Lab5: Network Penetration Testing Methodology-Internal (2/3)

INFO40587: ETHICAL HACKING

Kevin Harianto| 991602128| June 14, 2024

Contents

Contents

Executive Summary

{state the objectives, approaches, methods/tools used, learning outcome, comments/overall observations}.

The objective of this lab is the continuation of internal penetration testing, where tools such as Python, Metasploit, nmap, Finger as well as GUI tools such as Cain and Abel and LophtCrack will be leveraged.

Approach:
Starting off with Python in order to grab the banner of the ssh Service in relation for executing reconnaissance on Exercise 8, we have basically broken down a Python script and how it could be used to gain insight on a socket/connection. This means that we basically leverage python from the terminal which allowed us to learn about the importance of Python and how it could be leveraged to gain insight on a remote system or connection. This leads to my observation of how sockets can be used to gain insight on Services with Banner grab.

2nd Approach:
I have also leveraged Metasploit to fingerprint the version of HTTP and determine if there are any possible vulnerabilities. I also was able to observe the configuration files for later modification.

3rd Approach:
This approach I have learned from the lab involves leveraging nmap to gain insight on the SMB. This allowed me to learn about how nmap -sC can gain insight on the IP targeted such as the security mode.

4th Approach:
This approach goes more in depth with nmap from exercise 11, however it showcases how nmap is able to go through the subnet of the IP target for any live machines to target, as well as to look into any misconfigured services, specifically RPC. This allowed me to observe and understand how nmap is not just able to be used for fingerprinting in relation to search up vulnerabilities but is able to actively find the vulnerable systems and highlight them themselves.

5th Approach:
This approach involves the Finger protocol on the terminal, and it has allowed me to observe how the command is able to return logged in user information.

6th Approach:
From exercise 13, I have approached penetration testing using Cain and Able where I learned how to input a scan in between IP addresses to intercept passwords.

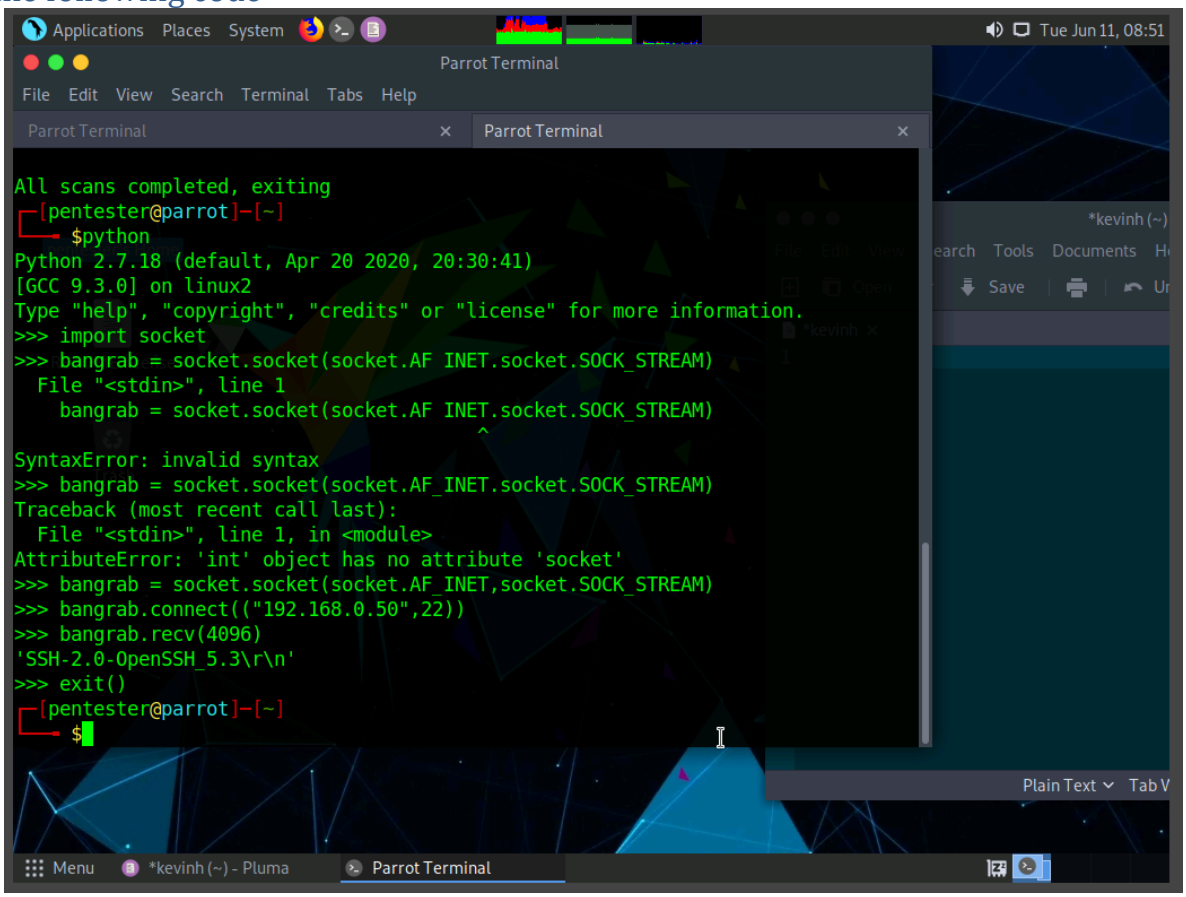
7th Approach:
From exercise 14, I have approached the penetration testing methodology using a Brute Force method using LophtCrack where I learned about how dictionary attacks can be simplified in a GUI manner to make password cracking easier.

8th Approach: I have approached penetration testing using Bash Scripts instead of Python where I learned several commands as well as insight on some of the Bash Script functionalities for executing penetration testing.

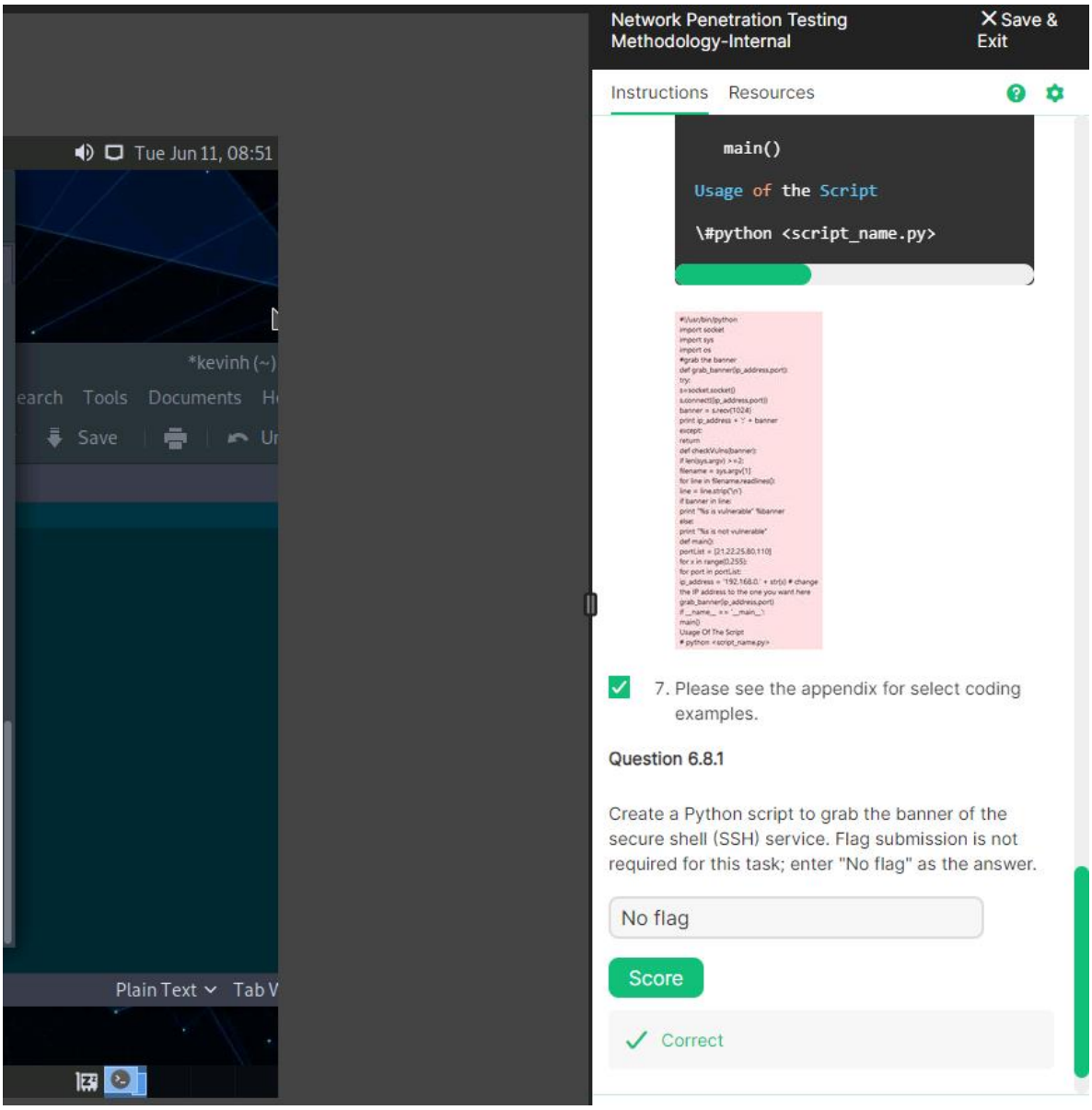
Exercise 8: Create a Python Script to Grab the Banner of the ssh Service

8.1 OUTPUT SCREENSHOTS

Exercise 8, Step 3: Open a terminal window on the Parrot machine and enter the following code



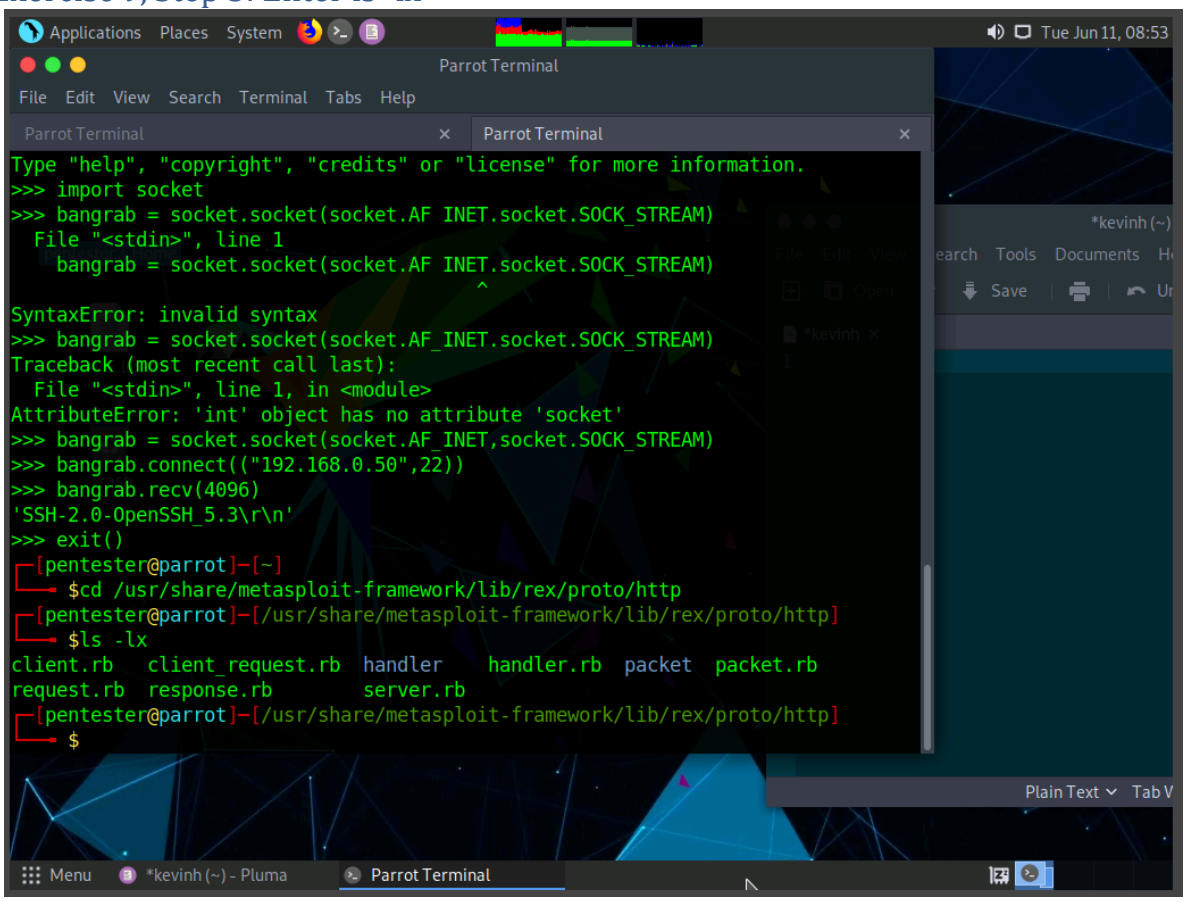
8.2 Questions


Tue Jun 11, 08:51
*kevinh (~)
earch Tools Documents H
Save
Plain Text
Tab V
Network Penetration Testing Methodology-Internal
Save & Exit
Instructions
Resources
main()
Usage of the Script
\#python <script_name.py>
7. Please see the appendix for select coding examples.
Question 6.8.1
Create a Python script to grab the banner of the secure shell (SSH) service. Flag submission is not required for this task; enter "No flag" as the answer.
No flag
Score
Correct

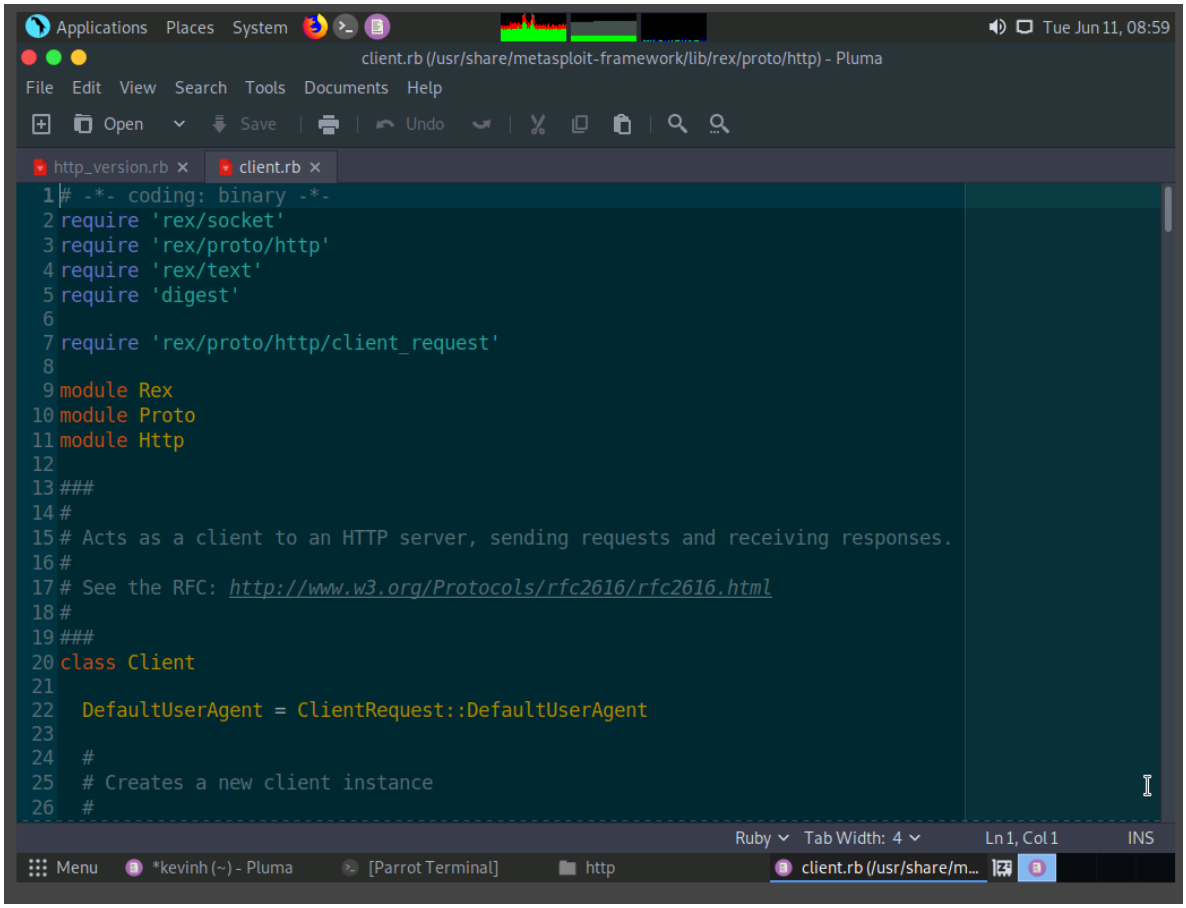
Exercise 9: Use Metasploit to Detect Version of HTTP

