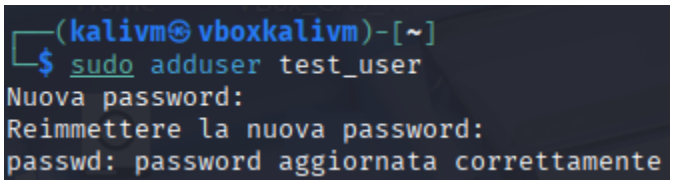
Authentication cracking w/ Hydra

Obiettivo: Simulare attacchi di Cracking dell'autenticazione dei servizi di rete con l'utilizzo di Hydra. Questo tool ci permette di effettuare attacchi utilizzando dizionari di Username e Password, o Brute Force puro.
Struttura dell'esercizio: l'esercizio è strutturato in due fasi. Nella prima fase, si procede a configurare SSH per poi testare la vulnerabilità delle credenziali con Hydra.
Nella seconda fase, vediamo il Cracking relativo al servizio FTP.

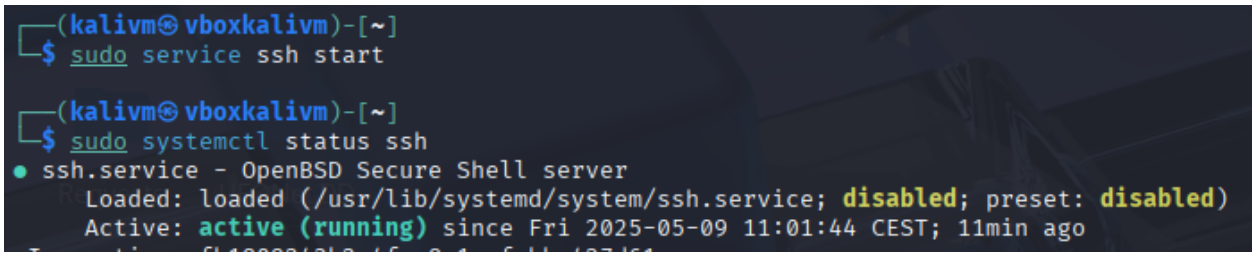
Fase 1 : Cracking dell'autenticazione di SSH con l'utilizzo di Hydra.

Per questo esercizio, si è scelto di utilizzare solo una macchina, imparando a configurare i servizi di rete e capire eventuali vantaggi/svantaggi delle tecniche di Cracking citate sopra.

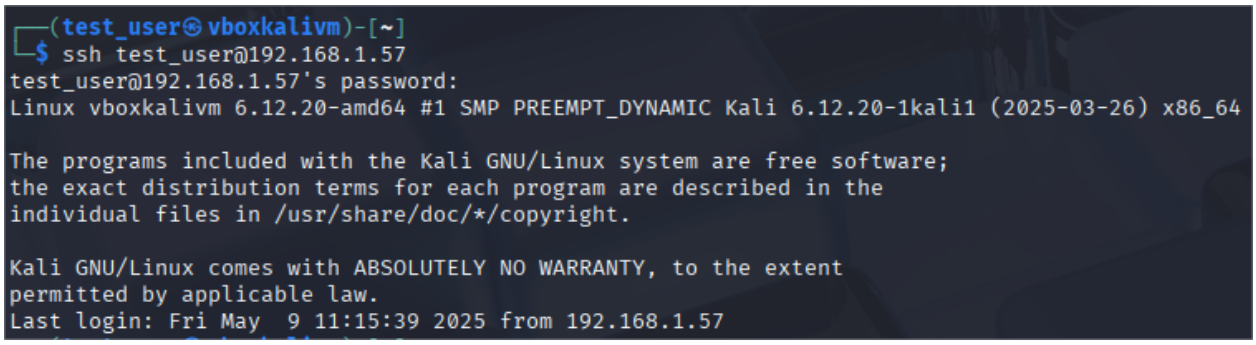
a) Il primo passo è stato quello di creare un nuovo utente, quindi su Kali, con il comando <**sudo adduser**> abbiamo creato un utente prova, di seguito chiamato "test_user" con relativa password "testpass".



b) Successivamente, è stato attivato il servizio SSH con il comando <**sudo service ssh start**> *utilizzabile anche con* <**sudo systemctl start ssh**>.

