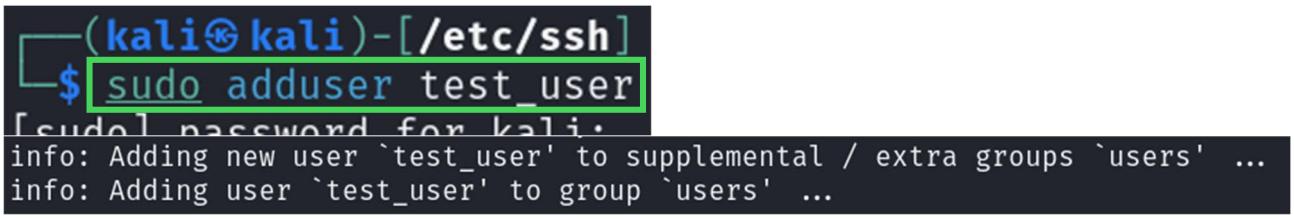
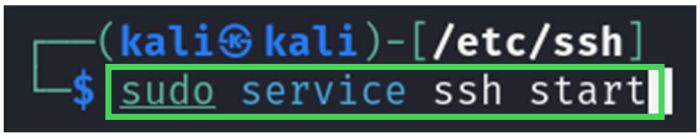
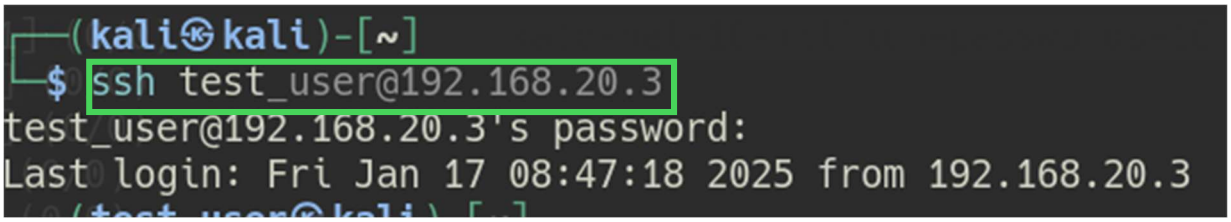
Come primo passo, ho creato un nuovo utente come richiesto, chiamato “test_user” tramite il comando:



Quindi ho avviato il servizio ssh con il comando:

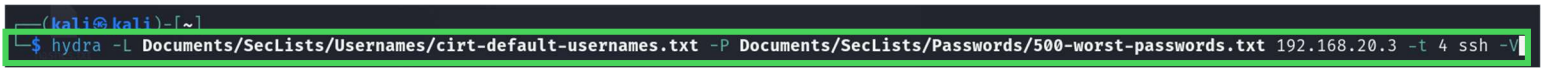


E successivamente testato se l’accesso non desse errori inserendo le credenziali:

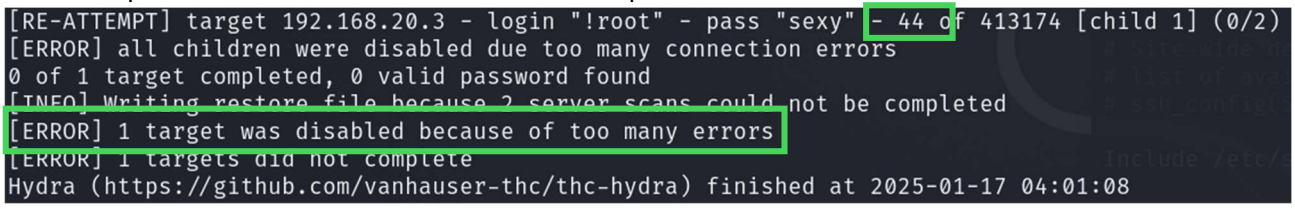


Dopo aver verificato la corretta autenticazione, sono andato a scansionare il target con nmap per vedere se il servizio fosse aperto e su quale porta:

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



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’acceso, ssh è il servizio su cui vogliamo fare la scansione e –V è usato per mostrare a schermo i risultati in tempo reale.



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 accesi.

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, cosí 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 - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Fri 2025-01-17 05:05:38 EST; 8min 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: 11.6M)
        CPU: 247ms
     CGroup: /system.slice/ssh.service
             └─55909 "sshd: /usr/sbin/sshd -D [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]:39680 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 41004 ssh2 [preauth]
Jan 17 05:06:20 kali sshd-session[56166]: Disconnecting invalid user root 192.168.20.3 port 41004: Too many authentication failures [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 c
Jan 17 05:06:20 kali sshd[55909]: drop connection #0 from [192.168.20.3]:39704 on [192.168.20.3]:22 penalty: failed authentication
Jan 17 05:06:20 kali sshd[55909]: drop connection #0 from [192.168.20.3]:39706 on [192.168.20.3]:22 penalty: failed authentication
```

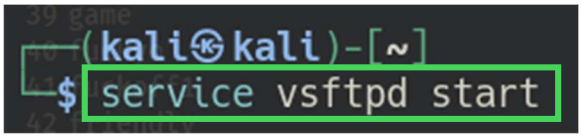
così ho ricercato nel file di configurazione trovando la voce che lo nomina e messa su "no"

```
# 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:



E verificarne lo stato facendo una scansione nmap:

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

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.