S6.L4 Le fasi di exploit/gli attacchi di rete

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

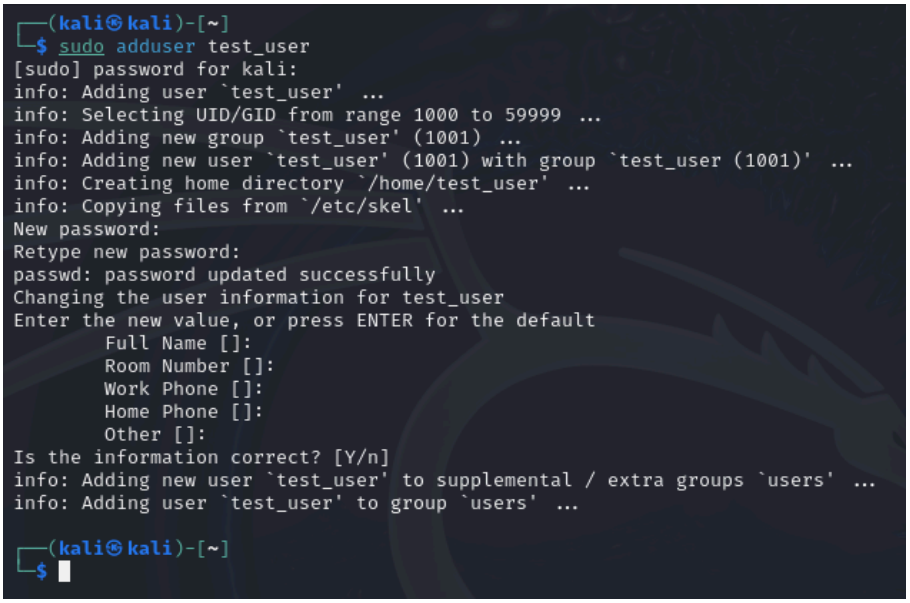
L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

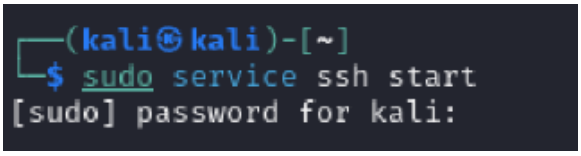
Fase 1: creazione test_user_

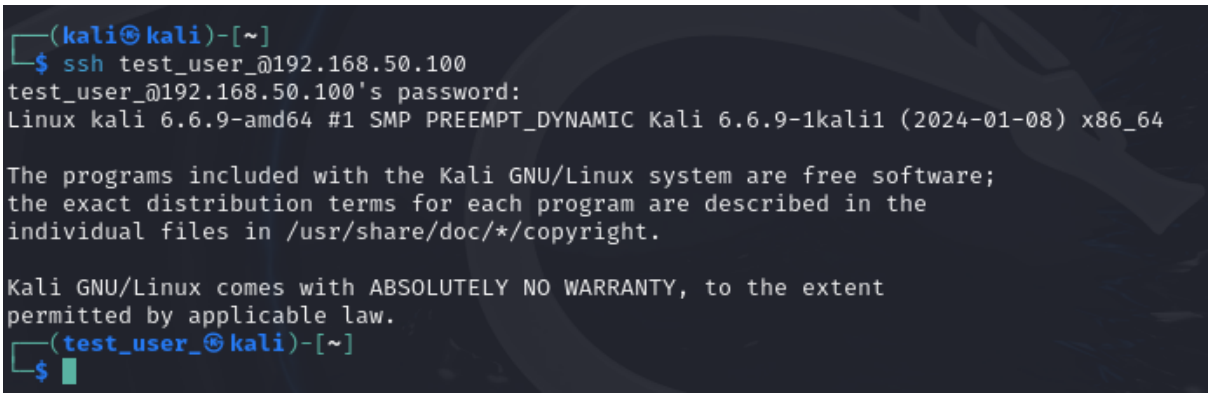
Obiettivo della Fase 1:
Creare un nuovo utente nel sistema che può essere utilizzato per testare l'autenticazione dei servizi di rete.
Dettagli:

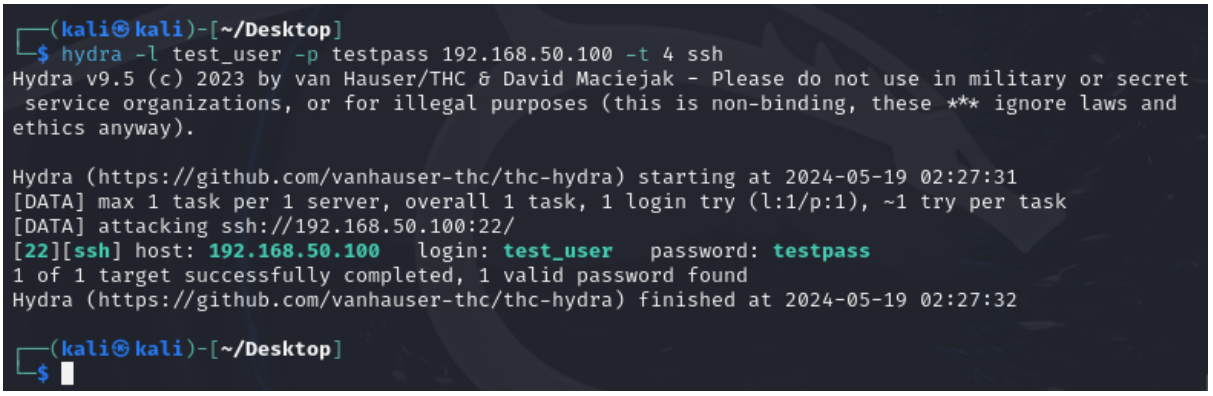
- Ho creato un utente chiamato test_user e ho configurato la sua password.
- L'utente è stato aggiunto ai gruppi appropriati per avere i permessi necessari.
- Questo utente sarà utilizzato nelle successive fasi dell'esercizio, in particolare per testare l'autenticazione con Hydra e altri strumenti.



Fase 2: Configurazione e cracking SSH







Obiettivo della Fase 2:
Configurare e testare il servizio SSH e successivamente utilizzare Hydra per eseguire un attacco di forza bruta sull'autenticazione SSH.
Dettagli:

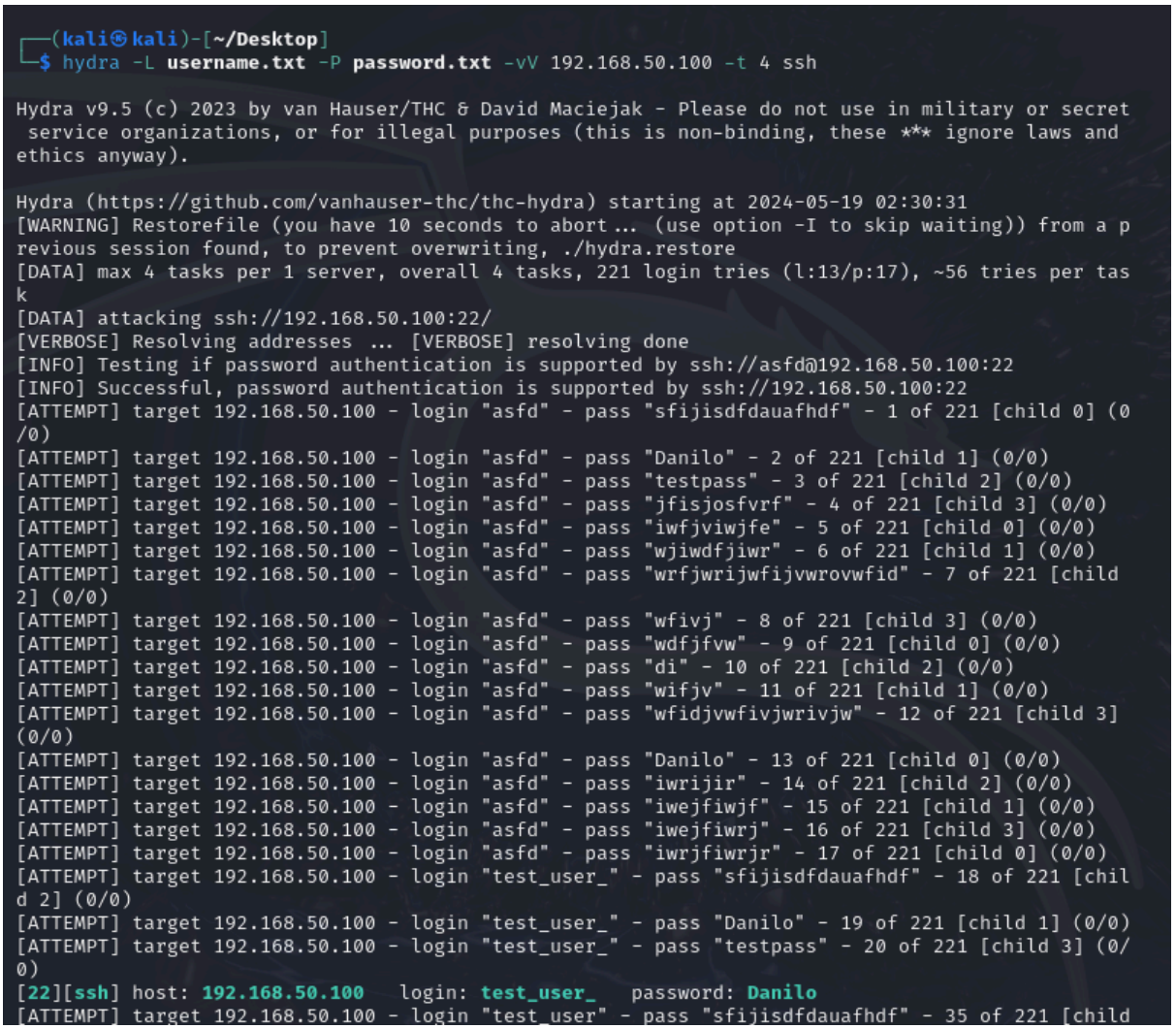
1. Configurazione del Servizio SSH:
    - Ho avviato il servizio SSH sul tuo sistema Kali Linux per permettere le connessioni remote.
    - Ho testato la configurazione effettuando una connessione SSH utilizzando l'utente test_user e la sua password, confermando che il servizio è operativo.