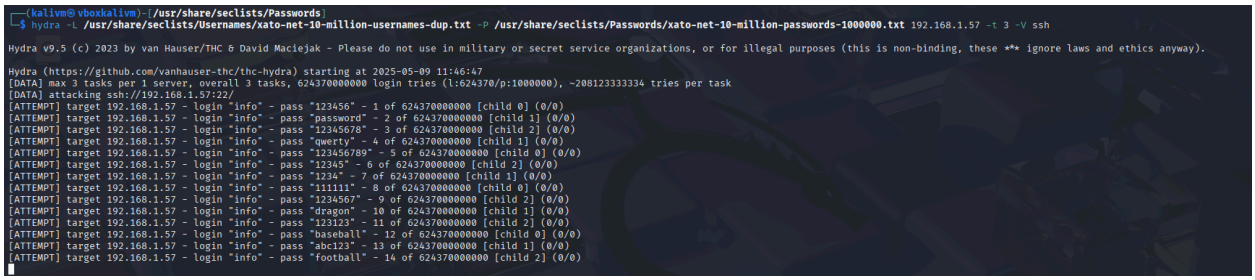


Una volta verificato che il servizio sia effettivamente stato attivato con <**sudo systemctl status ssh**> abbiamo potuto testarne la connessione con l'utente creato.
Quindi facendo <**test_user@192.168.1.57**> abbiamo avuto conferma della connessione.



c) Da qui, si ricorre all'utilizzo di Hydra, provando a crackare l'autenticazione del nuovo utente creato in precedenza.
Abbiamo due opzioni, a seconda di ciò che conosciamo. Con la prima, utilizzando gli switch -l e -p in minuscolo, possiamo provare a effettuare un attacco diretto, ossia presupponendo un determinato username e una determinata password. La seconda opzione, sfrutta un attacco a dizionario, quindi provando diverse combinazioni presenti in file .txt contenenti Username e Password.

In questo caso, si è effettuato il tentativo principale scaricando **Seclists,** che offre librerie di file contenenti username e password principali utilizzati nei sistemi.
Quindi: con il comando <**sudo apt install seclists**> abbiamo installato Seclists. Una volta installato, abbiamo provato ad effettuare un attacco a dizionario con l'aiuto delle liste.
Al comando è stato aggiunto lo switch -V per vedere in tempo reale i tentativi di Cracking:



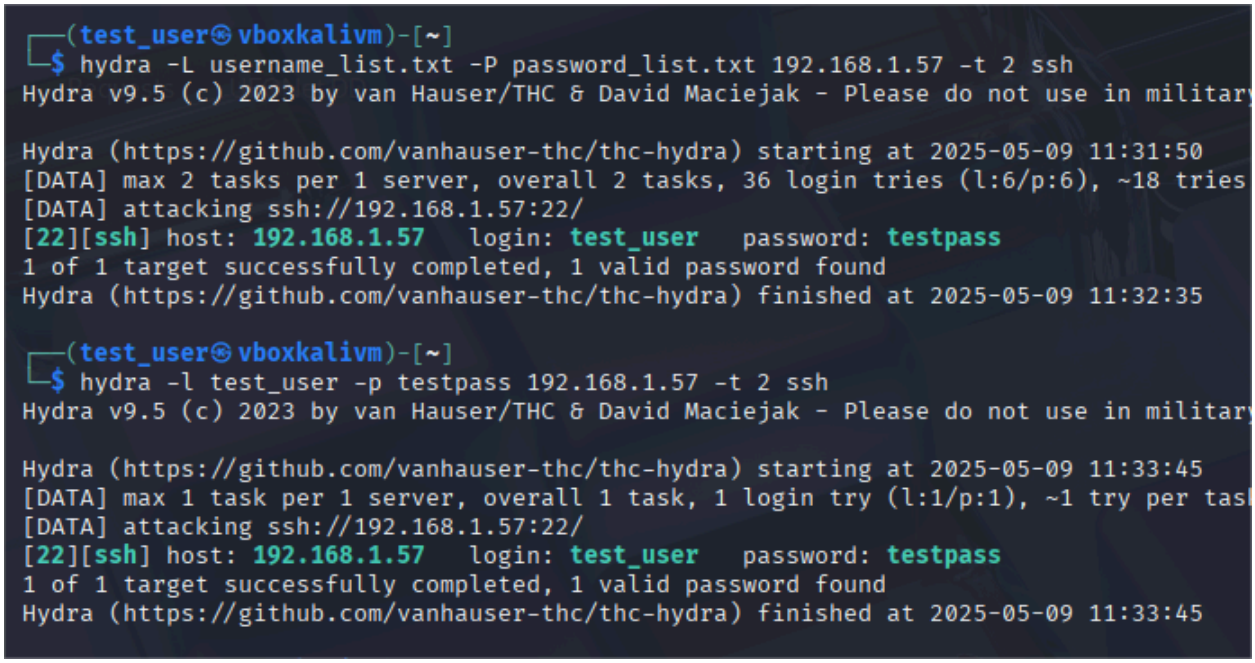
Il comando completo utilizzato è: <**hydra -L /usr/share/seclists/Usernames/xato-10-million-usernames-dup.txt - P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.57 -t 3 -V ssh**>

