**Fingerprinting con módulos auxiliares**

Nos permite hacer uso de módulos de Metasploit para conocer las versiones del software con base a sus características. Esto es conocido con fingerprinting, dado que, al igual que nuestras huellas cuentan con elementos y características específicas que los diferencian del resto, así sucede con las versiones de los sistemas en general.

Para esto debemos:

1. filtramos en metasploit los modulos especializados en versiones con el siguiente comando:

search type:auxiliary \_version

1. Seleccionamos el módulo que nos interese, es tan sencillo como tipear use, seguido del enumerador que aparece en la parte izquierda, de esta forma es más rápido que escribir toda la ruta.
2. vemos las opciones del módulo con:

options

#O también con:

show options

1. realiza las configuraciones específicas, por ejemplo, especificar el RHOST o cambiar un puerto si este no es el que necesitas.
2. Dale al run y disfruta la magia.

### ¿Qué es el Fingerprinting?

El fingerprinting (huella digital) es el proceso de recolectar información detallada sobre un sistema, red o aplicación para identificar sus características específicas. Esto incluye versiones de software, servicios en ejecución, sistemas operativos y configuraciones particulares. El objetivo es obtener una visión clara del entorno de destino para evaluar su seguridad.

### Realización de Fingerprinting con Módulos Auxiliares en Metasploit

**Metasploit** es una plataforma de pruebas de penetración que contiene una gran cantidad de herramientas y módulos para realizar tareas de reconocimiento y explotación. Los módulos auxiliares en Metasploit se utilizan para realizar tareas que no implican la explotación directa, como el escaneo, la enumeración y el fingerprinting.

Para realizar fingerprinting con módulos auxiliares, puedes utilizar herramientas como Metasploit en Kali Linux. Metasploit es una plataforma potente y flexible que ofrece una variedad de módulos auxiliares para realizar fingerprinting y otras tareas de reconocimiento.

### Pasos para Realizar Fingerprinting con Módulos Auxiliares en Metasploit

1. **Abrir Metasploit en Kali Linux**:
   * Abre una terminal en tu máquina Kali Linux y ejecuta:

bash

Copy code

sudo msfconsole

1. **Buscar Módulos Auxiliares para Fingerprinting**:
   * En la consola de Metasploit, puedes buscar módulos auxiliares relacionados con fingerprinting usando el comando search:

bash

Copy code

search auxiliary/scanner

* + Esto te mostrará una lista de módulos de escaneo disponibles en Metasploit.

1. **Seleccionar un Módulo Auxiliar**:
   * Aquí hay algunos módulos comunes que podrías usar para fingerprinting:
     + auxiliary/scanner/http/http\_version: Identifica la versión del servidor web.
     + auxiliary/scanner/portscan/tcp: Realiza un escaneo de puertos TCP.
     + auxiliary/scanner/snmp/snmp\_enum: Enumera información a través de SNMP.
     + auxiliary/scanner/smb/smb\_version: Identifica la versión de SMB en uso.
   * Para seleccionar un módulo, usa el comando use:

bash

Copy code

use auxiliary/scanner/http/http\_version

1. **Configurar el Módulo**:
   * Cada módulo tiene opciones específicas que necesitas configurar. Para ver las opciones disponibles, usa el comando show options:

bash

Copy code

show options

* + Configura las opciones requeridas, como la dirección IP del objetivo (RHOSTS):

bash

Copy code

set RHOSTS <IP\_de\_Ubuntu\_Server>

1. **Ejecutar el Módulo**:
   * Una vez configuradas las opciones, ejecuta el módulo con el comando run:

bash

Copy code

run

### Ejemplo de Uso

Vamos a usar el módulo http\_version como ejemplo:

1. **Abrir Metasploit y Seleccionar el Módulo**:

bash

Copy code

sudo msfconsole

use auxiliary/scanner/http/http\_version

1. **Configurar el Módulo**:

bash

Copy code

set RHOSTS 192.168.x.x

set RPORT 80

1. **Ejecutar el Módulo**:

bash

Copy code

run

Esto debería proporcionarte información sobre la versión del servidor web que está corriendo en tu servidor Ubuntu.

### Otros Módulos Auxiliares Útiles

* **Escaneo de Puertos**:

bash

Copy code

use auxiliary/scanner/portscan/tcp

set RHOSTS 192.168.x.x

set PORTS 1-1000

run

* **Enumeración de SMB**:

bash

Copy code

use auxiliary/scanner/smb/smb\_version

set RHOSTS 192.168.x.x

run

* **Enumeración de SNMP**:

bash

Copy code

use auxiliary/scanner/snmp/snmp\_enum

set RHOSTS 192.168.x.x

run

### Consideraciones Adicionales

* **Permisos**: Asegúrate de tener los permisos necesarios para realizar estos escaneos en el objetivo.
* **Uso Responsable**: Usa estas herramientas de manera responsable y solo en sistemas donde tengas autorización para realizar pruebas.

Si tienes alguna pregunta específica sobre algún módulo o necesitas más detalles, no dudes en preguntar.