Análisis de vulnerabilidades con WMAP

Con este plugin podemos hacer la búsqueda de vulnerabilidades más rápida y eficiente.

Primero, debemos configurar los sitios a analizar:

Pero antes validaremos si se ha cargado automáticamente algún sitio basado en nuestros escaneos.

wmap\_sites -l

Listo, si no contamos con ningún sitio, debemos añadir la bandera -a, de la siguiente forma:

wmap\_sites -a <https//:Nombre\_Dominio>

Ahora debemos añadir el target, que no es otro que la ip del dominio o sitio que auditaremos.

wmap\_target -t <https//:ip>

Listo, ahora solo queda ejecutar:

wmap\_run

Finalmente, para ver de manera organizada las vulnerabilidades encontradas por el plugin, escribiremos:

wmap\_vulns -l

Enjoy your hacking!

WMAP es un complemento (plugin) de Metasploit para realizar análisis de vulnerabilidades web. Este plugin facilita la identificación y explotación de vulnerabilidades en aplicaciones web, integrando la funcionalidad de escaneo de vulnerabilidades web directamente en el entorno de Metasploit.

**Configuración y Uso de WMAP en Metasploit**

**Paso 1: Cargar el Plugin WMAP**

Para usar WMAP, primero debes cargar el plugin en Metasploit:

bash

Copy code

msf6 > load wmap

**Paso 2: Configurar el Escaneo**

1. **Agregar el Sitio Web a Escanear**:

Debes agregar el objetivo que deseas escanear. Puedes hacerlo utilizando el siguiente comando:

bash

Copy code

msf6 > wmap\_sites -a http://example.com

1. **Agregar las URL de Inicio de Escaneo**:

Después de agregar el sitio, puedes agregar URLs específicas para iniciar el escaneo:

bash

Copy code

msf6 > wmap\_targets -t http://example.com/login

**Paso 3: Realizar el Escaneo**

WMAP tiene varios módulos que puedes usar para realizar diferentes tipos de escaneos. Aquí te muestro cómo configurar y ejecutar estos escaneos:

1. **Ver los Módulos Disponibles**:

Puedes listar los módulos disponibles con el siguiente comando:

bash

Copy code

msf6 > wmap\_run -t

Esto te mostrará una lista de módulos de escaneo disponibles, tales como:

* + Escaneo de contenido
  + Análisis de configuración
  + Detección de inyecciones SQL
  + Pruebas de cross-site scripting (XSS)
  + Etc.

1. **Seleccionar y Ejecutar un Módulo**:

Para ejecutar un módulo específico, usa el siguiente comando:

bash

Copy code

msf6 > wmap\_run -m <module\_name>

Por ejemplo, para ejecutar un análisis de inyección SQL:

bash

Copy code

msf6 > wmap\_run -m auxiliary/scanner/http/wmap\_sqlmap

**Paso 4: Revisar los Resultados**

Una vez que el escaneo haya terminado, puedes revisar los resultados utilizando los siguientes comandos:

1. **Listar los Objetivos Escaneados**:

bash

Copy code

msf6 > wmap\_sites -l

1. **Ver los Resultados del Escaneo**:

bash

Copy code

msf6 > wmap\_vulns -l

Esto listará las vulnerabilidades encontradas durante el escaneo.

**Ejemplo Completo de Uso de WMAP**

Aquí hay un ejemplo paso a paso de cómo usar WMAP para escanear un sitio web y analizar las vulnerabilidades encontradas:

1. **Cargar WMAP**:

bash

Copy code

msf6 > load wmap

1. **Agregar el Sitio a Escanear**:

bash

Copy code

msf6 > wmap\_sites -a http://example.com

1. **Agregar una URL Específica**:

bash

Copy code

msf6 > wmap\_targets -t http://example.com/login

1. **Ejecutar un Escaneo de SQL Injection**:

bash

Copy code

msf6 > wmap\_run -m auxiliary/scanner/http/wmap\_sqlmap

1. **Listar los Resultados del Escaneo**:

bash

Copy code

msf6 > wmap\_vulns -l

**Consideraciones de Seguridad y Ética**

* **Permisos**: Asegúrate de tener permiso explícito para escanear y probar cualquier sitio web o aplicación web. El escaneo no autorizado puede ser ilegal y puede tener consecuencias serias.
* **Legalidad**: Verifica la legalidad de tus acciones en tu jurisdicción.
* **Responsabilidad**: Utiliza estas herramientas de manera responsable y ética, con el propósito de mejorar la seguridad y no para causar daño.

Con estos pasos, puedes utilizar WMAP en Metasploit para realizar análisis de vulnerabilidades en aplicaciones web, identificar problemas de seguridad y tomar las medidas adecuadas para mitigarlas.