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

1. Introduzione - Obiettivo

L'obiettivo del presente laboratorio è analizzare in modo pratico il comportamento degli attacchi di brute-force sui meccanismi di autenticazione di servizi di rete, utilizzando lo strumento Hydra come framework di attacco automatizzato.
L'attività è finalizzata a comprendere non solo l'esecuzione operativa dell'attacco, ma anche l'impatto delle caratteristiche protocollari dei servizi target sulle prestazioni e sull'efficacia del brute-force.

Il laboratorio è stato strutturato in due fasi principali:

- una prima fase guidata dedicata alla configurazione e al test del servizio SSH;
- una seconda fase autonoma incentrata sulla configurazione del servizio Telnet e sull'esecuzione di un attacco comparativo.

Attraverso il confronto tra SSH e Telnet, l'esercitazione mira a evidenziare le differenze operative tra protocolli moderni e legacy, analizzando aspetti quali la gestione delle connessioni, la latenza di autenticazione e il comportamento degli strumenti di attacco in scenari reali di test controllato.

2. Ambiente di laboratorio

Il laboratorio è stato eseguito in un ambiente virtualizzato isolato, progettato per simulare uno scenario di rete controllato e riproducibile, evitando interferenze con reti esterne e garantendo sicurezza operativa durante le attività di test.

La topologia del laboratorio è composta da:

- **Kali Linux – Target**
  Sistema destinato all'esposizione dei servizi vulnerabili oggetto di test.
  Indirizzo IP: 192.168.50.155
  Servizi configurati:
  - OpenSSH Server
  - Telnet Server (inetutils)
- **Kali Linux – Attacker**
  Sistema utilizzato per l'esecuzione degli attacchi di brute-force tramite Hydra.
  Indirizzo IP: 192.168.50.151

- **Infrastruttura di rete**
  Le due macchine virtuali sono collegate tramite una rete locale di laboratorio con supporto pfSense per la gestione del traffico e dell'instradamento tra le interfacce virtuali.

- **Strumenti principali utilizzati**:

  - Hydra (tool di attacco brute-force)
  - SecLists (repository di wordlist)
  - OpenSSH Server
  - Telnet Server (inetutils)

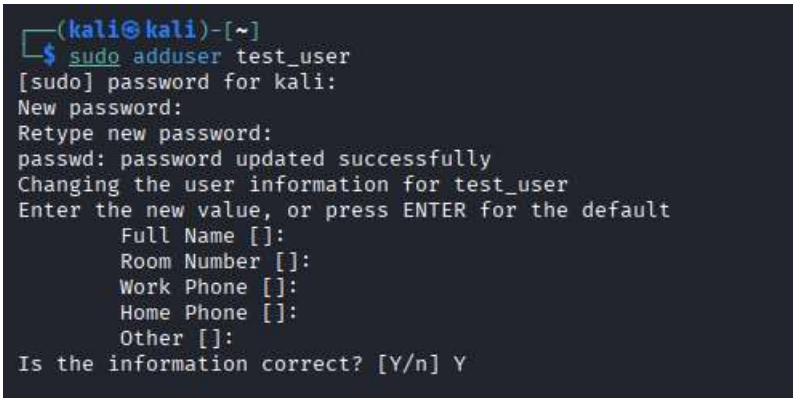
L'utilizzo di un ambiente virtualizzato ha consentito di replicare scenari reali di esposizione dei servizi, mantenendo al contempo il pieno controllo delle configurazioni e delle condizioni operative del test.

3. Creazione utente di test

Per garantire condizioni di test controllate e riproducibili, è stato creato un account dedicato esclusivamente alle attività di laboratorio, utilizzato come target per le operazioni di autenticazione remota e brute-force.

La creazione dell'utente è stata effettuata tramite il comando:

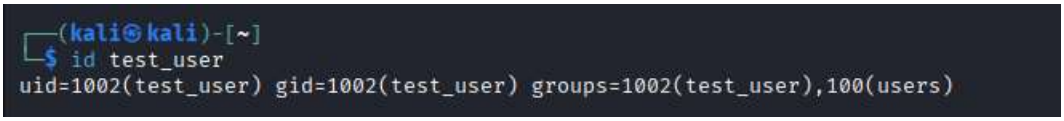
sudo adduser test_user



Output del comando adduser relativo alla creazione dell'account dedicato ai test di autenticazione

Successivamente è stata verificata la corretta registrazione dell'account nel sistema attraverso il comando:

id test_user



Output di conferma dell'assegnazione di UID, GID e gruppi per l'utente di test

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 stata effettuata la preparazione dell'ambiente di attacco, installando il repository SecLists, contenente collezioni di dizionari comunemente utilizzati nei test di sicurezza per attacchi di autenticazione.

