

Forum:[Hack Forums](#)

Thread: [\[FREE\]Hacking resource/TOOLS for those in starting out.](#)

22gotya - November 2, 2016, 10:10 am

Thread subject pretty much sums it up. The link that will follow will yield a great deal of the more common, basic, or free source beginner tools/resources. Even used by advanced users. Either way, this site has an extremely large number of the. I will mention a handful for reference. I know these are considered "Hacking tools" but I have noticed a lot of threads regards said tools in the Beginners section. I just hope it give some of you who already used or heard of it before some help. The link for each individual tool is right in the link.?

-Aircrack: Aircrack is a suite of tools for 802.11a/b/g WEP and WPA cracking. It implements the best known cracking algorithms to recover wireless keys once enough encrypted packets have been gathered. . The suite comprises over a dozen discrete tools, including airodump (an 802.11 packet capture program), aireplay (an 802.11 packet injection program), aircrack (static WEP and WPA-PSK cracking), and airdecap (decrypts WEP/WPA capture files).

-Cain and Abel: UNIX users often smugly assert that the best free security tools support their platform first, and Windows ports are often an afterthought. They are usually right, but Cain & Abel is a glaring exception. This Windows-only password recovery tool handles an enormous variety of tasks. It can recover passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. It is also well documented.

-John the Ripper: John the Ripper is a fast password cracker for UNIX/Linux and Mac OS X.. Its primary purpose is to detect weak Unix passwords, though it supports hashes for many other platforms as well. There is an official free version, a community-enhanced version (with many contributed patches but not as much quality assurance), and an inexpensive pro version. You will probably want to start with some wordlists.

-THC Hydra: 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 50 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.

-OPHcrack: 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.

-Medusa: Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer. It supports many protocols: AFP, CVS, FTP, HTTP, IMAP, rlogin, SSH, Subversion, and VNC to name a few. Other online crackers are THC Hydra and Ncrack.

-fgdump: fgdump is a newer version of the pwdump tool for extracting NTLM and LanMan password

hashes from Windows. It is also capable of displaying password histories if they are available. It outputs the data in L0phtCrack-compatible form, and can write to an output file. fgdump attempts to disable antivirus software before running. It then runs pwddump, cachedump (cached credentials dump), and pstgdump. (protected storage dump).

-L0phtcrack;L0phtCrack attempts to crack Windows passwords from hashes which it can obtain (given proper access) from stand-alone Windows workstations, networked servers, primary domain controllers, or Active Directory. In some cases it can sniff the hashes off the wire. It also has numerous methods of generating password guesses (dictionary, brute force, etc). LC5 was discontinued by Symantec in 2006, then re-acquired by the original L0pht guys and reborn as LC6 in 2009. For free alternatives, consider ophcrack, Cain and Abel, or John the Ripper.

-SolarWinds: SolarWinds has created and sells dozens of special-purpose tools targeted at systems administrators. Security-related tools include many network discovery scanners, an SNMP brute-force cracker, router password decryption, a TCP connection reset program, one of the fastest and easiest router config download/upload applications available and more.

-RainbowCrack: The RainbowCrack tool is a hash cracker that makes use of a large-scale time-memory trade-off. A traditional brute force cracker tries all possible plaintexts one by one, which can be time consuming for complex passwords. RainbowCrack uses a time-memory trade-off to do all the cracking-time computation in advance and store the results in so-called "rainbow tables". It does take a long time to precompute the tables but RainbowCrack can be hundreds of times faster than a brute force cracker once the precomputation is finished.

-Wfuzz: Wfuzz is a tool for bruteforcing Web Applications, it can be used for finding resources not linked (directories, servlets, scripts, etc), bruteforcing GET and POST parameters for different kinds of injections (SQL, XSS, LDAP, etc.), bruteforcing form parameters (user/password), fuzzing, and more.

-Brutus: This Windows-only cracker bangs against network services of remote systems trying to guess passwords by using a dictionary and permutations thereof. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NNTP, and more. No source code is available. UNIX users should take a look at THC Hydra.

<http://sectools.org/tag/pass-audit/> <LINKS for said tools will be found here.

Cheese - November 2, 2016, 8:02 pm

Wow this is actually a great thread for those looking to start, thanks for your contribution!

Cute - November 2, 2016, 8:30 pm

HQ thread and good for newer learners.
thanks for this OP.

22gotya - November 2, 2016, 8:54 pm

Thanks for the feedback everybody! I have seen a lot of questions in regards to this lately, felt as if somebody should make a newer thread for people to use as a reference. I appreciate the positive feedback for sure!