Lab4: Network Penetration Testing Methodology-Internal (1/3)

INFO40587: ETHICAL HACKING

Kevin Harianto| 991602128| June 1, 2024

Contents

Contents

Executive Summary

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

The objective of this lab is to provide knowledge on the network, system and user enumeration and other penetration testing methodologies that include:

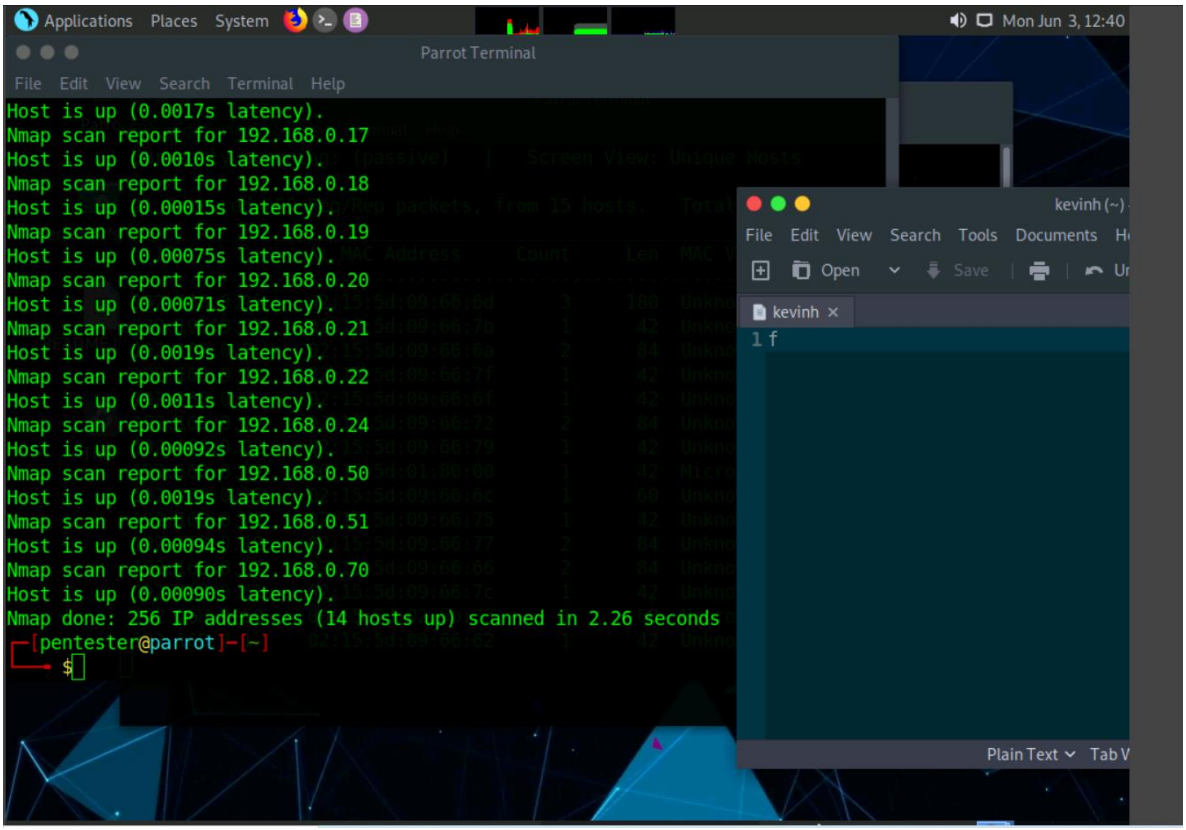
- Service enumeration
- Password audits
- Vulnerability Assessment
- OS pentesting
- Privilege Escalation

Some of the approaches that I have learned about are in relation to reconnaissance where I have leveraged tools such as nmap, ftp, Dmitry and Metasploit to gain insight into how the target database functions. This leads to me learning about the tools involved in the reconnaissance stage, where I was able to observe how tools such as nmap and Dmitry work in relation towards gaining insight into how the database make connections as well as determine whether there are any open ports for a possible attack to be launched against. I also observed how db_nmap can execute lengthy scanning to gain a higher in-depth level of understanding in the target IP Address for future attacks as well as ways in which Metasploit is able to provide a more centralized approach in relation to reconnaissance. From being able to map out the database all the way to obtaining the OS and its version.

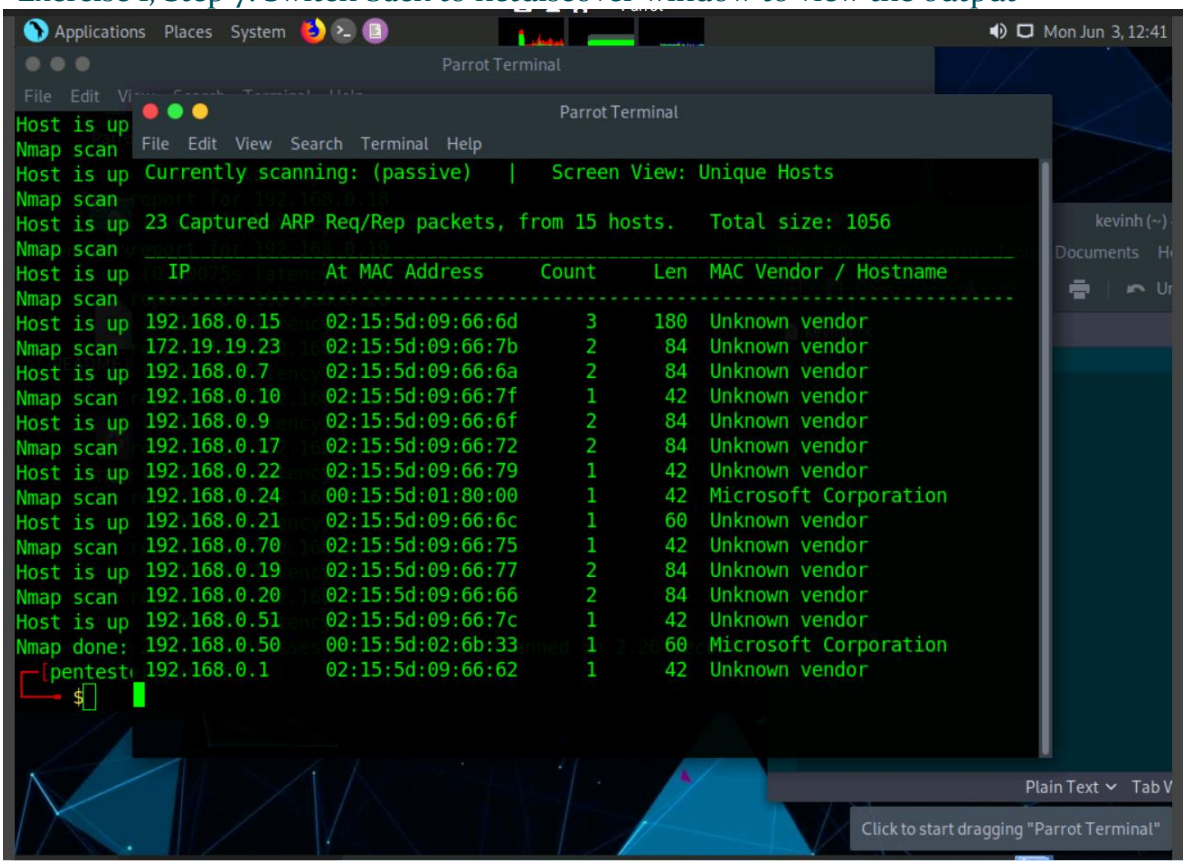
Exercise 1: Scanning with the Tool Netdiscover

1.1 OUTPUT SCREENSHOTS

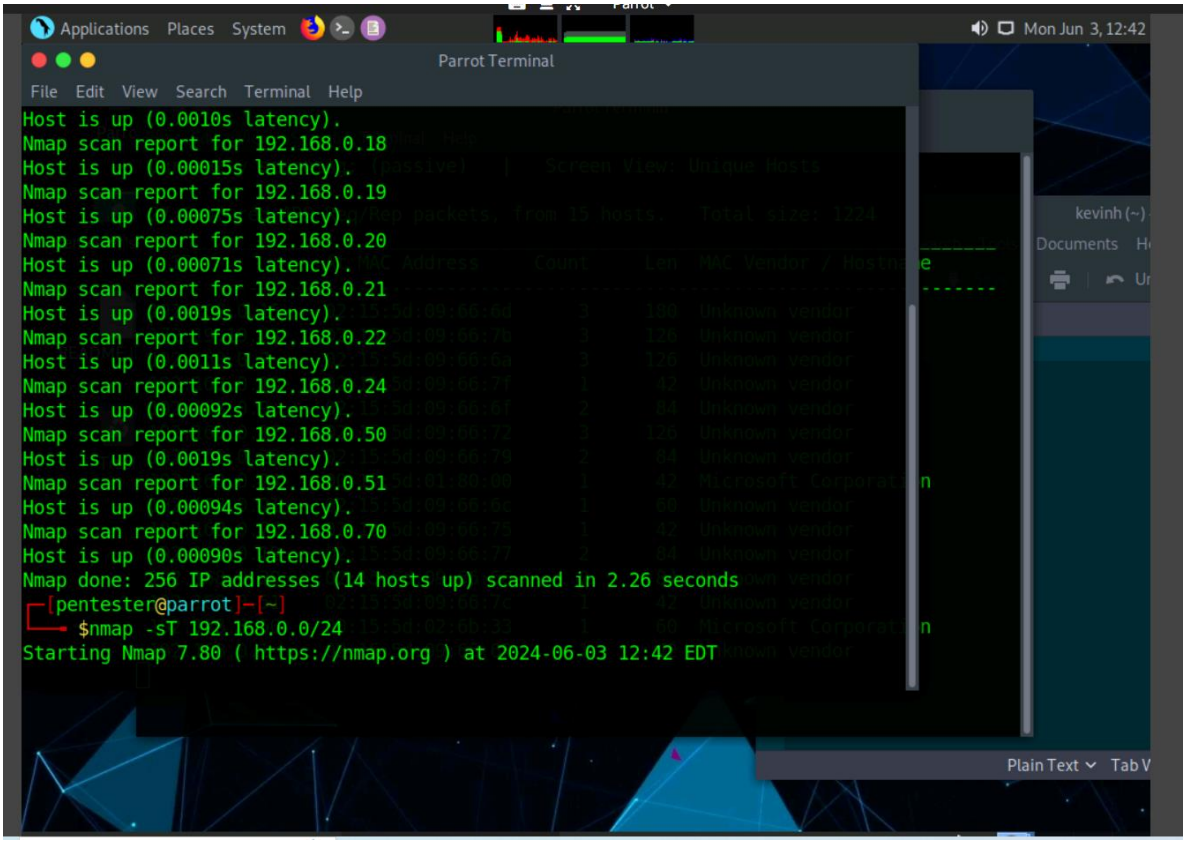
Exercise 1, Step 6: In a new terminal window, enter a Nmap ping sweep to generate traffic. To do a ping sweep, type nmap -sn 192.168.0.0/24 and press Enter.



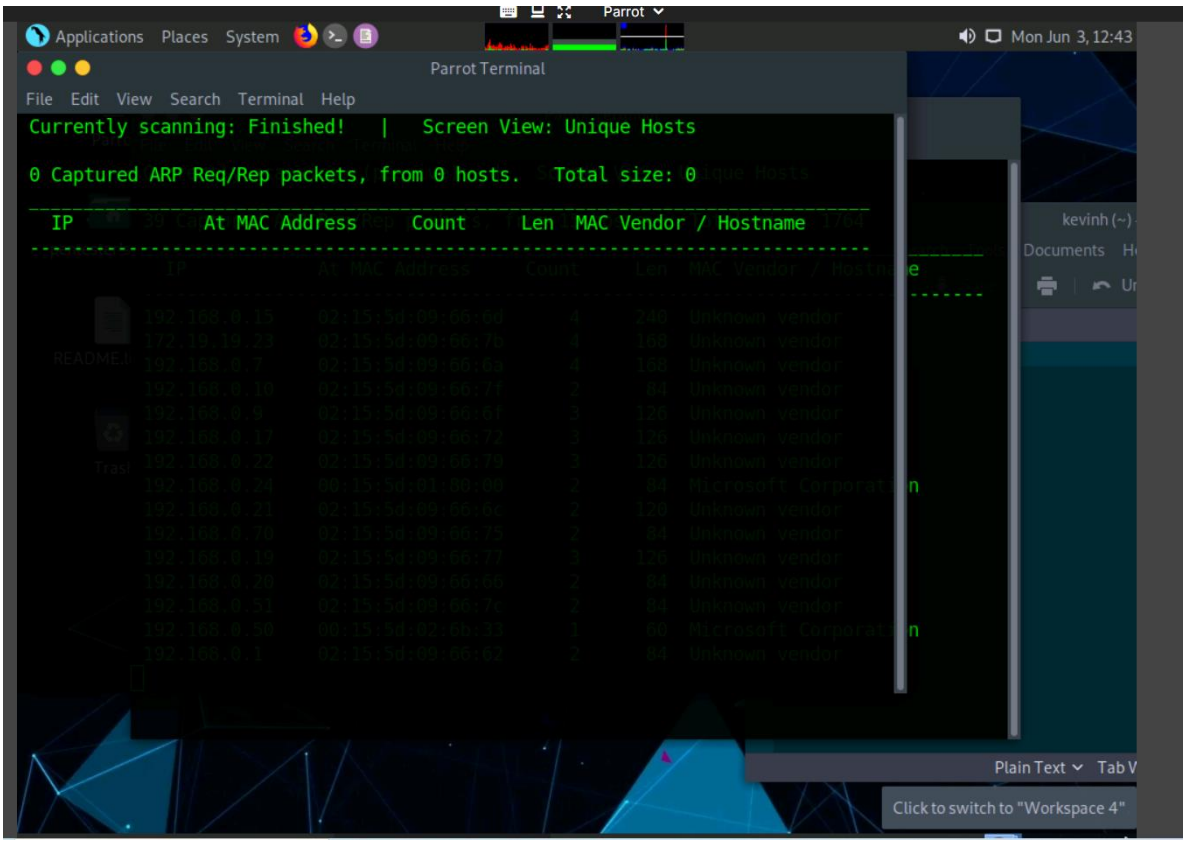
Exercise 1, Step 7: Switch back to netdiscover window to view the output



Exercise 1, Step 8: At times, some machines may not be discovered due to reasons such as the existence of a firewall or some other filter. At such situation, you may use a Transmission Control Protocol (TCP) scan to confirm the existence of the new machine. To perform a TCP scan, enter the command nmap -sT 192.168.0.0/24.



Exercise 1, Step 11: The targets will be displayed on the screen after some time, as shown in the screenshot.



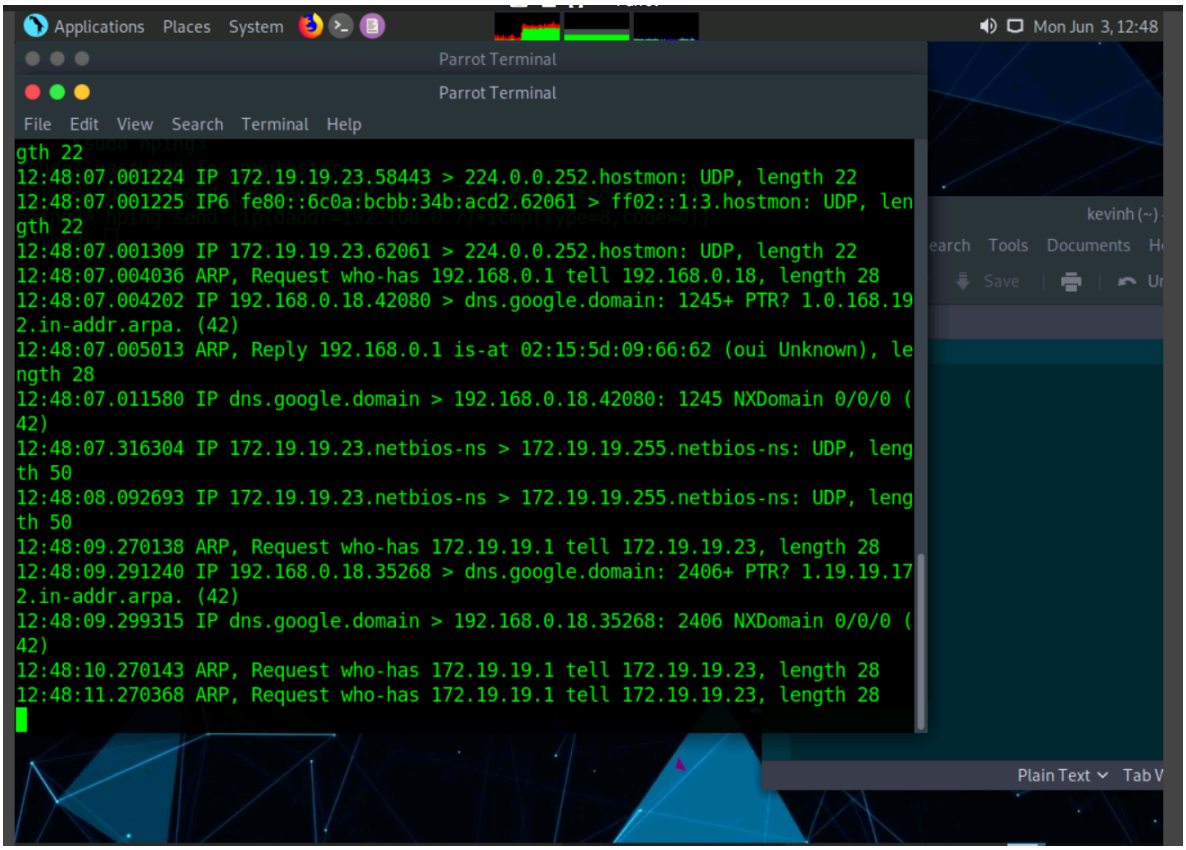
1.2 Questions

NOTE: there are no Questions in Exercise 1

Exercise 2: Scanning and Scripting with hping3

2.1 OUTPUT SCREENSHOTS

Exercise 2, Step 7: If the ICMP echo request is not visible, verify it by opening a new terminal window; type sudo tcpdump –i etho and press Enter. If you are asked you enter a password, type toor and press Enter. This will capture the network traffic. Run the command again and watch the output of the tcpdump command.



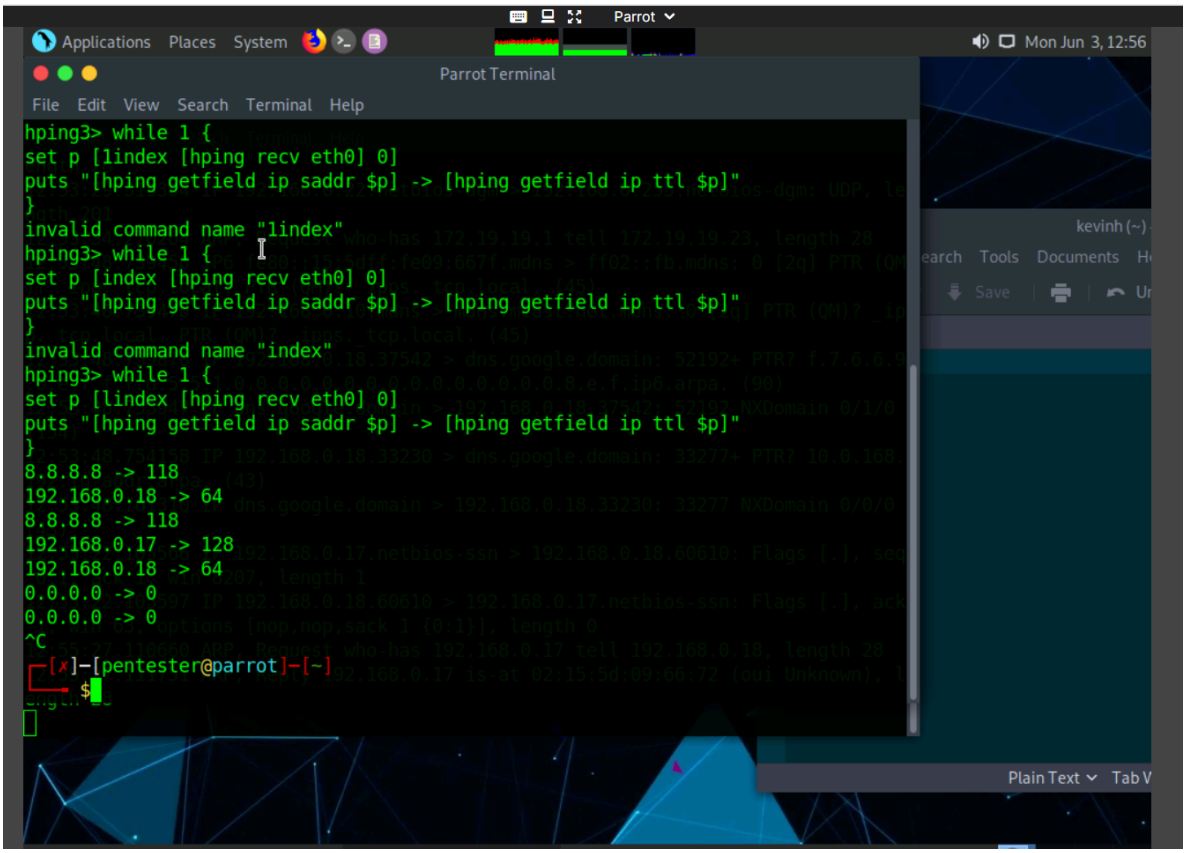
Exercise 2, Step 10: Enter a simple loop to receive packets. In the hping3 terminal window, enter the following command:

while 1 {

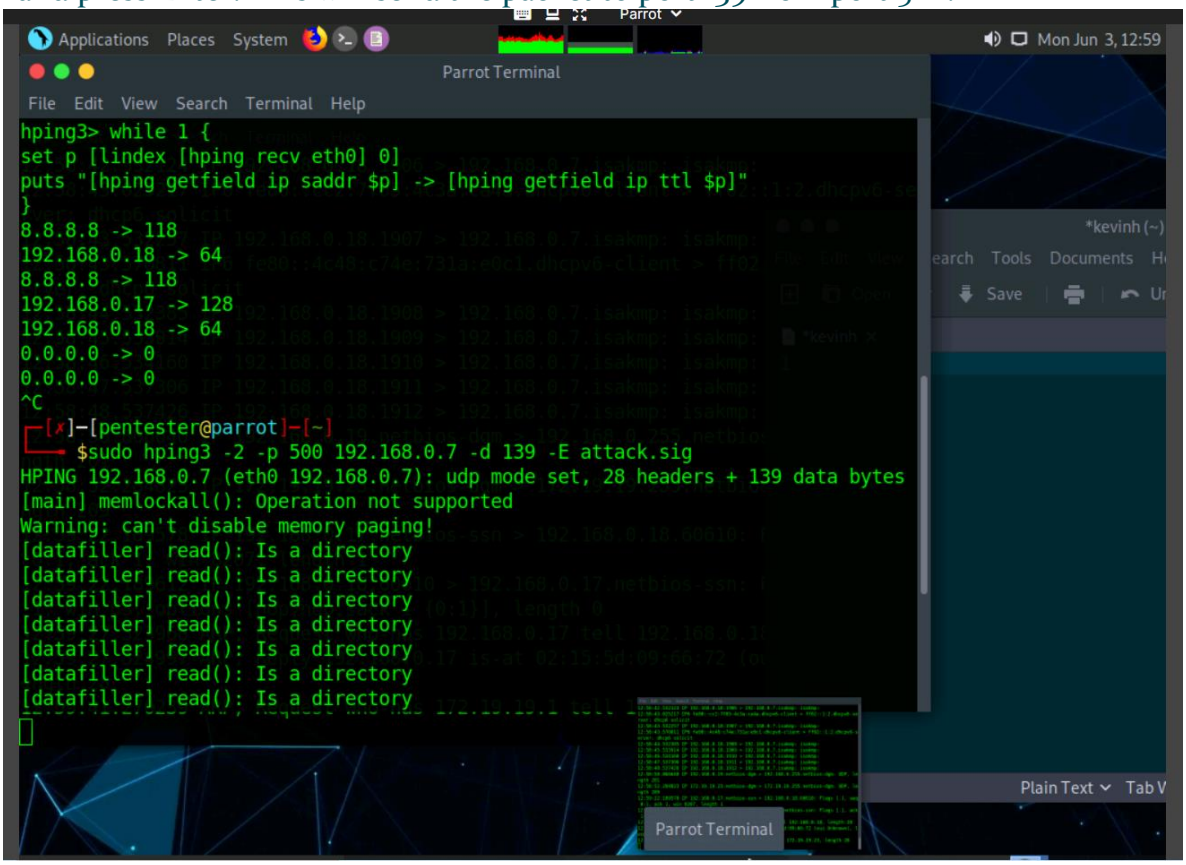
set p [lindex [hping recv etho] 0]

puts "[hping getfield ip saddr $p] -> [hping getfield ip ttl $p]"

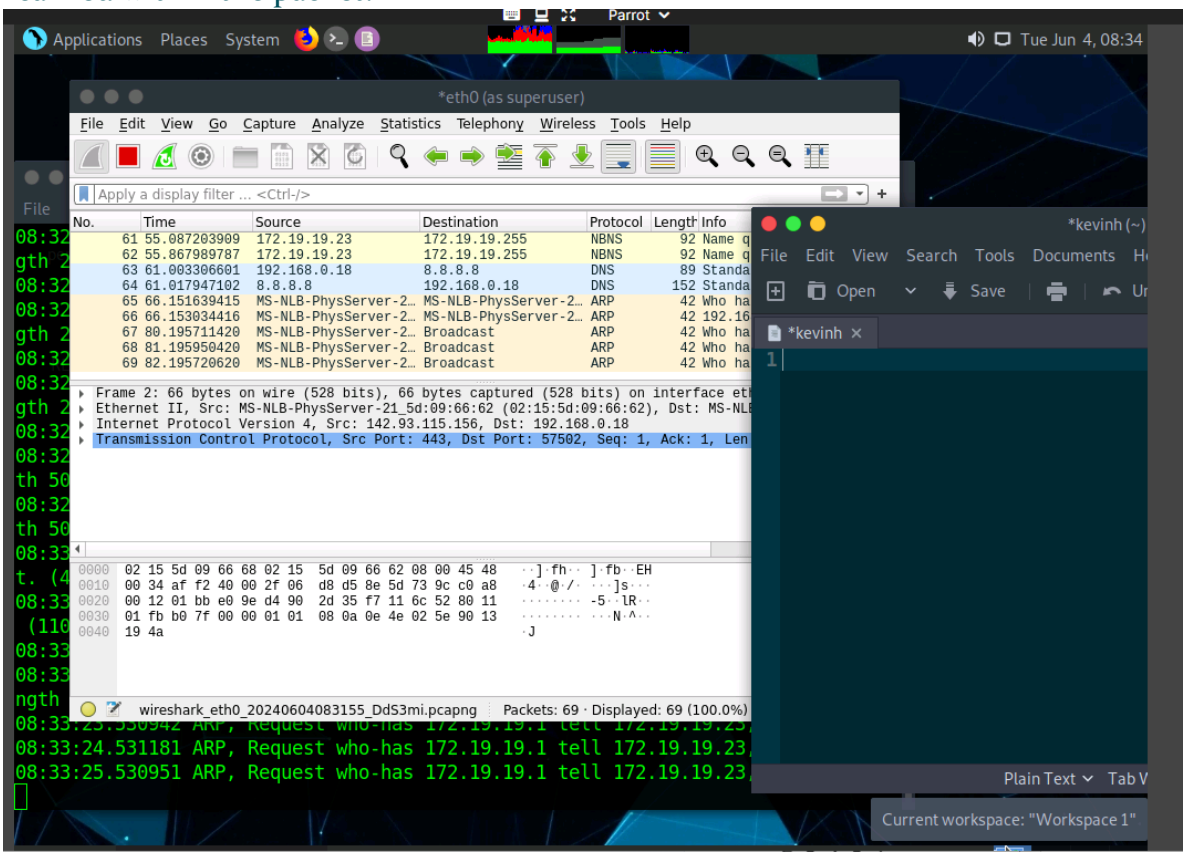
}



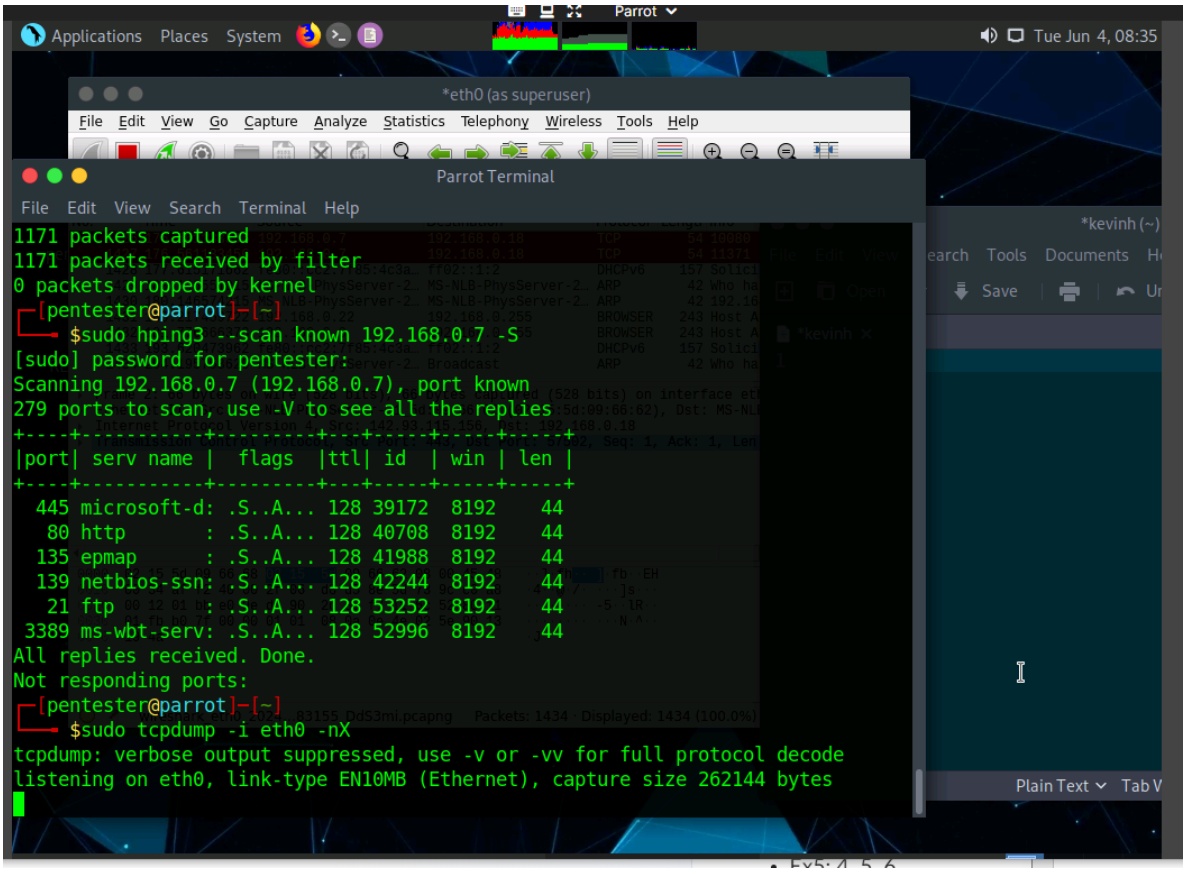
Exercise 2, Step 12: The hping3 tool allows users to send messages. Accordingly, send the message as a string. Open a new terminal window, type sudo hping3 -2 -p 500 192.168.0.7 -d 139 -E attack.sig, and press Enter. Type toor in the password field and press Enter. This will send the packet to port 139 from port 500.



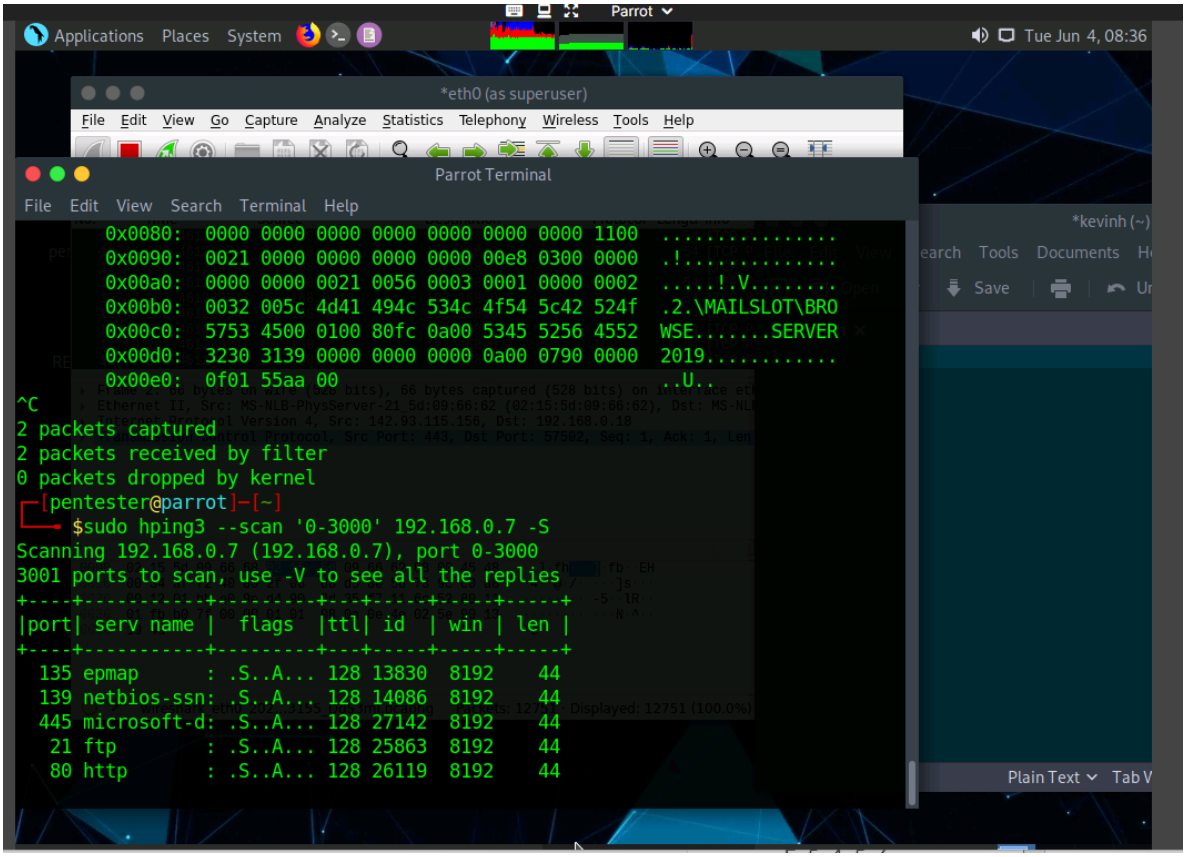
Exercise 2, Step 15: The window shows the Internet Security Association and Key Management Protocol (ISAKMP) traffic, as you are using User Datagram Protocol (UDP) port 500. The lower window also shows that the message you specified is carried within the packet.



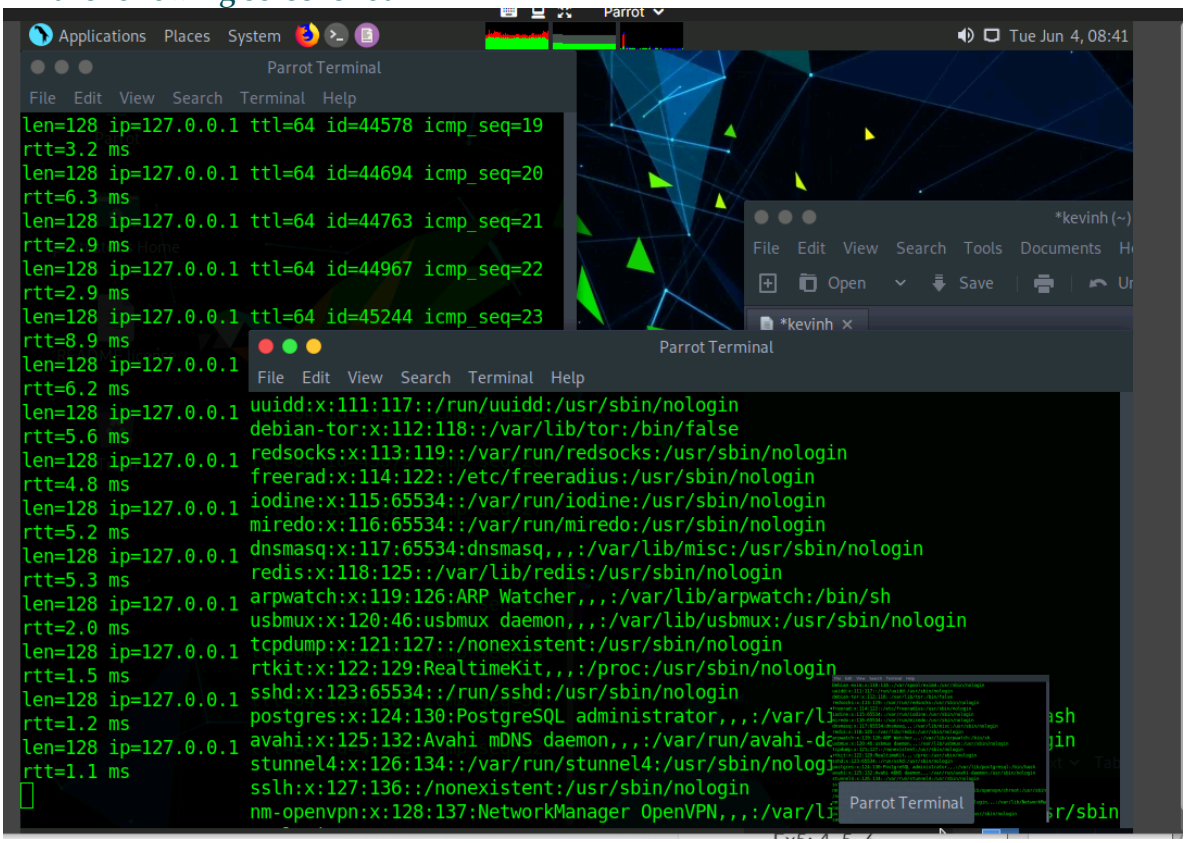
Exercise 2, Step 16: The message in the packet can also be displayed using tcpdump: Type sudo tcpdump –i etho –nX in the terminal window. If you are asked to enter the password, enter toor.



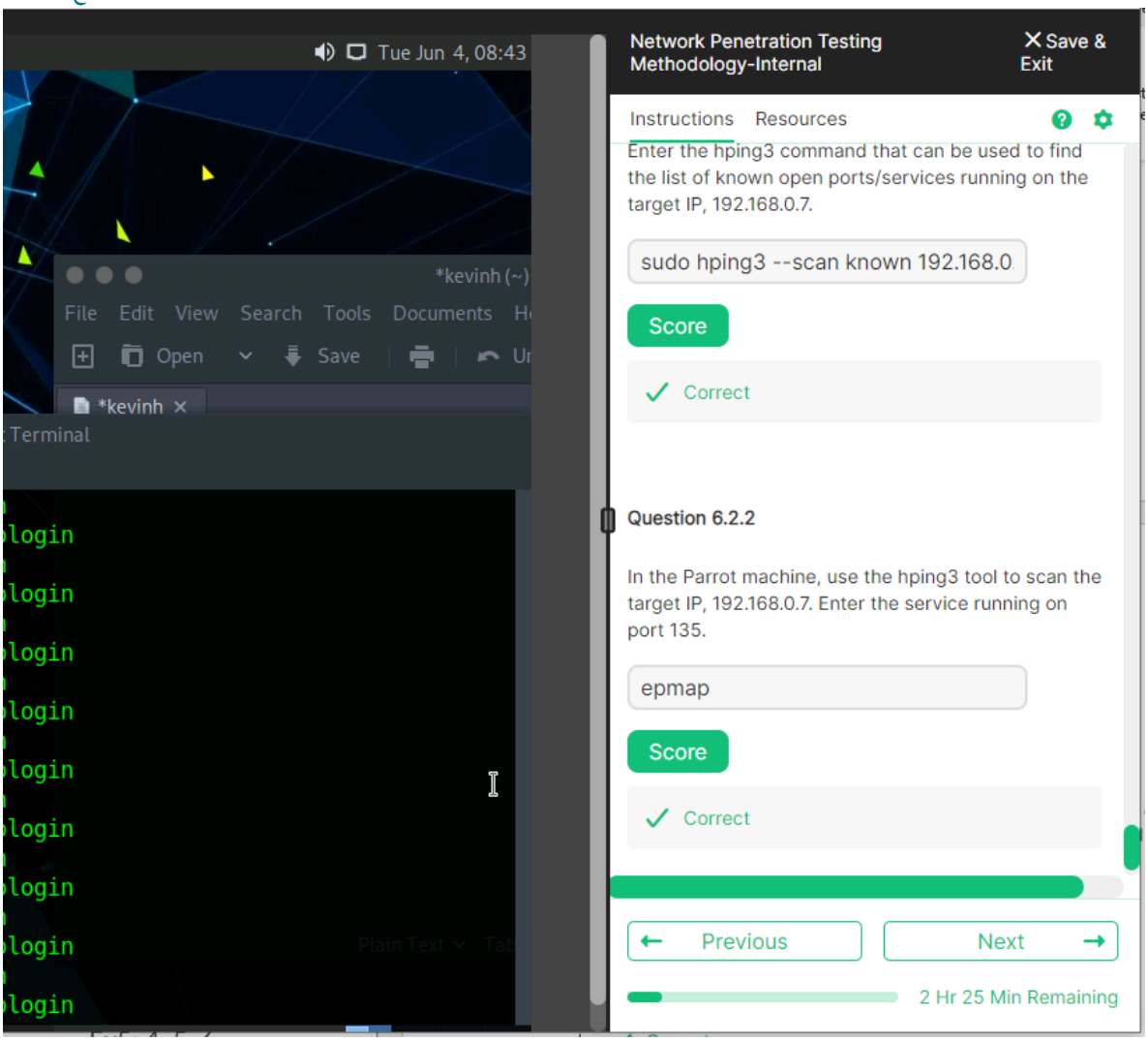
Exercise 2, Step 18: Hping3 is a powerful scanning tool that, in the previous example, only showed the known option for the ports listed in /etc/services. Next, specify a range to scan. In the terminal window, enter sudo hping3 --scan '0-3000' 192.168.0.7 –S, as shown in the screenshot



Exercise 2, Step 23: The file contents begin to appear in the first terminal as shown in the following screenshot



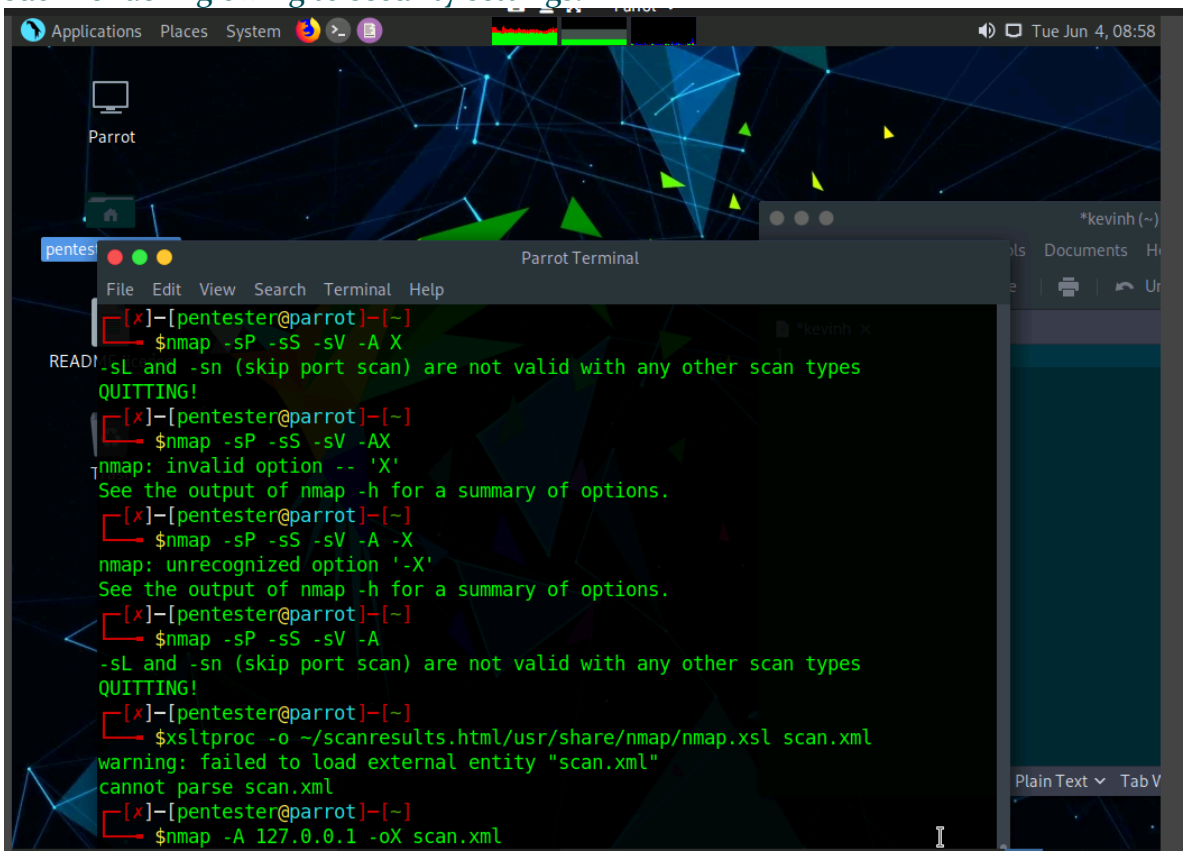
2.2 QUESTIONS



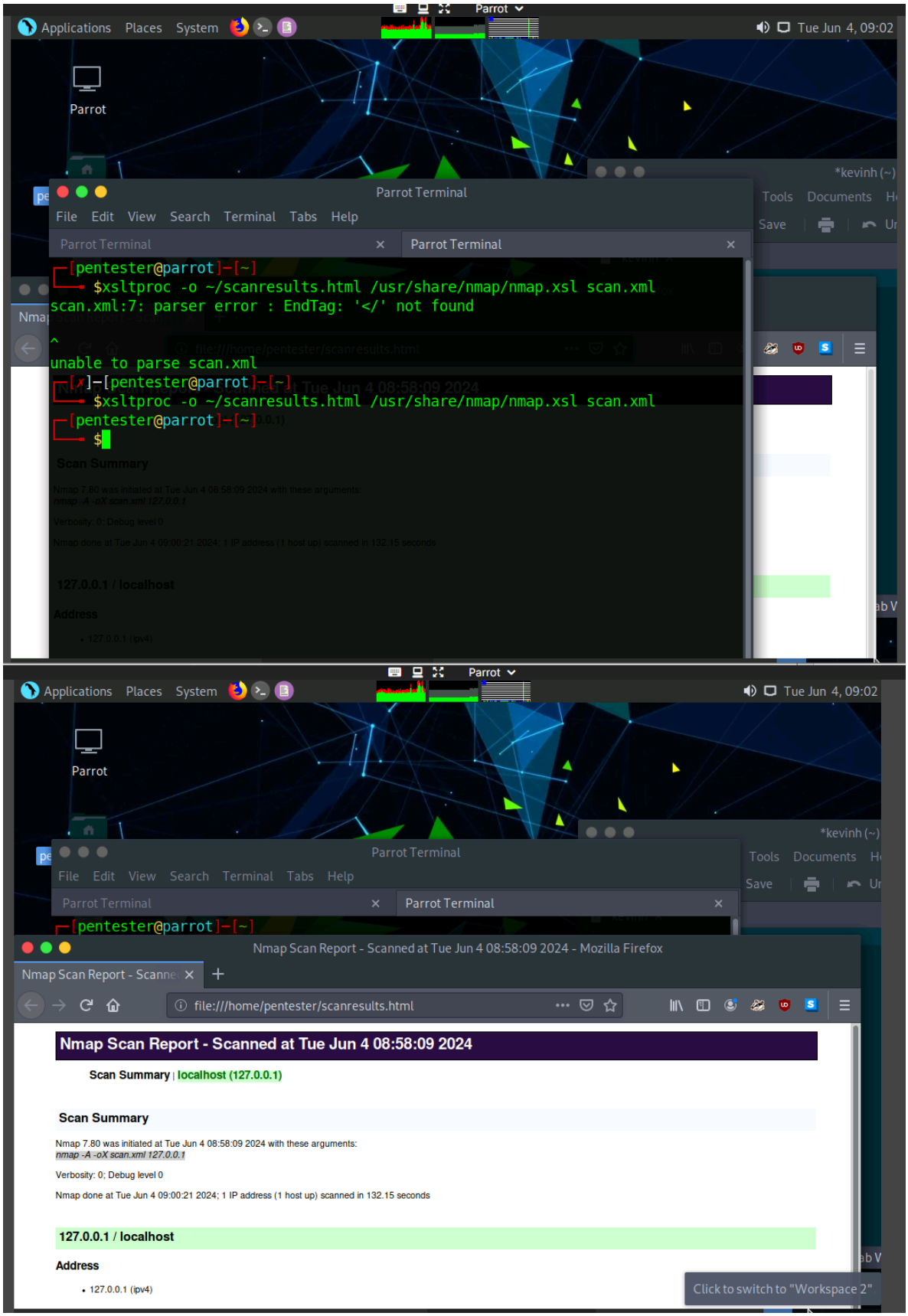
Exercise 3: Scanning and Building a Target Database

3.1 OUTPUT SCREENSHOTS

Exercise 3, Step 5: The output can be made into an XML format by adding "X" to the output option. This requires converting the output to HTML. Prior browsers could render the XML format, but this not reliable, since most browsers no longer allow such rendering owing to security settings.

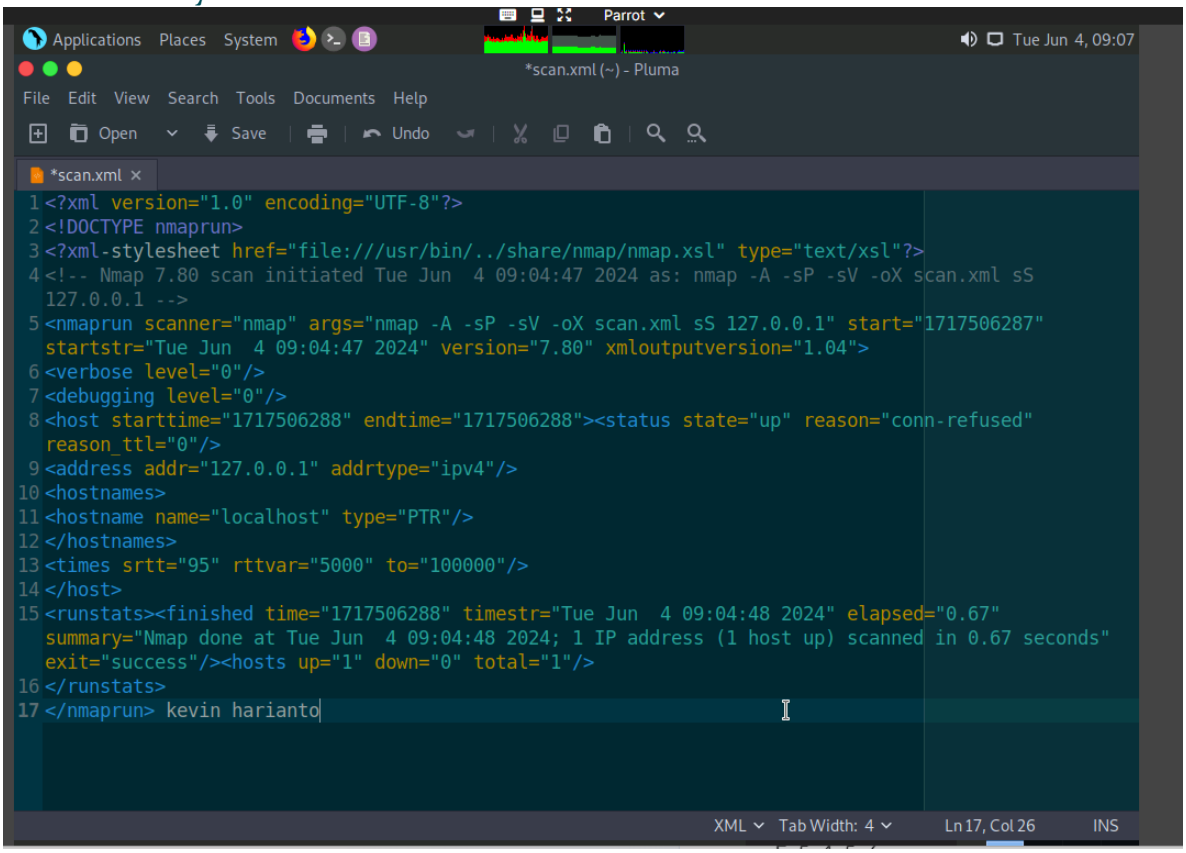


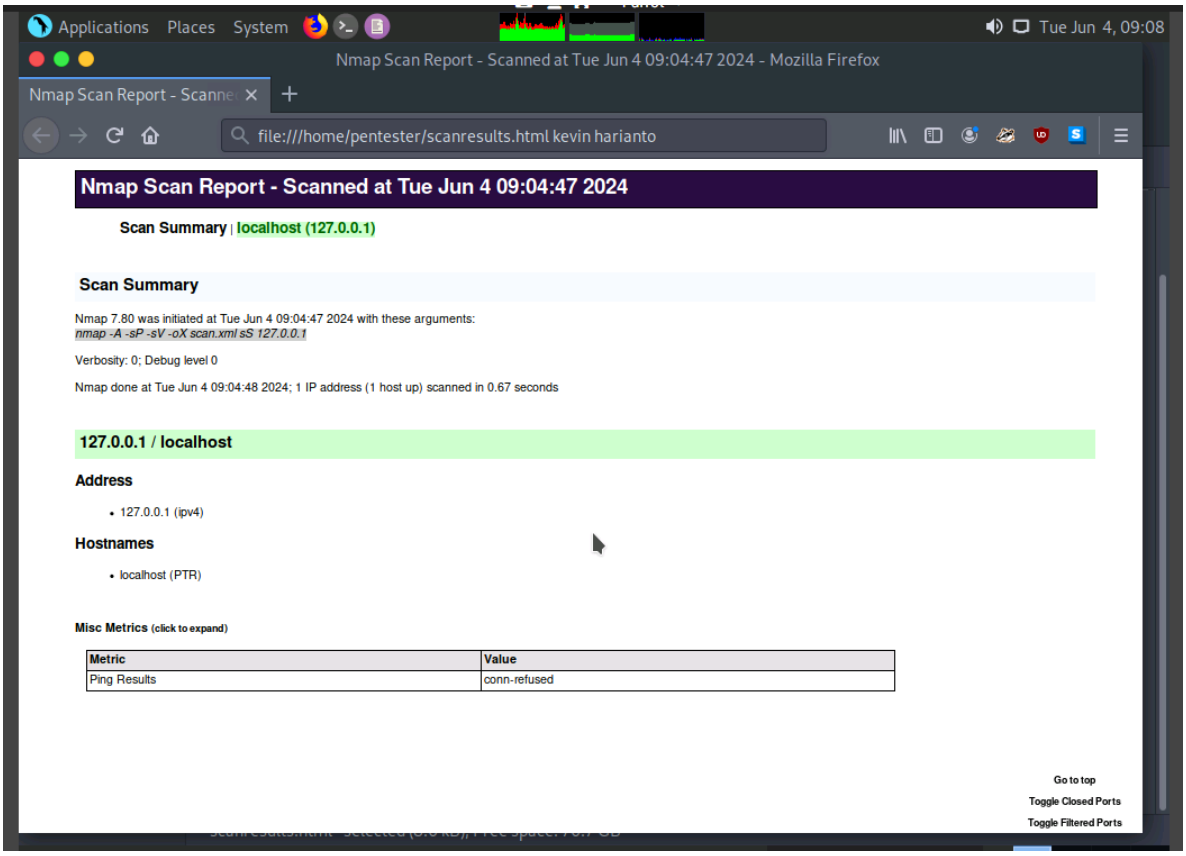
Exercise 3, Step 8: The XML format is a good choice for preparing and creating the database.



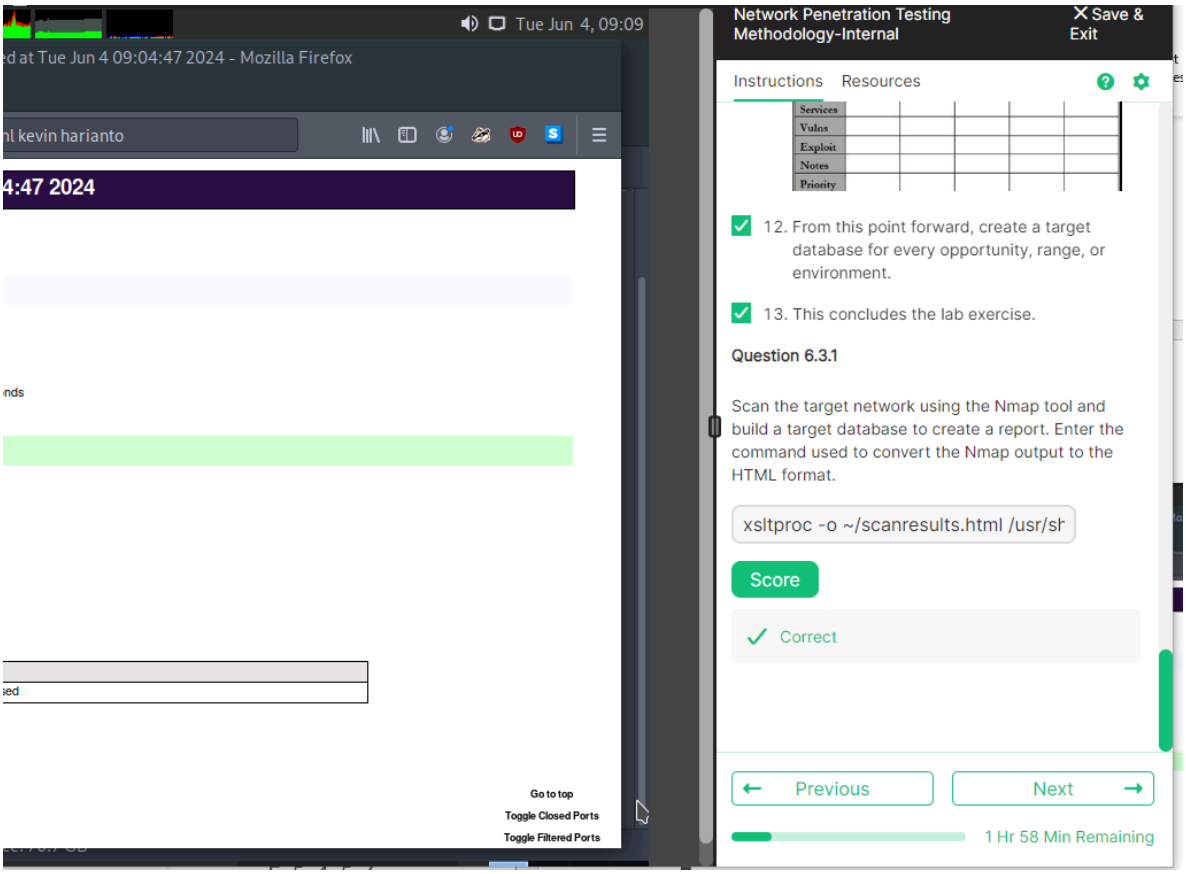
Exercise 3, Step 12: From this point forward, create a target database for every

opportunity, range, or environment.
NOTE: Due to the lack of software to display the table in this type of format, despite leveraging Firefox and utilizing multiple Nmap commands, I was unable to structure the data neatly but was still able to obtain it nonetheless.





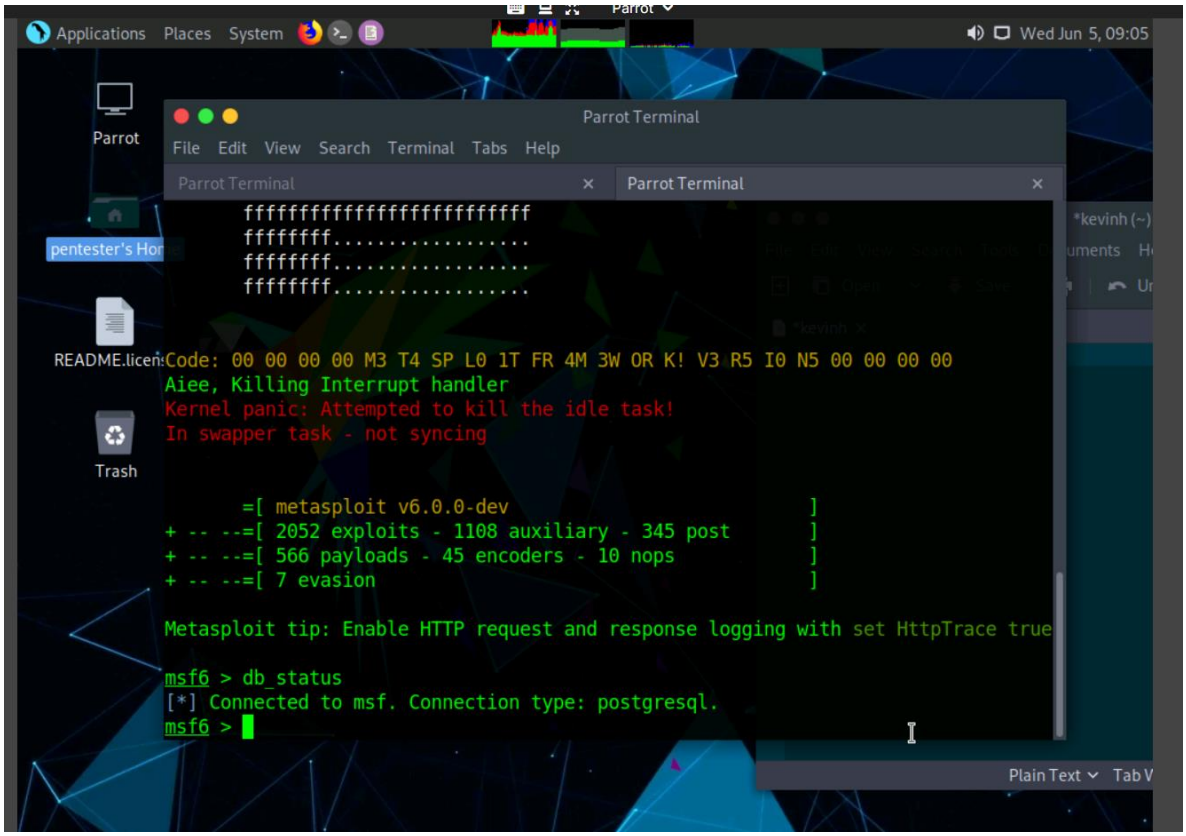
3.2 QUESTIONS



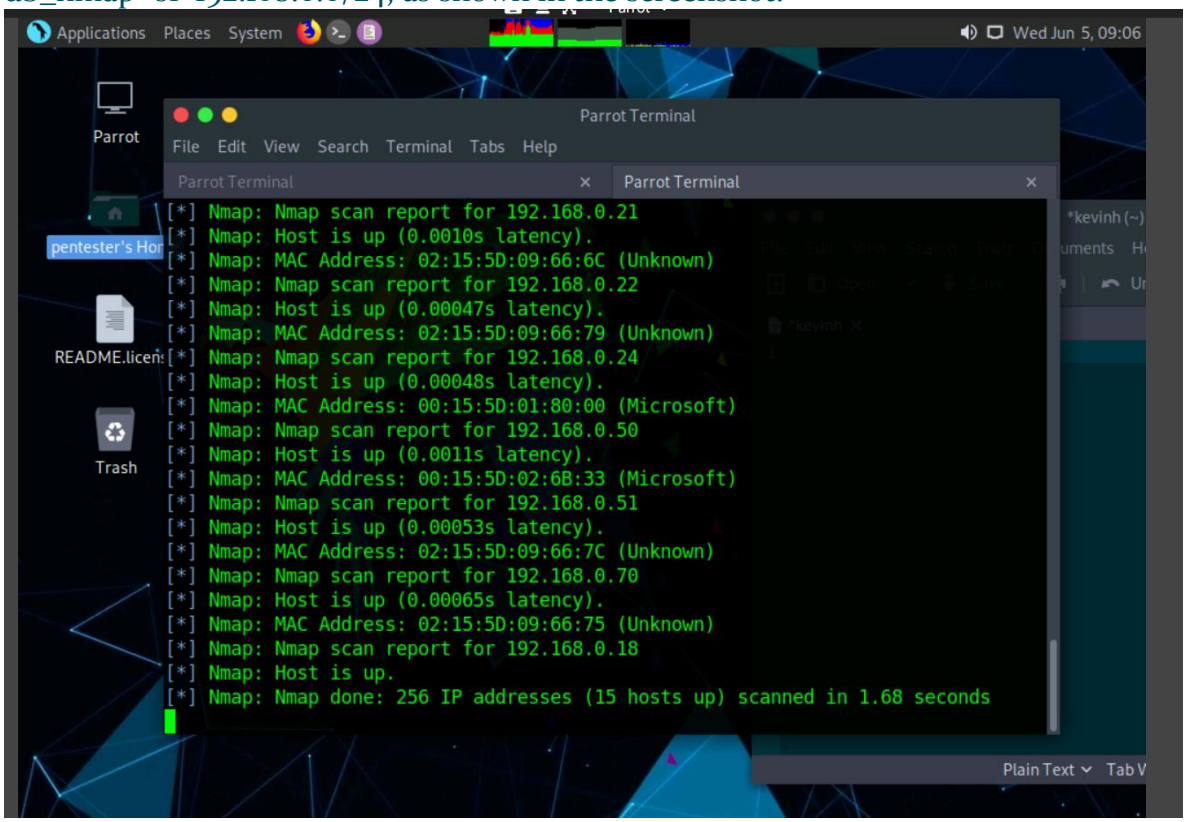
Exercise 4: Using Workspaces and db_nmap

4.1 OUTPUT SCREENSHOTS

Exercise 4, Step 7: To find out the status of the database, type db_status in the terminal window, as shown in the screenshot.

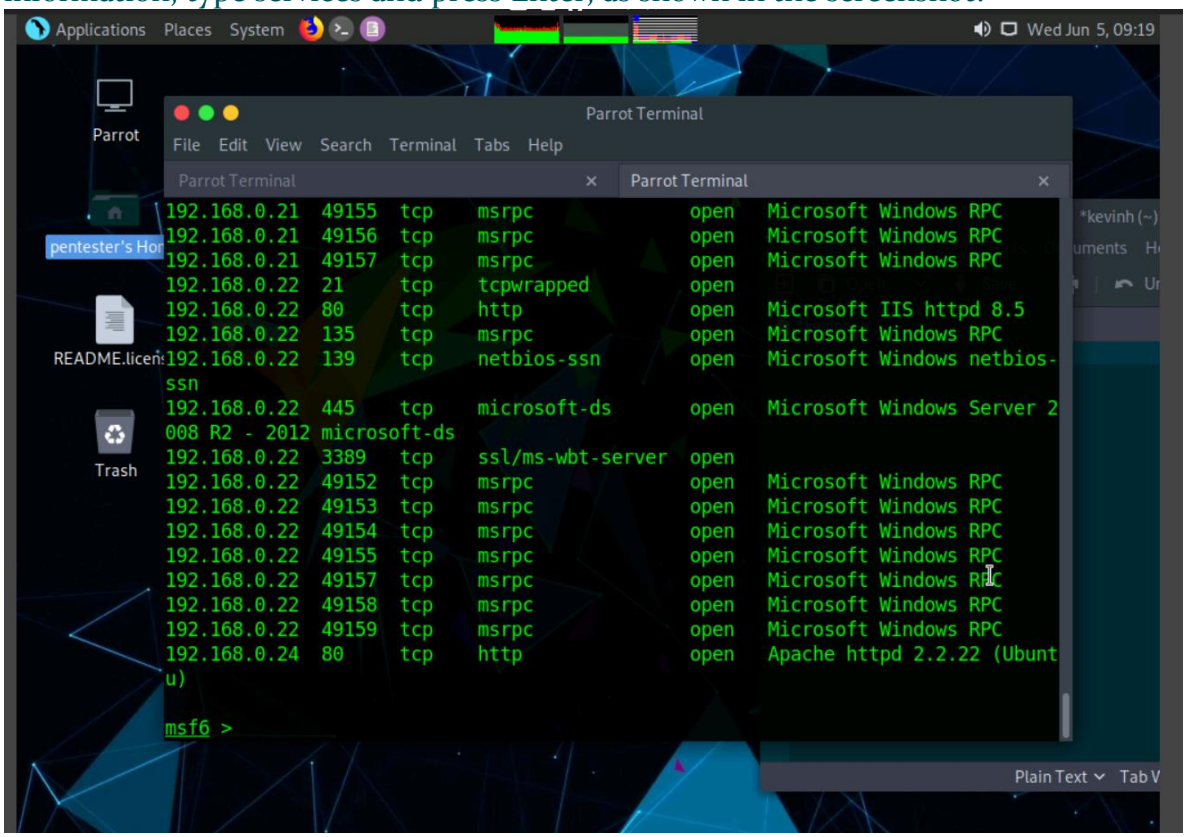


Exercise 4, Step 10: Next, use the tool to conduct the scanning methodology. Enter db_nmap -sP 192.168.0.0/24, as shown in the screenshot.

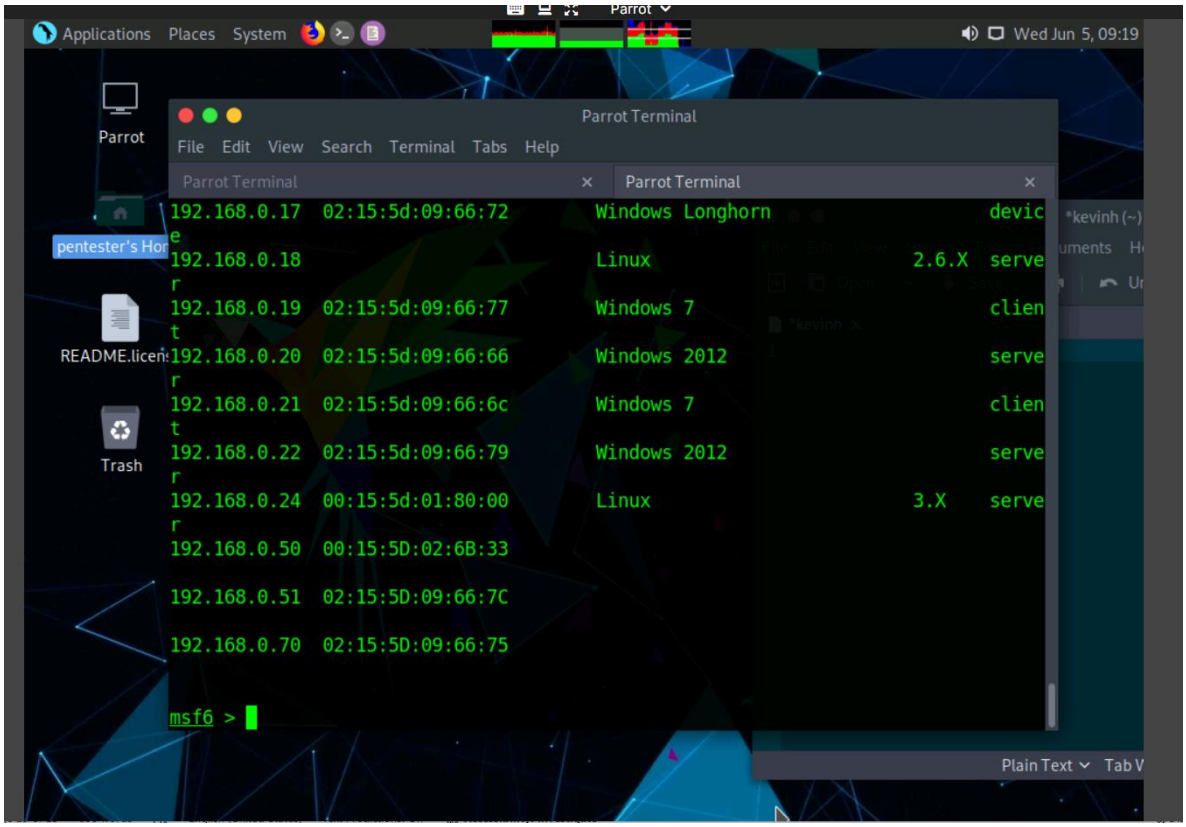


Exercise 4, Step 14: You have now conducted the bulk of the scanning methodology.

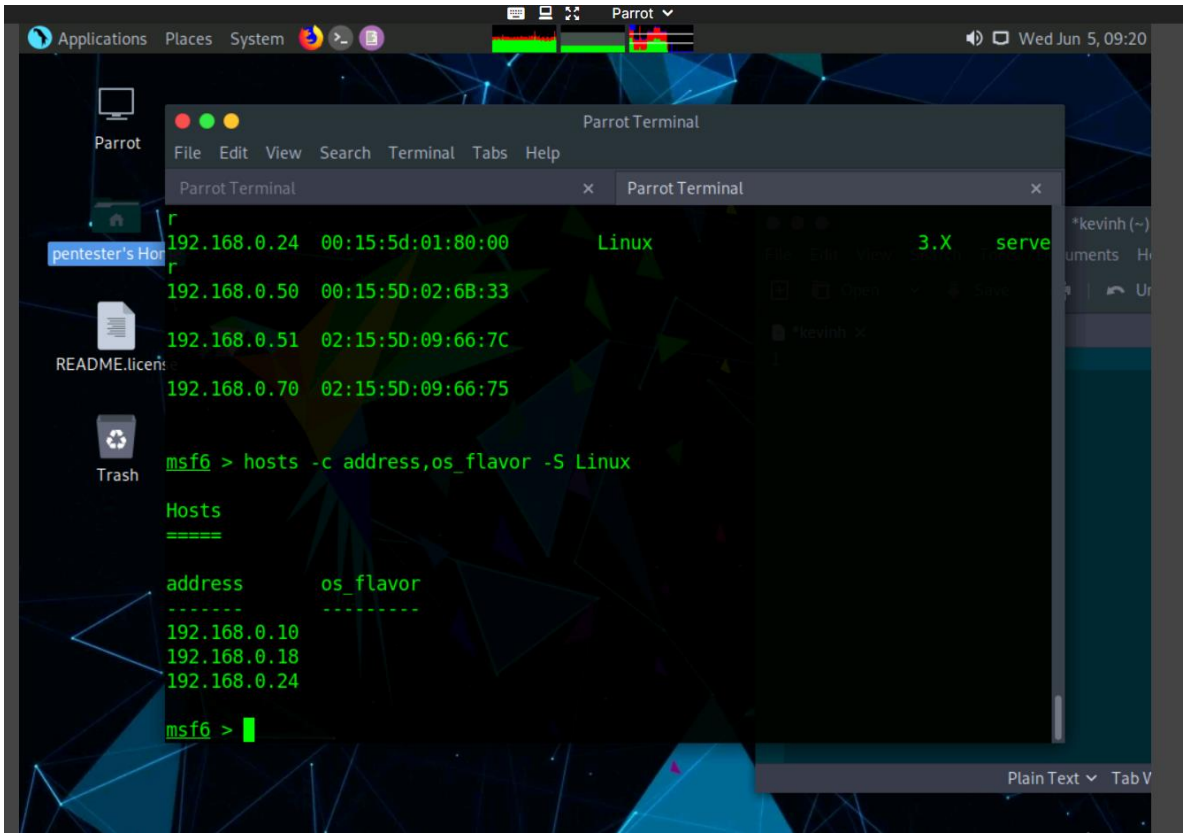
Sufficient data have been stored in the workspace. To examine the database information, type services and press Enter, as shown in the screenshot.



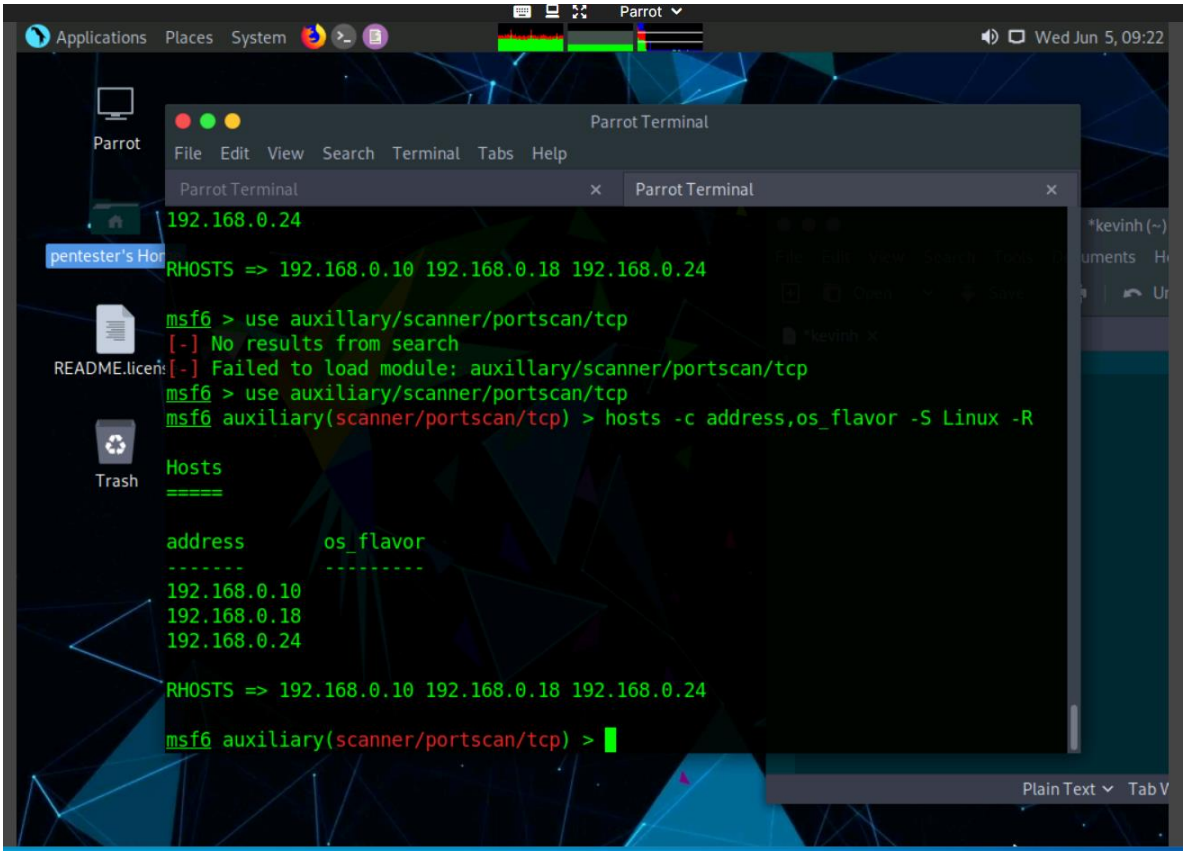
Exercise 4, Step 16: Next, examine the database list of hosts; type hosts, as shown in the screenshot



Exercise 4, Step 20: 'Note that you can also search all entries for a specific target. If you wish to find only Linux-based machines from the scan, use the "-S" option. This option can be combined with our previous example to fine-tune the results. Type hosts -c address,os_flavor -S Linux.

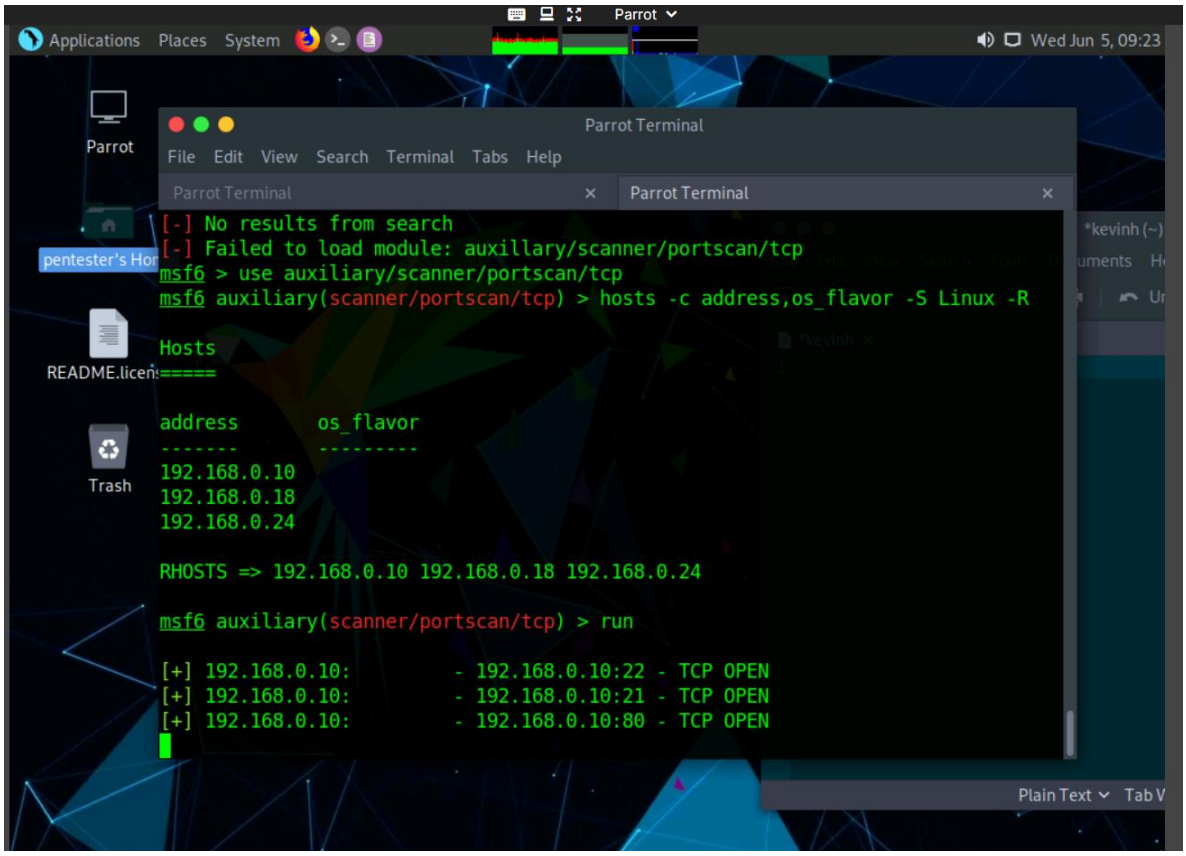


Exercise 4, Step 22: Input the data into the scanner by using the R option; type hosts -c address,os_flavor -S Linux -R and press Enter, as shown in the screenshot.

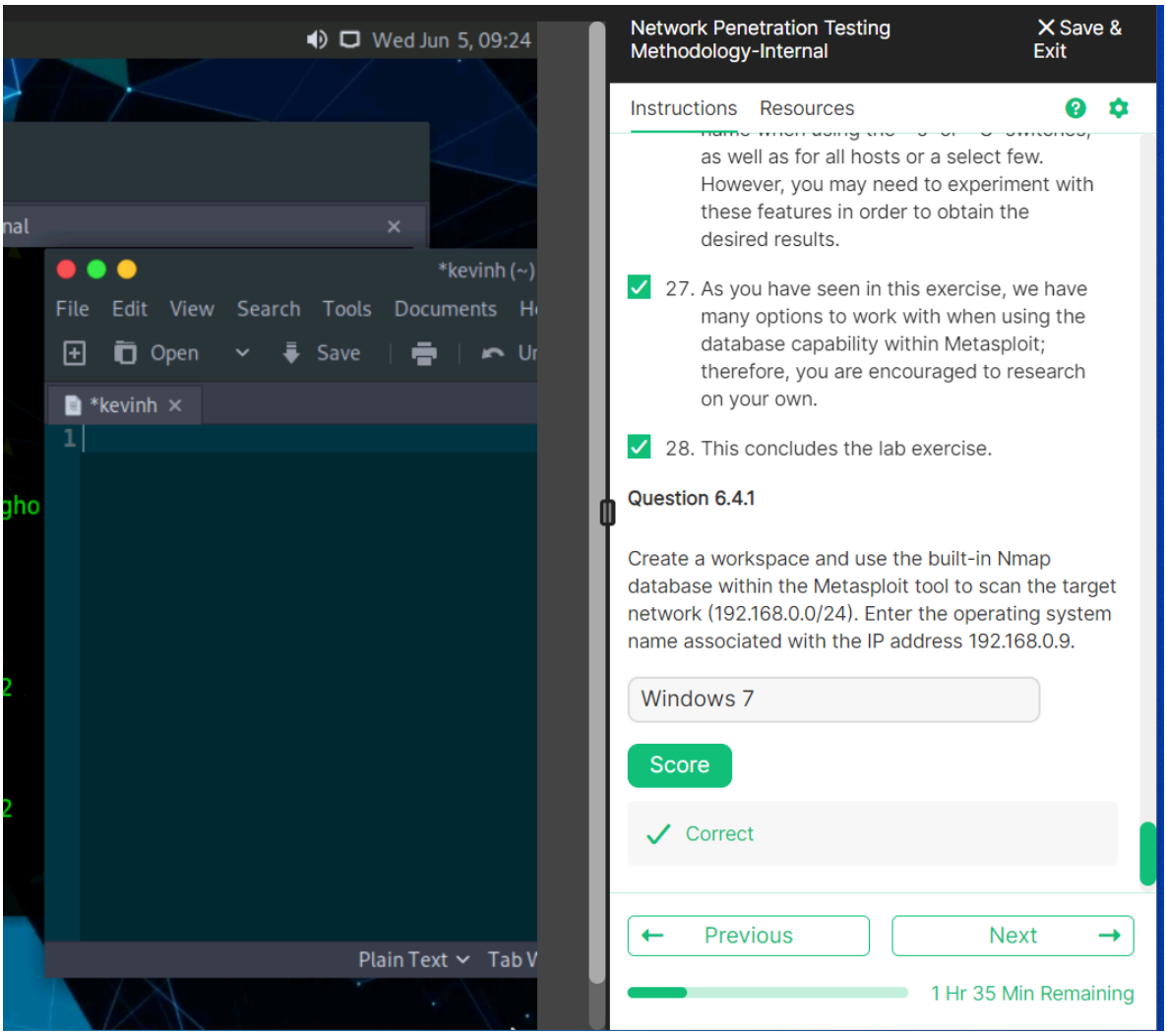


Exercise 4, Step 24: Once you are ready, type run and press Enter. The scan will be conducted against the target added to the database, as shown in the screenshot.

.



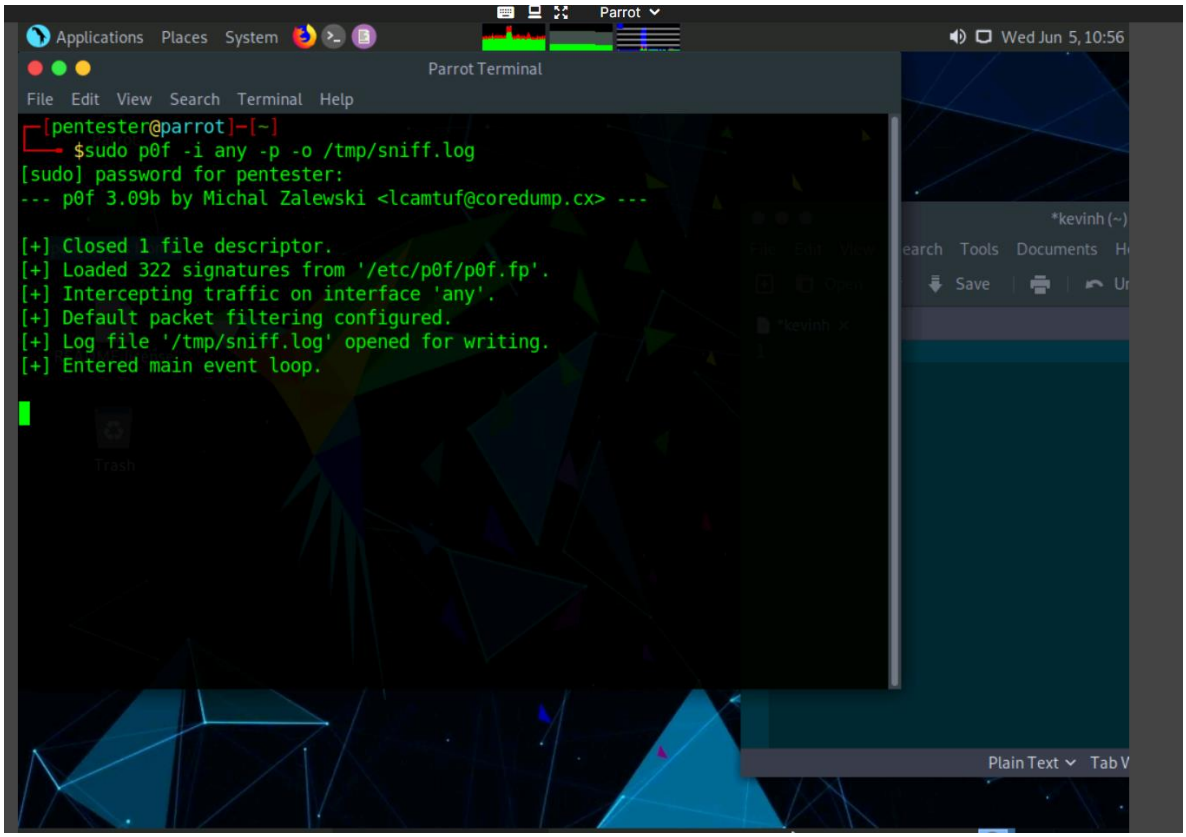
4.2 QUESTIONS



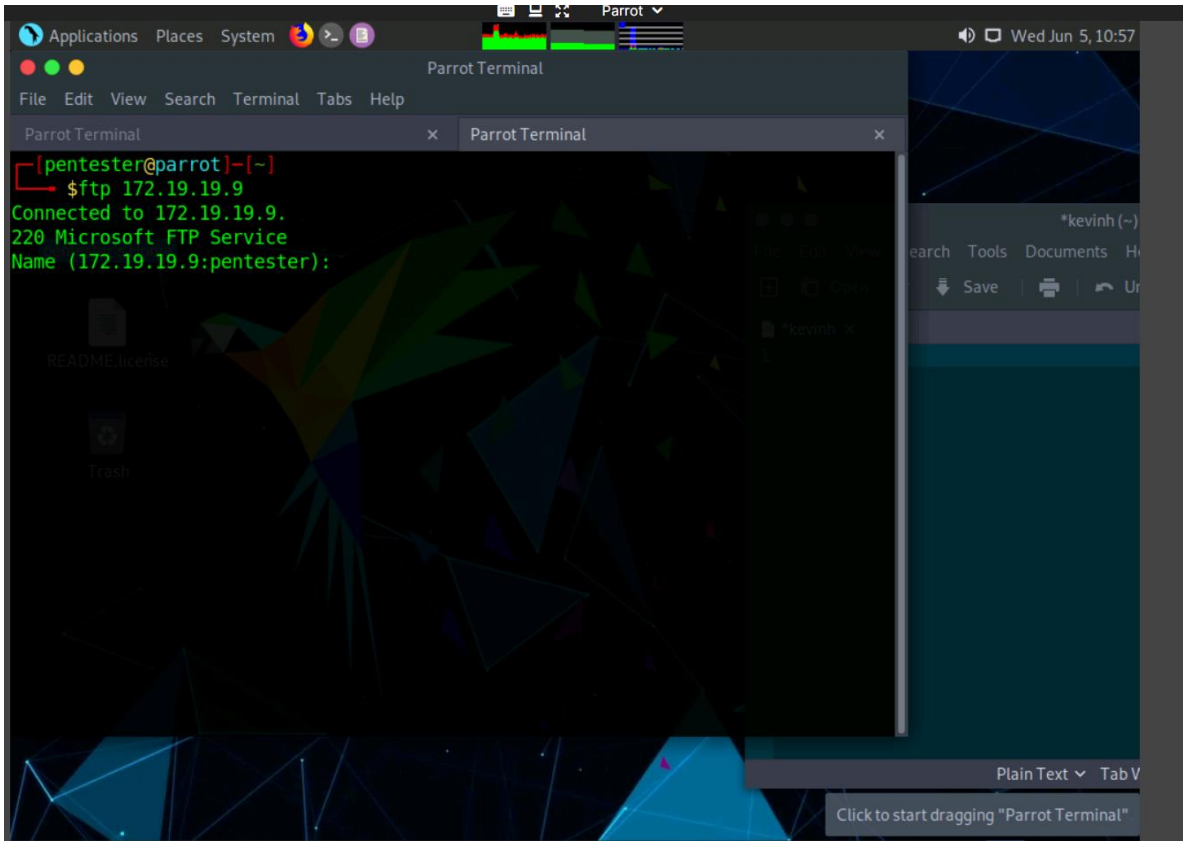
Exercise 5: Performing Passive OS Fingerprinting to Obtain Remote Operating System Information

5.1 OUTPUT SCREENSHOTS

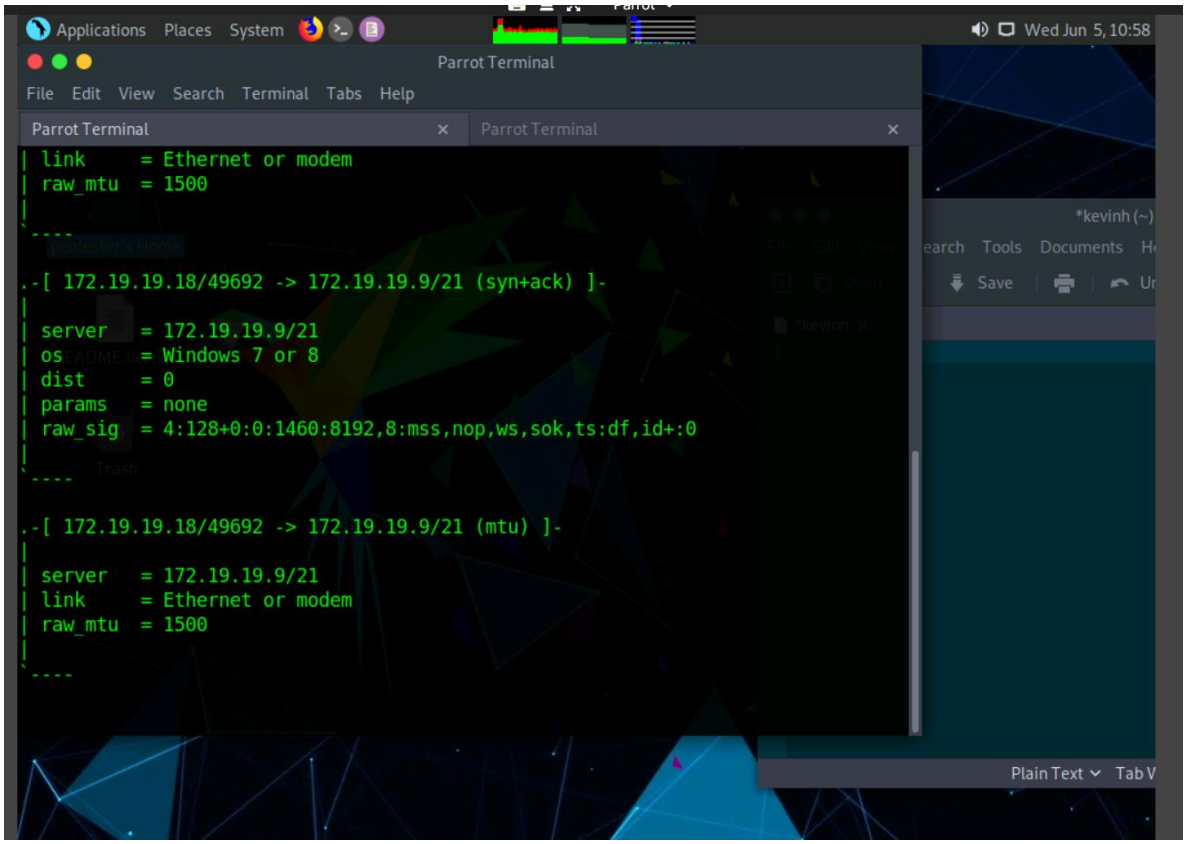
Exercise 5, Step 4: Now, launch a command line terminal, type sudo pof -i any -p -o /tmp/sniff.log and press Enter. Type toor and press Enter when prompted for password. pof begins to listen on all the interfaces of Parrot, and whenever it captures a packet, it decodes the header information and guesses the operating system.



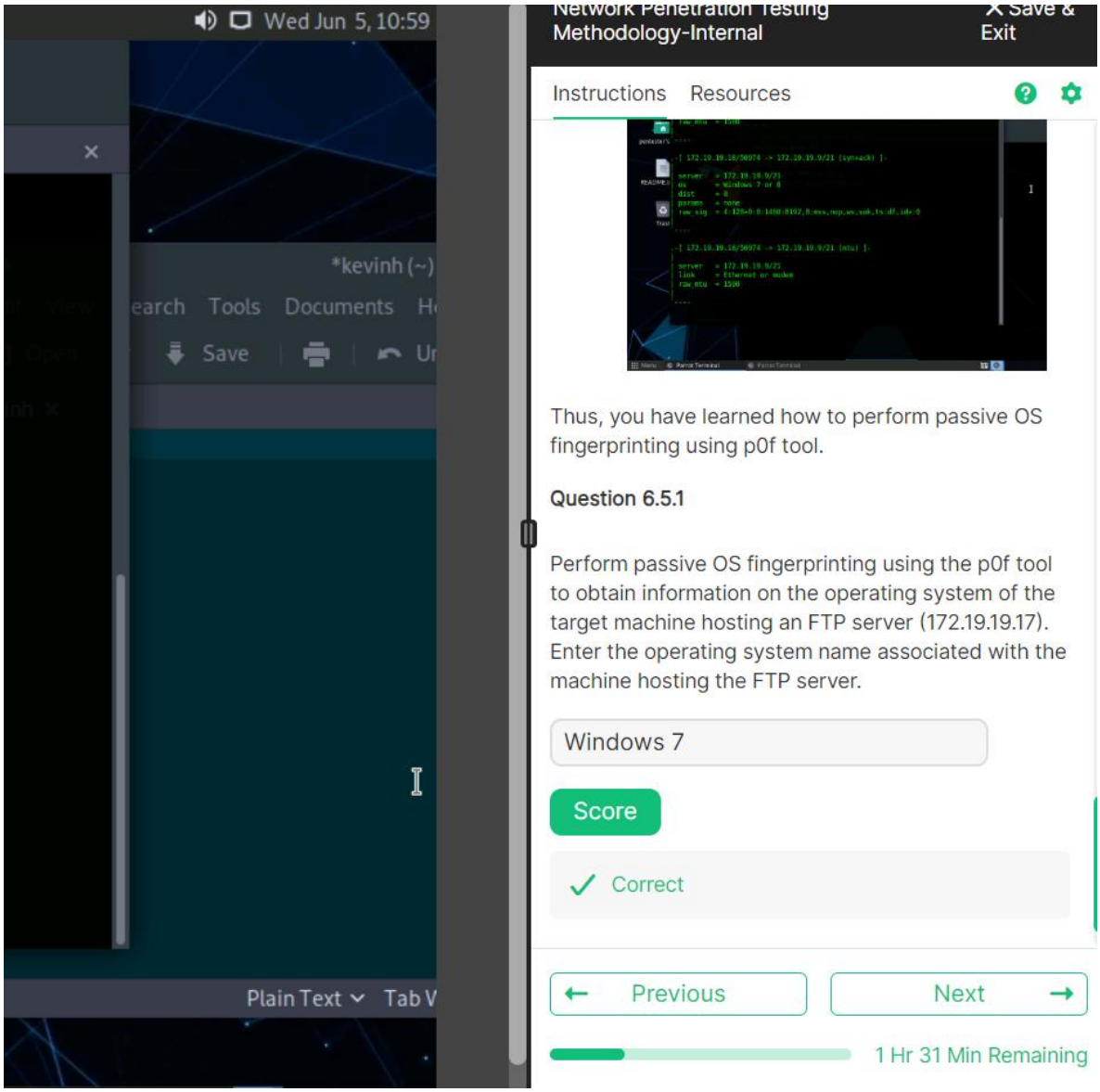
Exercise 5, Step 5: Now, launch another command line terminal, type ftp 172.19.19.9 and press Enter. This will ask you to enter login credentials. By doing so, the client i.e., Parrot machine will send the request and the machine hosting the FTP server will respond to the query.



Exercise 5, Step 6: Switch to the command line terminal where pof is running and scroll up the window. You will observe that pof has analyzed all the requests and responses and decoded them to display information such as OS, raw signature and raw mtu. In this lab, pof identified the operating system as Windows 7 or 8 (or its equivalent). Scroll down the window to view the header information of each packet decoded by the tool.



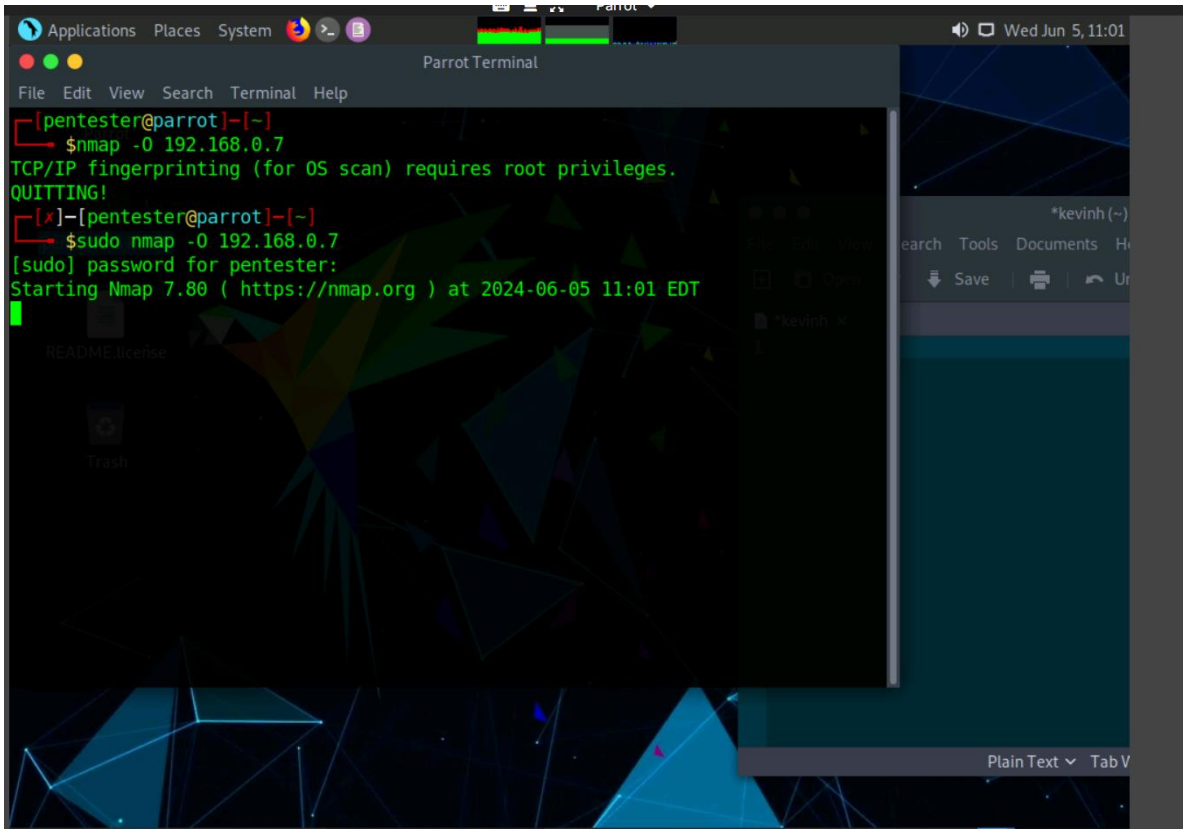
5.2 QUESTIONS



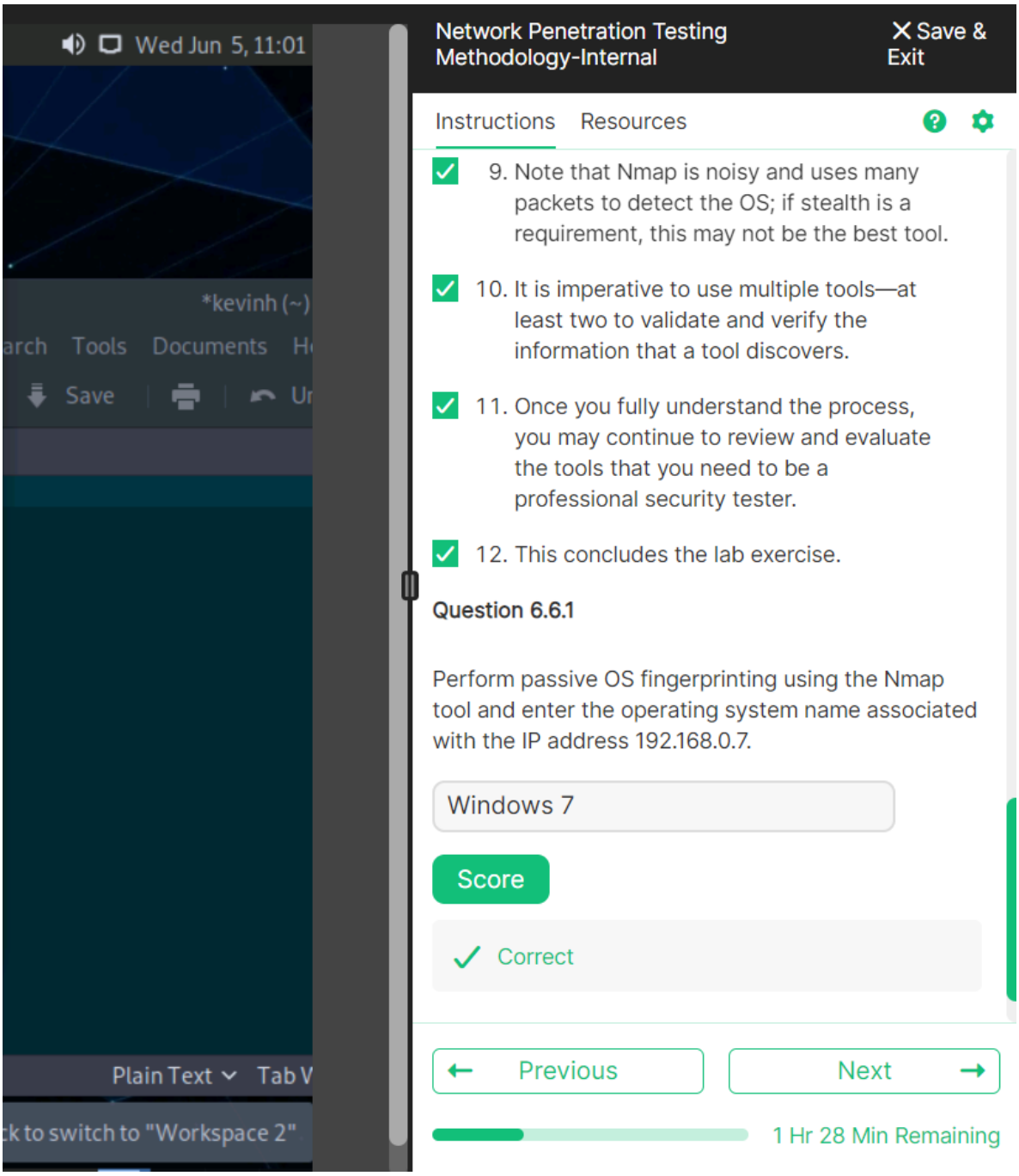
Exercise 6: OS Fingerprinting with Nmap

6.1 OUTPUT SCREENSHOTS

Exercise 6, Step 6: In a terminal window, type sudo nmap –O 192.168.0.X, replacing the “X” with the required IP address number from your target database, as shown in the screenshot



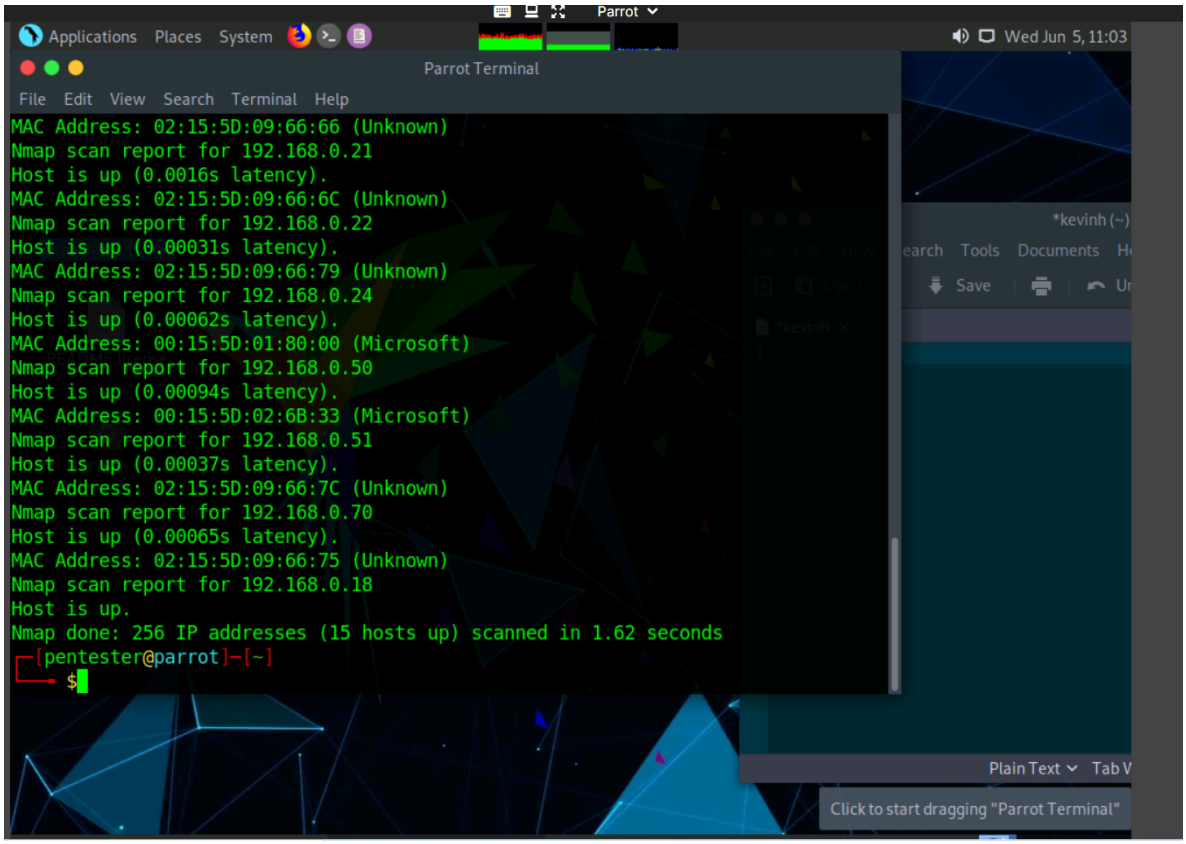
6.2 QUESTIONS



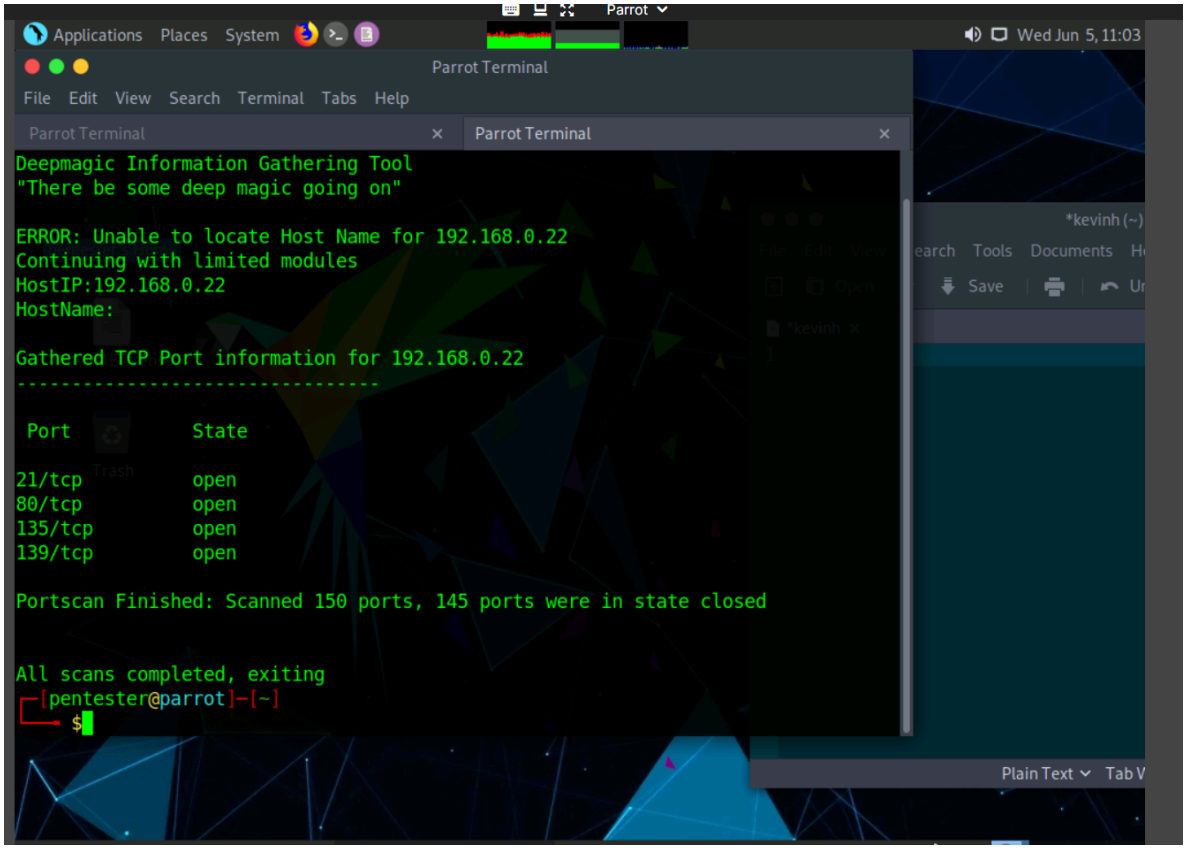
Exercise 7: Scanning with Dmitry

7.1 OUTPUT SCREENSHOTS

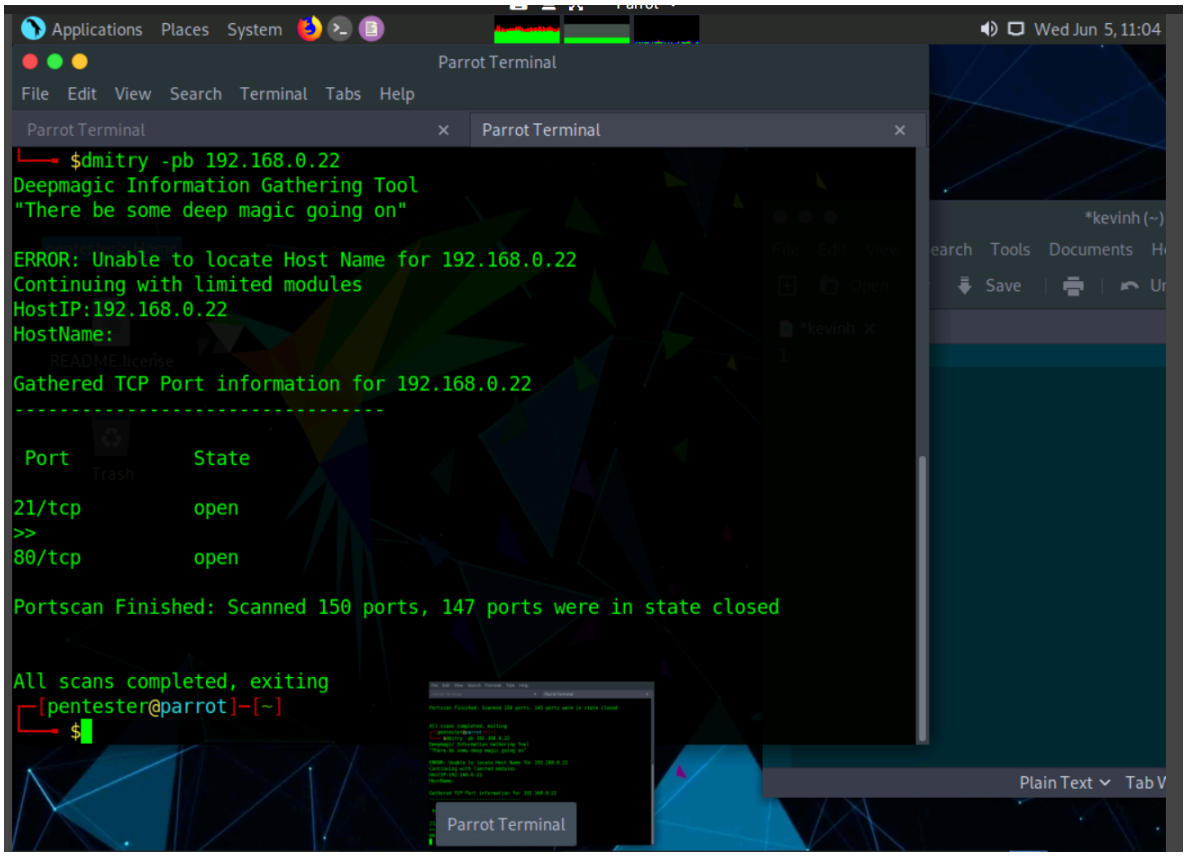
Exercise 7, Step 4: Enter sudo nmap -sn 192.168.0.0/24. Type toor if you are asked to enter the password. An example of a partial output from the command is shown in the screenshot.



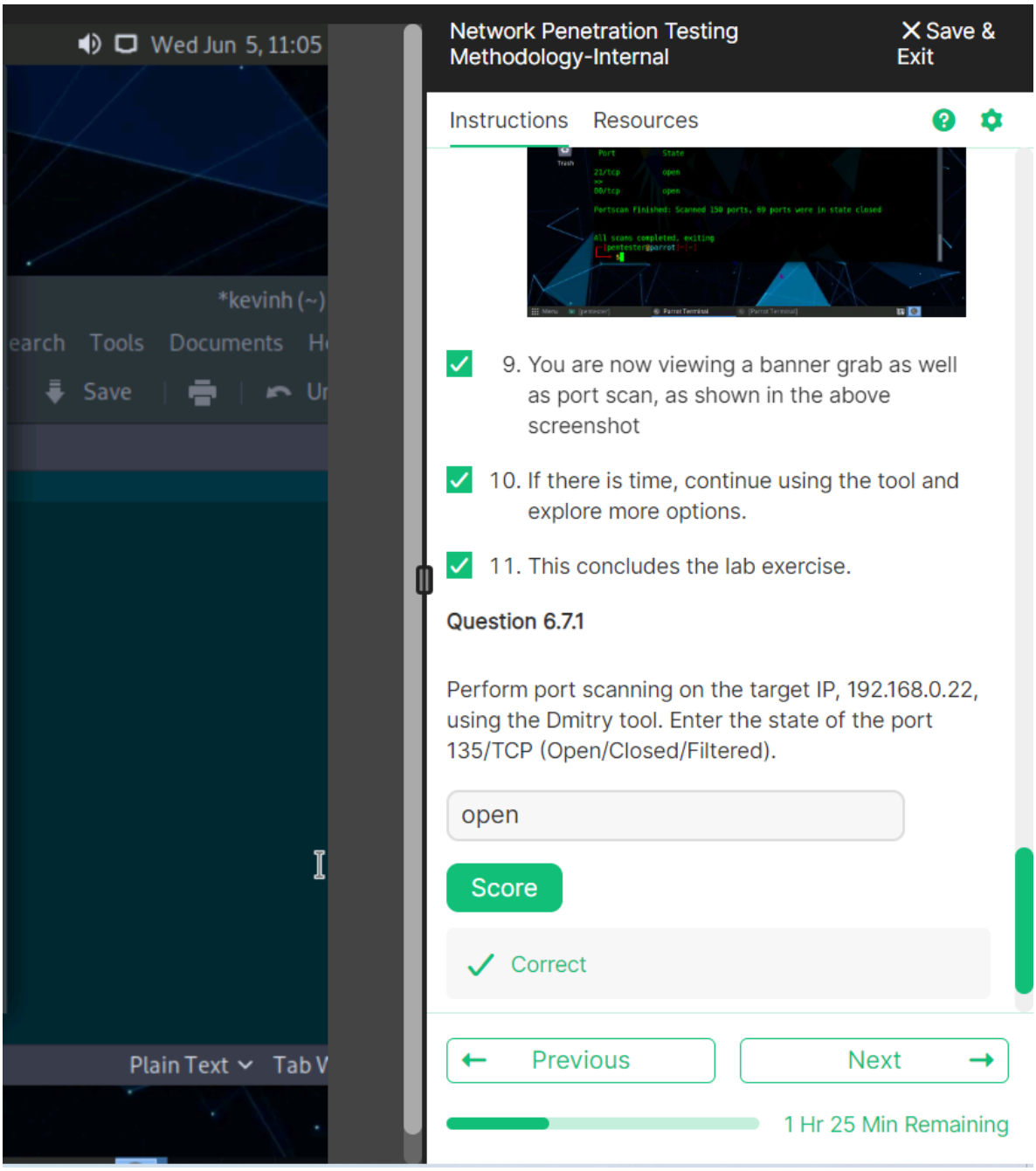
Exercise 7, Step 6: Open a terminal window and enter dmitry -pf 192.168.0.22, as shown in the screenshot



Exercise 7, Step 8: In the terminal window, enter dmitry -pb 192.168.0.22, as shown in the screenshot



7.2 QUESTIONS



Conclusion

In Conclusion, I have learned about how to leverage netdiscover to execute fingerprinting, hping3 to learn about the network communications that occur internally as well as any open ports. I also have learned how to leverage nmap for scanning more in depth as well as gaining insight to the database. I also have learned about Dmitry in relation to gaining insight on the ports that the organization has left open as well as how to leverage ftp to execute remote connections.