Penetration Testing Project Plan

Methodology: PTES (Penetration Testing Execution Standard)

---

1. Pre-Engagement Interactions

a. Authorization and Legal Documents

- Non-Disclosure Agreement (NDA)
- Rules of Engagement (RoE)
- Signed Authorization Letter
- Risk Acceptance Acknowledgment
- Scope Agreement Form

b. Scope Definition

- **Target IP Ranges:** 192.168.1.0/24, 10.0.0.0/24
- **Web Applications:** `example.com`, `admin.example.com`
- **Network Segments:** Internal LAN, DMZ
- **In-Scope Systems:** Web servers, internal services, employee portal
- **Out-of-Scope:** HR database, unsupported legacy systems, production financial systems (unless explicitly approved)

c. Objectives

- Identify vulnerabilities across web and internal assets
- Exploit weaknesses in a controlled, safe environment
- Provide mitigation and remediation advice
- Assess organization's detection and response capabilities
- Ensure all findings are clearly documented and reproducible

d. Timeline

Phase	Duration
Planning & Authorization	2 days
Intelligence Gathering	1 day
Vulnerability Scanning	2 days
Exploitation	2 days

Post-Exploitation	1 day
Reporting	2 days

e. Deliverables

- Signed Authorization and Scope Documents
- Executive Summary (Non-Technical)
- Detailed Technical Report
- Vulnerability Risk Ratings
- Screenshots, Logs, and PoCs
- Remediation and Mitigation Recommendations
- File Integrity Report

---

2. Intelligence Gathering

- **Tools:** `whois`, `nslookup`, `theHarvester`, `Recon-ng`, `Shodan`, Google Dorking
- **Goals:**
  - Identify subdomains and email addresses
  - Gather DNS records and IP ranges
  - OSINT on employees and infrastructure
  - Search for leaked credentials or breach data

---

3. Threat Modeling

- **Assets Identified:** Customer data, employee portal, internal documentation
- **Threat Actors:** Script kiddies, insiders, APT groups
- **Attack Vectors:** Web entry points, phishing simulation, network ports

---

4. Vulnerability Analysis

- **Tools:** `Nmap`, `Nessus`, `Nikto`, `OpenVAS`, `Burp Suite`, `OWASP ZAP`
- **Steps:**
  - Perform service enumeration
  - Scan for CVEs, weak configs, default creds
  - Confirm findings manually
  - Document vulnerabilities with screenshots and severity

---

5. Exploitation

- **Tools:** `Metasploit`, `SQLmap`, `Burp Suite`, `Hydra`, custom payloads
- **Process:**
  - Exploit validated vulnerabilities
  - Avoid causing DoS or system instability
  - Document entry vectors and success rate
  - Demonstrate privilege escalation

---

6. Post-Exploitation

- **Tools:** `Mimikatz`, `netcat`, `PowerShell`, `CrackMapExec`, `Impacket`
- **Actions:**
  - Gather password hashes and credentials
  - Maintain access (with permission)
  - Simulate data exfiltration scenarios
  - Demonstrate lateral movement and pivoting
  - Create timeline of compromise for Blue Team correlation

---

7. Reporting

- **Executive Summary:**
  - Non-technical overview of risks and business impact
- **Technical Report:**
  - Detailed methods, tools, findings, timelines
  - Step-by-step PoCs with screenshots
  - CVEs, CVSS scores, and mapped OWASP Top 10 categories
- **Recommendations:**
  - Fixes by priority (high, medium, low)
  - Short- and long-term remediation plans
- **Supporting Data:**
  - Network diagrams, scan results, logs
  - Integrity verification data using HMAC

---

8. Testing Environment Setup

- **Virtual Lab Environment:**
  - Kali Linux (attacker)

    - Metasploitable 2 & 3 (target systems)
    - DVWA, OWASP Juice Shop
    - Windows Server AD VM (for internal escalation tests)
- **Networking:**
    - Isolated environment via VirtualBox or VMware
    - VPN configured for remote access (if applicable)
- **Tools Included:**
    - `Wireshark`, `tcpdump`, `Burp Suite`, `John the Ripper`, `Hashcat`

---

9. Sample Engagement Summary (Redacted)

- **Client:** ABC Corp
- **Scope:** 192.168.50.0/24, `client-portal.abccorp.com`
- **Objectives:** Test internal network and web app defenses
- **Key Findings:**
    - SQL Injection in login form
    - RCE on internal server
    - Lateral movement via open SMB shares
    - Exfiltration of 200+ sensitive documents (simulated)
- **Remediation:**
    - Implement input validation and WAF
    - Patch vulnerable services
    - Enforce strong password policies
    - Segment internal network and enable monitoring