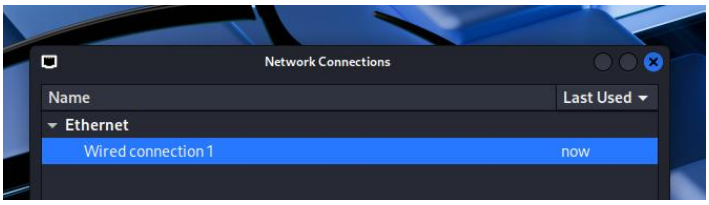
Test day M2S7L5

Traccia:
La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 - Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP 192.168.11.111
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP 192.168.11.112
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
  1) configurazione di rete.
  2) informazioni sulla tabella di routing della macchina vittima.

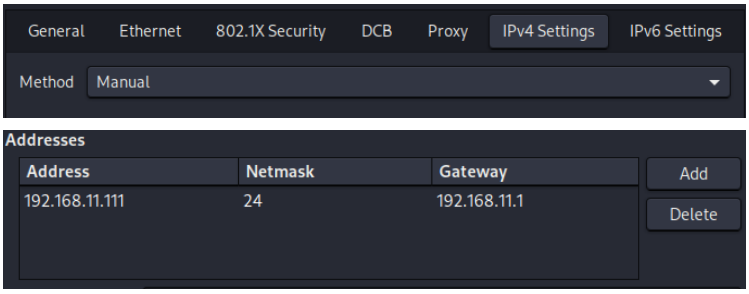
Report

Cominciamo nel settare i diversi ip, iniziando da Kali:

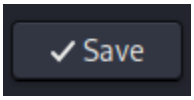


Su wired connection facciamo edit – e modifichiamo i parametri come segue.

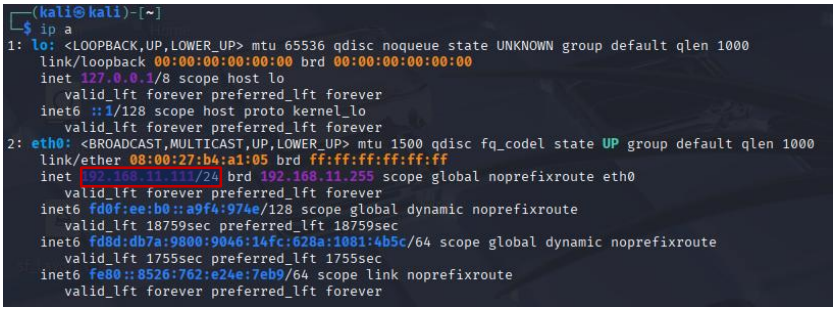
Su IPv4 Settings configuriamo il metodo su manual e settiamo noi l'ip della Kali:



Aggiungiamo l'ip dato dall'esercizio, settando anche la netmask ed il gateway.



Clicchiamo su Save e controlliamo ora il nostro ip.



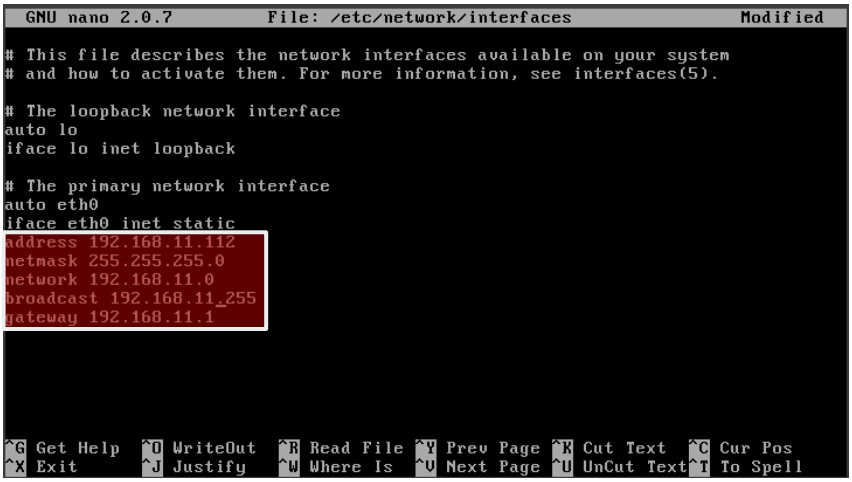
Aperta la console digitiamo il comando *'ip a'*, dove verificheremo appunto il nostro ip cambiato e che il tutto è andato a buon fine.

Passiamo ora a Metasploitable – dove faremo la stessa cosa, per procedere poi con l'exploitation finale.

```
msfadmin@metasploitable:~$ sudo nano /etc/network/interfaces
```

Una volta fatto il login come admin – lanciamo il comando '*sudo nano /etc/network/interfaces'*.

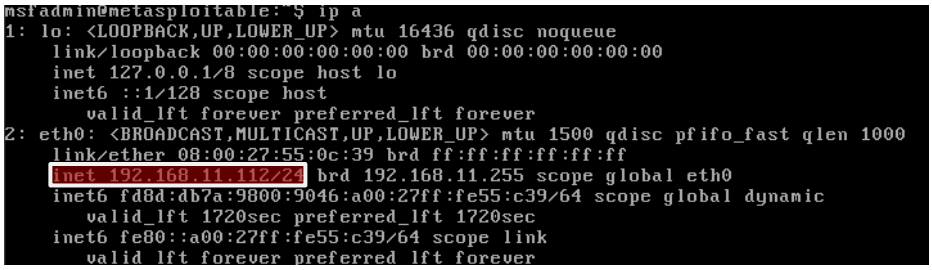
Questo comando aprirà un file nano a parte, dove potremo modificare i parametri del nostro ip su Metasploitable così di seguito:



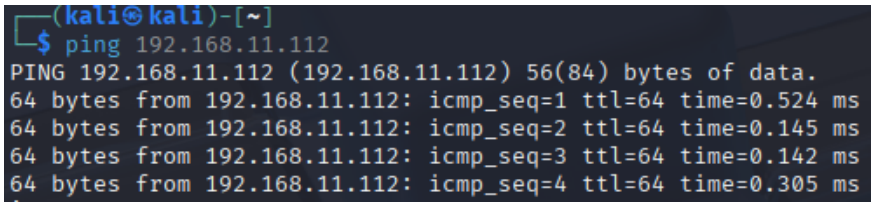
Inseriamo a questo punto tutti i parametri necessari, quali:

- address 192.168.11.112
- netmask 255.255.255.0
- broadcast 192.168.11.255
- gateway 192.168.11.1

Salviamo e riavviamo la macchina.



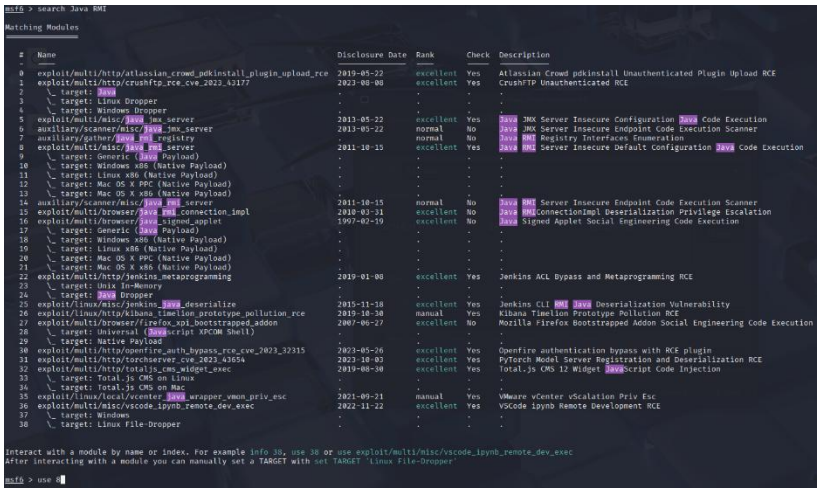
Una volta riavviata la nostra macchina, con il comando **'ip a'** verifichiamo che tutto sia andato a buon fine.



Facciamo il test finale pingando Metasploitable da Kali, e come vediamo le due macchine sono nella stessa subnet e comunicanti.

A questo punto le nostre macchine sono pronte. Avviamo ora **msfconsole** per exploitare Metasploitable.

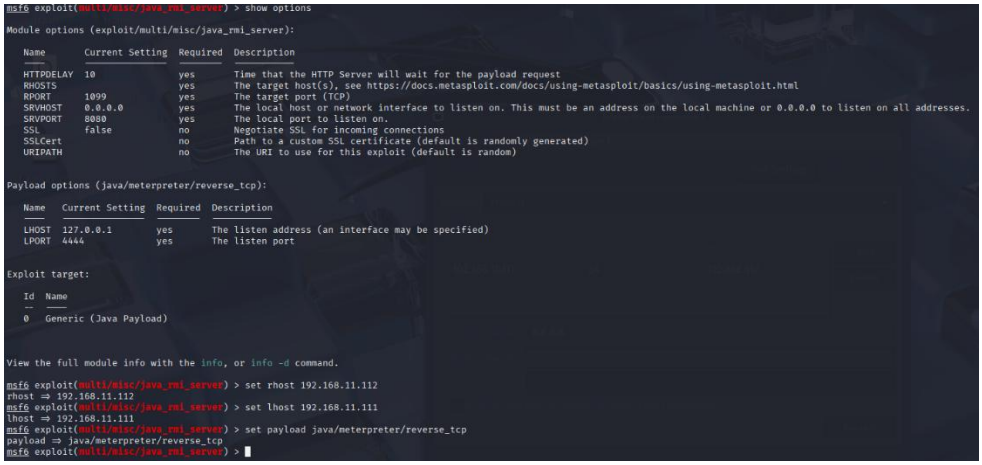
Su Kali avviamo *'msfconsole'*:
Purtroppo oggi non sono stata molto fortunata, non ho ricevuto il cuore rosso in risposta al comando in questione – (ogni volta esce un'immagine casuale) pare che il cuore rosso sia il più raro e rinomato tra i simboli che appaiono.
La leggenda narra che se riceviamo in risposta un cuore, tutte le nostre sessioni di exploit andranno a buon fine.
Sfideremo oggi la nostra sorte provando a farlo funzionare anche senza la benedizione di msfconsole.



Una volta avviata usiamo il comando *'search Java RMI'* e confrontiamo i risultati nella ricerca dell'exploit che utilizzeremo.

Individuato il nostro exploit lo avviamo con *'use 8'* – e procediamo a settare i parametri necessari alla riuscita dell'attacco.

Di seguito possiamo vedere il settaggio completo:

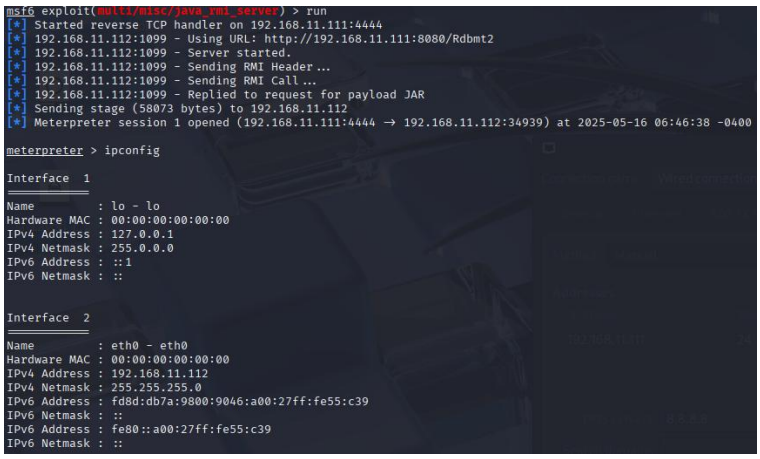


Configurando *RHOST* – l'ip della vittima in questo caso la nostra Metasploitable e *LHOST* l'ip della macchina attaccante in questo caso la nostra Kali, ed il **payload appropriato**.

Un payload è il codice che viene eseguito all'interno del sistema target una volta che l'exploit ha avuto successo: può essere una shell, un meterpreter o un comando specifico.

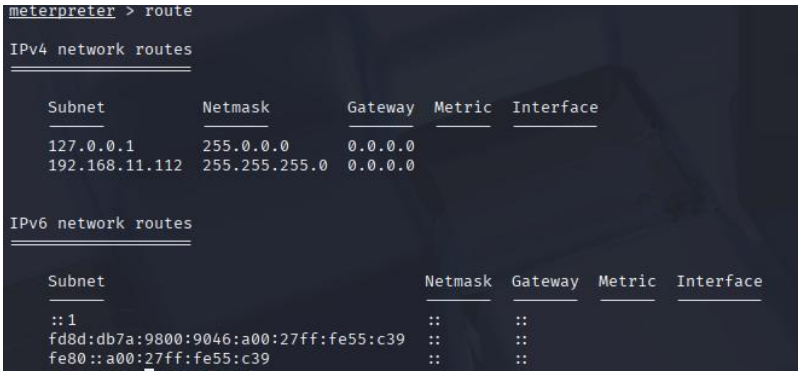
Lanciamo dunque il nostro attacco:

L'exploit è andato a buon fine abbiamo ricevuto una sessione Meterpreter, siamo quindi dentro la macchina.



Avviamo il comando '*ipconfig'* che confermerà l'identità della vittima.

Lanciamo anche il comando *'route'* come richiesto dall'esercizio per avere la tabella di routing della vittima.



Comandi come *'ipconfig'* e *'route'* vengono usati per raccogliere informazioni sulla rete della macchina compromessa.

A cosa serve usare questi comandi?

- Sapere **se la macchina ha accesso ad altre reti** (es. una rete interna isolata)
- Determinare **come raggiunge internet o altri host**
- Valutare se puoi eseguire un **pivoting** - ovvero usare la macchina già compromessa come punto di appoggio per raggiungere e attaccare altri sistemi nella rete interna della vittima.

Conclusione

L'esercitazione è stata completata con successo: abbiamo configurato correttamente entrambe le macchine virtuali, identificato e utilizzato l'exploit Java RMI tramite Metasploit, e ottenuto una sessione Meterpreter stabile.

Attraverso i comandi ipconfig e route, abbiamo raccolto informazioni fondamentali sulla struttura della rete interna della vittima, simulando così una fase iniziale di ricognizione che sarebbe tipica in uno scenario reale di penetration testing.

Questa attività ha permesso di consolidare le competenze nell'identificazione delle vulnerabilità, nella gestione delle reti virtuali e nell'uso degli strumenti professionali per l'exploitation.

Anche senza cuore rosso… la missione è riuscita!

Anais Fabriani
16/05/2025