



```
/home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-07 08:21 EST
Nmap scan report for 192.168.1.40 (192.168.1.40)
Host is up (0.00086s 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?
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
MAC Address: 08:00:27:3D:32:63 (Oracle VirtualBox virtual NIC)
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 69.25 seconds
```



kali@kali: ~

Minimize all open windows and show the desktop

File Actions Edit View Help

```
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
MAC Address: 08:00:27:3D:32:63 (Oracle VirtualBox virtual NIC)
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 69.25 seconds

(kali@kali)-[~]

\$ sudo nmap -sV 192.168.1.40 -p 23

Starting Nmap 7.94SVN (<https://nmap.org>) at 2023-11-07 08:24 EST

Nmap scan report for 192.168.1.40 (192.168.1.40)

Host is up (0.0036s latency).

PORT STATE SERVICE VERSION

23/tcp open telnet Linux telnetd

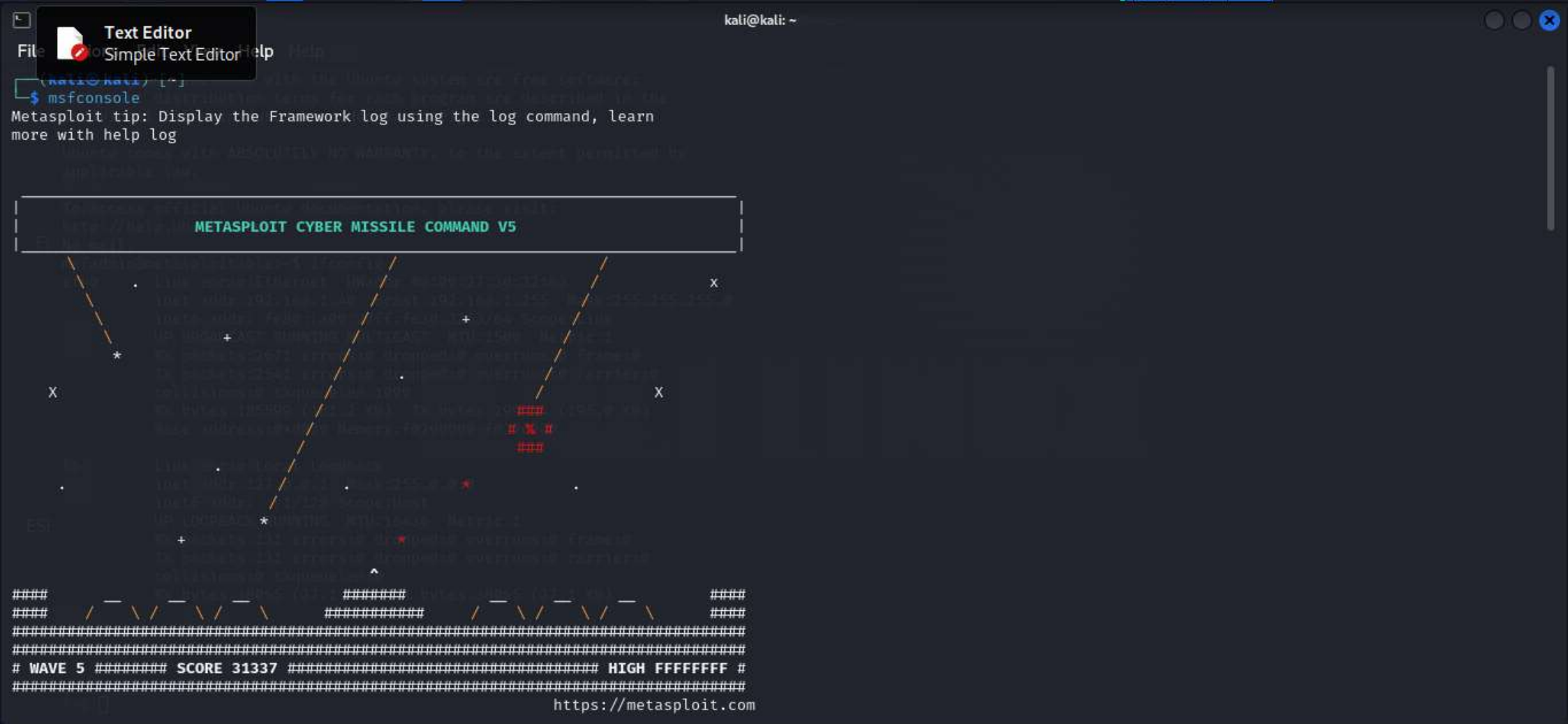