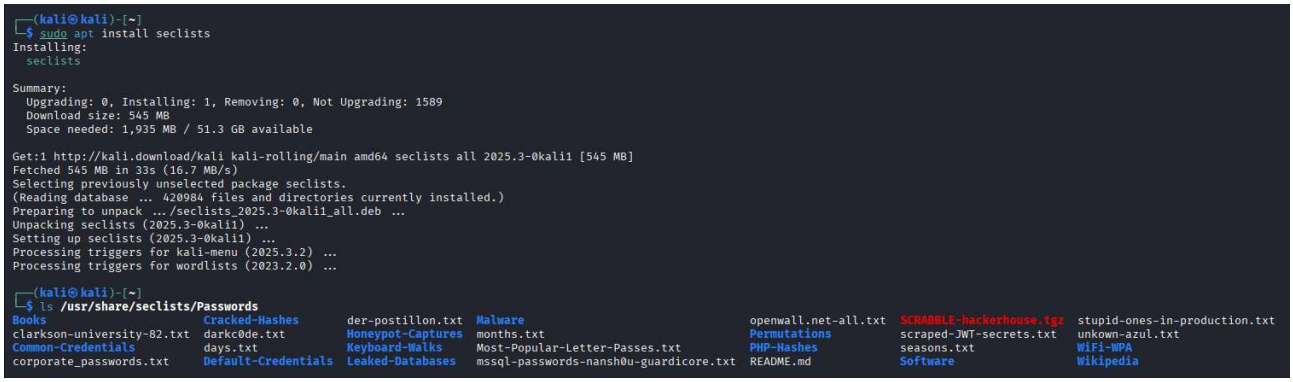
L'installazione è stata eseguita tramite il gestore di pacchetti:

sudo apt install seclists

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

/usr/share/seclists/

All'interno del repository sono state selezionate le directory relative a **Usernames** e **Passwords**, successivamente utilizzate come base dati per gli attacchi di autenticazione automatizzati con Hydra.



Verifica della presenza delle wordlist SecLists nel percorso standard /usr/share/seclists/ dopo l'installazione del pacchetto

5. Parte 1 — Configurazione e cracking del servizio SSH

5.1 Avvio del servizio SSH

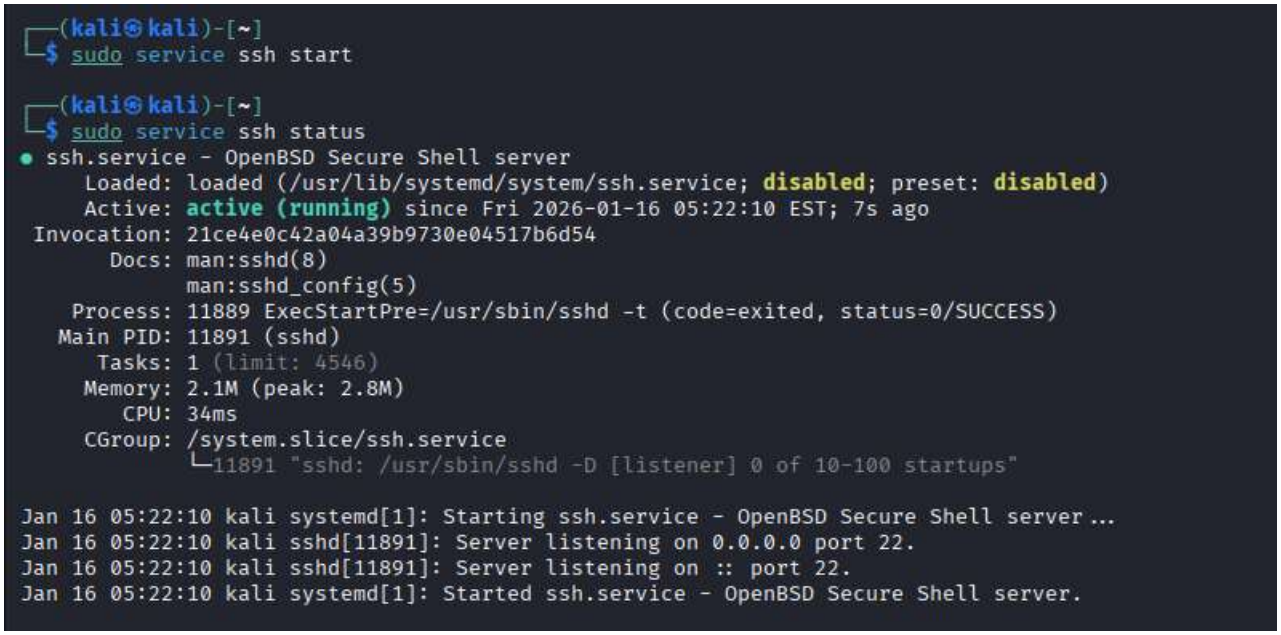
Il servizio OpenSSH Server è stato avviato sul sistema target tramite il comando:

sudo service ssh start

Successivamente è stato verificato lo stato del servizio per accertarne la corretta esecuzione:

sudo service ssh status

La verifica dello stato operativo del servizio è stata eseguita per assicurare che la porta SSH fosse attiva e pronta a ricevere connessioni remote prima di procedere con le fasi di test.



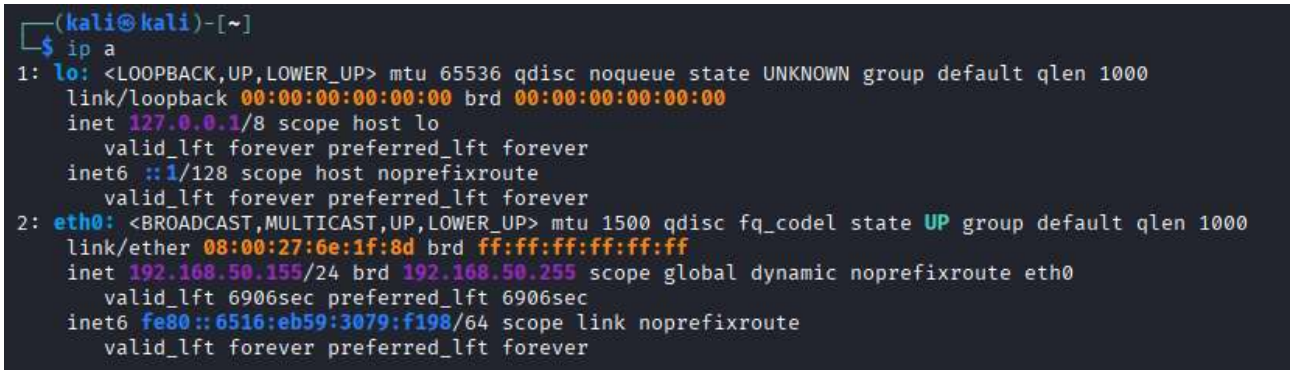
Output del comando di status che conferma l'attivazione del servizio OpenSSH Server sul sistema target

5.2 Verifica manuale accesso SSH

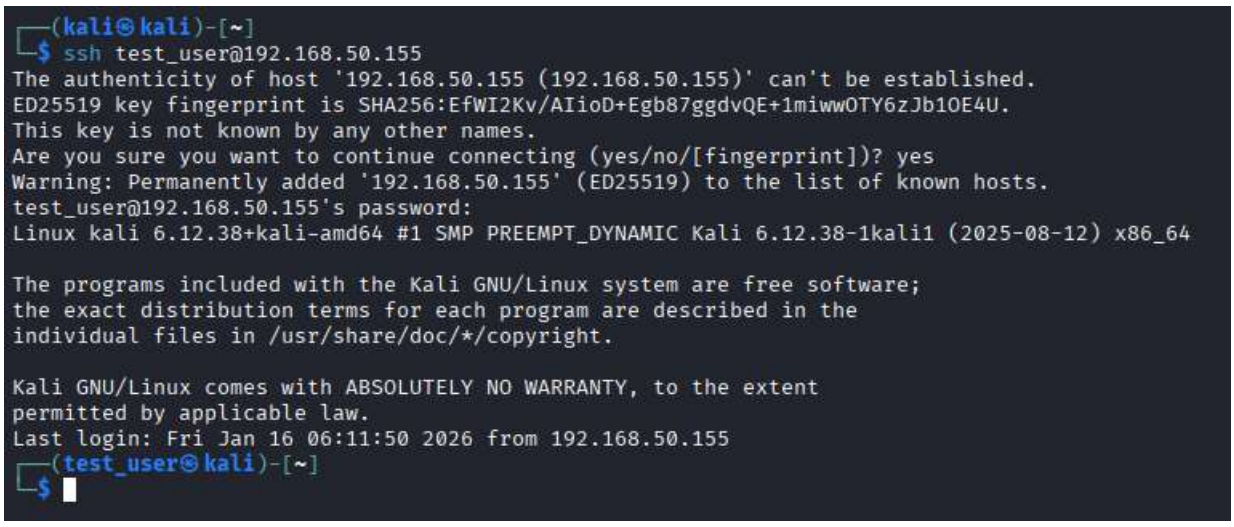
Prima dell'esecuzione dell'attacco automatizzato è stata effettuata una connessione manuale dal sistema attacker:

ssh test_user@192.168.50.155

L’accesso è avvenuto correttamente, confermando la raggiungibilità del servizio e la validità delle credenziali di test.
Questa fase preliminare consente di validare la configurazione del servizio ed evitare falsi negativi durante l’esecuzione dell’attacco brute-force.



Output del comando ip a utilizzato per confermare l’indirizzamento di rete del sistema target



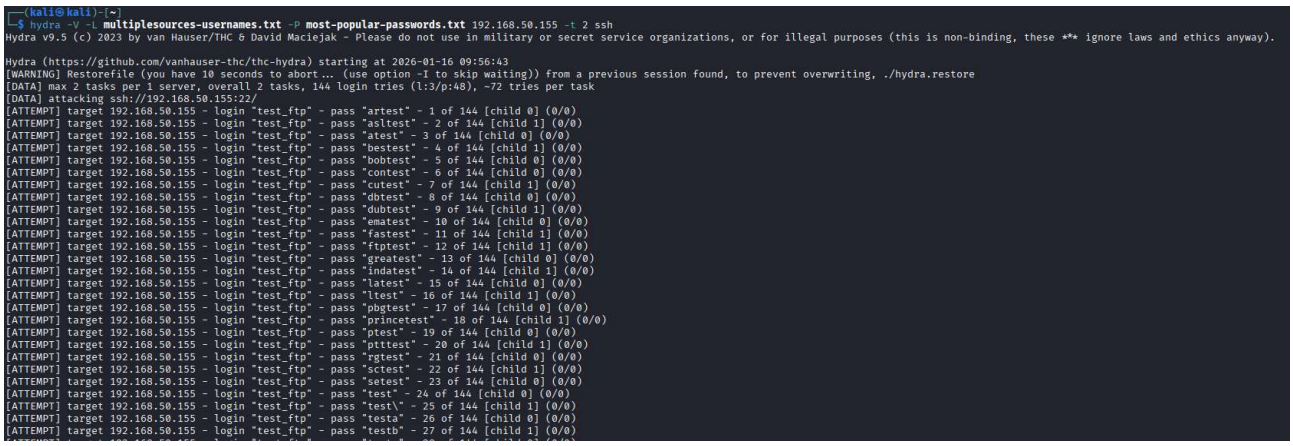
Test di autenticazione remota SSH effettuato dal sistema attacker per validare la corretta configurazione del servizio prima dell’esecuzione dell’attacco automatizzato

5.3 Attacco Hydra su SSH

L’attacco di brute-force è stato eseguito utilizzando Hydra con un numero limitato di thread, al fine di mantenere stabilità del servizio target e ridurre il rischio di saturazione delle connessioni concorrenti:

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

La scelta di utilizzare un basso livello di parallelizzazione (-t 2) è stata effettuata per simulare un comportamento più realistico di attacco controllato e per evitare eventuali meccanismi di limitazione delle connessioni da parte del servizio SSH.



Esecuzione del comando Hydra per l'attacco di autenticazione SSH sul sistema target con configurazione controllata dei thread

Nota sulla riduzione delle wordlist utilizzate

Al fine di mantenere tempi di esecuzione compatibili con le tempistiche di laboratorio e con i vincoli della consegna, 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**

