [**] 10.0.100.65:62179 -> 10.0.101.141:7
06/09-17:43:32.080004  [**] Null scan! [**] 10.0.100.65:62177 -> 10.0.101.141:7
06/09-17:43:32.486337  [**] Probable NMAP fingerprint attempt [**] 10.0.100.65:62178 ->
10.0.101.141:7

06/15-03:01:08.207263  [**] SUNRPC highport access! [**] 10.0.98.217:60850 -> 10.0.14.1:32771
06/15-03:01:35.764352  [**] connect to 515 from inside [**] 10.0.98.217:60850 -> 10.0.14.1:515
06/15-03:01:36.273436  [**] connect to 515 from inside [**] 10.0.98.217:60852 -> 10.0.14.1:515
06/15-03:01:45.768466  [**] WinGate 1080 Attempt [**] 10.0.98.217:60850 -> 10.0.14.1:1080
06/15-03:01:45.927619  [**] WinGate 1080 Attempt [**] 10.0.98.217:60851 -> 10.0.14.1:1080
06/15-03:01:46.248030  [**] WinGate 1080 Attempt [**] 10.0.98.217:60852 -> 10.0.14.1:1080
06/15-03:02:07.759091  [**] Null scan! [**] 10.0.98.217:60858 -> 10.0.14.1:7
06/17-00:01:54.768677  [**] SMB Name Wildcard [**] 10.0.111.156:137 -> 10.0.125.41:137
06/17-00:01:56.267614  [**] SMB Name Wildcard [**] 10.0.111.156:137 -> 10.0.125.41:137
06/17-11:57:35.862689  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
06/17-11:57:35.862797  [**] High port 65535 udp - possible Red Worm - traffic [**] 10.0.14.1:161
-> 10.0.5.10:65535

07/06-19:22:17.718241  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
07/06-19:22:17.719740  [**] High port 65535 udp - possible Red Worm - traffic [**] 10.0.14.1:161
-> 10.0.5.10:65535
07/06-19:22:17.739761  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
07/06-19:22:17.741241  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
07/06-19:22:17.742122  [**] High port 65535 udp - possible Red Worm - traffic [**] 10.0.14.1:161
-> 10.0.5.10:65535
07/06-19:22:17.742360  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
07/06-19:22:17.809133  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
07/06-19:22:17.811381  [**] High port 65535 udp - possible Red Worm - traffic [**] 10.0.14.1:161
-> 10.0.5.10:65535
07/06-19:22:18.396079  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
07/06-19:22:18.707053  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
07/06-19:22:18.707965  [**] High port 65535 udp - possible Red Worm - traffic [**] 10.0.14.1:161
-> 10.0.5.10:65535
07/06-19:22:19.342652  [**] High port 65535 udp - possible Red Worm - traffic [**]
10.0.5.10:65535 -> 10.0.14.1:161
```

Link Diagrams

In the search for potential intruders I took a special look at 10.0.6.15 and 10.0.222.86. The pictures are made with Microsoft Visio.

Link Diagram1

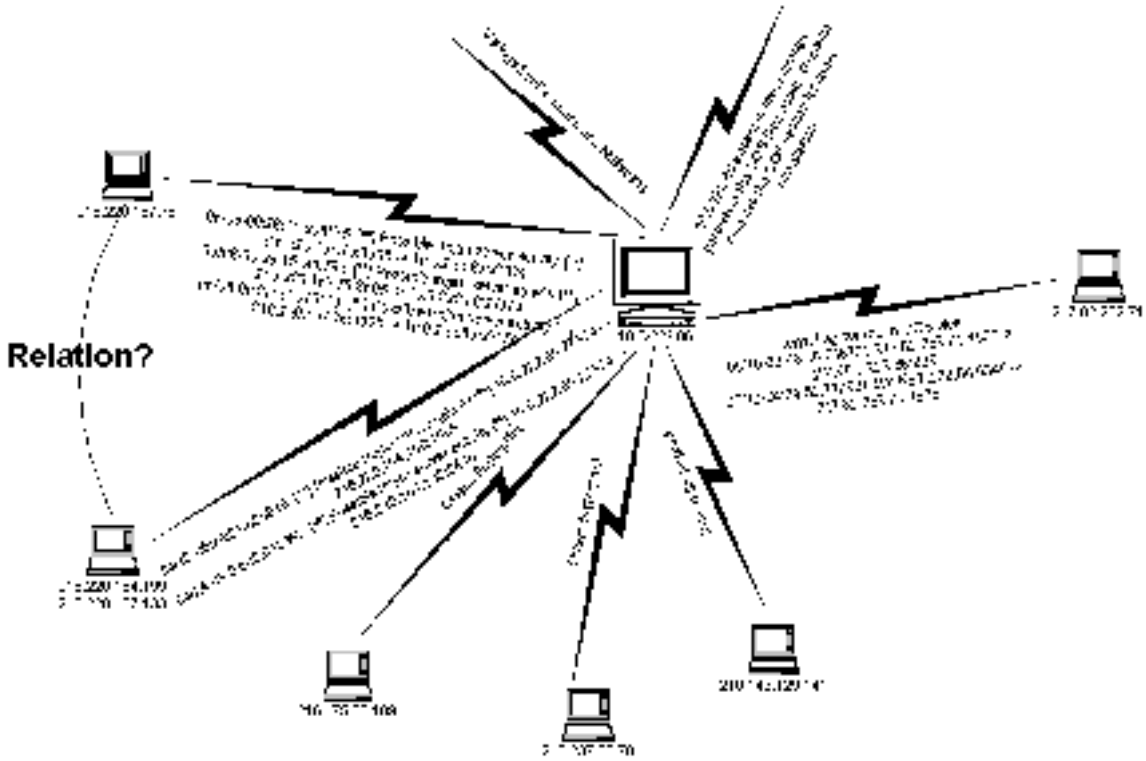
Looking logs for 10.0.6.15 you see a wide range of exploits and other traffic. With this picture i am trying to show some possible hacks and realations.



This machine is clearly under heavy attack and as mentioned above be looked into.

Link Diagram2

With 10.0.222.86 it was mostly the strange OO S that catched my eye.



In the picture above you can see some trojan activity and some various scans. The Trojan Activity is coming from the 216.175 network and it is seems to be transmitted both ways. Also be sure to check out some oos scans from thi s host (in the OOS section).

Please observe that i have not altered the MY.NET.xxx.xxx in the OOS logs.

Out of Spec

I have analysed some out of specs from 2001 -04-24 until 2001-04-29 for abnormal activity. Below I'm showing some examples of my findings . I also noticed that the timestamps are drifting with a few seconds on the various types of scans (when correlating with portscans). Timestamps are also drifting even more on the normal alerts which was confusing at first.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+ =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/24-01:41:57.771452 193.231.42.2:51274  -> MY.NET.253.125:80
TCP TTL:45 TOS:0x0 ID:0  DF
21S***** Seq: 0x93BFBE9C   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460
FE 69                                              .i

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/24-02:00:58.202984 193.231.42.2:54005  -> MY.NET.253.114:80
TCP TTL:45 TOS:0x0 ID:0  DF
21S***** Seq: 0xDD5C6264   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460
08 4B                                               .K
```

