🔐 Penetration Testing 1 Final Project Documentation

Title: Professional Penetration Testing Project
Based on Standards: PTES / OSSTMM

📘 1. Understanding the Methodology

Choose one of the following industry-standard methods:

🔸 PTES (Penetration Testing Execution Standard):

7 Phases:

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

🔸 OSSTMM (Open Source Security Testing Methodology Manual):

- Focuses on testing operational security of networks, systems, processes, and physical infrastructure
- Organized into areas like Information, Process, Internet, Wireless, Communications, and Physical Security

📌 **For this project, we'll use PTES for clarity and ease.**

🧾 2. Create a Detailed Test Plan

🗂️ Include the following sections:

A. Scope Definition

- **What will you test?**
  - **e.g., “A local web server running Apache and a login page”**
- **What’s not included?**
  - **e.g., “No testing on third-party APIs or physical devices”**

B. Objectives

- **What are you trying to achieve?**
  - **Find vulnerabilities, test authentication, evaluate password security**

C. Timeline

Phase	Duration
Pre-engagement	1 day
Scanning/Recon	2 days
Exploitation	2 days
Post-exploitation	1 day
Reporting	1 day

D. Deliverables

- **Test plan**
- **Vulnerability report**
- **Risk analysis**
- **Recommendations**

🧰 3. Configure Testing Environment

Set Up a Safe Lab:

- **Use VirtualBox or VMware**
- **Machines:**
  - **Attacker Machine: Kali Linux**
  - **Target Machine: Metasploitable 2 / DVWA / TryHackMe lab**

Install Tools:

- Recon: Nmap, Whois, Dig
- Exploitation: Metasploit, Hydra
- Web Testing: Burp Suite, Nikto
- Traffic Monitoring: Wireshark
- Brute-force Testing: John the Ripper

Document Configuration:

- List VMs used
- Network setup: "NAT / Host-Only"
- IP addresses of each machine
- Screenshot of setup

📄 4. Sample Engagement Using Standard Templates

Use this structure to conduct your sample pen test:

A. Pre-Engagement

- Fill out Authorization Form (sample below)
- Scope Agreement (what's allowed, what isn't)
- Rules of Engagement (e.g., test during certain hours only)

B. Intelligence Gathering

- Use Nmap: `nmap -A <target IP>`
- Record open ports and services
- Example output and analysis

C. Vulnerability Analysis

- Use Nikto or Nessus
- Identify vulnerabilities like outdated software, open login panels

D. Exploitation

- Use Metasploit to exploit a known vulnerability
- Document steps and results
- Screenshot of shell access or credential theft

E. Post-Exploitation

- What can you do now?

  - Check files, steal hashes, escalate privileges
- Make note of any sensitive data accessed

F. Reporting

- Write a short executive summary
- Include screenshots and vulnerability findings
- Risk level: High / Medium / Low
- Recommendations: Patching, encryption, stronger passwords

📝 5. Required Documentation Templates

✅ Authorization Form (Sample)

markdown
CopyEdit

```
Penetration Testing Authorization Form
-------------------------------------
Client: School Cybersecurity Lab
Tester: [Your Name]
Scope: 192.168.1.100 (Metasploitable VM)
Start Date: March 20, 2025
End Date: March 22, 2025
Authorized Activities:
- Port scanning
- Web app testing
- Exploitation of known services
Signature: ____________________
```

✅ Scope Agreement (Sample)

sql
CopyEdit

```
Scope:
- Included: Web server, login system
- Excluded: Physical devices, external IPs

Testing Boundaries:
```

```
- Testing must only occur within lab network
- No denial-of-service (DoS) testing allowed
```

✅ Rules of Engagement (Sample)

- **Testing Time: 9 AM – 4 PM**
- **No harm to data**
- **Reporting required for any critical vulnerability**

📎 Final Submission Package Should Include:

File	Description
`Test_Plan.pdf`	**Scope, objectives, timeline, deliverables**
`Lab_Setup.pdf`	**Screenshots of Kali & target VMs**
`Scan_Results.txt`	**Nmap, Nikto, or Nessus results**
`Exploitation_Report.pdf`	**Steps taken, results, screenshots**
`Risk_Report.pdf`	**Risk levels and recommendations**
`Authorization_Forms.pdf`	**Scope, consent, testing rules**