

Forum:[Hack Forums](#)

Thread: [20 Linux Tools For Hacking](#)

K0FIN - June 9, 2013, 3:43 pm

Hello, my name is K0FIN, and I will be introducing some tools for you today. These tools are designed for penetration testing, ethical hacking, and computer security and are all Linux based. Let's take a look-

0x01- Nmap

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and 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 official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Code `apt-get install nmap`

0x02- Nessus

[img]<http://static.tenable.com/oldsite/blog/img/6a00d8345495f669e20133f445cc65970b>[/img]

With more than 10 million downloads to date, Nessus® is the industry's most widely deployed vulnerability and configuration assessment product. Nessus is fueled by Nessus ProfessionalFeed® and is supported by an expert vulnerability research team. Nessus scales to serve the largest organizations and is easy to deploy. Basically, Nessus can scan anything, from the external network to the internal network to web applications. It is very popular, easy to use, and easy to acquire.

Code `http://www.tenable.com/products/nessus`

0x03- The Metasploit Framework

[img]<http://2.bp.blogspot.com/-3SArqE1tuKQ/T1Os-teCxqI/AAAAAAAAAQ/T9GklLvaiV0/s1600/metasploit.png>[/img]

The Metasploit Framework is a suite of tools designed to help penetration testers gain access to vulnerable computer systems by executing remote exploits against these systems, along with a plethora of other tools designed to assist the avid hacker, such as payload generating, determining offsets to the Instruction Pointer of a processor within a vulnerable program buffer, an encoder for evil payloads, and tons of others. The Metasploit Framework has various versions that are open source and some that cost money.

Code <http://www.rapid7.com/products/metasploit/>
0x04- SQLmap

[img]http://1.bp.blogspot.com/_d-EZxgE4Ho/UG0GpJyZ1XI/AAAAAAAAAOg/oPFfeJ1lrOK8/s1600/sqlmap.png[/img]

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Code <https://github.com/sqlmapproject/sqlmap/tarball/master>
0x05- Aircrack-ng

[img]<http://www.aircrack-ng.org/resources/aircrack-ng-new-logo.jpg>[/img]

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

In fact, Aircrack-ng is a set of tools for auditing wireless networks. It is also my favorite tool to use, as opposed to a tool like Kismet.

Code <http://download.aircrack-ng.org/aircrack-ng-1.2-beta1.tar.gz>
0x06- Wireshark

[img]<http://www.livehacking.com/web/wp-content/uploads/2011/11/wireshark.jpg>[/img]

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.

Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

Wireshark is one of those really cool tools you can use when performing Man In The Middle attacks too, just so you know ;)

Code `apt-get install wireshark`
0x07- John The Ripper

[img]http://www.zerodayclothing.com/products/designs/johntheripper1_design.png[/img]

John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix systems, supported out of the box are Windows LM hashes, plus lots of other hashes and ciphers in the community-enhanced version. This is by far the best password cracker for Unix systems, while Windows users have Cain

and Able.

Code apt-get install john
0x08- Nikto

[img]<http://cirt.net/images/nikto.png>[/img]

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 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.

Code apt-get install nikto
0x09- Ettercap

[img]<http://ettercap.github.io/ettercap/logo.png>[/img]

Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols (even ciphered ones) and includes many feature for network and host analysis.

Code apt-get install ettercap
0x10- w3af

[img]http://dilanwarnakulasooriya.files.wordpress.com/2012/07/w3af_dilan.png[/img]

W3af is an extremely popular, powerful, and flexible framework for finding and exploiting web application vulnerabilities. It is easy to use and extend and features dozens of web assessment and exploitation plugins. In some ways it is like a web-focused Metasploit.

Code <http://w3af.org/download>
0x11- THC Hydra

[img]http://4.bp.blogspot.com/-ciG5WGHEqeo/TzUEG6omPil/AAAAAAAAAE2s/Vavp_skxiKE/s640/THC-HYDRA+7.2+-+Fast+and+Flexible+network+login+Bruteforce+Tool+Updated.png[/img]

When you need to brute force crack a remote authentication service, Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 30 protocols, including telnet, ftp, http, https, smb, several databases, and much more. Like THC Amap this release is from the fine folks at THC. Other online crackers are Medusa and Ncrack. The Nmap Security Scanner also contains many online brute force password cracking modules.

