Authentication cracking con Hydra

Data: 16 Gennaio 2026

Autore: Francesco Sardi

Oggetto: Authentication cracking con Hydra su protocolli SSH e FTP

1. Obiettivi

Il presente report si pone due obiettivi principali:

1. **Fase 1:** Configurazione di un ambiente target, abilitazione del servizio SSH ed esecuzione di una sessione di cracking dell'autenticazione.
2. **Fase 2:** Configurazione ed esecuzione di un attacco di *password cracking* su un secondo servizio di rete (FTP).

2. Panoramica

In questo report vengono documentate le procedure per la creazione di un utente target su sistema Kali Linux (con privilegi limitati) e l'attivazione del demone SSH. Successivamente, viene dimostrata la vulnerabilità di credenziali deboli attraverso l'utilizzo del tool **Hydra**, effettuando un attacco a dizionario *(dictionary attack)*.

Nella seconda fase, la medesima metodologia viene applicata al protocollo FTP, verificando la versatilità del tool su diversi servizi di rete.

3. Fase 1: Setup dell'Ambiente e Servizio SSH

3.1 Creazione Utente Target

Per simulare un attacco reale, è stato creato un nuovo utente nel sistema Kali Linux. Per fini didattici, sono state impostate credenziali semplici.

- **Comando:** *adduser*
- **User:** *test_user*
- **Password:** *testpass*

Successivamente, è stato avviato il servizio SSH per rendere la macchina accessibile e attaccabile via rete.

```
└─$ sudo adduser test_user
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

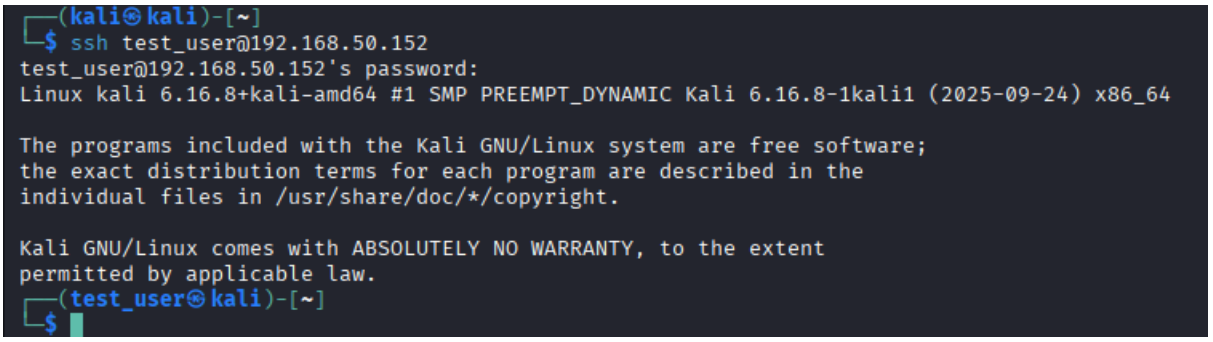
3.2 Verifica della Configurazione

È stata effettuata un'analisi preliminare del file di configurazione del demone SSH situato in */etc/ssh/sshd_config*.

3.3 Test di Connettività

Prima di procedere con l'attacco, è stata verificata la corretta funzionalità del servizio tentando una connessione legittima verso l'indirizzo **IP target** *192.168.50.152*.

Testo la connessione SSH dell'utente appena creato su sistema col comando *"ssh testuser@192.168.50.152"* verificando che tutto sia stato fatto correttamente.



Confermato il funzionamento del servizio e la creazione dell'utente, si procede alla fase offensiva ignorando le credenziali note per simulare un approccio "*black-box*".

4. Fase Operativa: Cracking delle Password

4.1 Preparazione delle Wordlist (Seclists)

Per l'attacco a dizionario è stato utilizzato il repository **Seclists**, che contiene milioni di credenziali comuni. Per ottimizzare i tempi di esecuzione a fini didattici, le wordlist sono state filtrate riducendo il numero di dati, mantenendo solo quelle contenenti la stringa "test".

Creazione wordlist Utenti:

- File user ridotto *(xato-username.txt)* con il comando : *"cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > xato-username.txt "*

Creazione wordlist Password:

- File password ridotto *(xato-password.txt)* con il comando *" cat /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords.txt | grep test > xato-passwords.txt ".*

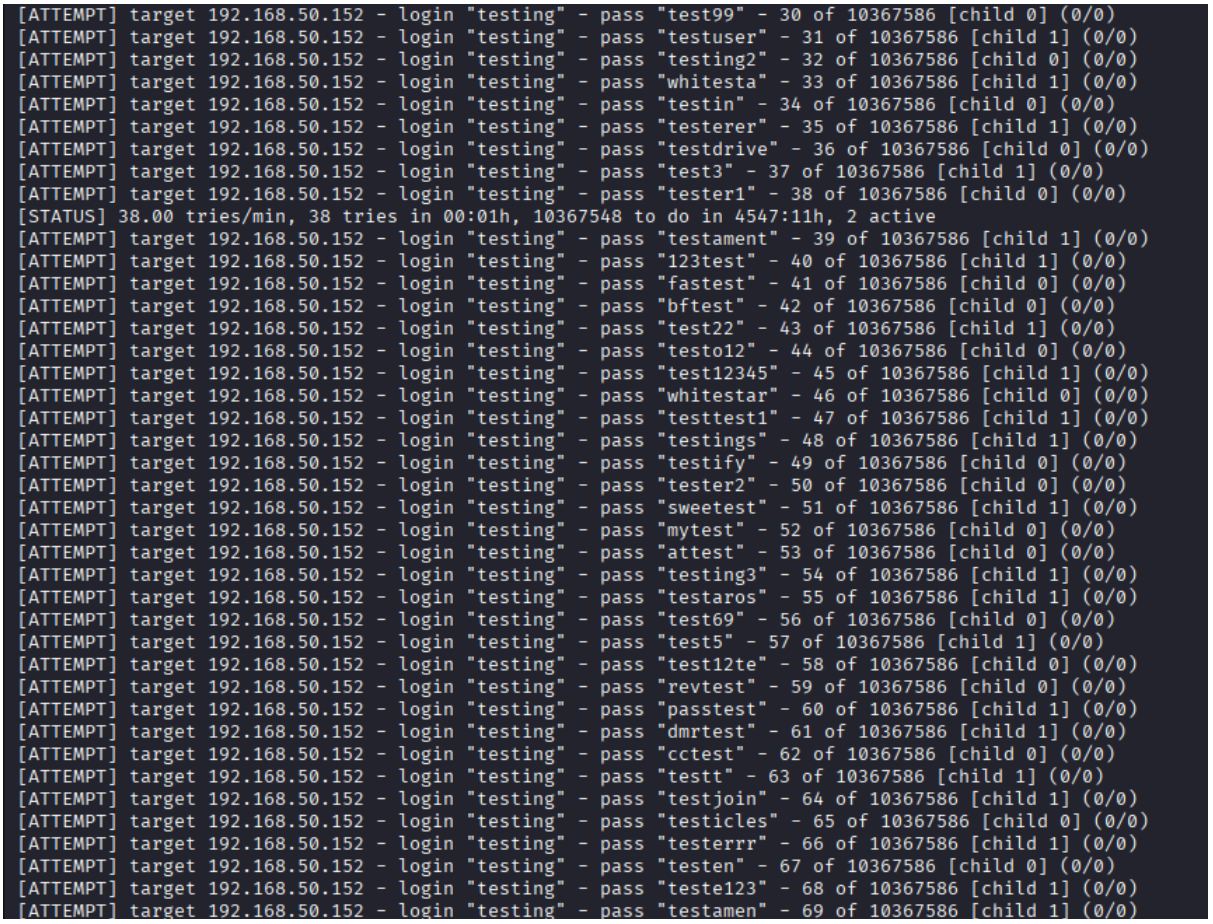
Questa operazione genera due file ridotti *(xato-username.txt e xato-passwords.txt)*, permettendo a Hydra di completare l'attacco in tempi brevi.

4.2 Esecuzione dell'Attacco SSH

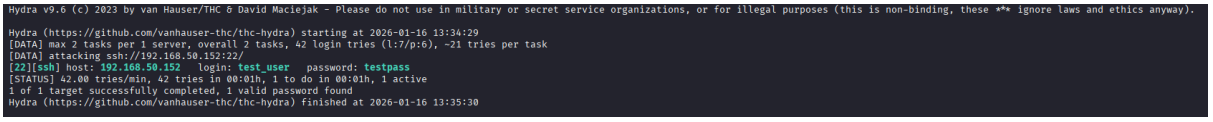
L'attacco è stato lanciato utilizzando **Hydra** con i seguenti parametri:

- **-L**: Specifica il file contenente la lista degli username.
- **-P**: Specifica il file contenente la lista delle password.
- **-t2**: Limita il numero di task paralleli a 2 (per non sovraccaricare il servizio).
- **-V**: Modalità "*Verbose*", per visualizzare il progresso in tempo reale.

Comando di attacco:
"hydra -L xato-username.txt -P xato-passwords.txt 192.168.50.152 -t2 -V ssh "



Risultato:
Hydra ha identificato con successo la combinazione corretta di username e password.

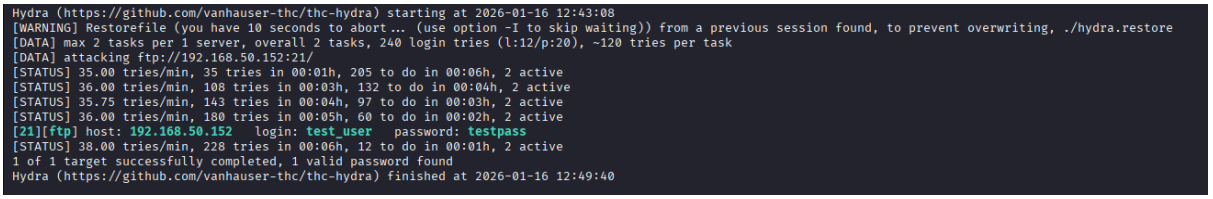


5. Fase 2: Cracking del Servizio FTP

Per la seconda parte del progetto, è stato scelto il protocollo **FTP**.Dopo aver assicurato che il servizio fosse attivo sulla macchina target, è stata applicata la medesima metodologia di attacco, adattando la sintassi del comando al nuovo protocollo.

Comando di attacco:
“hydra -L xato-username.txt -P xato-passwords.txt ftp://192.168.50.152 -t 2 “

Risultato:
Anche in questo caso, il tool è riuscito a effettuare il *brute-force* delle credenziali, dimostrando l'efficacia dell'attacco su protocolli differenti che non implementano meccanismi di blocco contro tentativi di accesso multipli falliti.



6. Conclusione

L'attività svolta ha permesso di analizzare in profondità il funzionamento degli attacchi di autenticazione online tramite l'utilizzo di **Hydra**.

Dai test effettuati emergono due considerazioni fondamentali in ambito Cybersecurity:

1. **L'efficacia degli attacchi a dizionario:** L'utilizzo di wordlist ottimizzate (come le Seclists) rende banale la compromissione di account che utilizzano credenziali comuni o prevedibili, indipendentemente dal protocollo utilizzato (SSH o FTP).
2. **L'importanza di policy di sicurezza robuste:** Il successo dell'attacco evidenzia la necessità critica di implementare password complesse e, soprattutto, meccanismi di difesa attiva o limitazioni sui tentativi di login. Senza queste contromisure, qualsiasi servizio esposto in rete è vulnerabile ad attacchi automatizzati in tempi molto rapidi.

In conclusione, Hydra si conferma uno strumento potente e versatile per il *penetration testing*, essenziale per verificare la robustezza delle configurazioni di accesso ai servizi di rete.