Progetto S7/L5 - Exploit Java RMI

Introduzione: l'obiettivo dell'esercizio è stato quello di individuare e sfruttare una vulnerabilità presente sul servizio Java RMI Registry (porta TCP 1099) esposto dalla macchina Metasploitable2. Tramite l'utilizzo del framework Metasploit, l'attaccante (macchina Kali Linux) deve ottenere una sessione remota Meterpreter sulla macchina vittima, al fine di raccogliere informazioni di rete (configurazione delle interfacce e tabella di routing).

Configurazione del laboratorio:

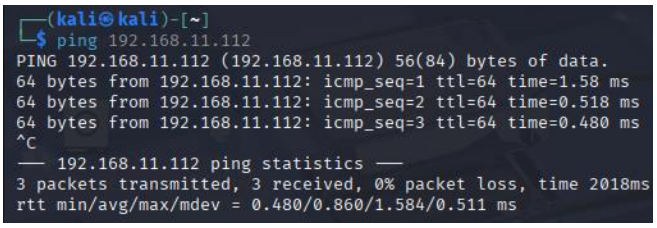
- Macchina attaccante (Kali Linux): 192.168.11.111
- Macchina vittima (Metasploitable2): 192.168.11.112

Entrambe le macchine sono state configurate sulla stessa rete virtuale, in modo da permettere la comunicazione diretta.

Attività svolte:

1. **Verifica della connettività**

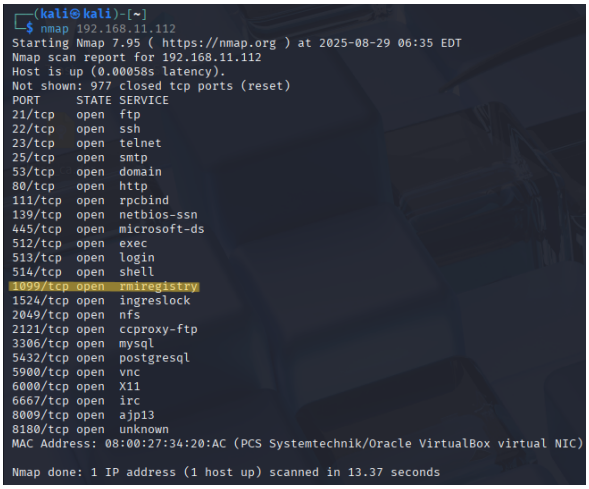
Il primo passo è stato verificare che la macchina attaccante potesse comunicare con la vittima tramite il comando ping.



La macchina ha risposto regolarmente, confermando la raggiungibilità.

2. **Scansione delle porte con Nmap**

Per identificare i servizi esposti sulla macchina vittima è stato utilizzato nmap.



La porta 1099/tcp risulta aperta, con il servizio rmiregistry.

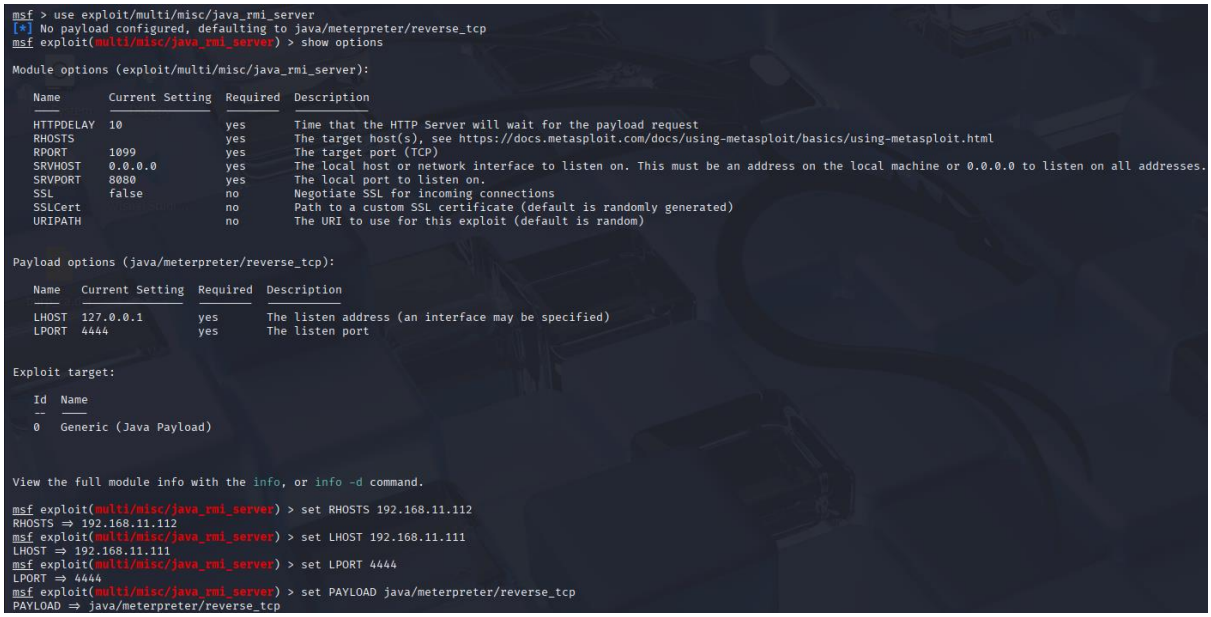
3. Avvio di Metasploit e ricerca exploit

È stato avviato il framework Metasploit tramite *msfconsole* e, successivamente, è stata eseguita la ricerca degli exploit relativi a Java RMI.

È stato individuato l'exploit *exploit/multi/misc/java_rmi_server*

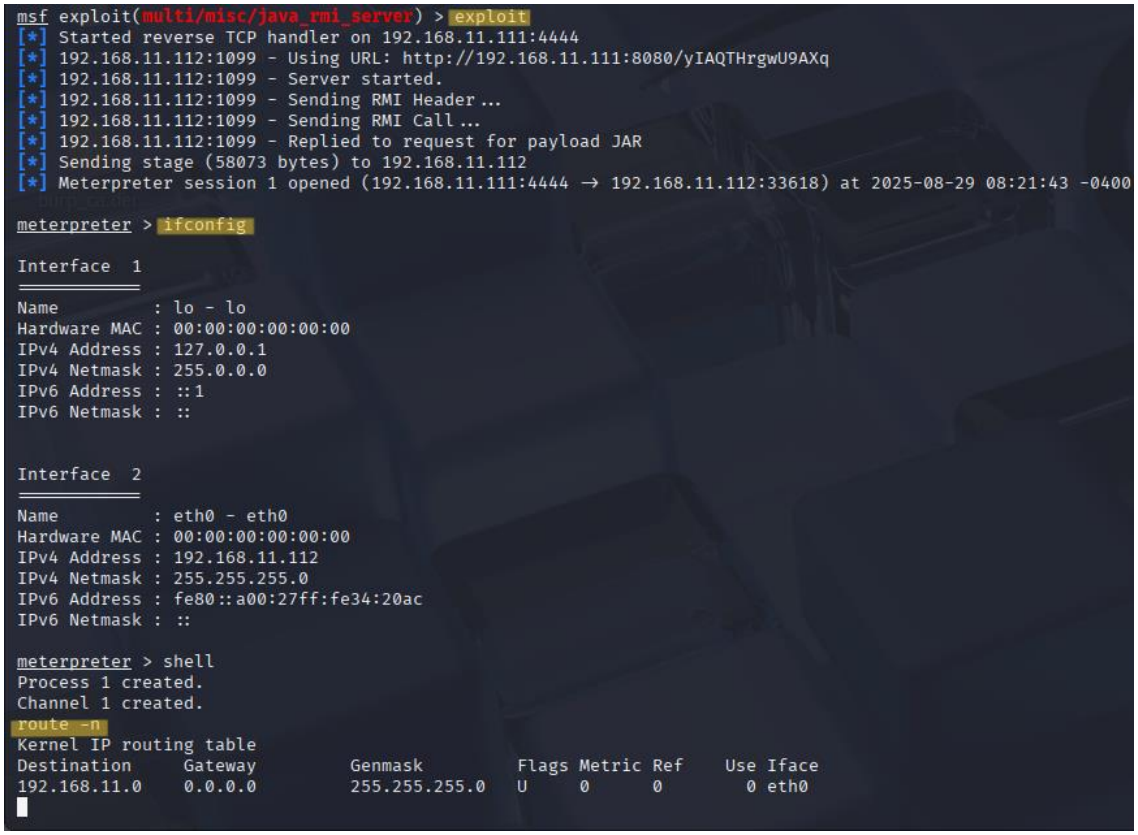
4. Configurazione dell'exploit

Dopo aver caricato l'exploit con *use exploit/multi/misc/java_rmi_server*, sono stati configurati i parametri.



5. Esecuzione dell'exploit e raccolta delle informazioni

L'exploit è stato lanciato con il comando *exploit* avviando una sessione Meterpreter sulla macchina vittima. Dalla sessione sono stati lanciati i comandi *ifconfig* e *route*.



Conclusioni

L’attività ha dimostrato come un servizio vulnerabile esposto in rete (Java RMI Registry su porta 1099) possa essere sfruttato per ottenere accesso remoto non autorizzato tramite Metasploit. In un ambiente reale, lasciare esposto un servizio non aggiornato come Java RMI rappresenta un rischio critico di compromissione. È quindi fondamentale limitare i servizi in ascolto, applicare aggiornamenti di sicurezza e monitorare le porte aperte.