S7L5: VULNERABILITA' JAVA RMI SU METASPLOITABLE 2

MATTIA GERARDI

SPIEGAZIONE BREVE DELL'ESERCIZIO

La macchina Metasploitable 2 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:

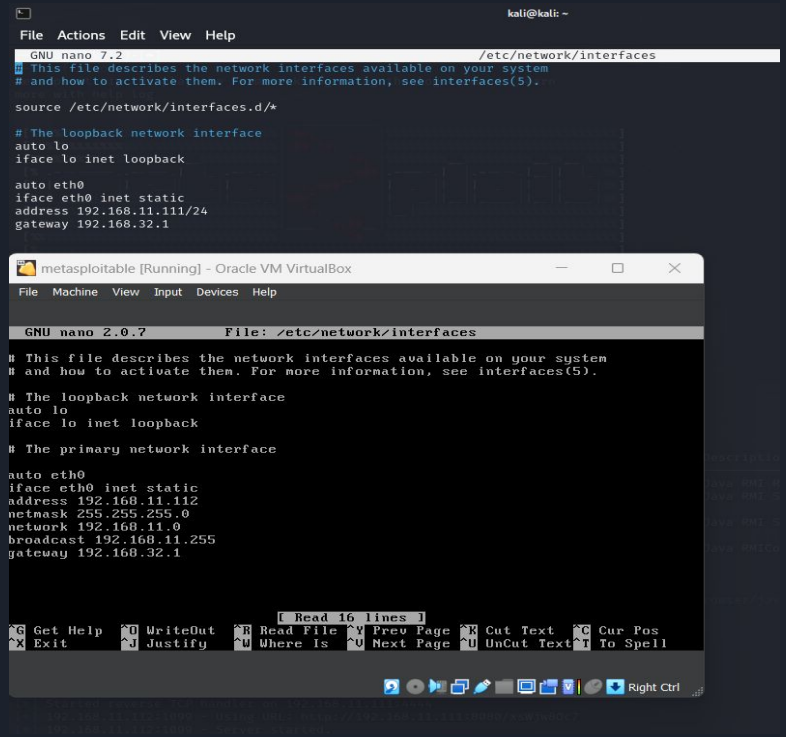
-La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111

-La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112

-Scansione della macchina con nmap per evidenziare la vulnerabilità.

-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.

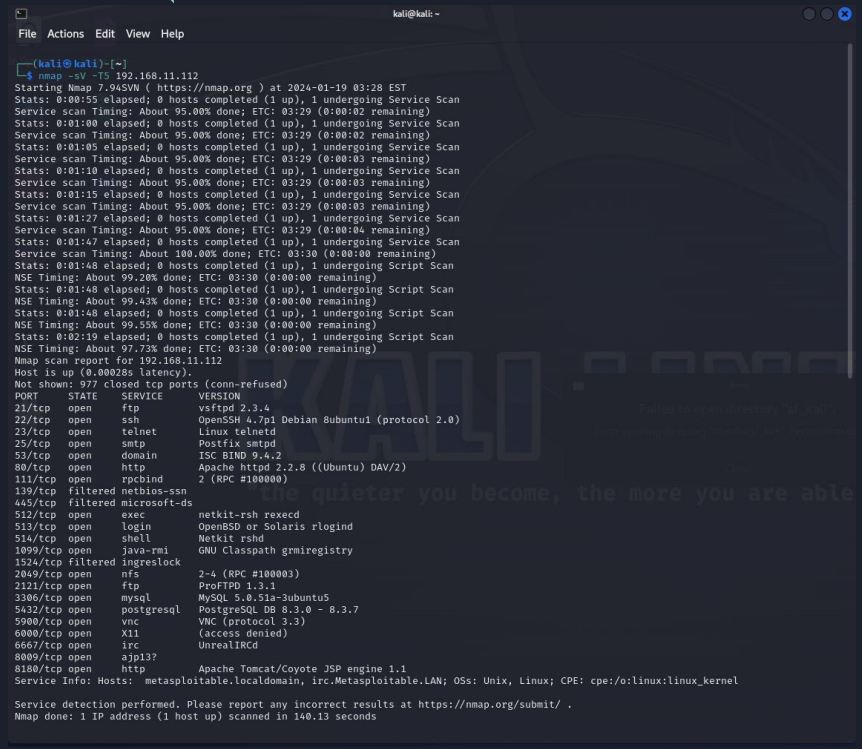
1) PRIMO STEP: CAMBIARE IP ALLE 2 MACCHINE, KALI E METASPLOITABLE



Per iniziare l'esercizio di oggi, andremo a modificare il file interfaces.d all'interno di entrambe le macchine al fine di cambiare l IP ad entrambe.

Come da screenshot, dopo aver dato a Kali l'IP 192.168.11.111 e a Meta 192.168.11.112 salveremo il file e riavvieremo per sicurezza le macchine per far entrare in funzione i cambiamenti.

