



The University of Texas at San Antonio™

ISCS 3523-003 Intrusion Detection and Incident Response

Lab #02 Malware Analysis The SimSpace Cyber Range

Student:

Dillen Dela Cruz, odv464

Prepared for Intrusion Detection and Incident Response

02/03/2024

Professor: Shawn Zumwalt

Contents

Images	1
Citations:	11

OBSERVATIONS:

From the Windows XP image (Image 1), it's evident that Windows XP has a single user account currently logged in under the name Daniel Faraday. The Nmap scan (Image 2) reveals the presence of 15 open ports. By employing Netcat, I successfully accessed the FTP server on port 21 and the IRC server on port 6666, providing me with command-line access to the Windows XP machine. Noteworthy among the observed ports is a VNC service, enabling remote control of a computer or server through a network. Additionally, there's another IRC service on port 6667, commonly exploited by various trojans and backdoors such as Dark Connection Inside, Dark FTP, Host Control, NetBus worm, ScheduleAgent, SubSeven, Trinity, WinSatan, among others (Speed Guide).

By utilizing port 6666, I successfully gained access to the command line of the user Daniel Faraday. Afterwards, I altered the user's password, allowing me to access Windows XP through the command "net user "Daniel Faraday" guest" (Image 3).

Active Processes/Logs:

Once I had access to the Windows XP account, my initial examination involved finding the active processes using the 'tasklist' command. The output yielded a total of 30 processes currently running on the system. Upon closer inspection, it became apparent that 12 out of the 13 were supposed to be from the 'windows32' directory, according to my outside research (Image 4). To verify their file locations, I executed the "dir /s /b C:<filename>" command for each file, confirming that all were indeed located within the 'windows32' directory. One particular file that drew my attention was "poisonivy.exe," as it deviated from the expected pattern of files found in the 'windows32' directory, an anomaly I will elaborate on shortly. The rest of the processes running appeared legitimate, serving specific program functionalities, or contributing to the Windows system. Additionally, the file locations correlated with their expected locations based on my external research (Image 5).

According to its properties, poisonivy.exe was created on Tuesday, May 25, 2010, at 5:52:24 PM, and modified on Saturday, May 22, 2010, at 2:25:37 PM. From what I gathered about this executable, this is a type of malware that should not be located in system32 or actively running, as it is linked to other malicious software like Breut and Darkmoon, as documented by MITRE. Examining the Windows Task Manager reveals that poisonivy is running under the user Daniel Faraday. It seems that poisonivy.exe has initiated a connection to a foreign address. However, the full connection establishment process (three-way handshake) hasn't been completed yet. This can be seen in the output of the "netstat -ano" command (Image 7).

With the recorded dates, I investigated Windows Events related to this file. Within the timeframe from May 20 to May 25, a series of intriguing events unfolded consecutively. It started with the ISS Admin entering the running state, followed by SMTP, World Wide Publishing, FTP, and the activation of HXD service 100 (Image 8-14). The sequence concluded with a system reboot, and following after, the event log stopped recording.

Starting with the ISS Admin, when IIS (Internet Information Services) and associated services start up successfully, it means that the necessary components, configurations, and connections have been initiated. IIS initializes its web server, FTP (File Transfer Protocol) service, and SMTP (Simple Mail Transfer Protocol) service during startup. The IIS Admin Service plays a role in coordinating the overall design of IIS and its services. A successful startup may indicate that these services are ready to handle incoming requests, whether they be web, FTP, or email related. This can be shown by the events that appeared consecutively after Admin IIS and in addition within the Internet Information Services window (accessible in the administrative tools), all three services are listed under it (Image 8-14).

I suspect that the FTP server played an important role in the creation of poisonivy.exe. The logs indicate a correlation between the FTP and HXD service 100s activation (between 5:27pm-5:59pm), during which poisonivy.exe and other services, including netcat, and VNC, were generated. Notably, some of these services are housed within the FTP directory. Further analysis of the FTP logs reveals that an intruder accessed the FTP server from the IP address 192.168.5.99, utilizing the anonymous login feature. During this unauthorized access, the intruder proceeded to create files.tar and 7za.exe. The presence of 7za.exe indicates the likelihood of it being a standalone version of 7-Zip. This assumption is supported by the fact that, in conjunction with the .tar file, which is commonly employed for archiving and transmitting multiple files, it is typically accessible using 7-Zip. In the end it could be possible that the intruder had passed on poisonivy.exe through this (Image 17).

The connection between these two different logs, despite time differences, became apparent when I noticed a recurring pattern in the System Event Viewer Logs. Specifically, there were consistent errors originating from the W32Time source. Two types of errors stood out: one indicating a "socket operation was attempted to an unreachable host," and another stating that "NtpClient has no source of accurate time." What's noteworthy is that these errors persisted even after the IIS events mentioned earlier had occurred (Image 18-19).

The key takeaway is that when the system struggles with accurate time synchronization, it can significantly impact the timestamps in logs. This, in turn, makes it challenging to precisely correlate events. This insight could help explain the observed time gap between the FTP logs and the Event Viewer logs.

Despite a thorough investigation, I couldn't find matching timestamps between the FTP logs and entries in the Application or System Event Viewer. Interestingly, there's only one FTP log in the Event Viewer for May 25, even though it occurred at different times. This led me to consider the possibility that these instances might be part of the same session. The absence of additional FTP logs within the Event Viewer for that day supports this notion.

Rootkit:

My next concern would be the HXD service 100 which is not a process regular to windows but a rootkit. After being installed and executed on the targeted system, the hacker can gain full control, and not even the system administrator can detect any security risks. Hxdef100 offers numerous customizable features and allows users to conceal crucial information such as file keys, process details, system services, drivers, registry keys, open ports, and create an illusion of available disk space (Alibaba Cloud). According to the logs, it appears that only a single occurrence of the HXD service was executed. In the preceding paragraph discussing the FTP server, I suspect that this program was grouped with other executables and subsequently executed after the completion of the file transfer.

Runasspc.exe:

I've identified another inconsistency in the logs where FTP records indicate the same anonymous user from the same IP address performing a file transfer, "runasspc.exe." Surprisingly, the Windows Event Viewer lacks any corresponding logs of an FTP session starting up or running. From my external search, "RunAsSpc.exe" is a tool associated with the "RunAsSpc" software, providing a means for users to execute programs with diverse credentials, typically with elevated privileges. This utility enables users to specify alternate credentials, like a different username and password, when running a program, eliminating the need to log in with a separate account. This functionality proves beneficial for tasks requiring administrative permissions, allowing limited users to run applications without logging in as administrators. (Robotronic) (Image 21).

Story:

Analyzing the open ports, I determined that 10 of them (21, 25, 80, 135, 139, 443, 445, 1033, 5000, 1025) were system-initiated, while 3 (6666, 5900, 5800) were initiated by the user Daniel Faraday. This deduction was made through examination of the "netstat -ano" command output, cross-referencing ports with their associated Process ID (PID). In the Windows Task Manager, these processes were attributed to the user's "SYSTEM" and "NETWORK SERVICE." It appears that the intruder likely exploited one of the 10 ports, with port 21 and port 139 being potential targets due to their known vulnerabilities (Image 21).

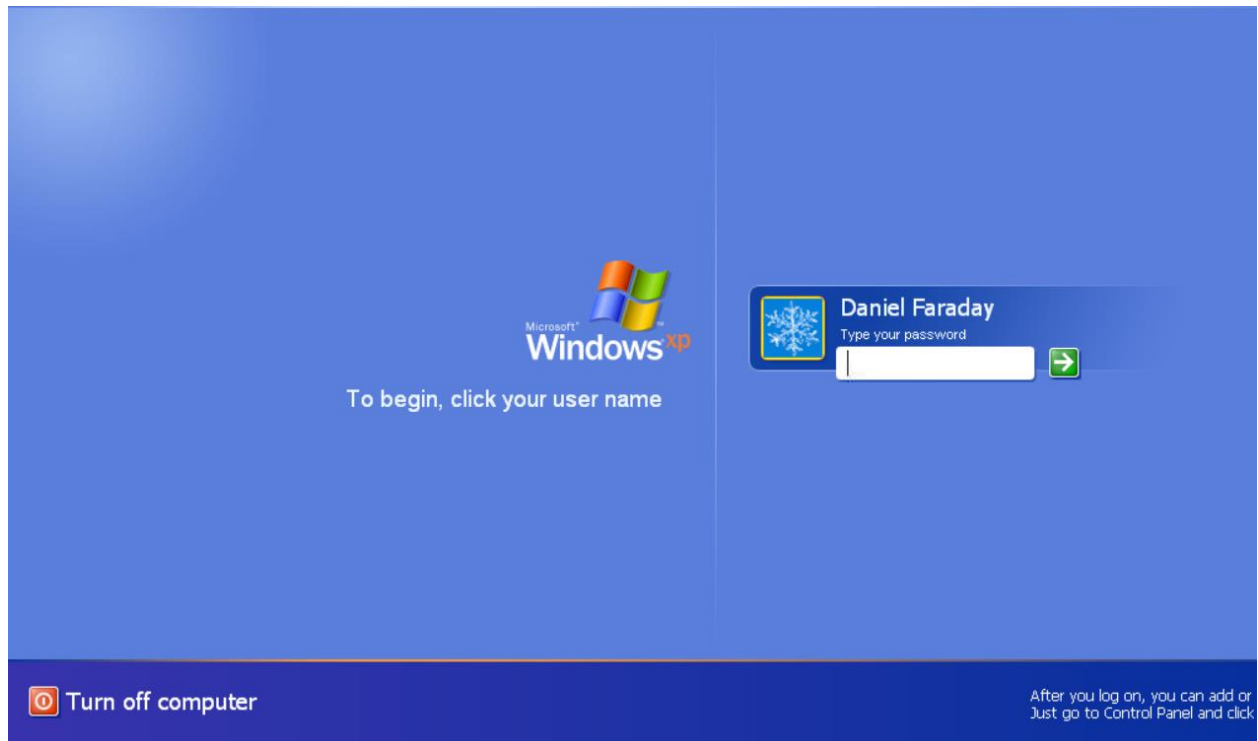
Upon gaining access, the intruder manipulated the NTP client, causing issues in obtaining time from configured sources. This interference not only impacts log times but also affects various processes and services on the system. Subsequently, the intruder transferred files, including what appears to be a rootkit, poisonivy.exe, as well as VNC and Netcat files. The discussion on poisonivy.exe under "Active Processes/Logs" sheds light on its malicious nature, as well as the other files that were transferred and ran. The poisonivy.exe file was observed attempting to connect to a remote server, although the connection couldn't complete the three-way handshake. Additionally, the intruder likely used Netcat to open port 6666, as indicated by the PID and netstat command. When using the netcat command on port 6666 you can see it connects you straight to the user's command line. The VNC server was also running, potentially opening ports 5900 and 5800, enabling remote desktop access on Windows XP. Within the same folder, the intruder executed the rootkit HXD 100 service. This rootkit has capabilities such as concealing open ports,

which aligns with the observation of port 6667 only being visible in the Nmap scan. Port 6667 is commonly associated with various trojans and backdoors, including Dark Connection Inside. It's crucial to note that all these actions were carried out under the user account Daniel Faraday. The intruder's activities involve exploiting vulnerabilities, executing malicious files, and setting up services to establish control and persistence on the compromised Windows XP system. Later on, another file transfer was completed which ran the "RunAsSpc.exe" is a tool associated with the "RunAsSpc" software, providing a means for the user to execute programs with diverse credentials, typically with elevated privileges.

The intruder's actions on the compromised Windows XP system suggest a complicated and potentially malicious agenda. By exploiting vulnerabilities and manipulating key system components, such as the NTP client and open ports, the intruder demonstrates a sophisticated understanding of system weaknesses. The transfer and execution of files, including the rootkit HXD service 100, poisonivy.exe, Netcat, and VNC, point towards activities aimed at establishing control, persistence, and remote access to the compromised system. The intruder's interest in concealing open ports, initiating file transfers through FTP, and altering passwords indicates a strategic effort to maintain covert access and control over the compromised system. The RunAsSpc.exe tool adds another layer of attack, suggesting an intent to execute programs with elevated privileges, potentially for further system manipulation or privilege escalation. While the precise motives remain speculative, potential reasons for such intrusive activities could include espionage, data exfiltration, financial gain, or the installation of a persistent backdoor for future malicious activities.

