Report: Test di Brute Force con Hydra su SSH e FTP

1. Creazione di un utente aggiuntivo su Kali Per i test di brute force, è stato creato un utente aggiuntivo sulla macchina Kali con le seguenti caratteristiche:

- **Username**: `test_user`
- **Password**: `kali`

Comando usato per creare l'utente:

```
sudo adduser test_user
```

Durante il processo di configurazione, è stata assegnata la password `kali` all'utente.

Abilitazione dei permessi di root: L'utente `test_user` è stato aggiunto al gruppo `sudo` per ottenere privilegi di root. Questo è stato fatto con il seguente comando:

```
sudo usermod -aG sudo test_user
```

Il funzionamento è stato verificato accedendo come `test_user` e utilizzando il comando `sudo -i`, confermando di avere accesso ai privilegi di root.

2. Test di brute force su SSH con Hydra Una volta configurato l'utente, sono stati avviati i test di brute force su SSH utilizzando lo strumento **Hydra**.

Primo test: Brute force con username e password singoli Il primo test consisteva nell'uso di un singolo username e di una singola password.

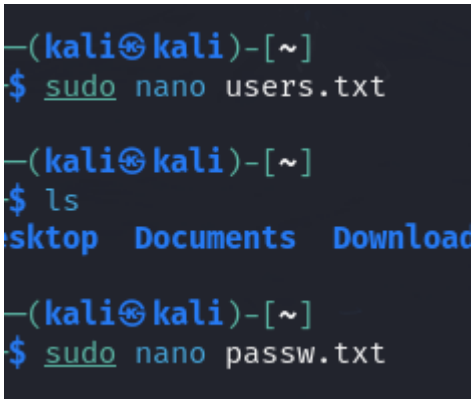
Comando eseguito:

```
hydra -l "test_user" -p "kali" -t 64 127.0.0.1 ssh
```

- **-l "test_user"**: Username utilizzato per il test.
- **-p "kali"**: Password utilizzata per il test.
- **-t 64**: Aumenta il numero massimo di thread a 64 per aumentare la velocità del test.
- **127.0.0.1**: Indirizzo IP della macchina target (loopback).
- **ssh**: Specifica il protocollo su cui effettuare il brute force.

Risultato: Il brute force ha avuto successo, dimostrando la validità del comando.

Secondo test: Brute force a dizionario Per il secondo test, è stato eseguito un attacco con dizionario utilizzando la wordlist **SecLists** preinstallata. Per facilitare il test, sono state create due liste personalizzate con 30 campi ciascuna per username e password, rendendo più chiaro il funzionamento di Hydra.

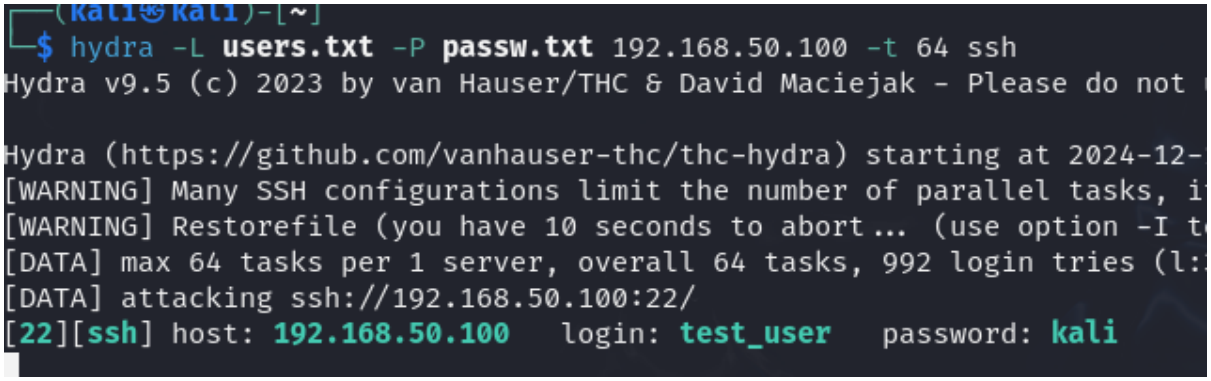


Comando eseguito:

```
hydra -L users.txt -P passw.txt -t 64 127.0.0.1 ssh
```

- **-L users.txt**: File di dizionario per la lista degli username (30 username).
- **-P passw.txt**: File di dizionario per la lista delle password (30 password).
- **-t 64**: Aumenta il numero massimo di thread a 64 per ottimizzare la velocità.
- **127.0.0.1**: Indirizzo IP della macchina target (loopback).
- **ssh**: Specifica il protocollo SSH.

