

PASSWORD CRACKING

Morgan Petrelli S6L4

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.

```
└─$ sudo adduser test_user
info: Adding user `test_user' to supplemental / extra groups `users' ...
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] y
info: Adding new user `test_user' to supplemental / extra groups `users'
...
info: Adding user `test_user' to group `users' ...
```

HO INIZIATO CREANDO UN
NUOVO UTENTE CON IL
COMANDO SUDO ADDUSER E HO
ASSEGNATO UN USERNAME
"TEST_USER" E UNA PASSWORD
"TESTPASS"

con il comando `sudo service ssh start` ho
attivato il servizio ssh.
in seguito con il comando `sudo nano
/etc/ssh/sshd_config` ho aperto il file di
configurazione del servizio

```
File Actions Edit View Help
GNU nano 7.2 /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/ga>

# 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
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes

[ Read 122 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

ho usato il comando ssh
test_user@193.168.50.100 per verificare
la connessione in ssh dell'utente creato,
inserendo le credenziali riceveremo il
prompt dei comandi del utente creato

```
(kali@kali)-[~] nrete      epicode_sc...
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be est
ablished.
ED25519 key fingerprint is SHA256:lFF9hMkdnL1BJ0x2X1Dq4deonB2cMjkMzc0Hf
Rj/g58.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of kn
own hosts.
test_user@192.168.50.100's password:
Linux kali 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-
04-09) 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.
```


USO DI HYDRA PER CRACK DELLA PASSWORD

ho usato il comando hydra -L lista_username
-P lista_password INDIRIZZO_IP -t 4 ssh -V
con il quale Hydra utilizzerà l'elenco di nomi
utente e l'elenco di password forniti per
provare diverse combinazioni nel tentativo di
ottenere l'accesso.

Come si può vedere dopo pochi minuti
essendo password molto facili è riuscito a
trovare user e password

```
root@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 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 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 17:15:38
[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, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 5 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 7 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "baseball" - 12 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 13 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 14 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 15 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 16 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 17 of 8295464295456 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 1000003 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 1000007 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 1000008 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 1000009 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 1000010 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 1000011 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 1000012 of 8295464295456 [child 0] (0/0)
```

per la seconda fase
dell'esercizio ho iniziato
installando il server FTP

in seguito ho startato il servizio

```
$ sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libabsl20220623 libadwaita-1-0 libaio1 libappstream5 libatk-adaptor
  libboost-dev libboost1.83-dev libopenblas-dev libopenblas-pthread-dev
  libopenblas0 libpython3-all-dev libpython3.12 libpython3.12-dev
  libstemmer0d libxmlb2 libxsimd-dev python3-all-dev python3-anyjson
  python3-beniget python3-gast python3-pyatspi python3-pypdf2
  python3-pyppeteer python3-pyrsistent python3-pythran python3.12-dev
  xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 143 kB of archives.
After this operation, 353 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b3 [143 kB]
Fetched 143 kB in 1s (266 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 421158 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
update-rc.d: We 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 (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...

(kali@kali)-[~]
$ service vsftpd start
```

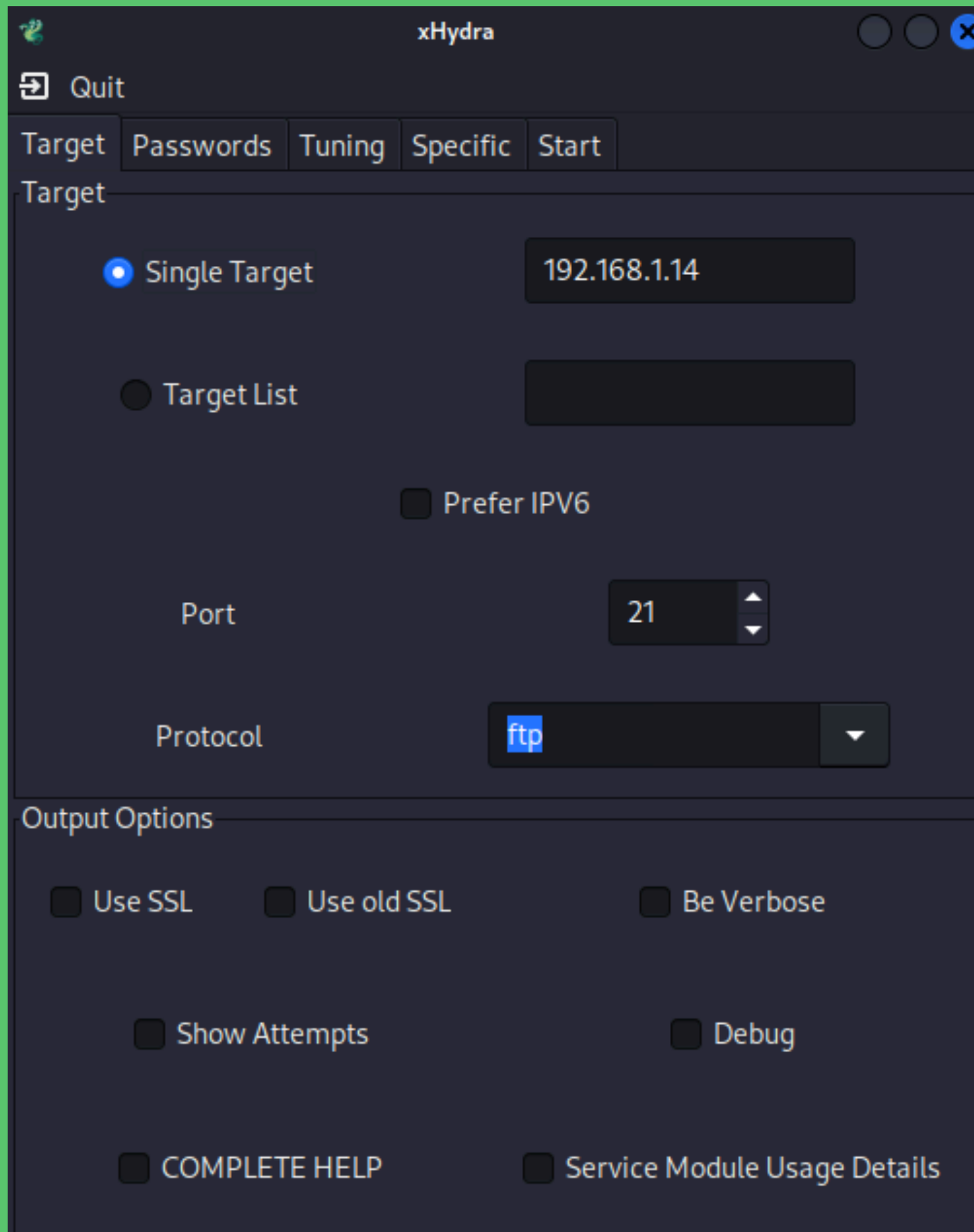
```
$ ftp 192.168.1.14
Connected to 192.168.1.14.
220 (vsFTPd 3.0.3)
Name (192.168.1.14:kali):
```

ho verificato che effettivamente il servizio fosse attivo

```
$ nmap -sV 192.168.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 17:40 CEST
Nmap scan report for kali.station (192.168.1.14)
Host is up (0.00011s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

ho usato nmap per vedere la porta
su cui gira il servizio che mi sarà
utile per Hydra



ho aperto Hydra versione grafica.
Nella pagina "Target" ho inserito l'IP, la porta e il tipo
di servizio che Hydra dovrà cercare di craccare
l'autenticazione

Target

Passwords

Tuning

Specific

Start

Username

☐ Username

☒ Username List

☐ Loop around users

☐ Protocol does not require usernames

yourname

ne/kali/Desktop/user.txt

Password

☐ Password

☒ Password List

☐ Generate

yourpass

ne/kali/Desktop/pass.txt

1:1:a

Colon separated file

☐ Use Colon separated file

☐ Try login as password

☐ Try empty password

☐ Try reversed login

nella pagina "Password" ho inserito la wordlist (ho creato una lista con poche parole altrimenti il processo sarebbe potuto durare ore) su cui Hydra si baserà per craccare l'user e la password

Target	Passwords	Tuning	Specific	Start
Output				
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 17:52:26				
[WARNING] Restorefile (you have 10 seconds to abort... (use option -l to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore				
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 17:52:34				
[WARNING] Restorefile (you have 10 seconds to abort... (use option -l to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore				
[DATA] max 16 tasks per 1 server, overall 16 tasks, 108 login tries (l:12/p:9), ~7 tries per task				
[DATA] attacking ftp://192.168.1.14:21/				
[21][ftp] host: 192.168.1.14 login: kali password: kali				
1 of 1 target successfully completed, 1 valid password found				
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 17:53:08				
<finished>				

dopo poco Hydra ci mostra in output l'user e la password

```
$ ftp 192.168.1.14
Connected to 192.168.1.14.
220 (vsFTPd 3.0.3)
Name (192.168.1.14:kali): kali
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

provando ad inserire le credenziali
verifichiamo che effettivamente siano giuste