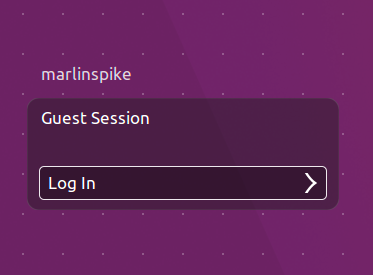
Basic Pentesting 1 is a box on vulnhub (<https://www.vulnhub.com/entry/basic-pentesting-1,216/>) created by Mr. Josiah Pierce. You can download it from: <https://download.vulnhub.com/basicpentesting/basic_pentesting_1.ova>

The Operating System our target machine uses is Ubuntu. We can see a user named *marlinspike.* Our motive here is to find the password of the user *marlinspike.*

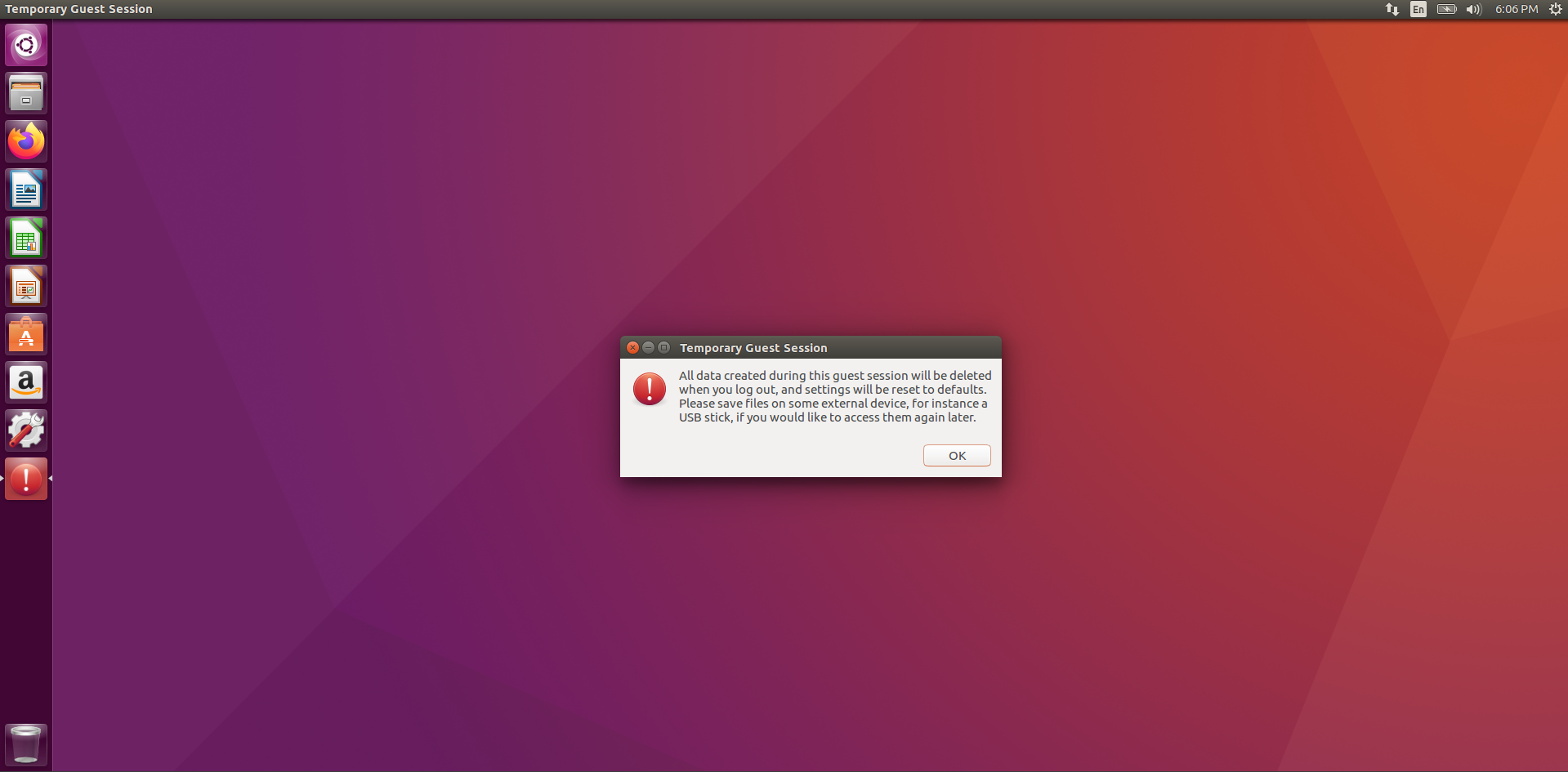


This is how we get the box.

We’ll login into the **guest** account to find the password of the user *marlinspike.* The guest account requires no password to login and can be taken access of.

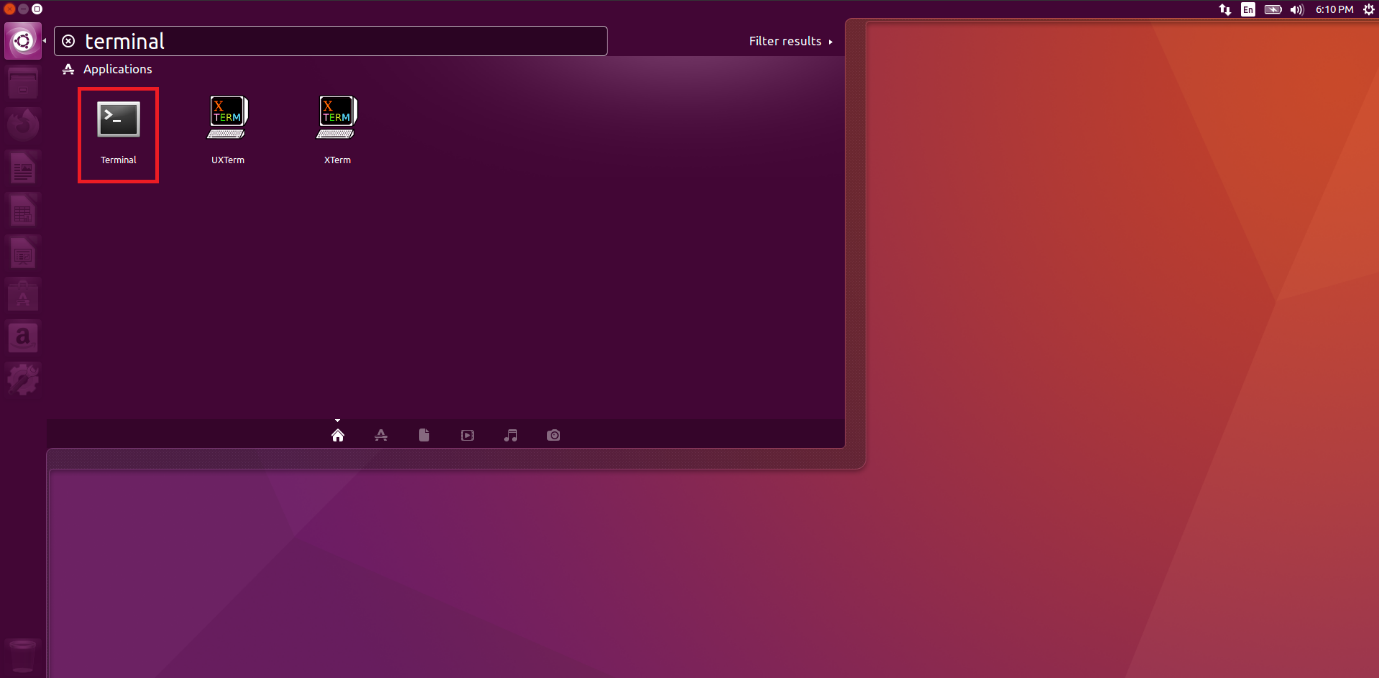


We can login from here.

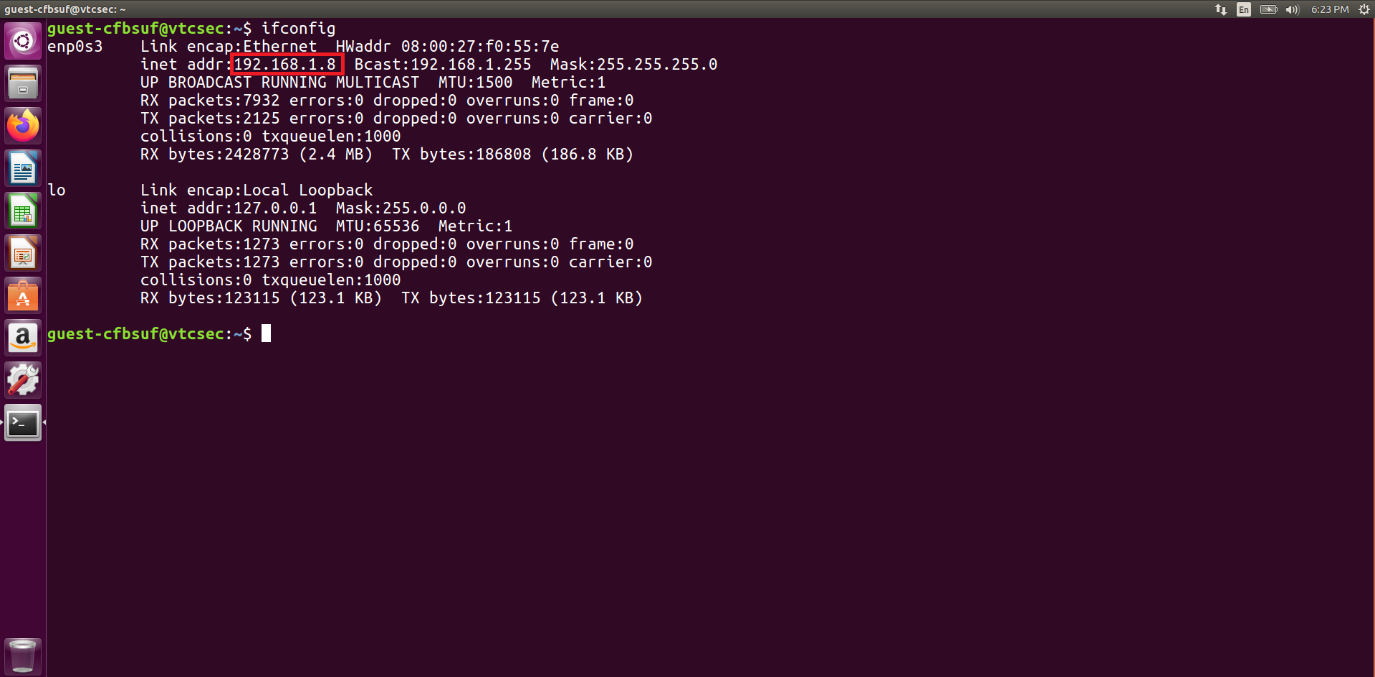


After we login, we can see a screen of the similar type with a pop-up which tells us that this is a temporary guest session whose contents will be deleted after we log-out of the account. We press *Ok* and move forward.

Next, we press the windows button on our keyboard and type – ***terminal****.* We can see the screen show us 3 options as in the below figure.



We will select the highlighted one and then type - ***ifconfig***in the terminal. The ***ifconfig*** command lists all the network adapters on the device and their present state. This command gives various information about the network devices. Here, we are mainly focused on retrieving the IP Address. This command also lists the MAC Address, IPv4, IPv6, names of the devices and other information. The output will look as such for us:

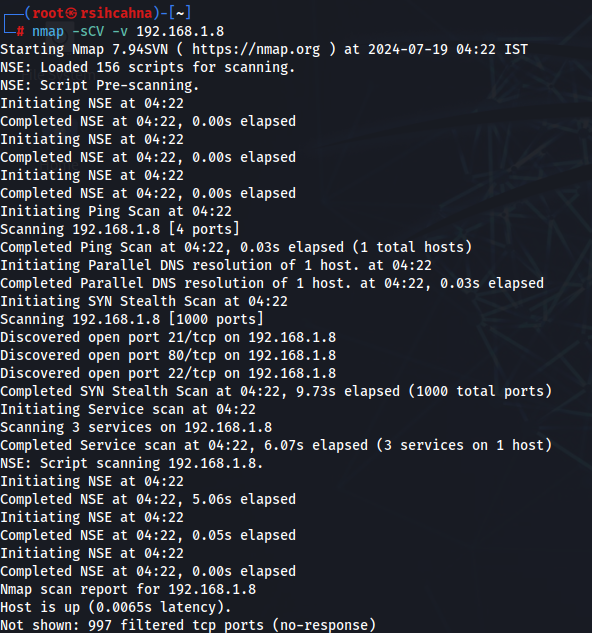


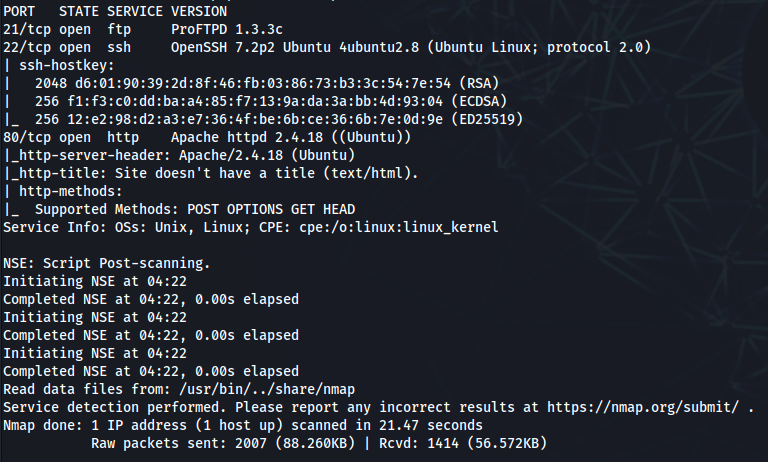
Here we find the address of our machine to be *192.168.1.8*

Now that we have the IP address of the machine, we can go and look for the services running on it from our Kali/Parrot machine.

We go ahead with a nmap scan using the switches -sC -sV and -v. [-sC -sV = -sCV]

The output of the above scan is underneath:

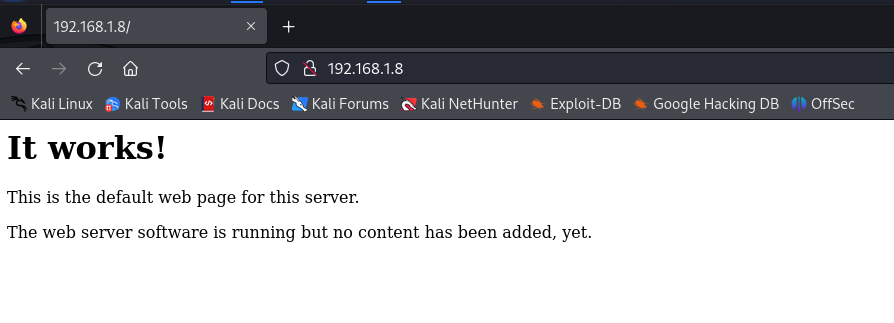




Here we can see 3 open ports – 21/tcp, 22/tcp and 80/tcp. We see that port 80 specifically is running a http service. Let’s check out what’s on the website! For this, we open up the firefox on our kali machine and type the IP Address and end it with a ‘:’ and 80 which redirects us to the specific port of the IP Address.



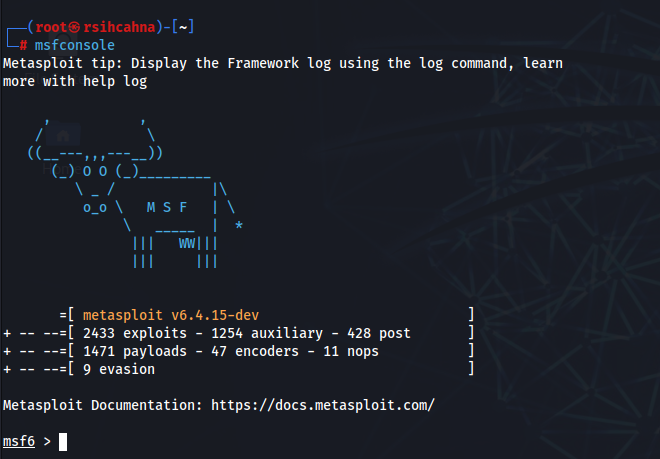
Unfortunately, we don’t see anything except for this:



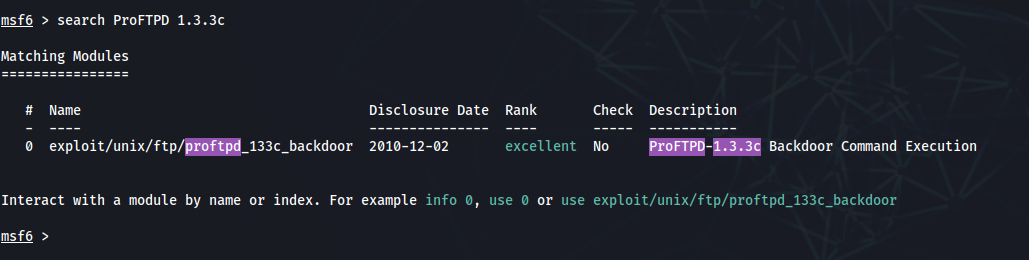
But it at least tells us the software is running but no content has been added yet. Which narrows our search area to the remaining 2 ports now, i.e., port 21 and 22.

On port 21, we see ProFTPD version 1.3.3c running. Let’s check if it is vulnerable. To check for vulnerabilities, we can either use ***searchsploit*** or ***Metasploit framework (msfconsole).*** In this walkthrough, we will be using ***msfconsole.***

Open up a new elevated terminal and type ***msfconsole*** to use the Metasploit Framework as shown below:

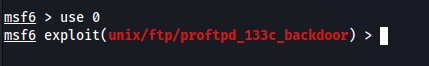


Now, we write the name of the service we can see on FTP, i.e., ProFTPD 1.3.3c with the keyword search as: ***search ProFTPD 1.3.3c***

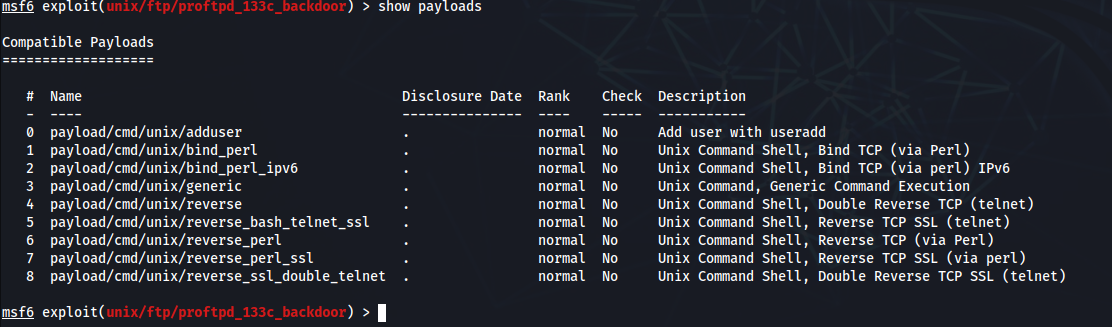


We found an exploit! Hence, we can try to move ahead with this one.

To use this exploit, we will type ***use 0*** which will then set this exploit to be used. Next, we need to set payloads. But we don’t know which payload to set so we’ll ask ***msf6*** to ***show payloads*** which will show us the compatible payloads that we can use.



Exploit has been set!



***show payloads*** shows us the following output. Now, we have to decide which one to use based on the exploit we have sent and the type of vulnerability we have.

For ProFTPD v1.3.3c, the vulnerability was that it allowed Backdoor Command Execution. Hence, the most appropriate payload to use is payload with # 4. But, since many a times, that might not work for some people like it did not work for me, hence, we will use the one above it; # 3.

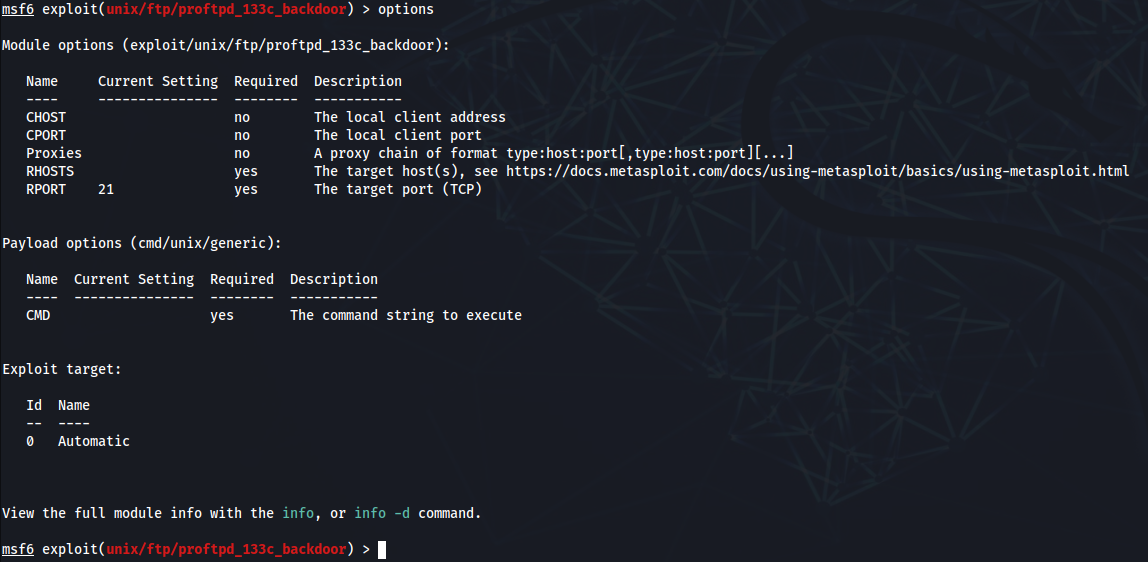
To set # 3 as the payload, we have 2 commands, any one will do the job. They are:

1. ***set payload 3***
2. ***set payload payload/cmd/unix/generic***

Any of the above commands set the payload we have chosen.



Payload has been set!

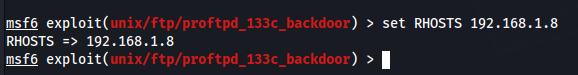
Now, we need to see the available options for the payload; to do so, we will type ***options.***

We can see that ***CHOST, CPORT, Proxies, RHOSTS, CMD*** have empty fields under ***Current Settings.***

Now, we will set only ***RHOSTS & CMD*** because they are the only ones which are ***Required*** (can be checked under the ***Required*** column)

***RHOSTS*** refers to the the IP of the target machine. So, to set the ***RHOSTS*** we type:

***set RHOSTS <target ip address>***

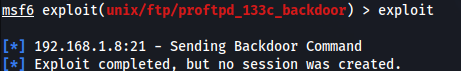


Now, we set the ***CMD*** option. ***CMD*** refers to the command we will be executing remotely. The command we will use is: ***set CMD python3 -m http.server 6789***



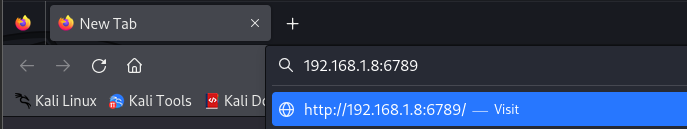
Using this command, we can start a temporary python server on the target which will allow us to access the directories of the Target machine using its IP on the port 6789.

Now that we have set the options for the Payload, lets exploit our target. We simply will use the command ***exploit.***

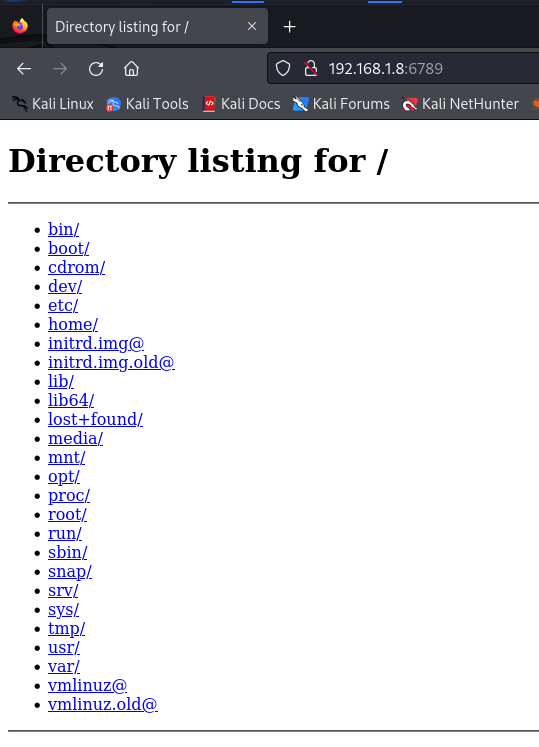


We get the above as the response of the above command.

You might think that we do not have a session which means that our attack failed, but this is where we don’t need the shell anymore! We have access to all the files and folders of the target machine without escalating any privileges! Just open the Mozilla Firefox browser on your kali machine and type: ***<target IP>:6789*** and press enter. This will allow you to see all the files and folders, directories and will be available for you to download on a single tap.

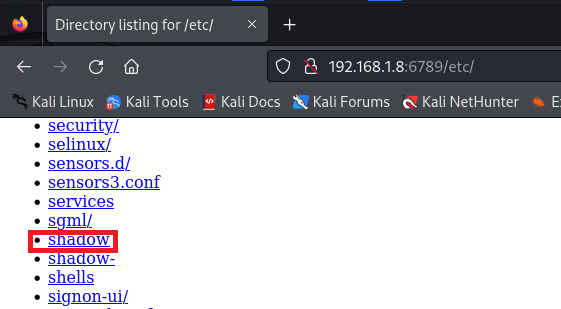


Press Enter!



The website we now have will look something like this. Now, to get the password of the user ***marlinspike*** is our actual motive. So how do we fulfil it from here?

Every OS saves passwords in a file for the users. For Linux based system, it is stored in etc/shadow file. Let us traverse there.



This is the file we are looking for. You might think, we have 2 shadow files, which one to download? Download the one without the ***–*** mark. Now that we have the file, lets open it.

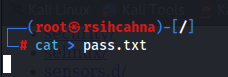
You will find many entries there, scroll down and you will find an entry with the name of ***marlinspike****.*It will look like this:



Now we have the user’s credentials, but it is all hashed. So how do we crack it? The passwords stored in Linux systems use ***sha512crypt*** hashing technique and to crack such hash, we will require the help of a tool named ***John The Ripper***.

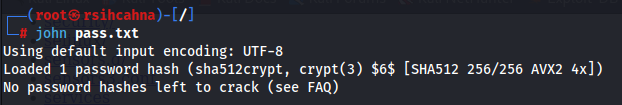
But before that, lets copy the whole sentence starting from m to the last colon.

After copying, open a new terminal and type: ***cat > pass.txt*** and press enter.



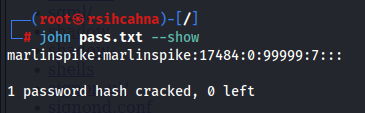
Now, paste the text you copied into it and again press enter! After you have pressed enter, use ***crtl+z***. This will save our text ad let us move out of the edit mode.

Now, type ***john pass.txt*** – This will make john hash the password of the file.

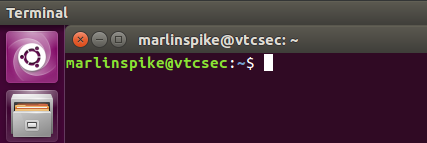


You will see such a prompt after running it.

Now use the command ***john pass.txt --show*** - This will reveal the hashed password of the user ***marlinspike***.



We can see that we do not have the gibberish anymore. The hashed password is ***marlinspike***. Now, to verify, let us use it to login into our Ubuntu! Logout from Guest user and type the password for ***marlinspike***. You will find that we can login into the system now. You can open the terminal to verify it.



We have logged into the user ***marlinspike*** without using any terminal or shell to hack into the system.