Risultato: L'attacco a dizionario è andato a buon fine, dimostrando che Hydra è in grado di identificare correttamente le credenziali in base ai dizionari forniti.



3. Test di brute force su FTP con Hydra Dopo i test su SSH, è stato abilitato il servizio FTP sulla macchina Kali per eseguire gli stessi test con il protocollo FTP.

Abilitazione del servizio FTP Il servizio FTP è stato abilitato su Kali con il seguente comando:

```
sudo service vsftpd start
```

Dopo aver avviato il servizio, sono stati eseguiti i seguenti test di brute force.

Primo test: Brute force con username e password singoli

```
hydra -l "test_user" -p "kali" -t 64 127.0.0.1 ftp
```

- **-l "test_user"**: Username utilizzato per il test.
- **-p "kali"**: Password utilizzata per il test.
- **-t 64**: Aumenta il numero massimo di thread a 64 per velocizzare il test.
- **127.0.0.1**: Indirizzo IP della macchina target (loopback).
- **ftp**: Specifica il protocollo FTP.

Risultato: Il brute force ha avuto successo, confermando la validità del comando anche per il protocollo FTP.

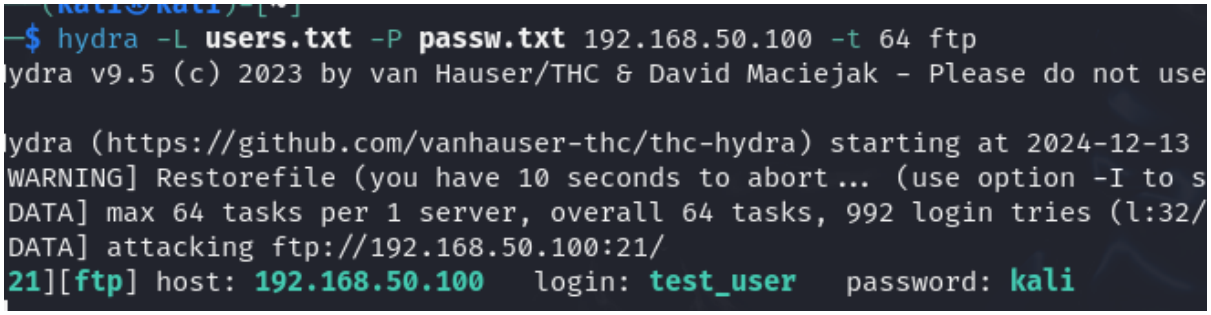
Secondo test: Brute force a dizionario Per il secondo test, è stato eseguito un attacco con dizionario utilizzando la wordlist **SecLists** preinstallata. Anche in questo caso, sono state utilizzate due liste personalizzate con 30 campi ciascuna per username e password.

Comando eseguito:

```
hydra -L usernames.txt -P passwords.txt -t 64 127.0.0.1 ftp
```

- **-L usernames.txt**: File di dizionario con la lista degli username (30 username).
- **-P passwords.txt**: File di dizionario con la lista delle password (30 password).
- **-t 64**: Aumenta il numero massimo di thread a 64 per aumentare la velocità.
- **127.0.0.1**: Indirizzo IP della macchina target (loopback).
- **ftp**: Specifica il protocollo FTP.

Risultato: L'attacco è stato completato con successo, dimostrando la funzionalità di Hydra anche per attacchi a dizionario su FTP.



4. Conclusione Il test ha dimostrato l'efficacia di Hydra per attacchi di brute force su SSH e FTP, sia con username e password singoli sia con dizionari personalizzati. L'utilizzo di parametri come **-t 64** ha migliorato le prestazioni, rendendo l'attacco più veloce. L'abilitazione dell'utente `test_user` con privilegi di root ha permesso una gestione più flessibile e l'utilizzo del loopback (127.0.0.1) ha consentito il test direttamente sulla macchina Kali.