Above we see a **potential fingerprinting** of two webservers from a University in Romania (Universitatea "Stefan cel Mare" Suceava). The intresting part is the reserved bits marked up with **fat**. There are much more examples like t his one.

The packages shown below are with high probability crafted packets:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/24-06:30:16.786625 130.239.139.173:6699  -> MY.NET.218.242:1527
TCP TTL:116 TOS:0x0 ID:14318  DF
21SFRPA* Seq: 0xC97B78   Ack: 0x4988E6   Win: 0x5010
TCP Options => EOL EOL
94 B0 D8 59 25 64                                  ...Y%d
```

Comment: Well it is atleast not URGent, otherwise it has **all the TCP Flags set, it is very crafted.** Its origin is from a Swedish Univ ersity (Umeå Universitet). Port 6699 tells me its Napster client data but its highly unlikely that it is infact regular Napster traffic.

The following packets seems like **retransmissions**. Their origin can either be of a spoofed nature or some form of comm unications failure. Their timestamps differs but the sequence number aswell as their source/dest ports are the same in these packets.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/24-12:17:00.061612 217.96.71.21: 1623 -> MY.NET.229. 162:6346
TCP TTL:50 TOS:0x0 ID:7177  DF
21S***** Seq:  0xFA290719   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 145336529 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/24-12:17:03.059963 217.96.71.21 :1623 -> MY.NET.229.162: 6346
TCP TTL:50 TOS:0x0 ID:7433  DF
21S***** Seq:  0xFA290719   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 145336829 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/24-12:17:09 .058588 217.96.71.21: 1623 -> MY.NET.229.162: 6346
TCP TTL:50 TOS:0x0 ID:7689  DF
```

```
21S***** Seq: 0xFA290719   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 145337429 0 EOL EOL EOL EOL
```

There was also some packets envolved with other fingerprinti ng techniques

=+
04/24-17:21:14.478552 **193.224.41.14:0** -> MY.NET.218.242:1209
TCP TTL:117 TOS:0x0 ID:7286 DF
*1SFR*AU Seq: 0x5001E Ack: 0xABDACF8E Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK

=+
04/24-17:23:11.058449 **193.224.41.14:1210** -> MY.NET.218.242:5
TCP TTL:117 TOS:0x0 ID:54150 DF
SFRU Seq: 0x86001E Ack: 0xB81BCFBE Win: 0x8010
C1 6E 3F E9 00 00 01 01 05 0A CF BE 52 DB CF BE .n?.........R...

Comment: Syn, Fin & Rst should never appear in a normal packet, this is definitely part of a fingerprinting.

There are much more examples that involves fingerprinting techniques so lets move on to another finding.

Data sent on SYN below is a example of this event

=+
04/29-14:13:32.962440 128.46.156.117:20 -> MY.NET.204.150:4050
TCP TTL:55 TOS:0x8 ID:13911 DF
21S***** Seq: 0xD7B3D558 Ack: 0x0 **Win: 0x16D0**
TCP Options => **MSS: 1460 SackOK TS: 320271** 0 EOL EOL EOL EOL

=+
04/29-14:13:36.739622 128.46.156.117:20 -> MY.NET.204.150:4054
TCP TTL:55 TOS:0x8 ID:63126 DF
21S***** Seq: 0xD823121F Ack: 0x0 **Win: 0x16D0**
TCP Options => **MSS: 1460 SackOK TS: 320649** 0 EOL EOL EOL EOL

=+
04/29-14:13:45.333566 128.46.156.117:20 -> MY.NET.204.150:4060
TCP TTL:55 TOS:0x8 ID:5929 DF
21S***** Seq: 0xD91CF0CD Ack: 0x0 **Win: 0x16D0**
TCP Options => **MSS: 1460 SackOK TS: 321508** 0 EOL EOL EOL EOL

=+

From the SANS conference I learned that this way can be used to fool the dete ction of the SYN's since they already carry a payload. Well no fooling me ☺

Comparing these OOS with the Scan detects you see that these malformed RESERVED bits gets in the log there aswell.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+   =+=+
04/27-16:46:09.062984 212.123.172.102:18245  -> MY.NET.179.77:21536
TCP TTL:111 TOS:0x0 ID:2137  DF
2*SFR*AU Seq: 0x2F746573   Ack: 0x742F6272   Win: 0x7365
54 50 2F 31 2E 31 0D 0A 41 63                     TP/1.1..Ac

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

The portscan logs has some correlation (in other cases aswell)

```
Apr 27 16:46:15 212.123.172.102:18245  -> 10.0.179.77:21536 INVALIDACK
2*SFR*AU RESERVEDBITS
Apr 27 16:46:15 212.123.172.102:18245  -> MY.NET.179.77:21536 INVALI DACK
2*SFR*AU RESERVEDBITS
```

The invalid acks are likely part of a nmap scan.

