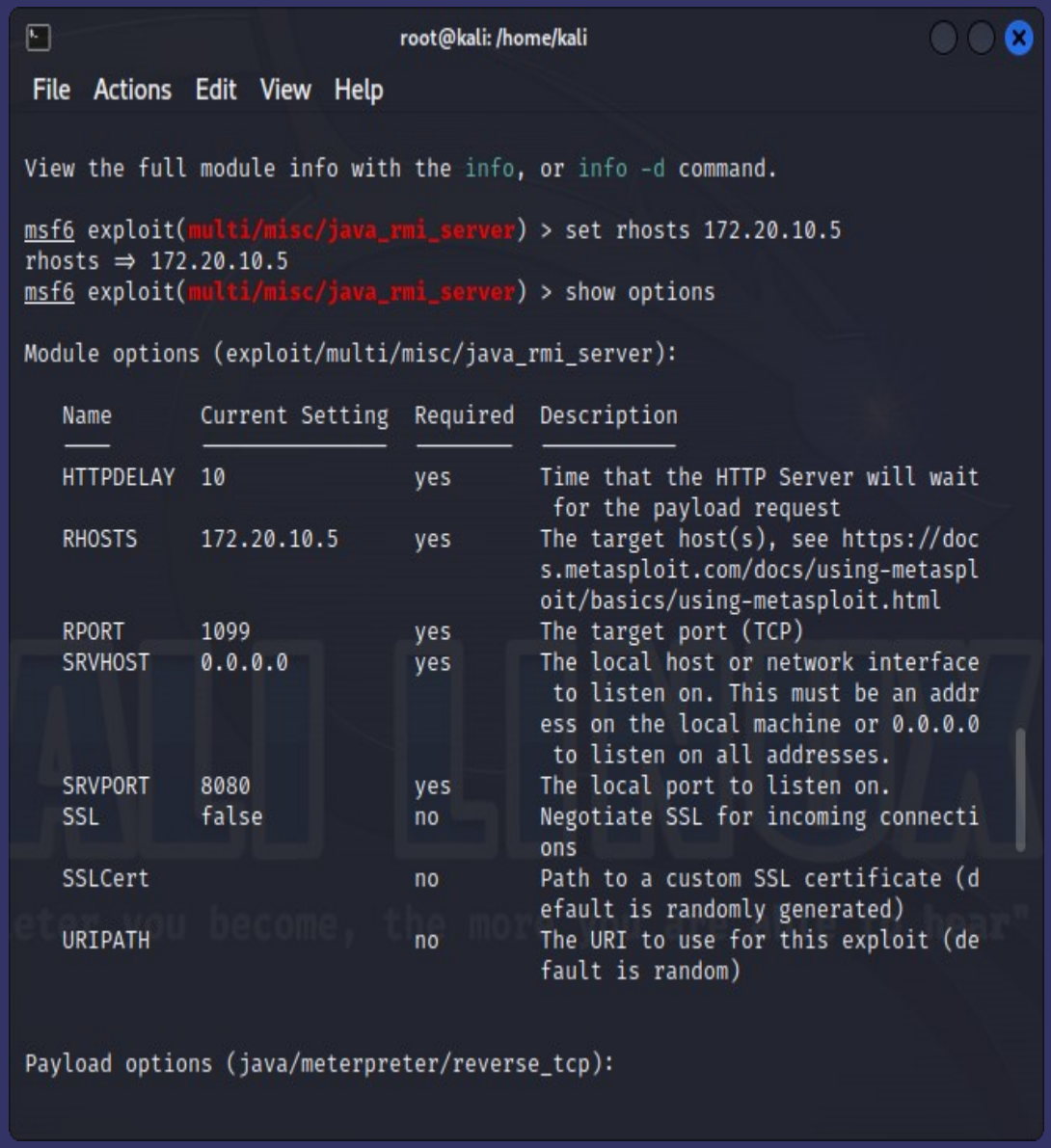
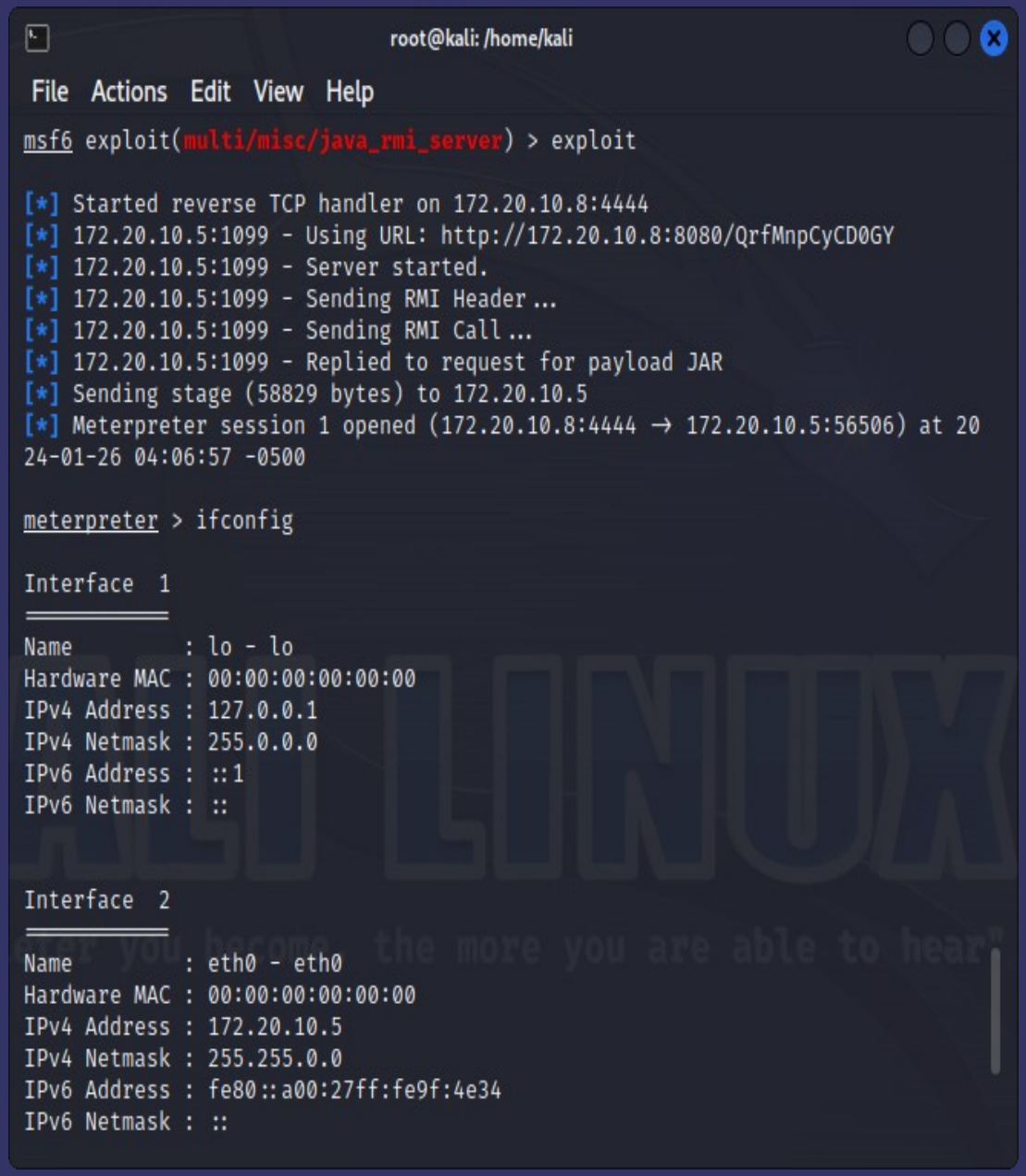
Progetto Settimana 7

