Penetration Testing Methodology

1. Introduction This document outlines a professional penetration testing engagement, following industry standards such as the Penetration Testing Execution Standard (PTES) and the Open Source Security Testing Methodology Manual (OSSTMM). The objective is to assess the security posture of a target environment through an authorized and structured approach.

2. Scope Definition

- **Targets:** Define IP ranges, domain names, applications, and systems to be tested
- **Exclusions:** List any systems or segments excluded from testing
- **Testing Type:** Specify the nature of testing (e.g., external, internal, web application, wireless, physical, social engineering)
- **Stakeholders:** Identify key personnel responsible for the engagement and decision-making

3. Objectives

- Identify vulnerabilities and assess potential exploitation
- Evaluate the effectiveness of current security measures
- Simulate real-world attack scenarios
- Provide actionable security recommendations

4. Timeline

- **Planning & Scoping:** Define the planning period
- **Reconnaissance & Scanning:** Outline the initial discovery phase
- **Exploitation:** Allocate time for testing identified vulnerabilities
- **Post-Exploitation & Reporting:** Set deadlines for analysis and documentation

5. Deliverables

- Pre-engagement documentation (authorization, scope agreement)
- Penetration test plan
- Detailed technical report with findings and risk analysis
- Remediation and mitigation recommendations
- Executive summary tailored to a non-technical audience

6. Testing Environment Configuration

- Use a controlled, isolated environment or test against authorized live systems
- Maintain detailed logs and records of tool configurations and testing procedures

7. Methodology

- **Pre-engagement Interactions:** Confirm goals, obtain authorization, define rules of engagement
- **Information Gathering:** Conduct passive and active reconnaissance using tools like:
    - WHOIS, nslookup, and Shodan for passive recon
    - Nmap for active network scanning
- **Threat Modeling:** Identify valuable assets and potential threat vectors
- **Vulnerability Analysis:** Utilize vulnerability scanners and manual testing:
    - Nessus for identifying known vulnerabilities
    - Burp Suite for web application testing
- **Exploitation:** Demonstrate risk using controlled exploitation:
    - Metasploit Framework for exploit delivery
    - Hydra brute-force attacks
- **Post-Exploitation:** Assess impact and perform privilege escalation or data extraction
    - Mimikatz for credential harvesting
    - BloodHound for Active Directory enumeration
- **Reporting:** Document findings, assign severity ratings, and provide clear remediation guidance

8. Documentation and Legal Compliance

- Ensure all parties sign an authorization to test
- Define and agree on scope and rules of engagement
- Document all actions taken during the test
- Establish clear boundaries to prevent unintended disruption

9. Sample Engagement Overview

- **Target:** Define the general system(s) or environment being tested
- **Scope:** Broadly describe the areas covered (e.g., internal network, web applications)
- **Tools Used:**
    - **Reconnaissance:** WHOIS, nslookup, Shodan
    - **Scanning:** Nmap
    - **Vulnerability Assessment:** Nessus, OpenVAS
    - **Exploitation:** Metasploit
    - **Web Testing:** Burp Suite, OWASP ZAP
    - **Post-Exploitation:** BloodHound
- **Summary of Findings:** General overview of types of vulnerabilities commonly found
- **Remediation Actions:** Standard best practices to address identified issues

10. Conclusion This methodology ensures a professional and ethical approach to penetration testing, aligned with recognized industry standards. It aims to uncover and help remediate vulnerabilities, improving the overall security posture of the target environment.