S6L5

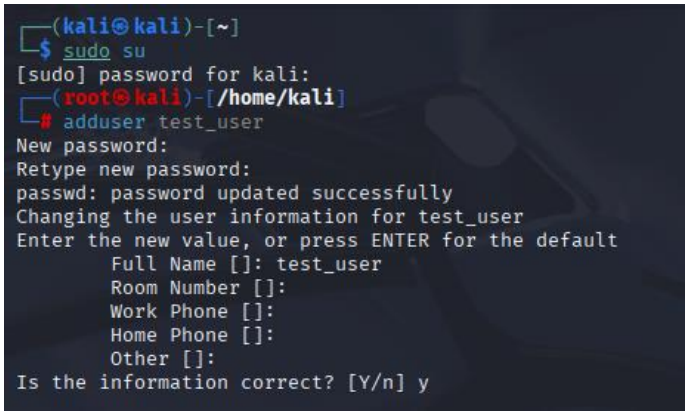
Questo documento è stato redatto per illustrare e documentare un esercizio pratico di penetration testing, focalizzato sulla valutazione della sicurezza dei servizi di rete.

L'obiettivo principale dell'attività è: acquisire padronanza nell'utilizzo dello strumento Hydra per condurre attacchi di forza bruta e a dizionario contro i sistemi di autenticazione, consolidare la conoscenza dei servizi di rete stessi attraverso la loro configurazione e analisi delle vulnerabilità.

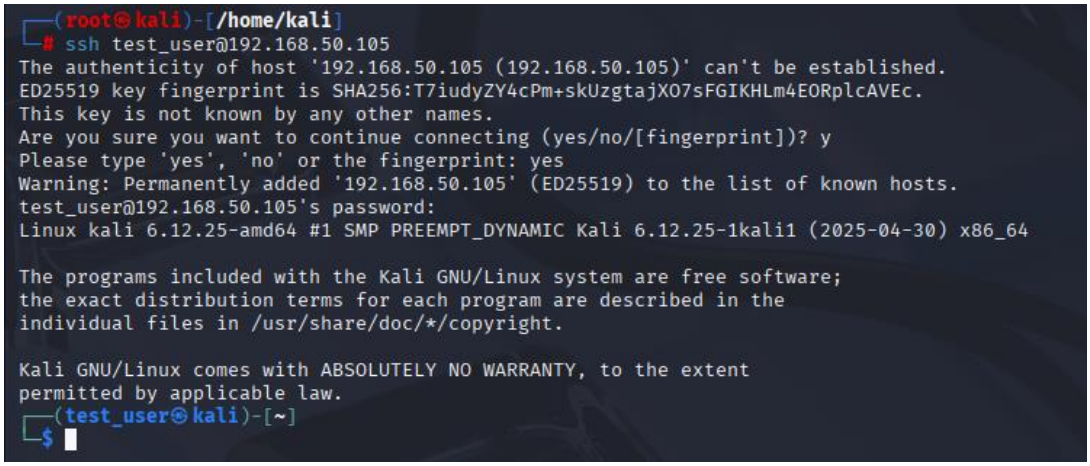
L'esercizio si è sviluppato in due fasi distinte: una prima fase guidata, che ha focalizzato l'attenzione sul protocollo SSH, dove è stato simulato un attacco di "password cracking". Successivamente, una seconda fase ha permesso di applicare le competenze acquisite in modo autonomo, configurando e attaccando un servizio di rete a scelta. (FTP)

Configurazione ambiente:

Dopo aver letto e compreso la richiesta dell'esercizio di oggi, ho iniziato con la configurazione di un nuovo utente sulla macchina Kali Linux con le seguenti credenziali, ID: **test_user** e PSW: **testpass**

