

PENETRATION TESTING LAB FROM RECONNAISSANCE TO PRIVILEGE ESCALATION

This document is designed to help you transition from the **lecture content** into the **hands-on lab session**. It outlines what you will be doing, what is expected, and how to prepare so you can approach the lab with confidence.

1. Connection to Your Lectures

In the lectures, you covered the **core concepts of penetration testing**, including:

- The **MITRE ATT&CK framework** (attack lifecycle)
- **Metasploit Framework** (structure, modules, terminology)
- Key phases of an attack:
 - Reconnaissance
 - Scanning & Enumeration
 - Exploitation
 - Post-Exploitation
 - Lateral Movement
 - Privilege Escalation

In this lab, you will apply all of these concepts practically in a controlled environment.

2. Lab Overview (What You Will Do)

You will simulate a real-world penetration testing scenario using virtual machines.

Systems Used

- Kali Linux (attacker machine)
- Metasploitable / Ubuntu server (target)
- Windows / OWASP vulnerable apps

3: Lab Activities (With Page References)

Phase 1: Setup & Environment Preparation

- p.6–8 → Tool setup (Nessus, database, workspace)
- Start all required virtual machines
- Open terminal on Kali Linux
- Launch Metasploit:

```
msfconsole
```

Phase 2: Reconnaissance

You will gather information about the target system.

Tasks:

- p.9–13 → DNS enumeration & MITRE recon phase
- Perform DNS queries (`dig`)
- Identify domains, IPs, and subdomains

Example:

```
dig A <target>
```

```
dig MX <target>
```

Metasploit DNS:

```
use auxiliary/gather/enum_dns
```

```
set DOMAIN <target>
```

```
run
```

Phase 3: Scanning

You will identify open ports and services.

Tasks:

- p.13–17 → Nmap scanning techniques

- Run Nmap scans:

```
nmap -sS <target>
```

```
nmap -sV <target>
```

```
nmap -O <target>
```

Goal: Discover:

- Open ports
- Running services
- Operating system

Phase 4: Enumeration

You will gather detailed information about services.

Tasks:

- **p.15–20** → Port scanning, service enumeration
- Use Metasploit auxiliary modules:

```
use auxiliary/scanner/ssh/ssh_version
```

```
use auxiliary/scanner/http/http_version
```

```
use auxiliary/scanner/ftp/ftp_version
```

Goal: Identify vulnerabilities and weak points

Phase 5: Exploitation

You will attempt to gain access to the system.

Tasks:

- **p.21–25** → Exploiting ProFTPD & Java RMI
- Search and run exploits:

```
search proftpd
```

```
use exploit/unix/ftp/proftpd_modcopy_exec
```

```
run
```

- Verify access:

```
whoami
```

```
shell
```

Goal: Obtain a shell (initial access)

Phase 6: Web Exploitation (XSS & OWASP)

You will perform client-side attacks.

Tasks:

- p.25–27 → XSS + BeEF + OWASP
- Test for XSS vulnerabilities
- Use BeEF to hook a browser

```
http://target/search.jsp?q=<script>alert('XSS')</script>
```

Goal:

- Control browser sessions
- Capture user actions and data

Phase 7: Post-Exploitation

You will explore the compromised system.

Tasks:

- p.28–32 → Post modules & system enumeration
- Run post modules:

```
use post/linux/gather/enum_configs
```

```
use post/linux/gather/enum_users_history
```

Goal:

- Collect system data
- Identify further attack paths

Phase 8: Credential & Data Extraction

Lab Pages:

- p.33–34 → Browser data, passwords, cookies

Tasks:

```
cd ~/.mozilla/firefox  
sqlite3 places.sqlite
```

Goal:

- Extract stored credentials
- Analyse user data

Phase 9: Lateral Movement

You will move to other systems in the network.

Tasks:

- p.35–36 → Internal network movement
- Attempt SSH access using credentials
- Scan internal network:

```
nmap 192.168.x.x/24  
ssh user@target
```

Goal: Expand access across machines

Phase 10: Privilege Escalation

You will attempt to gain higher privileges.

Tasks:

- p. 37+ → Internal network movement
- Check system files:

```
cat /etc/shadow
```

- Try privilege escalation techniques

Goal: Become root/admin

4. Preparation before the Lab

Make sure you:

- Have all virtual machines installed and working
- Can run Kali Linux terminal commands
- Understand basic Linux commands (`cd`, `ls`, etc.)
- Review lecture slides (especially attack lifecycle)

5. Tips for Success

- Follow the attack phases in order
- Take notes during the lab
- Don't rush—understand each step
- If something fails, troubleshoot (this is normal!)

Final Takeaway

This lab is your opportunity to **turn theory into practice**.

By the end, you should be able to:

- Perform a full penetration testing workflow
- Use real tools like Metasploit and Nmap
- Understand how attackers move through systems