Below we see some more advanced fingerprinting technique from the internal network

=+
04/28-19:03:33.328390 MY.N ET.217.182:6346 -> 212.199.23.151:1839
TCP TTL:126 TOS:0x0 ID:23545 DF
21*F*P** Seq: 0x15A2669D Ack: 0xA1 Win: 0x5010
TCP Options => EOL

=+
04/28-19:14:58.904429 MY.NET.217.182:6346 -> 212.199.23.151:1839
TCP TTL:126 TOS:0x0 ID:46994 DF
21*FRPA* Seq: 0x15A3 Ack: 0x8F2D00A2 Win: 0x5010
18 CA 07 2F 00 00 15 A3 8F 2D 00 A2 00 DD 50 10 .../..... -....P.
1D FA 41 26 00 20 20 20 20 20 ..A&.

This individual machine is al so in the port scan logs (see below in the Scans section). So my recommendation is that you look into this host closer.

During my search for materials for some link diagrams i came across some more strange activity in the OOS scans.

Port 6688 is asscoci ated with Napster, there are some strange flag combinations, Strange that the source port is 0. I am not an expert with Napster so i wouldnt know if this was normal, but based on the OOS above it is not!

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/07-12:45:28.437028 MY.NET.225.42:0 -> 170.140.23.35:6688
TCP TTL:126 TOS:0x0 ID:65319  DF
21SF***U Seq: 0x7540884   Ack: 0xD45F1017   Win: 0x5010
TCP Options => EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/07-12:45:53.155663 MY.NET.225.42:0 -> 170.140.23.35:6688
TCP TTL:126 TOS:0x0 ID:52018  DF
**SFRPAU Seq: 0x7550873   Ack: 0x518A1018   Win: 0x5018
00 00 A3 B9 C3 A5 4B 86 14 5E 2C D4 96 45        ......K..^,..E

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/07-12:50:47.590170 MY.NET.225.42:0 -> 170.140.23.35:6688
TCP TTL:126 TOS:0x0 ID:26734  DF
*1SFR*** Seq: 0x7590886   Ack: 0x7D50101C   Win: 0x5010
TCP Options => EOL EOL
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/07-12:51:07.404156 MY.NET.225.42:0 -> 170.140.23.35:6688
TCP TTL:126 TOS:0x0 ID:7284  DF
*1SFR*** Seq: 0x759089C   Ack: 0xFD50101C   Win: 0x5010
TCP Options => EOL EOL Opt 142 (9): A38C 9BF8 4442 57BA

