Report: Configurazione e cracking dell’autenticazione SSH tramite Hydra

---

Obiettivo dell’esercizio

L’esercizio ha avuto un duplice scopo:

1. Fare pratica con lo strumento **Hydra** per il cracking dell’autenticazione dei servizi di rete.
2. Consolidare le conoscenze relative alla **configurazione dei servizi di rete**, in particolare il servizio **SSH**.

Ambiente di lavoro

- **Sistema operativo**: Kali Linux (Virtual Machine su VirtualBox)
- **Servizio analizzato**: SSH
- **Strumento di attacco**: Hydra
- **Scenario**: attaccante e vittima coincidono (localhost), ambiente di laboratorio

---

Fase 1 – Configurazione del servizio SSH

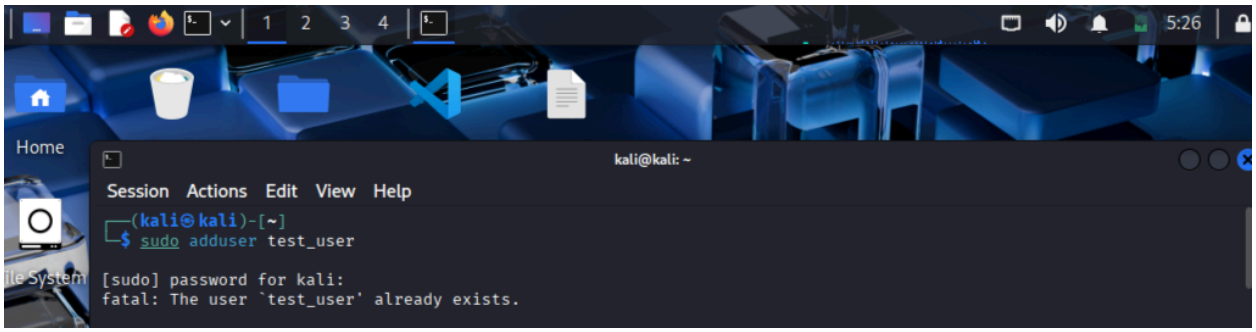
Creazione dell’utente di test

È stato creato un nuovo utente locale per simulare un account vulnerabile:

- **Username**: `test_user`
- **Password**: `testpass`

Il comando utilizzato è stato:

sudo adduser test_user



Avvio del servizio SSH

Il servizio SSH è stato avviato tramite il comando:

sudo service ssh start

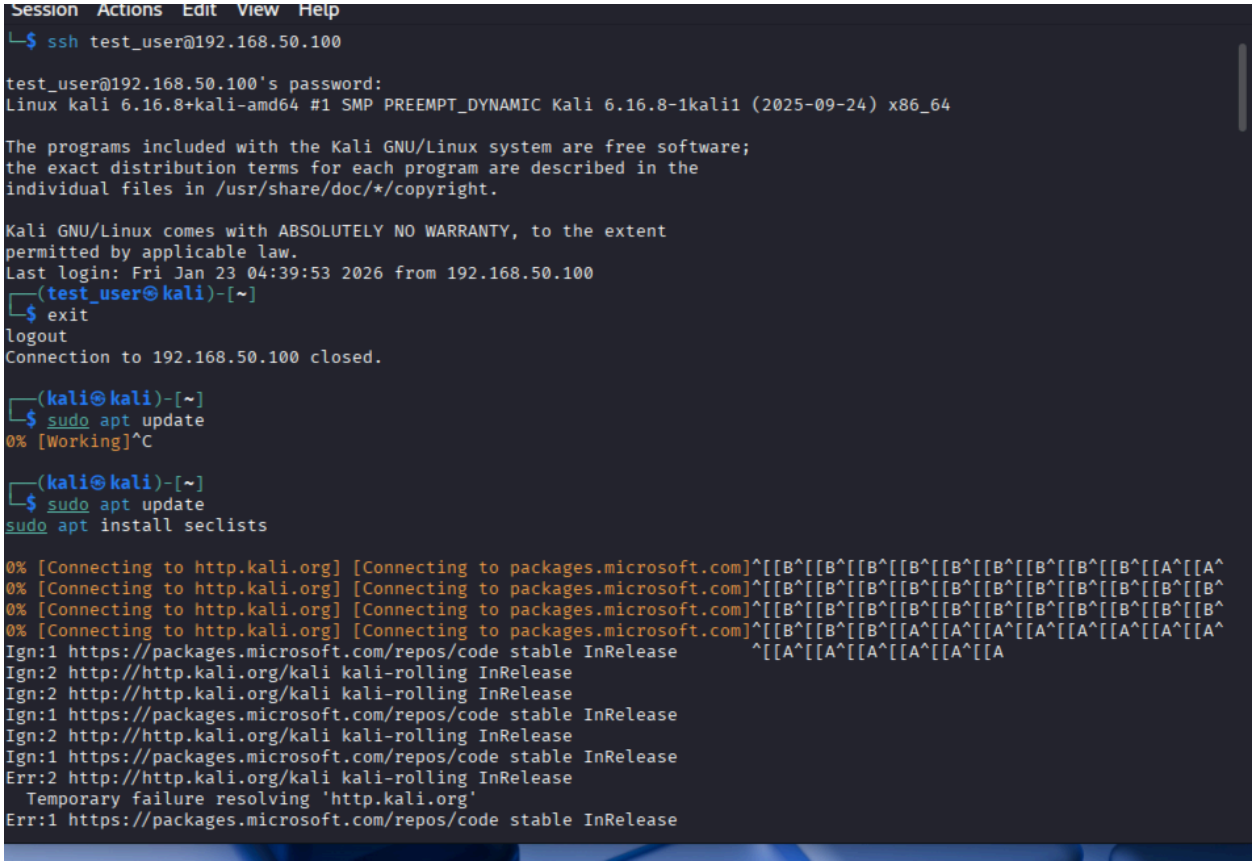
È stato inoltre verificato che il servizio fosse correttamente in esecuzione.

Verifica dell'accesso manuale

Prima di procedere con l'attacco, è stato testato l'accesso manuale via SSH:

ssh test_user@IP_KALI

L’accesso è avvenuto con successo, confermando il corretto funzionamento del servizio e delle credenziali.



Fase 2 – Preparazione delle wordlist

Durante l’esercizio **non è stato possibile installare la collezione SecLists** a causa di problemi di rete/DNS nella macchina virtuale.

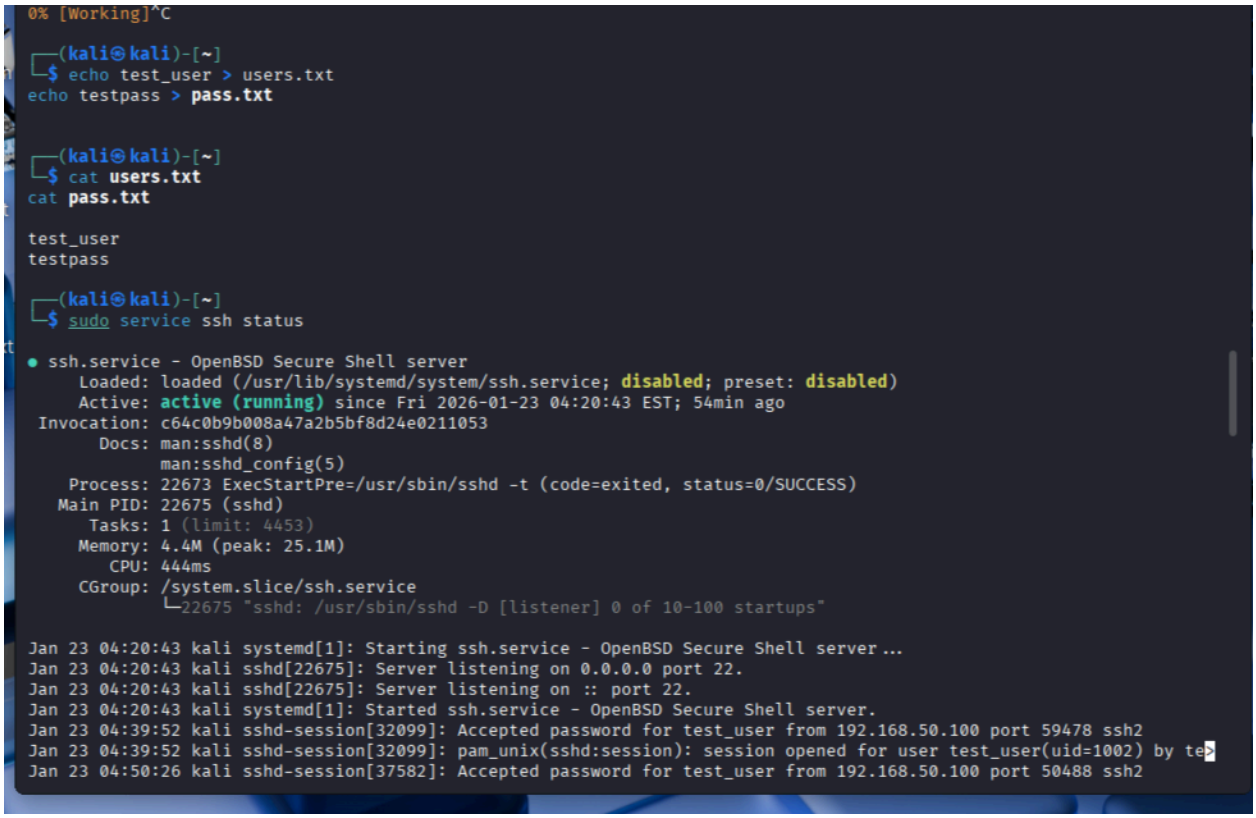
Per questo motivo, si è scelto di creare **manualmente delle wordlist personalizzate**, più che sufficienti per dimostrare il funzionamento di Hydra.

