

## S6L5

# Attacco di dizionario su SSH e FTP con Hydra

Marco Falchi

### Obiettivi dell'esercizio

1. Fare pratica con lo strumento Hydra per effettuare attacchi di brute force sull'autenticazione di servizi di rete.
2. Configurare i servizi SSH e FTP, consolidando la conoscenza di gestione e protezione dei servizi di rete.

---

### Passaggi Seguiti

#### 1. Configurazione del Servizio SSH

Creazione dell'utente per il test con conseguente password con comando:

**sudo add user test\_user**

- Nome utente: **test\_user**
- Password: **testpass**

---

#### 2. Attivazione del servizio SSH

Per attivare il servizio SSH è stato usato il seguente comando:

**sudo service ssh start**

```
(root@kali)-[/home/kali]
# sudo service ssh start

(root@kali)-[/home/kali]
# ssh test test_user@192.168.50.100
ssh: Could not resolve hostname test: No address associated with hostname

(root@kali)-[/home/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:W3dEn2wHajfwP12DywUeXhz3a1JFO//GKXWcnSN+8Bk.
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:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) 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)-[~]
$
```

## Configurazione del file di configurazione servizio SSH (scelta personale)

Ho deciso di configurare il file config del servizio SSH per aggiungere una maggiore personalizzazione e ho eseguito i seguenti comandi:

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

**Questo primo comando mi mostra il percorso file del config SSH**

Una volta nel file config ho modificato i seguenti parametri:

**PermitRootLogin yes**

**MaxStartups 10:30:60**

Questi due parametri sono fondamentali, infatti il primo consente all'utente root di connettersi direttamente tramite SSH mentre il secondo protegge da eventuali attacchi Ddos o Dos, infatti limita il numero di connessione non autenticate

10 (start): indica il numero di connessione non autenticate che possono essere stabilite prima che il “demone” inizi a rifiutarle

30 (rate) indica la percentuale di probabilità con cui il “demone” rifiuterà le nuove connessione una volta raggiunto il numero di connessioni start, ossia il 10

60 (full) indica il numero massimo di connessioni non autenticate possibili, una volta raggiunto ogni nuova connessione verrà rifiutata.

---

### 3. Verifica servizio SSH

Recupero dell'indirizzo IP con comando:

**ifconfig**

Test della connessione con comando:

**ssh test\_user@192.168.500.100**

---

### 4. Creazione delle wordlist personalizzate

Per il primo cracking della password ho creato delle wordlist personalizzate per simulare un attacco mirato con un range di parole predefinito, ho quindi creato due liste, una che si occupa dei possibili username e uno delle password e ho usato i seguenti comandi:

Creazione Wordlist delle password:

**echo -e**

**"password\n123456\nadmin123\ntestpass\nqwerty\nletmein\npassword1\nwelcome\n12345678\nchangeme\nroot123\ntoor\niloveyou\nsecurepass\npassword123" > passwords.txt**

Creazione Wordlist degli username:

**echo -e**

**"test\_user\nadmin\nroot\nuser1\nguest\noperator\nsupport\nmanager\ndeveloper\nservice\nbackup\ntester\naccount\nsuperuser\nsysadmin" > usernames.txt**

---

## 5. Utilizzo di Hydra su SSH

Ho usato Hydra per effettuare il “brute force” sul servizio SSH avviato in precedenza

Comando per Hydra:

**hydra -L usernames.txt -P passwords.txt 127.0.0.1 -t 1 ssh**

Spiegazione comando:

- -L usernames.txt: Specifica il file delle wordlist per i nomi utente.
- -P passwords.txt: Specifica il file delle wordlist per le password.
- 192.168.50.100: Indica il server SSH (localhost).
- -t 4: Esegue 4 thread alla volta per fare prima.

**NB: In casistiche semplici come questa basterebbe anche un t1 e quindi un thread per volta in quanto avere tanti thread potrebbe creare errori di connessione.**

```
(kali@kali)~$ hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t 4 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 2025-08-08 05:07:40
[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 4 tasks per 1 server, overall 4 tasks, 225 login tries (l:15/p:15), ~57 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
*%sS[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 2025-08-08 05:08:20
```

Vediamo quindi come abbiamo trovato sia la password che l'username evidenziati di verde grazie a hydra.

---

## 6. Configurazione del Servizio FTP

Ho installato inizialmente il server FTP con il comando:

**sudo apt-get install vsftpd -y**

Ho poi avviato il servizio con il comando:

**sudo service vsftpd start**

Ho successivamente creato un nuovo utente e una nuova password anche per il servizio FTP con il comando:

**sudo adduser ftp\_user**

- Nome utente: **ftp\_user**
- Password: **ftp\_pass**

---

## 7. Creazione wordlist personalizzate su servizio FTP

Ho quindi creato una nuova wordlist personalizzata sia per gli username che per le password

Creazione Wordlist degli username:

**echo -e**

**"ftp\_user\nadmin\nroot\nguest\nuser1\dottorrampino\callcenter\arena  
breakout\libro\libero\misentite" > ftp\_usernames.txt**

Creazione Wordlist delle password:

**echo -e**

**"123456\npassword\nftp\_pass\nadmin123\nwelcome\carino\simone  
marchica\consegnoalle18" > ftp\_passwords.txt**

## 8. Utilizzo di Hydra su FTP

Ho usato Hydra per effettuare il “brute force” sul servizio FTP avviato in precedenza

Comando per Hydra:

**hydra -L ftp\_usernames.txt -P ftp\_passwords.txt 192.168.50.100 -t 1 ftp**

Spiegazione comando:

- -L usernames.txt: Specifica il file delle wordlist per i nomi utente.
- -P passwords.txt: Specifica il file delle wordlist per le password.
- 192.168.50.100: Indica il server FTP (localhost).
- -t 4: Esegue 4 thread alla volta per fare prima.

**NB: In casistiche semplici come questa basterebbe anche un t1 e quindi un thread per volta in quanto avere tanti thread potrebbe creare errori di connessione.**

```
—(kali@kali)-[~]
└─$ hydra -L ftp_usernames.txt -P ftp_passwords.txt 192.168.50.100 -t 1 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 2025-08-08 07:09:15
[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 1 task per 1 server, overall 1 task, 25 login tries (l:5/p:5), ~25 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100 login: ftp_user password: ftp_pass
[STATUS] 21.00 tries/min, 21 tries in 00:01h, 4 to do in 00:01h, 1 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-08 07:10:40
```

Vediamo quindi come anche in questo caso abbiamo trovato sia la password che l'username evidenziati di verde grazie a hydra.

---

## **Conclusioni e Considerazioni**

L'esercizio ha dimostrato l'efficacia degli attacchi con dizionari mirati e ha messo in risalto degli aspetti fondamentali come la necessità di proteggere i servizi di rete configurando correttamente il file di configurazione e implementando sistemi di rilevamento.