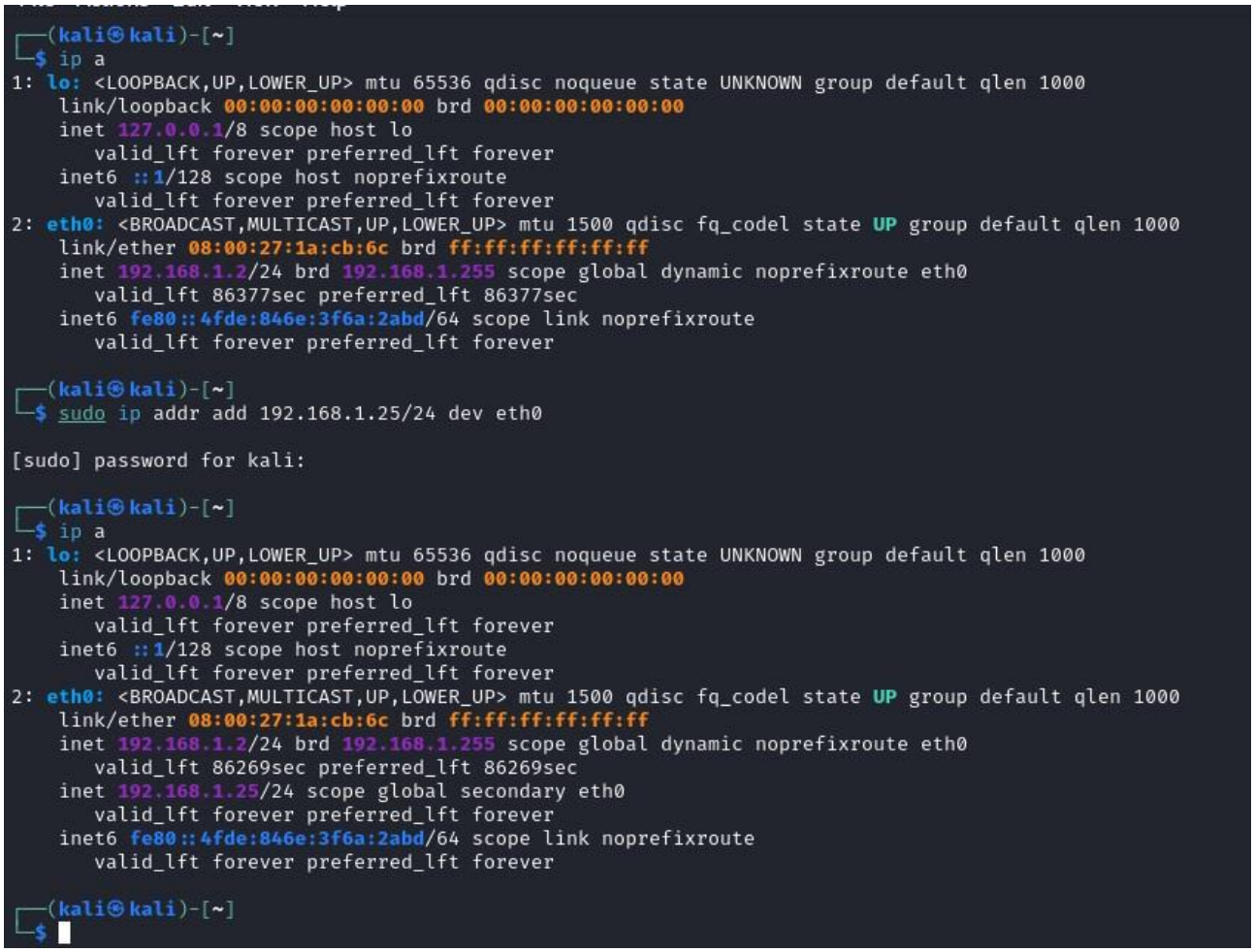
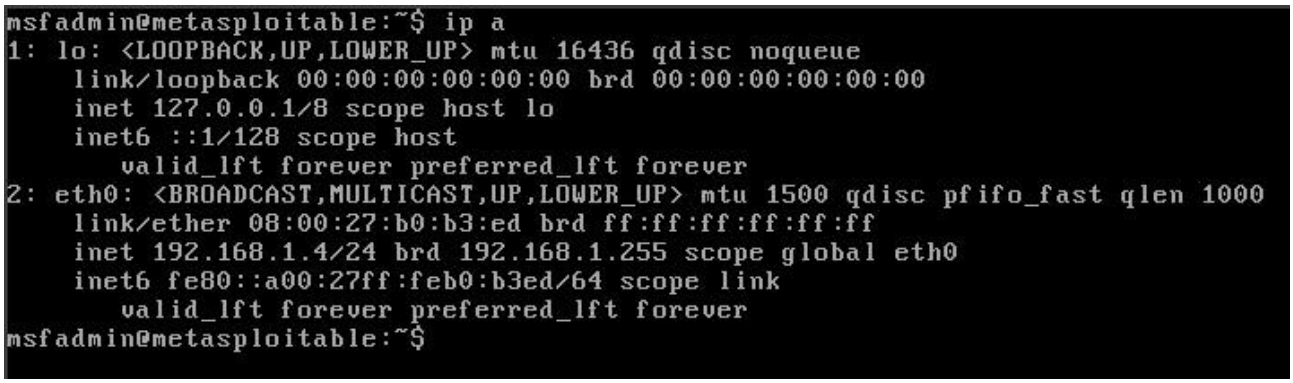
Exploit Telnet con Metasploit

1.Come primo step configuro gli IP come richiesto dall' esercizio:





2.Una volta settate le macchine avvio Metasploit con il comando msfconsole:

3. Dopo aver avviato il tool procedo a ricercare l' exploit necessario per l' esecuzione della traccia:

```
msf6 > search auxiliary telnet_version

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .                normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version            .                normal  No     Telnet Service Banner Detection

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

4. Dall' elenco dei moduli trovati seleziono il numero 1 e poi con il comando options verifico che input mi richiede l' exploit per essere avviato:

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > 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.
```

7. Setto l' RHOSTS inserendo l' IP di Metasploitable2:

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
```

8. Verifico ancora una volta con options che i settaggi siano stati caricati:

```
msf6 auxiliary(scanner/telnet/telnet_version) > 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.
```

9. Con il comando run avvio l’ exploit e ottengo il il Telnet service banner di Metasploitable2:

10. In conclusione su shell classica ho provato ad eseguire il comando telnet + IP Meta per avere in risposta il banner senza i binari: