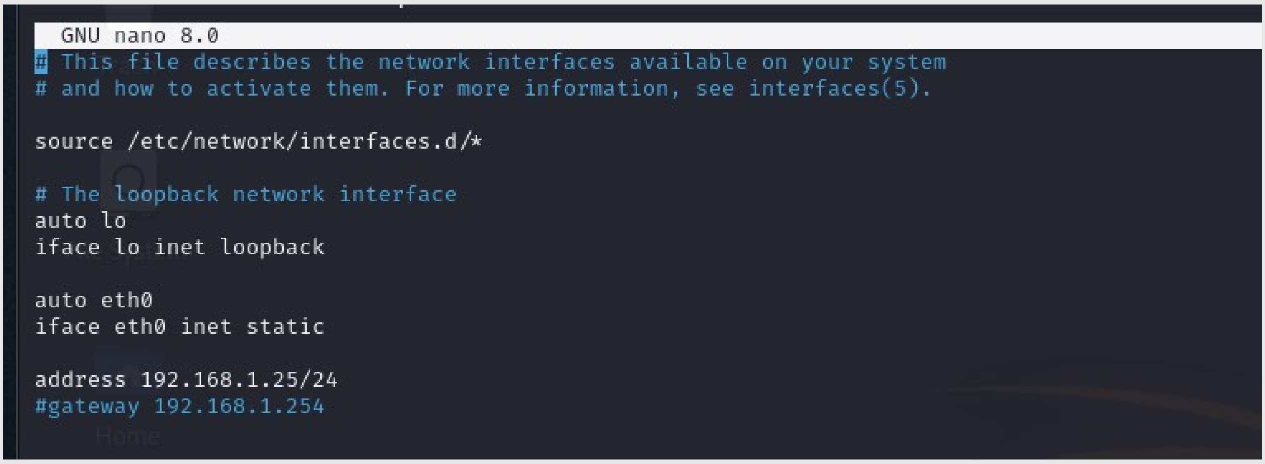
MAURIZIO MARCANTONI

S7/L2

WWW.DATASHIELDS.TECH

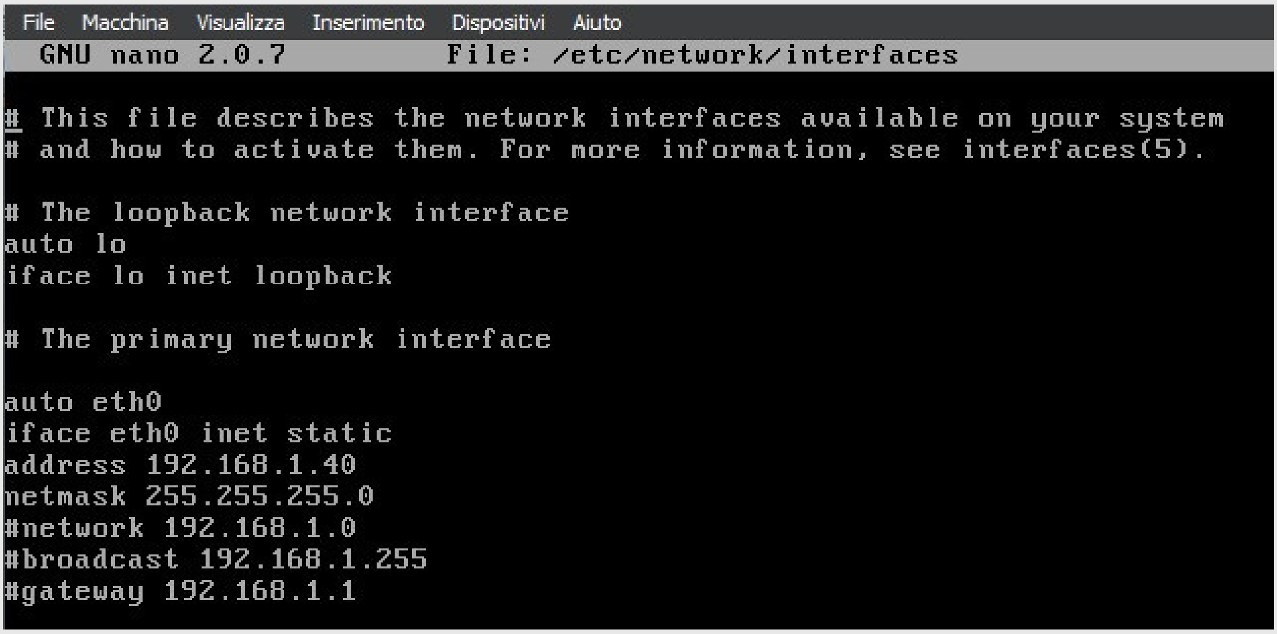
- **CAMBIO IP ALLE MACCHINE KALI E METASPLOIT COME RICHIESTO DALLA TRACCIA:**

