

Forum:[Hack Forums](#)

Thread: [{mega thread}Ultimate Linux Security Tools{Must have}}](#)

Tooth Fairy - April 9, 2010, 4:40 am

1) Wireshark – network traffic analyzer

Wireshark is a network traffic analyzer, or “sniffer”, for Unix and Unix-like operating systems. A sniffer is a tool used to capture packets off the wire. Wireshark decodes numerous protocols (too many to list). This package provides wireshark (the GTK+ version)

<http://www.wireshark.org>

2) Nessus – Remote network security auditor

The Nessus® vulnerability scanner, is the world-leader in active scanners, featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks.

<http://www.nessus.org>

3) Nmap – The Network Mapper

Nmap (“Network Mapper”) is a free and open source (license) utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and both console and graphical versions are available.

4) Etherape – graphical network monitor modeled after etherman

EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, ip and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display. It supports Ethernet, FDDI, Token Ring, ISDN, PPP and SLIP devices. It can filter traffic to be shown, and can read traffic from a file as well as live from the network.

<http://etherape.sourceforge.net>

5) Kismet – Wireless 802.11b monitoring tool

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.

<http://www.kismetwireless.net>

6) Chkrootkit – Checks for signs of rootkits on the local system

chkrootkit identifies whether the target computer is infected with a rootkit. Some of the rootkits that chkrootkit identifies are:

1. Lrk3, Lrk4, Lrk5, Lrk6 (and some variants);
2. Solaris rootkit;
3. FreeBSD rootkit;
4. t0rn (including latest variant);
5. Ambient's Rootkit for Linux (ARK);
6. Ramen Worm;
7. rh[67]-shaper;
8. RSHA;
9. Romanian rootkit;
10. RK17;
11. Lion Worm;
12. Adore Worm.

Please note that this is not a definitive test, it does not ensure that the target has not been cracked. In addition to running chkrootkit, one should perform more specific tests.

<http://www.chkrootkit.org>

7) Rkhunter – rootkit, backdoor, sniffer and exploit scanner

Rootkit Hunter scans systems for known and unknown rootkits, backdoors, sniffers and exploits.

It checks for:

- MD5 hash changes;
- files commonly created by rootkits;
- executables with anomalous file permissions;
- suspicious strings in kernel modules;
- hidden files in system directories;

and can optionally scan within files. Using rkhunter alone does not guarantee that a system is not compromised. Running additional tests, such as chkrootkit, is recommended.

<http://www.rootkit.nl>

8) tiger – Report system security vulnerabilities

TIGER, or the 'tiger' scripts, is a set of Bourne shell scripts, C programs and data files which are used to perform a security audit of UNIX systems. TIGER has one primary goal: report ways 'root' can be compromised. Debian's TIGER incorporates new checks primarily oriented towards Debian distribution including: md5sums checks of installed files, location of files not belonging to packages, check of security advisories and analysis of local listening processes.

9) GnuPG – GNU privacy guard

GnuPG is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures. It includes an advanced key management facility and is compliant with the proposed OpenPGP Internet standard as described in RFC2440. GnuPG does not use any patented algorithms so it cannot be compatible with PGP2 because it uses IDEA (which is patented worldwide).

<http://www.gnupg.org/>

10) Nemesis – TCP/IP Packet Injection Suite

Nemesis is a command-line network packet crafting and injection utility for UNIX-like and Windows systems. Nemesis, is well suited for testing Network Intrusion Detection Systems, firewalls, IP stacks and a variety of other tasks. As a command-line driven utility, Nemesis is perfect for automation and scripting.

Nemesis can natively craft and inject ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF, RIP, TCP and UDP packets. Using the IP and the Ethernet injection modes, almost any custom packet can be crafted and injected.

<http://nemesis.sourceforge.net>

11) Tcpcmdump – A powerful tool for network monitoring and data acquisition

This program allows you to dump the traffic on a network. tcpcmdump is able to examine IPv4, ICMPv4, IPv6, ICMPv6, UDP, TCP, SNMP, AFS BGP, RIP, PIM, DVMRP, IGMP, SMB, OSPF, NFS and many other packet types.

It can be used to print out the headers of packets on a network interface, filter packets that match a certain expression. You can use this tool to track down network problems, to detect “ping attacks” or to monitor network activities.

<http://www.tcpdump.org/>

12) OpenSSH – secure shell server

This is the portable version of OpenSSH, a free implementation of the Secure Shell protocol as specified by the IETF secsh working group. Ssh (Secure Shell) is a program for logging into a remote machine and for executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. It is intended as a replacement for rlogin, rsh and rcp, and can be used to provide applications with a secure communication channel. This package provides the sshd server.