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/07-12:51:07.439509 MY.NET.225.42:0 -> 170.140.23.35:6688
TCP TTL:126 TOS:0x0 ID:9588  DF
*1SFR*** Seq: 0x759089D   Ack: 0x1B04101C   Win: 0x5018
TCP Options => EOL EOL
```

Below we see traffic towards port 6346 that can be asociat ed with Gnutella, we have some strange flag combinations, also see the link diagram for this host on the internal network

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/10-03:14:51.621851 MY.NET.222.86:0 -> 205.162.20.161:6346
TCP TTL:126 TOS:0x0 ID:7804  DF
21S**P** Seq: 0xB0402B8   Ack: 0xCB44014C   Win: 0x5018
TCP Options => EOL EOL
00 10                                             ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/10-03:22:12.194088 MY.NET.222.86:0 -> 24.154.64.190:6346
TCP TTL:126 TOS:0x0 ID:53462  DF
21SFRP** Seq: 0xCC002D6   Ack: 0xFACF2F9E   Win: 0x5018
TCP Options => EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/10-04:15:39.248514 MY.NET.222.86:6346 -> 65.24.54.78:1868
TCP TTL:126 TOS:0x0 ID:21316  DF
21S**PA* Seq: 0x3002DE0   Ack: 0x8F0C   Win: 0x5018
00 00 69 33 60 2E 63 02 5C 18 07 07 02 1C        ..i3`.c.\.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/10-04:18:12.307129 MY.NET.222.86:0 -> 216.5.125.96:6346
TCP TTL:126 TOS:0x0 ID:28785  DF
21S**PAU Seq: 0x4A70309   Ack: 0xF278012C   Win: 0x5018
TCP Options => EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/10-04:23:25.570248 MY.NET.222.86:0 -> 128.255.140.111:6346
TCP TTL:126 TOS:0x0 ID:54734  DF
2*SFRP** Seq: 0x8650300   Ack: 0x2DC90148   Win: 0x5018
TCP Options => EOL EOL

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

Digging further down the OOS logs from 23:th of May i s ee

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/23-10:43:51.468489 MY.NET.222.86:0 -> 18.245.0.120:6346
TCP TTL:126 TOS:0x0 ID:61696  DF
21*F*P*U Seq: 0xFFB071A   Ack: 0x4ED2D08C   Win: 0x5018
00 00 18 CA 0F FB 07 1A 4E D2 D0 8C 08 E9 50 18  ........N.....P.
20 6D 44 F1 00 00 20 61 6E 61 6C 20 6C 65 73 62   mD... anal lesb
69 61                                             ia

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

from this internal host. Strange flag co mbo, and not so strange content if you just place that missing 'ns' at the end... (lesbians)

Without much hassle i find another Gnuttella friend

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/16-09:34:31.997421 MY.NET.217.182:6346 -> 217.0.50.80:1122
TCP TTL:126 TOS:0x0 ID:50569  DF
21SF**AU Seq: 0x22C   Ack: 0xA20F004E   Win: 0x5018
A2 0F 00 4E 2C F3 50 18 21 80 81 38 00 00 6E 20  ...N,.P.!..8..n
70 75 73 73 79 20 61 6E 64 20                     pussy and

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

