Progetto Metasploit

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.

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.

Esecuzione:

Differenza tra "exploit" e "malware":

La differenza tra "exploit" e "malware" riguarda principalmente il loro scopo e il modo in cui operano all'interno dei sistemi informatici. Un exploit è un pezzo di software, un comando o un insieme di dati che sfrutta una vulnerabilità o un bug in un altro software per causare un comportamento non previsto. Questo comportamento non previsto può includere l'acquisizione del controllo di un sistema, l'alterazione di funzioni del software o l'accesso a dati riservati. Mentre il malware si riferisce a qualsiasi software progettato per danneggiare, disturbare, o eseguire azioni non autorizzate su un sistema informatico. Il malware include virus, worm, trojan, ransomware, spyware e altri tipi di software dannoso. Gli exploit possono essere utilizzati per distribuire malware. Ad esempio, un exploit potrebbe sfruttare una vulnerabilità per ottenere l'accesso a un sistema, dopodiché installare un malware per compiere azioni dannose.

Le fasi principali di Exploit sono:

- Identificazione della Vulnerabilità: Prima di tutto, bisogna identificare una vulnerabilità nel software, che può essere un errore di programmazione, una configurazione non sicura o altre debolezze.
- Creazione dell'Exploit: Dopodiché, si sviluppa un exploit, cioè un codice o un metodo che sfrutta quella vulnerabilità per eseguire codice arbitrario o accedere a parti del sistema normalmente inaccessibili.
- Esecuzione dell'Exploit: Infine, si cerca di eseguire l'exploit contro il sistema target, che potrebbe portare al controllo totale o parziale di quel sistema.

Per proteggerti dagli exploit, è importante:

- Aggiornare Regolarmente i Software: I produttori rilasciano spesso aggiornamenti che correggono le vulnerabilità note. Mantenere aggiornato il sistema operativo e tutti i software è fondamentale.
- Praticare la Sicurezza Basata sul Principio del Minimo Privilegio: Ciò significa limitare i diritti di accesso degli utenti solo a ciò che è strettamente necessario per le loro attività.

- Backup Regolari: Avere backup regolari può aiutare a ripristinare i dati in caso di un attacco riuscito.

Metasploit:

Metasploit, è un popolare framework open-source utilizzato per lo sviluppo e l'esecuzione di exploit contro un sistema remoto. Serve principalmente per testare la sicurezza dei sistemi informatici.

Le sue principali funzionalità sono:

- Ricerca di Vulnerabilità
- Sviluppo e test di exploit
- Simulazione di attacchi
- Automazione di task di sicurezza

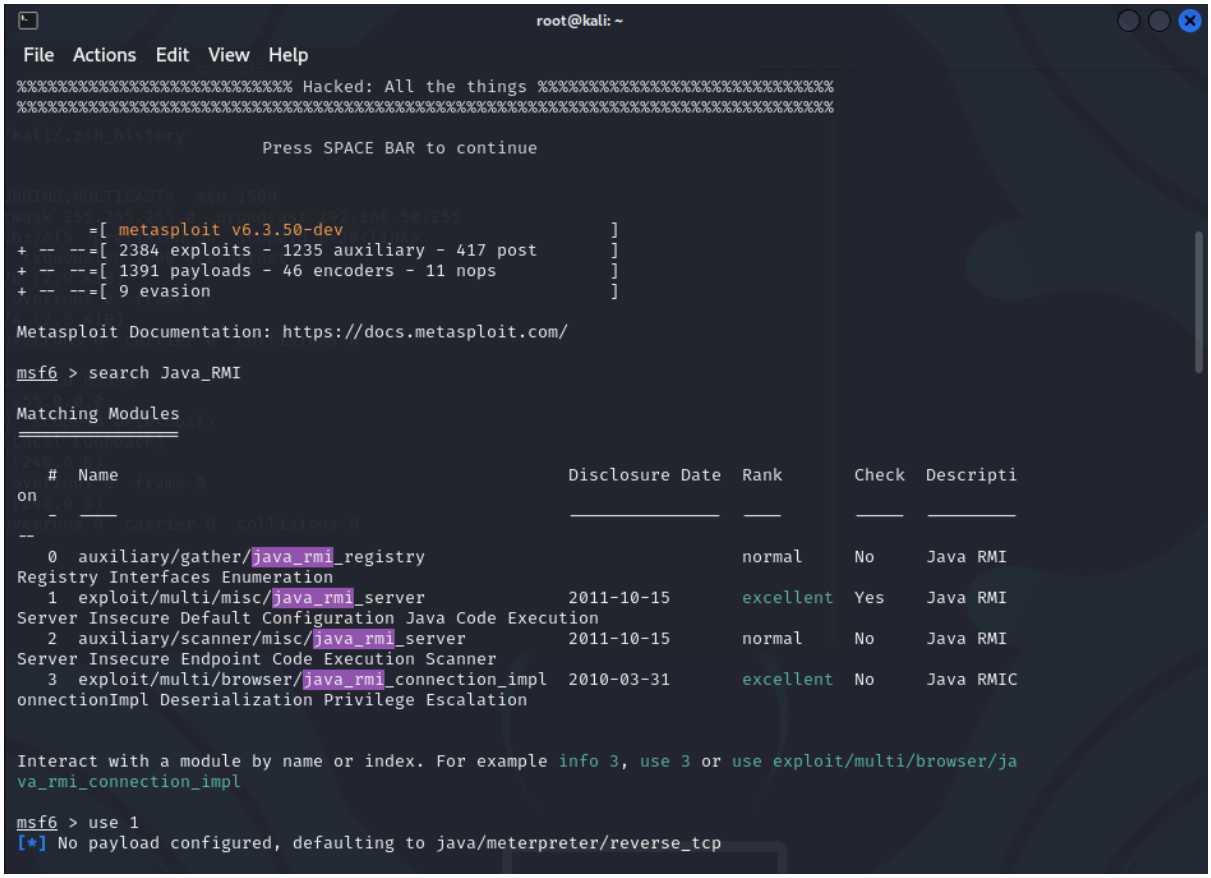
È importante notare che, mentre Metasploit è uno strumento potente per i professionisti della sicurezza, può anche essere utilizzato per scopi malevoli.

La vulnerabilità Java RMI su Metasploitable:

La vulnerabilità sulla porta 1099 è tipicamente associata a Java Remote Method Invocation (RMI). Java RMI è una tecnologia di Java che permette l'invocazione di metodi da remoto, facilitando la comunicazione tra applicazioni Java distribuite su diverse macchine. Tuttavia, questa tecnologia può essere soggetta a specifiche vulnerabilità di sicurezza, soprattutto se non configurata o gestita correttamente.

Se un server RMI non è adeguatamente protetto, gli attaccanti possono ottenere l'accesso (come nel nostro caso) non autorizzato alle funzionalità esposte tramite RMI, potenzialmente compromettendo il sistema.

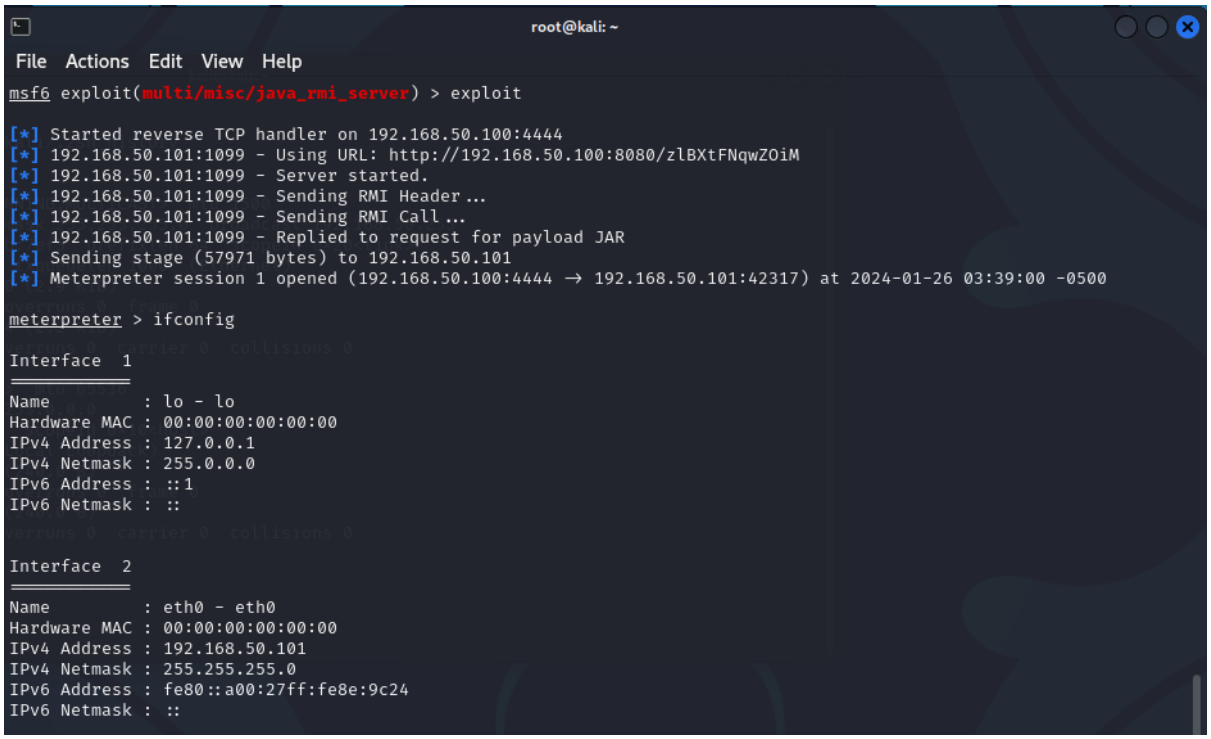
Nella Pratica:



Dopo aver fatto partire Metasploit andiamo a cercare se nella repository sia presente l'exploit Java_RMI da poter utilizzare sulla nostra macchina target che in questo caso è la macchina virtuale Metasploitable.

Dopo aver selezionato il nostro exploit andiamo a vedere le specifiche che richiede per il suo funzionamento e vediamo che ci richiede solo l'ip target della macchina bersaglio. Dopo aver inserito

l'ip target proviamo e vedere se l'exploit funziona con il Payload preselezionato dall'applicazione se in caso quel payload non avesse funzionato avremmo potuto scegliere la seconda alternativa.



Ora che siamo dentro la macchina target grazie a l'exploit andiamo a cercare le informazioni richieste dall'esercizio, ovvero la configurazione di rete e le informazioni sulla tabella di routing della macchina.

In conclusione, la vulnerabilità sulla porta 1099 legata a Java RMI rappresenta un serio rischio di sicurezza. Gli amministratori del sistema e dovrebbero essere consapevoli di questi rischi e adottare misure appropriate per mitigarli, al fine di proteggere le loro reti e sistemi da potenziali attacchi.