Kali Linux Tools List

List of Kali Linux Tools and Description of Each

- **Nmap -** Nmap, a network discovery and security auditing tool, is another frequently used tool. There are options that notify every open port on the target. The Nmap ("Network Mapper") tool is used in active reconnaissance to discover not only the live systems but also gaps in the system. This versatile tool is well supported and one of the best in the hacking community. Nmap is available for all operating systems and includes a graphical user interface. It is used to identify network flaws.
- **Amass** - is a command line open-source tool that helps information security professionals to perform network mapping of attack surfaces and perform external asset discovery using open source information gathering and active reconnaissance techniques.
- **SpiderFoot** - is an intelligence automation tool based on *open-source intelligence* **(OSINT).** Its purpose is to automate gathering intelligence about a specific target, which could be *an IP address, domain name, hostname, network subnet, ASN,* or *person's name*.
- **Maltego** - is an open source intelligence and forensics application. It will offer you timeous mining and gathering of information as well as the representation of this information in a easy to understand format. This package replaces previous packages matlegoce and casefile.
- **ike-scan** - discovers IKE hosts and can also fingerprint them using the retransmission backoff pattern. ike-scan does two things: a) Discovery: Determine which hosts are running IKE. This is done by displaying those hosts which respond to the IKE requests sent by ike-scan.
- **Nikto** - is an Open Source software written in Perl language that is used to scan a web-server for vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 servers and can detect problems with specific version details of over 200 servers. It comes packed with many features
- **Lynis** is probably one of the most complete tools available for cybersecurity compliance (e.g. PCI, HIPAA, SOx), testing, system hardening, and system auditing. That's why it's included in this Kali Linux tools list.

  Given its immense capabilities, Lynis also serves as a great vulnerability scanner and penetration testing platform.

- **Fierce** is a great tool for network mapping and port scanning. It can be used to discover non-contiguous IP space and hostnames across networks.

  It's similar to Nmap and Unicornscan, but unlike those, Fierce is mostly used for specific corporate networks.

  Once the penetration tester has defined the target network, Fierce will run several tests against the selected domains to retrieve valuable information that can be used for later analysis and exploitation.

- **WPScan** is recommended for auditing your WordPress installation security. By using WPScan you can check if your WordPress setup is vulnerable to certain types of attacks, or if it's exposing too much information in your core, plugin or theme files.

  This WordPress security tool also lets you find any weak passwords for all registered users, and even run a brute force attack against it to see which ones can be cracked.

  WPScan receives frequent updates from the wpvulndb.com WordPress vulnerability database, which makes it a great software for up-to-date WP security.

- **Wireshark** is an open source multi-platform network analyzer that runs Linux, OS X, BSD, and Windows.

  It's especially useful for knowing what's going on inside your network, which accounts for its widespread use in government, corporate and education industries.

  It works in a similar manner as tcpdump, but Wireshark adds a great graphical interface that allows you to filter, organize and order captured data so it takes less time to analyze. A text-based version, called tshark, is comparable in terms of features.

- **John the Ripper** is a multi-platform cryptography testing tool that works on Unix, Linux, Windows and MacOS. It allows system administrators and security penetration testers to launch brute force attacks to test the strength of any system password. It can be used to test encryptions such as DES, SHA-1 and many others.

  Its abilities to change password decryption methods are set automatically, depending on the detected algorithm.

  Licensed and distributed under the GPL license, it's a free tool available for anyone who wants to test their password security.

- **THC Hydra** is a free hacking tool licensed under AGPL v3.0, widely used by those who need to brute force crack remote authentication services.

  As it supports up to more than 50 protocols, it's one of the best tools for testing your password security levels in any type of server environment.

It also provides support for most popular operating systems like Windows, Linux, Free BSD, Solaris and OS X.

- **Metasploit** Framework is a Ruby-based platform used to develop, test and execute exploits against remote hosts. It includes a full collection of security tools used for penetration testing, along with a powerful terminal-based console — called msfconsole — which allows you to find targets, launch scans, exploit security flaws and collect all available data.

  Available for Linux and Windows, MSF is probably one of the most powerful security auditing tools freely available for the infosec market.

- **Yersinia** is a security network tool that allows you to perform L2 attacks by taking advantage of security flaws in different network protocols.

  This tool can attack switches, routers, DHCP servers and many other protocols. It includes a fancy GTK GUI, ncurses-based mode, is able to read from a custom configuration file, supports debugging mode and offers to save results in a log file.