

This lab focused on investigating a compromised Windows XP system that had signs of malware and suspicious activity. The goal was to think like an ethical hacker and a forensic analyst at the same time. I had to break into the system without knowing the password, identify suspicious programs and files, check for malicious connections, and finally test out using FTP to remotely interact with another machine in Simspace. The lab setup simulated what happens after a hacker takes over a computer.

I think Windows XP was chosen for this exercise because it is an old operating system that is no longer supported. That means it is much easier to hack since there are many known exploits and security gaps. In real life, running XP today would be a huge security risk because attackers can use these old flaws to break in. This makes it a good for training and learning because it shows what happens when a system is not updated and still in use.

The overall purpose of the lab was to practice forensic methods and learn how to spot indicators of compromise. The scenario explained that a workstation had been hacked, and malware was used to escalate privileges and gain access to an email server. This setup mirrors how phishing or malware attacks often lead to bigger breaches in the real world. By walking through this exercise, I could see how malware like Poison Ivy or Cryptcat gets planted and how attackers keep control of a compromised machine.

The first step in the lab was to log into the Windows XP system without having the original password. This forced me to go through the process of breaking back into a locked machine, which is something investigators sometimes have to do. The first thing we had to do was starting the machine in Safe Mode(Figure 1). Safe Mode is a boot option that loads only the basic drivers and tools for Windows. It also gives access to system management features.

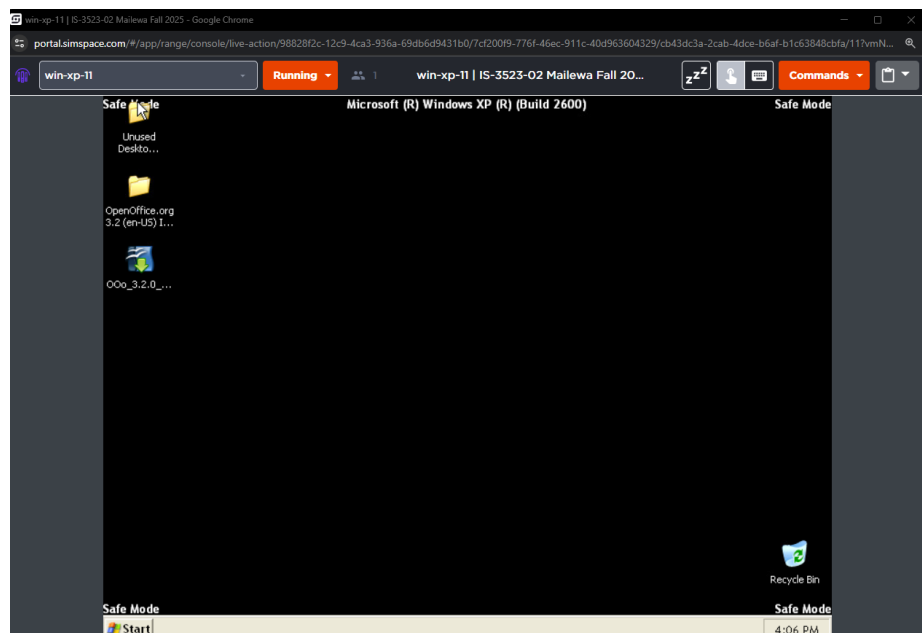


Figure 1

When the XP machine started, I pressed F8 to bring up the boot menu and chose Safe Mode. Once in, I was able to go into “My Computer,” right-click, and open “Manage.” From there, under Local Users and Groups, I could reset the password for the account on the system. The account name in this case was Daniel Faraday. I changed the password to WindowXP! so I could log after rebooting.

This step showed how easy it can be to reset a password on a machine without encryption or strong security policies. On older systems like XP, there is no built-in protection to stop someone with physical or administrative access from resetting a password in Safe Mode. In a real case, this would be both a risk and a forensic opportunity. It is risky because attackers can do the same thing if they get physical access. But it is helpful for investigators because it allows them to get into the system and start gathering evidence. So, it is kind of like a double-edged sword. After resetting the password, I restarted the computer and logged in using the new password. Now I had full access to the system and could begin going through the files and processes.

After logging in I opened Task Manager to see what processes were running. Right away I noticed a suspicious process called Poison Ivy (Figure 2). Poison Ivy is actually a well-known Remote Access Trojan (RAT). A RAT is malware that lets an attacker remotely control a system. Upon further investigation, Poison Ivy has been used for years by attackers because it gives them backdoor access, keylogging features, file transfer options, and the ability to spy on a victim. Seeing it running on the XP machine was a big red flag that the system was compromised.

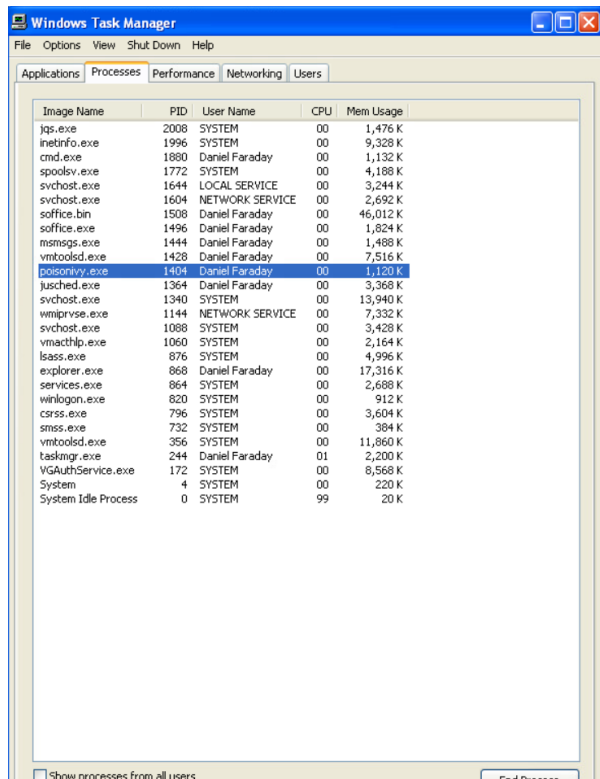


Image Name	PID	User Name	CPU	Mem Usage
jqs.exe	2008	SYSTEM	00	1,476 K
inetinfo.exe	1996	SYSTEM	00	9,328 K
cmd.exe	1880	Daniel Faraday	00	1,132 K
spoolsv.exe	1772	SYSTEM	00	4,188 K
svchost.exe	1644	LOCAL SERVICE	00	3,244 K
svchost.exe	1604	NETWORK SERVICE	00	2,692 K
soffice.bin	1508	Daniel Faraday	00	46,012 K
soffice.exe	1496	Daniel Faraday	00	1,824 K
msmsgs.exe	1444	Daniel Faraday	00	1,488 K
vmtoolsd.exe	1428	Daniel Faraday	00	7,516 K
poisonivy.exe	1404	Daniel Faraday	00	1,120 K
jusched.exe	1364	Daniel Faraday	00	3,368 K
svchost.exe	1340	SYSTEM	00	13,940 K
winiprvse.exe	1144	NETWORK SERVICE	00	7,332 K
svchost.exe	1088	SYSTEM	00	3,428 K
vmacthlp.exe	1060	SYSTEM	00	2,164 K
lsass.exe	876	SYSTEM	00	4,996 K
explorer.exe	868	Daniel Faraday	00	17,316 K
services.exe	864	SYSTEM	00	2,688 K
winlogon.exe	820	SYSTEM	00	912 K
csrss.exe	796	SYSTEM	00	3,604 K
smss.exe	732	SYSTEM	00	384 K
vmtoolsd.exe	356	SYSTEM	00	11,860 K
taskmgr.exe	244	Daniel Faraday	01	2,200 K
VGAUTHService.exe	172	SYSTEM	00	8,568 K
System	4	SYSTEM	00	220 K
System Idle Process	0	SYSTEM	99	20 K

Figure 2

Another suspicious file I discovered was Cryptcat.exe(Figure 3). Cryptcat is a tool similar to Netcat, which is often called a “Swiss Army knife” for networking. Attackers use Netcat to create backdoors, transfer files, or set up remote shells. Cryptcat is basically Netcat but with encryption, which makes it harder to detect. If an attacker plants Cryptcat, they can use it to open secret channels with the compromised machine and communicate without raising alarms. The fact that I saw Cryptcat meant the attacker wanted to hide their traffic and make the connection more secure for themselves.

I also found rundll32.exe in the Prefetch folder(Figure 3). Prefetch is a feature in Windows that stores information about programs that have been run so they can load faster next time. By checking Prefetch, investigators can see what programs were executed on the system. Rundll32.exe itself is a legitimate Windows file, but attackers often abuse it to run malicious code. If malware disguises itself under rundll32, it can look like a normal Windows process while actually running harmful instructions. The Prefetch entries confirmed that rundll32.exe, Poison Ivy, and Cryptcat had all been executed on this machine.

These discoveries showed me that the system was definitely backdoored and under remote control. Poison Ivy allowed the attacker to take over, Cryptcat gave them encrypted communication, and rundll32.exe was probably being abused.

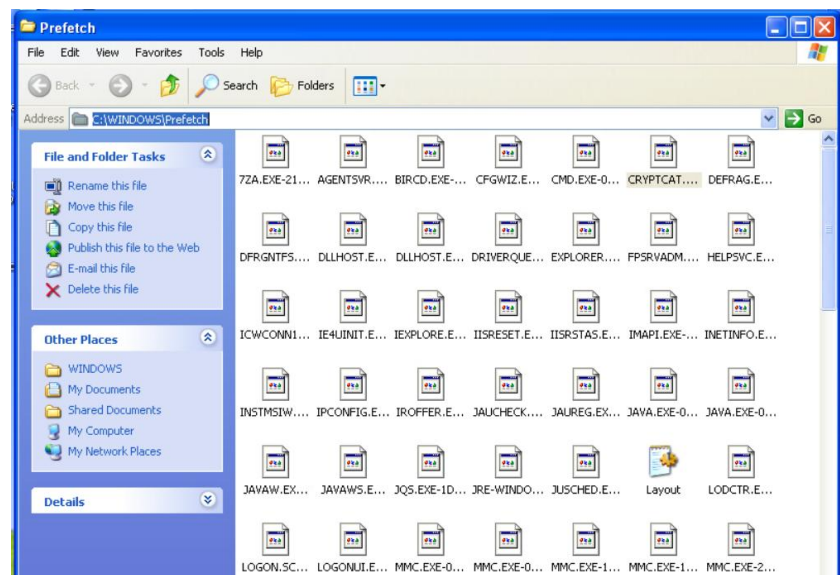


Figure 3

The next step was checking for live network connections. In the command prompt, I ran the command netstat -ano(Figure 4). This command shows all active connections, the ports being used, and the process IDs that are tied to those connections. By matching the process IDs with Task Manager, I could see which programs were talking to outside addresses.

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Active Connections

Proto Local Address          Foreign Address         State       PID
TCP    0.0.0.0:21              0.0.0.0:0               LISTENING   1996
TCP    0.0.0.0:25              0.0.0.0:0               LISTENING   1996
TCP    0.0.0.0:80              0.0.0.0:0               LISTENING   1996
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING   1088
TCP    0.0.0.0:443             0.0.0.0:0               LISTENING   1996
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   196
TCP    0.0.0.0:1025            0.0.0.0:0               LISTENING   1340
TCP    0.0.0.0:1027            0.0.0.0:0               LISTENING   1996
TCP    0.0.0.0:4400            0.0.0.0:0               LISTENING   200
TCP    0.0.0.0:5000            0.0.0.0:0               LISTENING   1644
TCP    10.10.0.225:139         0.0.0.0:0               LISTENING   4
TCP    127.0.0.1:5152          0.0.0.0:0               LISTENING   2008
TCP    172.16.3.221:139        0.0.0.0:0               LISTENING   4
UDP    0.0.0.0:135             *:*:                    1088
UDP    0.0.0.0:445             *:*:                    4
UDP    0.0.0.0:500             *:*:                    876
UDP    0.0.0.0:1026            *:*:                    1340
UDP    0.0.0.0:1028            *:*:                    1604
UDP    0.0.0.0:1029            *:*:                    1996
UDP    0.0.0.0:1034            *:*:                    1340
UDP    0.0.0.0:3456            *:*:                    1996
UDP    10.10.0.225:123         *:*:                    1340
UDP    10.10.0.225:137        *:*:                    4
UDP    10.10.0.225:138        *:*:                    4
UDP    10.10.0.225:1900        *:*:                    1644
UDP    127.0.0.1:123           *:*:                    1340
UDP    127.0.0.1:1900          *:*:                    1644
UDP    127.0.0.1:46789         *:*:                    200
UDP    172.16.3.221:123        *:*:                    1340
UDP    172.16.3.221:137        *:*:                    4
UDP    172.16.3.221:138        *:*:                    4
UDP    172.16.3.221:1900        *:*:                    1644

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

Figure 4

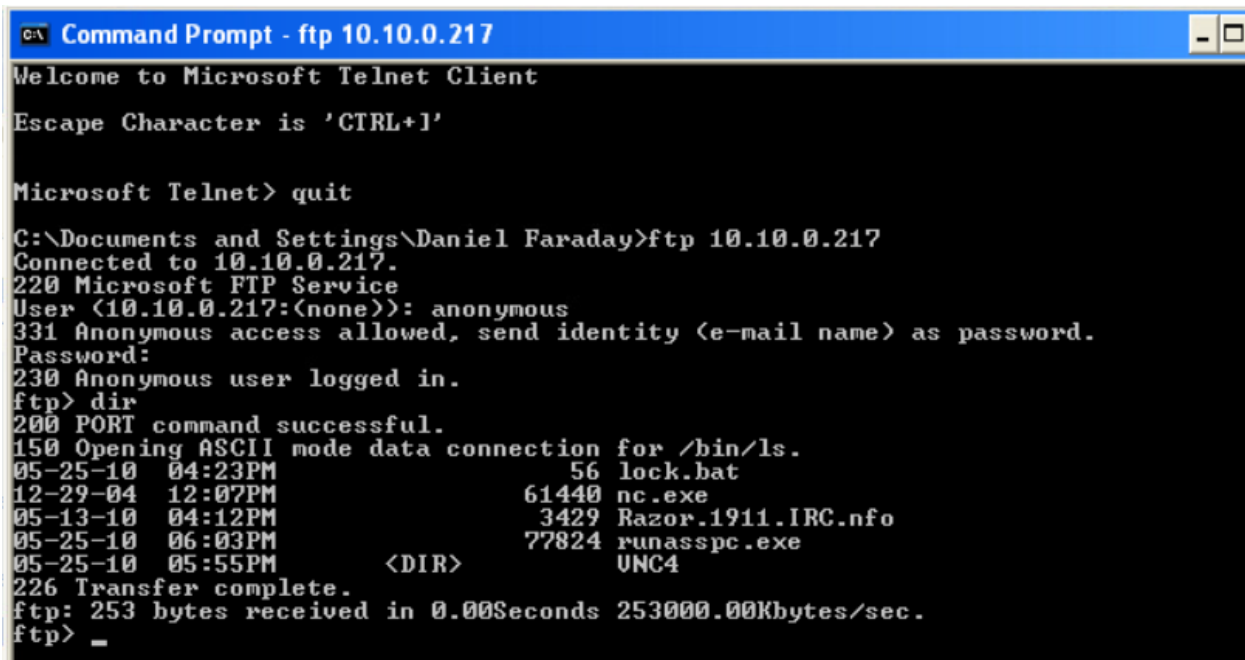
When I looked at the results, I saw suspicious established connections. These connections linked back to processes like Poison Ivy and Cryptcat. This means the system was actively communicating with an external attacker. The presence of established sessions shows that the attacker not only had planted malware but was also using it to maintain live control over the machine.

The fact that the machine had multiple connections open suggests the attacker may have been moving data or waiting for commands. Since this was an FTP server, it makes sense that the attacker would use it as a point for file transfers.

The lab instructions also included using FTP from another machine to connect back to the hacked XP system. FTP stands for File Transfer Protocol. It is one of the oldest ways to transfer files between computers over a network. Attackers and administrators both use FTP because it is simple and works on almost any system. The weakness is that FTP is not secure. It sends usernames and passwords in plain text, which makes it easy to intercept.

To test FTP(Figure 5), I opened the command prompt got into another virtual machine. The other machine was Win-XP-3 and typed ftp 10.10.0.217. After hitting enter, I was prompted for a username and password. Here I used the anonymous way to log in and had to use my

email. Once I logged in, I used the dir command to list the directory contents of the remote machine. This showed me the files that were accessible. Finally, I typed quit to close the FTP session.



```
C:\ Command Prompt - ftp 10.10.0.217
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+I'

Microsoft Telnet> quit

C:\Documents and Settings\Daniel Faraday>ftp 10.10.0.217
Connected to 10.10.0.217.
220 Microsoft FTP Service
User (10.10.0.217:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
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>          UNC4
226 Transfer complete.
ftp: 253 bytes received in 0.00Seconds 253000.00Kbytes/sec.
ftp> _
```

Figure 5

This exercise showed how FTP can be used to interact with a compromised system. For an attacker, FTP is a quick way to move stolen data off the machine. For an investigator, it is a way to confirm access and check what directories are exposed. In this case, just being able to log in and list the directory confirmed that the XP machine was set up as an FTP server and was vulnerable to remote connections.

Based on the investigation, it looks like the XP machine was compromised by malware that was planted to give remote access. The presence of Poison Ivy shows that the attacker wanted full control of the system. Cryptcat shows that they wanted secure, hidden communication. Rundll32 abuse and Prefetch evidence confirm that these programs were run multiple times. Netstat results backed this up by showing active connections to outside systems.

The likely way the attacker first got in could have been phishing, which was mentioned in the lab scenario. If the user ran a bad attachment or clicked on a link, malware could have been installed. From there, the attacker escalated privileges, planted Poison Ivy and Cryptcat, and then used the system as an FTP server to move data.

The attacker's goal was probably to steal sensitive information or use the XP machine to reach other systems. Poison Ivy and Cryptcat are both tools that point to an attacker since they are not just random viruses but chosen tools for remote control and encrypted communication.

What I learned from this lab was how important it is to investigate compromised systems in detail. By going through the steps in the lab like Safe Mode resets, Task Manager

checks, Prefetch analysis, netstat commands, and FTP testing, I was able to piece together what happened. The XP machine was compromised with PoisonIvy.exe, Cryptcat.exe, and rundll32 being the main indicators of compromise.

In conclusion, old systems like Windows XP are easy targets since they don't have modern security. Malware usually leaves signs if you know where to look. Hackers like to use tools such as RATs and backdoors so they can stick around on a system for a long time without being noticed like the hacker in the Cuckoo's Egg book. FTP is easy to use but not secure at all, and a bad actor can use it to steal data. Even small things, like Prefetch entries or strange processes in Task Manager, can be enough to figure out what really happened on a system as well.

## References

- YouTube Video: Learn Tech (n.d.). *Add and Delete User Accounts With Command Prompt in Windows*. YouTube. <https://www.youtube.com/watch?v=wkndnNEv20Q>
- YouTube Video: TechMeSpot. (n.d.). *How to Change Your Account Password using Command Prompt on Windows 10*. YouTube. [https://www.youtube.com/watch?v=3nrEb3Z\\_R5A](https://www.youtube.com/watch?v=3nrEb3Z_R5A)
- YouTube Video: MilanS Academy. (n.d.). *Old-Fashioned FTP Client Tutorial* (demonstration of using FTP in Windows). YouTube. <https://www.youtube.com/watch?v=WPRVS-zk9T4>
- Cybersecurity & Communications Integration Cell. (n.d.). *Poison Ivy: Trojan* [Web page]. New Jersey Cybersecurity & Communications Integration Cell. <https://www.cyber.nj.gov/threat-landscape/malware/trojans/poison-ivy>
- ScienceDirect. (n.d.). *Cryptcat* [Web page]. In Computer Science Topics. <https://www.sciencedirect.com/topics/computer-science/cryptcat>
- Red Canary. (2022). *rundll32 technique* [Threat detection report]. <https://redcanary.com/threat-detection-report/techniques/rundll32/>
- CyberForensicator57. (2020, April 15). *Prefetch files 101* [Blog post]. Medium. <https://medium.com/@cyberforensicator57/prefetch-files-101-2b19218124df>
- Forensics Wiki. (n.d.). *Windows Prefetch files: Forensics guide*. <https://forensics.wiki/prefetch/#:~:text=Windows%20Prefetch%20files%2C%20introduced%20in,supports%20hybrid%20hard%20disk%20drives>