EJERCICIOS METASPLOIT BÁSICO Prerrequisitos

Kali Linux

Metasploitable2

Ejercicio 1 - OSINT y Metasploit

Vulnerabilidad: CVE-2004-2687 (Distcc)

Ficha de la vulnerabilidad:

Descripción

permite a un atacante ejecutar comandos arbitrarios en el sistema afectado

A que software afecta

distcc

Utilidad del software

distribuye la carga de trabajo de compilación entre varios equipos en una red

Versiones del software afectadas

anteriores a la 2.18.3

Puertos que lo utilizan

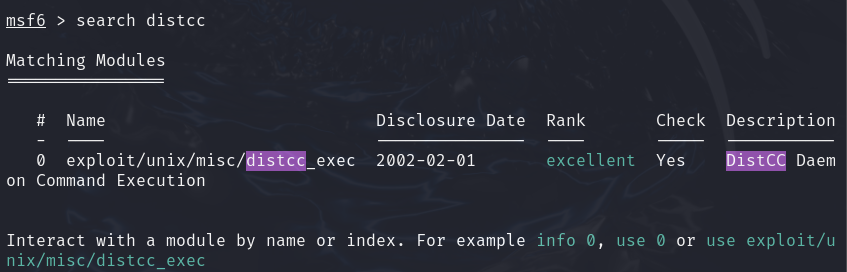
3632

Módulos de metasploit relacionados

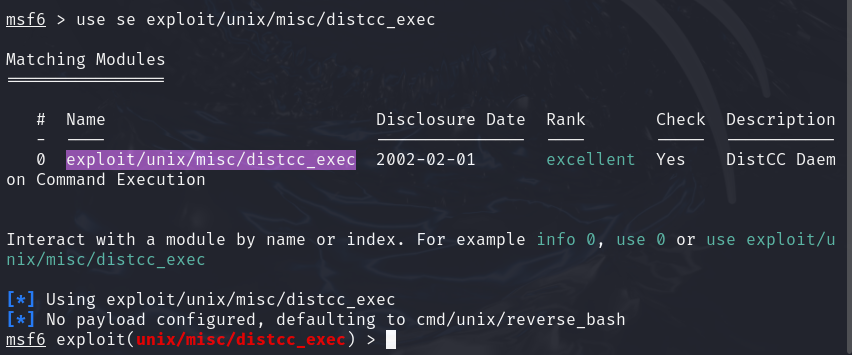
unix/misc/distcc\_exec

Explotar la vulnerabilidad:

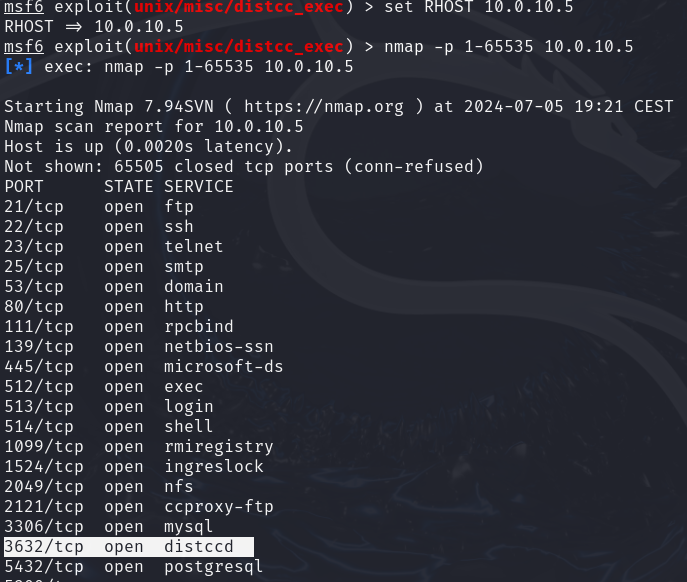
Buscar módulos de exploit en Metasploit

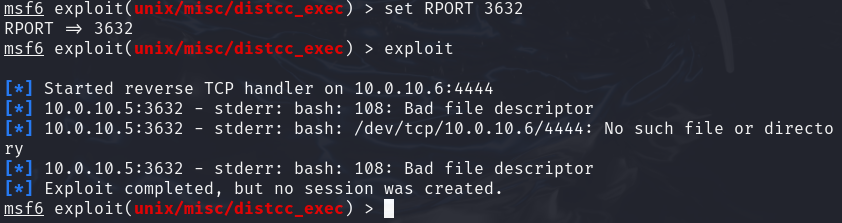


Elegir payload



Configurar y explotar





Ejercicio 2 - OSINT y Metasploit

Vulnerabilidad: CVE-2007-2447 (Samba)

