Tools of Kali Linux

Do you want to learn more about cybersecurity tools?

Have you ever opened Kali Linux and not know where to begin?
Here we have created a small list of tools that are part Kali Linux. Some of our career field experts have given us their short list of tools that they would recommend for individual interested in learning more about cybersecurity. Looking at the menus in Kali Linux can be overwhelming. Hopefully this short list can help you navigate the introduction to Kali Linux Operating System (OS). You don’t need to have Kali Linux to try any of these tools, but it does make it much easier.

John the Ripper

John the Ripper is the name of the password cracker tool that is developed by Openwall. As the name, it is used to crack password hashes by using its most popular inbuilt program, rules and codes that are also an individual password cracker itself in a single package.
It automatically detects types of password hashes; you can also customize this tool according to your wish. It can be used to crack password-protected compressed files like Zip, Rar, Doc, pdf etc.

Nmap

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.
Gordon Lyon (pseudonym Fyodor) wrote Nmap as a tool to help map an entire network easily and to find its open ports and services.

Nmap Scripting Engine (NSE)

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. Those scripts are executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap, or write their own to meet custom needs.

Wireshark

Wireshark is the world’s foremost and widely-used network protocol analyzer. It lets you see what’s happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

Metasploit

Metasploit is one of the best penetration testing frameworks that help a business find out and shore up vulnerabilities in their systems before exploitation by hackers. To put it simply, Metasploit allows hacking with permission.
Metasploit was conceived and developed by H D Moore in October 2003 as a Perl-based portable network tool for the creation and development of exploits. By 2007, the framework was entirely rewritten in Ruby. In 2009, Rapid7 acquired the Metasploit project, and the framework gained popularity as an emerging information security tool to test the vulnerability of computer systems. Metasploit 4.0 was released in August 2011 and includes tools that discover software vulnerabilities besides exploits for known bugs.

Armitage

Armitage is a fantastic Java-based GUI front-end for the Metasploit Framework developed by Raphael Mudge. Its goal is to help security professionals better understand hacking and help them realize the power and potential of Metasploit.

OpenVAS – Open Vulnerability Assessment Scanner

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
The scanner obtains the tests for detecting vulnerabilities from a feed that has a long history and daily updates.
OpenVAS has been developed and driven forward by the company Greenbone Networks since 2006. As part of the commercial vulnerability management product family Greenbone Enterprise Appliance, the scanner forms the Greenbone Vulnerability Management together with other Open-Source modules.

MASSCAN

MASSCAN is aTCP port scanner which transmits SYN packets asynchronously and produces results similar to nmap, the most famous port scanner. Internally, it operates more like scanrand, unicornscan, and ZMap, using asynchronous transmission. It’s a flexible utility that allows arbitrary address and port ranges.

Harvester

Harvester is a modern Hyperconverged infrastructure (HCI) solution built for bare metal servers using enterprise-grade open-source technologies including Kubernetes, Kubevirt and Longhorn. Designed for users looking for a cloud-native HCI solution, Harvester is a flexible and affordable offering capable of putting VM workloads on the edge, close to your IoT, and integrated into your cloud infrastructure.