

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 configurerete e craccherete il servizio ftp.

SVOLGIMENTO:

```
Session Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
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 []: 
```

ho creato un nuovo utente con una nuova password

```
Session Actions Edit View Help
GNU nano 8.0 /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(8) for more information.
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
Include /etc/ssh/sshd_config.d/*.conf
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
# Ciphers and keying
#KeyExchange default none
# Logging
#SyslogFacility AUTH
#LogLevel INFO
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
Read 124 lines
Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy To Bracket Where Was Previous Next Back Forward Prev Word Next Word Home End
```

ho testato il nuovo utente con la connessione SSH eseguendo il comando come da screenshot, le credenziali sono giuste perchè ho ricevuto il prompt dei comandi dell'utente `tester_user` sulla kali.

```
Session Actions Edit View Help
(kali@kali)~$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt -t 4 -vv ssh://192.168.50.100

Session Actions Edit View Help
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-17 13:46:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://info@192.168.50.100:22
[INFO] Successful, password authentication is supported by ssh://192.168.50.100:22
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 11 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 12 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "abc123" - 13 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "football" - 14 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "monkey" - 15 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "letmein" - 16 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "696969" - 17 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "shadow" - 18 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "master" - 19 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "666666" - 20 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwertyuiop" - 21 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123321" - 22 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "mustang" - 23 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567890" - 24 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "michael" - 25 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "654321" - 26 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "pussy" - 27 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "superman" - 28 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1qaz2wsx" - 29 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "7777777" - 30 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "fuckyou" - 31 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "121212" - 32 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "000000" - 33 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qazwsx" - 34 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123qwe" - 35 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "killer" - 36 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "trustno1" - 37 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "jordan" - 38 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "jennifer" - 39 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "zxcvbnm" - 40 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "asdfgh" - 41 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "hunter" - 42 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "" - 43 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "buster" - 44 of 8295455000000 [child 2] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
```

ho lanciato il comando da hydra come da screenshot per trovare la password del nuovo utente creato debole di proposito, solo che nonostante vari tentativi non ha trovato la password ho controllato che ssh accetti la connessione e l'autenticazione con password ho riprovato ma niente se per favore nel feedback dell'esercizio mi dici cosa ho sbagliato o se dovevo provare qualche altra cosa così da riprovarci, grazie.

```
(kali@kali)~$ sudo apt install vsftpd
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  libbluray2 libgdata-common libgeoip3 libgd4 libframe1 libgoup2-4 libtheora0 libtheoraenc1 libvpx9 python3-packaging-whl python3-wheel-whl
  libgda36 libgdata22 libgda4-0-alt libqt5ct-common libsigsegv2 libsoup2-4-common libtheoradec1 libudfread0 linux-image-6.12.25-amd64 python3-pyinstaller-hooks-contrib
Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 752
  Download size: 151 kB
  Space needed: 381 kB / 47.7 GB available

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.3 [151 kB]
Fetched 151 kB in 1s (200 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 437915 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.3_amd64.deb ...
Unpacking vsftpd (3.0.5-0.3) ...
Setting up vsftpd (3.0.5-0.3) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty + /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
update-rc.d: I have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.2) ...

(kali@kali)~$ sudo service vsftpd start
```

poi ho installato ftp come da comando come da esercizio ma poi mi sono persa perchè quel giorno quando siamo stati divisi in squadre non mi sembra che l'abbiamo fatto oppure io mi sono persa in questo caso chiedo scusa.