Images

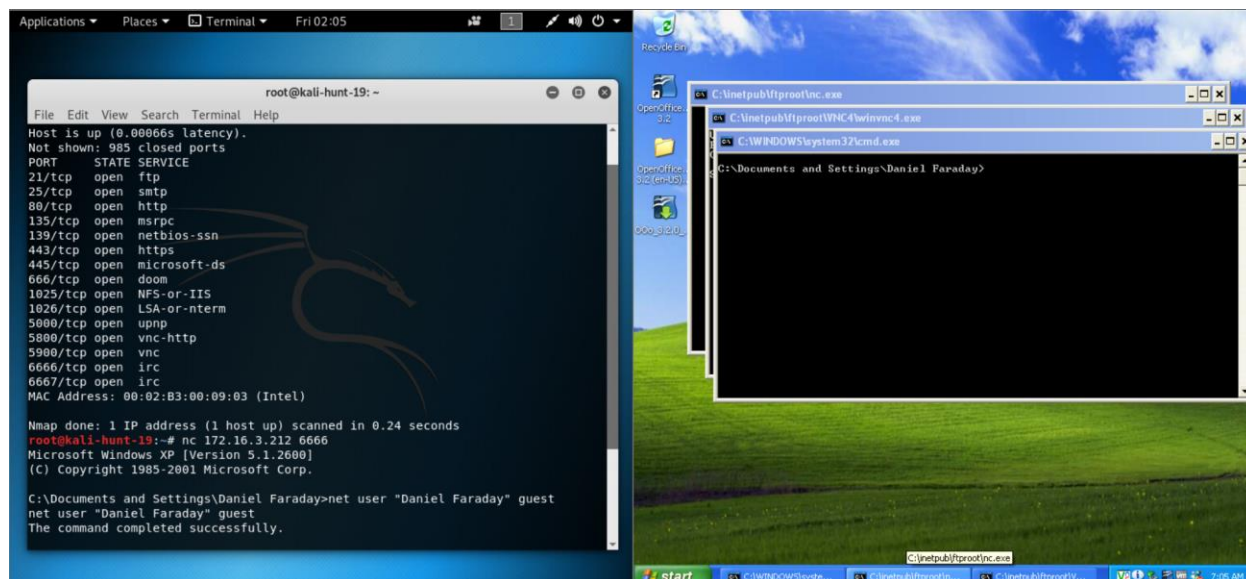
1.



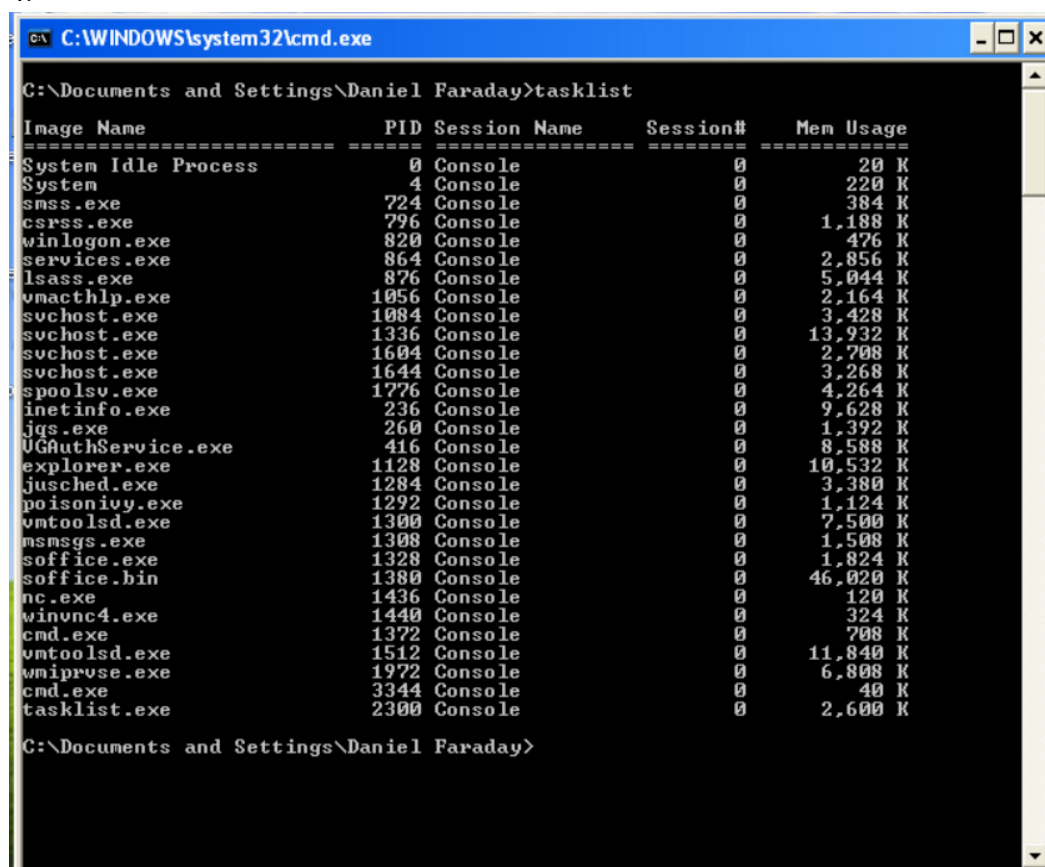
2.

```
root@kali-hunt-19: ~  
File Edit View Search Terminal Help  
Starting Nmap 7.70 ( https://nmap.org ) at 2024-03-08 02:01 EST  
Nmap scan report for 172.16.3.212  
Host is up (0.00066s latency).  
Not shown: 985 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
25/tcp    open  smtp  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
666/tcp   open  doom  
1025/tcp  open  NFS-or-IIIS  
1026/tcp  open  LSA-or-nterm  
5000/tcp  open  upnp  
5800/tcp  open  vnc-http  
5900/tcp  open  vnc  
6666/tcp  open  irc  
6667/tcp  open  irc  
MAC Address: 00:02:B3:00:09:03 (Intel)  
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds  
root@kali-hunt-19:~#
```

