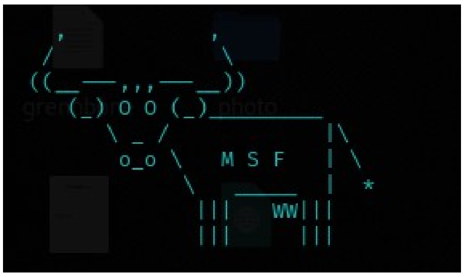
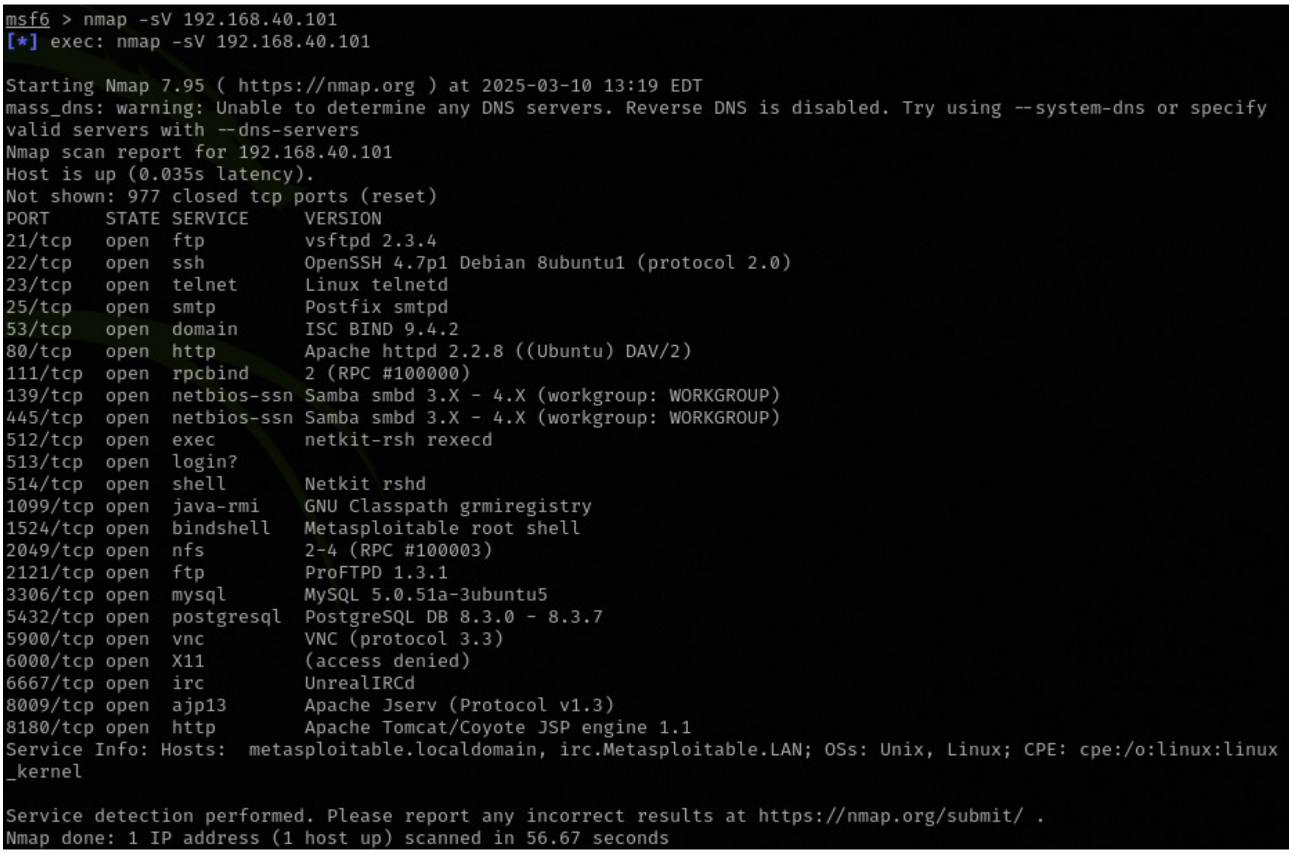
EXPLOIT TELNET CON METASPLOIT