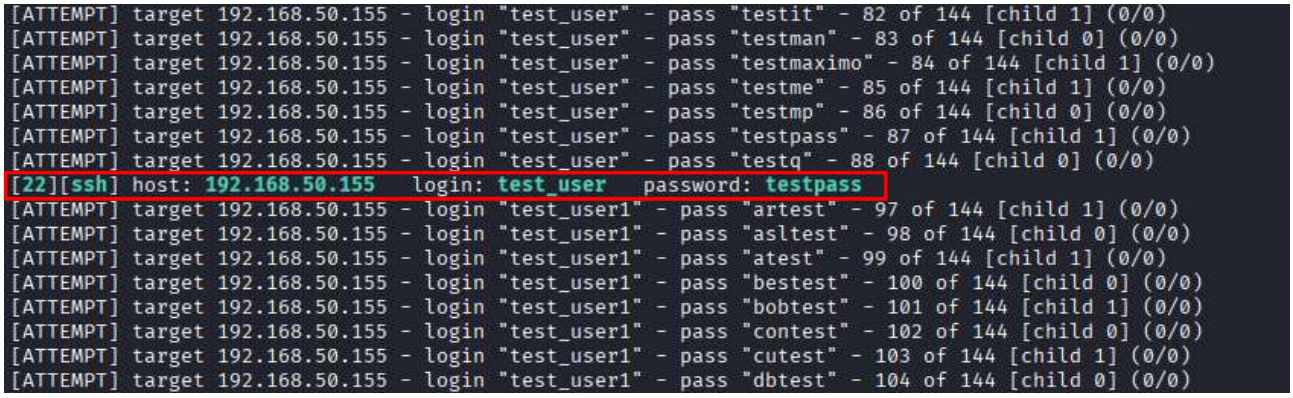
Questa operazione ha consentito di limitare il numero totale di combinazioni testate, mantenendo una base dati sufficiente per dimostrare il funzionamento del meccanismo di brute-force e il comportamento dello strumento Hydra.

La scelta rispecchia una pratica comune nei contesti di laboratorio e di test controllato, dove l'obiettivo principale è la validazione del processo di attacco e dell'interazione tra strumento e servizio target, piuttosto che l'esecuzione di campagne di brute-force estese su dataset completi, tipiche invece di scenari reali non vincolati da limiti temporali.

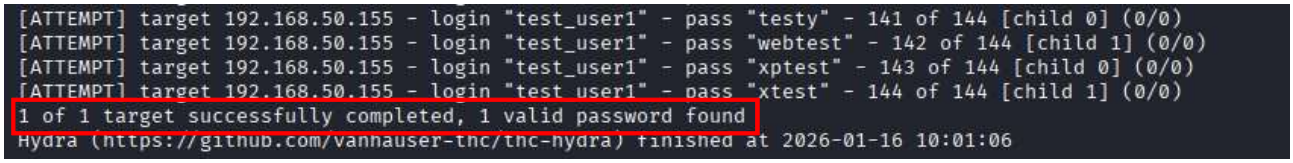
5.4 Risultati dell'attacco SSH

L'attacco ha portato all'individuazione corretta delle credenziali valide dell'utente di test.
Questo risultato dimostra come l'assenza di contromisure quali politiche di password robuste, limitazione dei tentativi di autenticazione (rate limiting), blocco temporaneo degli account e autenticazione multifattore renda il servizio vulnerabile ad attacchi di forza bruta.

L’esito positivo dell’attacco conferma inoltre l’efficacia degli strumenti automatizzati nel contesto di servizi esposti in rete e sottolinea l’importanza dell’adozione di misure di hardening sui servizi SSH in ambienti di produzione.



Avanzamento dell’attacco automatizzato SSH con visualizzazione dei tentativi di autenticazione in corso e identificazione delle credenziali dell’utente target



Esito positivo dell’attacco di brute-force SSH

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. Questa scelta riflette la natura obsoleta e insicura del protocollo, che viene normalmente disabilitato nei sistemi moderni.

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.

Durante la fase di installazione il sistema ha richiesto la conferma per il riavvio automatico dei servizi che dipendono da librerie di sistema critiche, quali libc, libpam e libssl.
Questa richiesta è dovuta al fatto che alcuni processi in esecuzione potrebbero continuare a utilizzare versioni precedenti delle librerie aggiornate.

Nell'ambiente di laboratorio è stata accettata l'opzione di riavvio automatico dei servizi al fine di garantire la coerenza delle dipendenze runtime e prevenire eventuali comportamenti anomali durante le successive fasi di test.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install telnetd
[sudo] password for kali:
Upgrading:
  inetutils-telnet  libc-bin  libc-dev-bin  libc-l10n  libc6  libc6-dev  libc6-i386  locales

Installing:
  telnetd

Installing dependencies:
  inetutils-inetd  inetutils-telnetd  libc-gconv-modules-extra  tcpd

Summary:
  Upgrading: 8, Installing: 5, Removing: 0, Not Upgrading: 1581
  Download size: 13.4 MB
  Space needed: 2,357 kB / 49.4 GB available

Continue? [Y/n] Y
Get:2 http://kali.download/kali kali-rolling/main amd64 libc-l10n all 2.42-5 [749 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 locales all 2.42-5 [3,927 kB]
Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 libc-gconv-modules-extra amd64 2.42-5 [1,127 kB]
Get:9 http://kali.mirror.garr.it/kali kali-rolling/main amd64 tcpd amd64 7.6.q-36 [23.5 kB]
Get:10 http://kali.mirror.garr.it/kali kali-rolling/main amd64 inetutils-inetd amd64 2:2.7-1 [81.5 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libc6 amd64 2.42-5 [1,888 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libc-bin amd64 2.42-5 [674 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libc6-i386 amd64 2.42-5 [2,557 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libc-dev-bin amd64 2.42-5 [60.3 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 libc6-dev amd64 2.42-5 [2,091 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 inetutils-telnet amd64 2:2.7-1 [127 kB]
Get:12 http://kali.download/kali kali-rolling/main amd64 inetutils-telnetd amd64 2:2.7-1 [103 kB]
Get:13 http://http.kali.org/kali kali-rolling/main amd64 telnetd all 0.17+2.7-1 [40.1 kB]
Fetched 13.4 MB in 5s (2,899 kB/s)
Preconfiguring packages ...
(Reading database ... 427306 files and directories currently installed.)
```

Fase di installazione del servizio Telnet con risoluzione automatica delle dipendenze e aggiornamento delle librerie di base del sistema

Prompt di gestione delle dipendenze di sistema (libc, PAM, SSL) visualizzato durante l'installazione del servizio Telnet

6.2 Abilitazione servizio Telnet

Dopo l'installazione, il servizio Telnet non risulta attivo di default su Kali per motivi di sicurezza. È stato quindi necessario abilitarlo manualmente tramite configurazione del file:

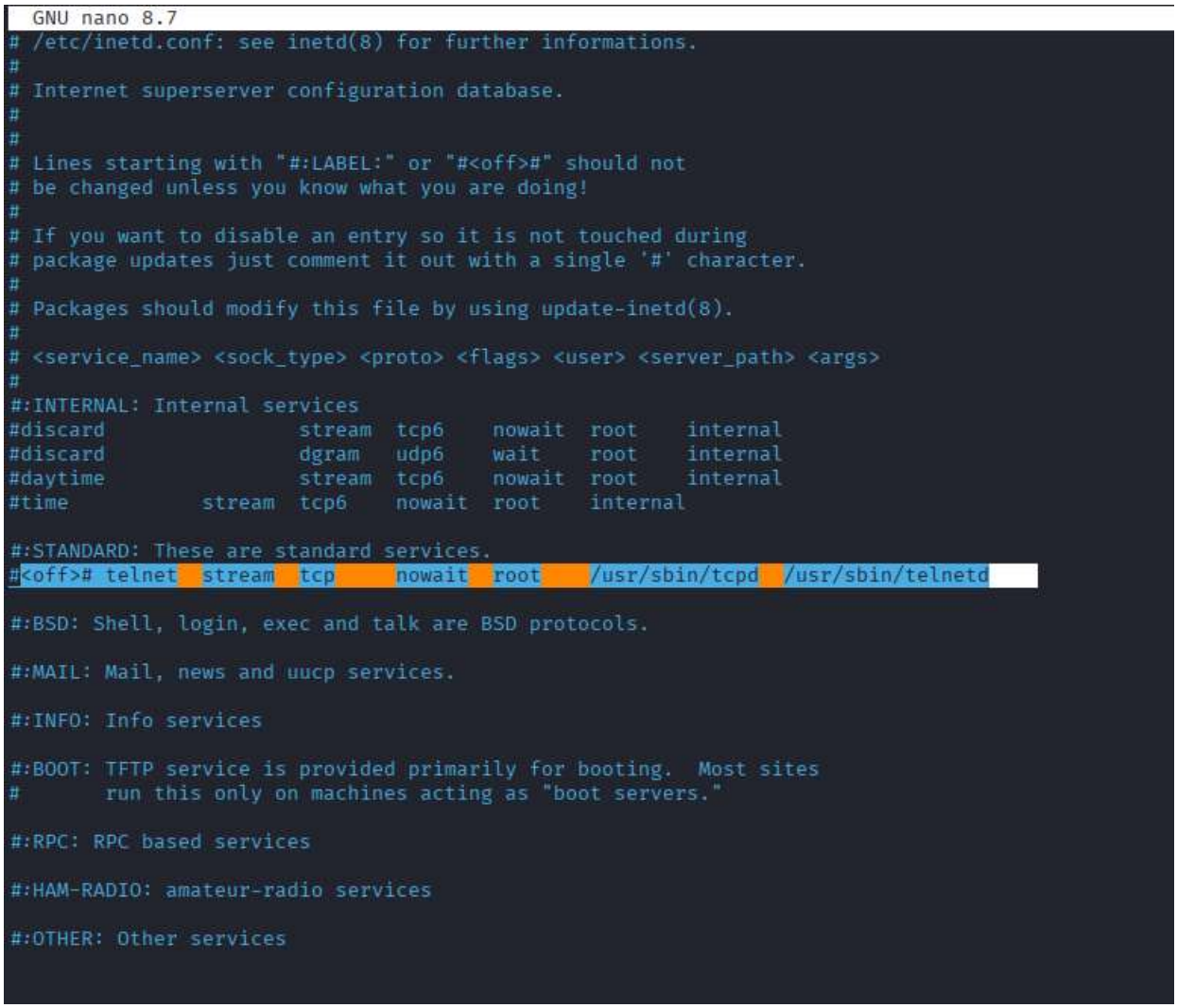
/etc/inetd.conf

Abilitando manualmente la seguente voce:

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

Successivamente è stato riavviato il servizio inetd per applicare le modifiche:

sudo systemctl restart inetutils-inetd



