Report Authentication Cracking con Hydra e Configurazione Servizi

Studente: Nicola Cassandra

Data: 16/01/2026

Target IP: 192.168.1.165

Tool Utilizzati: Kali Linux, THC Hydra.

Introduzione Teorica

THC Hydra è uno strumento di cracking di password online, estremamente rapido e potente, utilizzato da professionisti della sicurezza per il *penetration testing*. La sua efficacia deriva dalla capacità di eseguire attacchi in modo *parallelo* su numerosi protocolli e servizi (come FTP, SSH, database e interfacce web), accelerando notevolmente il processo. Hydra supporta principalmente due metodologie: l'***Attacco a Dizionario*** (più veloce, basato su liste di password comuni) e l'***Attacco Brute-Force*** (sistematico ma più lento). Nel contesto etico, è impiegato per simulare attacchi, identificare credenziali deboli e correggere vulnerabilità, fungendo da strumento essenziale per l'auditing della sicurezza delle password.

Configurazione e Cracking del servizio SSH

In questa prima fase, abbiamo configurato un ambiente vulnerabile controllato per testare le capacità di Hydra sul protocollo SSH.

Configurazione dell'Ambiente

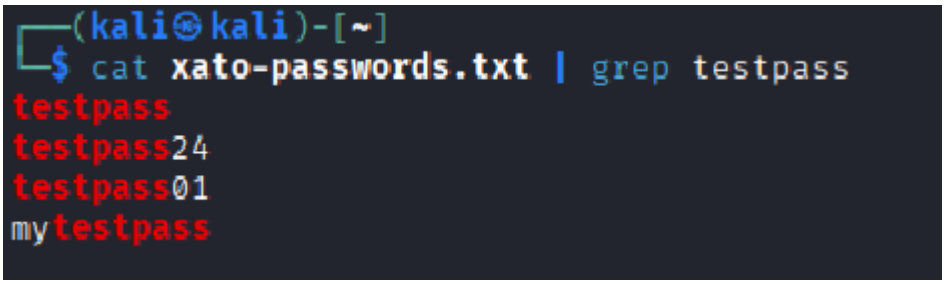
> Per preparare l'ambiente, è stato innanzitutto creato un nuovo utente sulla macchina Kali. Questo utente, chiamato `test_user`, è stato configurato con la password `testpass` utilizzando il comando `adduser`. Successivamente, per consentire l'accesso remoto e i tentativi di cracking, il servizio SSH è stato attivato tramite l'esecuzione del comando `sudo service ssh start`.

Attacco con Hydra (SSH)

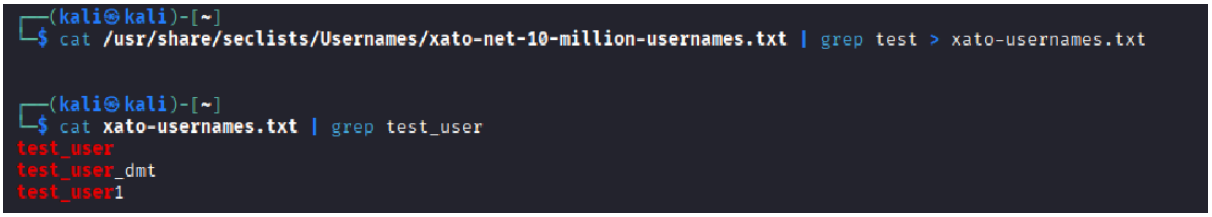
Abbiamo configurato Hydra per eseguire un attacco a dizionario e abbiamo utilizzato le flag maiuscole `-L` e `-P` per indicare l'uso di liste di utenti e password.

Creazione File Testo Passwords

Verifica Presenza Oggetto



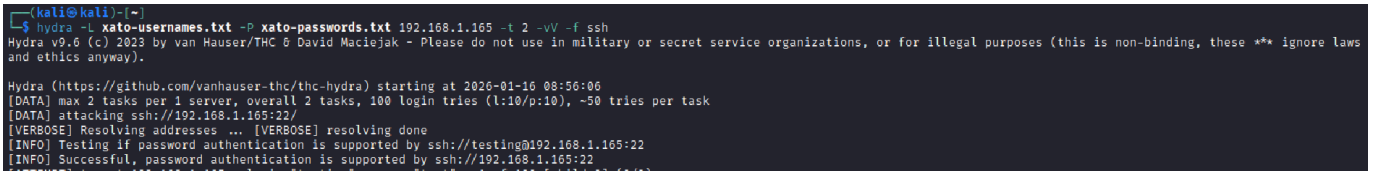
Creazione File Testo Usernames e Verifica Presenza Oggetto



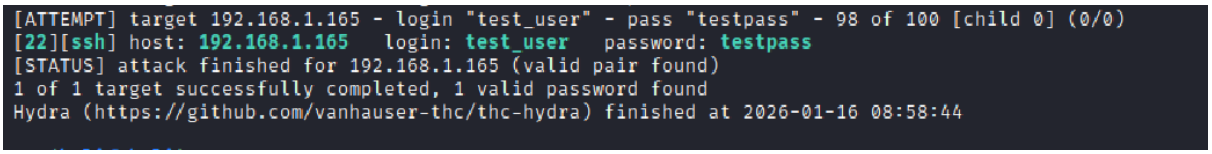
Parametri dell'attacco:

- **Target:** 192.168.1.165
- **Wordlists:** `xato-usernames.txt` e `xato-passwords.txt` (versioni ridotte delle wordlist originali *seclists* per ottimizzare i tempi).
- **Thread:** `-t 4` (numero di task paralleli).

Comando eseguito:



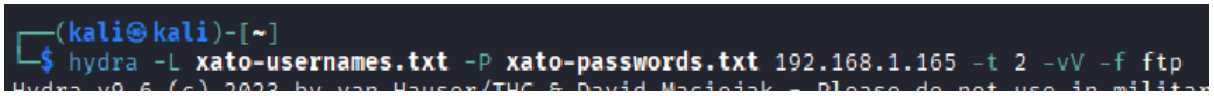
Risultato Finale SSH:



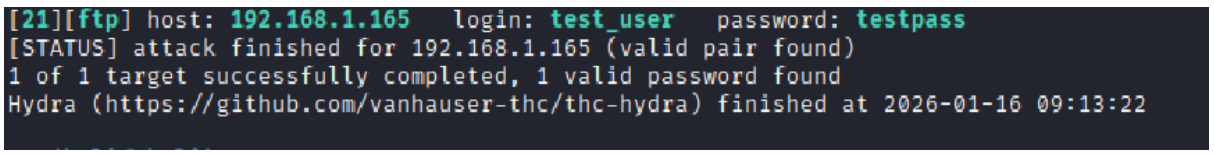
Installazione e Configurazione vsftpd

È stato scelto il servizio `vsftpd` (Very Secure FTP Daemon) come consigliato, una volta installato e avviato il servizio si procede con l'attacco:

Comando eseguito:



Risultato Finale:



---

4. Conclusioni e Osservazioni

Possiamo notare come l'esercizio abbia dimostrato l'efficacia degli attacchi a dizionario contro servizi configurati con password deboli.

- **Tempo di esecuzione:** L'utilizzo di wordlist ridotte (xato-usernames.txt e xato-passwords.txt) è stato fondamentale. L'uso di wordlist complete (come rockyou o seclists integrali) richiederebbe molto tempo senza una limitazione mirata.
- **Output:** Hydra ha identificato correttamente la coppia login: `test_user` e password: `testpass` sia per SSH che per FTP, confermando la vulnerabilità dell'account.