Relazione sull'esercizio di sfruttamento della vulnerabilità Java RMI con Metasploit

Presentation

15/11/2024

Silvia Arnetta

Cybersecurity

01

Introduzione

L'obiettivo di questo esercizio è sfruttare una vulnerabilità nel servizio Java RMI in esecuzione sulla porta 1099 della macchina Metasploitable per ottenere una sessione remota **Meterpreter** tramite **Metasploit**.
Successivamente, vengono richieste due evidenze dalla macchina vittima:

1. Configurazione di rete.
2. Informazioni sulla tabella di routing.

Setup dell’ambiente

Macchina attaccante (kali Linux)

- IP: 192.168.11.111

Macchina vittima (Metasploitable)

- IP: 192.168.11.112

Servizio vulnerabile

- Java RMI (Remote Method Invocation) in esecuzione sulla porta 1099

Java RMI (Remote Method Invocation) è una tecnologia che consente a programmi Java di comunicare ed eseguire metodi su oggetti remoti, anche su computer diversi. Viene utilizzata per creare applicazioni distribuite in modo semplice. Tuttavia, può essere vulnerabile quando è configurata senza protezioni adeguate. La mancanza di autenticazione, il caricamento di classi da fonti non sicure e l’assenza di controlli sugli oggetti inviati possono permettere ad un attaccante di sfruttare il servizio. Usando oggetti malevoli, è possibile eseguire codice dannoso sul server. Questo rende importante proteggerlo con configurazioni sicure e aggiornamenti costanti.

Procedura eseguita

1. Avvio di metasploit

Ho avviato **Metasploit** sulla macchina attaccante
con il comando: msfconsole

Metasploit è una piattaforma open-source utilizzata per test di penetrazione e sicurezza informatica. Fornisce strumenti per identificare, sfruttare e dimostrare vulnerabilità nei sistemi, includendo una vasta libreria di exploit e payload. È ampiamente usato per simulare attacchi, aiutare nella verifica delle difese e formare professionisti della sicurezza. Grazie alla sua flessibilità, supporta la creazione e l'implementazione di exploit personalizzati.

2. Configurazione del modulo

Ho configurato il modulo con i parametri richiesti:

- **RHOST**: 192.168.11.112 (IP della macchina vittima).

Procedura eseguita

3. Ricerca del modulo di exploit

Ho utilizzato il comando seguente per trovare un modulo exploit adatto al servizio Java RMI: search rmi

Tra i risultati, ho selezionato il modulo exploit/multi/misc/java_rmi_server.

L'exploit `java_rmi_server` di Metasploit sfrutta vulnerabilità nel servizio Java RMI (Remote Method Invocation), che è spesso configurato in modo insicuro, esponendo il servizio su porte come la 1099. L'attaccante invia oggetti malevoli a un server RMI vulnerabile per eseguire codice remoto sulla macchina vittima. Questo exploit può portare a una sessione Meterpreter, consentendo all'attaccante di eseguire comandi, raccogliere dati e compromettere ulteriormente il sistema. Le principali misure di protezione includono la limitazione dell'accesso, l'autenticazione RMI e l'aggiornamento delle librerie Java.

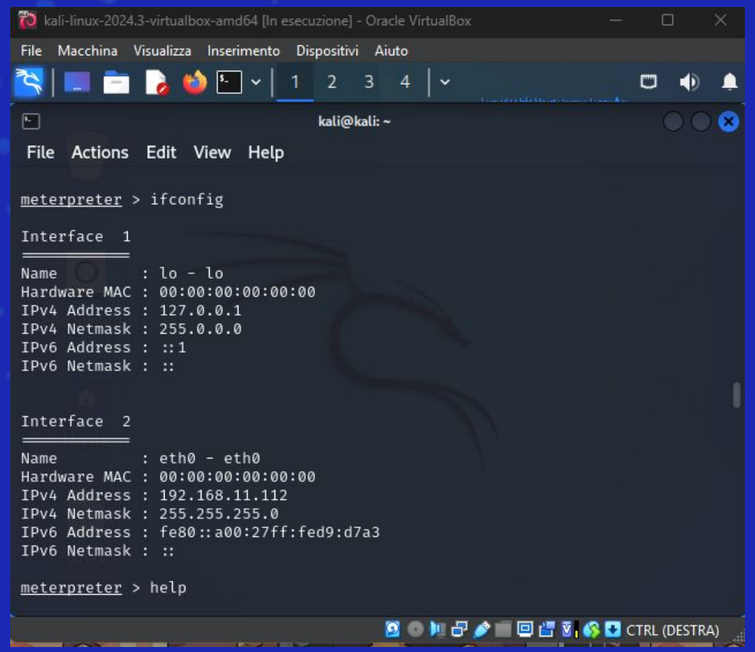
4. Esecuzione dell’exploit

Ho avviato l'exploit con il comando: exploit

Al termine, ho ottenuto una sessione **Meterpreter** connessa alla macchina vittima.

