AUTHENTICATION CRACKING CON HYDRA

1)PUNTI CHIAVE

- Installazione e configurazione servizio FTP
- Creazione liste (username/password) filtrate
- Login cracking w/HYDRA
- Accesso a vsftpd

2)INTRODUZIONE

La sicurezza dei servizi di rete dipende dalla robustezza delle credenziali di accesso. Spesso, l'uso di password semplici o ripetitive rappresenta uno dei principali vettori di attacco utilizzati dagli attaccanti per ottenere un accesso non autorizzato ai sistemi.

Un chiaro esempio è l'uso di **Hydra**,tool che permette di lanciare attacchi come **Brute Force** (generazione di combinazioni possibili) **e Dizionario** (uso di liste precompilate)**,** volti a superare l'autenticazione recuperando le credenziali deboli degli utenti.

A fini dimostrativi, è stato creato un secondo utente in locale (Kali) come target per il login cracking:

- **Nome:** Jake2
- **Password:** testpass123

3)OBIETTIVO

L'obiettivo è di ottenere un accesso non autorizzato ai diversi servizi come SSH o FTP attraverso l'identificazione di credenziali di autenticazione .

4)STRUMENTI

- **Hydra** ----> tool per lanciare attacchi di Brute Force e Dizionario
- **Vsftpd** ----> servizio FTP target

5)SVOLGIMENTO

5.1) INSTALLAZIONE E CONFIGURAZIONE SERVIZIO FTP

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
```

*Fig.1 Installazione vsftpd

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start vsftpd
```

*Fig.2 Avvio servizio ftp

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status vsftpd
[sudo] password for kali:
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: active (running) since Fri 2026-01-16 06:21:14 EST; 17min ago
 Invocation: d9aa5b75ced9425aad04ba101c4b5e52
    Process: 98438 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 98440 (vsftpd)
      Tasks: 1 (limit: 11714)
     Memory: 868K (peak: 20.6M)
        CPU: 486ms
     CGroup: /system.slice/vsftpd.service
             └─98440 /usr/sbin/vsftpd /etc/vsftpd.conf
```

*Fig.3 Verifica stato servizio ftp

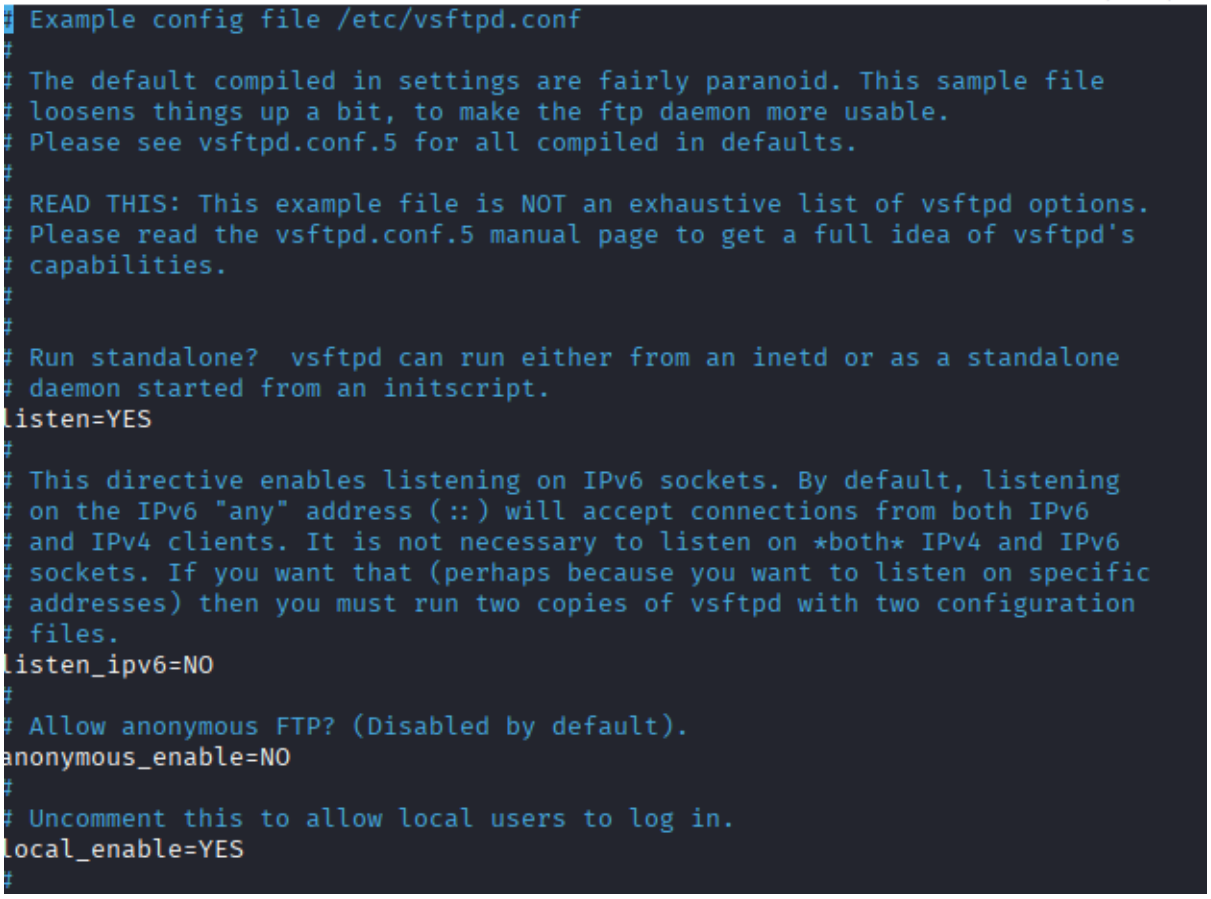

Fig.4 Configurazione server

Come servizio target per l'authentication cracking è stato scelto il servizio **FTP** gestito da **vsftpd**(Very Secure FTP Daemon) che permette di trasferire file via rete, offrendo funzionalità avanzate come l'uso di utenti virtuali e il supporto per crittografia SSL/TLS, rendendolo ideale per la condivisione di file in modo sicuro ed efficiente.

Il servizio inoltre è stato attivato su ambiente Kali Linux per testare la solidità delle credenziali tramite attacchi a dizionario con **Hydra**.

Dopo l'installazione, si è proceduto con l'attivazione e la verifica dello stato del servizio che, come mostrato in **Fig. 3**, risulta attivo; è possibile procedere con la sua configurazione.

Con il comando ***$sudo nano /etc/vsftpd.conf,*** è stato possibile trovare il file di configurazione di vsftpd.

Nel file sono stati modificati principalmente 2 parametri:

- **Listen=YES** ----> ciò permette di rimanere in ascolto sulla porta 21 e ricevere direttamente connessioni.
- **Local_enable=YES** ----> per permettere agli utenti creati in locale di accedere al servizio

---

5.2) CREAZIONE LISTE FILTARTE

```
└─$ cat xato-net-10-million-usernames.txt | wc -l
3295455
```

Fig.5 Dimensione originale lista username

```
└─$ cat xato-net-10-million-passwords.txt |wc -l
5189454
```

Fig.6 Dimensione originale lista password

```
┌──(kali㉿kali)-[~]
└─$ cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt |grep Jack
Jackson
Jack
Jackie
Jacky
Jackal
Jackoff
Jacko
Jackass
BigJack
JackVal
JackRyan
Jackson5
Jackhammer
Jackey
Jackdaw
BlackJack
Jackyl
Jacksonville
Jackpot
Jackpakk
Jackme
Jackman
JackDaniels
JackDan
JackAnD
Jack123
TheJackal
Jackster
Jackson789
Jacks
```

Fig.7 Filtraggio lista username

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt |grep Jack > xato-usernames.txt

┌──(kali㉿kali)-[~]
└─$ cat xato-usernames.txt | wc -l
1406
```

Fig.8 Dimensione lista username

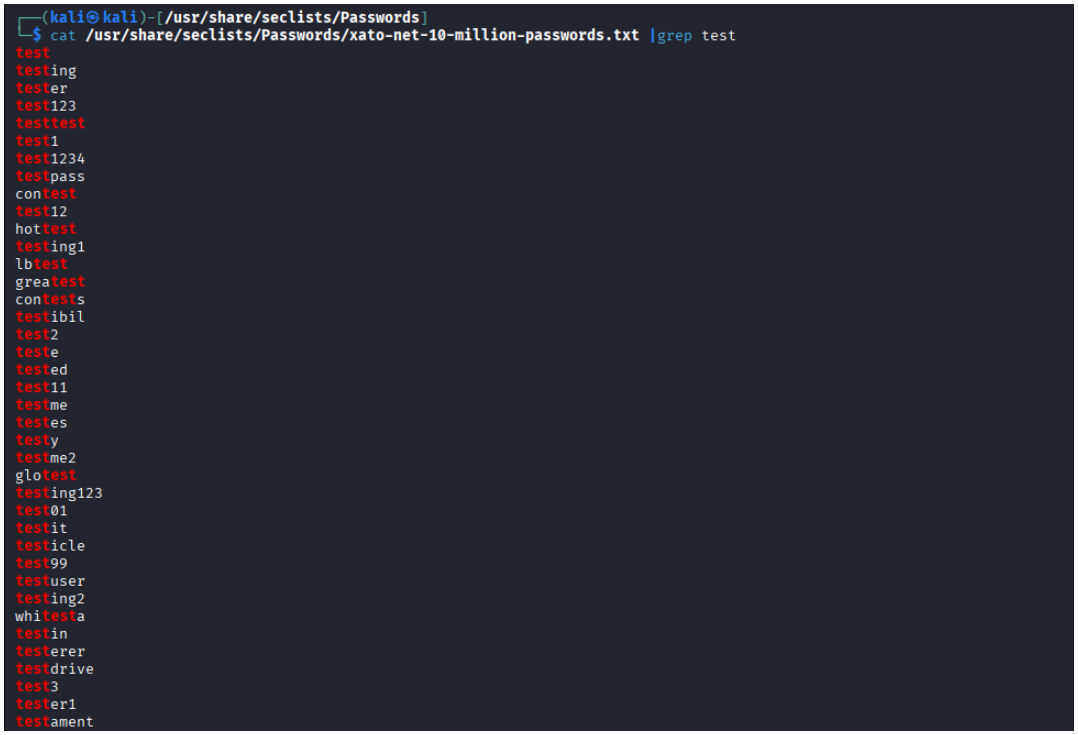

Fig.9 Filtraggio lista password

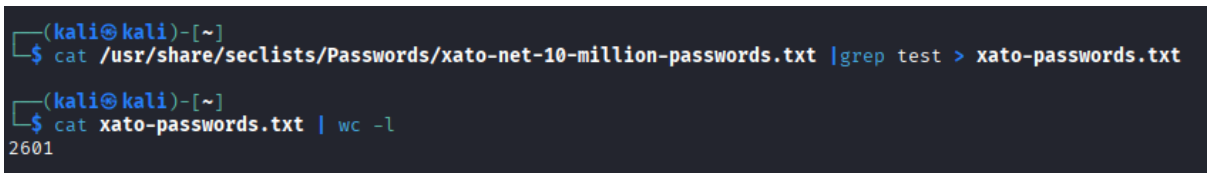

Fig.10 Dimensione lista password

Prima di passare alla fase di cracking, grazie al comando ***$cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt |grep Jack > xato-usernames.txt,*** è stata filtrata la lista degli username in modo da estrarre solo quelli contenenti la parola 'Jack' all'interno di un file **.txt**, riducendo notevolmente il numero.

Questo per evitare tempi di attesa elevati dovuti alla dimensione originaria delle liste come visto dai comandi:

Stesso procedimento vale per le passwords: ***$cat /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt |grep test > xato-passwords.txt***

Viene filtrata la lista delle passwords in modo da estrarre solo quelle contenenti la parola 'test'.

5.3) LOGIN CRACKING W/HYDRA

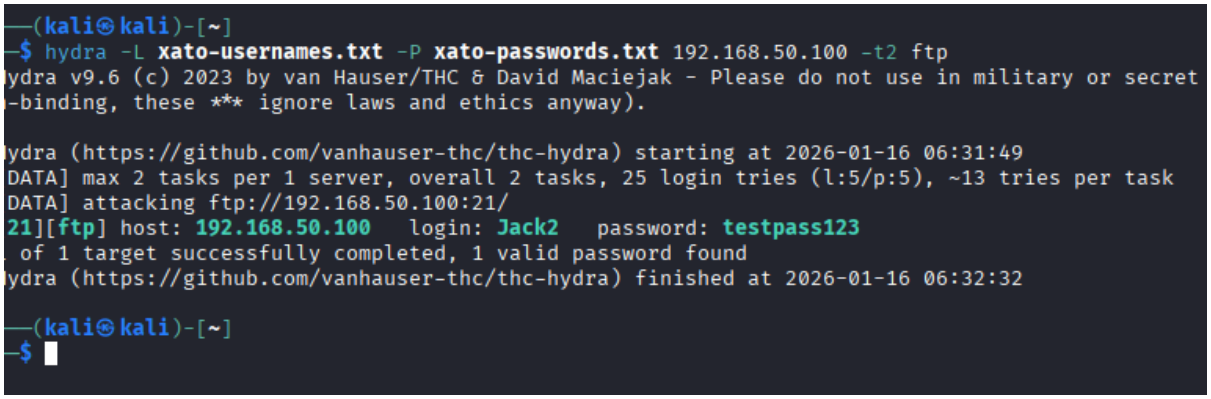

*Fig.11 Cracking credenziali ftp

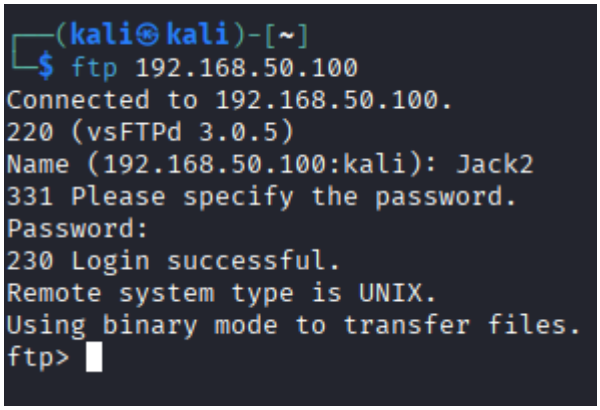

*Fig 12 Accesso al server

Completata la riduzione del numero complessivo di usernames e passwords, si procede con l'utilizzo di **Hydra.**

Per lanciare l'attacco, si utilizza il comando ***$hydra -L xato-usernames.txt -P xato-passwords.txt 192.168.50.100 -t2 ftp*** dove:

- **-L** ---->indica di caricare una lista username
- **Xato-usernames.txt** ----> file contenenti gli utenti Jake
- **-P** ---->indica di caricare una lista password
- **Xato-passwords.txt** -----> file contenenti le password test
- **192.168.50.100** ----> indirizzo IPv4 target (Kali)
- **-t2** ----> numero di thread(chiamate simultanee) per non sovraccaricare il server e la Kali
- **Ftp** ----> protocollo target

Per velocizzare l'esecuzione del test, le wordlist sono state ridotte a 5 utenti e 5 password.

Finita la scansione, come mostrato in **Fig.11,** Hydra ha rilevato le credenziali di un utente, identificando l'username: 'Jack2' e password: 'testpass123'.

In conclusione, il test ha confermato l'effettivo accesso al servizio FTP come utente locale .

---

6)CONCLUSIONE

Il report dimostra come l'uso di credenziali deboli o ripetitive, possa compromettere la sicurezza dell'utente evidenziando come questo fattore non dipenda solo dall'integrità del servizio ma anche dalla corretta gestione degli accessi.

Delle soluzioni per mitigare queste problematiche, possono essere:

- **Passphrase ----->** combinazione di più parole, offrendo maggiore sicurezza es: quattro-cani-mangiano-patate
- **Password Manager ----->**Genera password lunghissime e completamente casuali per ogni singolo sito, memorizza tutto in modo sicuro e garantisce l'unicità es: **k$P9!vR2t&mQz5*W**
- **Attiva Sempre l'Autenticazione a Più Fattori (MFA) ----->** Anche se la password venisse scoperta**,** l'autenticazione impedirebbe all'attaccante di procedere con l'accesso.