Another pair in the OOS files that seemed strange was:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/24-11:26:44.242677 62.59.148.34:18245 -> MY.NET.253.125:21536
TCP TTL:106 TOS:0x0 ID:8035  DF
**SFRP*U Seq: 0x2F7E6473   Ack: 0x63686D69   Win: 0x736F
31 2F 73 6F 75 6E 64 73 2F 63 6F 77 2E 77 61 76  1/sounds/cow.wav
20 48 54 54 50 2F                                HTTP/

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/24-11:26:44.242837 62.59.148.34:18245 -> MY.NET.253.125:21536
TCP TTL:106 TOS:0x0 ID:8035  DF
**SFRP*U Seq: 0x2F7E6473   Ack: 0x63686D69   Win: 0x736F
31 2F 73 6F 75 6E 64 73 2F 63 6F 77 2E 77 61 76  1/sounds/cow.wav
20 48 54 54 50 2F                                HTTP/

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/24-11:26:44.242999 62.59.148.34:18245 -> MY.NET.253.125:21536
TCP TTL:106 TOS:0x0 ID:8035  DF
**SFRP*U Seq: 0x2F7E6473   Ack: 0x63686D69   Win: 0x736F
31 2F 73 6F 75 6E 64 73 2F 63 6F 77 2E 77 61 76  1/sounds/cow.wav
20 48 54 54 50 2F                                HTTP/

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/24-11:26:44.243159 62.59.148.34:18245 -> MY.NET.253.125:21536
TCP TTL:106 TOS:0x0 ID:8035  DF
**SFRP*U Seq: 0x2F7E6473   Ack: 0x63686D69   Win: 0x736F
31 2F 73 6F 75 6E 64 73 2F 63 6F 77 2E 77 61 76  1/sounds/cow.wav
20 48 54 54 50 2F                                HTTP/

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

It appears by looking at http://archives.neohapsis.com/archives/incidents/2001-01/0079.html that it seems to be a Nortel CVX that could be messing up the packets.

Scans:

I have analyzed the scans from 2001 -03-01 until 2001-07-13 (and correlation work with the above OOS) for abnormal activity, without knowing what targets are important doing a summary.

Scanning is being made both to and from the network . Unknowing of the policy in practice I choose not judge this further. But I would advise to keep such individuals under close surveillance.

An example of this is:

```
Apr 28 20:04:07 10.0.217.182:0 -> 24.94.194.148:6346 INVALIDACK *1SF**AU RESERVEDBITS
Apr 28 20:29:14 10.0.217.182:6346 -> 193.2.68.118:2813 NOACK *1SFR**U RESERVEDBITS
Apr 28 20:42:26 10.0.217.182:0 -> 217.80.252.25:6346 NOACK 2***RP** RESERVEDBITS

(where 10.0 is MY.NET)
```

There seems to be rather big and **repetitive sweeps**. Seems like being part of bigger sweeps. These are really not active targeting but rather inventory of the network. Sometimes these "netmaps" are used at a later time for newer exploits. Could be regarded as highrisk in the long term but lowrisk in the short term.

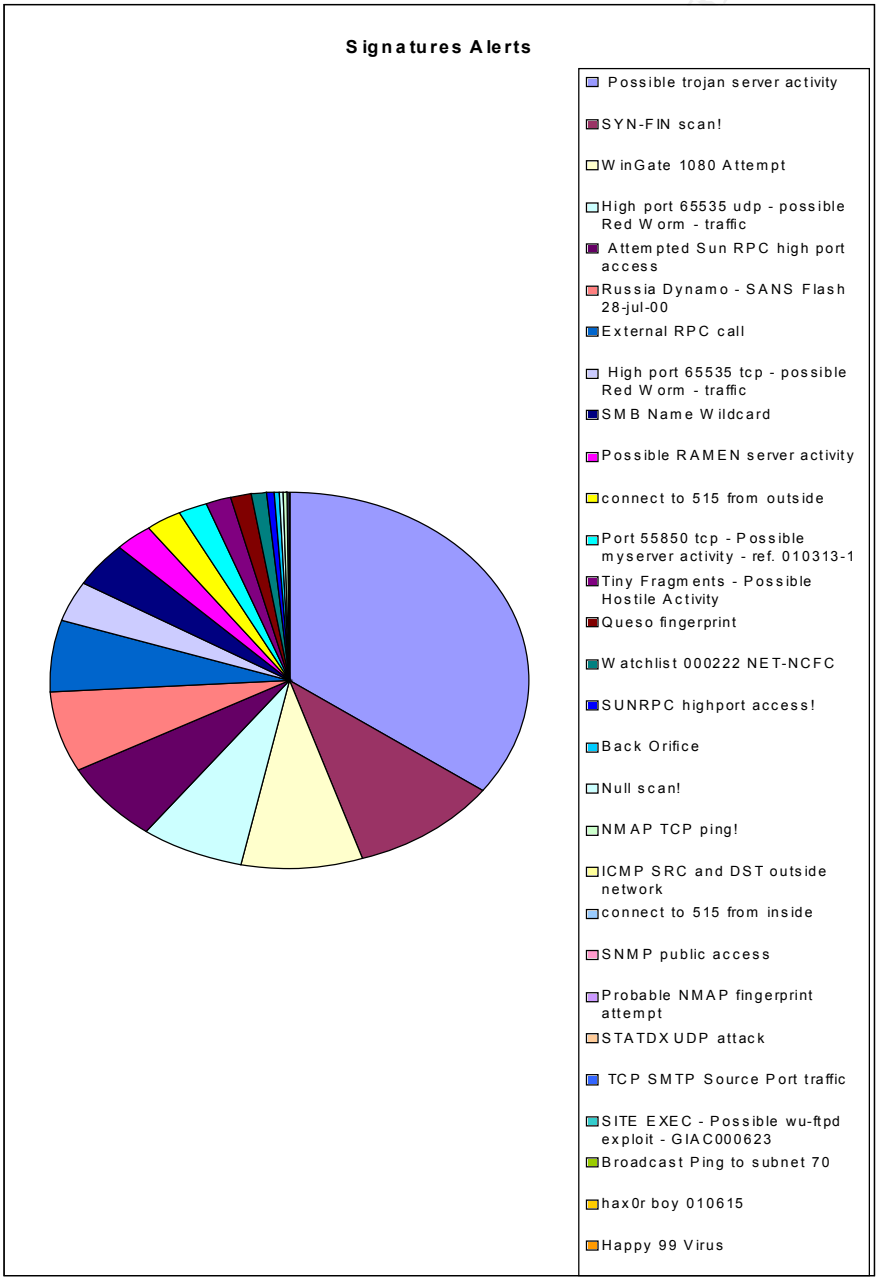
Some sweeps are targetet for just **certain ports**, looking for services offered. This includes trojans and commonly exploitable ports. Examples are port 53 and 515