Meterpreter è un payload avanzato di Metasploit che consente il controllo remoto di un sistema compromesso tramite una connessione sicura. Permette agli attaccanti di eseguire comandi, accedere ai file, fare screenshot, intercettare il traffico di rete e persino ottenere privilegi elevati sulla macchina vittima. Essendo un payload iniettato direttamente in memoria, è meno rilevabile dagli antivirus. È uno strumento potente per la gestione di sistemi compromessi e l'esecuzione di attacchi laterali in una rete.

Raccolta delle evidenze



Configurazione di rete

Per visualizzare la configurazione di rete della macchina vittima, ho utilizzato il comando `ifconfig` in Meterpreter. Questo ha mostrato i dettagli della rete di **Metasploitable**, la macchina compromessa, inclusi il suo indirizzo IP, la subnet mask e altre informazioni delle interfacce di rete. Questo IP appartiene alla macchina bersaglio, non a Kali Linux, che è la macchina attaccante.

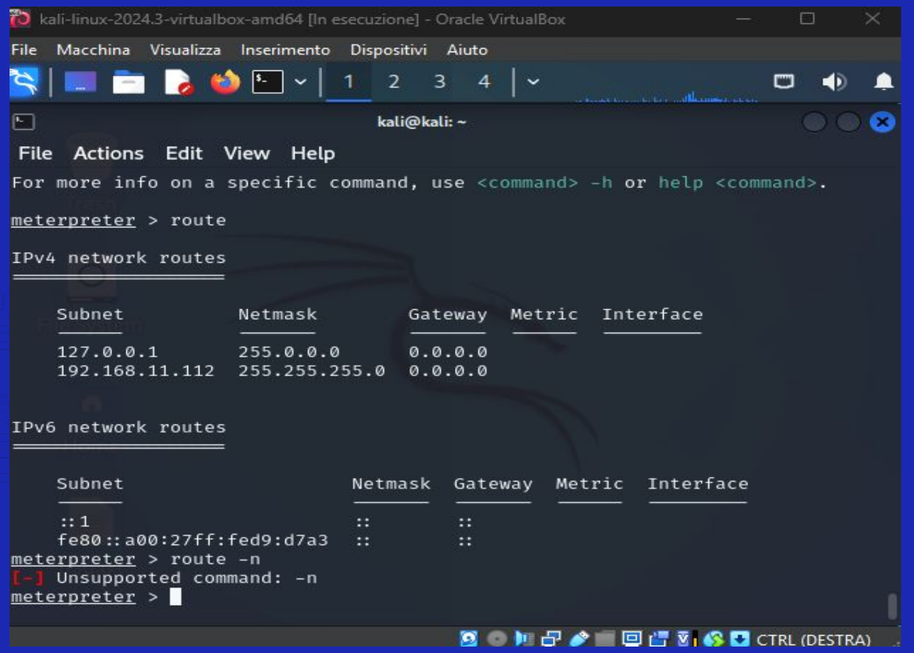


Tabella di routing

Il comando `route` in Meterpreter viene utilizzato per raccogliere informazioni sulla tabella di routing della macchina compromessa. Mostra come il traffico di rete viene instradato, elencando le reti raggiungibili, i gateway configurati e le interfacce utilizzate. Questo permette di capire quali percorsi il sistema usa per comunicare con altre reti o dispositivi. È particolarmente utile per identificare segmenti di rete non direttamente visibili dall'attaccante e pianificare movimenti laterali. Analizzando la tabella, è possibile scoprire nuove potenziali destinazioni per espandere l'attacco nella rete.

Perchè configurare HTTDALAY A 20

Impostare `HttpDelay` a 20 in Metasploit significa fare in modo che il payload, come Meterpreter, si colleghi al server ogni 20 secondi. Questo aiuta a nascondere l'attività, rendendo il traffico meno evidente ai sistemi di sicurezza. Un ritardo maggiore fa sembrare il comportamento più normale, ma rallenta anche il controllo del sistema compromesso. È una scelta per bilanciare discrezione e velocità di comunicazione.

Se il parametro `HttpDelay` fosse stato configurato con un valore troppo basso o inappropriato, potrebbe causare problemi di comunicazione tra il payload (ad esempio Meterpreter) e il server di comando e controllo. Un ritardo troppo breve genera un volume elevato di richieste, che potrebbe sovraccaricare il sistema bersaglio o il server, causando errori o rendendo l'attività più visibile ai sistemi di sicurezza. Inoltre, se il ritardo è incoerente con le caratteristiche della rete (ad esempio, in presenza di latenza elevata), il server potrebbe non ricevere le connessioni in tempo, interrompendo la sessione.

Conclusione

L'esercizio è stato completato con successo:

- È stata sfruttata la vulnerabilità Java RMI per ottenere una sessione **Meterpreter** sulla macchina vittima.
- Sono state raccolte le evidenze richieste riguardanti la configurazione di rete e la tabella di routing.

L'esercizio ha dimostrato l'importanza della protezione dei servizi RMI e della corretta configurazione di firewall e permessi per prevenire attacchi remoti.

L'exploit exploit/multi/misc/java_rmi_server di Metasploit sfrutta una vulnerabilità del servizio **Java RMI (Remote Method Invocation)**. In particolare, mira a servizi RMI configurati in modo insicuro, permettendo agli attaccanti di eseguire codice arbitrario sulla macchina vittima.