KALI 192.168.1.25



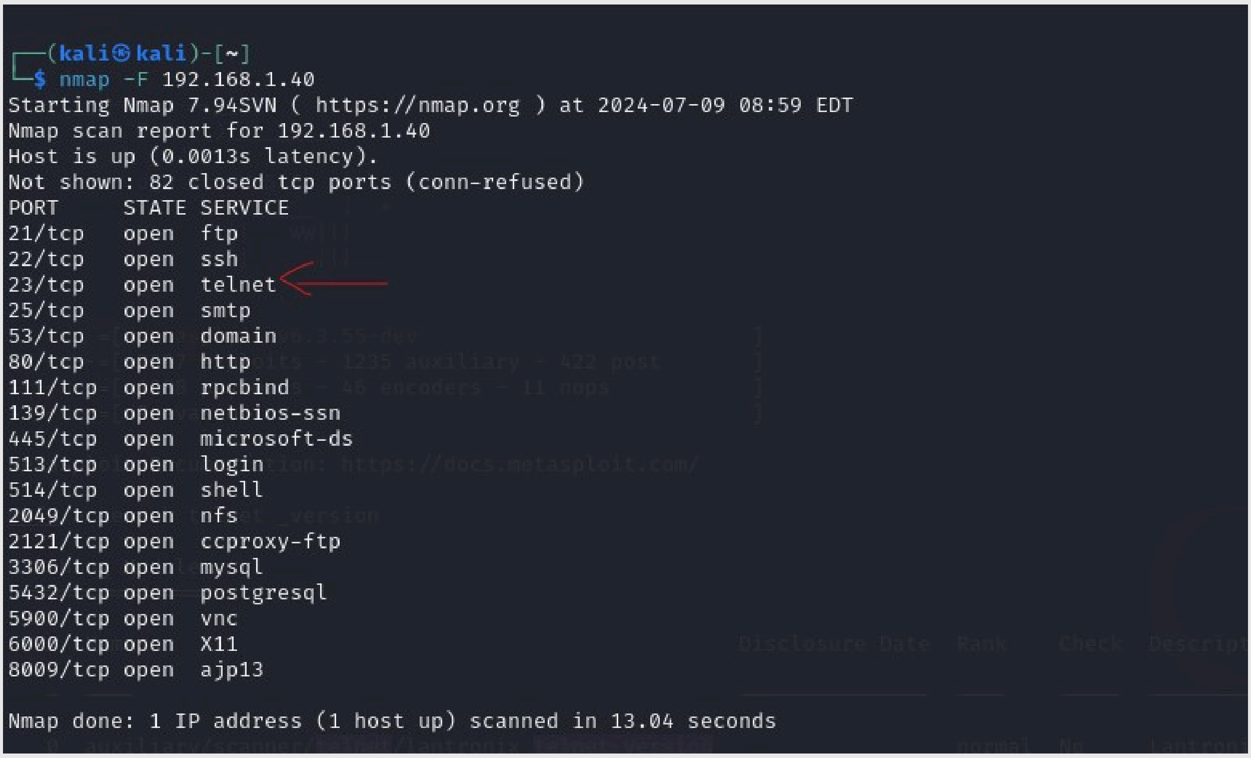
```
  GNU nano 8.0
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static

address 192.168.1.25/24
#gateway 192.168.1.254
```

METASPLOIT 192.168.1.40



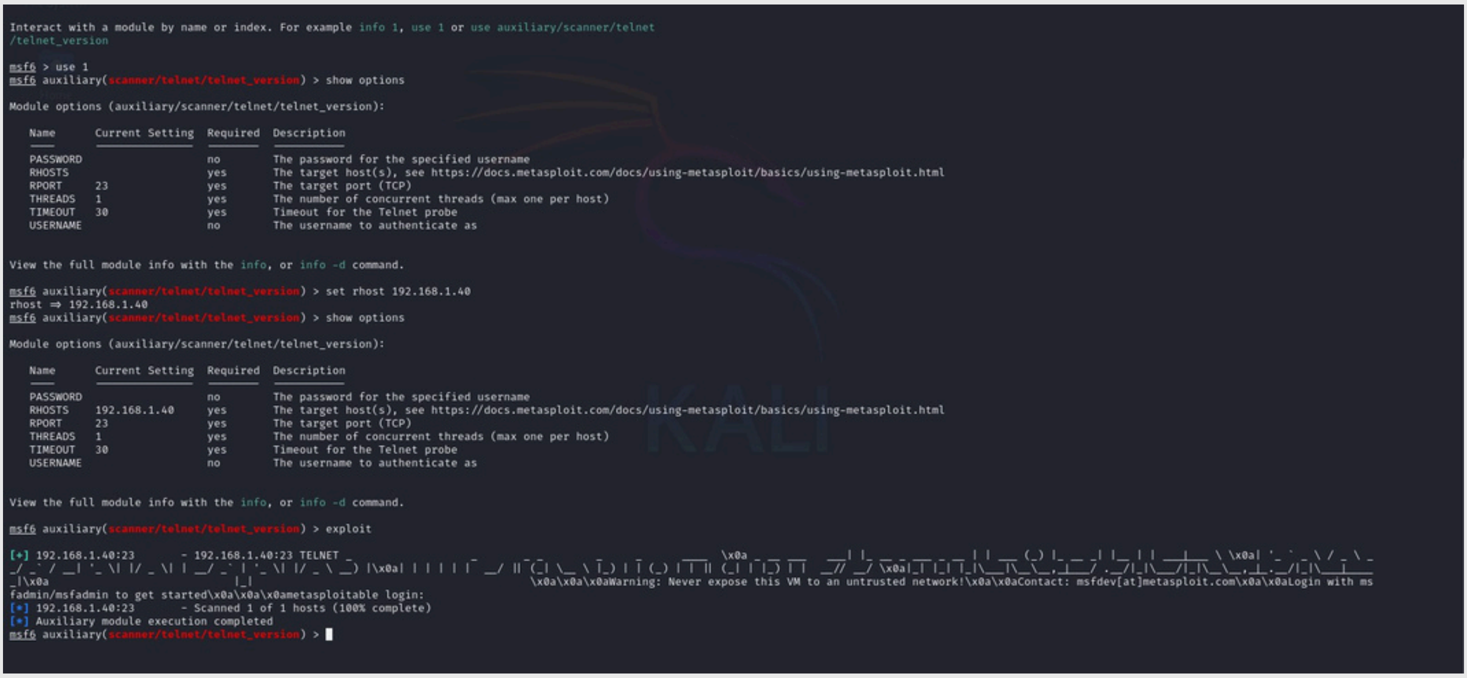
```
  GNU nano 2.0.7           File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
#network 192.168.1.0
#broadcast 192.168.1.255
#gateway 192.168.1.1
```

