EXTERNAL PENETRATION TESTING CHECKLIST

RECONNAISSANCE

- [ ] Passive information gathering (shodan, censys, google dorking)
- [ ] Whois lookup (domain registration information)
- [ ] DNS, subdomain enumeration (nslookup, dnrecon, sublist3r, crt.sh)
- [ ] Internet archives (wayback URL, wayback machines)
- [ ] Historical DNS data
- [ ] Network scan (netscan, hping3, nmap)
- [ ] Services enumeration (netcat, nmap, masscan)
- [ ] OS fingerprinting/Banner grabbing (nmap, telnet, IDserve)
- [ ] SSL/TLS certificate (e.g., expiry dates, authorities)
- [ ] Employees email addresses (hunter.io, snov.io)
- [ ] Breached credentials (breach-parse, dehashed)
- [ ] Leaked credentials (e.g., GitHub, GitLab)
- [ ] Web technologies (e.g, WAF, CDN)
- [ ] Framework, CMS (e.g., Laravel, WordPress, drupal)
- [ ] JavaScript Libraries (e.g jQuery, nodeJS
- [ ] Content Discovery (e.g., robots.txt, sitemap.xml, metadata)
- [ ] Directory, file enumeration (e.g., login portals, admin pages, backup, config file)

SCANNING

- [ ] Automated scan (nessus, nexpose, qualys, openVAS)
- [ ] Http, https enumeration (gobuster, dirb, burp, sublist3r, dirsearch, testssl, shcheck)
- [ ] SSH enumeration (nmap)
- [ ] FTP enumeration (nmap)
- [ ] WebDAV enumeration (nmap, cadaver)
- [ ] Cloud services enumeration (prowler, microburst)
- [ ] Azure blob, AWS S3 buckets,
- [ ] Firebase misconfigurations and insecure permissions.
- [ ] Web application/services scanning and enumeration

EXPLOITATION

- [ ] Credential stuffing, password spraying, bruteforce (hydra, john the ripper).
- [ ] Web application attacks and exploitation.
- [ ] Vulnerability assessments and research (e.g., cve.org, cvedetails.com).
- [ ] Exploit databases (e.g., Exploit-DB, packetstorm security, metasploit-framework, github)
- [ ] Vendor security releases and advisories