Relazione Tecnica: Authentication Cracking con Hydra

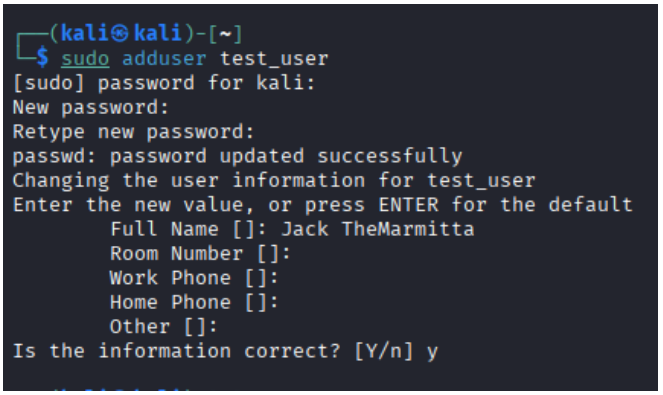
Introduzione

In questa attività ho esplorato le tecniche di cracking delle credenziali per i servizi di rete SSH e FTP, utilizzando lo strumento Hydra.

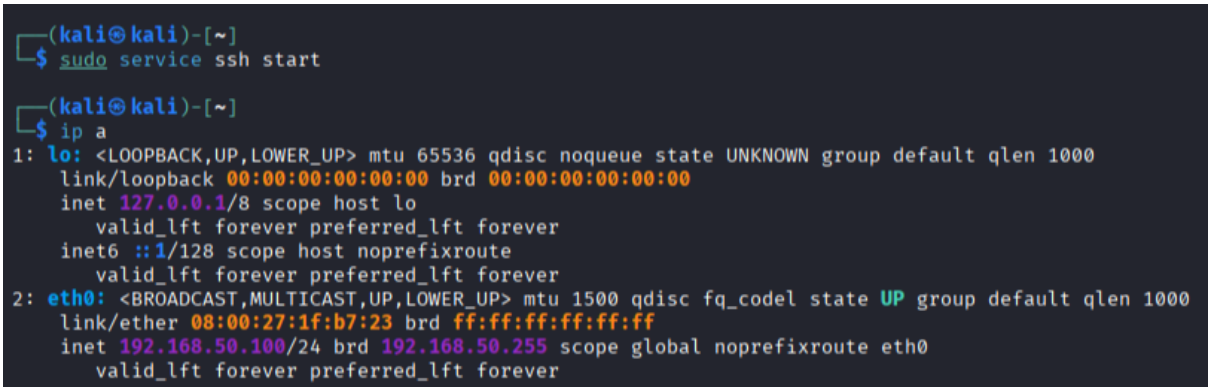
Fase 1: Configurazione e Cracking SSH

L'obiettivo iniziale è stato quello di preparare un bersaglio valido sulla mia macchina Kali Linux per testare l'efficacia di un attacco a dizionario.

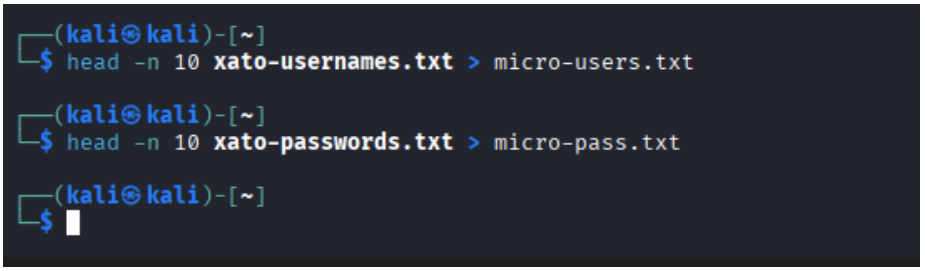
1. **Preparazione dell'utenza**: Ho creato un nuovo utente nel sistema chiamato `test_user`, impostando come password `testpass`.