L'operazione è risultata troppo lunga in termini di tempo, così abbiamo creato due liste di file contenenti le opzioni più comuni di Username in un file e le password più comuni in un'altro file, entrambi **.txt**.

In questo modo, Hydra ha trovato effettivamente l'Username e la Password utilizzati per l'autenticazione al servizio SSH.

Una volta risaliti ad essi, si è provato il comando con gli switch minuscoli per avere un ulteriore conferma.
Quindi con <**hydra -L username_list.txt -P password_list.txt 192.168.1.57 -t 2 ssh**>
Abbiamo utilizzato le liste, per poi avere la conferma prendendo il singolo user e la singola password con <**hydra -l test_user -p testpass 192.168.1.57 -t 2 ssh**>

L’esempio:



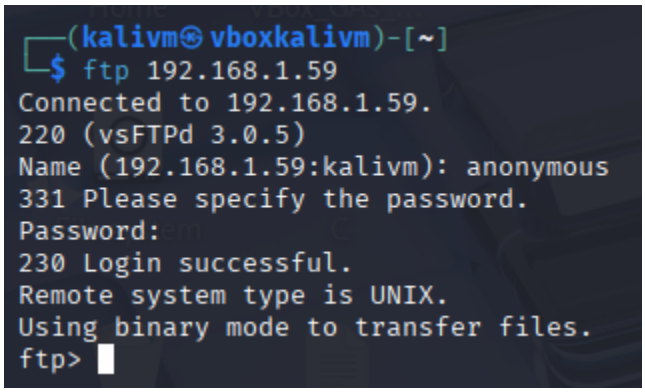
Fase 2: Cracking del servizio FTP.

In questa fase, per prima cosa, abbiamo configurato FTP.

Con i comandi <**sudo apt install vsftpd**> per installare FTP e con <**sudo service vsftpd start**> per avviarlo, abbiamo effettuato la configurazione.

Successivamente, abbiamo provato le stesse tecniche utilizzate nella fase 1, quindi con i comandi di Hydra, abbiamo effettuato degli attacchi a dizionario.
Tuttavia, essendo numerose combinazioni, il tempo richiesto sarebbe stato troppo elevato, abbiamo quindi optato per una vulnerabilità comune in servizi FTP attivi.

Infatti, nella cartella di vsftpd, precisamente in **/etc/vsftpd.conf**, troviamo il file di configurazione del servizio. In molti casi, ci si dimentica di disabilitare l’accesso con l’utente Anonymous, per questo abbiamo provato con risultato positivo.



Tuttavia, l’accesso con l’utente Anonymous ci ha permesso di entrare solo in modalità passiva, quindi non avendo privilegi come utente root, le operazioni da effettuare all’interno sono limitate.

Le operazioni da fare in questo caso, potrebbero essere: <**pwd**> (utile per conoscere il percorso in cui ci troviamo), <**cd**> per cambiare directory e <**-ls -la**> per trovare eventuali file nascosti.
In questo caso, essendo stata una pratica, non abbiamo trovato nessun file nella directory.

Conclusioni: Anche servizi di rete che apparentemente sembrano affidabili come SSH e FTP possono diventare bersagli di attacco se mal configurati.
Configurarli sempre in modo da limitare l'accesso il più possibile, in questo caso dal file **vsftpd.conf** rimuovere l'opzione dell'accesso Anonymous.
Le password deboli sono maggiormente esposte ad attacchi di cracking a Dizionario,
Utilizzare sempre password contenenti più caratteri come lettere maiuscole e minuscole con simboli, in modo da ridurre l'esposizione.
Utilizzare sempre l'autenticazione a chiave pubblica per SSH e disabilitare l'accesso con password, monitorando i log.