Code apt-get install hydra
0x12- sslstrip

[img]http://3.bp.blogspot.com/_p3XlIipv981Y/S88RVdmcG1I/AAAAAAAAAEA/g3d5W2XJFFs/s1600/MITM.jpg[/img]

sslstrip is an SSL stripping proxy, designed to make unencrypted HTTP sessions look as much as

possible like HTTPS sessions. It converts https links to http or to https with a known private key. It even provides a padlock favicon for the illusion of a secure channel. Many HTTPS sites are normally accessed from a redirect on an HTTP page, and many users don't notice when their connection isn't upgraded.

Code <http://thoughtcrime.org/software/sslstrip/sslstrip-0.9.tar.gz>
0x13- Ophcrack

[img]<http://www.amitbhawani.com/blog/wp-content/uploads/2010/12/OphCrack-Logo.png>[/img]

Ophcrack is a free rainbow-table based cracker for Windows passwords (though the tool itself runs on Linux, Windows, and Mac). Features include LM and NTLM hash cracking, a GUI, the ability to load hashes from encrypted SAM recovered from a Windows partition, and a Live CD version. Some tables are provided as a free download but larger ones have to be bought from Objectif Sécurité.

Code `apt-get install ophcrack`
0x14- TrueCrypt

[img]<http://russell.ballestrini.net/wp-content/uploads/2011/04/truecrypt.png>[/img]

TrueCrypt is an excellent open source disk encryption system for Windows, Mac, and Linux systems. Users can encrypt entire filesystems, which are then on-the-fly encrypted/decrypted as needed without user intervention beyond initially entering their passphrase. A clever hidden volume feature allows you to hide a second layer of particularly sensitive content with plausible deniability about whether it even exists. Then if you are forced to give up your passphrase, you give them the first-level secret. That only allows them access to the innocuous material you have there, without proving that a second level key even exists.

Code `apt-get install truecrypt`
0x15- Acunetix

[img]http://3tech.com.hk/SDCHK/fck_images/image/acunetix_logo_150x100%281%29.gif[/img]

Acunetix WVS (web vulnerability scanner) automatically checks web applications for vulnerabilities such as SQL Injections, cross site scripting, arbitrary file creation/deletion, and weak password strength on authentication pages. It boasts a comfortable GUI, an ability to create professional security audit and compliance reports, and tools for advanced manual webapp testing.

Code <http://www.acunetix.com/vulnerability-scanner/>

DrDinosaur - June 9, 2013, 9:18 pm

You're missing five, but still a decent compilation. I think most of the tools (if not a respectable equivalent) are already pre-installed on Kali, so most of the installation commands are unnecessary.

_Silky - June 9, 2013, 10:31 pm

Looks like you took this straight from the Nmap website. Some more of my favorites are

My own
TheHarvester
BeEF
SET
OneSixtyOne
PBNJ

SMB <-- By Far The Top 3.

I actually find the little dirty scripts/tools more useful than the major/most popular tools.

Succeeding - June 9, 2013, 10:48 pm

I do not like Acunetix the rest is all ready preinstalled in Kali/Backtrack as said.

RA4W - June 10, 2013, 4:07 am

Thanks for these tools will try some of them

Letoll - June 10, 2013, 6:36 am

Must say, I use theHarvester quite a bit, also wifite, reaver, armitage, openvas, and metasm

K0FIN - June 10, 2013, 1:17 pm

Thanks for the feedback guys. I know there are a ton more, but these are what I have come across in a major way when working with hacking/pentesting tools. Basically they are the most popular, and yes they do come preinstalled on pentesting operating systems like Kali or BackTrack.

Pocked - June 10, 2013, 1:54 pm

Thank you dude, usefull information.

K0FIN - June 10, 2013, 2:05 pm

(Jun 10, 2013 01:54 PM)Pocked Wrote: [\[CITE\]](#) Thank you dude, usefull information.

No problem man. I really just put this compilation together for beginners. Notice you don't see any debuggers or anything like that.

shadowfox48 - June 13, 2013, 6:11 pm

really neat. never heard of nikto.

edit: just installed and unpacked using now. thanks mate!

K0FIN - June 13, 2013, 7:04 pm

(Jun 13, 2013 06:11 PM)shadowfox48 Wrote: [\[CITE\]](#) really neat. never heard of nikto.

edit: just installed and unpacked using now. thanks mate!

No problem, just take into account Nikto is pretty loud (it's not hard for an IDS to tell that Nikto is being run against it's server), so at least try to tunnel the tool through something like proxychains.