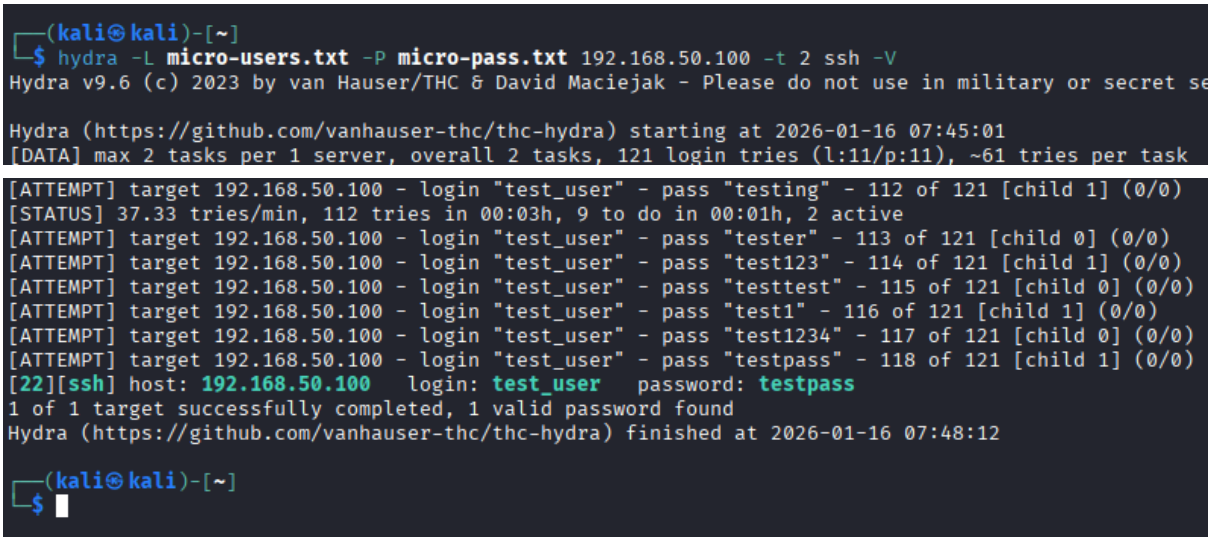
2. **Attivazione del Servizio**: Ho avviato il demone SSH tramite il comando `sudo service ssh start`. Ho inoltre verificato l'indirizzo IP locale della macchina per definire il target dell'attacco.



3. **Filtraggio delle Wordlist (Grepping)**: Ho installato il pacchetto `seclists`. Ho proceduto a una prima riduzione dei file tramite il comando `grep`, filtrando i termini contenenti la stringa "test".
    - *Comando:* `cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > xato-usernames.txt`
4. **Ottimizzazione finale dei tempi (Head)**: Durante l'esecuzione, ho notato che i file ottenuti dal grepping erano ancora troppo voluminosi, portando a tempi di attesa incompatibili con la consegna prevista per le ore 18:00. Ai fini del corretto svolgimento dell'esercitazione e per risolvere il problema, ho eseguito un'ulteriore estrazione tramite il comando `head`:
    - *Comando:* `head -n 10 xato-usernames.txt > micro-users.txt`
    - Ho quindi aggiunto manualmente le credenziali reali (`test_user` e `testpass`) in fondo a queste "micro-liste" per assicurarmi che il cracking avesse successo pur limitando i tentativi.



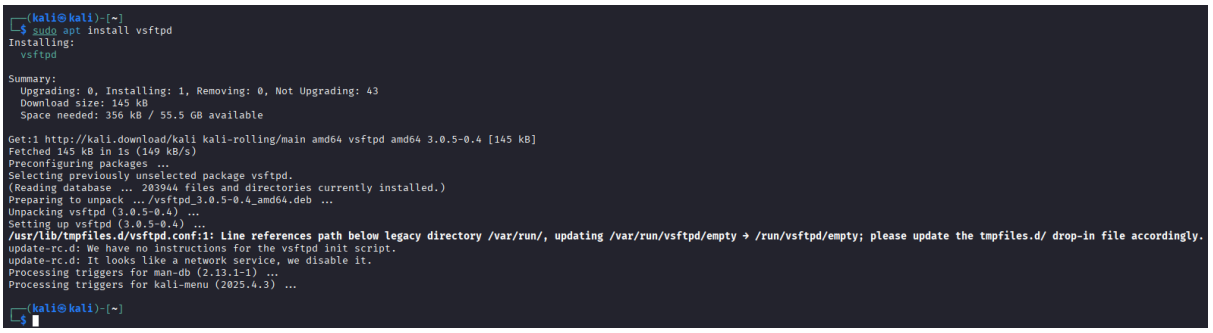
5. **Esecuzione dell'Attacco**: Ho lanciato Hydra in modalità "blackbox" (utilizzando gli switch `-L` e `-P` per simulare la non conoscenza di utenti e password). Ho impostato il numero di thread a 2 (`-t 2`) per garantire la stabilità del servizio durante il processo.
    - **Comando finale:** `hydra -L micro-users.txt -P micro-pass.txt 192.168.50.100 -t 2 ssh -V`.



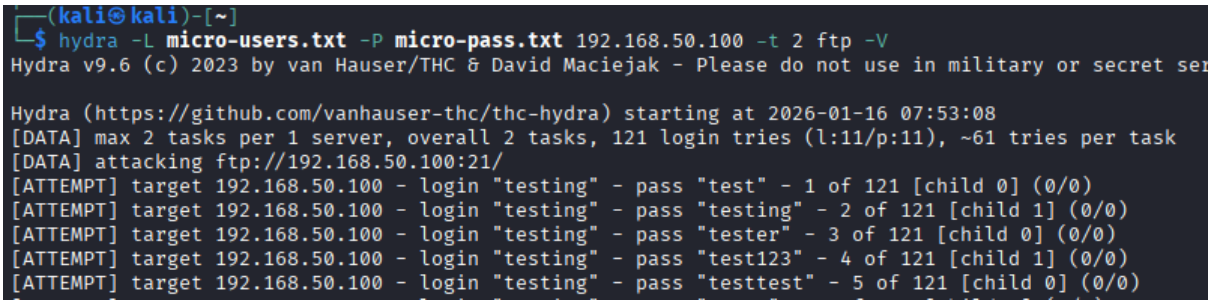
Fase 2: Configurazione e Cracking FTP

Nella seconda fase ho configurato il servizio FTP per consolidare le conoscenze sulla gestione dei demoni di rete.

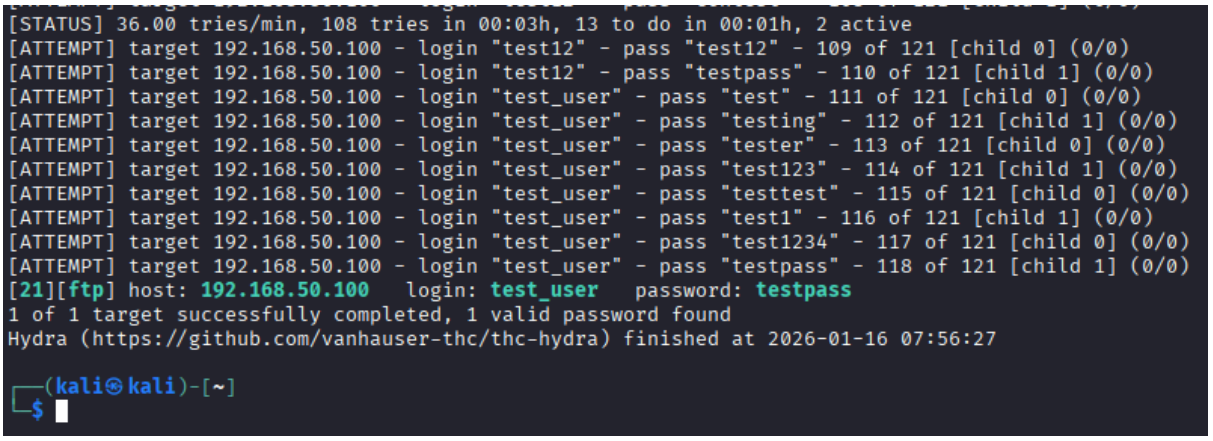
1. **Installazione e Avvio**: Ho installato il server FTP tramite `sudo apt install vsftpd` e l'ho avviato con `sudo service vsftpd start`.



2. **Attacco Comparativo**: Ho riutilizzato le micro-liste create in precedenza per attaccare il protocollo FTP.
    - **Comando:** `hydra -L micro-users.txt -P micro-pass.txt 192.168.50.100 -t 2 ftp -V`



3. **Analisi dei Risultati**: Hydra ha individuato la password correttamente. Ho osservato che il cracking su FTP è significativamente più veloce rispetto a quello su SSH. Questa differenza è dovuta alla natura del protocollo FTP che, a differenza di SSH, non richiede complessi handshake crittografici per ogni tentativo di connessione, riducendo drasticamente i tempi di risposta del server.



Conclusioni

L'esercizio ha confermato che la configurazione dei servizi costituisce parte integrante della sicurezza. Ho appreso che, per quanto gli strumenti automatizzati come Hydra siano potenti, la gestione corretta delle wordlist e la comprensione dei limiti temporali sono competenze fondamentali per un analista di cybersecurity.