ANALIZZO CON NMAP LE PORTE CON STATUS “OPEN”. TROVO APERTA LA PORTA TELNET 23



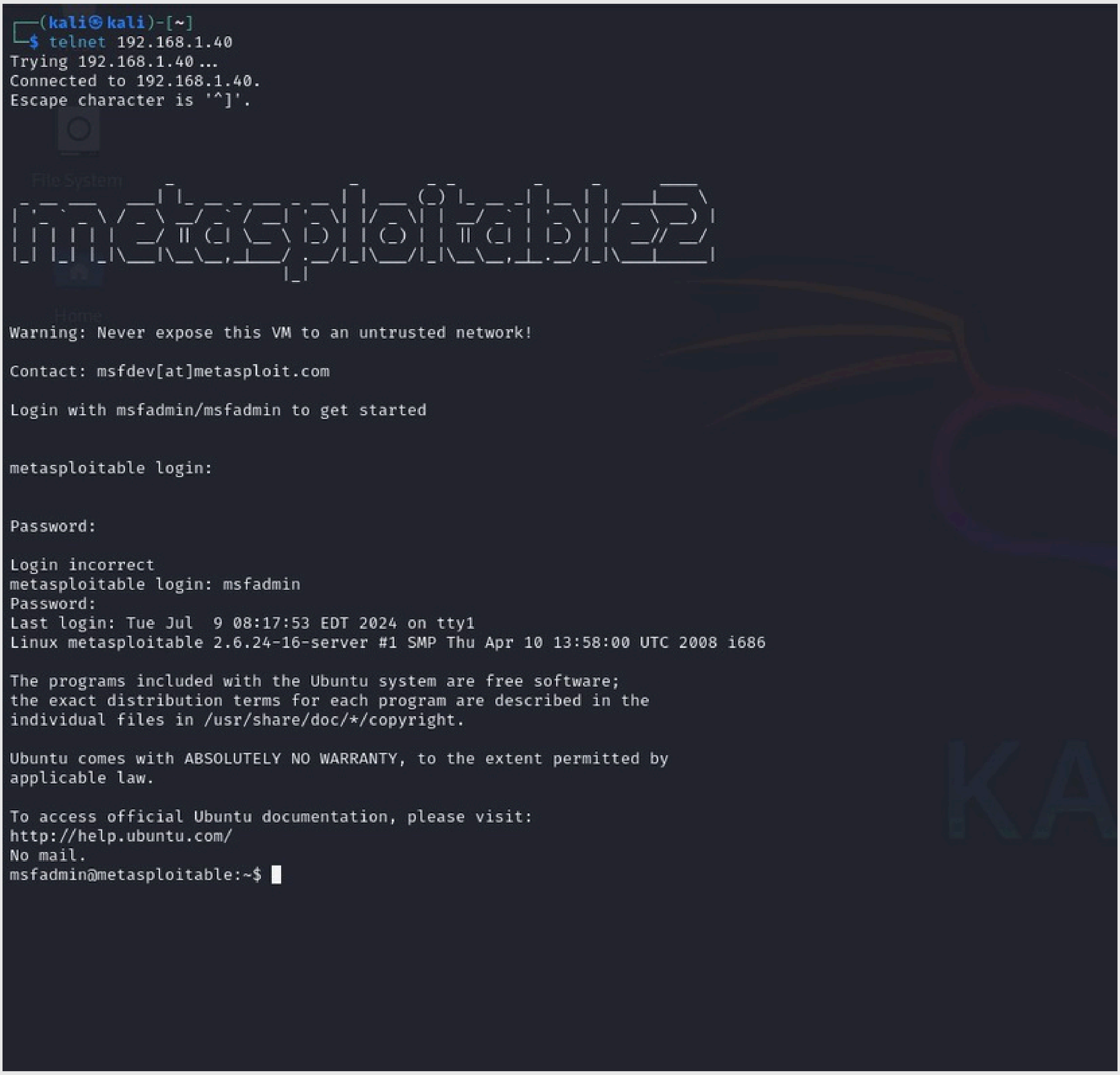
```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 08:59 EDT
Nmap scan report for 192.168.1.40
Host is up (0.0013s latency).
Not shown: 82 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds
```

APRO MSFCONSOLE ED APRO IL TOOL AUXILIARY DI ATTACCO TELNET. SUCCESSIVAMENTE SETTO L’HOST TARGET ED ESEGUO IL COMANDO “EXPLOIT”. SCOPRO COSI LE CREDENZIALI PER ACCEDERE AL SERVIZIO.



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

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show 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) > set rhost 192.168.1.40
rhost ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.1.40     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) > exploit

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _          _ _           _      _          ____     \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ _
_/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____
_|\x0a                          |_|                                        \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with ms
fadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

INSERISCO LE CREDENZIALI OTTENUTE TRAMITE ATTACCO AUXILIARY. EFFETTUO CORRETTAMENTE L’ACCESSO ALLA MACCHINA METASPLOIT



```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
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:


Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Tue Jul  9 08:17:53 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 
```