In some countries it may be illegal to use any encryption at all without a special permit.

<http://www.openssh.com/>

13) Denyhosts – an utility to help sys admins thwart ssh hackers

DenyHosts is a program that automatically blocks ssh brute-force attacks by adding entries to /etc/hosts.deny. It will also inform Linux administrators about offending hosts, attacked users and suspicious logins. Synchronization with a central server is possible too.

Differently from other software that do same work, denyhosts doesn't need support for packet filtering or any other kind of firewall in your kernel

<http://denyhosts.sourceforge.net/>

14) Snort – Flexible Network Intrusion Detection System

Snort is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. Snort has a real-time alerting capability, with alerts being sent to syslog, a separate “alert” file, or even to a Windows computer via Samba.

This package provides the plain-vanilla snort distribution and does not provide database (available in snort-pgsql and snort-mysql) support.

<http://www.snort.org/>

15) Firestarter – gtk program for managing and observing your firewall

Firestarter is a complete firewall tool for Linux machines. It features an easy to use firewall wizard to quickly create a firewall. Using the program you can then open and close ports with a few clicks, or stealth your machine giving access only to a select few. The real-time hit monitor shows attackers probing your machine.

<http://www.fs-security.com>

16) clamav – anti-virus utility for Unix – command-line interface

Clam AntiVirus is an anti-virus toolkit for Unix. The main purpose of this software is the integration with mail servers (attachment scanning). The package provides a flexible and scalable multi-threaded daemon in the clamav-daemon package, a command-line scanner in the clamav package, and a tool for automatic updating via the Internet in the clamav-freshclam package. The programs are based on libclamav3, which can be used by other software.

This package contains the command line interface. Features:

- built-in support for various archive formats, including Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS and others;
- built-in support for almost all mail file formats;
- built-in support for ELF executables and Portable Executable files compressed with UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack and obfuscated with SUE, Y0da Cryptor and others;
- built-in support for popular document formats including Microsoft Office and Mac Office files, HTML, RTF and PDF.

For scanning to work, a virus database is needed. There are two options for getting it:

- clamav-freshclam: updates the database from Internet. This is recommended with Internet access.
- clamav-data: for users without Internet access. The package is not updated once installed. The clamav-getfiles package allows creating custom packages from an Internet-connected computer.

<http://www.clamav.net/>

17) Ettercap – Multipurpose sniffer/interceptor/logger for switched LAN

Ettercap supports active and passive dissection of many protocols (even ciphered ones) and includes many feature for network and host analysis. Data injection in an established connection and filtering (substitute or drop a packet) on the fly is also possible, keeping the connection synchronized.

Many sniffing modes were implemented to give you a powerful and complete sniffing suite. It's possible to sniff in four modes: IP Based, MAC Based, ARP Based (full-duplex) and PublicARP Based (half-duplex).

It has the ability to check whether you are in a switched LAN or not, and to use OS fingerprints (active or passive) to let you know the geometry of the LAN.

<http://ettercap.sourceforge.net/>

18) Netcat – TCP/IP swiss army knife

A simple Unix utility which reads and writes data across network connections using TCP or UDP protocol. It is designed to be a reliable “back-end” tool that can be used directly or easily driven by other programs and scripts. At the same time it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

<http://netcat.sourceforge.net>

19) MTR – mtr combines the functionality of the ‘traceroute’ and ‘ping’ programs in a single network diagnostic tool.

As mtr starts, it investigates the network connection between the host mtr runs on and a user-specified destination host. After it determines the address of each network hop between the machines, it sends a sequence ICMP ECHO requests to each one to determine the quality of the link to each machine. As it does this, it prints running statistics about each machine.

<http://www.bitwizard.nl/mtr/>

20) Hping3 – Active Network Smashing Tool

hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols. Using hping3, you can test firewall rules, perform (spoofed) port scanning, test network performance using different protocols, do path MTU discovery, perform traceroute-like actions under different protocols, fingerprint remote operating systems, audit TCP/IP stacks, etc. hping3 is scriptable using the TCL language.

<http://www.hping.org> 21) ngrep – grep for network traffic

ngrep strives to provide most of GNU grep's common features, applying them to the network layer. ngrep is a pcap-aware tool that will allow you to specify extended regular expressions to match against data payloads of packets. It currently recognizes TCP, UDP and ICMP across Ethernet, PPP, SLIP and null interfaces, and understands bpf filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop.

<http://ngrep.sourceforge.net/>

22) john – active password cracking tool

john, mostly known as John the Ripper, is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired.

It can also be used with different cyphertext formats, including Unix's DES and MD5, Kerberos AFS passwords, Windows' LM hashes, BSDI's extended DES, and OpenBSD's Blowfish.

<http://www.openwall.com/john/>

23) tcptrace – Tool for analyzing tcpdump output

Tcptrace is a tool for analyzing and reporting on tcpdump (or other libpcap) dump files. It can summarize the data or generate graph data for use with the gnuplot tool from the gnuplot package. Graph data can be created for throughput, RTT, time sequences, segment size, and cwin.

<http://jarok.cs.ohiou.edu/software/tcptrace/> 24) netdude – NETwork DUmP data Displayer and

Editor for tcpdump trace files

It is a GUI-based tool that allows you to make detailed changes to packets in tcpdump trace files, in particular, it can currently do the following: Set the value of any field in IP, TCP and UDP packet headers.

Copy, move and delete packets in the trace file. Fragment and reassemble IP packets.

Netdude constantly communicates with a tcpdump process to update the familiar tcpdump output that corresponds to the trace. This

also means that any changes made to your local version of tcpdump are reflected in Netdude. Plugin architecture: people can easily add plugins for specific tasks. The code comes with a plugin for checksum correction in IP, TCP and UDP, and a dummy plugin.

Through the plugin mechanism, Netdude provides a good facility for writing tcpdump trace file filters.

<http://netdude.sourceforge.net>

I did a lot of work to make it so please reply to make it even better.??

Kaleb - April 9, 2010, 5:02 am

Almost all those progs do the same thing.

Tooth Fairy - April 9, 2010, 5:05 am

25) tcpreplay – Tool to replay saved tcpdump files at arbitrary speeds

Tcpreplay is aimed at testing the performance of a NIDS by replaying real background network

traffic in which to hide attacks. Tcpreplay allows you to control the speed at which the traffic is replayed, and can replay arbitrary tcpdump traces. Unlike programmatically-generated artificial traffic which doesn't exercise the application/protocol inspection that a NIDS performs, and doesn't reproduce the real-world anomalies that appear on production networks (asymmetric routes, traffic bursts/lulls, fragmentation, retransmissions, etc.), tcpreplay allows for exact replication of real traffic seen on real networks.

<http://tcpreplay.synfin.net>

26) Dsniff – Various tools to sniff network traffic for cleartext insecurities

This package contains several tools to listen to and create network traffic: arpspoof – Send out unrequested (and possibly forged) arp replies.

dnsspoof – forge replies to arbitrary DNS address / pointer queries

on the Local Area Network. dsniif – password sniffer for several protocols.

filesnarf – saves selected files sniffed from NFS traffic. macof – flood the local network with random MAC addresses.

mailsnarf – sniffs mail on the LAN and stores it in mbox format. msgsnarf – record selected messages from different Instant Messengers.

sshmitm – SSH monkey-in-the-middle. proxies and sniffs SSH traffic. sshow – SSH traffic analyser.

tcpkill – kills specified in-progress TCP connections. tcpnice – slow down specified TCP connections via “active” traffic shaping.

urlsnarf – output selected URLs sniffed from HTTP traffic in CLF. webmitm – HTTP / HTTPS monkey-in-the-middle. transparently proxies.

webspy – sends URLs sniffed from a client to your local browser (requires libx11-6 installed).

<http://www.monkey.org/~dugsong/dsniff/>

27) scapy – Packet generator/sniffer and network scanner/discovery

Scapy is a powerful interactive packet manipulation tool, packet generator, network scanner, network discovery, packet sniffer, etc. It can for the moment replace hping, 85% of nmap, arpspoof, arp-sk, arping, tcpdump, tethereal, p0f, ...

In scapy you define a set of packets, then it sends them, receives answers, matches requests with answers and returns a list of packet couples (request, answer) and a list of unmatched packets. This has the big advantage over tools like nmap or hping that an answer is not reduced to (open/closed/filtered), but is the whole packet.

<http://www.secdev.org/projects/scapy/>

28) Ntop – display network usage in top-like format

ntop is a Network Top program. It displays a summary of network usage by machines on your network in a format reminiscent of the unix top utility. It can also be run in web mode, which allows the display to be browsed with a web browser.

<http://www.ntop.org/>

29) NBTscan – A program for scanning networks for NetBIOS name information

NBTscan is a program for scanning IP networks for NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address (such as Ethernet).

