Penetration Testing Checklist

- 1. Pre-Engagement (Planning & Scoping)

[ ] Define goals and scope (e.g., external, internal, web app, social engineering).

[ ] Identify authorized targets and limitations (IP ranges, systems, etc.).

[ ] Sign rules of engagement and legal agreements (NDA, contract).

[ ] Agree on testing methods (black-box, gray-box, white-box).

[ ] Schedule testing and define communication protocols.

- 2. Reconnaissance (Information Gathering)

Passive Recon:

[ ] WHOIS information, DNS records.

[ ] Publicly available data (OSINT): LinkedIn, social media, job postings.

[ ] Email harvesting (e.g., Hunter.io).

[ ] Google dorking.

[ ] Leaked credentials (e.g., HaveIBeenPwned).

Active Recon:

[ ] Port scanning (Nmap).

[ ] Service enumeration (e.g., banners, versions).

[ ] Subdomain enumeration (Sublist3r, Amass).

[ ] Detect firewalls, WAFs, IDS/IPS.

[ ] Identify operating systems and technologies.

- 3. Vulnerability Analysis

[ ] Automated vulnerability scanning (e.g., Nessus, OpenVAS, Nikto).

[ ] Manual verification of findings.

[ ] Identify misconfigurations, unpatched systems, outdated software.

[ ] Cross-reference with CVE databases and exploit repositories (Exploit-DB, NVD).

- 4. Exploitation

[ ] Exploit vulnerabilities to gain access (Metasploit, custom scripts).

[ ] Privilege escalation (local exploits, misconfigurations).

Penetration Testing Checklist

[ ] Bypass authentication mechanisms.

[ ] Exploit web vulnerabilities (e.g., SQLi, XSS, LFI/RFI).

[ ] Exploit misconfigured cloud storage, containers, etc.

- 5. Post-Exploitation

[ ] Maintain access (e.g., reverse shells, backdoors).

[ ] Dump credentials (Mimikatz, LSASS dump).

[ ] Pivot and move laterally within the network.

[ ] Data exfiltration (without causing damage).

[ ] Collect evidence: screenshots, logs, hashes.

- 6. Cleanup

[ ] Remove payloads, shells, users, backdoors.

[ ] Restore any changed settings (if applicable).

[ ] Inform client of any leftover artifacts.

[ ] Verify system stability.

- 7. Reporting

[ ] Executive summary (non-technical overview).

[ ] Technical details of findings (steps, evidence, risk level).

[ ] Proof of concepts (screenshots, logs, code).

[ ] Remediation recommendations.

[ ] Risk rating (CVSS or custom scoring).

[ ] Final debrief meeting with client.

- 8. Remediation Testing (Optional)

[ ] Re-test fixed vulnerabilities.

[ ] Confirm patches and configuration changes.

[ ] Validate that the system is now secure.