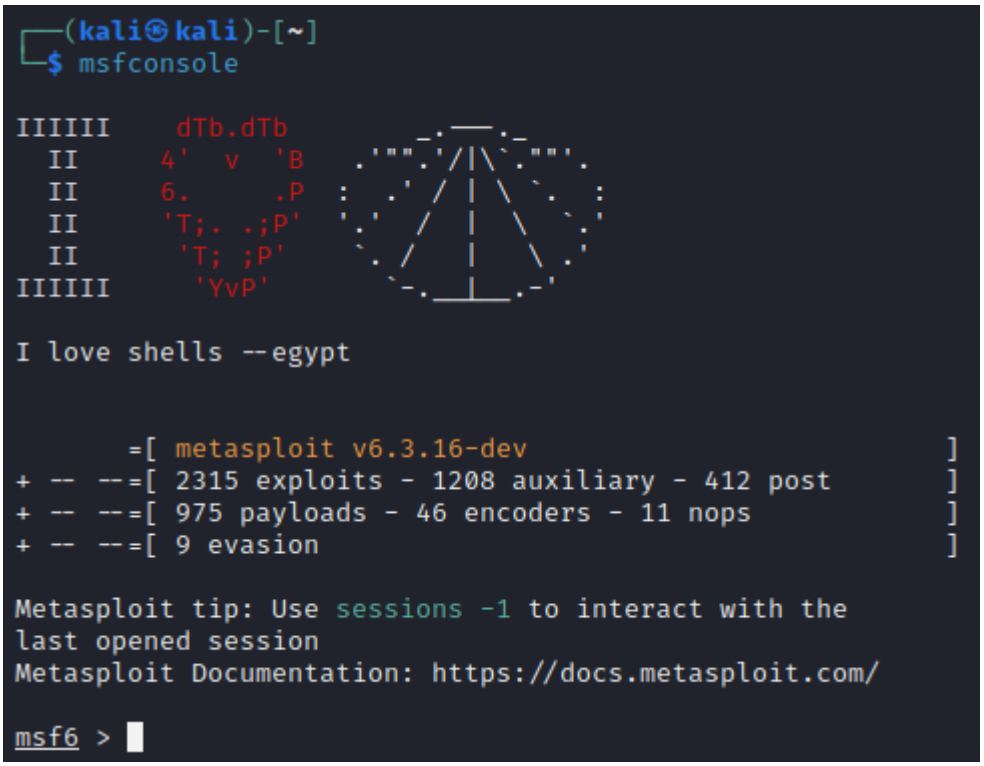
REPORT UNIT 2 WEEK 7

Modulo 2

Avvio con **msfconsole**.

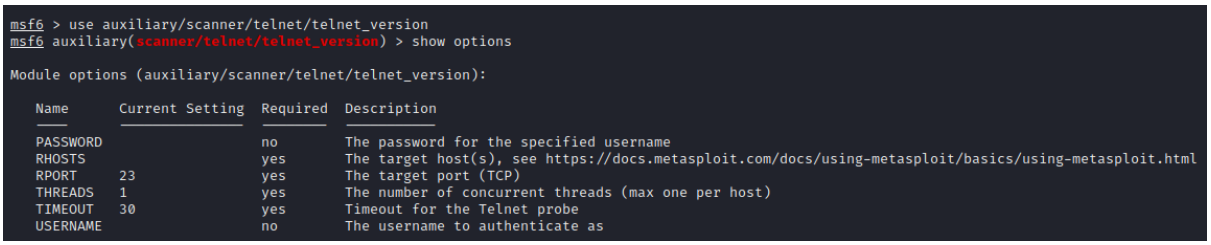


Con **nmap -sV** vedo le porte aperte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-11 18:40 EDT
Nmap scan report for 192.168.50.100
Host is up (0.038s 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;
```

L’esercizio ci chiede di sfruttare telnet (23).
Faccio **search** per la versione telnet richiesta

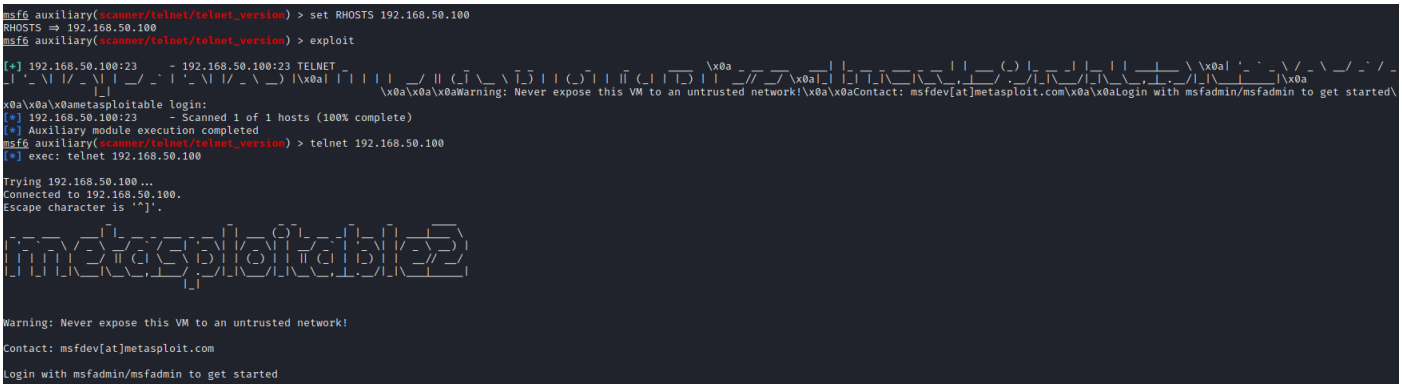
Scelgo il modulo **scanner/telnet/telnet_version** e faccio show options per vedere i parametri necessari.



Imposto il target host con **set RHOSTS** ed uso exploit.

Non sono presenti payloads.

Testo il risultato collegandomi alla telnet ed inserendo username e password trovate.



Infine, esco con **exit** e torno ai comandi principali con **back**.