# Using Hydra for Security Testing


Hydra is a brute forcing tools that can be used to brute force a connection to a target system. It does this via trying lots of username against lots of passwords.

```
$ hydra
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak

Syntax: 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]]

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

The hydra tool supports a wide variety of protocols such as:

- adam6500 asterisk cisco cisco-enable cobaltstrike 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

The hydra tool can be invoked as follows. In the following we can specify a username to target (**ajcblyth**) and we are using a list of passwords contained in the file **passlist.txt**.

```
$ hydra -l ajcblyth -P passlist.txt ftp://192.168.2.12
```

Within Kali standard word dictionaries can be located within the following usr/share/wordlists

- amass -> /usr/share/amass/wordlists
- dirb -> /usr/share/dirb/wordlists
- dirbuster -> /usr/share/dirbuster/wordlists
- fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
- fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
- john.lst -> /usr/share/john/password.lst
- legion -> /usr/share/legion/wordlists
- metasploit -> /usr/share/metasploit-framework/data/wordlists
- nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
- rockyou.txt.gz
- sqlmap.txt -> /usr/share/sqlmap/data/txt/wordlist.txt
- wfuzz -> /usr/share/wfuzz/wordlist
- wifite.txt -> /usr/share/dict/wordlist-probable.txt