2. Attacco di Forza Bruta con Hydra:
    - Ho utilizzato Hydra, uno strumento di cracking delle password, per eseguire un attacco di forza bruta sull'autenticazione SSH del server 192.168.50.100.
    - Hydra ha tentato di autenticarsi utilizzando le credenziali fornite (test_user e testpass) e ha avuto successo.

Prossimi Passaggi

- Ulteriori Test con Hydra: Potrei voler provare Hydra con diverse liste di username e password per vedere come varia l'efficacia degli attacchi.
- Esplorazione di Altri Servizi di Rete: Considero di configurare e testare altri servizi di rete (es. FTP,)

Fase 3: Attacco brute force hydra list.txt



Obiettivo della Fase 3:
Eseguire un attacco brute force utilizzando Hydra per identificare credenziali di accesso valide attraverso liste di username e password.
Dettagli:

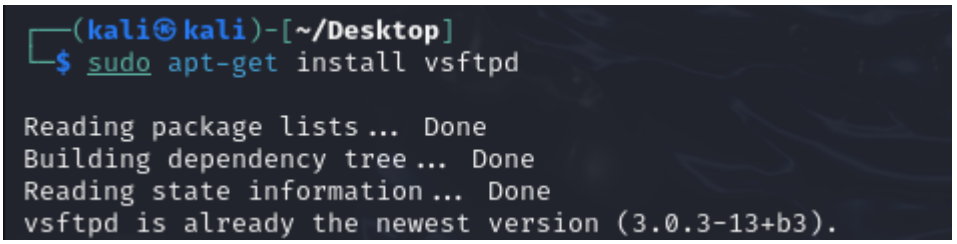
1. Preparazione delle Liste di Username e Password:

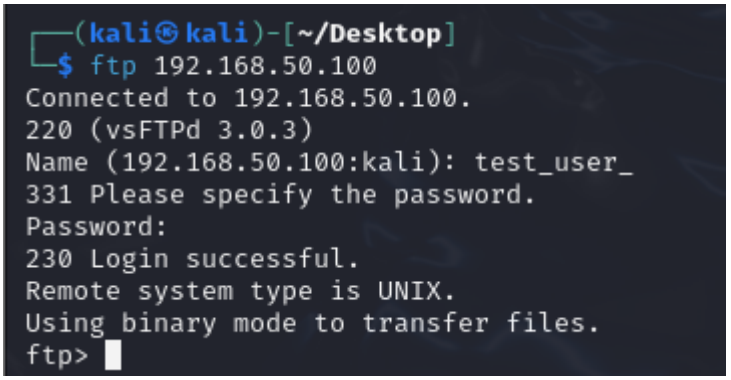
- Ho preparato due file (username.txt e password.txt) contenenti rispettivamente una lista di username e una lista di password da testare.

