15 Linux Security Tools

1. Firejail

Firejail is a c-based community SUID project that minimizes security breaches by managing the access that applications using Linux namespaces and seccomp-bpf run.

Firejail can easily sandbox server, GUI apps, and login session processes and because it ships with several security profiles for different Linux programs including Mozilla Firefox, VLC, and transmission, it is simple to set up.

2. ClamAV

ClamAV antivirus is open-source and it is excellent at detecting viruses and trojans among other security and privacy threats. It is so reliable it is considered an open-source standard for mail gateway scanning software.

It features a multi-threaded scanner daemon, support for multiple file formats, multiple signature languages, and command line utilities.

3. John the Ripper

John the Ripper is among the fastest password crackers and it is available for multiple platforms including OpenVMS, Windows, DOS, and several Unix flavors.

It is open-source and right out of the box it supports Windows LM hashes and its community-enhanced version packs a lot more features like support for more hashes and ciphers.

4. Nessus

Nessus is a proprietary software for scanning network vulnerability. It is free to use for personal tasks in non-enterprise environments.

Its free version allows you to scan up to 16 IP addresses per scanner at high speed complete with in-depth assessments. If you need more user options then you will need to purchase a subscription.

How to Install Gnome Shell Extensions

5. Wireshark

Wireshark is a popular open-source multi-platform utility for analyzing network protocols and packets. It features rich VoIP analysis, a simple GUI, live capture and offline analysis, export to XML, PostScript, powerful display filters, and many more features that make it an excellent utility for education.

6. KeePass

KeePass is a cross-platform open-source password manager that absolves you of the need to remember all your passwords. It stores all its passwords in encrypted databases which can be unlocked with a single master password or key file.

It features a simple UI with a tree view of its folder structure, password groups, export/import, multi-language support, etc.

7. Nmap

Nmap is a flexible, portable, open-source tool for scanning networks and making security audits. It is well documented and you can use it to manage service upgrade schedules, network inventory, monitoring server uptime, etc.

8. Nikto

Nikto is an open-source web scanner for detecting outdated server software, dangerous files, cookies, and performing both generic and server type specific checks.

It features a template engine for reports, full HTTP proxy support, subdomain guessing, logging to Metasploit, LibWhisker's IDS encoding techniques, etc.

9. Snort

Snort is an open-source network intrusion detection software currently developed by Cisco. It features all the tools required to stay abreast of the latest security trends and a comprehensive documentation to jump start its usage.

10. OSQuery

OSQuery is an open-source and cross-platform framework for analyzing networks and security leaks. It is an industry standard for performing continuous tests to check thread safety, detect memory leaks, and binary reproducibility.

OSQuery enables you to query your devices like you would a relational database using SQL commands for security, compliance, and developer operations.

11. Metasploit framework

Metasploit is mainly used for penetration testing but you can also use it for authenticating vulnerabilities, conducting security assessments, and improving your security awareness to stay ahead of potential attackers.

12. Gufw

Gufw is an open-source firewall app that focuses on efficiency and ease-of-use. It features a user-friendly UI with the option to work with a simple or advanced options set. Either way, Gufw is among the easiest firewalls to set up.

13. Chkrootkit

Chkrootkit is an open-source utility for detecting local rootkits. A rootkit is any set of software tools used by a 3rd party to hide the changes made to a computer system after a successful security bridge.

14. Rsync Backup

Rsync is an open source bandwidth-friendly utility for making speedy incremental file transfers locally and remotely on Unix and Linux computers.

15. MTR

MTR is a network diagnostic tool containing a consolidated functionality of the trace-route and ping utilities. It is simple to use, command line-based and gives reports in real-time.