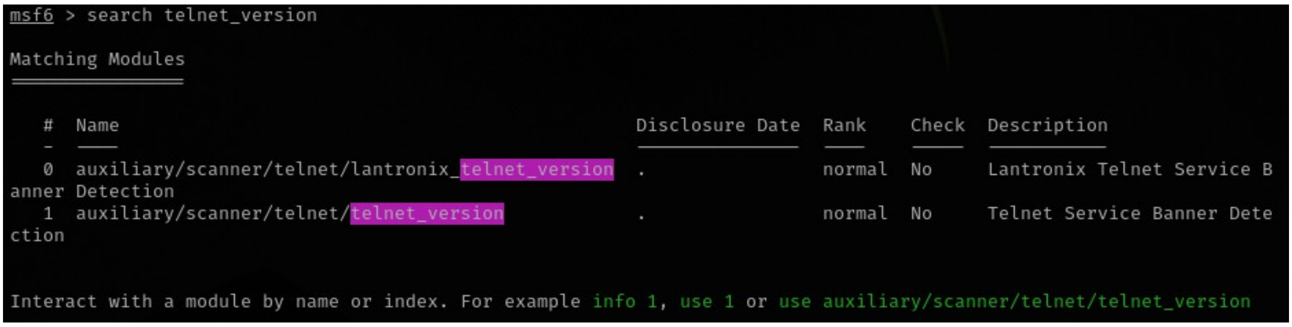
Come da traccia dell'esercizio, sfrutteremo la vulnerabilità relativa a Telnet con il modulo **auxiliary telnet_version**.
Per questo esercizio abbiamo impostato Kali con IP 192.168.50.100 e la Metasploitable2 con IP 192.168.40.101.

Controlliamo le porte aperte con il comando **nmap -sV 192.168.40.101**



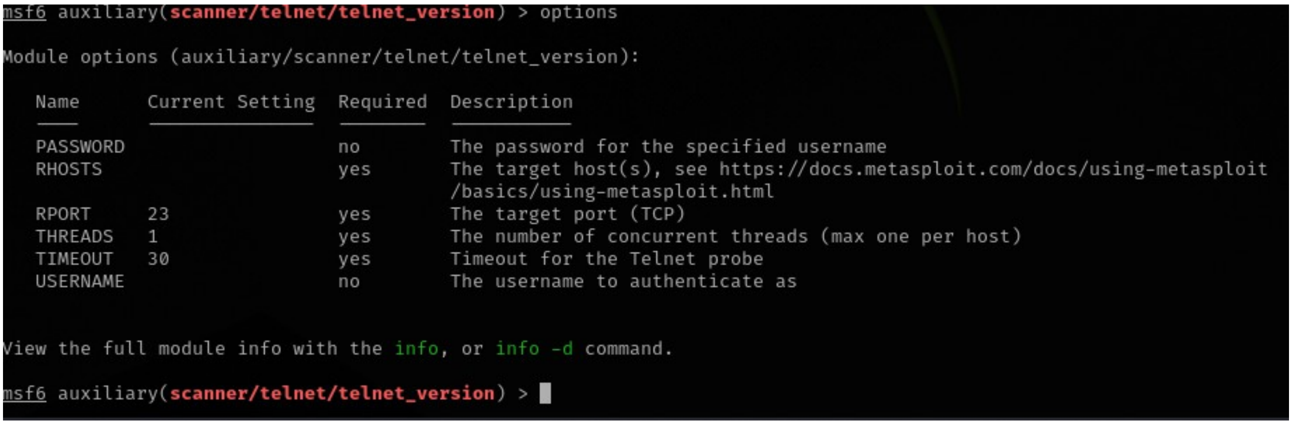
```
msf6 > nmap -sV 192.168.40.101
[*] exec: nmap -sV 192.168.40.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 13:19 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.40.101
Host is up (0.035s 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?
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 56.67 seconds
```

Per sfruttare questa particolare vulnerabilità del servizio Telnet, utilizziamo un modulo ausiliario che potete trovare al path **auxiliary/scanner/telnet/telnet_version**



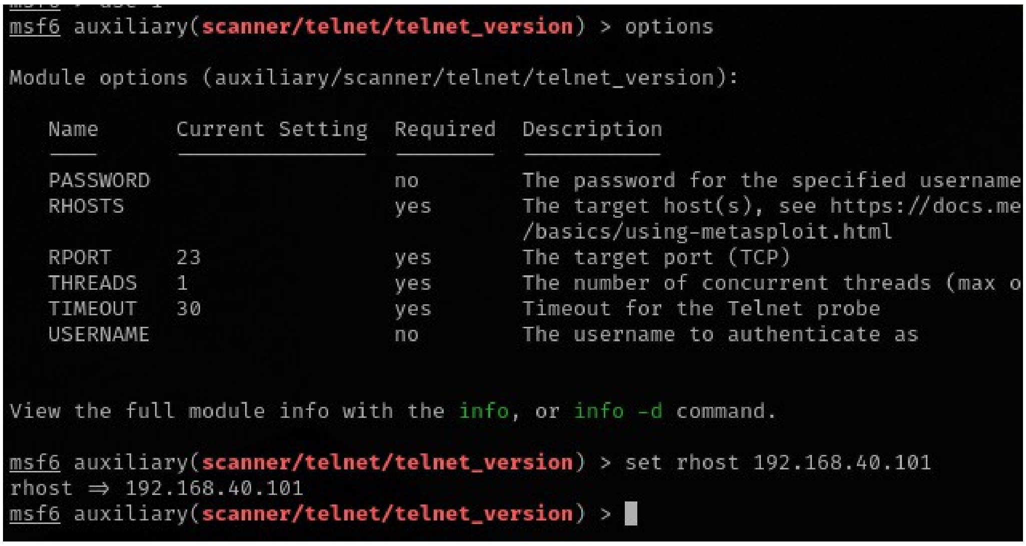
```
msf6 > search telnet_version

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

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .          normal  No     Lantronix Telnet Service B
anner Detection
   1  auxiliary/scanner/telnet/telnet_version              .          normal  No     Telnet Service Banner Dete
ction


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
```

