Information Gathering Tools

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Tool | Latest Version | Description/ Features | Scripting Language | Outcome |
| 1 | Zenmap (nmap) | 7.90 | * Free & open-source. * Utility for network and security auditing. * Can dig deeper using NSE scripts (581). * Finding vuln’s using scripts. * Evasion & spoofing. * Better ipv6 support [1]. * Better TLS/SSL Scanning. | Lua | * Host discovery. * Port scanning. * Service & version detection. * OS detection. * Timing & performance. |
| 2 | Whois | 4.2.2 (May-21-2018) | * To check domain names for expiration. * Checking domain names for registration. * Authorities may check when investigating criminal activity. | Php/Python/Ruby | * Name. * Address. * Email. * Phone numbers. * Associated IP addresses. |
| 3 | Sparta | - | * Can run nmap from Sparta. * Also can import XML output of nmap. * Default credential check for most common services using hydra’s internal wordlists. * Website screenshot taker. * Define automated task for services (i.e. nikto http service, sslscan etc.) * Various options like in-built brute force, netcat, telnet & dirbuster. | Python | * Host scan. * Nmap scan results. * Screenshot. * Hydra scan results. * Snmp-enum. * Netcat. * Nikto. |
| 4 | Nikto | 1.32 | * SSL Support. * Full HTTP proxy support. * Full HTTP proxy support. * Subdomain guessing. * Guess credentials. | Dockerfile/Python | *Image is in the repository for an overview..* |
| 5 | nslookup | - | * DNS lookup. | JS | * DNS details (IP addresses, mx records). |
| 6 | Dig  (domain information groper) | - | * Interrogation of DNS name servers. * Allows reverse DNS lookups. | Shell | * DNS records (nameservers, mail exchange, host addresses) |
| 7 | Xprobe2 | 2.0.3 | * OS fingerprinting | C++ | * OS details along with version. |
| 8 | Wireshark | 3.4.2 | * Troubleshoot network issues. * Examining network security issues. * For networking apps, also a debugging tool. | C | * Network packets. |
| 9 | telnet |  | * Access computer virtually & provides 2-way text based communication channel between two machines. | Ruby | * Server details which leads to vulnerabilities in it afterwards. |
| 10 | goBuster | 3.1 | * Brute forces (URL’s, DNS subdomains, virtual host names, open amazon s3 bucket). | GO | * Details regarding IP, webserver, admin and domain. |
| 11 | FOCA | 3.4.6.2 | * Fingerprinting tool. * Capable of analyzing documents i.e. MS Office, Open Office, PDF, Adobe SVG files etc. | *To run:*   * .net * C++ * SQL server. | * Output in the form of documents or files as mentioned in the descriptive path. |
| 12 | Shodan |  | * Search engine * Fast/bulk IP lookups * Network alerts * Bulk data downloads | Python | *Image is in the repository for an overview.* |
| 13 | Punkspider | 3.0 | * Powerful tool. * To provide free information to users about website. | Python | * XSS * SQL injection * JS analyzer |
| 14 | Httprint | 301 | * Web server fingerprinting tool. | Python | * Web servers. * Web enabled devices such as access points, routers, switches, cable modems, etc. * SSL information gathering. |