University of Texas at San Antonio

Lab Report 3

Vincent Cruz (hza026)

IS 3523-003

Juan Munoz

November 16, 2022

Introduction

This lab report covers the response to a simulated incident including a computer suspected of containing malware. Malware is a growing problem today and must be handled carefully to prevent its spread to more computers. Working with a "virtual image" will help to ensure the malware does not spread to my computer during the analysis. This is one of the many upsides to using virtual machines. Tools on other virtual machines will be used to investigate files on the suspect computer.

Procedures

Upon opening the windows XP VM, two user accounts are available to log into. As expected, both accounts are password protected. There is not much to go off of so far, but with some scanning, there will surely be a weakness to use in order to get into the computer.

After looking at the IP address ISCS-Security subnet connection on the Windows XP virtual machine (VM), the IP address was found to be 172.16.3.216 along with another IP address of 10.10.0.221. With this information, the Windows XP can be pinged from another VM to check for a working connection. A kali VM was used to ping the XP machine and was successful in making a connection. A screen capture of the ping results will be pasted in the appendix labeled as Image A.

To gain information about the Windows XP VM and its possible open ports, nmap will be used to scan it. After looking through the nmap scan results, an important component of the results is the open ports. If I can gain access to the open ports on the XP VM, there is important information about the users which is accessible. Two of the open ports were 6666 and 6667, which are IRC chat channels. Using these ports would enable the kali VM to talk directly to the XP VM. A screen capture of the nmap results will be placed in the appendix labeled Image B.

Netcat will be a great way to communicate with the XP machine through this port. After trying to run netcat to connect to 172.16.3.216, the connection is refused. This is likely because this IP sits behind a NAT or has better security. However, when the same command was run with the 10.10.0.221 IP address, the IRC connection was established. Once the connection was established, I ran the command net user which allows changes to be made to user accounts. I then changed the password of the administrator account to my own password. A screen capture of this command will be provided in the appendix under Image C.

Now that the Windows XP machine was able to be accessed, the next step was to create an image of the disk to be sent to a separate virtual machine to be examined using Autopsy. However, after countless hours and many obstacles between getting the disk file formatted correctly for Autopsy, the file size being too big for FTP, and the Windows XP machine running

out of space to hold the image file, the conclusion was made that this approach would not be the optimal solution anymore.

Instead, the XP machine would be examined for suspicious files using command prompt and file explorer. After spending some time scrolling through file directories, it is clear the first files were put on the XP machine around the year 2001. Though dates of malicious files can likely be spoofed, I inferred that any malicious files downloaded onto this VM would be long after the year 2001.

Furthermore, knowing that most malware/spyware are downloaded as applications so as to run themselves on the machine, I narrowed the searched down to .exe files. Combining this reasoning with the previous paragraph, I sorted the .exe files by date, to skip over the files from 2001. At the top of the search results was an application file named poisonivy. After googling the suspicious name, Poison Ivy is known to be a remote access trojan (NJCCIC). A screen capture showing the file is in the appendices labeled Image D.

After looking through log files which were modified near the date the poison ivy file was modified, there was clear evidence of new accounts being created. The screen capture will be posted in the appendices under Image E. The IP address from these logs is far different from the current IP address belonging to the VM.

Conclusion

The Windows XP VM was able to be logged into using nmap to locate open ports on the computer, and next using netcat and using the open port used for IRC communication to modify the admin's password. The VM was victim to a Remote Access Trojan used to steal files and credentials. More clear evidence lies in the log files which proceeded the RAT being installed in May 2010.

Appendices

Image A

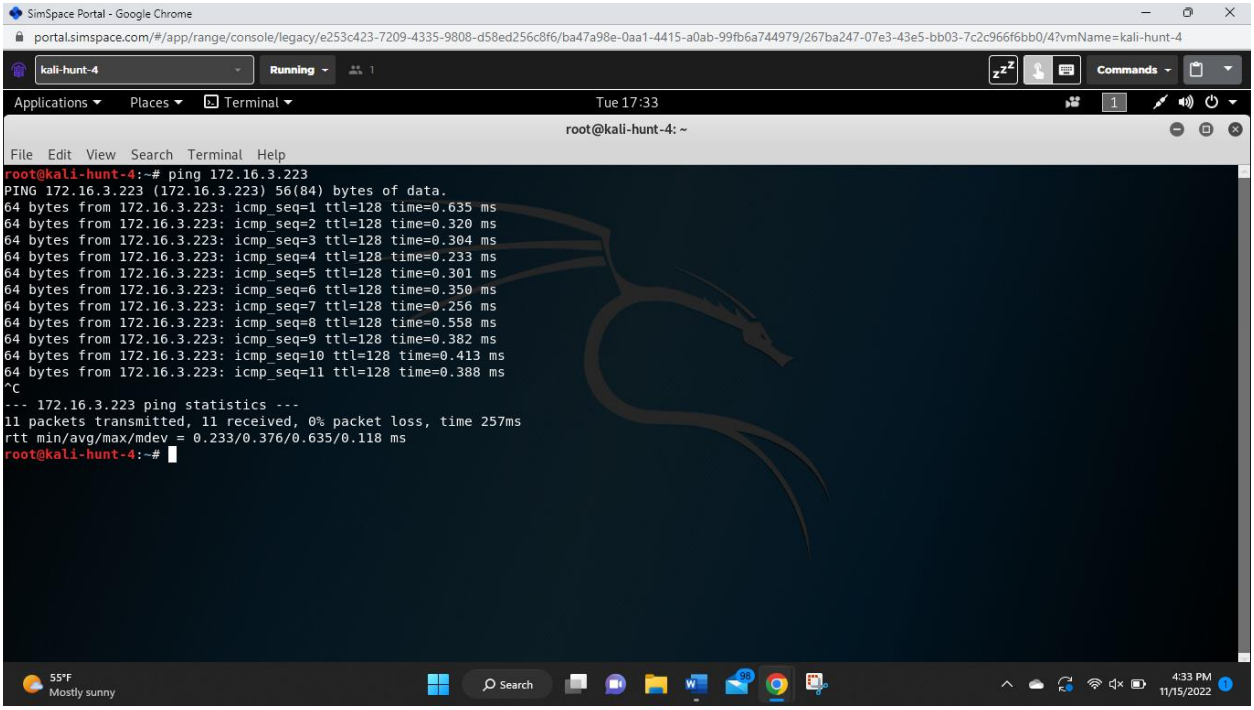


Image B

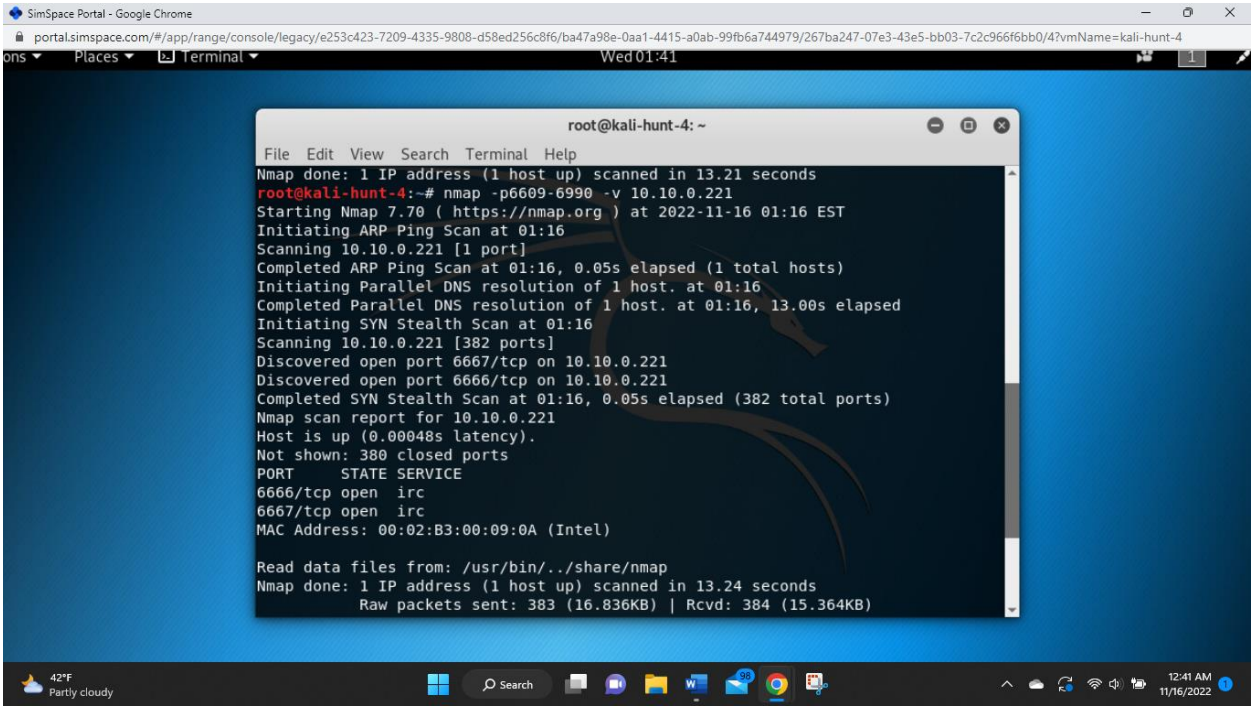


Image C

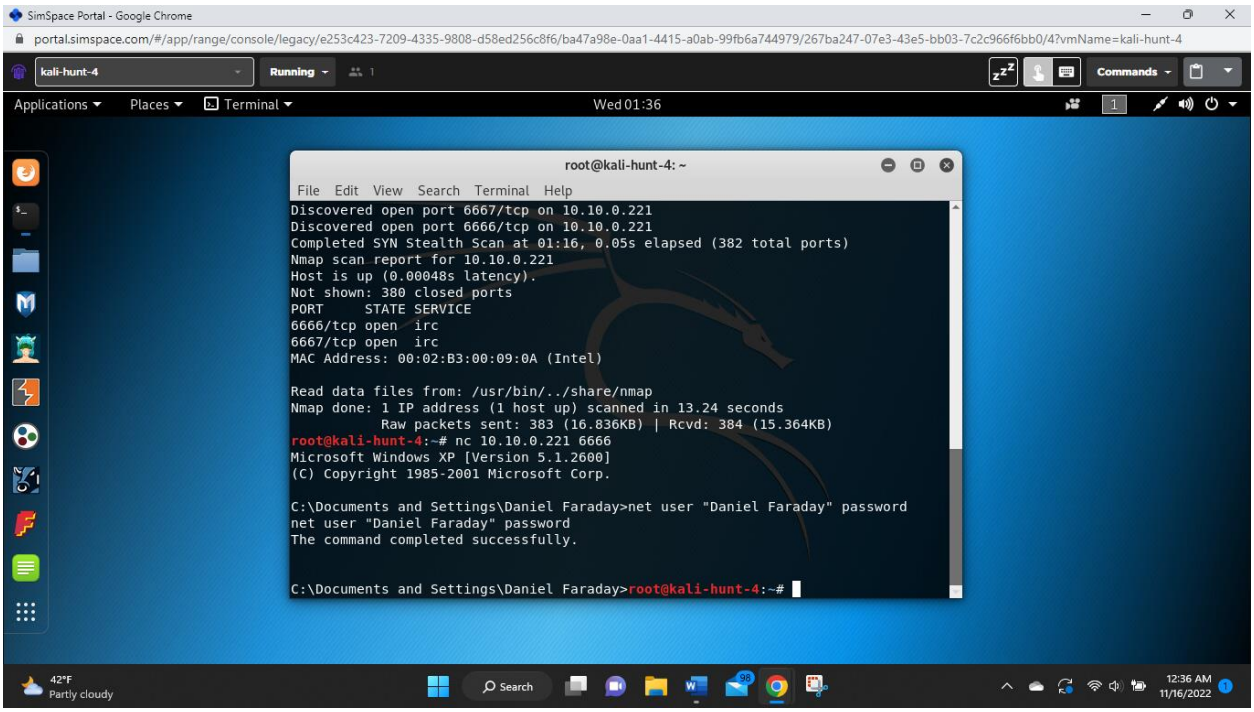


Image D

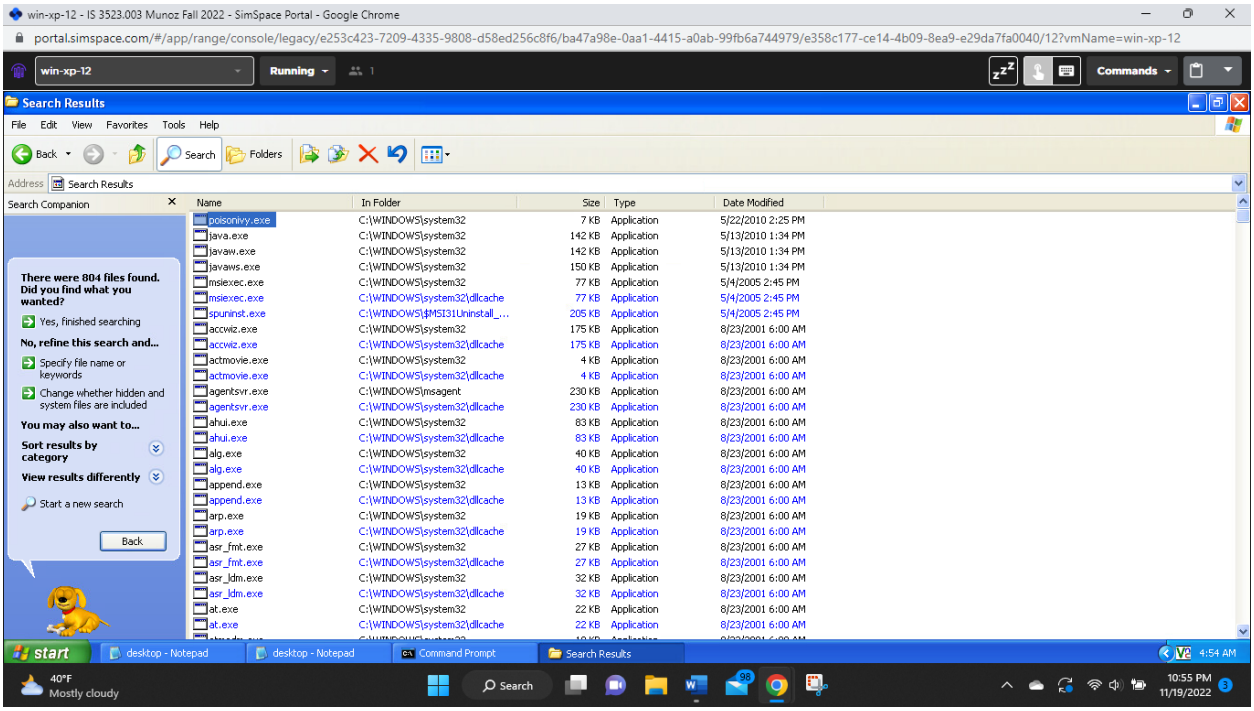
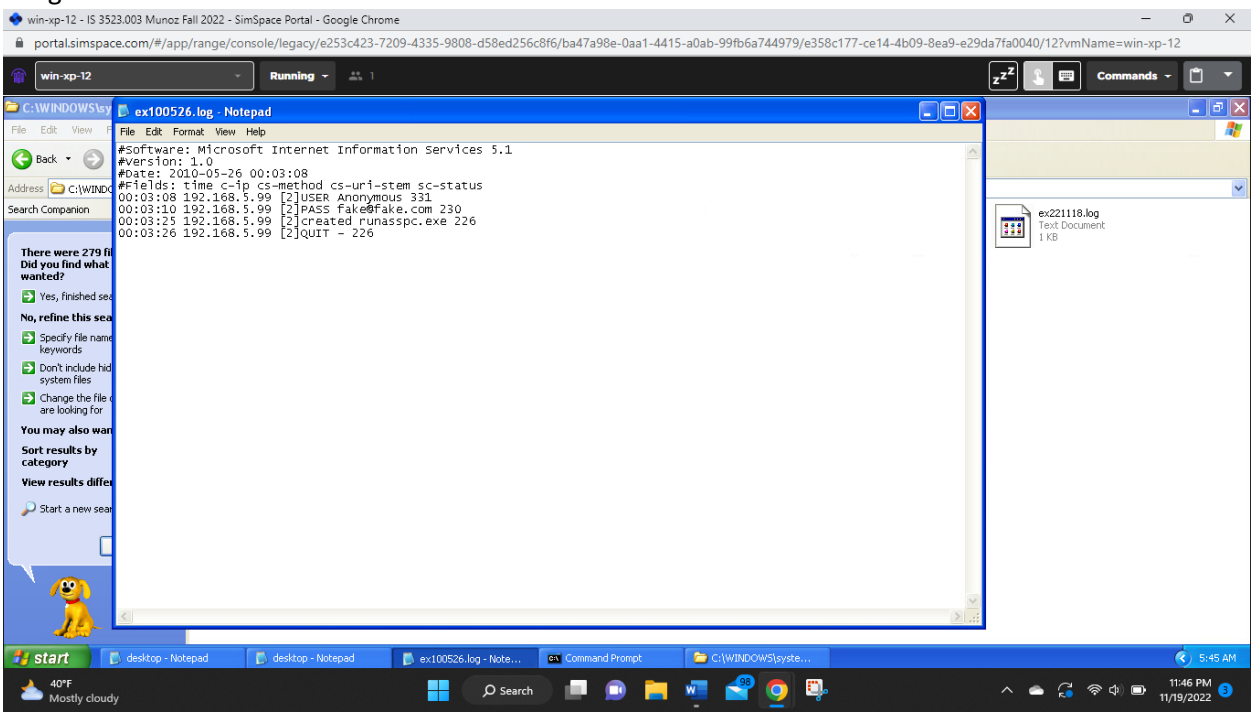


Image E


win-xp-12 - IS 3523.003 Munoz Fall 2022 - SimSpace Portal - Google Chrome
portal.simspace.com/#/app/range/console/legacy/e253c423-7209-4335-9808-d58ed256c8f6/ba47a98e-0aa1-4415-a0ab-99fb6a744979/e358c177-ce14-4b09-8ea9-e29da7fa0040/12?vmName=win-xp-12
win-xp-12
Running
Commands
ex100526.log - Notepad
File Edit Format View Help
#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
ex221118.log
Text Document
1 KB
start
desktop - Notepad
desktop - Notepad
ex100526.log - Note...
Command Prompt
C:\WINDOWS\syste...
5:45 AM
40°F
Mostly cloudy
Search
11:46 PM
11/19/2022

Works Cited

"Poison Ivy", NJCCIC, 4/12/2017. https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/poison-ivy