9.1 OUTPUT SCREENSHOTS

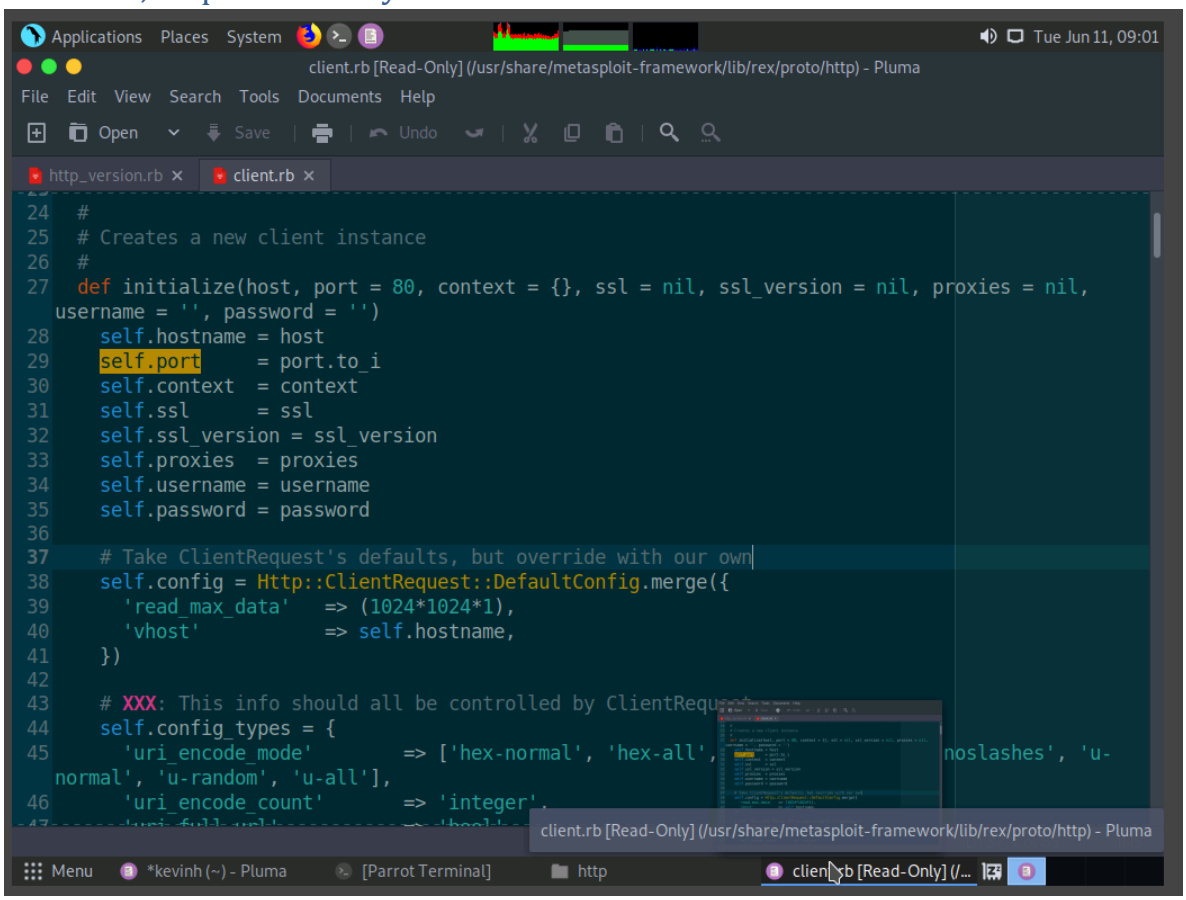
Exercise 9, Step 5: Enter ls -lx



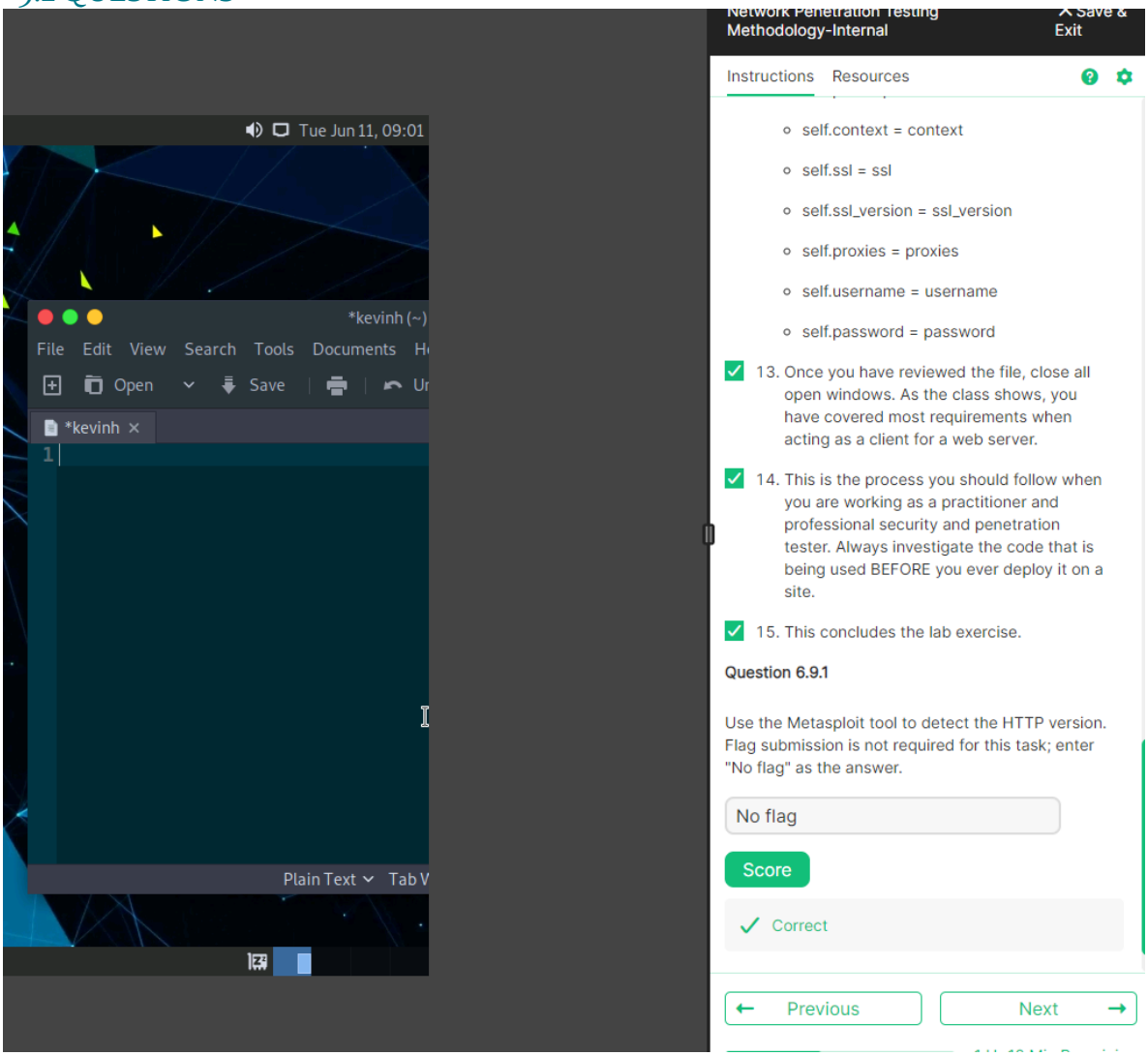
Exercise 9, Step 11: An example of an excerpt of the code is shown in the screenshot



Exercise 9, Step 12: The key to this routine is in the defined class:



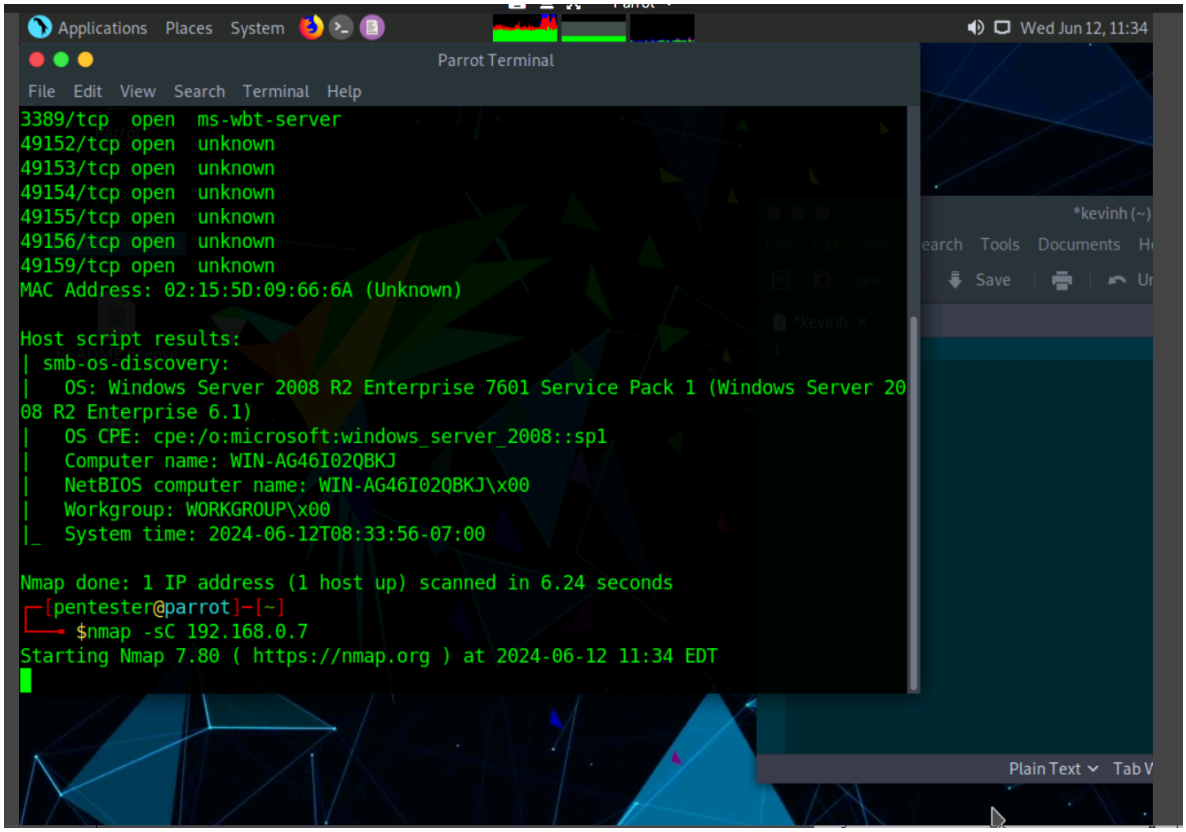
9.2 QUESTIONS



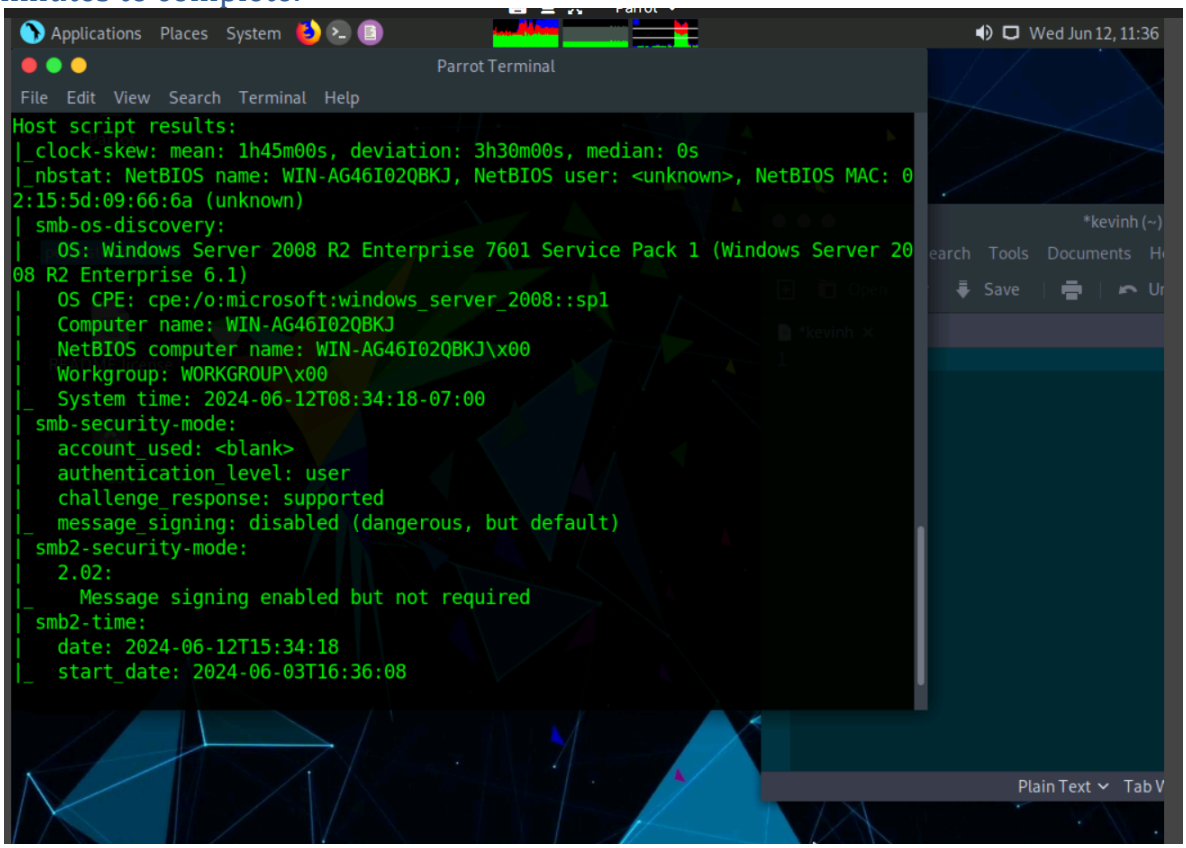
Exercise 10: Enumerating SMB

10.1OUTPUT SCREENSHOTS

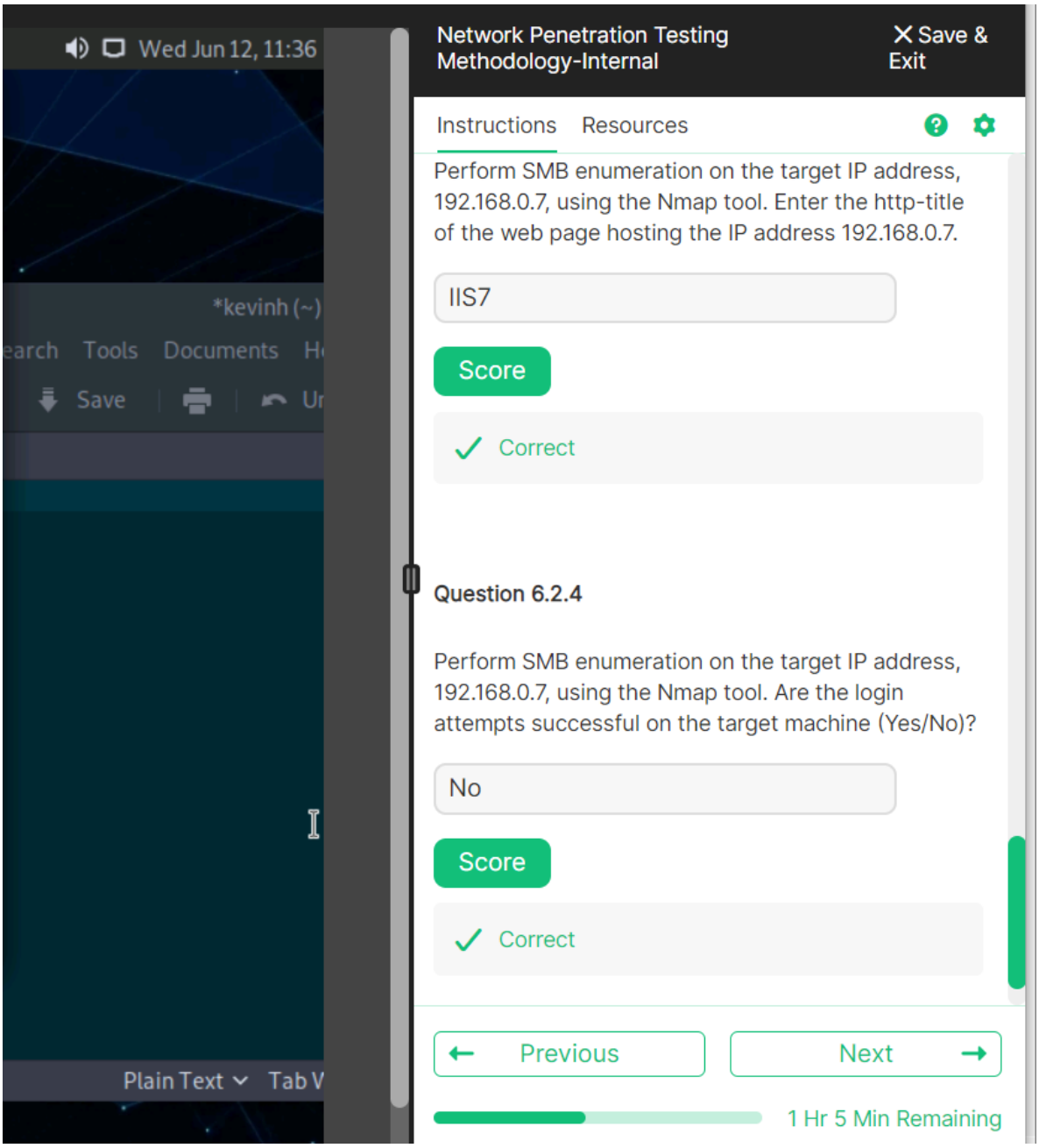
Exercise 10, Step 5: In the terminal window, type nmap –sC 192.168.0.7 and press Enter



Exercise 10, Step 6: The output of the command in step 5 reveals more details than that of the command in step 4. The scan may take approximately 5 to 10 minutes to complete.



