THC-Hydra 8.6

Hydra is born more than 10 years ago, this page is used as a recap of the functionalities it provides, but also the differences in feature sets, services coverage and code between the most popular network authentication cracker tools available. Each feature is compared against Hydra as of the current version. This table is updated as new features are added to the project. If you find any inaccuracies on this page please do not hesitate to contact us.

[0x00] News and Changelog

Check out the feature sets and services coverage page – including a speed comparison against ncrack and medusa (yes, we win :-))
Development code is available at a public github repository:
https://github.com/vanhauser-thc/thc-hydra
There is a new section below for online tutorials.
Read below for Linux compilation notes.

CHANGELOG for 8.6
==========
! Development moved to a public github repository: https://github.com/vanhauser-thc/thc-hydra

! Reports came in that the rdp module is not working reliable sometimes, most likely against new Windows versions. please test, report and if possible send a fix
* added radmin2 module by catatonic prime – great work!
* smb module now checks if SMBv1 is supported by the server and if signing is required
* http-form module now supports URLs up to 6000 bytes (thanks to petrock6@github for the patch)
* Fix for SSL connections that failed with error:00000000:lib(0):func(0):reason(0) (thanks gaia@github for reporting)

* Added new command line option:
-c TIME: seconds between login attempts (over all threads, so -t 1 is recommended)
* Options put after -R (for loading a restore file) are now honored (and were disallowed before)
* merged several patches by Diadlo@github to make the code easier readable. thanks for that!
* merged a patch by Diadlo@github that moves the help output to the invididual module

You can also take a look at the full CHANGES file

[0x01] Introduction

Welcome to the mini website of the THC Hydra project.

Number one of the biggest security holes are passwords, as every password security study shows.
Hydra is a parallized login cracker which supports numerous protocols to attack. New modules
are easy to add, beside that, it is flexible and very fast.

Hydra was tested to compile on Linux, Windows/Cygwin, Solaris 11, FreeBSD 8.1, OpenBSD, OSX,
QNX/Blackberry, and is made available under GPLv3 with a special OpenSSL license expansion.

Currently this tool supports:
Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST,
HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-POST, HTTPS-HEAD,
HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle,
PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, RTSP, S7-300, SAP/R3, SIP, SMB, SMTP,
SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

For HTTP, POP3, IMAP and SMTP, several login mechanisms like plain and MD5 digest etc. are supported.

This tool is a proof of concept code, to give researchers and security consultants the
possiblity to show how easy it would be to gain unauthorized access from remote to a system.

The program was written van Hauser and is additiionally supported by David Maciejak.

[0x02] Screenshots

(1) Target selection

(2) Login/Password setup

(3) Hydra start and output

[0x03] Documentation

Hydra comes with a rather long README file that describes the details about the usage and special options.

But sometimes detailed online help can vastly improve your efficency.
The following links on the global internet are a recommended read.

General usage and options:
https://www.aldeid.com/wiki/Thc-hydra
Online Dictionary Attack:
https://resources.infosecinstitute.com/online-dictionary-attack-with-hydra/

HTTP basic auth:
https://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
https://www.sillychicken.co.nz/Security/how-to-brute-force-your-router-in-windows.html

HTTP form based auth:
https://www.art0.org/security/performing-a-dictionary-attack-on-an-http-login-form-using-hydra
https://insidetrust.blogspot.com/2011/08/using-hydra-to-dictionary-attack-web.html
https://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html
https://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29

Multiple protocols: https://wiki.bywire.org/Hydra
https://www.attackvector.org/brute-force-with-thc-hydra/
https://www.madirish.net/content/hydra-brute-force-utility

Telnet:
https://www.theprohack.com/2009/04/basics-of-cracking-ftp-and-telnet.html
https://www.adeptus-mechanicus.com/codex/bflog/bflog.html

For those people testing with DVWA, this is what you want:
hydra -l admin -p password http-get-form «/dvwa/login.php:username=^USER^&password=^PASS^&submit=Login:Login failed»

If you find other good ones, just email them in (vh(at)thc(dot)org).

[0x04] Disclaimer

1. Please do not use in military or secret service organizations or for illegal purposes.
2. The Affero General Public License Version 3 (AGPLv3) applies to this code.
3. A special license expansion for OpenSSL is included which is required for the Debian people

[0x05] The Art of Downloading: Source and Binaries

1. PRODUCTION/RELEASE VERSION:
The source code of state-of-the-art Hydra: hydra-8.6.tar.gz
(compiles on all UNIX based platforms – even MacOS X, Cygwin on Windows, ARM-Linux, Android, iPhone, Blackberry 10, etc.)

2. DEVELOPMENT VERSION:
You can download and compile the current development version of hydra always in its public GITHUB repository:
https://github.com/vanhauser-thc/thc-hydra by either
svn co https://github.com/vanhauser-thc/thc-hydra
or
git clone https://github.com/vanhauser-thc/thc-hydra.git
Note that this is the development state! New features – and new bugs. Things might not work!

3. The source code of an old, deprecated version of Hydra ONLY in case v7.x gives you problems on unusual and old platforms:
hydra-5.9.1-src.tar.gz

4. The Win32/Cywin binary release: – not anymore –
Install cygwin from https://www.cygwin.com
and compile it yourself. If you do not have cygwin installed – how
do you think you will do proper securiy testing? duh …

5. ARM and Palm binaries here are old and not longer maintained:
ARM: hydra-5.0-arm.tar.gz
Palm: hydra-4.6-palm.zip

[0x06] Compilation Help

Hydra compiles fine on all platforms that have gcc – Linux, all BSD, Mac OS/X, Cygwin on Windows, Solaris, etc.

It should even compile on historical SunOS, Ultrix etc. platforms :-)

There are many optional modules for network protocols like SSH, SVN etc. that require libraries.
If they are not found, these optional libraries will not be supported in your binary.

If you are on Linux, the following commands install all necessary libraries:

Ubuntu/Debian: apt-get install libssl-dev libssh-dev libidn11-dev libpcre3-dev libgtk2.0-dev libmysqlclient-dev libpq-dev libsvn-dev firebird2.1-dev libncp-dev libncurses5-dev
Redhat/Fedora: yum install openssl-devel pcre-devel ncpfs-devel postgresql-devel libssh-devel subversion-devel libncurses-devel
OpenSuSE: zypper install libopenssl-devel pcre-devel libidn-devel ncpfs-devel libssh-devel postgresql-devel subversion-devel libncurses-devel

This enables all optional modules and features with the exception of Oracle, SAP R/3 and the
Apple filing protocol – which you will need to download and install from the vendor’s web sites.
For Oracle this is (install the basic and SDK packages): https://www.oracle.com/technetwork/database/features/instant-client/index.html

For all other Linux derivates and BSD based systems, use the system software installer and look for
similar named libraries like in the command above.
In all other cases you have to download all source libraries and compile them manually;
the configure script output tells you what is missing and where to get it from.

[0x07] Development & Contributions

Your contributions are more than welcomed!

If you find bugs, coded enhancements or wrote a new attack module for a service,
please send them to vh (at) thc (dot) org

Interesting attack modules would be:
OSPF, BGP, PIM, PPTP, …
(or anything else you might be able to do (and is not there yet))

Please note that you can also download and commit via github:
https://github.com/vanhauser-thc/thc-hydra

Comments and suggestions are welcome.

Yours sincerly,

van Hauser
The Hackers Choice
https://www.thc.org/thc-hydra