S7L5 PROGETTO SETTIMANALE WEB APPLICATION

Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.

Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

I requisiti dell’esercizio sono:

● La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111 (Opzionale)

● La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112 (Opzionale)

● Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:

1) configurazione di rete.

2) informazioni sulla tabella di routing della macchina vittima.

Per sfruttare la vulnerabilità di Java RMI sulla porta 1099 su Metasploitable e ottenere una sessione di Meterpreter sulla macchina da remoto ci sono certi passaggi da seguire. Ovviamente in ambito reale per questo ci serve di avere l'autorizzazione legale per eseguire questo tipo di attività.

DEFINIZIONE

**Metasploit**

Metasploit è un ampio framework open-source utilizzato per testare la sicurezza dei sistemi informatici attraverso attività di penetration testing ed ethical hacking.

Sviluppato da Rapid7, Metasploit fornisce uno strumento completo e modulare per identificare e sfruttare vulnerabilità nei sistemi informatici.

Ecco alcune caratteristiche chiave di Metasploit:

**Framework**: Metasploit è strutturato come un framework (*architettura modulare e organizzata che consente agli utenti di sfruttare varie funzionalità per condurre test di penetrazione e attività di ethical hacking*) che offre una base modulare per lo sviluppo, il test e l`esecuzione di exploit.

Ciò consente ai professionisti della sicurezza di personalizzare e estendere la sua funzionalità.

**Exploits**: Metasploit include una vasta collezione di exploits (*porzioni di software o codice progettate per sfruttare vulnerabilità o debolezze presenti in un sistema, un'applicazione o un dispositivo al fine di ottenere un accesso non autorizzato o eseguire determinate azioni malevole*) pre-costruiti per una vasta gamma di vulnerabilità.

Questi exploits possono essere utilizzati per testare e valutare la sicurezza di sistemi e reti.

**Payloads**: Un payload è una porzione di codice che viene eseguita su un sistema di destinazione dopo un'exploit di successo. Metasploit offre vari payloads, tra cui shellcode, Meterpreter (*un payload avanzato e multi-funzione*) e altri.

Moduli ausiliari (Auxiliary Modules): Questi sono moduli aggiuntivi che svolgono varie attività, come raccolta di informazioni, scansione e ricognizione. I moduli ausiliari non coinvolgono necessariamente l'exploit, ma sono cruciali per il processo generale di penetration testing.

**Meterpreter**

Meterpreter è un payload avanzato e versatile utilizzato nel contesto di Metasploit per eseguire una varietà di operazioni su un sistema compromesso. Questo payload è progettato per fornire una shell interattiva con una vasta gamma di funzionalità, consentendo agli operatori di penetration testing o agli hacker etici di eseguire operazioni avanzate sui sistemi che hanno compromesso.

Ecco alcune delle caratteristiche principali di Meterpreter:

**Shell Interattiva**: Meterpreter fornisce una shell interattiva che consente agli operatori di eseguire comandi direttamente sul sistema compromesso. Questo offre un controllo flessibile sul sistema e facilita l`esplorazione delle risorse.

**Funzionalità Remote**: Meterpreter è progettato per funzionare in un ambiente remoto. Gli operatori possono utilizzare le funzionalità di Meterpreter da una macchina remota per eseguire comandi sul sistema di destinazione.

**Accesso a Risorse di Sistema**: Meterpreter consente di accedere e manipolare una varietà di risorse di sistema, inclusi file, registri di sistema, processi in esecuzione e così via.

**Miglioramenti alla Sicurezza**: Meterpreter include funzionalità avanzate di evasione e nascondimento, rendendolo più difficile da rilevare da parte delle soluzioni antivirus e degli strumenti di sicurezza

**Funzionalità di Post-Compromesso**: Una volta che un sistema è stato compromesso e Meterpreter è stato eseguito con successo, è possibile utilizzare varie funzionalità di post-compromesso.

Ciò può includere il rilevamento e la raccolta di informazioni sensibili, il monitoraggio delle attività utente e altro ancora.

**Shell**

Quando si parla di hacking o penetration testing, il termine "shell" si riferisce a una shell di sistema ottenuta in modo non autorizzato su un sistema target. In questo contesto, ottenere una "shell" significa ottenere accesso e controllo sulla linea di comando o sull'ambiente operativo del sistema remoto.

Ecco un aspetto più dettagliato della shell come Interfaccia Utente:

**Interfaccia a Linea di Comando (CLI):** Una shell può essere un’interfaccia a linea di comando, che è un ambiente testuale in cui gli utenti interagiscono con un sistema utilizzando comandi di testo. Questa è spesso chiamata shell di sistema o shell di comando. Gli utenti possono inserire comandi e ricevere output direttamente tramite il testo.

**Interfaccia Grafica Utente (GUI):** In alternativa, una shell può essere un'interfaccia grafica attraverso la quale gli utenti interagiscono con il sistema utilizzando elementi visivi come finestre, icone e menu. Questa è spesso chiamata shell grafica o ambiente desktop.

**Shell come Processo o Ambiente di Esecuzione**:

**Shell di Sistema Operativo**: Può anche riferirsi a un ambiente di esecuzione in cui i comandi e i programmi vengono eseguiti. Ad esempio, in sistemi operativi basati su Unix (come Linux), la shell è un interprete di comandi che esegue istruzioni fornite dagli utenti o da script.

**Configurazione di rete**

La configurazione di rete si riferisce al processo di impostazione e gestione delle connessioni e delle impostazioni di rete su un dispositivo o su una rete di dispositivi. Questo processo coinvolge la definizione di vari parametri, tra cui gli indirizzi IP, le maschere di sottorete, i gateway, i server DNS e altri parametri che consentono ai dispositivi di comunicare tra loro attraverso una rete.