2. Esecuzione dell'Attacco con Hydra:
   - Hydra ha utilizzato le liste di username e password per tentare di autenticarsi al server SSH specificato (192.168.50.100).
   - Ogni combinazione di username e password è stata testata, con Hydra che ha mostrato ogni tentativo effettuato in modalità verbose.
3. Identificazione delle Credenziali Valide:
   - Hydra ha trovato con successo una combinazione di username e password valida: test_user con la password Danilo.

Configurazione e cracking ftp

Fase1: installazione e test di connessione





Obiettivo della Fase 1:
Installare e configurare il server FTP vsftpd su Kali Linux, quindi testare la connessione per assicurarsi che il server FTP sia funzionante e accessibile.
Dettagli:

Installazione di vsftpd:

- Ho utilizzato il comando sudo apt-get install vsftpd per installare il server FTP vsftpd.
- Il pacchetto è stato installato con successo e la versione più recente era già presente nel sistema.

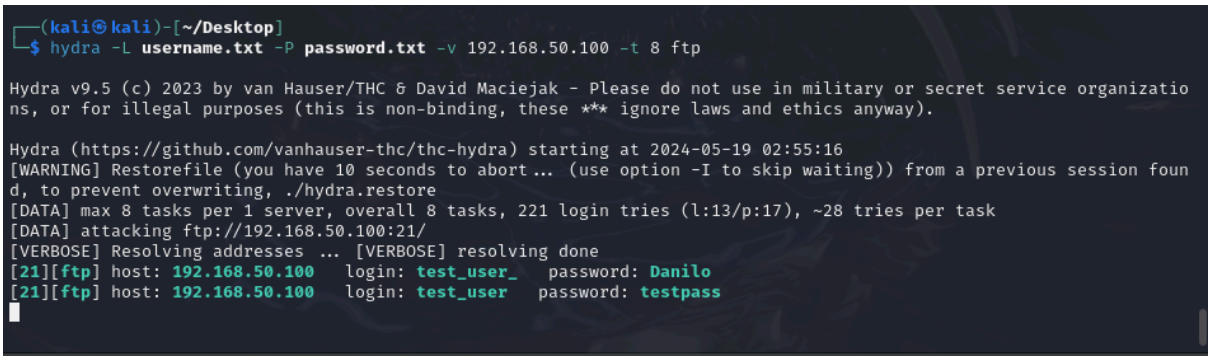
Test di Connessione FTP:

- Ho utilizzato il comando ftp per connettermi al server FTP all'indirizzo 192.168.50.100.

- La connessione è stata stabilita con successo, dimostrando che il server FTP è operativo.
- Ho effettuato il login con l'utente test_user creato precedentemente e la connessione è stata autenticata correttamente.

Questo passaggio è fondamentale per garantire che il server FTP sia configurato correttamente e accessibile, il che è necessario per le fasi successive dell'esercizio. assicurarmi che il servizio FTP sia attivo e pronto per essere testato con strumenti di cracking come Hydra.

Fase2: Brute force ftp



Obiettivo della Fase 2:
Eseguire un attacco brute force utilizzando Hydra per identificare credenziali di accesso valide al servizio FTP attraverso liste di username e password.
Dettagli:

1. Preparazione delle Liste di Username e Password:
   - Ho preparato due file (username.txt e password.txt) contenenti rispettivamente una lista di username e una lista di password da testare.
2. Esecuzione dell'Attacco con Hydra:
   - Hydra ha utilizzato le liste di username e password per tentare di autenticarsi al server FTP specificato (192.168.50.100).
   - Ogni combinazione di username e password è stata testata, con Hydra che ha mostrato ogni tentativo effettuato in modalità verbose.
3. Identificazione delle Credenziali Valide:
   - Hydra ha trovato con successo due combinazioni di username e password valide: test_user con la password Danilo e test_user con la password testpass.