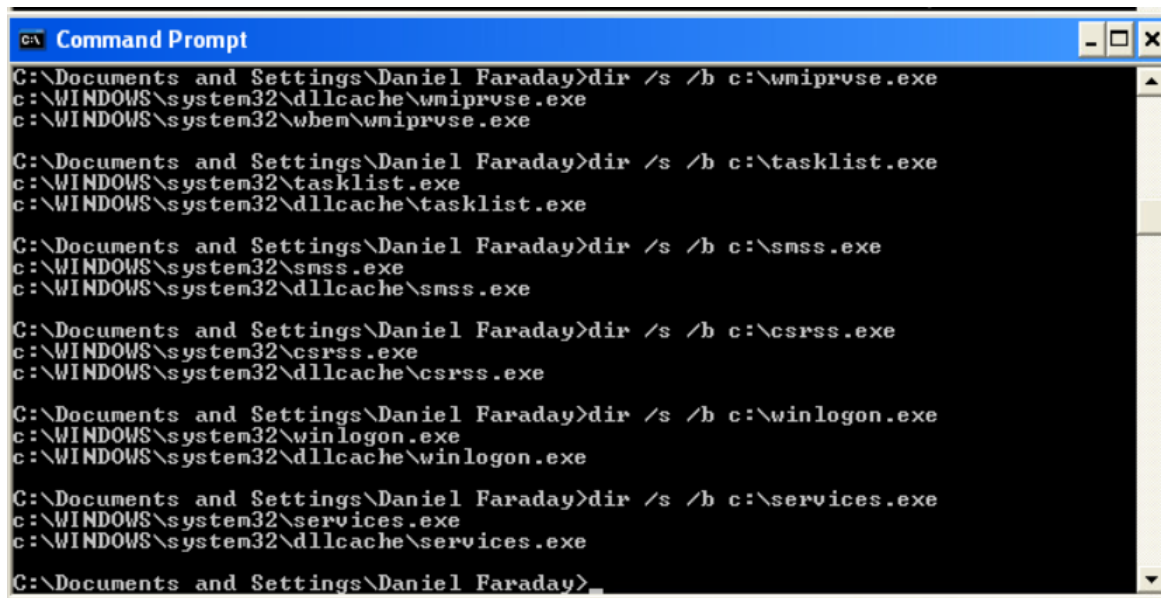
3.



4.



5.



```

C:\Documents and Settings\Daniel Faraday>dir /s /b c:\wmiprvse.exe
c:\WINDOWS\system32\dlldata\wmiprvse.exe
c:\WINDOWS\system32\wbem\wmiprvse.exe

C:\Documents and Settings\Daniel Faraday>dir /s /b c:\tasklist.exe
c:\WINDOWS\system32\tasklist.exe
c:\WINDOWS\system32\dlldata\tasklist.exe

C:\Documents and Settings\Daniel Faraday>dir /s /b c:\smss.exe
c:\WINDOWS\system32\smss.exe
c:\WINDOWS\system32\dlldata\smss.exe

C:\Documents and Settings\Daniel Faraday>dir /s /b c:\csrss.exe
c:\WINDOWS\system32\csrss.exe
c:\WINDOWS\system32\dlldata\csrss.exe

C:\Documents and Settings\Daniel Faraday>dir /s /b c:\winlogon.exe
c:\WINDOWS\system32\winlogon.exe
c:\WINDOWS\system32\dlldata\winlogon.exe

C:\Documents and Settings\Daniel Faraday>dir /s /b c:\services.exe
c:\WINDOWS\system32\services.exe
c:\WINDOWS\system32\dlldata\services.exe

C:\Documents and Settings\Daniel Faraday>

```

6.

```

C:\Windows\System32:
smss.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
svchost.exe
spoolsv.exe
inetinfo.exe
explorer.exe
poisonivy.exe
cmd.exe (2) 2
wmiprvse.exe
tasklist.exe

C:\Program Files\vmware\vmware tools:
vmacthlp.exe
vgauthservice.exe
vmtoolsd.exe (2) ?

C:\Program Files\Java\jre6\bin:
jqs.exe

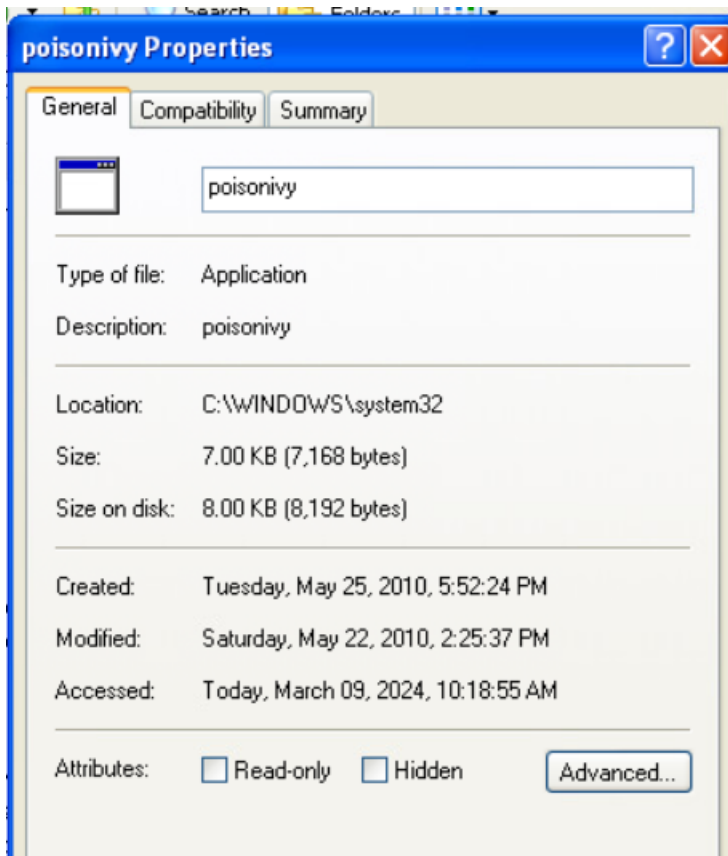
C:\Program Files\Common Files\Java\Java Update:
jusched.exe

C:\Program Files\Messenger:
msmsgs.exe

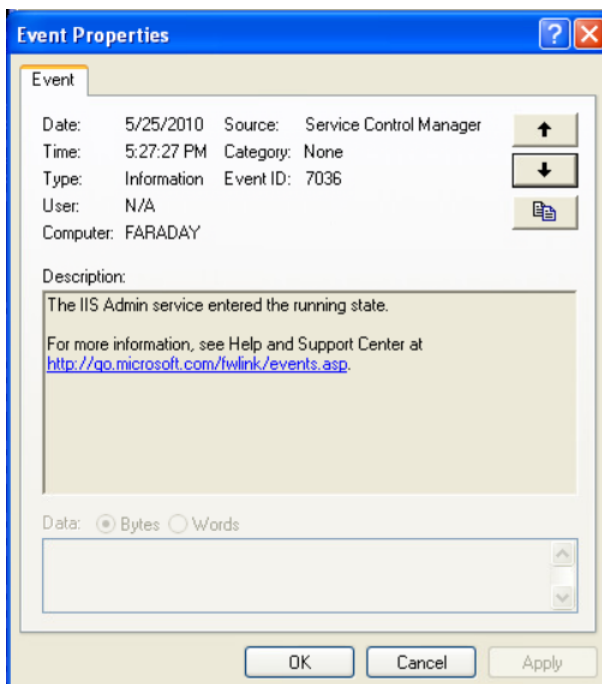
C:\Program Files\OpenOffice.org 3\program\soffice.exe:
soffice.exe
soffice.bin
C:\WINDOWS\Installer\{6ADD0603-16EF-400D-9F9E-486432835002}:
soffice.exe

C:\Inetpub\ftproot:
nc.exe
winvnc4.exe