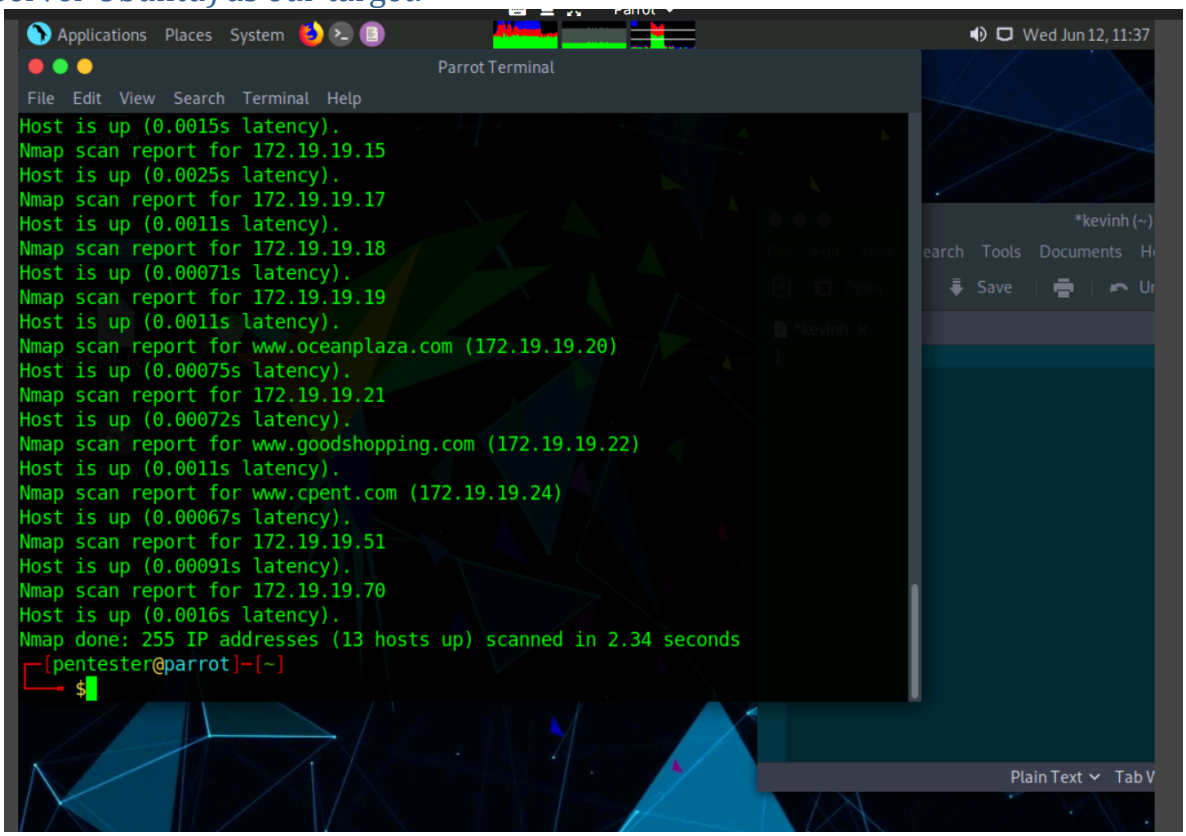
10.2 QUESTIONS



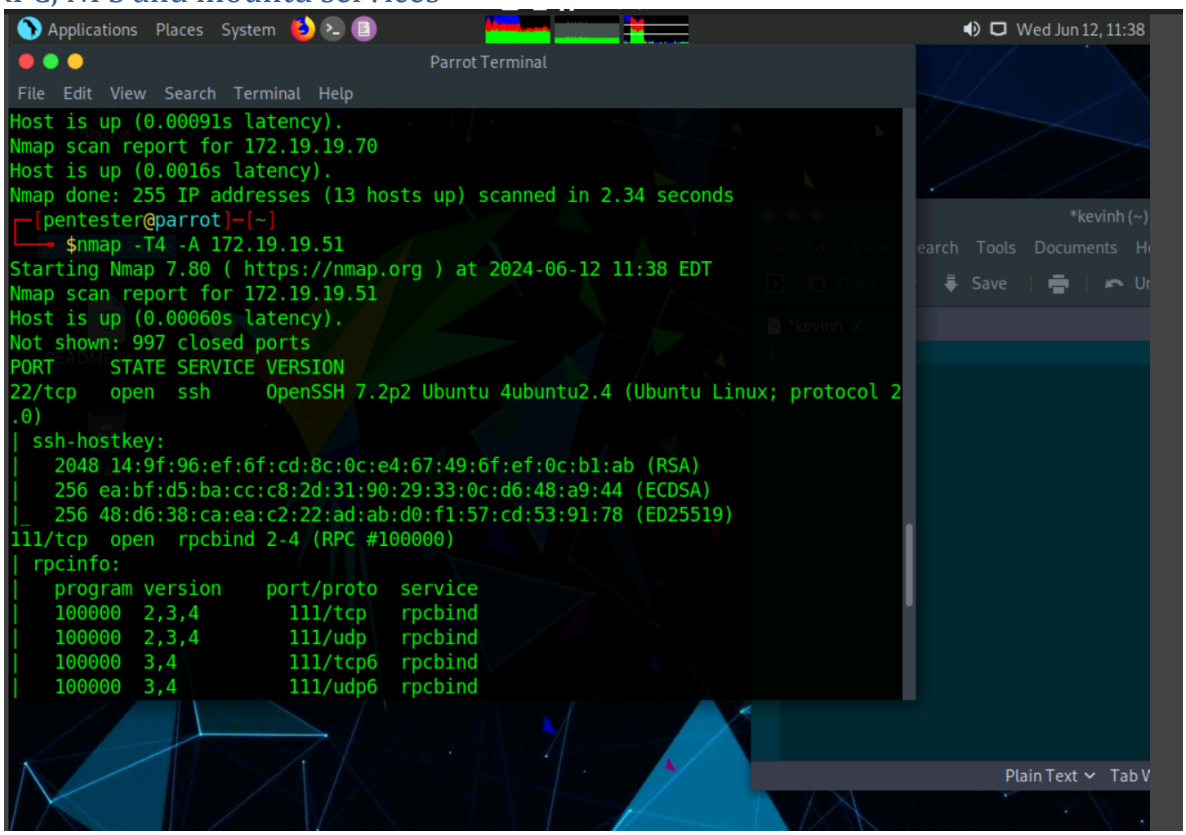
Exercise 11: Pentesting Misconfigured RPC Service and NFS Shares

11.1 OUTPUT SCREENSHOTS

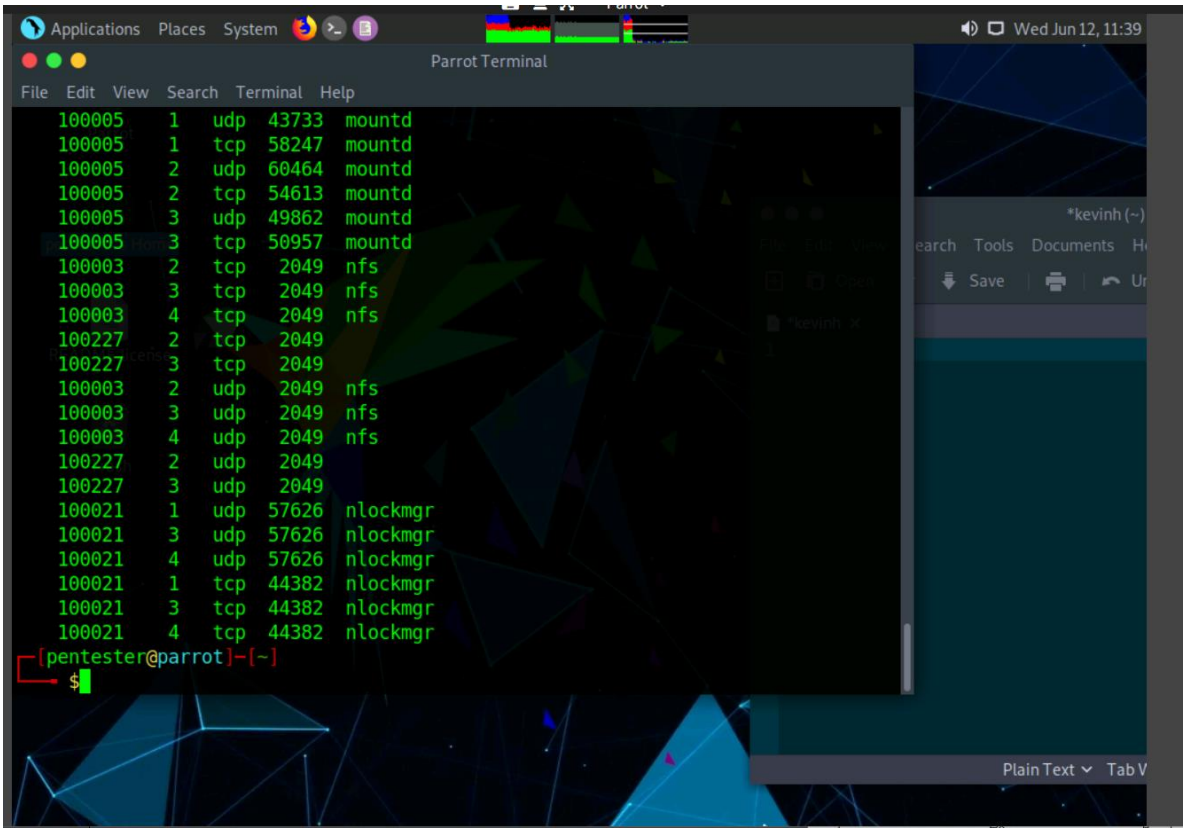
Exercise 11, Step 3: In this lab, we will be scanning a subnet for live machines. Select one machine and pentest the machine to gain access to it. For doing a quick scan, we will do a ping sweep using Nmap. In this lab, we are choosing an internal network for pentesting. Launch a command line terminal, type nmap -sP 172.19.19.1-255 and press Enter. This displays all the hosts that are up in the network within a minute. In this lab, we are choosing 172.19.19.51 (RPC Server Ubuntu) as our target.



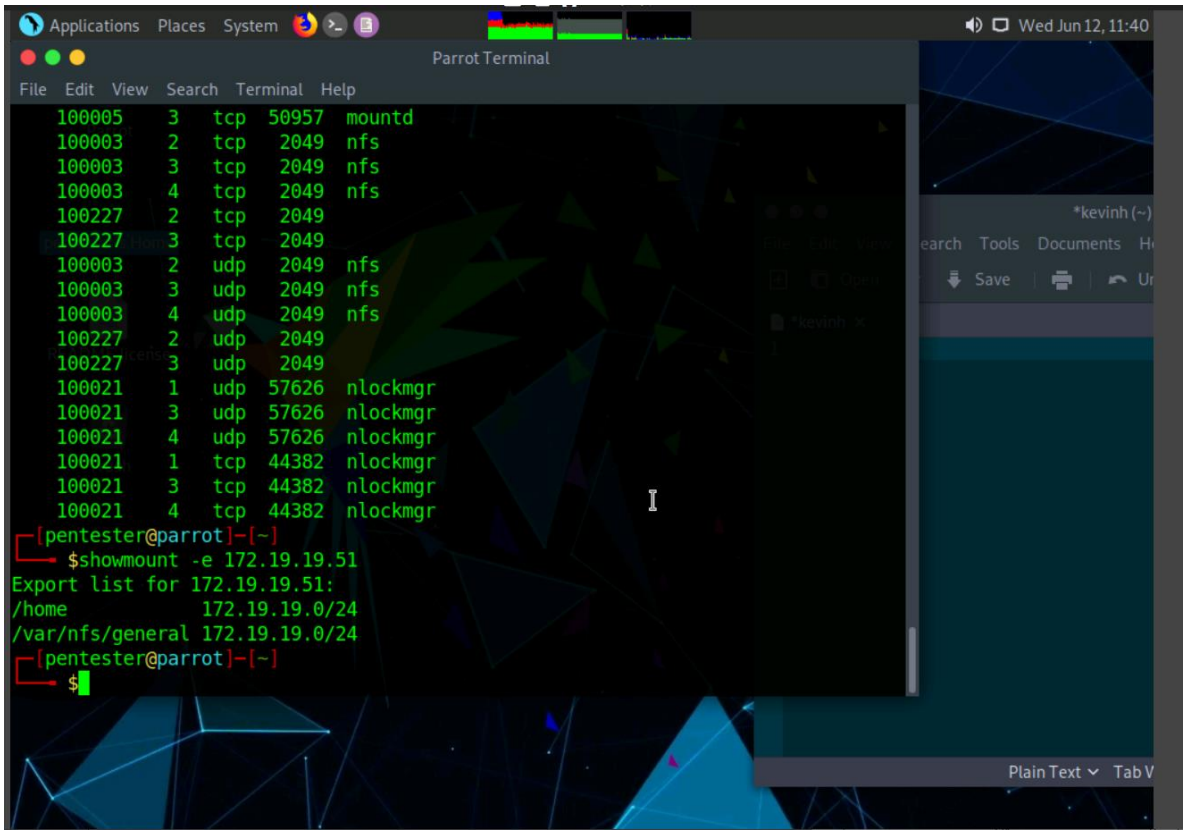
Exercise 11, Step 5: Nmap takes around 30 seconds to complete the scan. On completing the scan, you will observe that the services rpc, ftp, nfs and mountd are running on the victim machine. From the scan, it is observed that an NFS File system is mounted on the remote machine. In this lab, we shall focus on the RPC, NFS and mountd services



Exercise 11, Step 7: We observe that nfs and mountd services are active on the remote machine

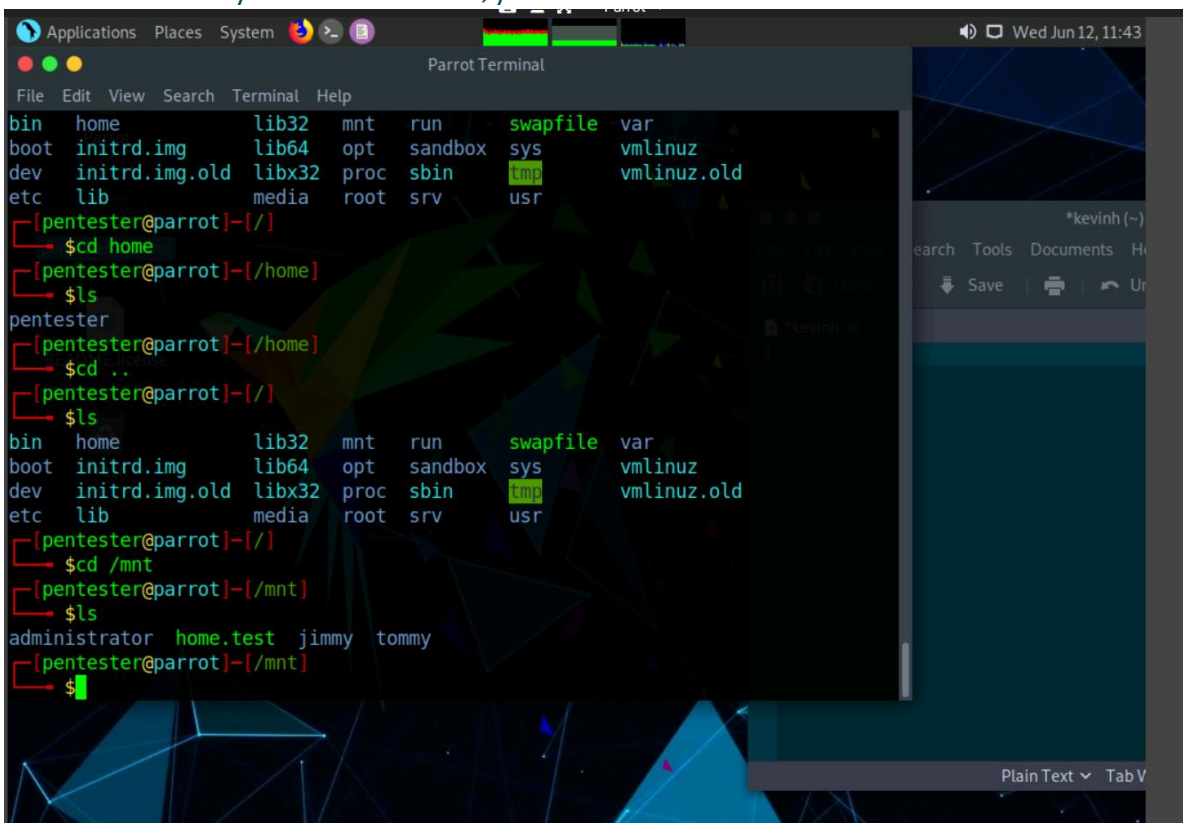


Exercise 11, Step 8: Now, we shall issue the showmount command to discover NFS shares listed in /etc/exports file of the remote machine. Type showmount -e 172.19.19.51 and press Enter. This will display all the NFS shares on the remote machine as shown in the screenshot below

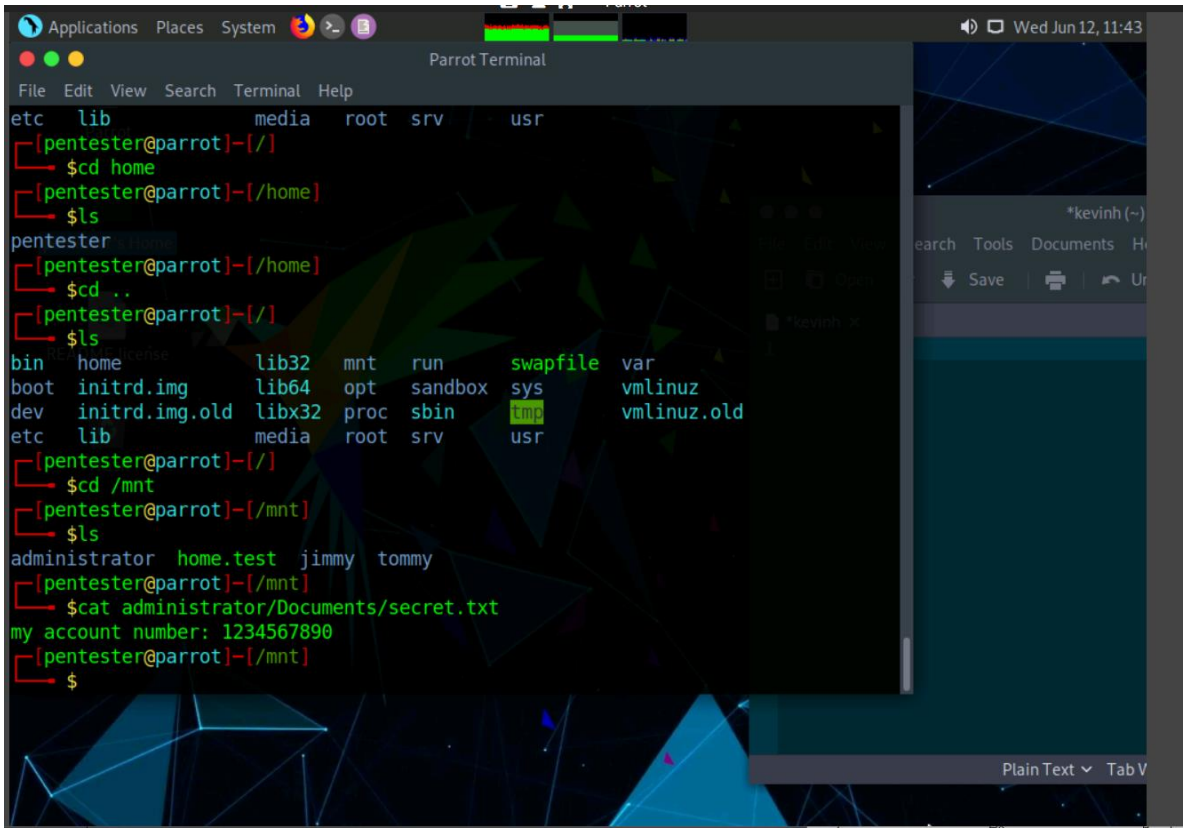


Exercise 11, Step 9: As we saw in the previous task, the /home file system was shared on the remote machine. We will be mounting this file system on the Parrot machine to the mnt directory. To mount, type sudo mount -t nfs 172.19.19.51:/home /mnt -o nolock and press Enter. Type toor and press Enter when prompted.

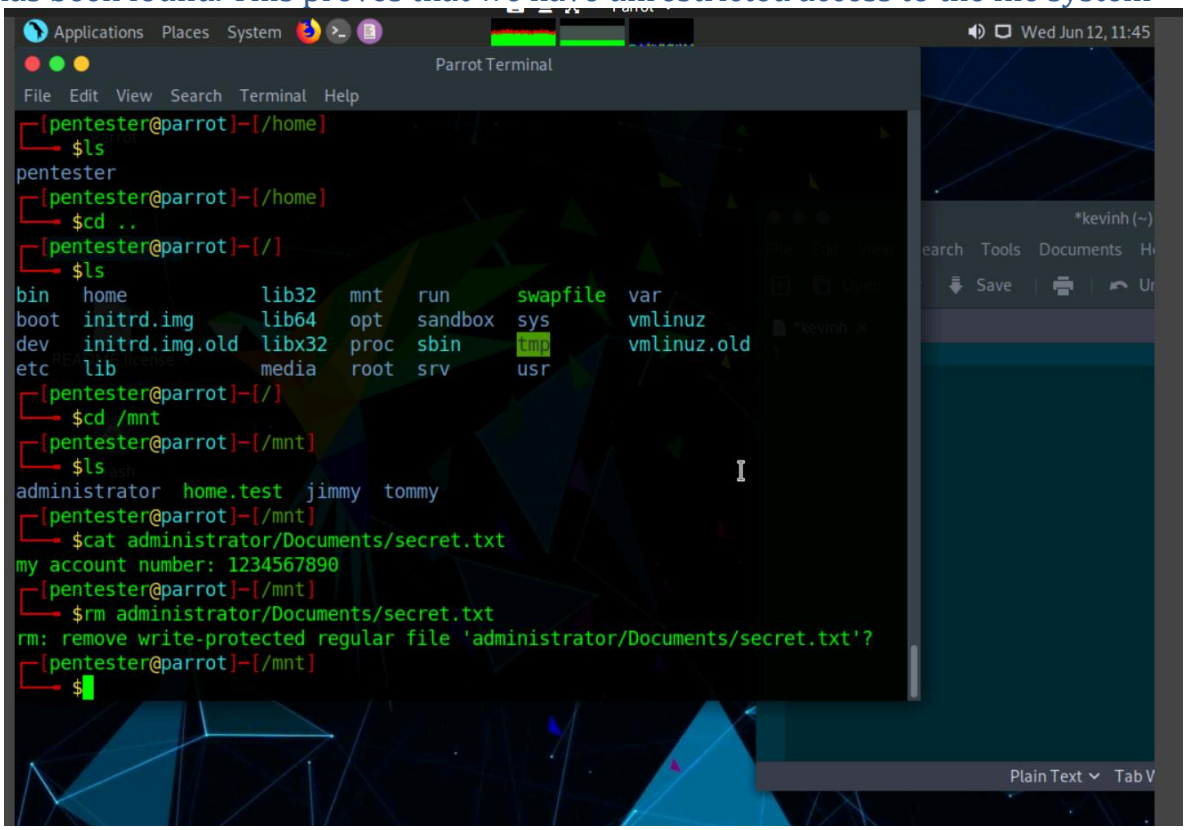
Exercise 11, Step 11: Type ls and press Enter to view the files and directories contained in the /home folder i.e., /mnt.



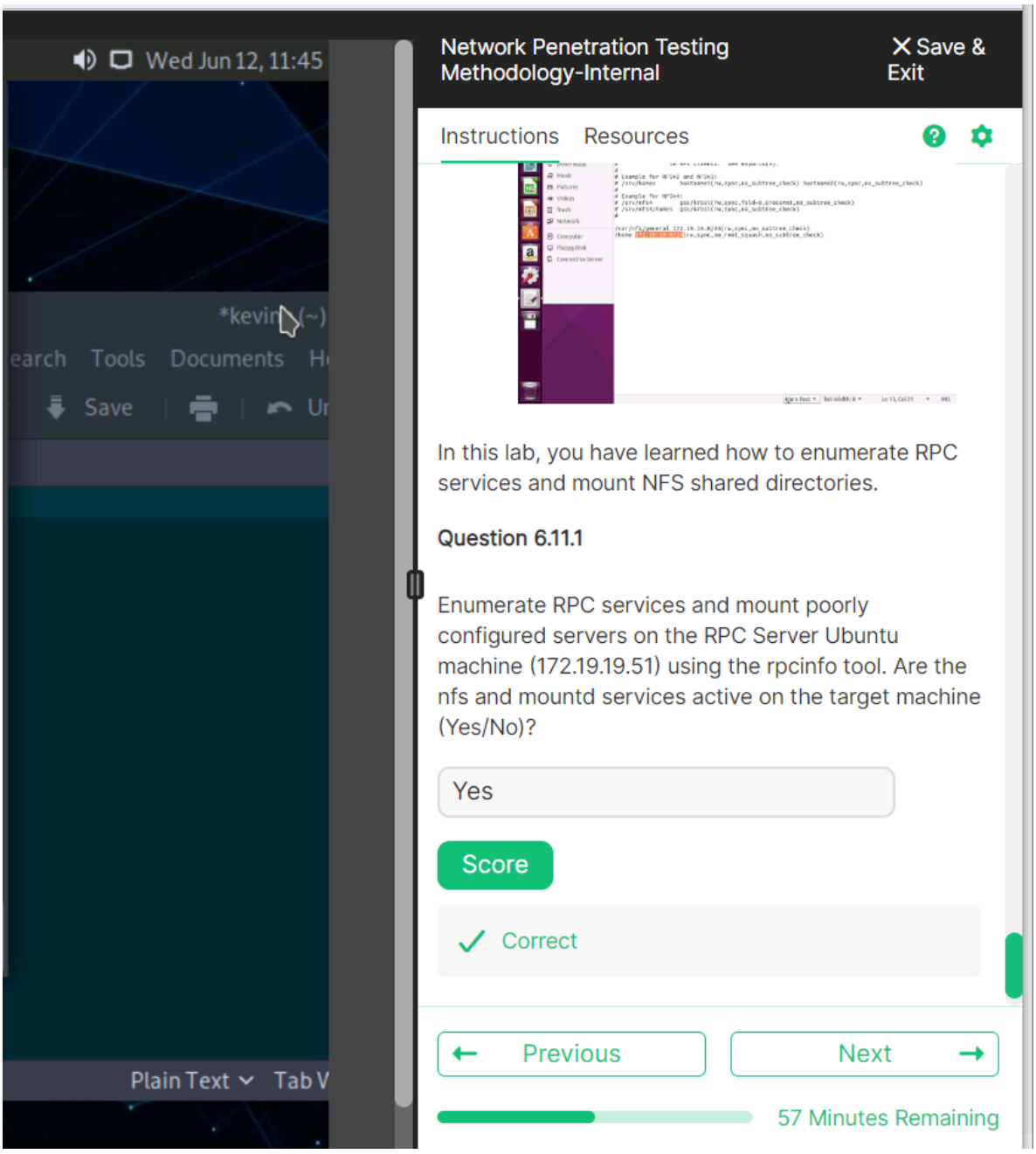
Exercise 11, Step 13: On entering the command in the previous task, the cat command displays the file contents in the secret.txt file successfully, meaning we have successfully mounted the remote file system and accessed the contents in it.



Exercise 11, Step 15: Now, we shall see if we are able to tamper/delete the files in the remote file system. Type rm administrator/Documents/secret.txt and press Enter. Type y and press Enter to confirm the deletion. To confirm that the file has been successfully deleted, type cat administrator/Documents/secret.txt and press Enter. The terminal displays an error stating no such file or directory has been found. This proves that we have unrestricted access to the file system



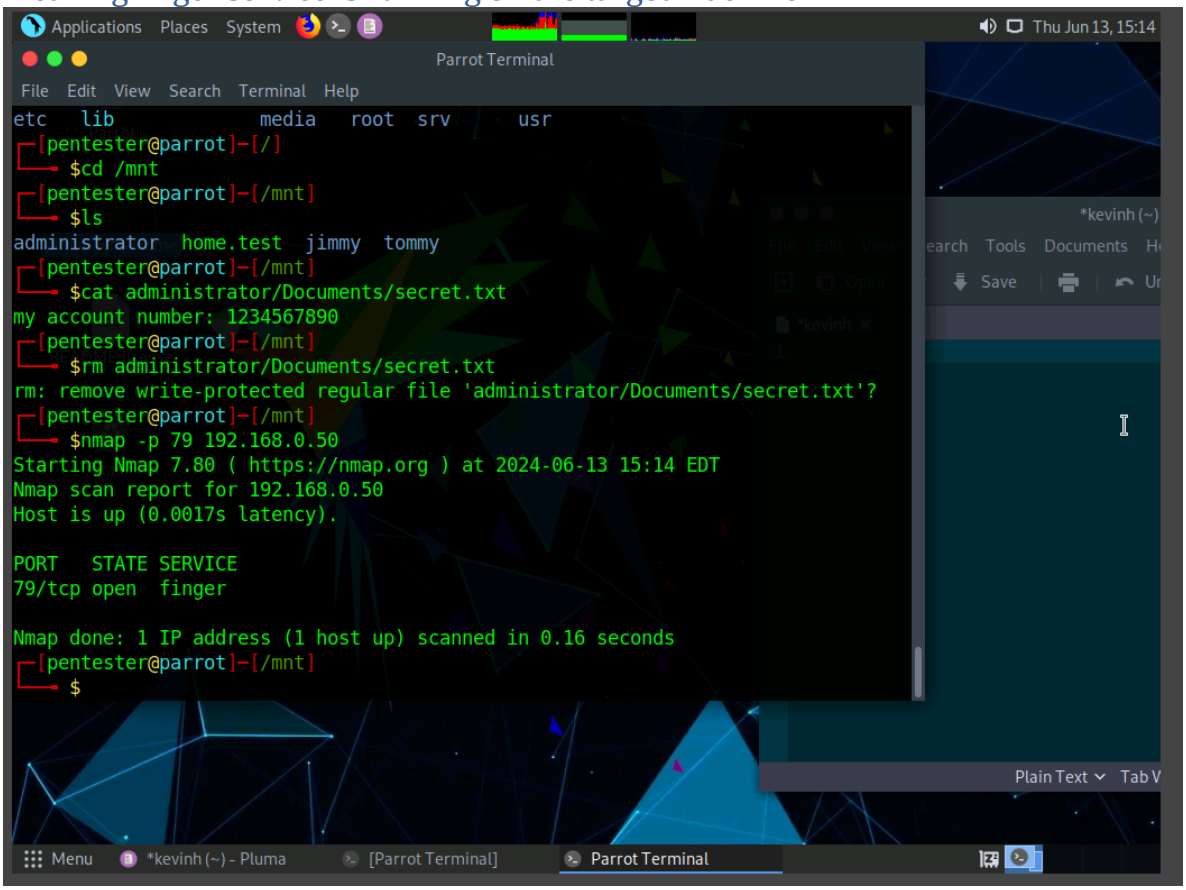
11.2 QUESTIONS



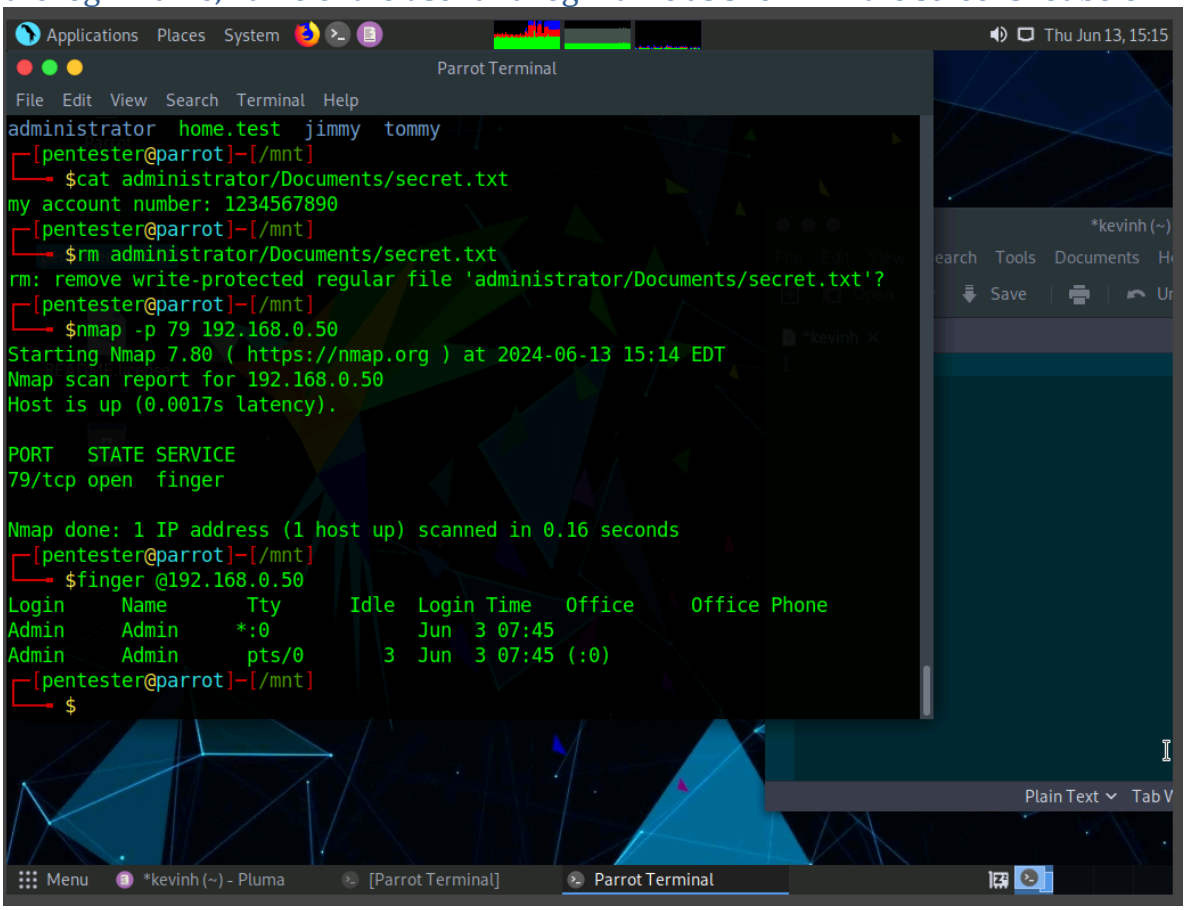
Exercise 12: Enumerating Logged on Users Using Finger Protocol

12.1 OUTPUT SCREENSHOTS

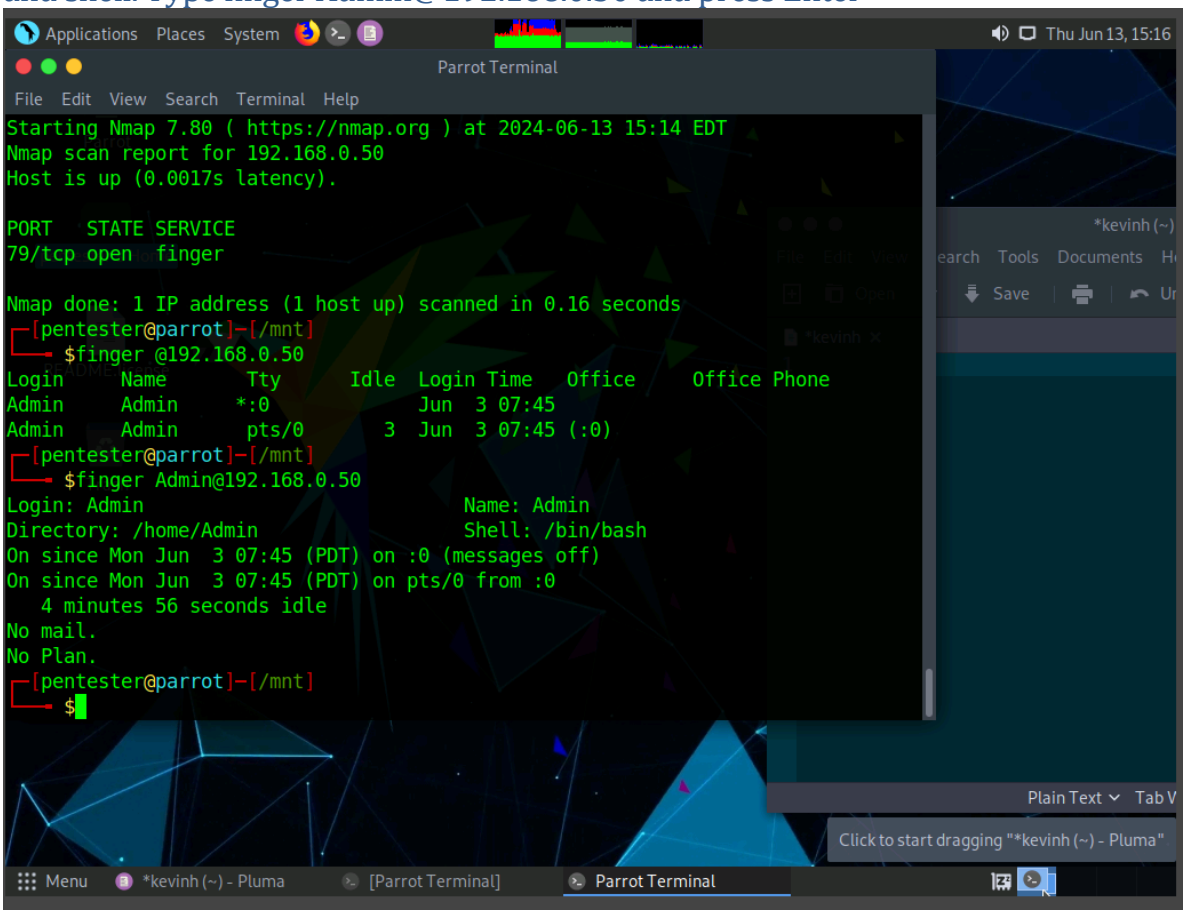
Exercise 12, Step 6: You will observe that the port 79 is open in the Nmap result, meaning finger service is running on the target machine.



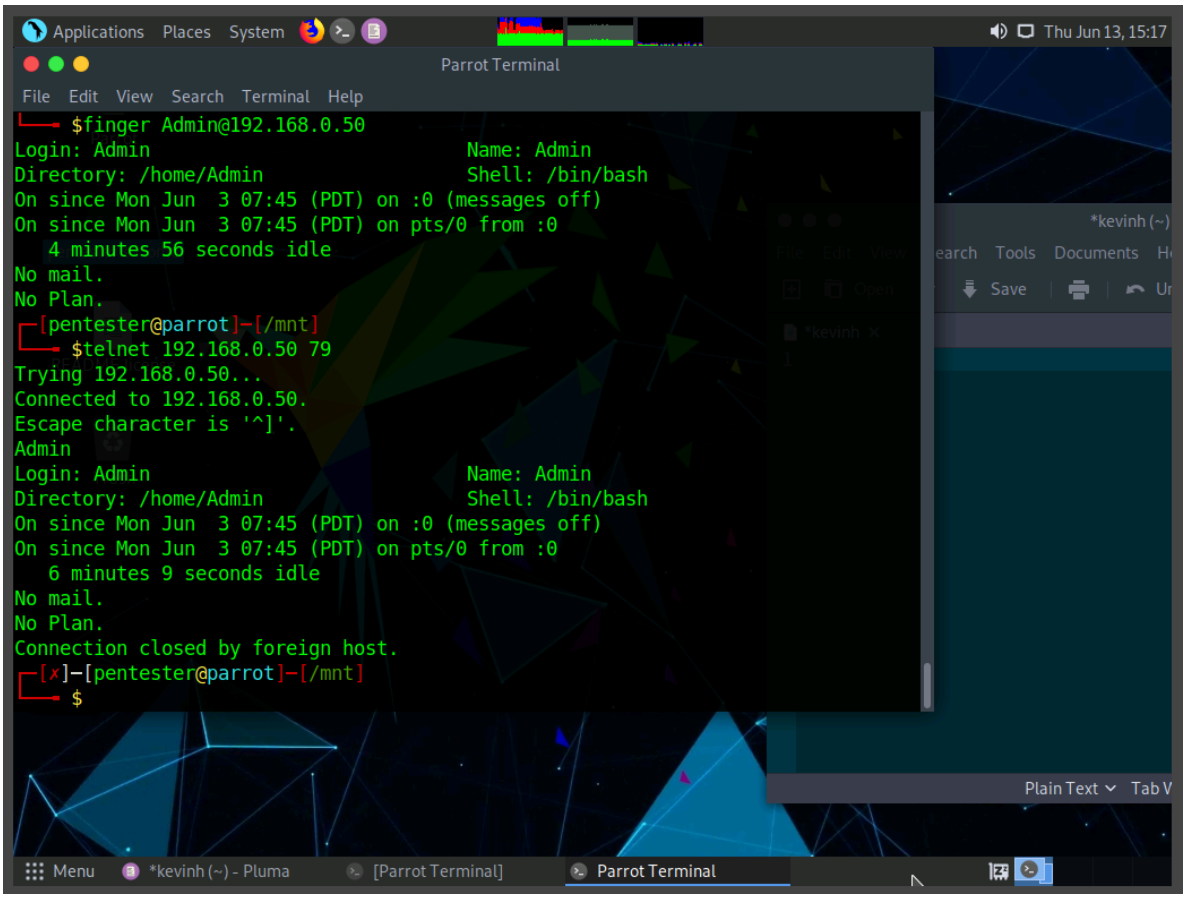
Exercise 12, Step 8: Finger client returns the logged in user information such as the login name, name of the user and login time as shown in the screenshot below



Exercise 12, Step 9: Since we found the username, we shall use this to extract additional information such as the name of the user, home directory, login name, and shell. Type finger Admin@192.168.0.50 and press Enter

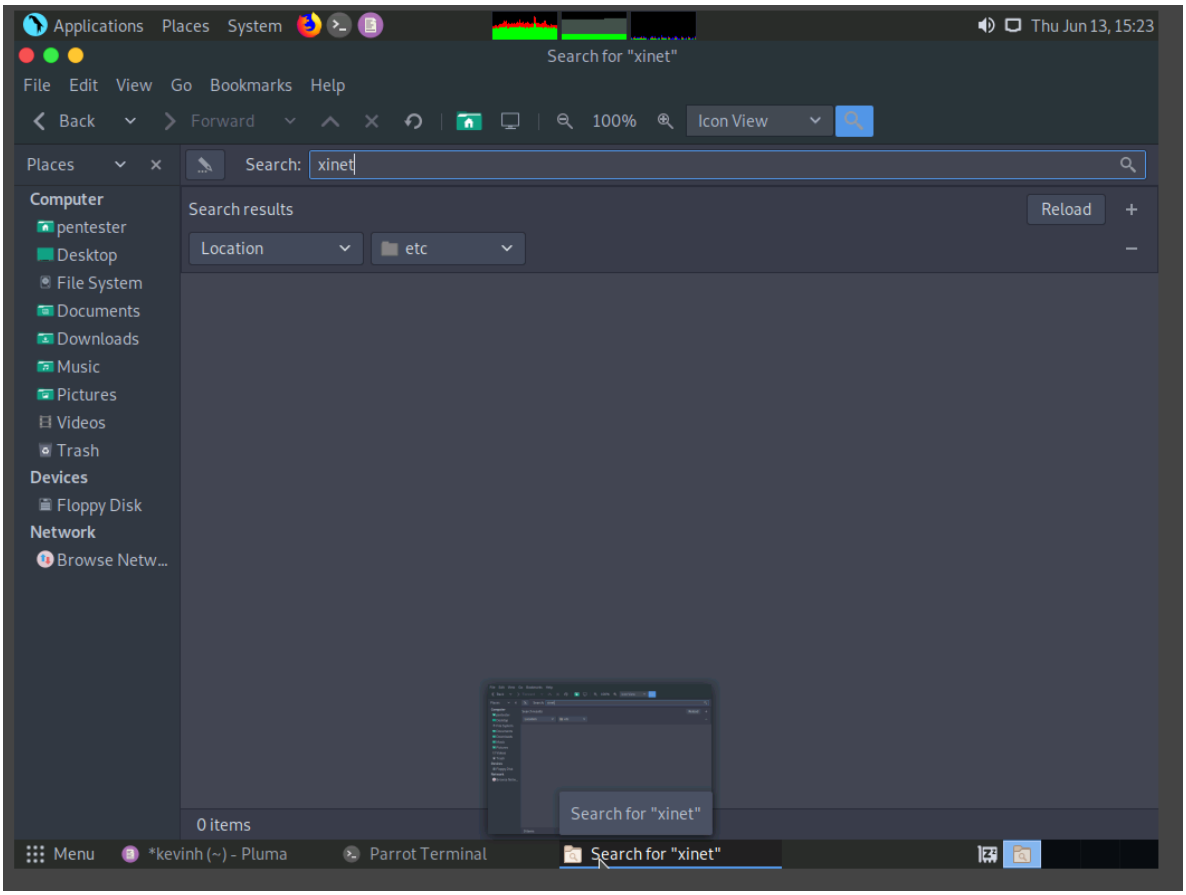


Exercise 12, Step 11: Type Admin and press Enter. This displays the enumerated user information as shown in the screenshot below

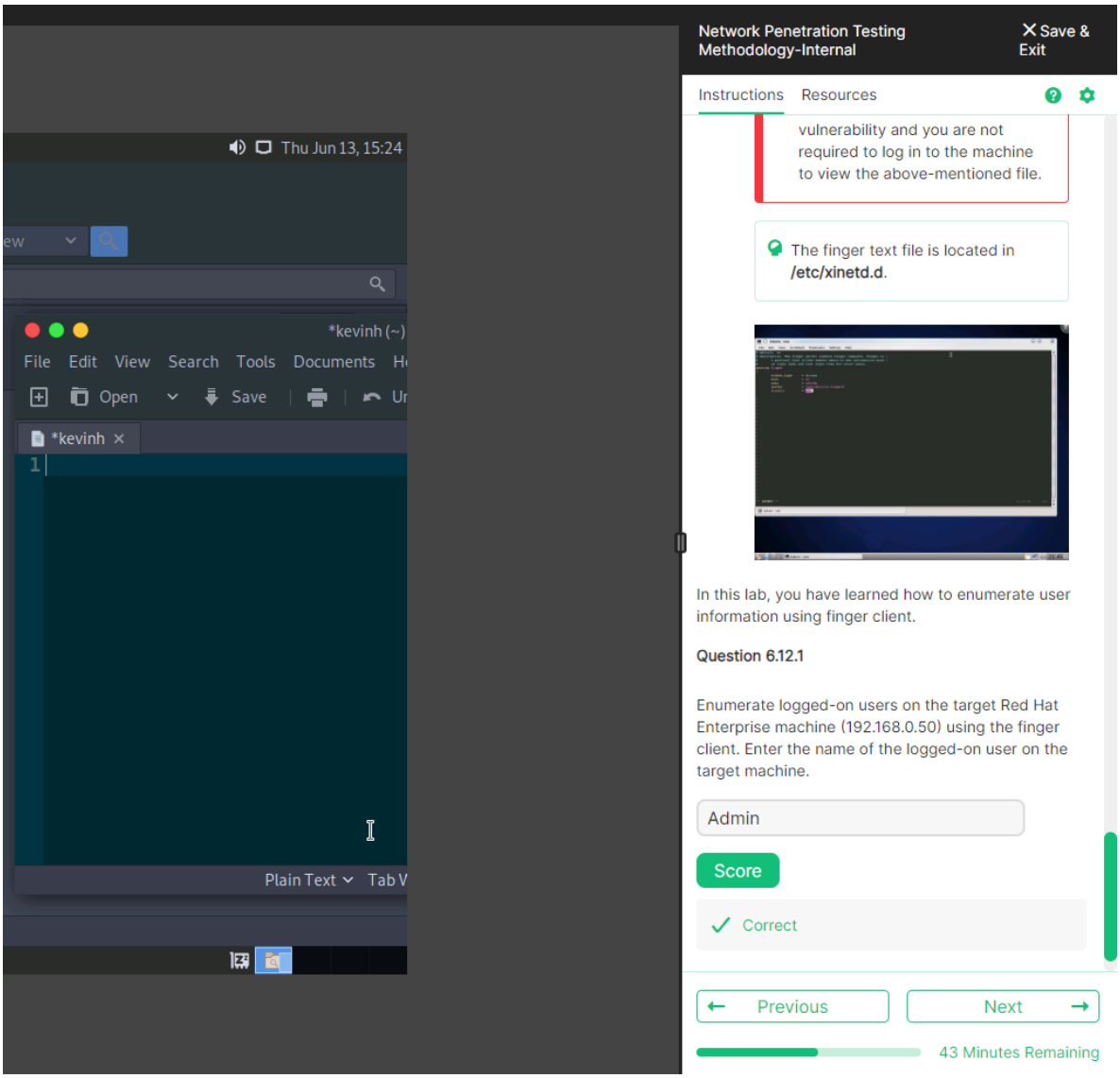


Exercise 12, Step 12: To safeguard your machine from returning the logged in user information, it is recommended to disable finger service on the machine by editing the finger text file located in the /etc/xinetd.d.

NOTE: Due to the fact that the remote host machine is not able to be logged in remotely by the current machine. The text file is unable to be accessed remotely as per the Lab.



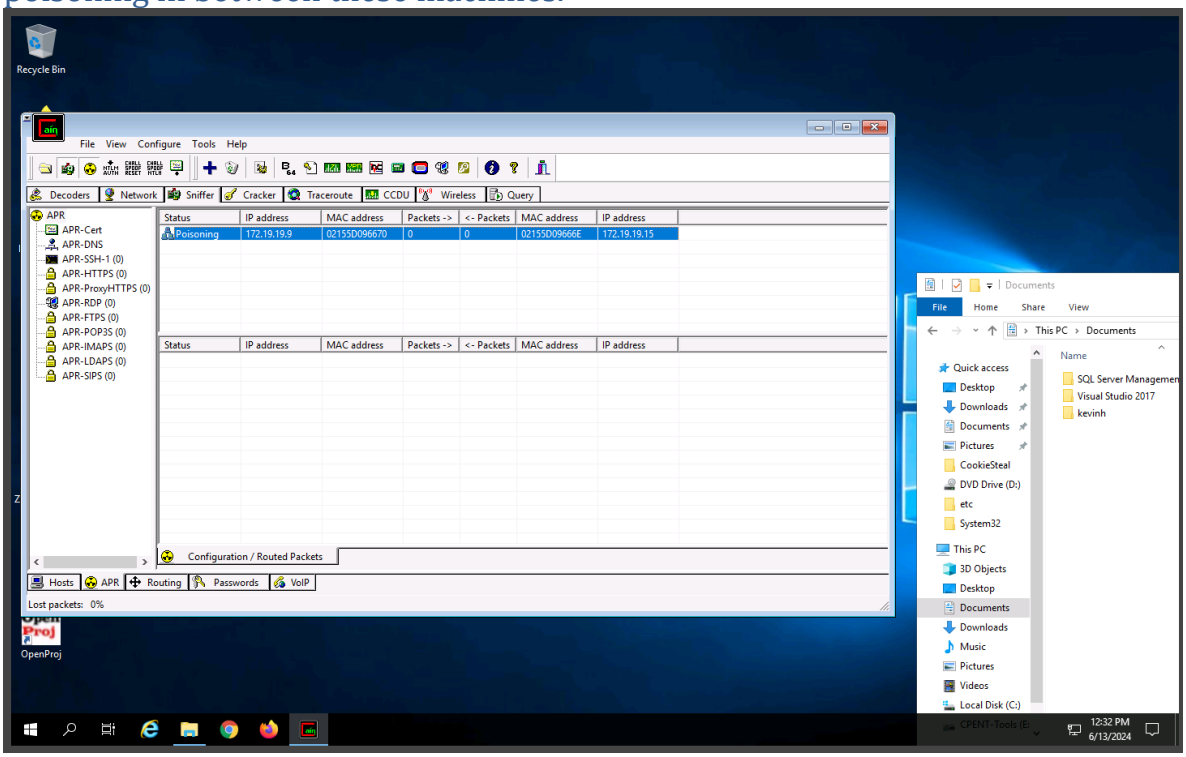
12.2 QUESTIONS



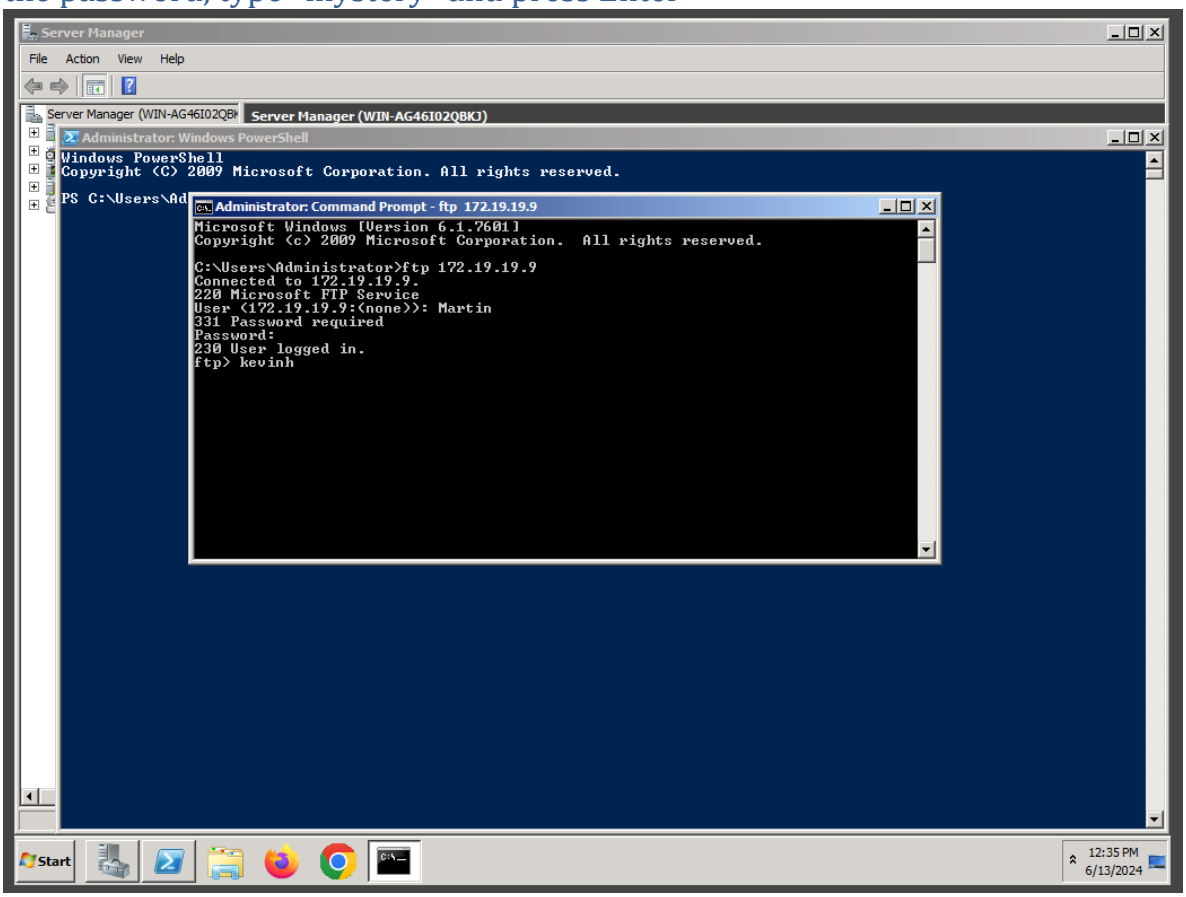
Exercise 13: Performing Man-in-the-Middle Attack using Cain & Abel

13.1 OUTPUT SCREENSHOTS

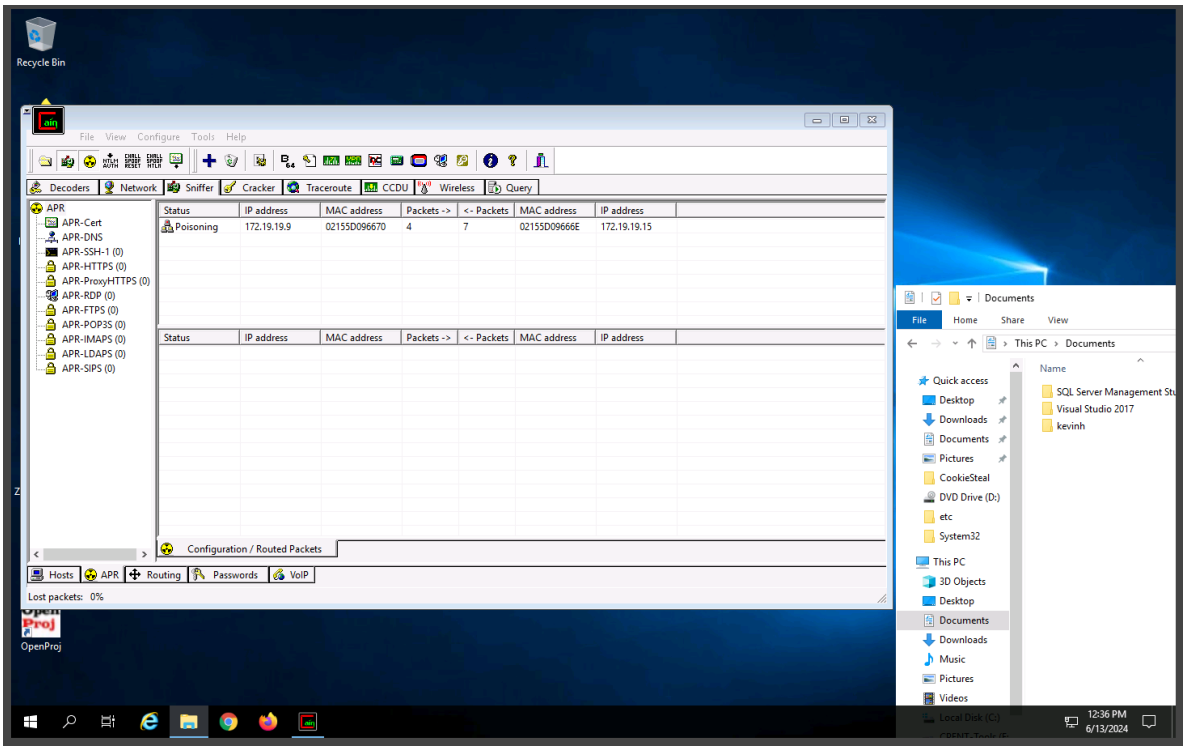
Exercise 13, Step 15: Select the added IP address in the Configuration/Routed packets, and click Start/Stop APR (third icon from left) icon. Cain begins ARP poisoning in between these machines.



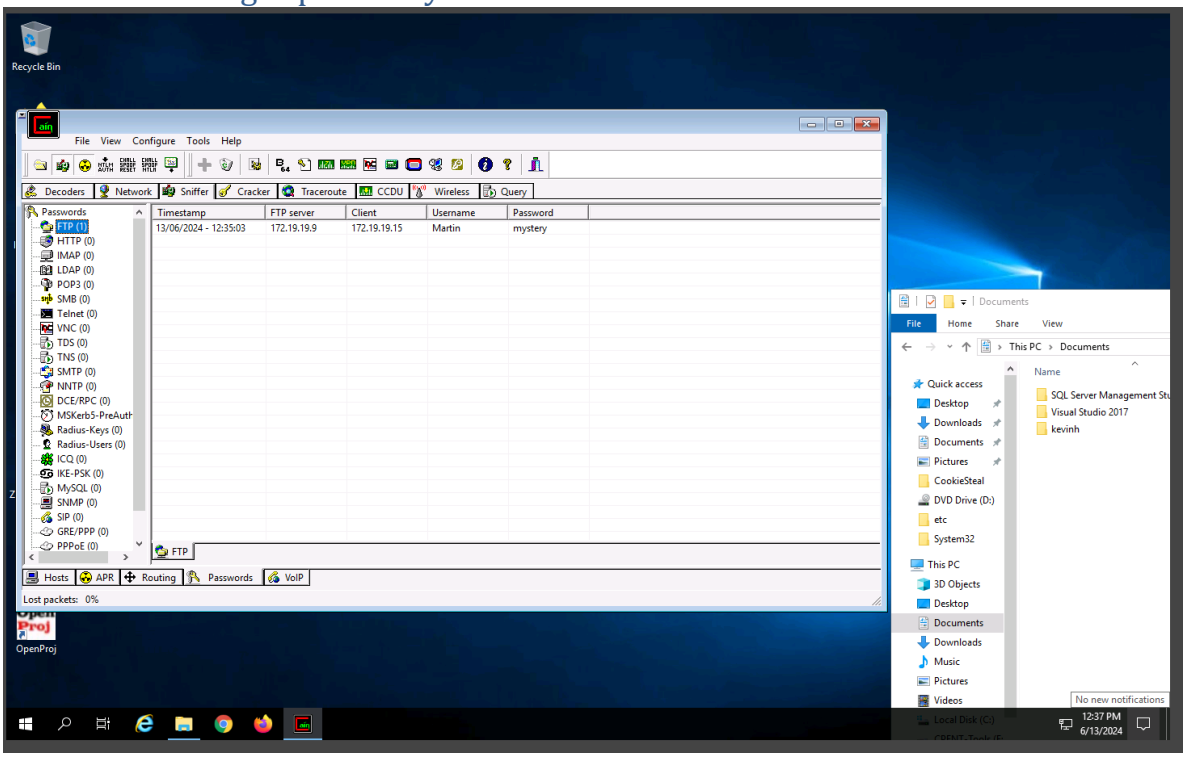
Exercise 13, Step 20: Now launch a command prompt in the machine, type ftp 172.19.19.9 (IP address of FTP Server machine) and press Enter. When prompted for the Username, type "Martin" and press Enter. When prompted for the password, type "mystery" and press Enter



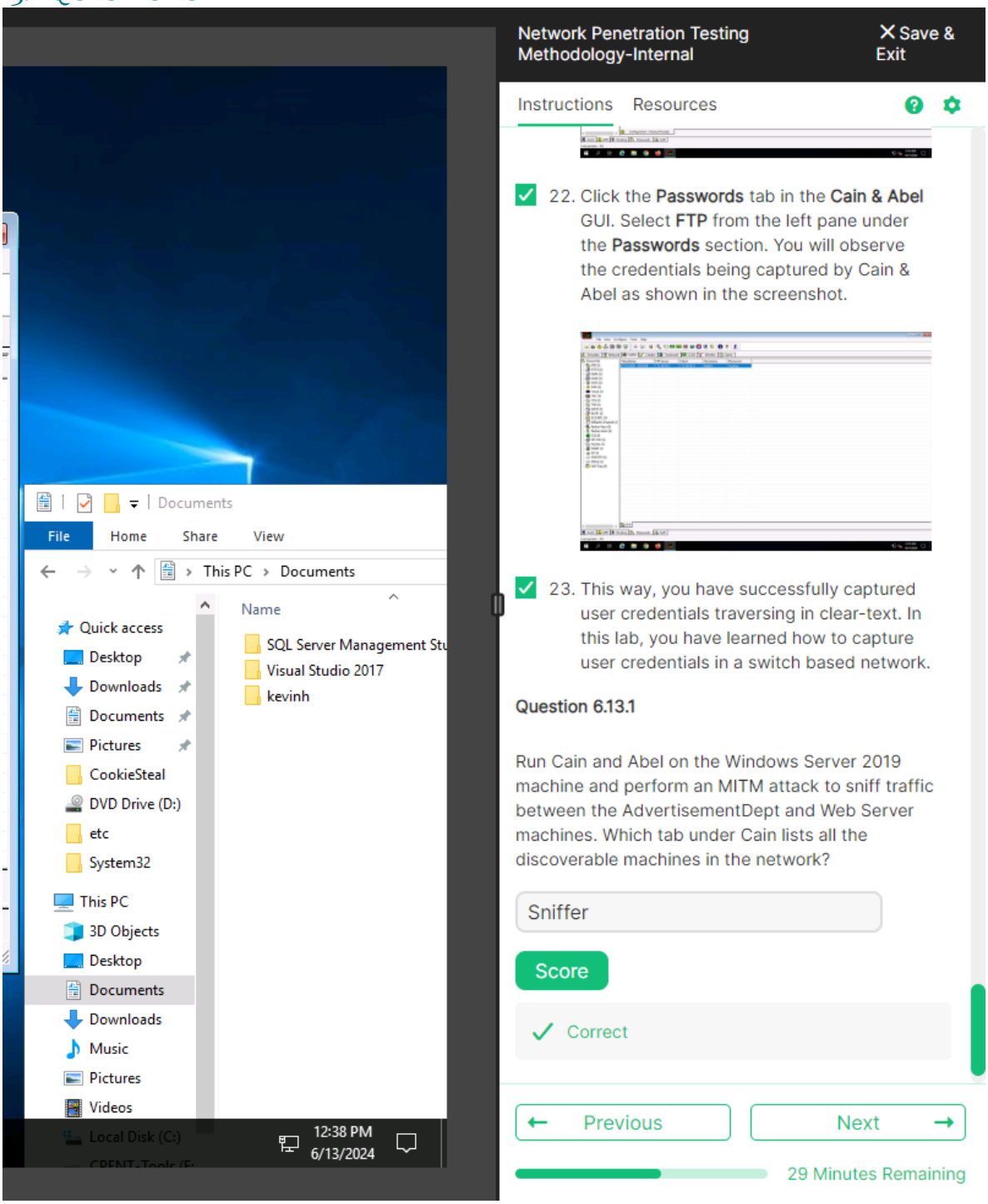
Exercise 13, Step 21: You will observe that Cain & Abel captured some packets which can be observed under the Packets field.



Exercise 13, Step 22: Click the Passwords tab in the Cain & Abel GUI. Select FTP from the left pane under the Passwords section. You will observe the credentials being captured by Cain & Abel as shown in the screenshot



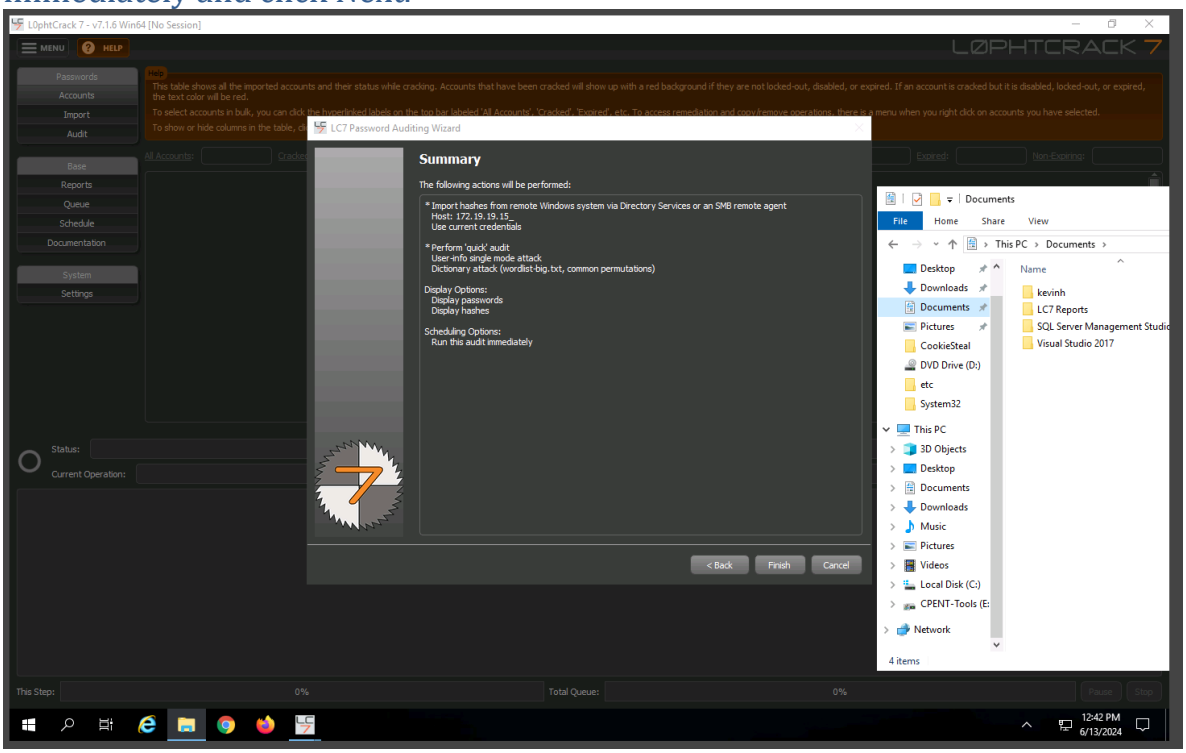
13.2 QUESTIONS



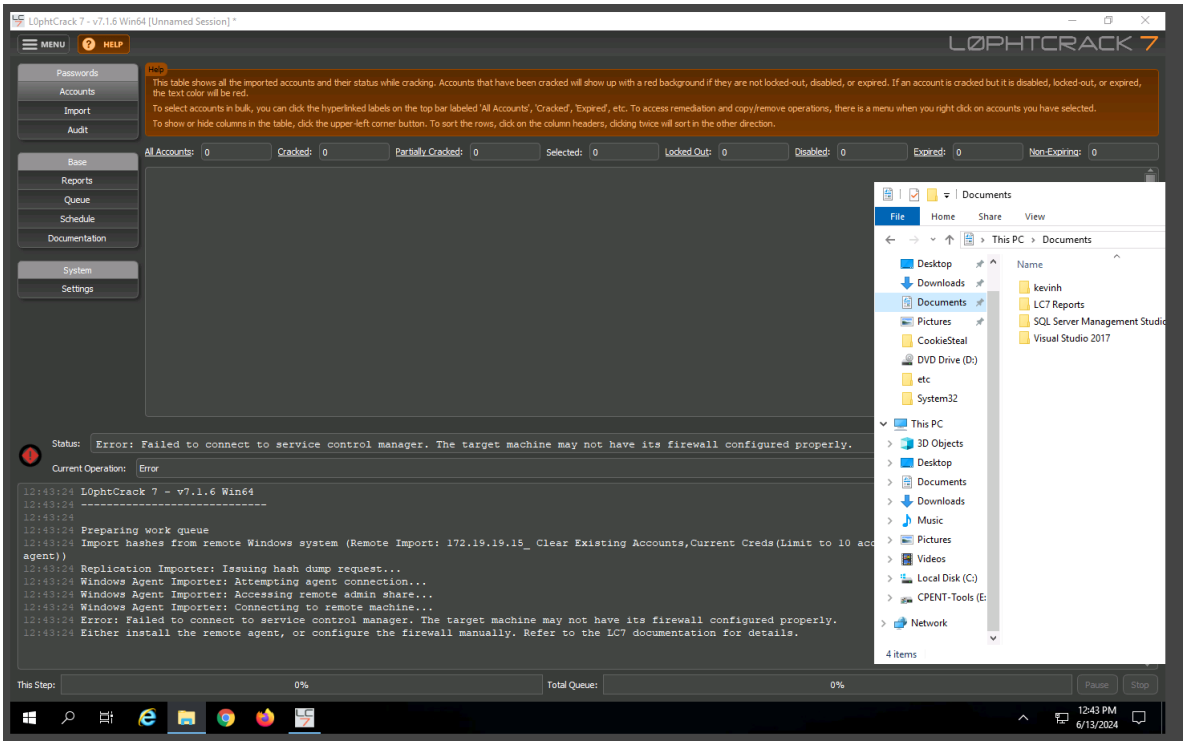
Exercise 14: Auditing a Machine for Weak Passwords Using LophtCrack

14.1OUTPUT SCREENSHOTS

Exercise 14, Step 13: In the Job Scheduling window, select Run this job immediately and click Next.

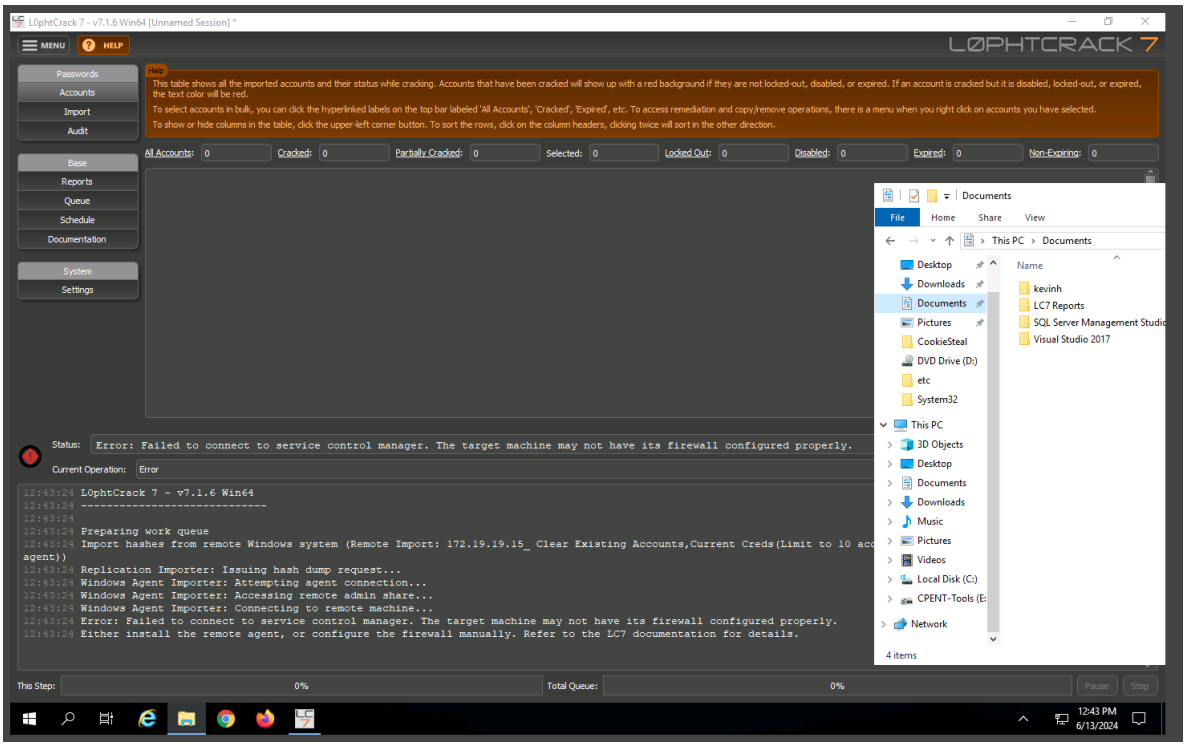


Exercise 14, Step 15: A caution box appears regarding changed LC7Agent on the remote machine as shown in the screenshot. Click Yes.

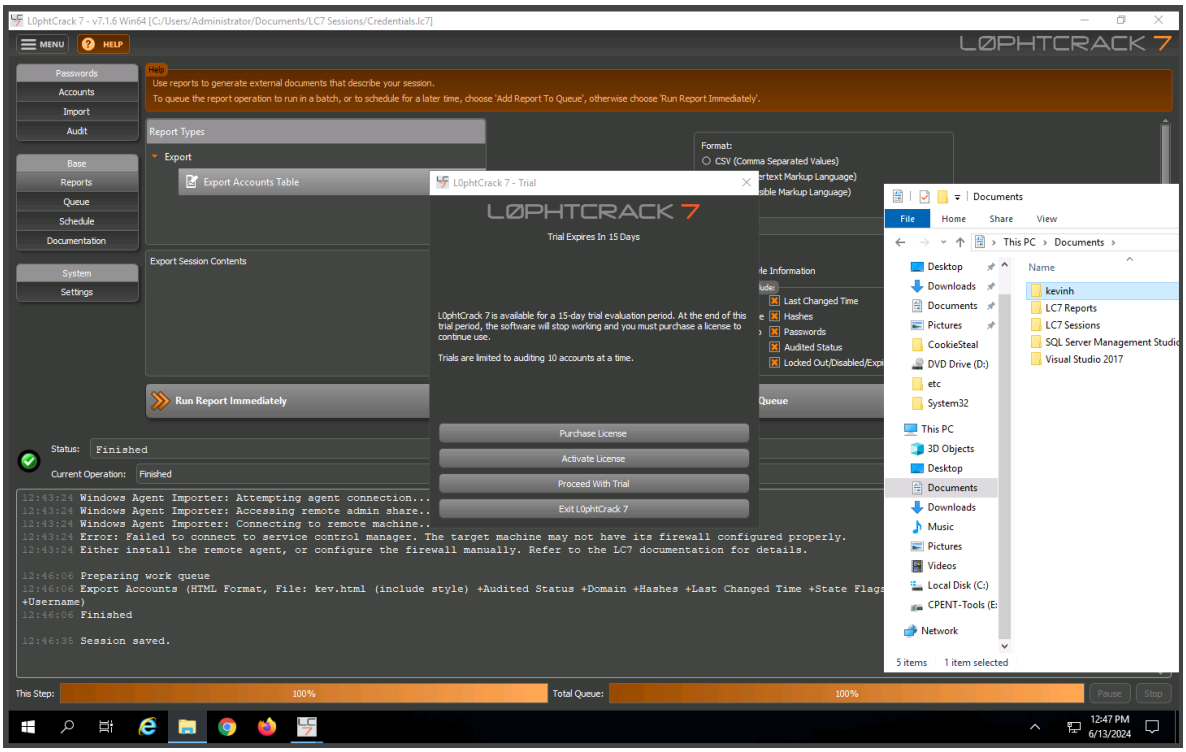


Exercise 14, Step 16: L0phtCrack will begin to decode the hashes. You can see the Progress bar in the lower right-hand corner of the window. Once done with the password auditing, it displays the weak passwords set for the respective user accounts present in Advertisement Dept machine as shown in the screenshot

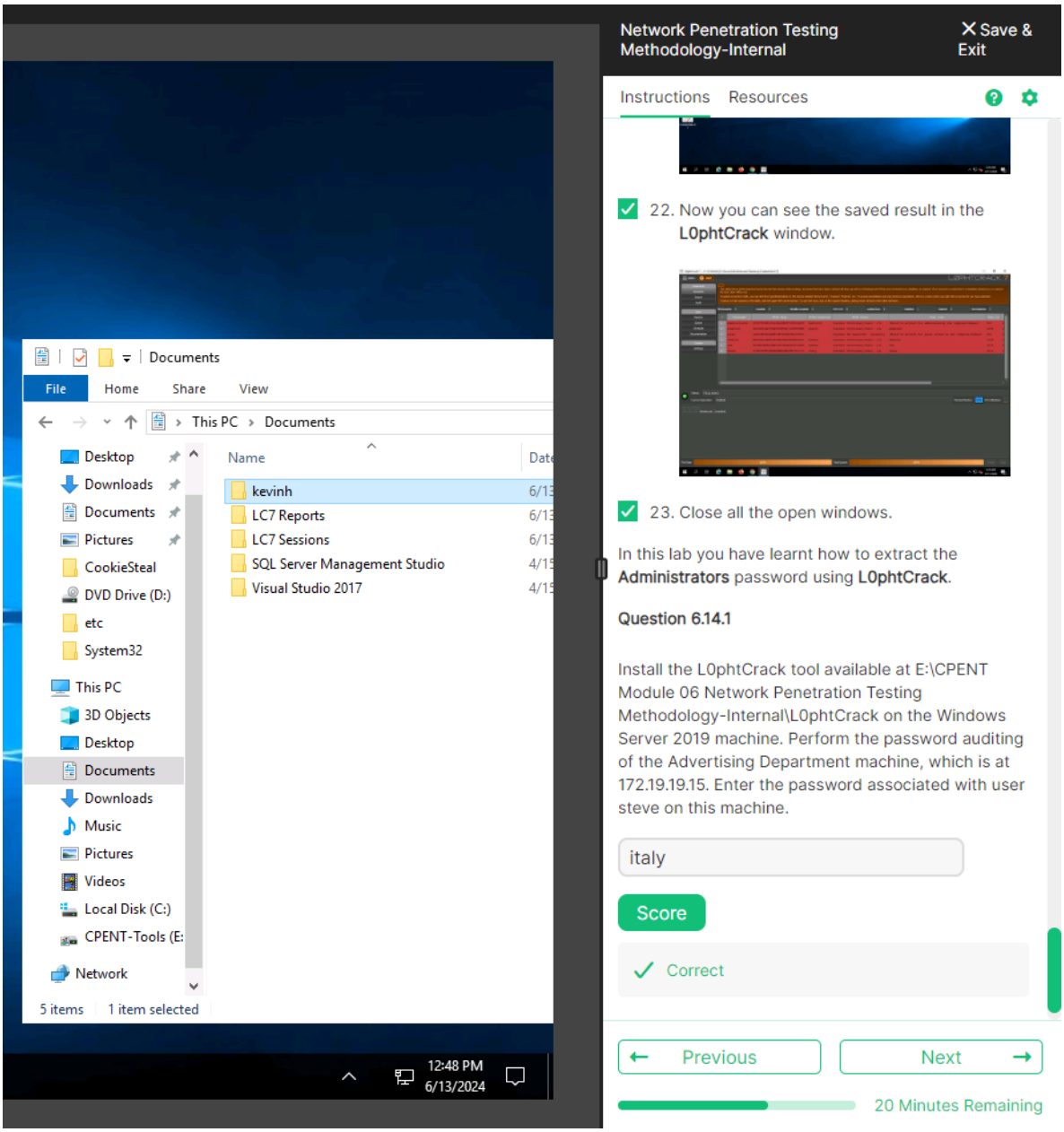
NOTE: The tool is currently experiencing an error due to the establishment of a firewall incorporated between labs. Still able to run the tool, just not obtain the desired output of data.



Exercise 14, Step 20: To open the saved result, navigate to Desktop and double-click the Credentials.lcs file to view result.



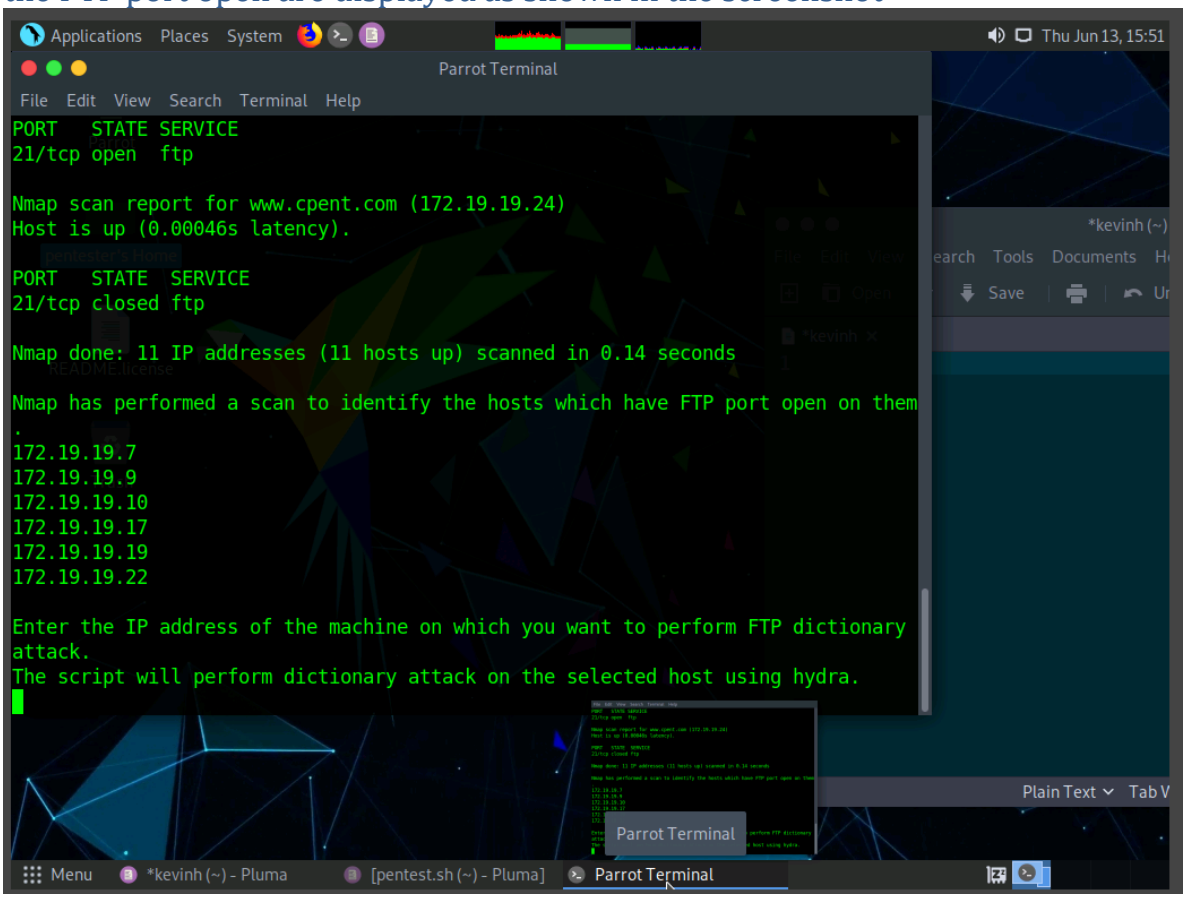
14.2 QUESTIONS



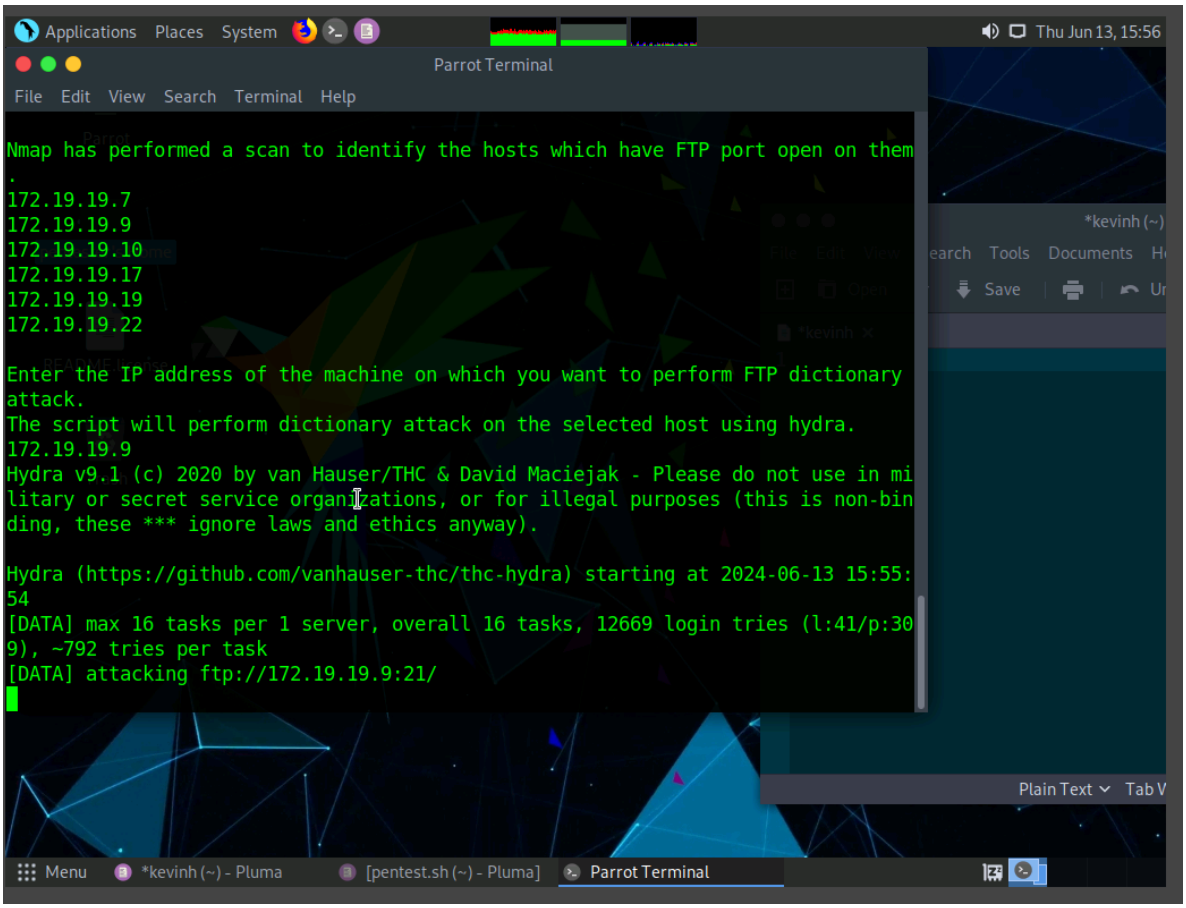
Exercise 15: Automating Penetration Testing Tasks Using Bash Scripting

15.1 OUTPUT SCREENSHOTS

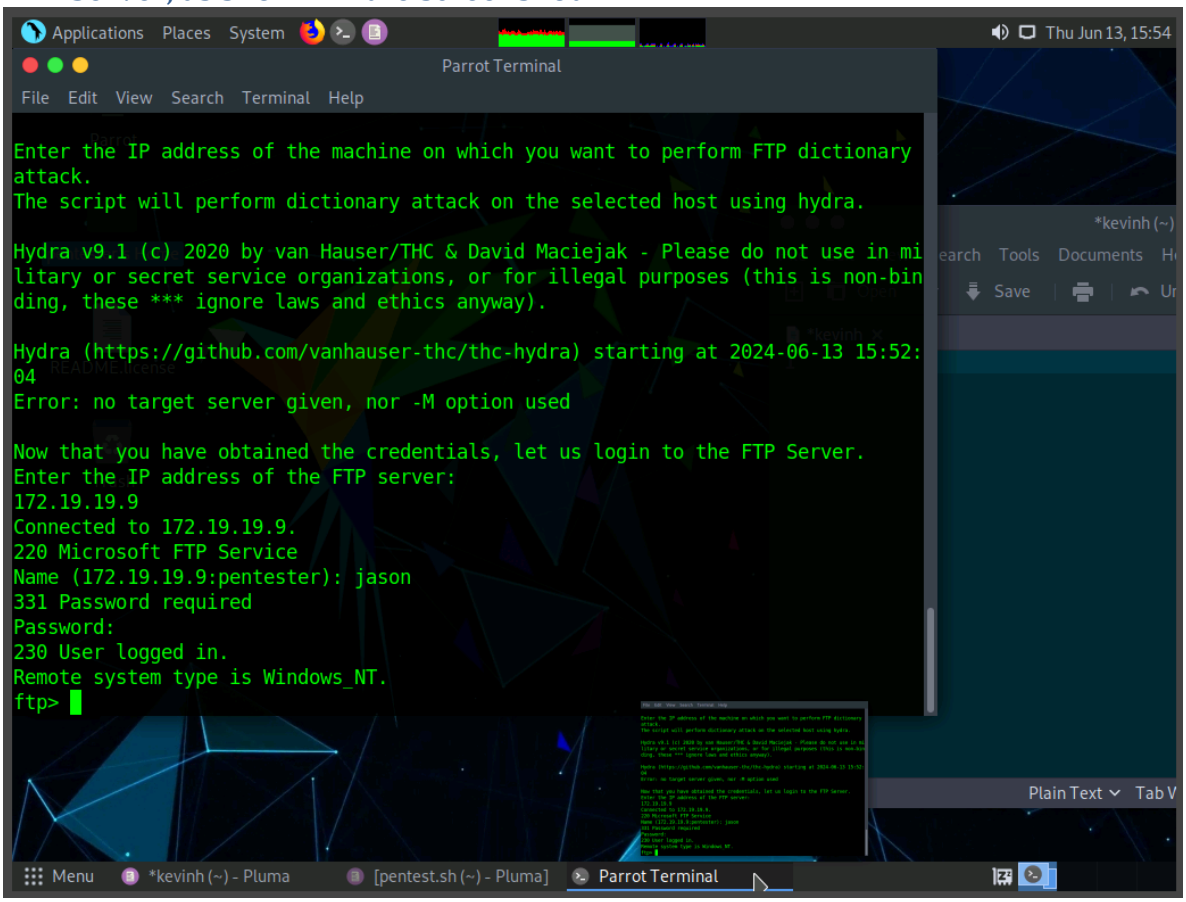
Exercise 15, Step 18: Now, minimize the text editor window and maximize the command line terminal. Nmap has performed live host identification on the given IP Address range. Once the live hosts are identified, the script is written in such a way, that a new nmap scan is initiated to find the machines (among the identified live hosts) that have the FTP port open. The live machines with the FTP port open are displayed as shown in the screenshot



Exercise 14, Step 23: Minimize the text editor window and maximize the command line terminal. On issuing the IP Address, Hydra begins to a perform Dictionary attack on the machine and starts displaying the user credentials as shown in the screenshot.

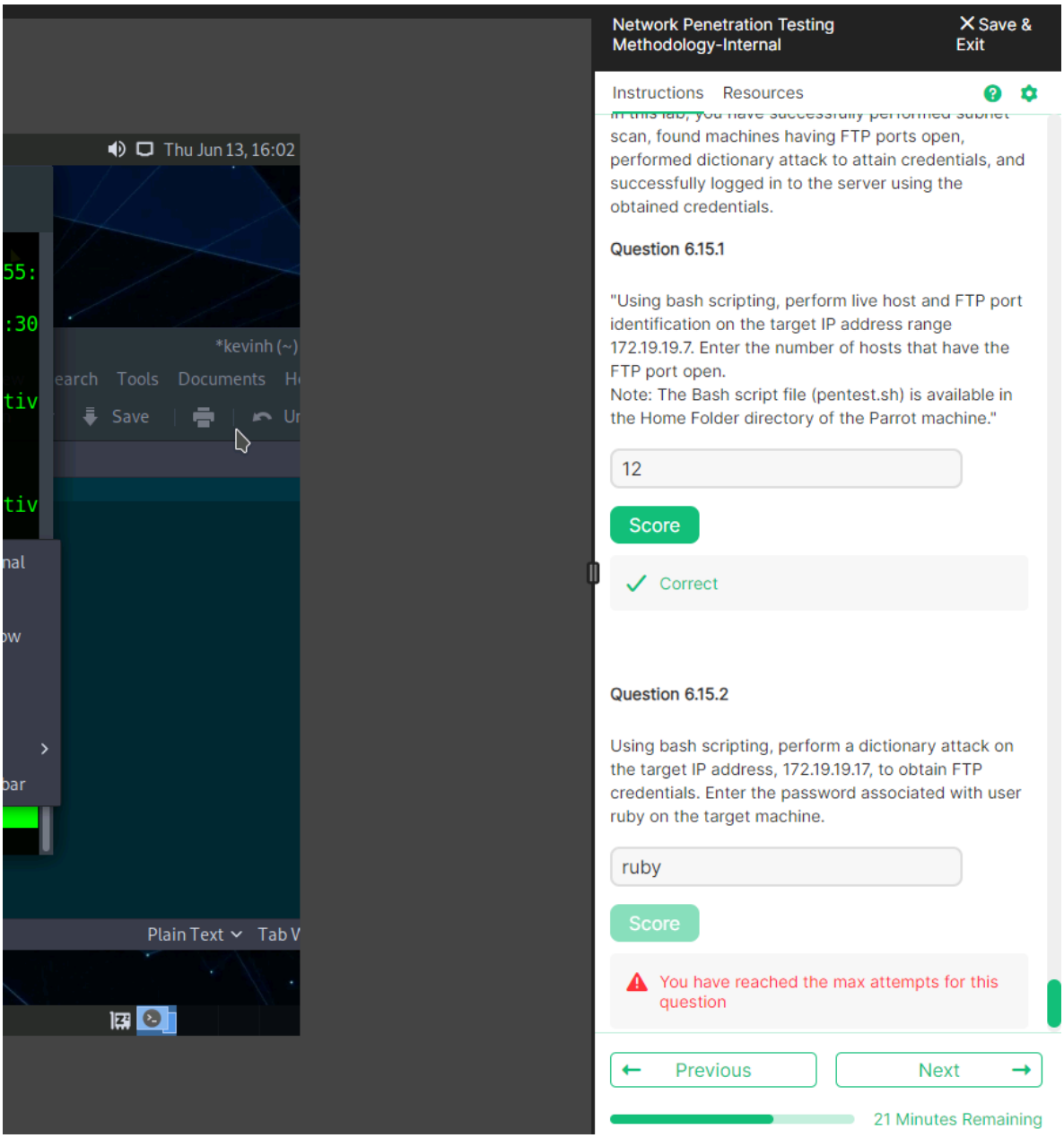


Exercise 14, Step 30: On issuing the user credentials, you will be logged in to the FTP Server, as shown in the screenshot



15.2 QUESTIONS

NOTE: due to the lab locking up and was unable to re-specify the FTP target as well as to interact with the lab, I was unable to find the answer for the final question. I was still able to learn how to use FTP still however.


Thu Jun 13, 16:02
*kevinh (~)
Tools
Documents
Save
Plain Text
Network Penetration Testing Methodology-Internal
Save & Exit
Instructions
Resources
scan, found machines having FTP ports open, performed dictionary attack to attain credentials, and successfully logged in to the server using the obtained credentials.
Question 6.15.1
"Using bash scripting, perform live host and FTP port identification on the target IP address range 172.19.19.7. Enter the number of hosts that have the FTP port open.
Note: The Bash script file (pentest.sh) is available in the Home Folder directory of the Parrot machine."
12
Score
Correct
Question 6.15.2
Using bash scripting, perform a dictionary attack on the target IP address, 172.19.19.17, to obtain FTP credentials. Enter the password associated with user ruby on the target machine.
ruby
Score
You have reached the max attempts for this question
Previous
Next
21 Minutes Remaining