Ecco alcuni degli elementi chiave che possono essere configurati in una rete:

**Indirizzo IP**: Un identificatore univoco assegnato a ciascun dispositivo di rete. Può essere assegnato staticamente o dinamicamente (tramite DHCP).

**Maschera di Sottorete**: Specifica quali bit dell’indirizzo IP sono utilizzati per identificare la rete e quali sono utilizzati per identificare l'host all'interno della rete.

**Gateway Predefinito**: Un router o un dispositivo di rete utilizzato per instradare il traffico tra reti diverse.

**Server DNS**: Specifica i server che devono essere consultati per risolvere i nomi di dominio in indirizzi IP.

**DHCP** (*Dynamic Host Configuration Protocol*): Un protocollo che assegna automaticamente indirizzi IP e altre configurazioni di rete ai dispositivi quando si connettono a una rete.

**Configurazione del Firewall**: Impostazioni che regolano quali tipi di traffico sono consentiti o bloccati sulla rete.

La configurazione di rete può avvenire su diversi livelli, inclusi:

**Livello di Sistema Operativo**: Utilizzando strumenti e file di configurazione del sistema operativo.

**Livello di Router e Switch**: Configurando le impostazioni di routing e le regole di commutazione su dispositivi di rete.

**Livello di Apparecchiature di Rete**: Configurando le impostazioni su dispositivi come router, switch, firewall, access point, ecc.

La corretta configurazione di rete è fondamentale per garantire la comunicazione efficiente e sicura tra i dispositivi in una rete. La configurazione varia a seconda delle esigenze specifiche della rete, delle politiche di sicurezza e di altri fattori.

**Tabella di routing:**

Una tabella di routing è una componente critica nelle configurazioni di rete. Essa è utilizzata dai router e da altri dispositivi di rete per determinare il percorso migliore attraverso cui instradare i pacchetti di dati da una sorgente a una destinazione.

La tabella di routing contiene informazioni sulle reti e i percorsi disponibili.

Sfruttamento della Vulnerabilità

**Aprire Metasploit**

Apriamo Metasploit Framework sul terminale Root di Kali Linux essendo già installato con il seguente comando: *msfconsole*

**Trovare e Selezionare l'Exploit**

Cerchiamo un modulo di exploit per la vulnerabilità Java RMI. Possiamo farlo utilizzando il comando: *search java rmi* dopo aver elencato la lista dei payloads con commando *show payloads.*

Scegliamo un modulo di exploit appropriato: *use exploit/multi/misc/java\_rmi\_server*

**Configura l'Exploit**

Configuriamo i parametri dell'exploit con l'indirizzo IP della macchina vittima con commando: *set RHOSTS 192.168.11.112*

**Eseguire l'Exploit**

Eseguire l'exploit per tentare di ottenere l'accesso sulla macchina vittima: *exploit*

Attendere che Metasploit completi l'esecuzione dell'exploit.

**Ottenere una Sessione Meterpreter**

Una volta che l'exploit ha successo, dovresti ottenere una sessione Meterpreter. Assicuriamoci di aver stabilito la connessione.

Il commando *sessions -i 1* si collega alla sessione Meterpreter appena creata.

**Raccogliere Evidenze**

Dopo aver ottenuto una sessione Meterpreter sulla macchina remota, si puo raccogliere le evidenze richieste:

**Configurazione di Rete**

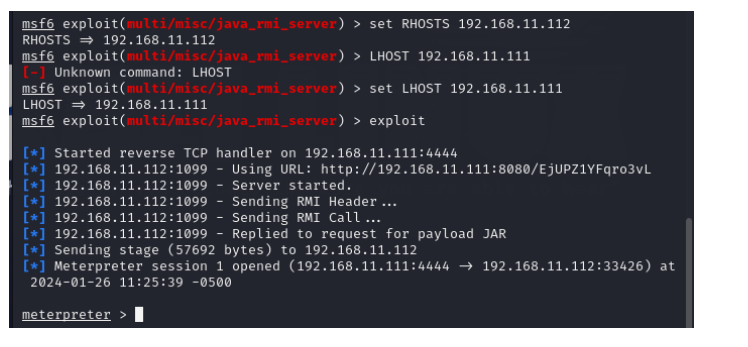
Usiamo il commando *run ipconfig*

**Informazioni sulla Tabella di Routing**

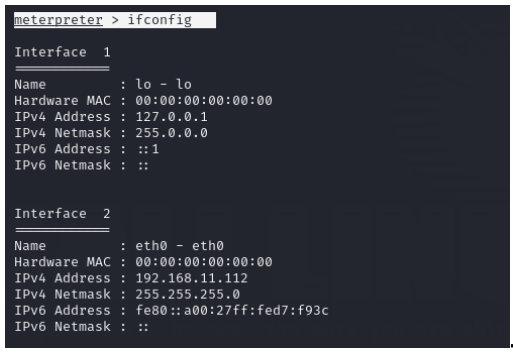
Il commando *run route,* verra eseguito sulla macchina remota attraverso la sessione Meterpreter.

**Repport**

Possiamo vedere che la macchina Host a risposta alla richiesta del payload e una sessione di *Meterpreter* è stata *aperta*. Tra le due macchine.



Con commando *ifconfig* si può esattamente confermare che una connessione è stata elaborata tra le due macchine.



Con commando *syninfo* si conferma le informazioni di sincronizzazione con la macchina metasploitable.