```

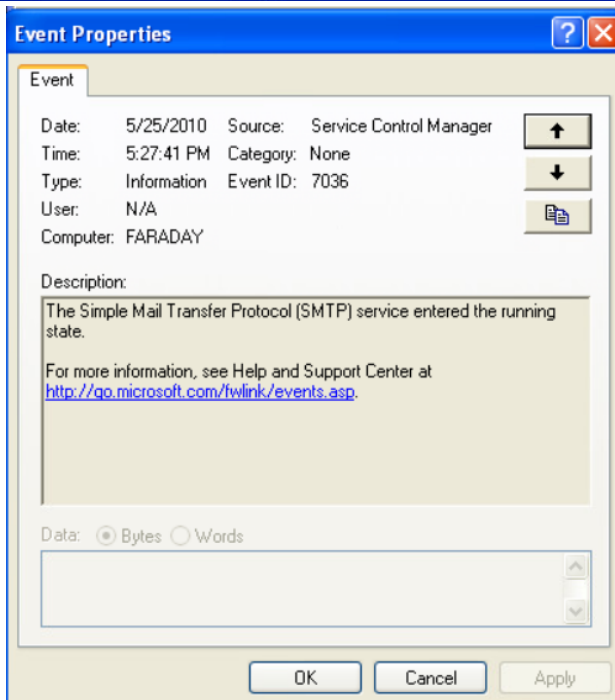
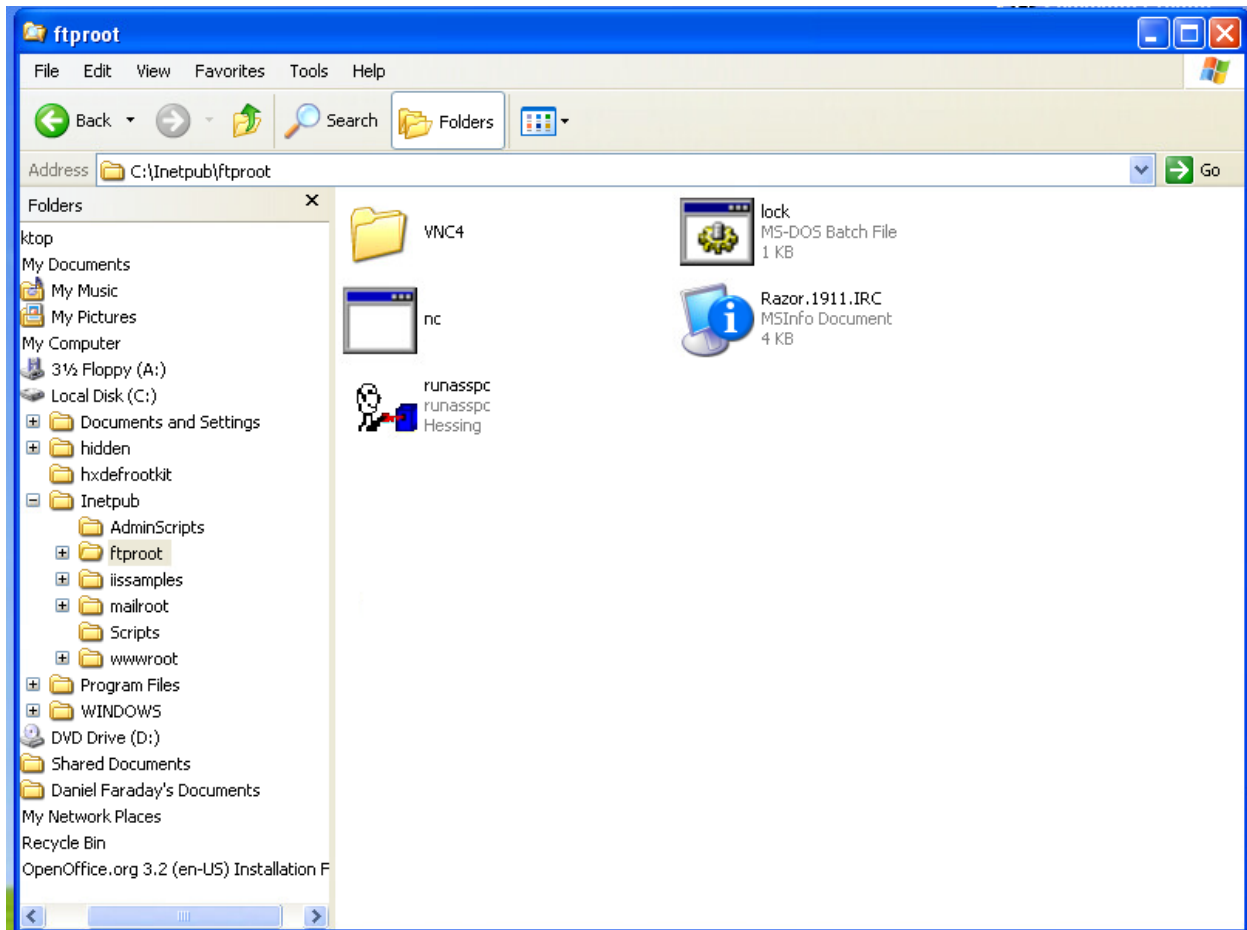


7.