Wordlist utilizzate

- **users.txt**

test_user

- **Pass.txt**
- testpass



Questa scelta è coerente con uno scenario di laboratorio e permette di concentrarsi sulla sintassi e sul funzionamento dello strumento.

Fase 3 – Cracking dell'autenticazione SSH con Hydra

Comando utilizzato

L'attacco a dizionario contro il servizio SSH è stato eseguito con il seguente comando:

hydra -L users.txt -P pass.txt IP_KALI -t 2 -V ssh

Spiegazione dei parametri

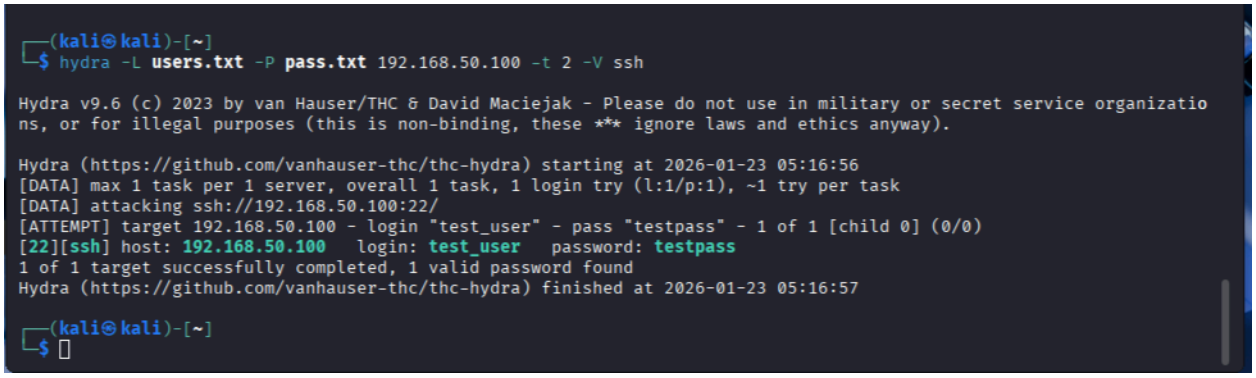
- `-L users.txt` → lista degli username
- `-P pass.txt` → lista delle password
- `IP_KALI` → indirizzo IP della macchina target
- `-t 4` → numero di thread
- `-V` → modalità verbose
- `ssh` → servizio bersaglio

Risultato

Hydra ha individuato correttamente le credenziali valide:

- **Username**: `test_user`
- **Password**: `testpass`

Dimostrando che il servizio SSH era vulnerabile a un attacco a dizionario basato su credenziali deboli.



Considerazioni di sicurezza

L'esercizio evidenzia come:

- L'utilizzo di **password deboli** renda i servizi di rete facilmente attaccabili.
- Hydra non sfrutta vulnerabilità software, ma **debolezze nella configurazione e nelle credenziali**.

Possibili contromisure

- Utilizzo di password complesse
- Disabilitazione dell'autenticazione a password in SSH (uso di chiavi)
- Implementazione di sistemi di rate-limiting o **fail2ban**
- Limitazione degli accessi tramite firewall

Conclusione

L'obiettivo dell'esercizio è stato raggiunto con successo. Dopo aver configurato un servizio SSH funzionante, è stato possibile dimostrare l'efficacia di un attacco a dizionario tramite Hydra, anche utilizzando wordlist create manualmente.

L'attività ha permesso di comprendere sia il funzionamento dello strumento di attacco sia l'importanza di una corretta configurazione dei servizi di rete dal punto di vista della sicurezza.