Ficha de la vulnerabilidad:

Descripción

permite a un atacante hacer ejecución remota de código

A que software afecta

samba

Utilidad del software

permite a sistemas linux compartir archivos e impresoras con sistemas windows

Versiones del software afectadas

anteriores a las que incluyeron el parche

Puertos que lo utilizan

445

Módulos de metasploit relacionados

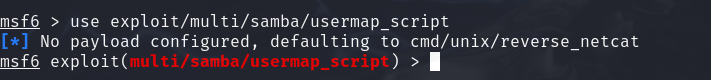
metasploit framework

Explotar la vulnerabilidad:

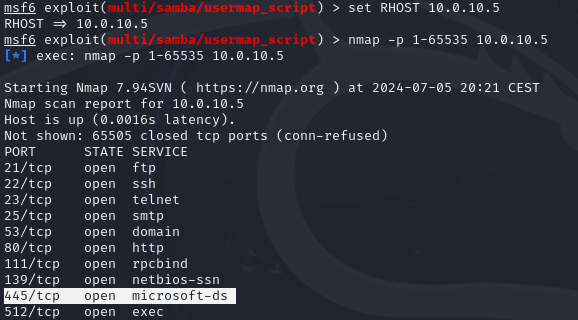
Buscar módulos de exploit en Metasploit

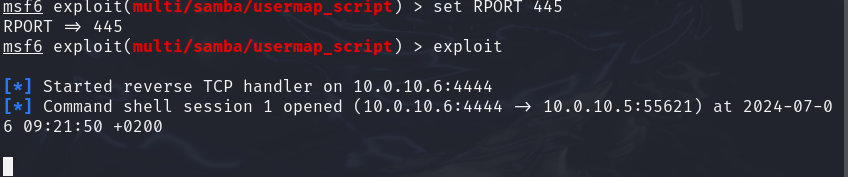


Elegir payload



Configurar y explotar





aquí se ha quedado bloqueado y no ha terminado el exploit aunque habiendo reinicializado las dos machinas virtuales

Ejercicio 3 - OSINT y Metasploit

Vulnerabilidad: CVE-2011-3556 (Java RMI)

Ficha de la vulnerabilidad:

Descripción

permite a un atacante hacer ejecución remota de código

A que software afecta

RMI

Utilidad del software

permite a las aplicaciones java invocar métodos en objetos remotos

Versiones del software afectadas

cualquier aplicación java que implemente RMI sin las configuraciones de seguridad

Puertos que lo utilizan

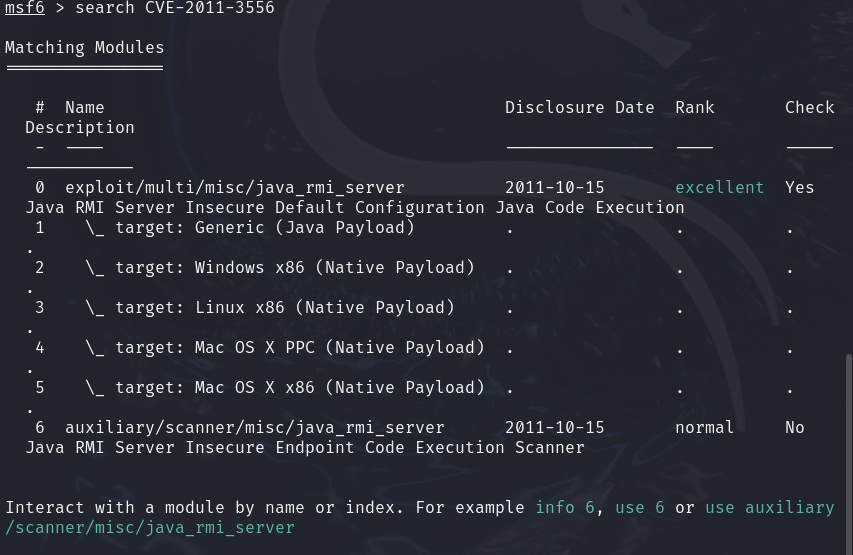
por encima de 1024

Módulos de metasploit relacionados

metasploit framework

Explotar la vulnerabilidad:

Buscar módulos de exploit en Metasploit



Elegir payload



Configurar y explotar