```
Jul 12 08:05:35 200.206.165.19:2489  -> 10.0.137.13: 515 SYN **S*****
Jul 12 08:05:35 200.206.165.19:2491  -> 10.0.137.15: 515 SYN **S*****
Jul 12 08:05:35 200.206.165.19:2493  -> 10.0.137.17: 515 SYN **S*****
```

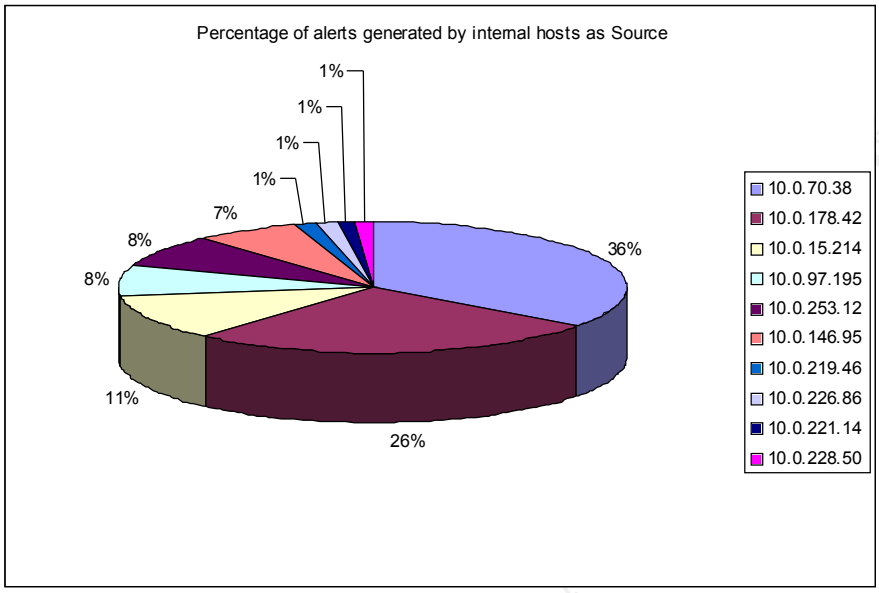
I do recommend that you do internal portscans for an inventory of the services offered within the network!

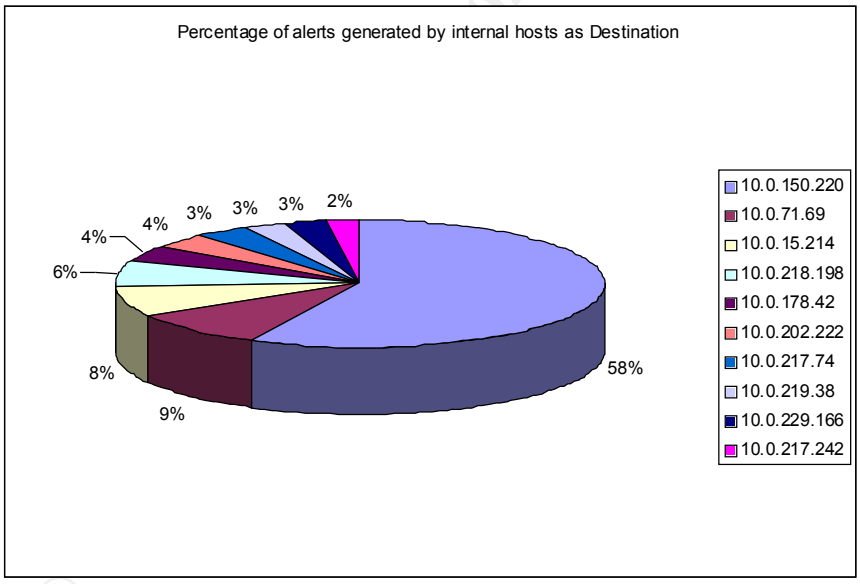
Summarations and diagrams:

All data from these diagrams has been gathered from the alert files from 2001 -03-01 until 2001-07-13. Excluded in these reports are traffic from outside network. For the data gathering i have used shell commands in BSD and a custom DOS application for statistics (available upon request). The statistics of the alerts should be available when double clicking on the diagrams (I have used Excel).

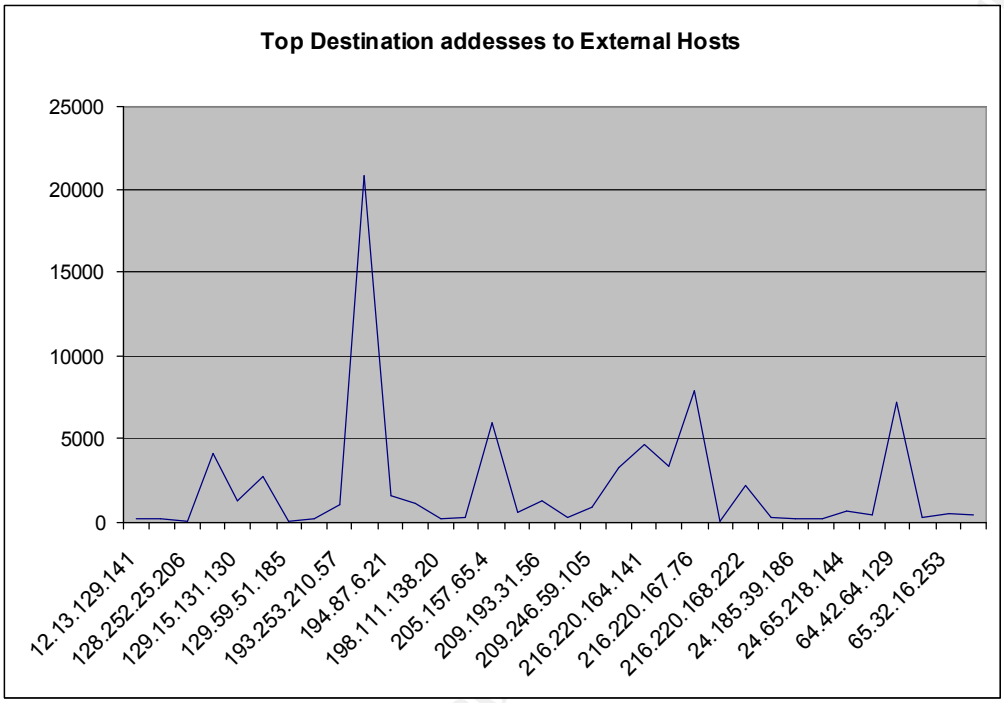


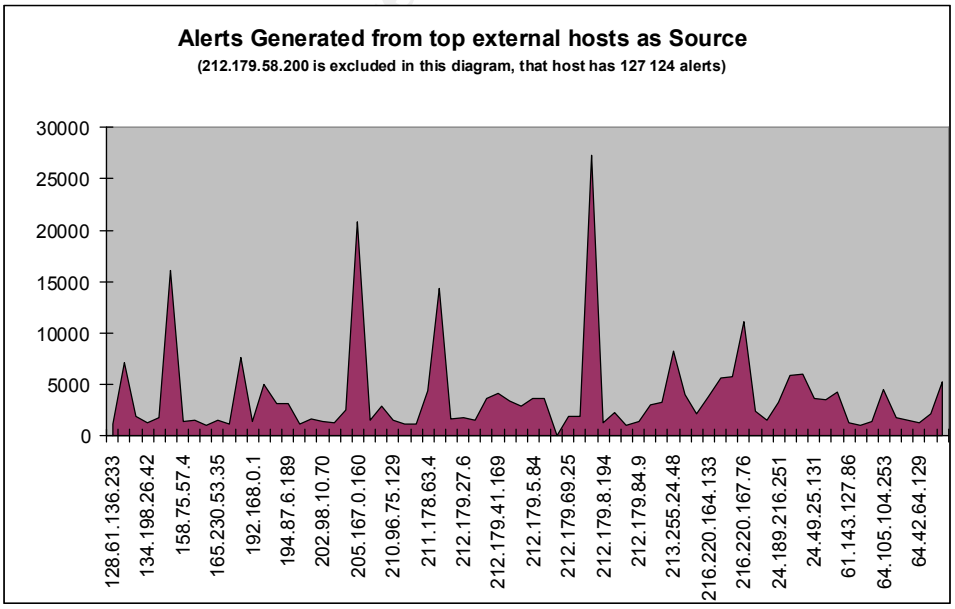
Statistics for internal hosts



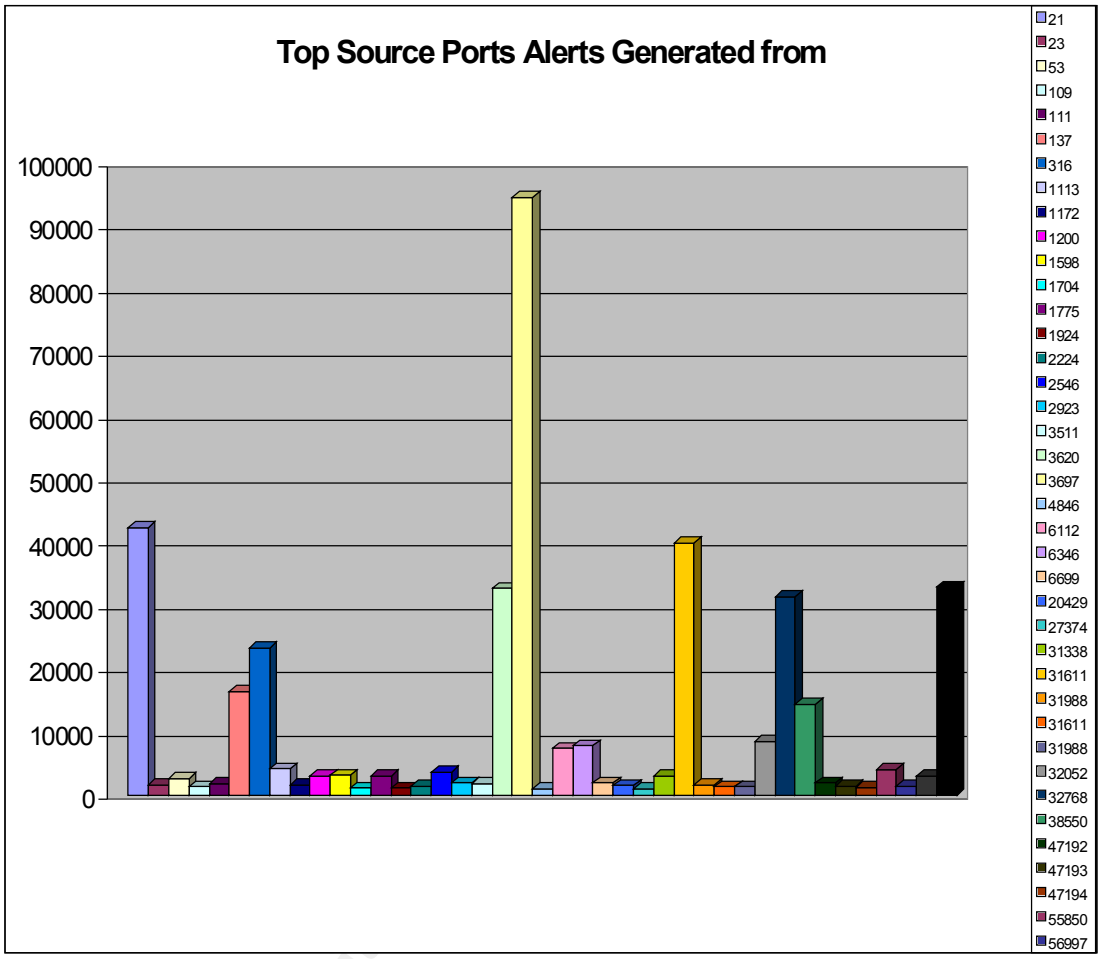


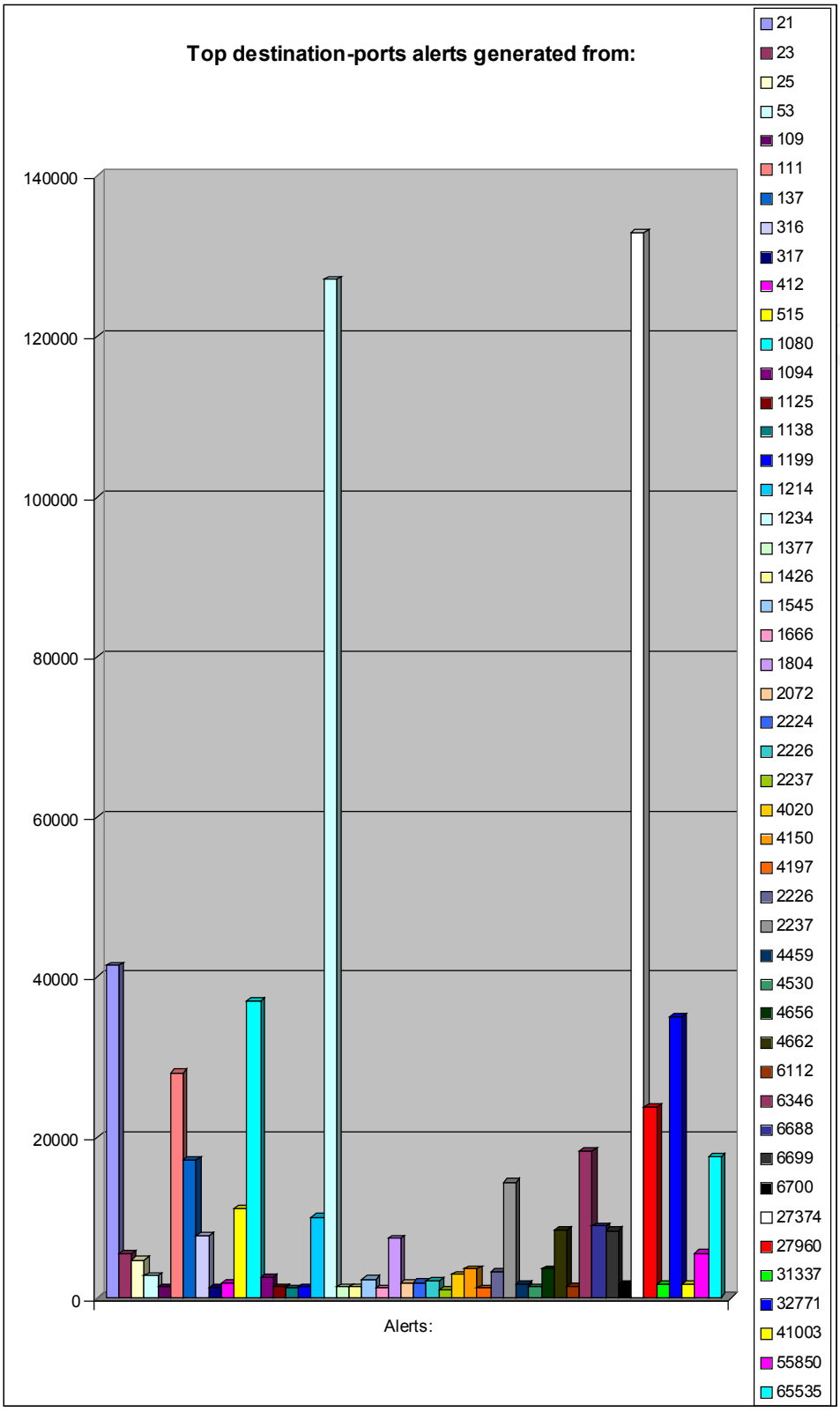
Statistics for external hosts.





Statistics for ports





Recommendations

The following sections can be implemented in project forms e ither by internal personal or by external consultants. It is however important that the management and technicians work together for a successful Infrastructure and Policy enforcement.

- Firewall/NAT usage for blocking unwanted traffic
- Proxy server, with so me form of content filtering for malicious content
- Revision of Policy and enforcing of it.
- Antivirus software for all clients and antivirus/trojan scanning for SMTP level
- Internal/External Security Audit
- NTP usage for synchronized the logs
- Centralize serv ers such as SMTP and webservers, no need to have them scattered?
- Continued usage of IDS and logging.

For further information about these projects some good information can be found on:
http://www.sans.org/infosecFAQ/securitybasics/basics_list.htm
http://www.incidents.org/detect/ih_faq.php

