db\_nmap es una herramienta poderosa dentro del framework Metasploit que permite realizar escaneos de puertos utilizando Nmap y almacenar los resultados directamente en la base de datos de Metasploit. Esto facilita la gestión y análisis de los resultados del escaneo.

A continuación, te muestro cómo realizar un escaneo de puertos con db\_nmap en Metasploit:

**Paso 1: Iniciar Metasploit**

1. **Abre una terminal** y escribe:

bash

Copy code

msfconsole

**Paso 2: Conectar a la Base de Datos**

1. **Inicia la base de datos** (si aún no está iniciada):

bash

Copy code

sudo systemctl start postgresql

sudo msfdb init

1. **Conecta Metasploit a la base de datos**:

bash

Copy code

db\_connect -y /path/to/database.yml

Asegúrate de que el archivo database.yml contiene la configuración correcta para la base de datos PostgreSQL.

**Paso 3: Usar db\_nmap para Escanear Puertos**

1. **Ejecuta el comando db\_nmap con las opciones deseadas**. Por ejemplo, para realizar un escaneo básico de puertos:

bash

Copy code

db\_nmap -sV -p 1-65535 <target>

Donde:

* + -sV: Detecta versiones de servicios.
  + -p 1-65535: Escanea todos los puertos.
  + <target>: Reemplaza con la dirección IP o rango de direcciones IP objetivo.

**Paso 4: Ver los Resultados del Escaneo**

1. **Ver hosts descubiertos**:

bash

Copy code

hosts

1. **Ver servicios descubiertos**:

bash

Copy code

services

**Ejemplos de Comandos db\_nmap**

1. **Escaneo rápido de puertos comunes**:

bash

Copy code

db\_nmap -F <target>

1. **Escaneo con detección de SO**:

bash

Copy code

db\_nmap -O <target>

1. **Escaneo con scripts de Nmap**:

bash

Copy code

db\_nmap --script vuln <target>

Este comando utiliza scripts de Nmap para buscar vulnerabilidades conocidas.

**Gestión Avanzada de Resultados**

* **Buscar servicios específicos**:

bash

Copy code

services -p 80,443

Esto muestra todos los servicios en los puertos 80 y 443.

* **Buscar hosts vulnerables**:

bash

Copy code

vulns

**Consejos Adicionales**

* **Documentación y ayuda**: Puedes obtener más información sobre las opciones de db\_nmap directamente en Metasploit:

bash

Copy code

help db\_nmap

Realizar escaneos de puertos con db\_nmap en Metasploit te permite integrar los resultados directamente en el flujo de trabajo de Metasploit, facilitando la explotación y gestión de vulnerabilidades. Asegúrate de usar estas herramientas de manera ética y en entornos autorizados.