

THC-Hydra v9.1 Cheatsheet (ingenieriainformatica.uniovi.es)

Offline password cracking tool



<https://tools.kali.org/password-attacks/hydra>

GENERAL USAGE

hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT]][/OPT]]

NOTES

Hydra is a tool to guess/crack valid login/password pairs.

OPTIONS

-C FILE: colon separated "login:pass" format, instead of -L/-P options
-h: more command line options (COMPLETE HELP)
-l LOGIN or -L FILE: login with LOGIN name, or load several logins from FILE
-M FILE: list of servers to attack, one entry per line, ':' to specify port
-m OPT: options specific for a module, see -U output for information
OPT: some service modules support additional input (-U for module help)
-p PASS or -P FILE: try password PASS, or load several passwords from FILE
-t TASKS: run TASKS number of connects in parallel per target (default: 16)
-U: service module usage details
server: the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)

EXAMPLES

hydra -l user -P passlist.txt ftp://192.168.0.1

operario@kali:~\$ hydra -l redondo -P /usr/share/wordlists/metasploit/unix_passwords.txt ftp://192.168.20.10
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-24 16:55:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1009 login tries (l:1/p:1009), ~64 tries per task
[DATA] attacking ftp://192.168.20.10:21/
[STATUS] 211.00 tries/min, 211 tries in 00:01h, 798 to do in 00:04h, 16 active
[STATUS] 208.00 tries/min, 624 tries in 00:03h, 385 to do in 00:02h, 16 active
[STATUS] 208.00 tries/min, 832 tries in 00:04h, 177 to do in 00:01h, 16 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-24 17:00:38
operario@kali:~\$

OPTIONS

service: the service to crack (see below for supported protocols)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s]
http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum
icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql
mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2
rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp
socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

by José Manuel Redondo López