AUTHENTICATION CRACKING CON HYDRA - PROGETTO S6/ L5

Autore: Francesco Fontana
Data: 09/05/2025
Piattaforma di Test: Kali Linux 2023 (UTM)
Strumenti:

- SSH daemon (openssh-server)
- VSFTPD (vsftpd)
- THC-Hydra (hydra)
- SecLists (seclists)
- SSHPass (sshpass)

1. Obiettivo e Scenario

Testare la robustezza delle autenticazioni sui servizi di rete SSH e FTP attraverso attacchi a dizionario automatizzati con **THC-Hydra**, evidenziando:

1. Configurazione base dei servizi.
2. Verifica manuale del funzionamento.
3. Esecuzione di attacchi “single credential” e “dictionary attack”.
4. Analisi dei tempi e delle contromisure consigliate.

2. Configurazione dell’Ambiente di Lavoro

Componente	Versione / Dettagli
Kali Linux	2023, Kernel 6.x
OpenSSH Server	8.x
VSFTPD	3.0.5
THC-Hydra	9.x (github.com/vanhauser-thc/thc-hydra)
SecLists	Ultima release dal repository ufficiale
SSHPass	1.09

2.1 Preparazione

sudo apt update && sudo apt upgrade -y
sudo apt install -y openssh-server hydra seclists sshpass vsftpd

2.2 Creazione Utente di Test

sudo adduser --gecos "Test User,RoomNumber,WorkPhone,HomePhone" test_user
# Inserire “testpass” quando richiesto

2.3 Avvio e Verifica dei Servizi

sudo service ssh start
sudo service vsftpd start

# Controllo stato
sudo systemctl status ssh | head -5
sudo systemctl status vsftpd | head -5
Verificare che SSH sia in ascolto su porta 22 e VSFTPD sulla 21:

sudo ss -tlnp | grep -E ":(22|21)"

3. Verifiche Manuali di Connessione

3.1 Accesso SSH

ssh test_user@192.168.20.20
inserire testpass

- **Esito:** Prompt test_user@kali:~$ comparso in < 1s.

3.2 Accesso FTP

ftp 192.168.20.20
at prompt:
Name (192.168.20.20:test_user): test_user
Password: testpass
ftp> quit

- **Output chiave:**
  220 (vsFTPd 3.0.5)

- 331 Please specify the password.
- 230 Login successful.
- 221 Goodbye.
-

4. Attacchi Automatizzati con Hydra

4.1 Modalità “Single Credential” (SSH)

- **Scopo:** Validare la sintassi e il funzionamento di base di Hydra.
- **Comando:**
  hydra -l test_user -p testpass 192.168.20.20 -t 4 ssh
- **Risultato:**
  [22][ssh] host: 192.168.20.20 login: test_user password: testpass

Hydra identifica correttamente le credenziali note in pochi secondi.

4.2 Modalità “Dictionary Attack” (SSH)

- **Wordlist impiegate:**
  - **Usernames:** /usr/share/seclists/Usernames/top-usernames-shortlist.txt (≈5.000 record)
  - **Passwords:** /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt (10.000 record)
- **Comando:**
  hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt \
- -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt \
- 192.168.20.20 -t 8 ssh -V
- **Parametri notevoli:**
  - -t 8: 8 thread concorrenti (bilanciamento tra velocità e carico di rete)
  - -V: output “verbose” per seguire ogni tentativo

- **Durata Indicativa:** ~2 minuti (soggetto a risorse hardware e condizioni di rete)
- **Risultato:** “test_user:testpass” individuata circa a metà delle combinazioni.

4.3 Modalità “Dictionary Attack” (FTP)

- **Comando analogo a SSH:**
  hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt \
- -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt \
- 192.168.20.20 -t 8 ftp -V

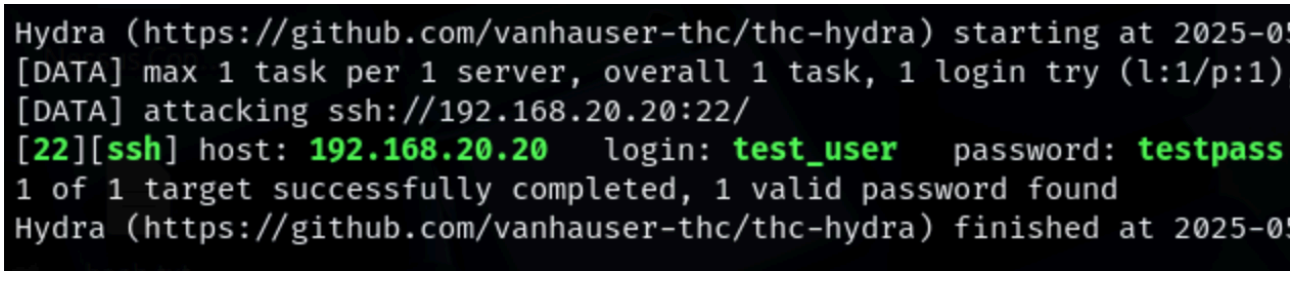
- **Osservazioni:**
  - FTP non cifra le credenziali: tutti i tentativi e la password corretta sono visibili in chiaro sul wire (sniffable).
  - Hydra ha completato il cracking in <1 min a causa della rapidità del protocollo FTP.

5. Analisi dei Tempi e delle Risorse

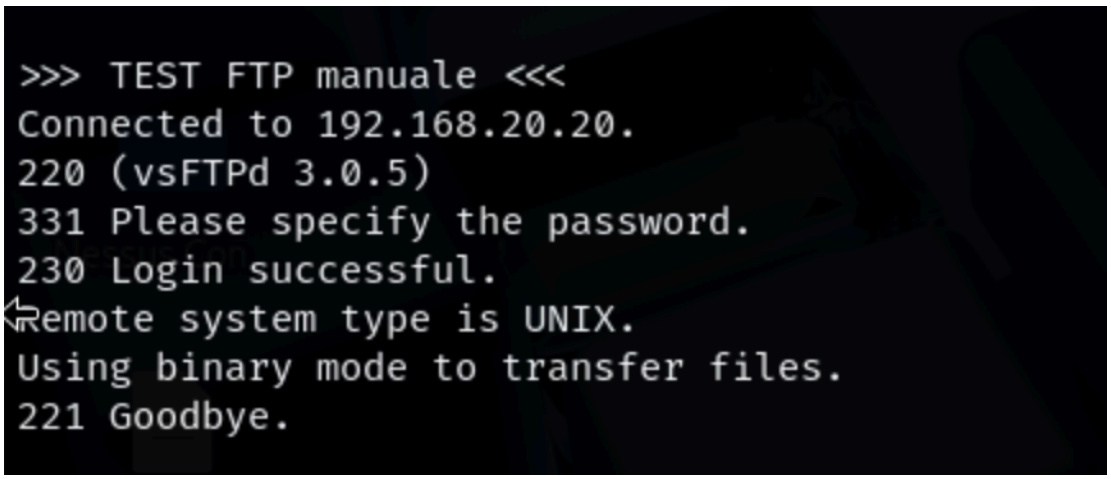
Attacco	Thread	Wordlist Size	Tempo Stimato	Note
SSH – single user/ pass	4	–	< 5s	Credenziali note
SSH – dizionario	8	5k × 10k combin.	~2′	CPU-bound + round-trip network
FTP – dizionario	8	5k × 10k combin.	< 1′	Protocollo più leggero

6. Screenshot dei risultati dei test

1) SSH:



2) FTP:



6. Raccomandazioni di Sicurezza

1. **Password Policy Rigorosa**
    - Minimo 12 caratteri, alfanumeriche, simboli.
    - Scadenza periodica e blacklist di password comuni.
2. **Limiti di Tentativi**
    - Implementare Fail2Ban o equivalente per bloccare IP dopo N tentativi falliti.
3. **Autenticazione a Chiave Pubblica (SSH)**
    - Disabilitare completamente l'accesso via password.
    - Abilitare solo chiavi RSA/ECDSA con passphrase.
4. **Crittografia e Hardening dei Servizi**
    - FTP → migrare a SFTP o FTPS.
    - Disabilitare protocolli obsoleti e versioni vulnerabili.
5. **Monitoraggio e Logging Avanzato**

- Centralizzare i log con SIEM.
- Allarmi in tempo reale su ripetuti insuccessi di login.

7. Conclusioni

L’esercizio ha dimostrato come attacchi a dizionario automatizzati possano compromettere rapidamente servizi con credenziali deboli. L’adozione di misure difensive (strong password, limitazione tentativi, autenticazione a chiave, transport encryption) è essenziale per mitigare tali minacce.