I see no need to explain them in further detail during this report. However if you should find the need to use my expertise in these areas Im sure Im going to elaborate on them further in other GIAC certifications.

Further recommendations can be found within the report.

Thank you for your time reading this report!

David Hed in Sweden

References used in this practical assignment either alive or still at this moment available through Googles cache.

Assignment 1

http://www.cert.org/advisories/CA -1998-05.html
http://packetderm.cotse.com/CIE/RFC/1035/59.htm
http://www.samspade.org
http://www.internic.net
http://www.insecure.org/sploits/Microsoft.frontpage.insecurities.html
http://www.securiteam.com/windowsntfocus/5NP0J0U1FO.html)
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/office/reskit/fp98serk/ appendixes /A_UNPERM.asp
http://www.securityfocus.com/bid/1174
http://www.sans.org/y2k/
http://www.insecure.org/sploits/Microsoft.frontpage.insecurities.html
http://www.securiteam.com/windowsntfocus/5NP0J0U1FO.html
http://www.microsoft.com/technet/treeview/ default.asp?url=/TechNet/prodtechnol/office/reskit/fp98serk/appendixes /A_UNPERM.asp
http://www.securityfocus.com/bid/1174
http://www.sans.org/y2k/062000.htm
http://www.cert.org/advisories/CA -2001-19.html
http://www.cert.org/advisories/CA -2001-13.html
http://www.cisco.com/warp/public/707/cisco -code-red-worm-pub.shtml
http://www.worm.com *LOL*
http://www.eeye.com/html/Research/Tools/CodeRedScanner.exe
http://www.incidents.org/diary/diary.php
http://archives.neohapsis.com/archives/bugtraq/2001 -07/0396.html
http://www.cert.org/advisories/CA -2001-19.html
http://www.onlamp.com/pub/a/bsd/2001/04/04/FreeBSD_Basics.html
http://www.sys -security.com/archive/papers/ICMP_Scanning_v3.0.pdf
http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids4
http://advice.networkice. com/Advice/Intrusions/2000309/default.htm
http://www.incidents.org/react/code_red.php

Assignment 2

State of Intrusion Detection (Hardware and planning)