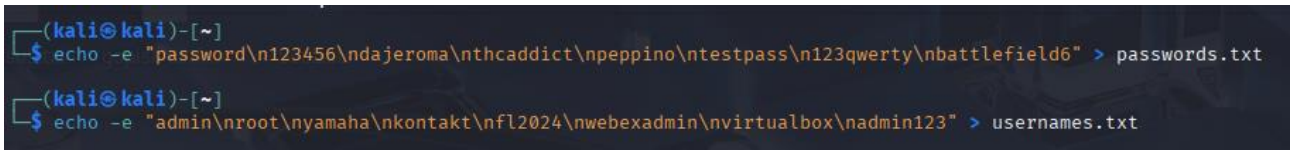


Una volta creato il nuovo utente, attivo il servizio SSH e verifico il corretto funzionamento con la connessione in SSH dell'utente test_user precedentemente creato, eseguendo il comando: **ssh test_user@192.168.50.105**



Come possiamo vedere dall'immagine sopra, siamo entrati nella shell di test_user;

Una volta verificata la corretta funzionalità dell'utente test_user, passo sull'utente Kali e creo due file .txt differenti che useremo come wordlist. Uno per combinazioni di passwords, e uno per gli usernames, così da poterli impiegare per una sessione di cracking tramite Hydra.



Adesso non resta altro che avviare Hydra e dargli **hydra –L username_list –P password_list IP_KALI–t 1 ssh -V**

Questo comando utilizza lo strumento Hydra per eseguire un attacco di forza bruta contro un servizio SSH, tramite

-L specifichiamo un file (**usernames.txt**) che contiene una lista di nomi utente da testare. Hydra tenterà di accedere con ogni nome utente presente in questo file.

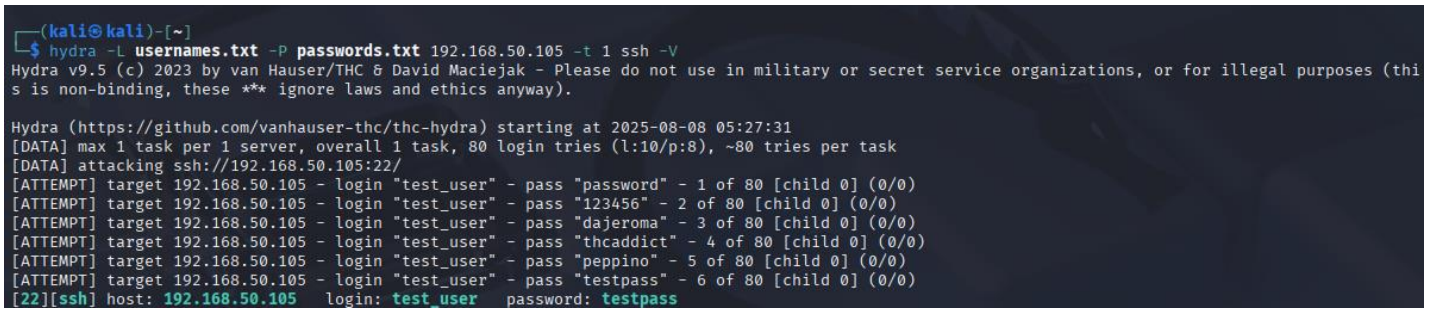
-P Specifica un file (**passwords.txt**) che contiene una lista di password da testare. Hydra anche qui proverà ogni password del file per ogni nome utente. ***Questo è il cuore dell'attacco a dizionario***.

198.168.50.105: È l'indirizzo IP del server bersaglio a cui Hydra cercherà di connettersi.

-t 1: Imposta il numero di tentativi paralleli (thread) a 1. Questo significa che Hydra farà 1 tentativo alla volta.

SSH: Specifica il protocollo di rete su cui eseguire l'attacco. In questo caso, il comando tenterà di crackare le credenziali di accesso al servizio **Secure Shell (SSH)** del server.