Oggi andremo a effettuare una sessione di hacking, tramite metasploit, verso la nostra macchina virtuale metasploitable.
Metasploit è uno strumento di pentesting ampiamente utilizzato, abbina l'exploit a un payload utile e adatto al compito da svolgere.
Un exploit è un programma che, a differenza di un malware, sfrutta una vulnerabilità già presente all'interno del software o hardware, riuscendo cosi a infiltrarsi.
Il payload è il vero e proprio codice nocivo che attacca il target. Riuscendo così a creare un varco da modo a l'host esterno di interagire direttamente con la macchina attaccata.



- Dopo aver avviato sia kali che metasploitable, ho verificato che le macchine comunicassero. Dopo ho effettuato una scansione con “nmap” del nostro target cosi da verificare quali porte fossero aperte. Ho avviato metasplot e ricercato un exploit adatto al nostro target, finita la ricerca, ho impostato solo l'ip del target da attaccare essendo lunico campo obbligatorio vuoto.



- Con il comando “exploit” ho fatto partire l'attacco, andato a buon fine, avviando cosi una sessione di shell tramite meterpreter. Sono riuscito cosi tramite il comando “ifconfig” a visualizzare la configurazione di rete della macchina attaccata, verificando l'effettivo collegamento.

- In fine ho ricercato informazioni della tabella di routing con il comando “router”. Quest'ultima una tabella di dati, memorizzata in un router o in un host, che elenca le rotte di destinazione di una data rete e di ciascuna rotta presente. La tabella contiene informazioni sulla topologia della rete immediatamente circostante.