Con options controlliamo quali parametri sono necessari



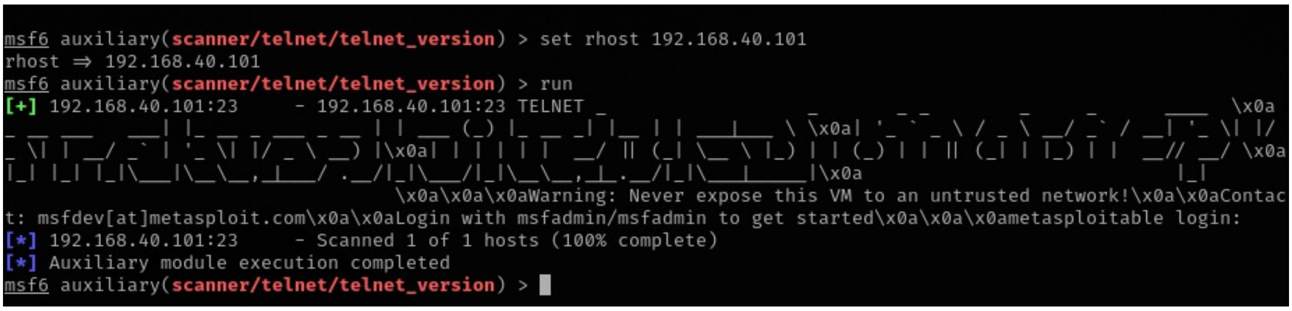
```
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                        /basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Impostiamo l'IP RHOST, cioè quello della macchina target con il comando **set rhost 192.168.40.101**



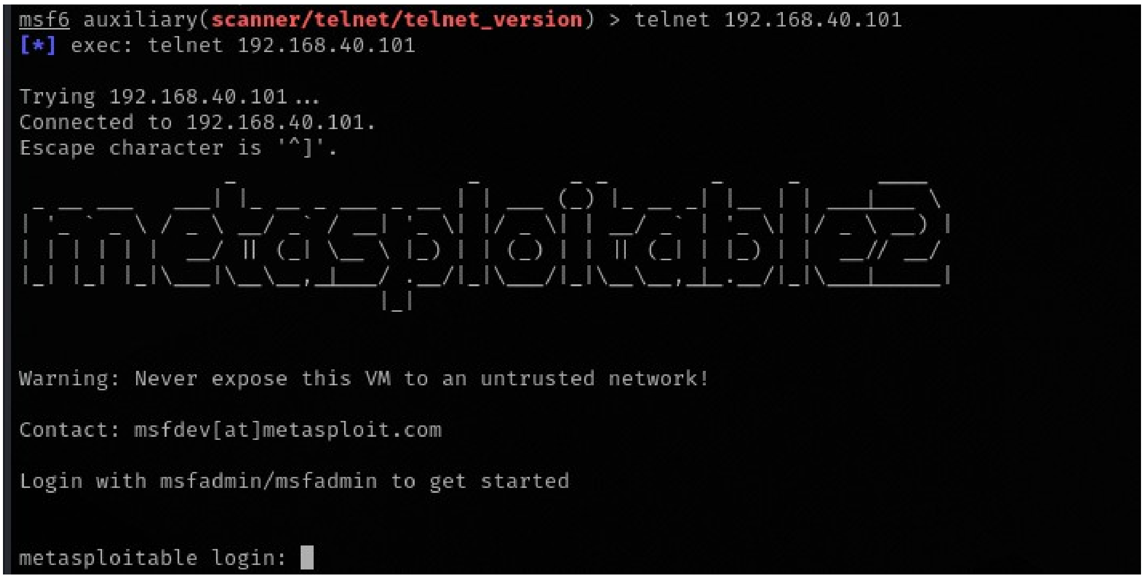
```
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.me
                                        /basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max o
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.40.101
rhost => 192.168.40.101
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Procediamo con il romando **run**



```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.40.101
rhost ⇒ 192.168.40.101
msf6 auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.40.101:23     - 192.168.40.101:23 TELNET _                  _       _ _        _     _      ____  \x0a
_ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/
_ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                            |_|
                                          \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContac
t: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.40.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Il modulo ausiliario ha funzionato. Dando il comando **telnet 192.168.40.101** possiamo notare che riporta alla pagina di accesso della Metasploitable2



```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.40.101
[*] exec: telnet 192.168.40.101

Trying 192.168.40.101...
Connected to 192.168.40.101.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```