<http://www.unixwiz.net/tools/nbtscan.html>

30) tripwire – file and directory integrity checker

Tripwire is a tool that aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

<http://www.tripwire.com/>

Xdem0 - April 9, 2010, 6:38 am

(Apr 9, 2010 05:02 AM)HeatwavE Wrote: [\[CITE\]](#) Almost all those progs do the same thing. Far from it.

@op Nice List ? Nikto is also good pen-testing utility for webapps.
<http://cirt.net/nikto2>

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6100 potentially dangerous files/CGIs, checks for outdated versions of over 950 servers, and version specific problems on over 260 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

codepoet - April 9, 2010, 8:33 am

Very nice share... But most have the same functions. lol

Ps. Double posted

Tooth Fairy - April 9, 2010, 10:30 am

I found these tools and I liked to share them with you all,I posted some same type of tools to give you many choices to choose from :)

Clerisy - April 17, 2010, 6:19 pm

What about firewall for Linux :)?

Enter Shikari - April 17, 2010, 6:36 pm

(Apr 9, 2010 10:30 AM)???????x ?™ Wrote: [\[CITE\]](#) I found these tools and I liked to share them with you all,I posted some same type of tools to give you many choices to choose from :)

Thank you! I'm installing Ubuntu in VirtualBox to start learning everything, and this will really help in my quest!

Is there a way to request this for a sticky? Because I would.

Phizo - April 17, 2010, 8:02 pm

Thanks for the information mate.

Buffer_Overflow - April 17, 2010, 8:48 pm

Really good list you have here. Thanks for it.

Tooth Fairy - April 17, 2010, 9:28 pm

My pleasure to help :)

Tooth Fairy - April 18, 2010, 11:46 am

(Apr 17, 2010 08:48 PM)Buffer_Overflow Wrote: [\[CITE\]](#) Really good list you have here. Thanks for it. Thanks for the complement.

Therion - April 18, 2010, 3:37 pm

(Apr 17, 2010 06:19 PM)Troll Wrote: [\[CITE\]](#) What about firewall for Linux :)?

There's no such thing like a Desktop-Firewall nor is their a use for (though its possible to restrict programs).

Usually you want Linux' packetfilter which is usually controlled over iptables program.

Tooth Fairy - April 21, 2010, 6:36 am

154 views and only 12 replies.

Dan08 - April 22, 2010, 4:43 pm

Guys, do not use clamav. it screwed my computer up. now firefox is not working properly and my mouse is not working at all. i have to use an external one. But nice guide mate, im actually gonna install some of them right now hahaha :)

Tooth Fairy - April 22, 2010, 9:44 pm

Sorry for that, but any ways thanks for the complement.

Xdem0 - April 23, 2010, 12:18 am

(Apr 22, 2010 04:43 PM)Dan08 Wrote: [\[CITE\]](#) Guys, do not use clamav. it screwed my computer up. now firefox is not working properly and my mouse is not working at all. i have to use an external one. But nice guide mate, im actually gonna install some of them right now hahaha :)

You don't even need an anti-virus on a *nix computer, unless your running a mail-server and want to make sure your not passing on infected attachments to windows users.

v0lt4g3 - April 23, 2010, 9:26 am

Nice list!

As for linux firewalls, yes there are desktop linux firewalls such as Firestarter, which was listed in the initial post.

There's also gufw firewall, available via Synaptic.

Another cool tool I have is w3af, web attack framework, also available via Synaptic.

Thanks for the share!

evilfr0g - April 18, 2011, 6:09 pm

Nice thread very helpfull, thanks !

TheAxis - April 19, 2011, 10:58 am

This is a great post, thanks for taking the time to make this

Aquines - April 19, 2011, 2:46 pm

Awesome post man!

Thanks for going to the trouble to compile all this! Very helpful.

Tooth Fairy - April 21, 2011, 4:10 am

Anything for HackForums and to help you all . ?

kerneljinkin - May 29, 2011, 9:58 pm

While I always go to Sectools.org for the top 100 list, this is still a great compilation. Nice job putting this together! It's sad to say that most H-F members won't get any use out of it due to using winblows. Very, very sad. Again, nice job putting all this together like you did!

GayFish - May 30, 2011, 3:24 am

Win list :3

Thanks for the list.

HelPaMe - May 30, 2011, 6:32 am

nice list..thanking you..

GamingManiac - May 30, 2011, 9:29 am

People.

Year old thread - stop posting please

dru2670 - May 30, 2011, 7:56 pm

Great post seems like you definitely should have added metasploit and cain and abel to the this list.
Other than that you chose very good programs.