Penetration Testing Template

Penetration Testing Template/
├── Engagement Overview
├── Information Gathering
├── Exploitation
├── Post-Exploitation
├── Reporting
├── Additional Notes
└── Signature

Engagement Overview

Purpose:
Provide a high-level description of the engagement, including scope, objectives, and methodologies.

• **Target Description:** [IP addresses, systems, domains, network ranges]

• **Scope**:

◇ In-Scope: [List All the systems, IP addresses, applications, services etc. that are allowed in this test]

◇ Out-of-Scope: [List all the systems, IP addresses, applications, services, and network segments that must not be tested or interfered with]

• **Testing Type**:[Explain the type of testing being performed:**Black Box, Grey Box, White Box**]

• **Duration**: [Clearly state the start and end dates of the engagement.]

• **Tools Used**: [Provide a list of all tools used during the assessment]

• **Authorization**:

Information Gathering

Purpose:
Provide a high-level description of the engagement, including scope, objectives, and methodologies.

• **Passive Reconnaissance:** [Gathering information without interacting directly with the target (e.g., WHOIS lookups, DNS records, Google dorking)]

• **Active Reconnaissance:** [Directly interacting with the target to gather information (e.g., Nmap scans, OS fingerprinting, service detection).]

• **Network Mapping:** [Documenting network topology, subnets, devices, services, and their relationships.]

• **Open Ports & Services:** [Detailed results of port scanning and service enumeration.]

• **Vulnerabilities Identified (Initial):** [Preliminary list of potential attack vectors discovered during scanning.]

Screenshots

Screenshots to Include:

◇ Nmap scan results.

◇ WHOIS lookups.

◇ Open Ports & Services identification.

◇ OS detection outputs.

◇ Network topology diagrams (if applicable).

Exploitation

Purpose:
Exploit identified vulnerabilities to gain access to systems.

• **Exploits Used:** [Detailed description of the tools, scripts, or techniques used (e.g., Metasploit modules, custom scripts, manual exploitation).]

• **Vulnerabilities Exploited:** [Clearly describe the vulnerabilities targeted, including CVE IDs, CWE IDs, or misconfigurations.]

• **Proof of Concept:** [Provide screenshots, command outputs, files, or logs that demonstrate successful exploitation.]

• **Privilege Escalation:** [Document steps taken to escalate privileges if applicable.]

• **Mitigation Bypass:** [Describe techniques used to bypass firewalls, IDS/IPS, WAFs, etc.]

Screenshots

Screenshots to Include:

◇ Successful exploitation commands.

◇ Proof of access (e.g., shell access, web shell interface, RCE).

◇ Evidence of exploited vulnerabilities (e.g., Metasploit output, manual exploitation results).

◇ Privilege escalation results.

Post-Exploitation

Purpose:
Document actions taken after successful exploitation to maintain access and gather information.

• **Maintaining Access:** [Techniques used to create backdoors, new user accounts, or persistence mechanisms.]

• **Data Exfiltration:** [Evidence of data extraction or proof of capability to extract data.]

• **Lateral Movement:** [Document methods used to move between systems within the network.]

• **Cleanup:** [Steps taken to remove logs, indicators of compromise, or artifacts left behind.]

• **Impact Analysis:** [Assessment of potential damage or impact from the exploitation.]

Screenshots

Screenshots to Include:

◇ Created backdoors or persistence mechanisms.

◇ Exfiltrated data or files (evidence of data access).

◇ Lateral movement techniques (if applicable).

◇ Proof of cleanup (e.g., deleted logs, removed artifacts).

Reporting

Purpose:
Provide a formal report detailing the findings, impact analysis, and remediation recommendations.

• **Executive Summary:** [High-level overview of the assessment, suitable for non-technical stakeholders.]

• **Technical Findings:** Detailed description of all vulnerabilities discovered, including:

▪ **Vulnerability Name**

▪ **Severity Level:** Critical, High, Medium, Low.

▪ **Description:** Explanation of the vulnerability, including how it was found and why it is a problem.

▪ **Evidence:** Proof of concept including screenshots, logs, or commands showing exploitation.

▪ **Remediation Recommendations:** Clear steps to fix the issue and prevent future exploitation.

▪ **References:** CVE IDs, CWE IDs, or links to further reading and best practices.

• **Impact Analysis:** [Explanation of the potential damage if the vulnerabilities were exploited.]

• **Conclusion:** [Summary of the overall assessment and key takeaways.]

Screenshots

Screenshots to Include:

◇ Vulnerability evidence with corresponding severity ratings.

◇ Proof of concept images (e.g., login screens bypassed, unauthorized access interfaces).

◇ Visual representation of impact or compromised data.

◇ Remediation testing results (if applicable).

Additional Notes

Purpose:
Record any additional observations or findings that do not fit into the structured sections above.

Observations/Findings:

Signature

Tester Name:
Date: [Date of Completion]
Signature: