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 in the repository.* |
| 5 | nslookup | - | * DNS lookup. | JS | * DNS details (IP addresses, mx records). |
| 6 | Dig  (domain information groper) |  | * Interrogation of DNS name servers. |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |
| --- | --- |
| # | Reference |
| 1 | https://nmap.org/ |
| 2 | Same as Nmap |
| 3 | <https://github.com/rfc1036/whois>  <http://www.phpwhois.org/>  <https://github.com/weppos/whois> |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

NSE = Nmap Scripting Engine