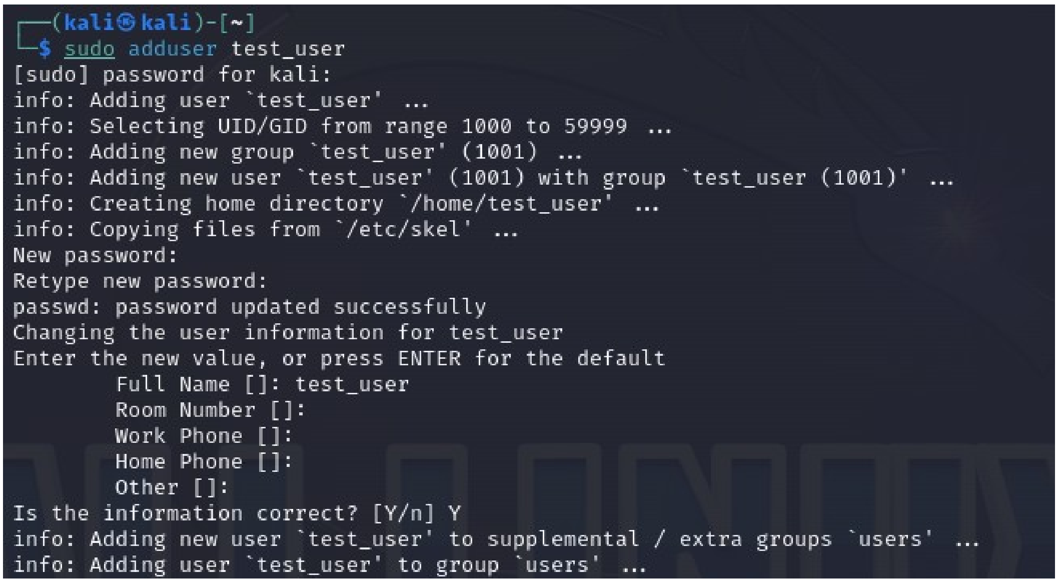
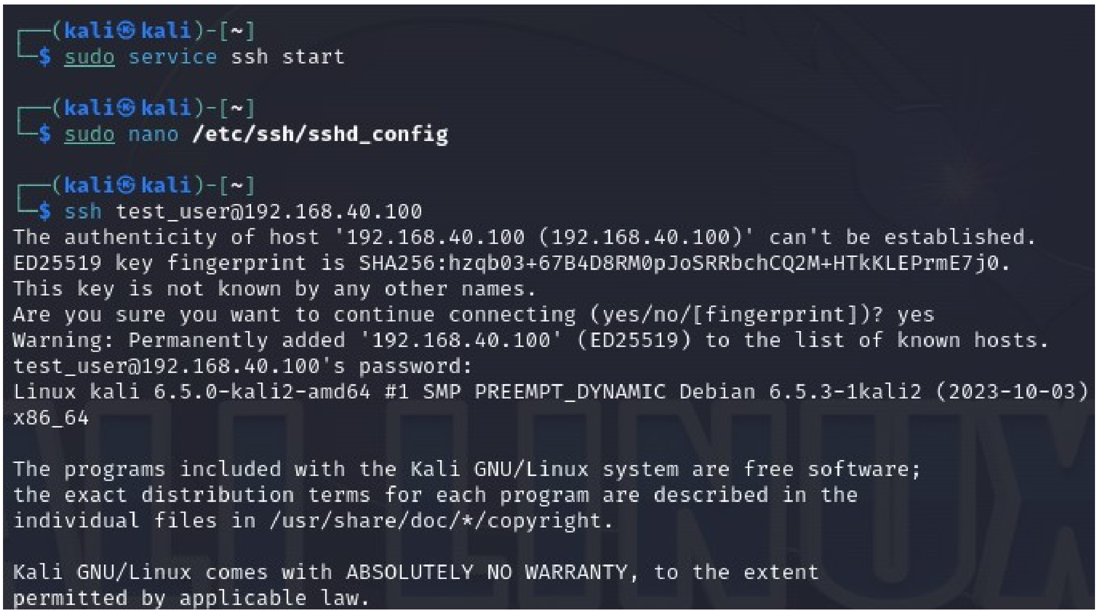
Report Hydra password craking

Nell'esercizio di oggi sono andato a creare un nuovo utente su Kali da usare come test per un attacco tramite Hydra.



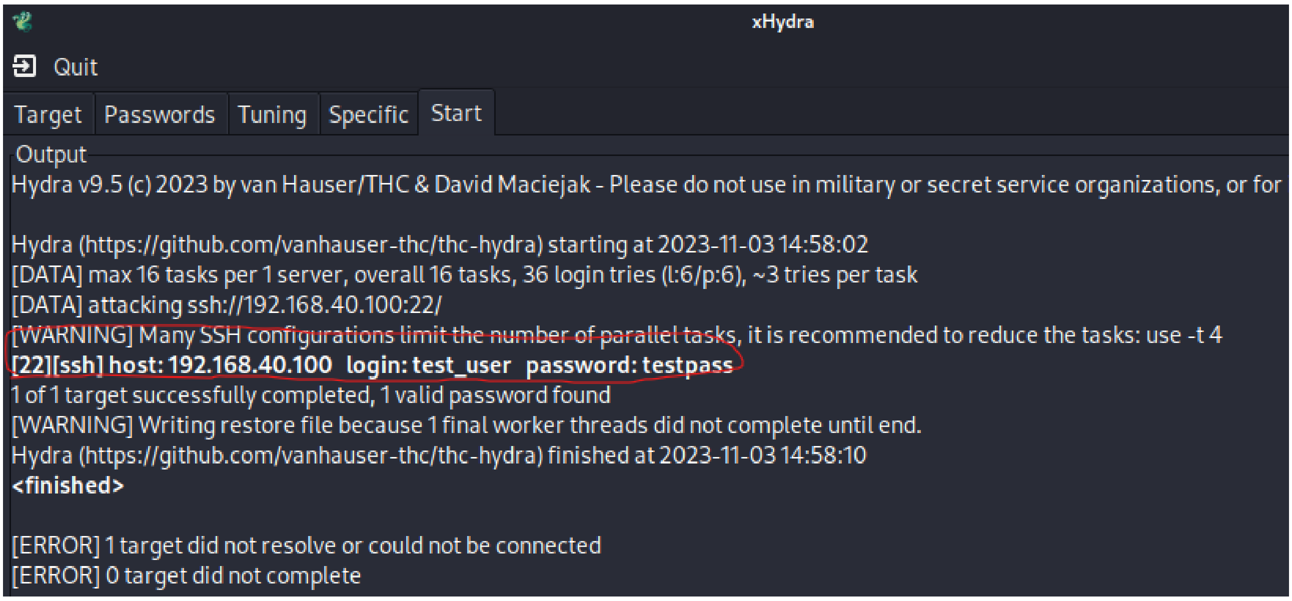
```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home 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' ...
```

Dopodiché ho fatto partire il servizio SSH e testato che funzionasse tramite il nuovo utente.



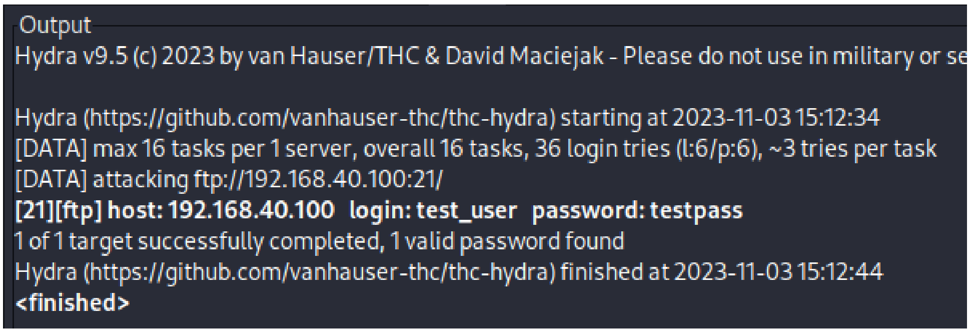
```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start

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

┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.40.100
The authenticity of host '192.168.40.100 (192.168.40.100)' can't be established.
ED25519 key fingerprint is SHA256:hzqb03+67B4D8RM0pJoSRRbchCQ2M+HTkKLEPrmE7j0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.40.100' (ED25519) to the list of known hosts.
test_user@192.168.40.100's password:
Linux kali 6.5.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali2 (2023-10-03)
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.
```

Avendo stabilito che il servizio è in funzione, ho proceduto all'attaco a dizionario tramite Hydra (un attacco che sfrutta liste di username e password comuni). Vediamo che Hydra trova username e password.



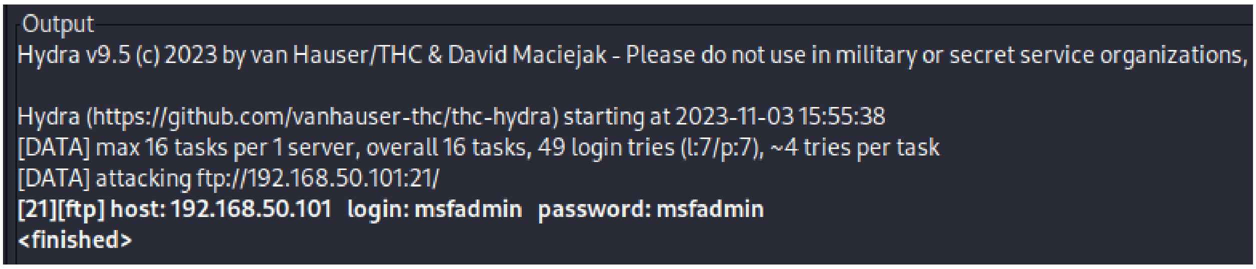
```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 14:58:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ssh://192.168.40.100:22/
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[22][ssh] host: 192.168.40.100   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 14:58:10
<finished>

[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
```

Per la seconda parte dell'esercizio ho installato il protocollo FTP e avviato il servizio, quindi ripetuto la stessa procedura con Hydra, che ha trovato anche in questo caso username e password tramite un attacco a dizionario.



```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 15:12:34
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ftp://192.168.40.100:21/
[21][ftp] host: 192.168.40.100   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 2023-11-03 15:12:44
<finished>
```

Infine ho provato a crackare la password di Metasploitable tramite il protocollo FTP.



```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 15:55:38
[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:7/p:7), ~4 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
<finished>
```