-V per avere un report dei tentativi di cracking da parte di Hydra in tempo reale

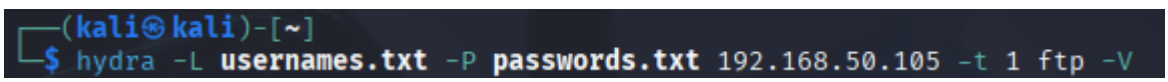


Come possiamo constatare dall'immagine, Hydra ha letto il primo user contenuto nel file usernames.txt e ha tentato tutte le password contenute nel file passwords.txt. In sintesi in questo caso è stato condotto un attacco di tipo **"attacco dizionario"** e **"brute-force"** contro il servizio SSH. L'attacco ha tentato di combinare i nomi utente presenti nel file usernames.txt con le password presenti nel file passwords.txt.

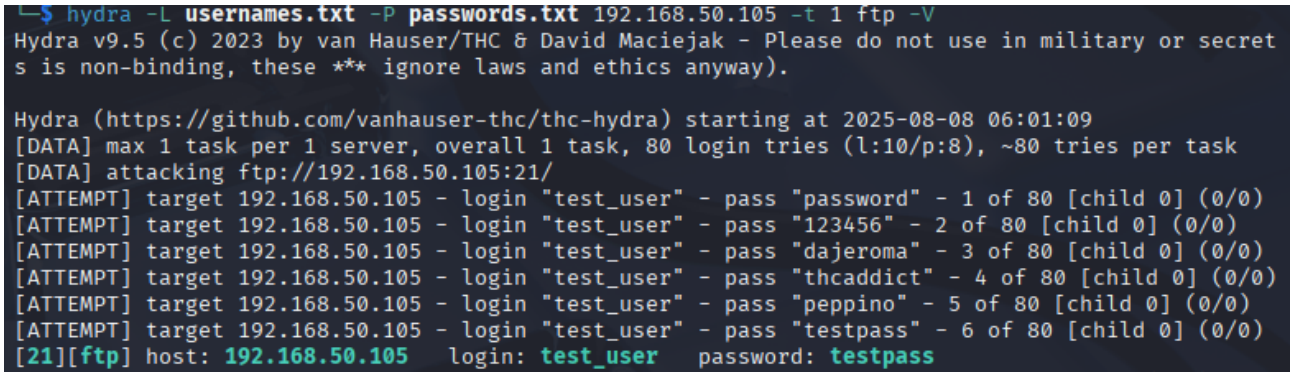
Cracking contro un servizio FTP

Vista la configurazione iniziale dell'ambiente, a questo punto è semplice per noi, effettuare un attacco come questo su un altro tipo di servizio. Infatti ci basterà installare ed attivare il servizio ftp sulla macchina e dopo di che cambiare il servizio da SSH in FTP nel comando che daremo ad Hydra e il gioco è fatto:

Comando:



Risultato:



Questo è il risultato del cracking sul servizio FTP.

Questo esercizio simula l'applicazione pratica di un attacco di brute-force su un servizio SSH e FTP tramite l'utilizzo di Hydra, un tool molto potente, noto anche come THC Hydra, è un tool open-source ampiamente utilizzato nel campo della cybersecurity, specialmente nel penetration testing. Il suo scopo principale è quello di effettuare attacchi di "password cracking" online, in particolare attacchi a dizionario e di forza bruta, contro i servizi di autenticazione di rete.

Analizzando le diverse fasi, possiamo notare l'importanza di adottare **policy di sicurezza robuste**, come l'uso di password complesse, l'attivazione di sistemi di blocco degli account dopo tentativi falliti (ad esempio con fail2ban) e l'impiego di protocolli di autenticazione più sicuri, come l'autenticazione a chiave pubblica.

Attraverso l'esercizio svolto oggi, ho appreso come replicare un attacco a dizionario e brute-force tramite l'impiego del tool Hydra, ma mi ha aiutato a comprendere anche le contromisure necessarie per rafforzare la sicurezza contro le minacce più comuni.