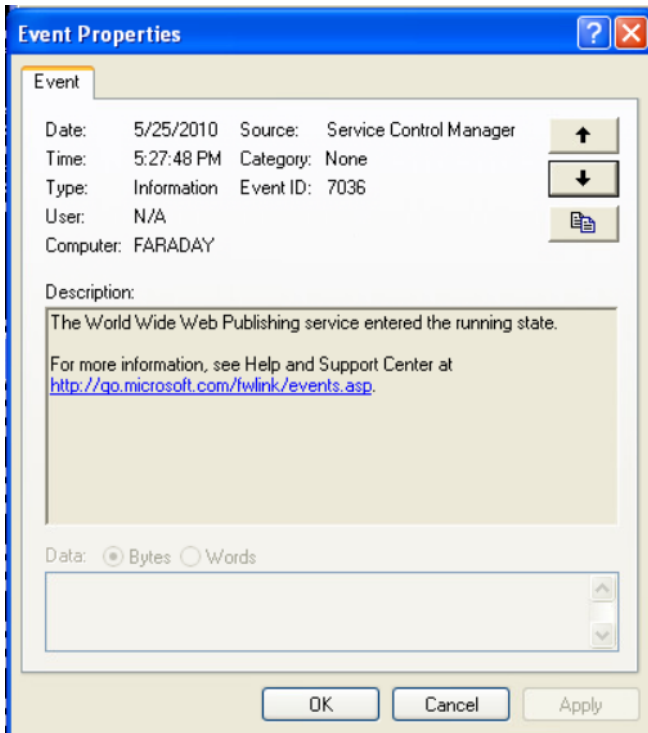


8.

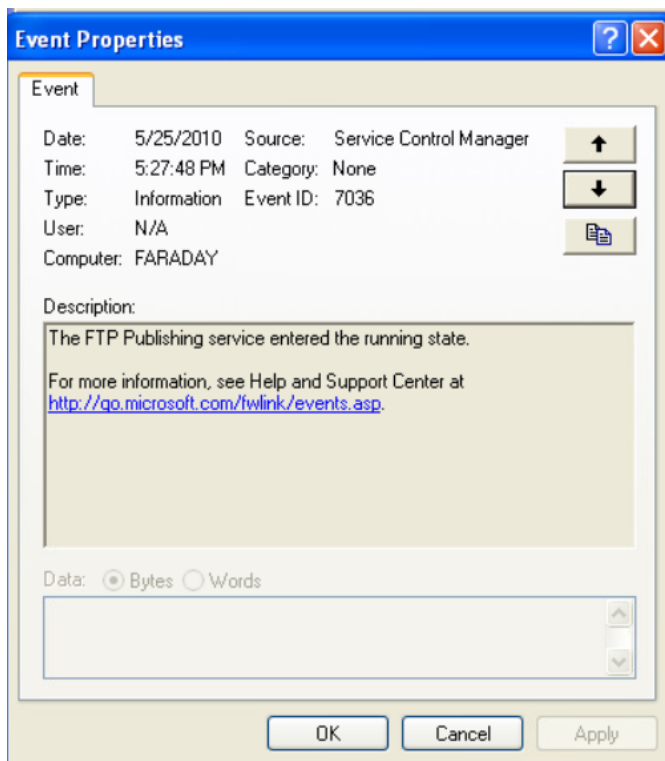
9.



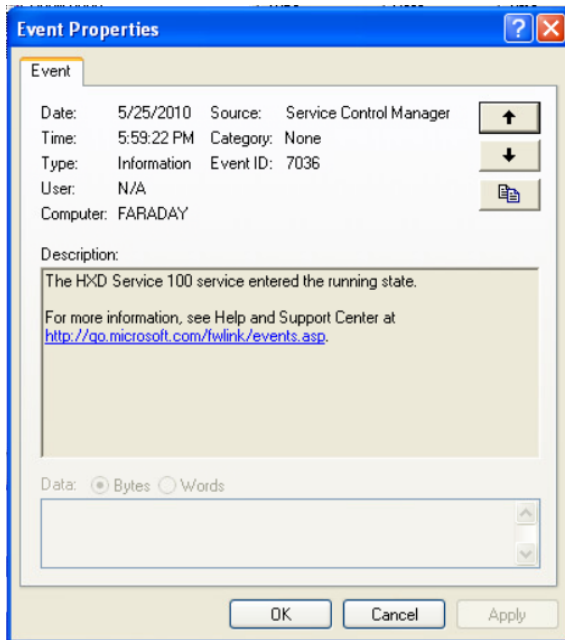
10.



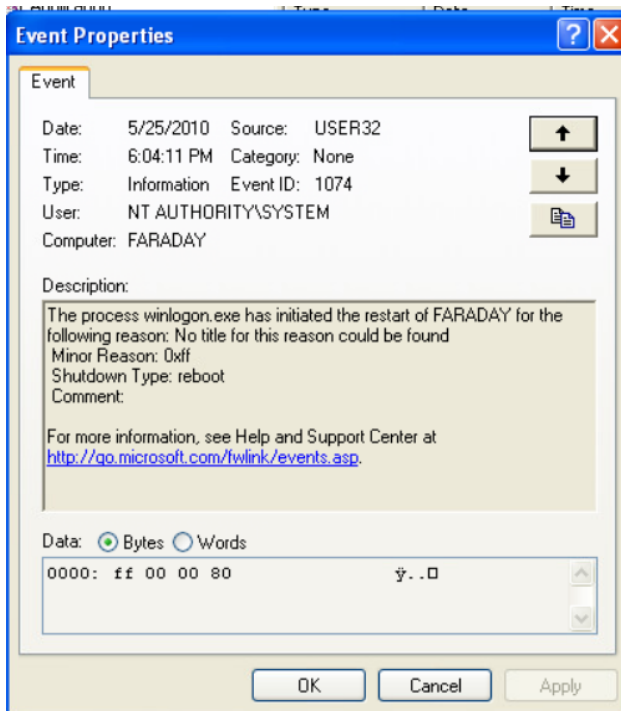
11.