2) SECONDO STEP: SCANSIONE CON NMAP PER EVIDENZIARE LA VULNERABILITÀ'



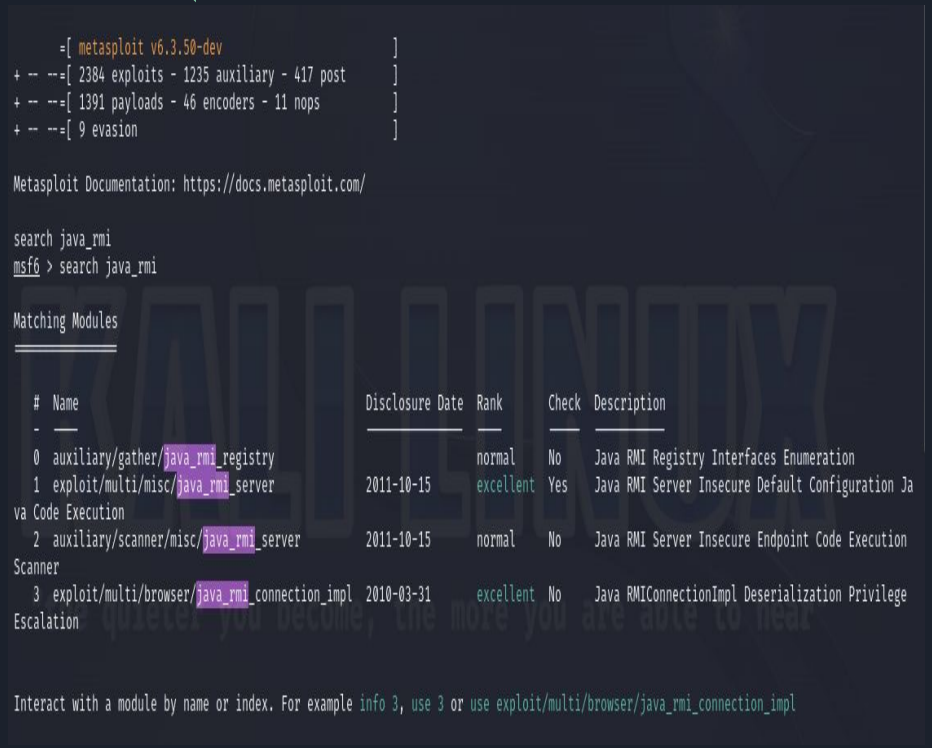
Come passo successivo, eseguiremo una semplice ma efficace scansione utilizzando il potente tool nmap verso l'IP di Meta per individuare le porte e i servizi/protocolli ad esse associate.

Come da traccia, possiamo confermare che la porta 1099/TPC e' aperta e corrisponde a Java-RMI.

3) TERZO STEP: AVVIAMO MSFCONSOLE

Ora che abbiamo confermato che Metasploitable ha sulla porta 1099/TCP il servizio/protocollo Java-RMI attivo, utilizzeremo per i rimanenti step dell'esercizio il framework Metasploit su Kali, avviabile con il comando "msfconsole"

4) QUARTO STEP: RICERCA VULNERABILITA' ALL'INTERNO DI MSFCONSOLE

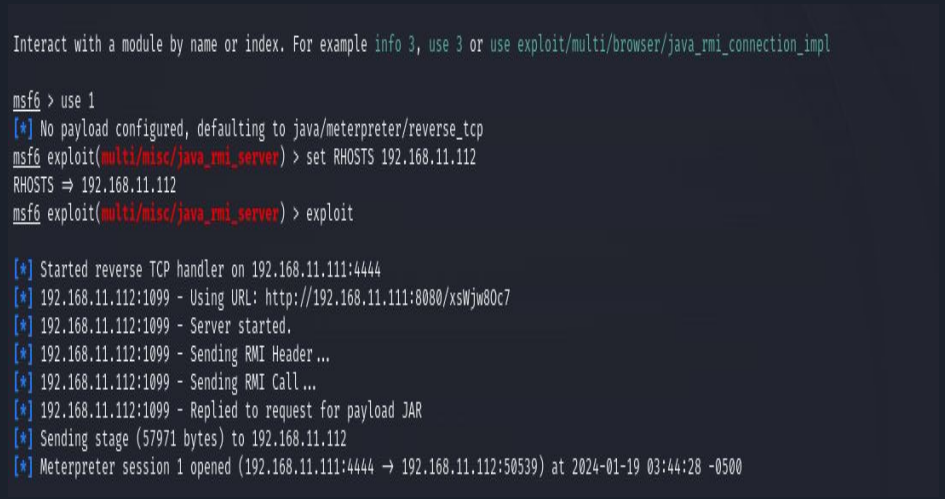


Avendo ora avviato il framework via terminale di Metasploit usando il comando "msfconsole", possiamo ora procedere a cercare con il comando "search java_rmi" i vari exploit che possiamo utilizzare.

In questo caso utilizzeremo il numero 1 con path exploit/multi/misc/java_rmi_server

Inseriremo dunque su terminale il comando "use 1"

5) QUINTO STEP: ESECUZIONE DELL'EXPLOIT



Dopo aver digitato il comando "use 1" per selezionare l'exploit che vogliamo utilizzare, andremo a settare la variabile RHOSTS assegnandogli l'IP di Metasploitable 2, cosicché il framework saprà' quale IP dovrà utilizzare per eseguire l'attacco.

Per eseguire l'exploit, dopo aver settato RHOSTS, utilizzeremo il comando "exploit" per avviare l'attacco.

6) ULTIMO STEP: SESSIONE REMOTA DI METERPRETER

Avendo eseguito l'exploit con successo e avendo avviato una sessione di meterpreter sulla macchina target da remoto, ora possiamo concludere l'esercizio utilizzando due comandi per ottenere la configurazione di rete e la tabella di routing della macchina vittima: "ifconfig/ipconfig" e "route".

Abbiamo quindi ora completato l'esercizio!