MAC Address: 08:00:27:3D:32:63 (Oracle VirtualBox virtual NIC)

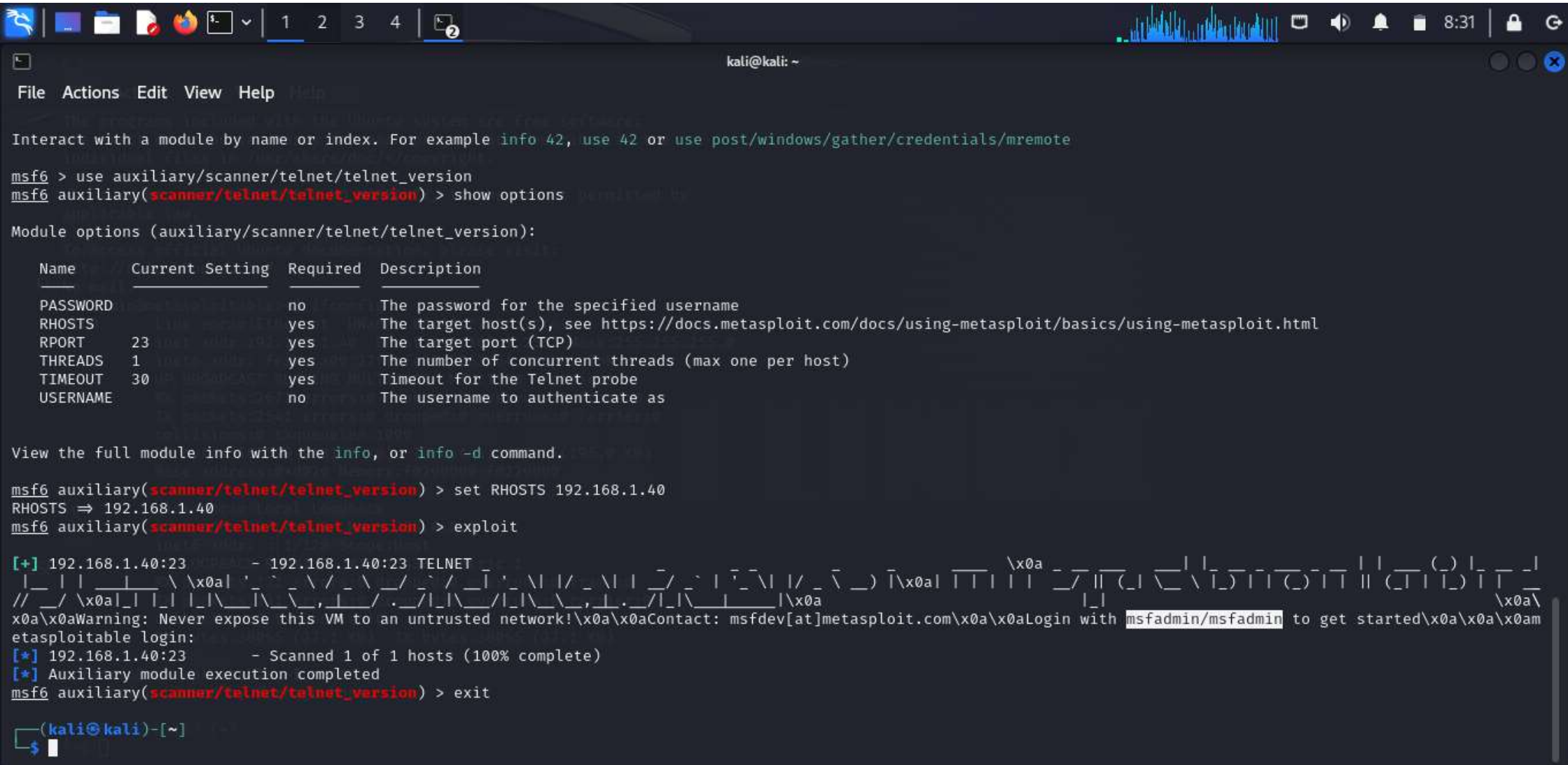
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds

(kali@kali)-[~]

\$






```
File Edit View Help
Simple Text Editor

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
(kali@kali)-[~]
msf6 $ telnet 192.168.1.40
msf6 Trying 192.168.1.40 ...
msf6 Connected to 192.168.1.40.
Modu Escape character is '^]'.

N.
-
P.
R.
R.
T.
T.
U: Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

View
Login with msfadmin/msfadmin to get started

msf6
RHOS
msf6 metasploitable login: msfadmin
msf6 Password:
[+] Last login: Tue Nov  7 08:20:53 EST 2023 on tty1
// Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
x0a The programs included with the Ubuntu system are free software;
etas the exact distribution terms for each program are described in the
[*] individual files in /usr/share/doc/*/copyright.
[*]
msf6 Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ To access official Ubuntu documentation, please visit:
```