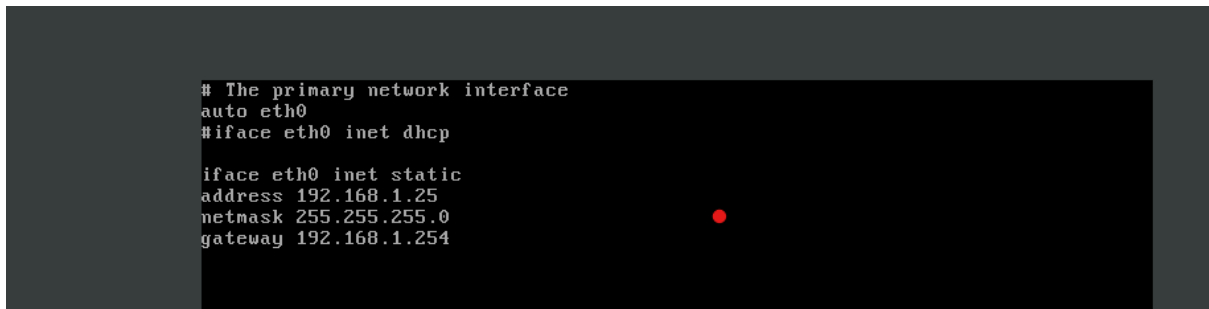


S7L2 - Moduli ausiliari e Telnet

In questo esercizio, abbiamo utilizzato **Metasploit** per condurre una scansione sul servizio **Telnet** della macchina vulnerabile **Metasploitable**. L'obiettivo era raccogliere informazioni di sistema e successivamente accedere con le credenziali fornite. Abbiamo configurato correttamente le macchine virtuali Kali Linux e Metasploitable, eseguendo il modulo `telnet_version` di Metasploit per visualizzare il banner del servizio e verificare l'accesso.



```
# The primary network interface
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.1.25
netmask 255.255.255.0
gateway 192.168.1.254
```

Abbiamo configurato la macchina virtuale **Metasploitable** con l'indirizzo IP **192.168.1.25**. Questa configurazione era necessaria per preparare l'ambiente di esercitazione e garantire che la macchina fosse pronta per l'interazione con Kali Linux. La scelta di un IP statico semplifica la gestione del test. Lo screenshot allegato mostra chiaramente i dettagli di rete impostati, inclusi IP, subnet mask, e gateway, confermando che la macchina è in ascolto sulla rete locale.


```
metasploitable login: msfadmin
Password:
Last login: Tue Nov 12 09:26:49 EST 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:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:db:ad:b1
          inet addr:192.168.1.25  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2a01:e11:1407:3d10:a00:27ff:fedb:adb1/64  Scope:Global
          inet6 addr: fe80::a00:27ff:fedb:adb1/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:230 errors:0 dropped:0 overruns:0 frame:0
          TX packets:220 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20488 (20.0 KB)  TX bytes:21358 (20.8 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:307 errors:0 dropped:0 overruns:0 frame:0
          TX packets:307 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:116395 (113.6 KB)  TX bytes:116395 (113.6 KB)

msfadmin@metasploitable:~$ █
```

Utilizzando le credenziali msfadmin/msfadmin ottenute dal banner, siamo riusciti ad accedere alla macchina **Metasploitable** tramite il servizio Telnet. Questo ha dimostrato l'efficacia del modulo di ricognizione nel raccogliere informazioni critiche. Lo screenshot mostra l'accesso riuscito e la conferma che Telnet è vulnerabile a un semplice attacco di autenticazione. Questo passaggio sottolinea l'importanza di proteggere i servizi esposti nella rete.