http://www.shmoo.com/mail/ids/nov99/msg00047.html (archived discussion about hardware/ids)
http://www .metases.com/files/Shomiti.pdf (document on Shomiti taps with Cisco2900)
http://www.finisar -systems.com/products/index.html (Ethernet and Fiberchannel taps)
http://www.niksun.com/products/netvcr.html (if you dont want to build your trafficdumper by yourse lf)
http://www.sans.org/y2k/practical/Charles_Hutson_GCIA.doc (assignment2 is about outsourcing)
http://www.tcpdump.org/ (TCPDUMP)
http://www.snort.org/ (Snort IDS) *no its not spelled Snorth, Mr.Consult -know-it-all*
http://www.nswc.navy.mil/ISSEC/CID/ (Shadow IDS)
http://www.cert.org/kb/acid/ (Analyst Console for Intrusion Databases)
http://www.freebsd.org (Highperformance and stable Operating System)
http://www.openbsd.org (Highly secured and stable Operating System)

Books & other info

Network In trusion Detection: An Analyst's Handbook: Stephen Northcutt, Judy Novak, Donald McLachlan (2000)

Manpages from the BSD distibutions can learn you alot! Also be sure to check out TCPDUMP

Assignment2old Trojan correlation with known ports

http://www.sys -security.com/html/papers/trojan_list.html
http://www.sans.org/newlook/resources/IDFAQ/oddports.htm
http://www.simovits.com/trojans/
http://dark -e.com/archive/trojans/
http://www.certcc.or.kr/advisory/
http://www.dark -e.com/cgi -bin/quiz.cgi
http://www.zonel abs.com/knowledgebase/trojanports.html
http://www.multimania.com/cdc/trojanh.htm

Assignment 3

http://www.sans.org/y2k/practical/chris_kuethe_gcia.html
http://lists.insecure.org/incidents/2000/Oct/0141.html
http://www.google.com/search?q=cache:d9xVEpq0_pc: www.sans.org/y2k/082200.htm++myserver+55850&hl=sv
http://www.incidents.org/archives/y2k/082200.htm
http://www.sans.org/infosecFAQ/securitybasics/basics_list.htm
http://www.incidents.org/detect/ih_faq.php
http://archives.neohapsis.com/archives/incidents/200 1-01/0079.html

Last Updated: July 23rd, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced