X Project 3: Penetration Testing in a Lab



© Goal

Simulate a penetration test against a vulnerable machine in a safe lab environment, then document the findings in a professional pentest report.

You'll show you can:

- Use common pentesting tools (Nmap, Nikto, Hydra, Metasploit)
- Follow a structured methodology
- Document vulnerabilities and mitigation steps

Setup

- **Attacker VM** → Kali Linux
- **Target VM** → Metasploitable 2 or DVWA (Damn Vulnerable Web App on Ubuntu)
- Network → Host-only/bridged so Kali can reach the victim



Step 1: Reconnaissance & Scanning

From Kali, scan the victim:

nmap -A <victim-ip>

- Identify open ports, running services, OS details.
- Example findings:
 - o Port 22 (SSH) open
 - o Port 80 (HTTP, Apache) open
 - o Port 3306 (MySQL) open

Take a screenshot of Nmap output.



🔙 Step 2: Web Vulnerability Scanning

If port 80 is open:

nikto -h http://<victim-ip>

- Detect outdated Apache, default files, XSS, SQL injection possibilities.
- Take screenshots of results.



Step 3: Brute Force Login Attempt

Try brute forcing SSH or web login:

hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://<victim-ip>

If using DVWA (web app):

- Login with admin:password (default creds).
- Test SQL Injection: in login field \rightarrow 'OR '1'='1
- **a** Take screenshots of login attempts.

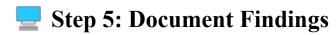


Step 4: Exploitation (Metasploit)

Example: Exploit a vulnerable service.

msfconsole search vsftpd use exploit/unix/ftp/vsftpd 234 backdoor set RHOSTS <victim-ip> run

- If successful → you get a shell on the victim.
- Screenshot the shell session.



Create a **Penetration Test Report**. Structure:

Executive Summary

- Scope: Internal penetration test on vulnerable VM.
- Objective: Identify and exploit security flaws.

Methodology

- 1. Recon (Nmap)
- 2. Scanning (Nikto)
- 3. Exploitation (Hydra, Metasploit)

Findings (Example)

- Vulnerability: Weak SSH Passwords
 - o Evidence: Hydra cracked admin: 123456
 - o **Impact:** Unauthorized remote access
 - o **Remediation:** Enforce password complexity, enable MFA
- Vulnerability: SQL Injection (DVWA)
 - o Evidence: Login bypassed using 'OR '1'='1
 - o **Impact:** Full database access possible
 - o **Remediation:** Use prepared statements, sanitize inputs

Conclusion

- System is vulnerable to multiple attacks.
- Recommend patching, monitoring, and security awareness training.

Deliverables for Portfolio

- Pentest Report PDF (with findings, CVEs, screenshots, remediation)
- Screenshots (Nmap, Nikto, Hydra, Metasploit, exploited shell)
- GitHub Repo Folder:
- project3-pentest/
- pentest-report.pdf
- screenshots/
 - methodology.md