# Chapter 2: Penetration Testing & Red Teaming

## 📘 Description

This chapter focuses on advanced techniques for penetration testing (ethical hacking) and red teaming. You'll learn how security professionals simulate real-world attacks to uncover vulnerabilities, improve defenses, and assess an organization's readiness.

## 🎯 Learning Objectives

By the end of this chapter, you will be able to:

- Understand the phases of a penetration test
- Differentiate between penetration testing and red teaming
- Apply frameworks like OSSTMM and MITRE ATT&CK
- Use professional tools to simulate advanced attacks
- Write a professional pentest report

## ⚙️ Section 1: Penetration Testing vs. Red Teaming

| Aspect | Penetration Testing | Red Teaming |
|---|---|---|
| **Goal** | Find and exploit vulnerabilities | Simulate real-world attack scenarios |
| **Scope** | Limited to defined systems | Broader and goal-based (e.g., access sensitive data) |
| **Timeframe** | Short-term (1–3 weeks) | Long-term (months) |

| | | |
|---|---|---|
| **Approach** | Known vulnerabilities, automated tools | Covert operations, manual tactics |

---

# 🧭 Section 2: Phases of a Penetration Test

1. **Reconnaissance**
    - Passive (WHOIS, Google, LinkedIn)
    - Active (port scanning, banner grabbing)
2. **Scanning & Enumeration**
    - Identify live hosts, open ports, services
    - Nmap, Nessus, Nikto
3. **Exploitation**
    - Gaining unauthorized access
    - Tools: Metasploit, SQLMap, Hydra
4. **Post-Exploitation**
    - Privilege escalation, pivoting
    - Data exfiltration, lateral movement
5. **Reporting**
    - Document findings, risk levels, proof-of-concepts
    - Include recommendations and remediation

---

# 🧪 Section 3: Key Tools and Frameworks

## 🔧 Tools

- **Nmap** – Network scanner
- **Burp Suite** – Web application security
- **Metasploit Framework** – Exploit development and execution
- **Nessus/OpenVAS** – Vulnerability scanners
- **Cobalt Strike** – Advanced red teaming tool

### 🧠 Frameworks

- **OSSTMM (Open Source Security Testing Methodology Manual)**
- **PTES (Penetration Testing Execution Standard)**
- **MITRE ATT&CK** – Tactics, techniques, and procedures (TTPs)

---

## 🧠 Section 4: Social Engineering in Red Teaming

- **Phishing simulations**
- **Pretexting and impersonation**
- **USB drop attacks**
- **Physical security tests** (e.g., tailgating, lockpicking)

---

## 📄 Section 5: Crafting a Professional Report

**Should Include:**

- Executive Summary (non-technical)
- Scope, methodology, tools used

- List of findings with risk ratings (CVSS)
- Screenshots or logs as evidence
- Clear recommendations and timelines

---

## ✅ Chapter Summary

- Penetration testing identifies and exploits security weaknesses to strengthen defenses.
- Red teaming simulates realistic attack scenarios to test overall security posture.
- Tools like Nmap, Burp Suite, and Metasploit are essential in offensive security.
- Comprehensive reporting is crucial for remediation and compliance.