12.



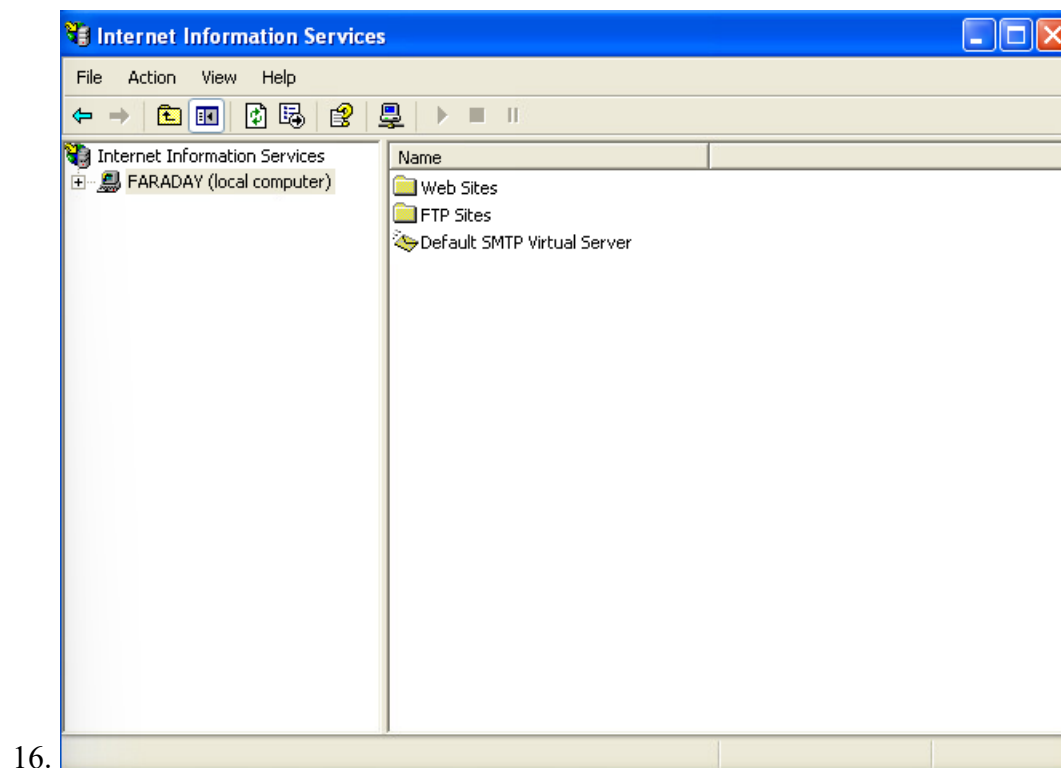
13.



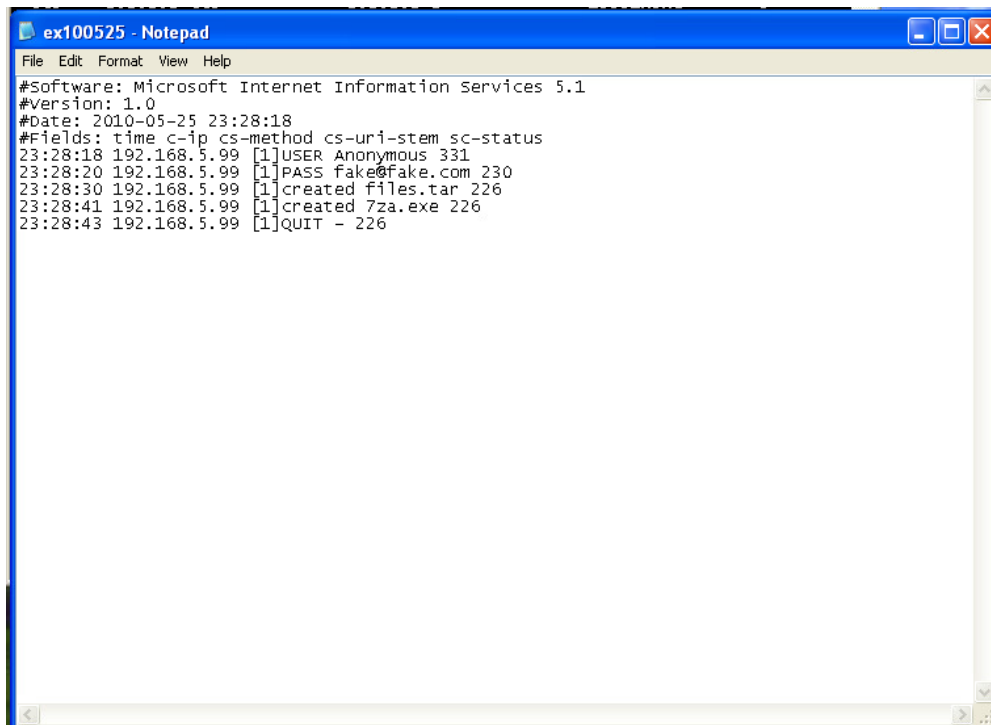
14.

15. Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING	268
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING	268
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	268
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	268
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:666	0.0.0.0:0	LISTENING	328
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	1344
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING	268
TCP	0.0.0.0:2919	0.0.0.0:0	LISTENING	1884
TCP	0.0.0.0:4400	0.0.0.0:0	LISTENING	336
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	1984
TCP	0.0.0.0:5900	0.0.0.0:0	LISTENING	1984
TCP	10.10.0.219:139	0.0.0.0:0	LISTENING	4
TCP	172.16.3.214:139	0.0.0.0:0	LISTENING	4
TCP	172.16.3.214:2919	192.168.5.98:3460	SYN_SENT	1884
TCP	172.16.3.214:6666	0.0.0.0:0	LISTENING	1940



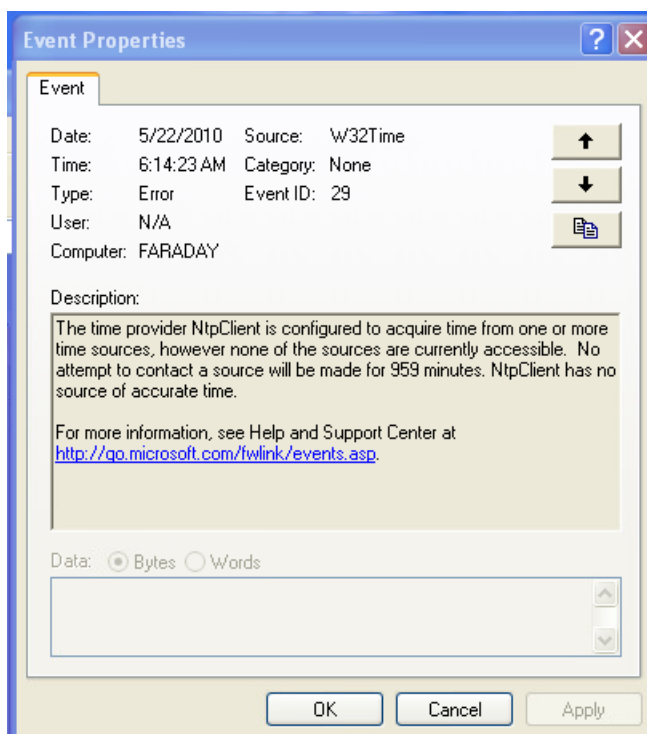
17.



```

#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
  
```

18.



Event Properties

Event

Date: 5/22/2010 Source: W32Time
 Time: 6:14:23 AM Category: None
 Type: Error Event ID: 29
 User: N/A
 Computer: FARADAY

Description:

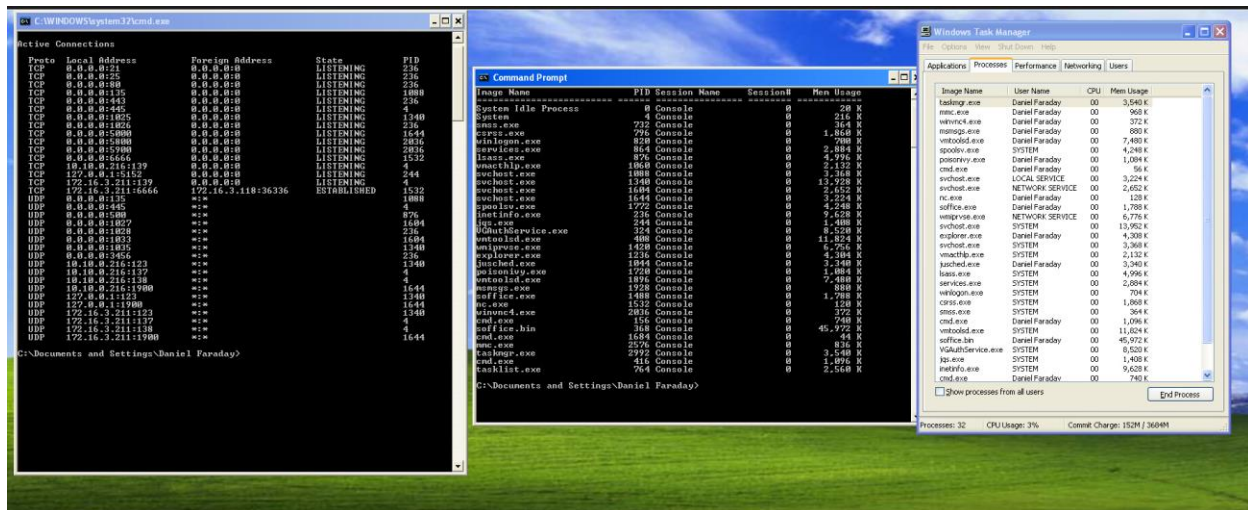
The time provider NtpClient is configured to acquire time from one or more time sources, however none of the sources are currently accessible. No attempt to contact a source will be made for 959 minutes. NtpClient has no source of accurate time.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Data: ☒ Bytes ☐ Words

OK Cancel Apply

21.



Citations:

Alibaba Cloud. YouTube: Home, 9 November 2017, https://topic.alibabacloud.com/a/hxdef100-configuration-and-usage_8_8_31759914.html. Accessed 9 March 2024.

Fisher, Tim. "List of Windows XP Command Prompt Commands." Lifewire, 8 September 2022, <https://www.lifewire.com/windows-xp-commands-4687695>. Accessed 7 March 2024.

IBM. YouTube: Home, 9 November 2017, <https://www.ibm.com/docs/en/i/7.4?topic=i-configuring-anonymous-ftp>. Accessed 7 March 2024.

Jain, Sandeep. "Introduction to Netcat." GeeksforGeeks, 25 April 2023, <https://www.geeksforgeeks.org/introduction-to-netcat/>. Accessed 7 March 2024.

Nmap. “A Quick Port Scanning Tutorial.” Nmap, <https://nmap.org/book/port-scanning-tutorial.html>. Accessed 7 March 2024.

robotronic. Runas with password and encrypted administrator credentials by RunAsSpc, <https://robotronic.net/runasspcen.html>. Accessed 10 March 2024.

Serv-u. “List of FTP Commands for Windows.” Serv-U, <https://www.serv-u.com/ftp-server-windows/commands>. Accessed 7 March 2024.

Speed Guide. “Port 6667 (tcp/udp).” SpeedGuide, <https://www.speedguide.net/port.php?port=6667>. Accessed 7 March 2024.

Unihost. “How to connect to FTP server: step by step tutorial for basic methods.” Unihost, <https://unihost.com/blog/how-to-connect-to-ftp-server/>. Accessed 7 March 2024.