

10 Best Hacking and Security Software Tools for Linux

Contributed by Horia Puscuta
Monday, 06 July 2009
Last Updated Monday, 06 July 2009

Linux is a hacker's dream computer operating system. It supports tons of tools and utilities for cracking passwords, scanning network vulnerabilities, and detecting possible intrusions. I have here a collection of 10 of the best hacking and security software tools for Linux. Please always keep in mind that these tools are not meant to harm, but to protect.

1. John the Ripper

John the Ripper is a free password cracking software tool initially developed for the UNIX operating system. It is one of the most popular password testing/breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix flavors (based on DES, MD5, or Blowfish), Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL and others.

2. Nmap

Nmap is my favorite network security scanner. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services on a network despite the fact that such services aren't advertising themselves with a service discovery protocol. In addition Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card.

Nmap runs on Linux, Microsoft Windows, Solaris, and BSD (including Mac OS X), and also on AmigaOS. Linux is the most popular nmap platform and Windows the second most popular.

{mosgoogle}

3. Nessus

Nessus is a comprehensive vulnerability scanning software. Its goal is to detect potential vulnerabilities on the tested systems such as:

-Vulnerabilities that allow a remote cracker to control or access sensitive data on a system.

-Misconfiguration (e.g. open mail relay, missing patches, etc).

-Default

passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.

-Denials of service against the TCP/IP stack by using mangled packets

Nessus

is the world's most popular vulnerability scanner, estimated to be used by over 75,000 organizations worldwide. It took first place in the 2000, 2003, and 2006 security tools survey from SecTools.Org.

4. chkrootkit

chkrootkit

(Check Rootkit) is a common Unix-based program intended to help system administrators check their system for known rootkits. It is a shell script using common UNIX/Linux tools like the strings and grep commands to search core system programs for signatures and for comparing a traversal of the /proc filesystem with the output of the ps (process status) command to look for discrepancies.

It can be used from a

"rescue disc" (typically a Live CD) or it can optionally use an alternative directory from which to run all of its own commands. These techniques allow chkrootkit to trust the commands upon which it depend a bit more.

There are inherent limitations to the reliability of any program that attempts to detect compromises (such as rootkits and computer viruses). Newer rootkits may specifically attempt to detect and compromise copies of the chkrootkit programs or take other measures to evade detection by them.

5. Wireshark

Wireshark

is a free packet sniffer computer application used for network troubleshooting, analysis, software and communications protocol development, and education. In June 2006, the project was renamed from Ethereal due to trademark issues.

The functionality Wireshark

provides is very similar to tcpdump, but it has a GUI front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.

Wireshark uses the

cross-platform GTK+ widget toolkit, and is cross-platform, running on various computer operating systems including Linux, Mac OS X, and Microsoft Windows. Released under the terms of the GNU General Public License, Wireshark is free software.

6. netcat

netcat is a computer networking utility for reading from and writing to network connections on either TCP or UDP.

Netcat

was voted the second most useful network security tool in a 2000 poll conducted by insecure.org on the nmap users mailing list. In 2003, it gained fourth place, a position it also held in the 2006 poll.

The original version of netcat is a UNIX program. Its author is known as *Hobbit*. He released version 1.1 in March of 1996.

Netcat is fully POSIX compatible and there exist several implementations, including a rewrite from scratch known as GNU netcat.

7. Kismet

Kismet

is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b and 802.11g traffic.

Kismet is unlike most other wireless network detectors in that it works passively. This means that without sending any loggable packets, it is able to detect the presence of both wireless access points and wireless clients, and associate them with each other.

Kismet also includes basic wireless IDS features such as detecting active wireless sniffing programs including NetStumbler, as well as a number of wireless network attacks.

8. hping

hping

is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de facto tools for security auditing and testing of firewalls and networks, and was used to exploit the idle scan scanning technique (also invented by the hping author), and now implemented in the Nmap Security Scanner. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time.

Like most tools used in computer security, hping is useful to both system administrators and crackers (or script kiddies).

9. Snort

Snort

is a free and open source Network Intrusion prevention system (NIPS) and network intrusion detection (NIDS) capable of performing packet logging and real-time traffic analysis on IP networks.

Snort

performs protocol analysis, content searching/matching, and is commonly used to actively block or passively detect a variety of attacks and probes, such as buffer overflows, stealth port scans, web application attacks, SMB probes, and OS fingerprinting attempts, amongst other features. The software is mostly used for intrusion prevention purposes, by dropping attacks as they are taking place. Snort can be combined with other software such as SnortSnarf, sguil, OSSIM, and the Basic Analysis and Security Engine (BASE) to provide a visual representation of intrusion data. With patches for the Snort source from Bleeding Edge Threats, support for packet stream antivirus scanning with ClamAV and network abnormality with SPADE in network layers 3 and 4 is possible with historical observation.

10. tcpdump

tcpdump

is a common computer network debugging tool that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

In some Unix-like operating systems, a user must have superuser privileges to use tcpdump because the packet capturing mechanisms on those systems require elevated privileges. However, the `-Z` option may be used to drop privileges to a specific unprivileged user after capturing has been set up. In other Unix-like operating systems, the packet capturing mechanism can be configured to allow non-privileged users to use it; if that is done, superuser privileges are not required.

The user may optionally apply a BPF-based filter to limit the number of packets seen by tcpdump; this renders the output more usable on networks with a high volume of traffic.