FULL PENETRATION TESTING CHECKLIST

-By Alham Rizvi

1. Pre-Engagement & Authorization

□ Written permission obtained
□ Scope clearly defined
□ Out-of-scope assets documented
□ Test type defined (Black / Grey / White)
□ Allowed attack techniques approved
□ DoS restrictions agreed
□ Social engineering allowed / excluded
□ Cloud provider approval obtained
□ Emergency contact identified
□ Data handling rules defined

2. Asset Discovery & Mapping

□ Live hosts identified
□ Network ranges mapped
□ External assets identified
□ Internal assets identified
□ Critical systems identified
□ Third-party integrations identified
□ Legacy systems identified
□ Admin & management interfaces identified

3. Reconnaissance

Passive Recon

□ Domain enumeration
□ Subdomain enumeration
□ DNS records analyzed
□ IP & ASN ownership identified
□ Technology stack fingerprinted
□ Public document metadata reviewed
□ Employee naming patterns identified
□ Email format identified
□ Breach exposure checked
□ Public repositories reviewed
□ Cloud storage exposure checked

Active Recon

- □ Host discovery completed
- □ TCP port scan completed
- □ UDP port scan completed
- □ Services identified
- □ Service versions identified
- □ OS fingerprinting completed
- □ SSL/TLS configuration reviewed

4. Network Security Testing

- □ Open ports reviewed
- □ Unnecessary services identified
- □ Default credentials tested
- □ Weak authentication identified
- □ SMB configuration reviewed
- □ FTP anonymous access tested
- □ SNMP misconfigurations checked
- □ NFS shares reviewed
- □ RDP security reviewed
- □ SSH configuration reviewed
- □ Firewall rules validated
- □ VPN configuration reviewed

5. Vulnerability Assessment

- □ Known CVEs identified
- □ Missing patches identified
- □ End-of-life software found
- □ Misconfigurations identified
- □ Weak cryptography identified
- □ Insecure protocols detected
- □ Hardcoded credentials found
- □ Excessive permissions identified
- □ Insecure backups found
- □ Debug modes identified

6. Web Application Testing

Authentication & Session

□ Weak password policy
□ Brute-force protection missing
□ Credential stuffing protection missing
□ Session fixation vulnerability
□ Session timeout issues
□ Insecure cookies
□ MFA bypass possibility
□ Password reset flaws

Authorization

□ IDOR vulnerabilities
□ Privilege escalation possible
□ Role separation failures
□ Missing access controls

Input Handling

□ SQL injection
□ NoSQL injection
□ Command injection
□ XSS (Stored)
□ XSS (Reflected)
□ XSS (DOM)
□ Server-side template injection
□ XML / XXE injection
□ File upload vulnerabilities
□ Path traversal
□ LFI / RFI

Application Logic

□ Business logic flaws
□ Workflow bypass
□ Price manipulation
□ Race conditions
□ Rate-limit bypass

Security Configuration

□ Debug endpoints exposed
□ Stack traces exposed
□ Directory listing enabled
□ Missing security headers
□ CORS misconfiguration

7. API Security Testing

□ Authentication enforced
□ Token handling issues
□ Broken Object Level Authorization
□ Broken Function Level Authorization
□ Mass assignment
□ Excessive data exposure
□ Missing rate limiting
□ Insecure deserialization
□ API versioning flaws

8. Wireless Security Testing (If In Scope)

□ Open wireless networks detected
□ Weak encryption detected
□ WPS enabled
□ Rogue access points possible
□ Client isolation disabled
□ Network segmentation enforced

9. Internal Network Testing

□ Domain enumeration completed
□ Trust relationships identified
□ Weak internal passwords found
□ Credential reuse detected
□ Local admin sprawl identified
□ Privilege escalation paths identified
□ Lateral movement possible
□ File share permissions weak
□ Backup access insecure
□ Endpoint protections reviewed

10. Cloud Security Testing

□ Public storage exposure
□ IAM misconfigurations
□ Over-privileged roles
□ Insecure service endpoints
□ Metadata service exposed
□ Logging enabled
□ Key rotation enforced
□ Secrets management secure
□ Network security groups reviewed

11. Post-Exploitation

□ Privilege escalation validated
□ Access scope confirmed
□ Sensitive data exposure verified
□ Lateral movement confirmed
□ Persistence risk identified
□ Test artifacts removed

12. Detection & Response

□ Alerts triggered
□ Logs generated
□ SOC visibility confirmed
□ Incident response timing reviewed
□ Alert accuracy verified

13. Reporting

□ Executive summary written
□ Risk ratings assigned
□ Impact analysis completed
□ Proof of concept included
□ Affected assets listed
□ Reproduction steps documented
□ Remediation guidance provided
□ Security maturity assessed
□ Compliance mapping included

14. Remediation Validation

□ Fixes verified
□ Regression testing completed
□ Risk re-rated
□ Findings closed