Abilitazione del demone Telnet mediante rimozione del commento della voce di servizio nel file /etc/inetd.conf

6.3 Verifica apertura porta Telnet

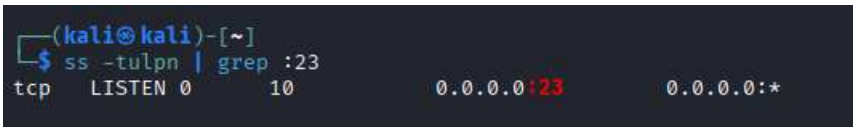
La corretta esposizione del servizio è stata verificata tramite:

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.

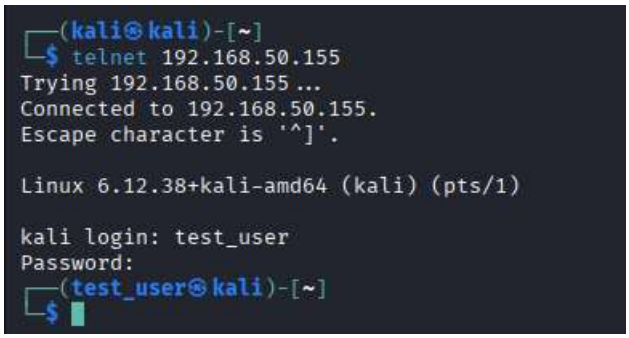


Output del comando ss -tulpn che conferma l'apertura della porta TCP 23 e l'associazione al servizio Telnet

6.4 Test manuale di connessione Telnet

Prima dell'esecuzione dell'attacco automatizzato è stato effettuato un test manuale di connessione dal sistema attacker:

telnet 192.168.50.155



Test di accesso Telnet con visualizzazione del prompt di autenticazione sul sistema target

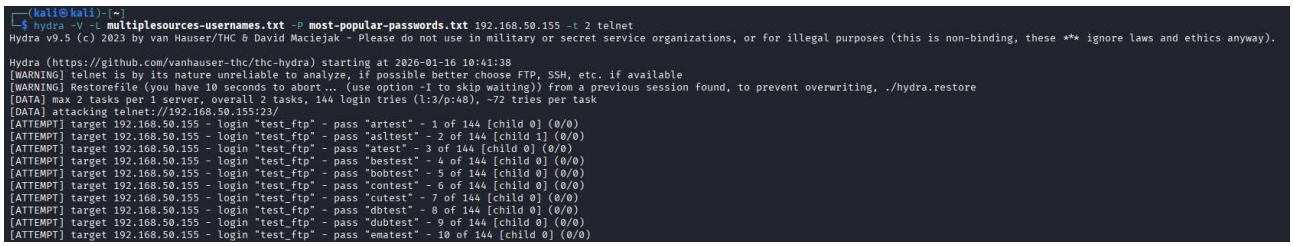
Il prompt di login è stato visualizzato correttamente, confermando la raggiungibilità del servizio.

6.5 Attacco Hydra su Telnet

L'attacco di brute-force è stato eseguito utilizzando Hydra con gli stessi dataset di username e password impiegati per il test SSH, al fine di mantenere condizioni sperimentali comparabili:

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

È stato mantenuto lo stesso livello di parallelizzazione (-t 2) per consentire un confronto coerente delle prestazioni tra i due protocolli.

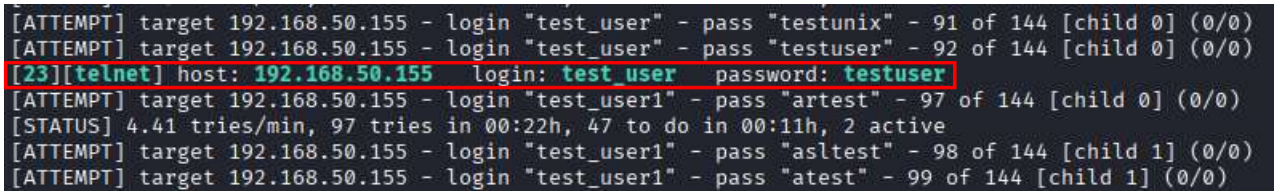


Avvio dell'attacco di brute-force sul servizio Telnet tramite Hydra dal sistema attacker

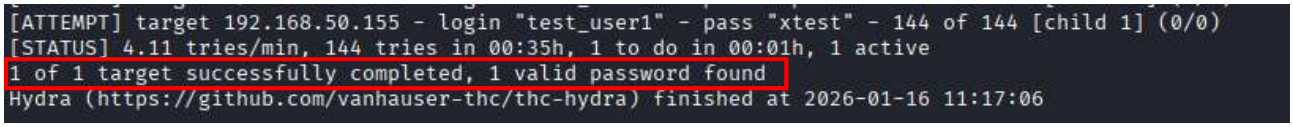
6.6 Risultati dell'attacco Telnet

L'attacco ha portato all'individuazione corretta delle credenziali valide anche per il servizio Telnet.
Durante l'esecuzione è stato osservato un tempo complessivo di attacco superiore rispetto al servizio SSH, nonostante l'utilizzo dello stesso dataset di credenziali e della medesima configurazione di Hydra.

Questa differenza è attribuibile alle caratteristiche del protocollo Telnet, che utilizza un modello di comunicazione interattivo basato su prompt testuali e negoziazione delle opzioni di sessione (Telnet option negotiation), aumentando la latenza per singolo tentativo di autenticazione rispetto al flusso più strutturato di SSH.



Avanzamento dell'attacco automatizzato Telnet con visualizzazione dei tentativi di autenticazione in corso e identificazione delle credenziali dell'utente target



Esito positivo dell'attacco di brute-force Telnet

7. Conclusioni

L'attività di laboratorio ha consentito di analizzare in modo pratico il comportamento degli attacchi di brute-force sui servizi di autenticazione SSH e Telnet, partendo dalla configurazione controllata dell'ambiente fino all'esecuzione degli attacchi automatizzati tramite Hydra.

I risultati ottenuti hanno evidenziato come entrambi i servizi risultino vulnerabili in

assenza di adeguate contromisure di sicurezza, quali politiche di password robuste, meccanismi di limitazione dei tentativi di autenticazione (rate limiting), blocco temporaneo degli account e autenticazione multifattore.

Dal confronto tra i due protocolli è emersa una differenza significativa nei tempi di esecuzione dell'attacco. In particolare, il servizio Telnet ha mostrato una maggiore latenza complessiva rispetto a SSH, nonostante l'utilizzo dello stesso dataset di credenziali e della medesima configurazione di Hydra. Tale comportamento è attribuibile alla natura interattiva del protocollo Telnet, basata su prompt testuali e negoziazione delle opzioni di sessione, che introduce un overhead per ogni tentativo di autenticazione. Al contrario, SSH, pur implementando meccanismi di cifratura e handshake crittografico, presenta un flusso di autenticazione più strutturato e maggiormente ottimizzato per l'automazione.

Il laboratorio ha inoltre evidenziato l'elevato rischio operativo associato all'utilizzo di protocolli legacy come Telnet, che oltre a risultare vulnerabili al brute-force trasmettono le credenziali in chiaro, rendendo possibile l'intercettazione passiva del traffico di autenticazione.

Nel complesso, l'esercitazione ha permesso di comprendere non solo il funzionamento operativo degli strumenti di attacco, ma anche l'importanza della corretta configurazione dei servizi di rete e dell'adozione di misure di hardening come elemento fondamentale per la protezione dei sistemi esposti.