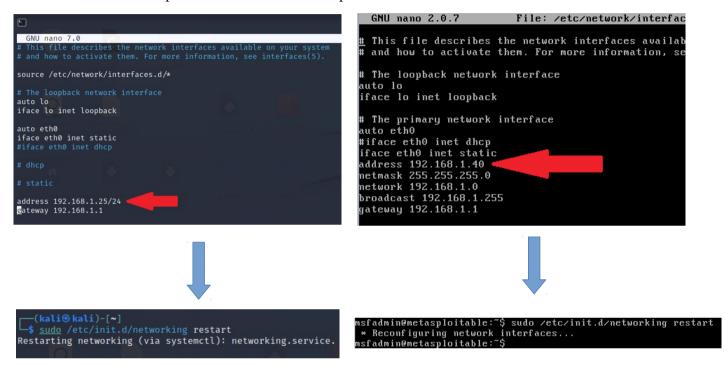
TASK:

Sfruttare la vulnerabilità Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable. Configurare l'IP di Kali con 192.168.1.245 e l'IP di Metasploitable con 192.168.1.40

Per prima cosa tramite il comando sudo nano /etc/network/interfaces sono andato a modificare gli indirizzi IP prima su kali e poi su Metasploitable. Dopo averli cambiati seguendo le indicazioni della traccia ho fatto ripartire i servizi di network per rendere effettivi i cambiamenti:



Prima di procedere ad utilizzare Metasploit ho lanciato nmap per vedere le porte attive e i relativi servizi collegati ad esse e nel riquadro rosso possiamo vedere il servizio tramite il quale attaccare la macchina:

```
(kali® kali)-[~]
$ nmap -p- 192.168.1.40

Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 08:26 EST

Nmap scan report for 192.168.1.40

Host is up (0.00031s latency).

Not shown: 65505 closed tcp ports (conn-refused)

PORT STATE SERVICE
23/tcp open telnet
25/tcp
53/tcp
                                  SMTP
                                 domain
 80/tcp
111/tcp
139/tcp
                                  rpcbind
netbios-ssn
microsoft-ds
                     open
                     open
open
  45/tcp
   12/tcp
                     open
open
                                  login
shell
 513/tcp
 1099/tcp open rmiregistry
1524/tcp open ingreslock
```

A questo punto ho avviato sulla macchina Kali ho lanciato il comando msfconsole e sono andato a cercare il modulo per il servizio auxiliary telnet_version:

Il modulo che ci interessa è il 6 quindi sono andato a selezionare quello:

```
msf6 > use 6
msf6 auxiliary(scanner/telnet/telnet_version) > info
```

Sono prima andato a vedere le informazioni del modulo lanciando il comando info:

```
msf6 auxiliary(
       Name: Telnet Service Banner Detection
    Module: auxiliary/scanner/telnet/telnet_version License: Metasploit Framework License (BSD)
       Rank: Normal
Provided by:
 hdm <xahdm.io>
Check supported:
Basic options:
           Current Setting Required Description
 PASSWORD
                                            The password for the specified username
 RHOSTS
RPORT 23
THREADS 1
TIMEOUT 30
                                           The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
The target port (TCP)
                              yes
yes
yes
                                           The number of concurrent threads (max one per host)
                                            Timeout for the Telnet probe
 USERNAME
Description:
 Detect telnet services
View the full module info with the info -d command.
```

A questo punto sono andato a inserire RHOSTS che sarebbe l'IP della macchina attaccata, nel nostro caso Metsploitable:

```
\frac{\text{msf6}}{\text{RHOSTS}} \text{ auxiliary}(\frac{\text{scanner}}{\text{telnet}} \frac{\text{telnet}}{\text{version}}) > \text{ set RHOSTS } 192.168.1.40
\frac{\text{msf6}}{\text{msf6}} \text{ auxiliary}(\frac{\text{scanner}}{\text{telnet}} \frac{\text{telnet}}{\text{version}}) > \boxed{}
```

Sono andato a controllare se dovessi inserire altre info per effettuare l'exploit e se dovessi inserire il payload ma non si è rilevato necessario:

Ho quindi lanciato l'exploit:

Da esso sono riuscito ad ottenere le informazioni per fare il login. A questo punto, per ottenere i provilegi di root sono andato sulla macchina attaccante e ho eseguito il comando telnet inserendo l'IP della macchina che ho attaccato:

Una volta entrati tramite le credenziali recuperate precedentemente sono andato a fare un comando id per vedere chi fossi (sottolineato in verde). Per ottenere i privilegi di root ho quindi eseguito il comando sudo su (prima sottolineatura in rosso) e ho lanciato nuovamente il comando id per avere conferma di avere ottenuto i privilegi di root (seconda sottolineatura in rosso).