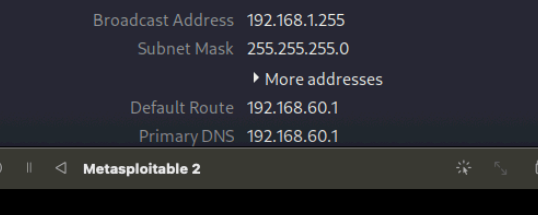


L'esercizio di oggi verteva a sfruttare una vulnerabilità nota in Metasploitable, che presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su canale non cifrato. Questo significa che un potenziale attaccante potrebbe intercettare la comunicazione e rubare informazioni sensibili come username, password e i comandi scambiati tra client e server.



The screenshot shows a Metasploit terminal window with a dark background. At the top, a table displays IPv4 configuration details: IP Address (192.168.1.25), Broadcast Address (192.168.1.255), Subnet Mask (255.255.255.0), Default Route (192.168.60.1), and Primary DNS (192.168.60.1). A link 'More addresses' is visible below the Subnet Mask. Below the table, the terminal shows the command 'sudo /etc/init.d/networking restart' being executed, followed by the output 'Reconfiguring network interfaces...' and 'ioctl: No such process'. Then, the command 'ip addr show' is executed, displaying details for the loopback interface 'lo' and the ethernet interface 'eth0'. The 'lo' interface has an IP of 127.0.0.1 and a scope of host. The 'eth0' interface has a broadcast address of 192.168.1.255 and a scope of global.

IPv4	
IP Address	192.168.1.25
Broadcast Address	192.168.1.255
Subnet Mask	255.255.255.0
► More addresses	
Default Route	192.168.60.1
Primary DNS	192.168.60.1

```

msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces...
ioctl: No such process

msfadmin@metasploitable:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 0a:e9:12:a7:b7:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fd29:93eb:985:5bd1:8e9:12ff:fea7:b73e/64 scope global dynamic
  
```

[illegible]

Il modulo ha recuperato i dati di login del servizio. Ci sta dicendo che le credenziali da utilizzare sono username: «msfadmin», password «msfadmin».

A questo punto per verificare la correttezza delle informazioni eseguiamo il comando **telnet 192.168.1.40** . A questo punto accediamo con le credenziali che abbiamo appena recuperato per verificare che siano corretti, e come ci si può aspettare accederà a Metasploitable

```
Connected to 192.168.1.40.
Escape character is '^]'.

msfdev@metasploitable:~$

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

msfdev@metasploitable:~$ msfadmin login: msfadmin
Password:
Last login: Tue Mar 11 10:40:24 EDT 2025 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.
msfdev@metasploitable:~$
```