Progetto S6/L5 - Authentication Cracking con Hydra su SSH e Telnet

1. Introduzione - Obiettivo

L'obiettivo del presente laboratorio è quello di comprendere il funzionamento degli attacchi di brute-force sull'autenticazione dei servizi di rete mediante l'utilizzo dello strumento Hydra, consolidando allo stesso tempo le competenze relative alla configurazione dei servizi stessi.

L'esercitazione è stata suddivisa in due parti principali: una prima fase guidata relativa alla configurazione e al cracking del servizio SSH, e una seconda fase autonoma nella quale è stato scelto e configurato il servizio Telnet per eseguire un'ulteriore sessione di attacco.

2. Ambiente di laboratorio

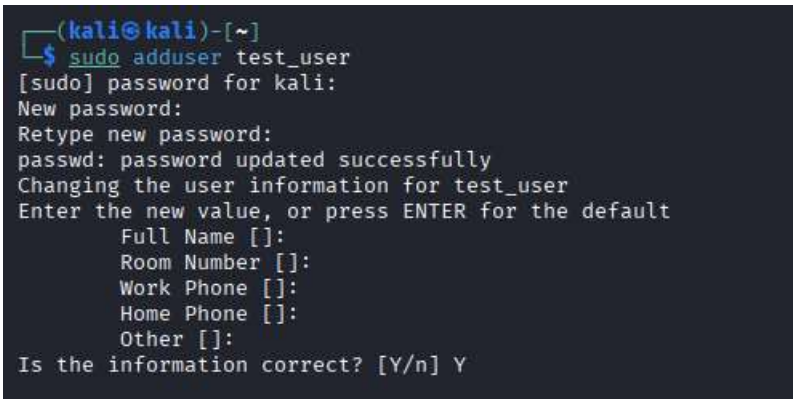
Il laboratorio è stato eseguito in ambiente virtualizzato utilizzando le seguenti componenti:

- **due macchine virtuali Kali Linux con ruoli distinti:**
    - **Kali Target:** sistema su cui sono stati configurati i servizi SSH e Telnet (IP Address:192.168.50.155)
    - **Kali Attacker**: sistema utilizzato per eseguire gli attacchi Hydra (IP Address:192.168.50.151)
- **Strumenti principali**:
    - Hydra
    - OpenSSH Server
    - Telnet Server (inetutils)
    - SecLists (wordlist)
- **Tipologia ambiente**: rete locale di laboratorio (+ pfsense per la comunicazione tra le due vm kali)

3. Creazione utente di test

È stato creato un account dedicato ai test:

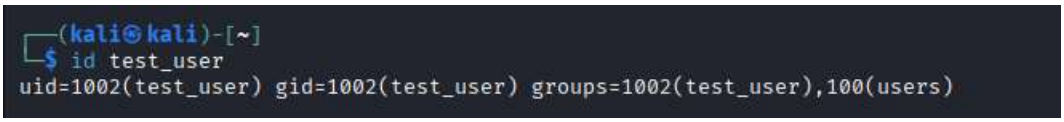
sudo adduser test_user



Output di creazione dell'utente test_user

Successivamente, è stata verificata la corretta creazione dell'utenza mediante il comando:

id test_user



Output di verifica della corretta creazione

L'output ha confermato la presenza dell'utente nel sistema, mostrando l'assegnazione dell'UID, del GID e dei gruppi associati.
Questa verifica è stata effettuata per assicurare che l'account fosse correttamente registrato nel sistema prima di procedere con la fase di autenticazione remota e di brute-force tramite Hydra.

4. Installazione delle wordlist SecLists

Prima di procedere con la fase di brute-force è stato installato il pacchetto SecLists, contenente collezioni di dizionari comunemente utilizzati nei test di sicurezza per attacchi di autenticazione.

L'installazione è stata eseguita tramite il gestore di pacchetti:

sudo apt install seclists

Al termine dell'installazione è stata verificata la corretta presenza delle wordlist nel percorso standard:

/usr/share/seclists/

Le directory relative a Usernames e Passwords sono state successivamente utilizzate per la selezione dei dizionari impiegati durante le fasi di attacco con Hydra.

Output di installazione e relative presenze nel suddetto path indicato

5. Parte 1 — Configurazione e cracking del servizio SSH

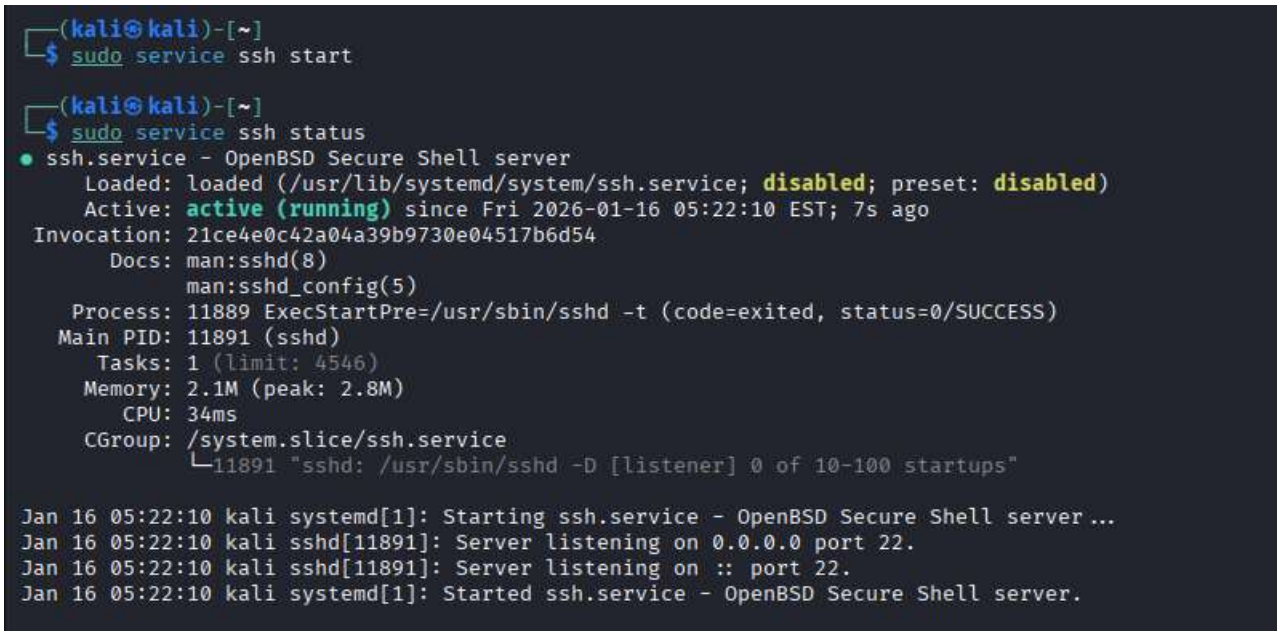
5.1 Avvio del servizio SSH

Il servizio SSH è stato avviato tramite:

sudo service ssh start

Successivamente si è verificata l'attivazione del servizio tramite:

sudo service ssh status



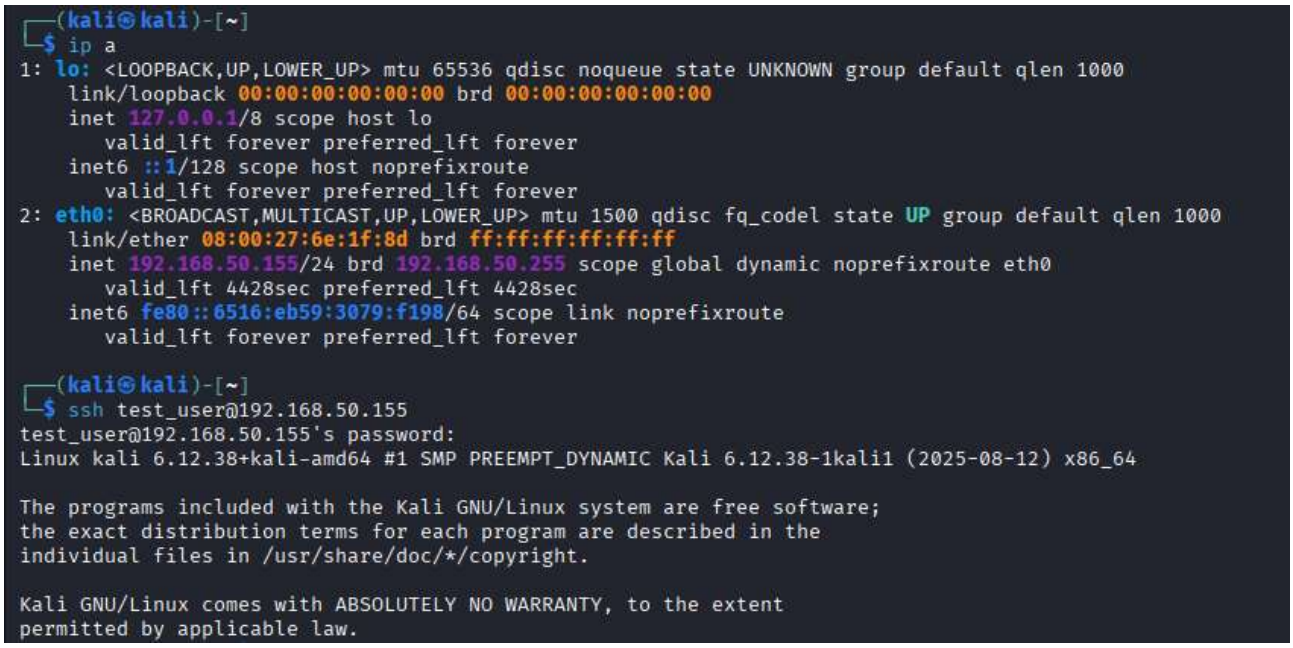
Output atteso in fase di attivazione e verifica del servizio SSH

5.2 Verifica manuale accesso SSH

È stata verificata la corretta funzionalità del servizio mediante:

ssh test_user@192.168.50.155

Il login è avvenuto con successo, confermando la corretta configurazione del servizio.



Output di avvenuto accesso tramite SSH

5.3 Attacco Hydra su SSH

Per l'attacco è stato utilizzato Hydra con numero limitato di thread al fine di mantenere stabilità del servizio:

hydra -V -L multiplesources-usernames.txt -P most-popular-passwords.txt 192.168.50.155 -t 2 ssh

La scelta di -t 2 è stata effettuata per evitare sovraccarico del servizio SSH, che utilizza handshake crittografico.

Nota sulla riduzione delle wordlist utilizzate

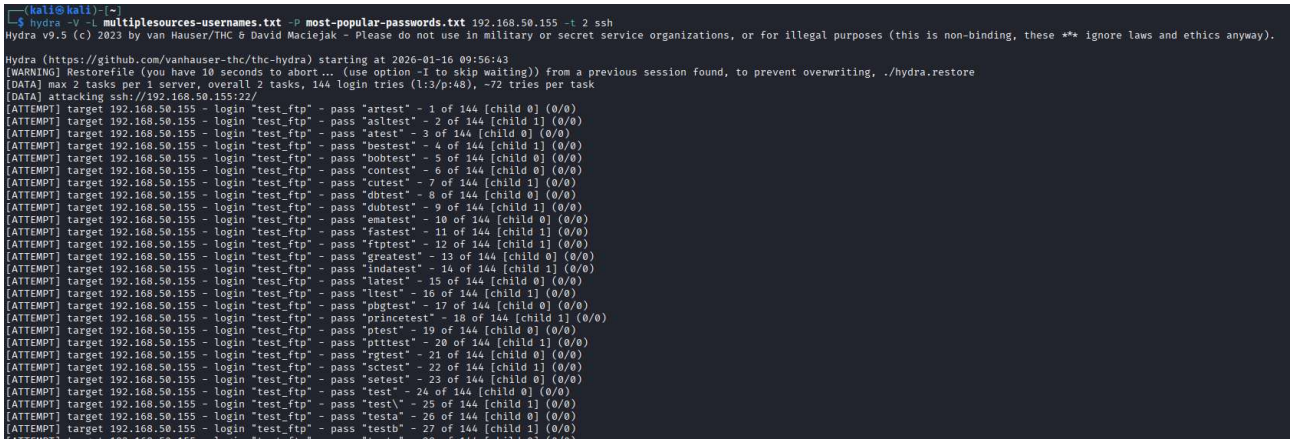
Al fine di mantenere tempi di esecuzione compatibili con le tempistiche di laboratorio e con la consegna dell'esercitazione, le wordlist utilizzate per l'attacco SSH sono state preventivamente ridotte.

In particolare:

- il file multiplesources-usernames.txt è stato ridotto a 3 username
- il file most-popular-passwords.txt è stato ridotto a 48 password

Questa operazione ha permesso di limitare il numero totale di combinazioni testate, mantenendo comunque una base dati rappresentativa per la dimostrazione del funzionamento dell'attacco di brute-force.

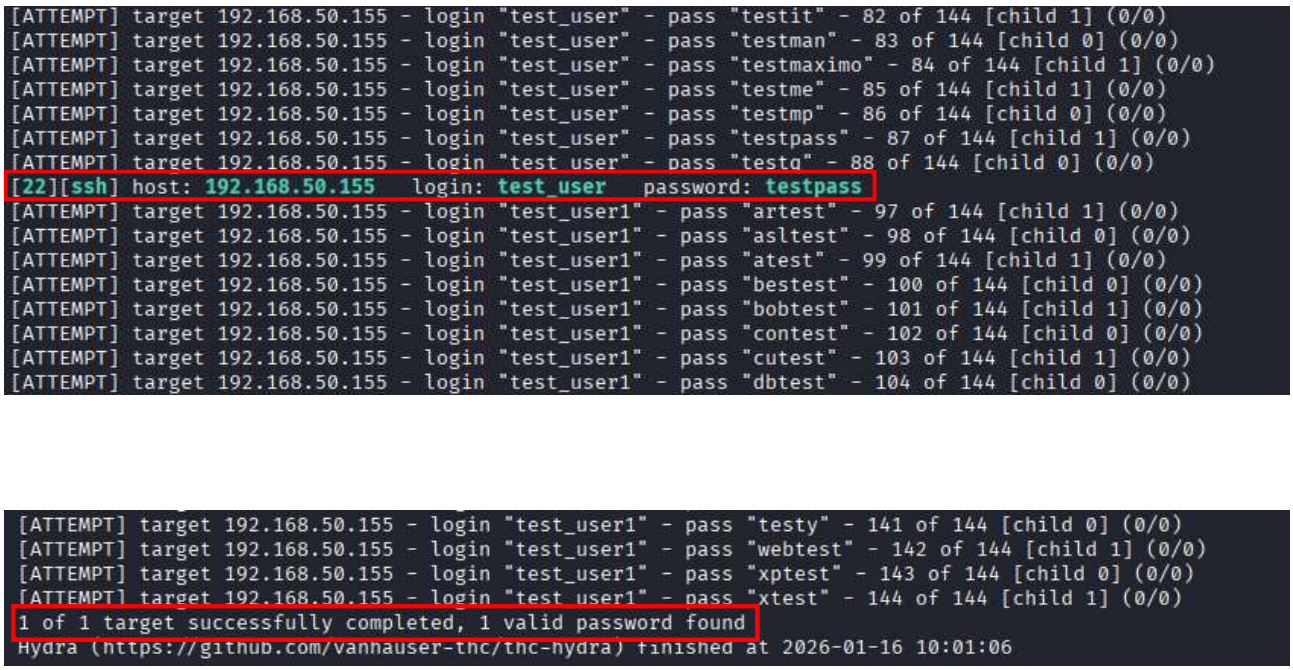
La scelta di ridurre i dizionari è coerente con le buone pratiche di laboratorio, dove l'obiettivo principale è la validazione del processo di attacco piuttosto che l'esecuzione di brute-force estesi su dataset completi.



Avvio di hydra sull'indirizzo target

5.4 Risultati SSH

Hydra ha individuato correttamente le credenziali valide, dimostrando la vulnerabilità dei servizi esposti in presenza di password deboli o prevedibili.



Risultato di hydra sull'esito del brute force

6. Parte 2 — Configurazione e cracking del servizio Telnet

6.1 Installazione del servizio Telnet

Poiché il demone Telnet non risulta installato di default su Kali Linux per motivi di sicurezza, è stato necessario procedere all'installazione manuale del pacchetto server.

L'installazione è stata effettuata tramite:

sudo apt install telnetd

Questo comando ha installato i componenti necessari, inclusi inetutils-inetd e il demone telnetd, utilizzati per la gestione dei servizi legacy in modalità on-demand.

6.2 Abilitazione servizio Telnet

Il servizio Telnet non risulta attivo di default su Kali per motivi di sicurezza. È stato quindi necessario abilitarlo manualmente tramite configurazione del file:

/etc/inetd.conf

Abilitando manualmente la seguente voce:

telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin/telnetd

Successivamente è stato riavviato il servizio inetd:

sudo systemctl restart inetutils-inetd

6.3 Verifica apertura porta Telnet

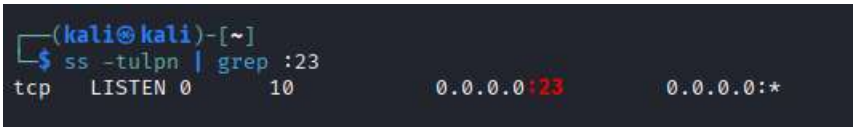
La corretta esposizione del servizio è stata verificata tramite:

ss -tulpn | grep :23

Risultato:

tcp LISTEN 0 10 0.0.0.0:23 0.0.0.0:*

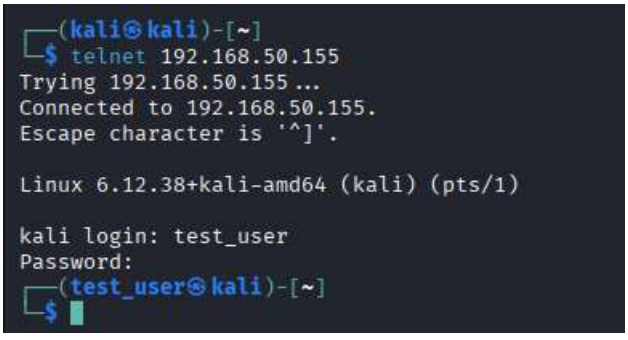
Questo output conferma che il servizio Telnet risulta in ascolto sulla porta standard 23.



6.4 Test manuale di connessione Telnet

Prima di procedere con l'attacco automatico è stato effettuato un test manuale dal sistema attacker:

telnet 192.168.50.155

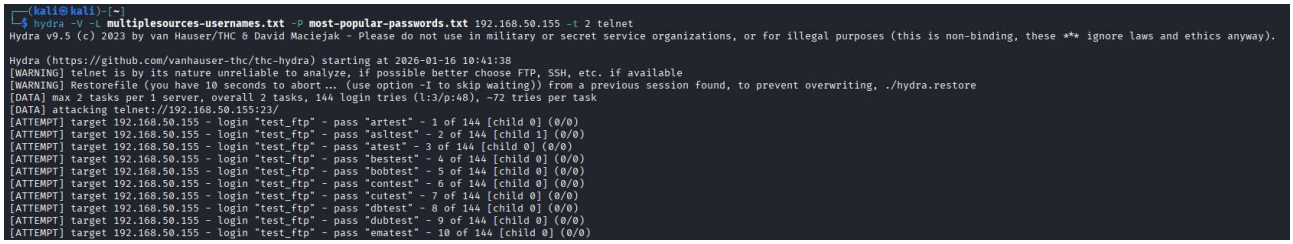


Il prompt di login è stato visualizzato correttamente, confermando la raggiungibilità del servizio.

6.5 Attacco Hydra su Telnet

L'attacco Telnet è stato eseguito dalla seconda macchina Kali utilizzando Hydra:

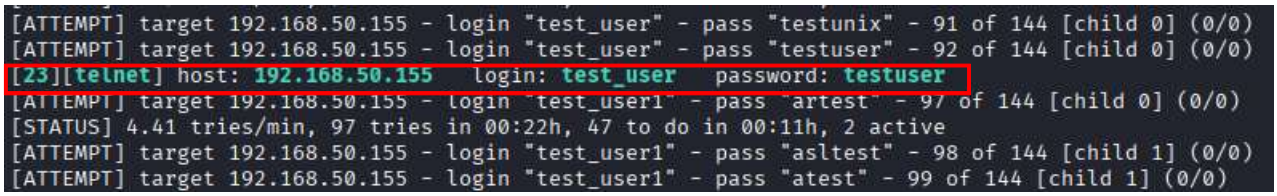
hydra -V -L multiplesources-usernames.txt -P most-popular-passwords.txt 192.168.50.155 -t 2 telnet

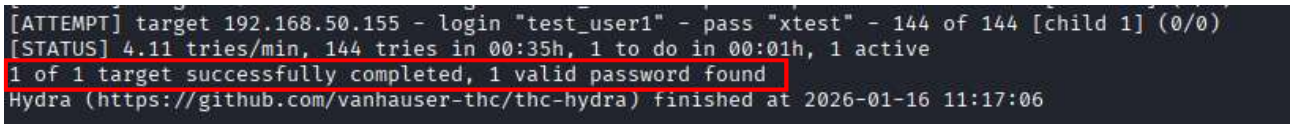


Screenshot del comando di avvio di hydra sul target

6.6 Risultati Telnet

Hydra ha individuato correttamente le credenziali valide.





7. Conclusioni

L'attività di laboratorio ha permesso di testare in modo pratico l'utilizzo dello strumento Hydra per l'esecuzione di attacchi di autenticazione sui servizi SSH e Telnet, partendo dalla configurazione dei servizi target fino alla fase di esecuzione degli attacchi automatizzati.

Durante l'esercitazione sono stati osservati tempi di esecuzione differenti in base al servizio analizzato e alla configurazione adottata, evidenziando come le prestazioni dell'attacco siano influenzate da molteplici fattori, tra cui il protocollo utilizzato, il numero di thread impostati, la gestione delle connessioni da parte del servizio e la

dimensione delle wordlist impiegate.

Il laboratorio ha inoltre consentito di comprendere l'importanza della fase di preparazione dell'ambiente, che include l'installazione e l'abilitazione dei servizi, la verifica manuale della raggiungibilità e il controllo dello stato delle porte di rete prima dell'avvio delle attività di test.

Nel complesso, l'esercitazione ha fornito una panoramica operativa sul funzionamento degli attacchi di brute-force e sull'interazione tra strumenti di attacco e servizi di rete, contribuendo a consolidare le competenze pratiche nell'ambito della sicurezza dei sistemi.