Penetration Test Java RMI (Porta 1099)

Analista: Victor Rosati

Data: 23 Gennaio 2026

Target: Metasploitable 2 - Servizio Java RMI

---

1. Obiettivo dell'Attività

Lo scopo dell'esercitazione è sfruttare una vulnerabilità nota nel servizio **Java RMI** sulla porta **1099** per ottenere una sessione **Meterpreter** remota. L'attività richiede la configurazione di una rete specifica e la raccolta di evidenze post-exploitation (configurazione di rete e tabella di routing).

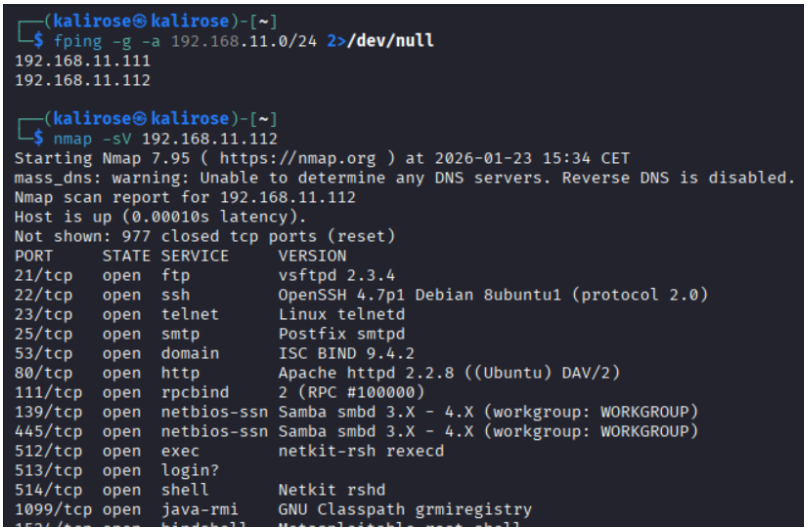
---

2. Configurazione della Rete (Setup Manuale)

Come richiesto dalla traccia, le macchine sono state configurate con i seguenti indirizzi IP statici:

- **Macchina Attaccante (Kali):** `192.168.11.111`
- **Macchina Vittima (Metasploitable):** `192.168.11.112`

Evidenza di connettività: Il comando `fping` ha confermato che entrambi gli host sono attivi e comunicanti nella sottorete `192.168.11.0/24`.



---

3. Analisi dei Servizi (Scanning)

La scansione `nmap -sV` sul target ha rilevato il servizio vulnerabile:

- **Porta:** 1099/tcp
- **Servizio:** java-rmi
- **Versione:** GNU Classpath grmiregistry

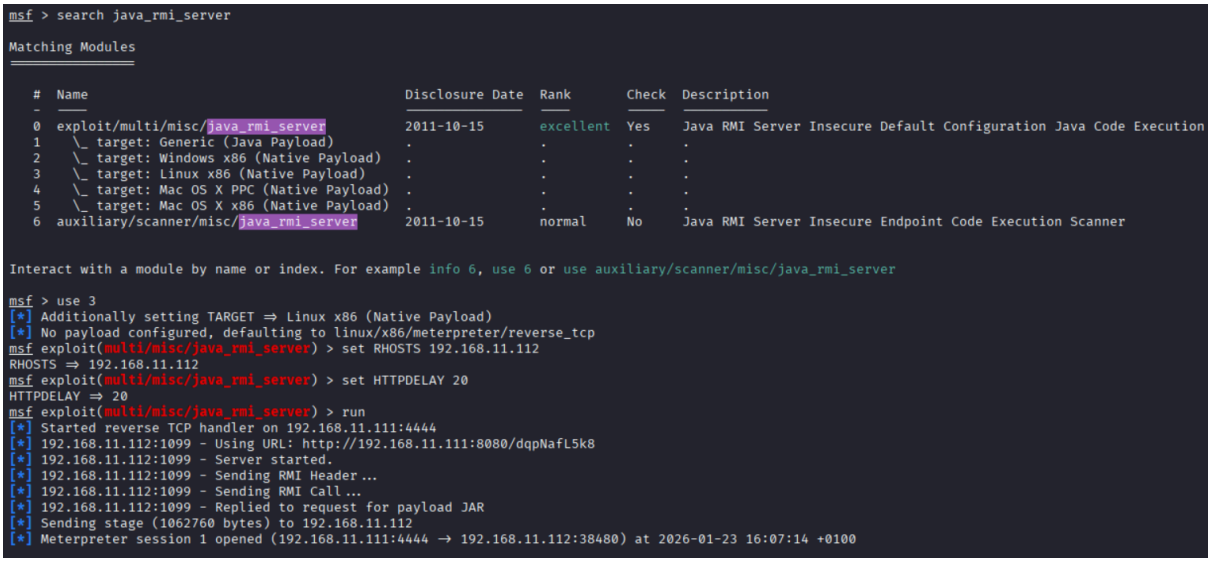
---

4. Fase di Exploitation

Per l'intrusione è stato utilizzato il framework Metasploit, seguendo la procedura documentata nei log di sessione:

1. **Selezione Modulo:** È stato selezionato il modulo exploit tramite l'indice della ricerca effettuata (`use 3`) corrispondente a `exploit/multi/misc/java_rmi_server`.
2. **Configurazione Target:** L'indirizzo della vittima è stato impostato tramite `set RHOSTS 192.168.11.112`.
3. **Ottimizzazione del Payload:** Per prevenire il fallimento dell'attacco dovuto a latenza nel caricamento del payload JAR (timeout), è stato configurato il parametro `set HTTPDELAY 20`.
4. **Esecuzione:** L'attacco è stato lanciato tramite il comando `run`.

Esito: Apertura della sessione **Meterpreter 1** alle 16:07:14.

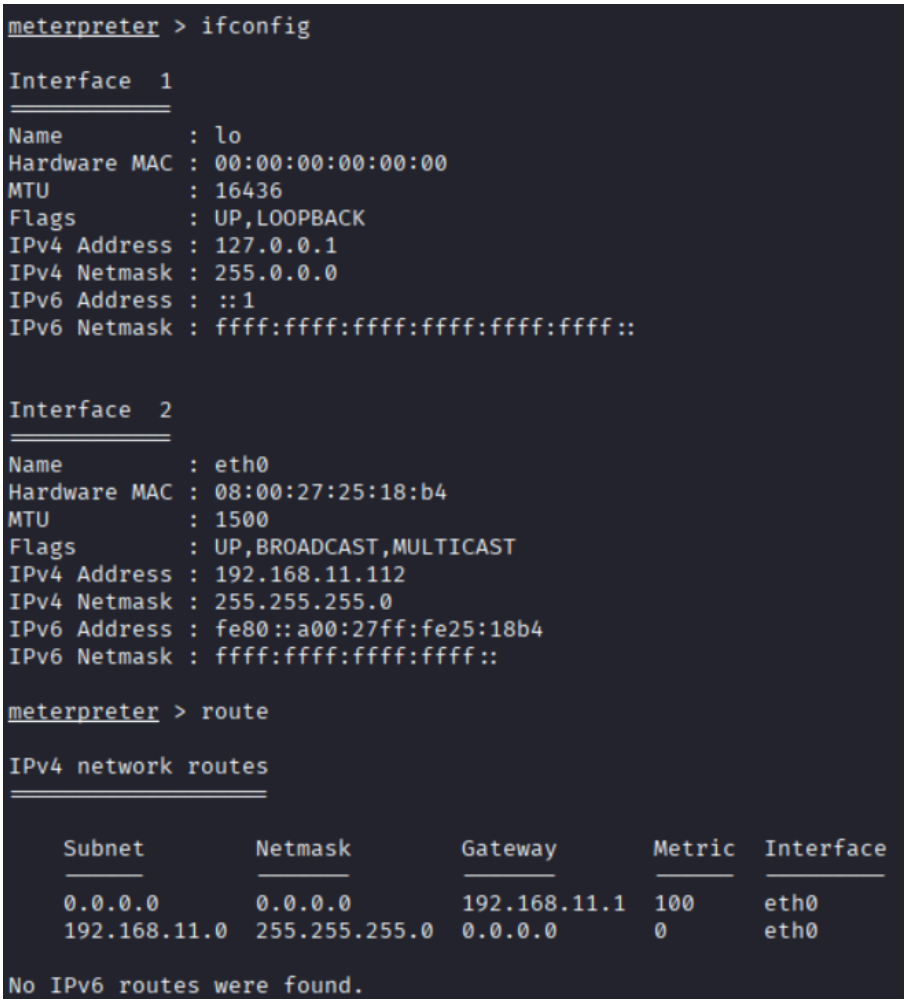


---

5. Raccolta Evidenze (Requisiti Traccia)

Una volta stabilita la sessione remota, sono stati eseguiti i comandi richiesti per il report finale:

- **Evidenza 1: Configurazione di Rete (`ifconfig`)** Conferma dell'indirizzo IP `192.168.11.112` sull'interfaccia `eth0` del target.
- **Evidenza 2: Tabella di Routing (`route`)** Mostra le rotte attive sulla macchina remota, inclusa la rotta locale per la subnet `192.168.11.0`.



---

6. Conclusioni

L'attacco è andato a buon fine rispettando tutti i parametri di rete e tecnici richiesti. La calibrazione del parametro `HTTPDELAY` è stata determinante per superare le criticità di timeout e garantire la stabilità della sessione. Il sistema è ora pronto per le esercitazioni avanzate previste per la prossima settimana.