Wpscan es una herramienta para encontrar vulnerabilidades en sitios web creados con Wordpress. Hay tres tipos de puntos debiles de Wordpress donde se pueden encontrar vulnerabilidades: el core, los plugins y los temas.

ejemplo comando:

wpscan --url https://platzi.com -e --api-token XXX

Es requerido que se suminstre un API KEY al comando de escaneo para que pueda mostrar las vulnerabilidades encontradas. Este API KEY se puede obtener en el sitio de wpscan, previo registro y login del usuario.

Entiendo que quieres utilizar wpscan en Kali Linux para realizar pruebas de seguridad en una aplicación web. Aquí tienes una guía detallada sobre cómo usar wpscan para escanear tu servidor web (en este caso, Mutillidae).

### Instalación de WPScan en Kali Linux

WPScan ya viene preinstalado en Kali Linux, pero en caso de que necesites actualizarlo o instalarlo, sigue estos pasos:

1. **Actualizar los repositorios y el sistema**:

bash

Copy code

sudo apt update && sudo apt upgrade

1. **Instalar WPScan (si no está ya instalado)**:

bash

Copy code

sudo apt install wpscan

### Preparación del Entorno

1. **Asegúrate de que Apache esté corriendo en Ubuntu Server**:

bash

Copy code

sudo systemctl start apache2

1. **Asegúrate de que tu Ubuntu Server tenga una dirección IP válida y que esté accesible desde tu máquina Kali**:
   * En Ubuntu Server:

bash

Copy code

ip a

* + Verifica la dirección IP (por ejemplo, 192.168.x.x).

1. **Desde Kali Linux, verifica la conectividad con Ubuntu Server**:
   * En Kali Linux:

bash

Copy code

ping <IP\_de\_Ubuntu\_Server>

* + Asegúrate de reemplazar <IP\_de\_Ubuntu\_Server> con la dirección IP de tu Ubuntu Server.

### Uso de WPScan

WPScan se usa principalmente para escanear sitios web basados en WordPress, pero también puede proporcionar información útil sobre otros tipos de aplicaciones web.

1. **Escanear el sitio web con WPScan**:
   * Ejecuta WPScan en tu máquina Kali Linux para escanear tu servidor Ubuntu donde está corriendo Mutillidae:

bash

Copy code

wpscan --url http://<IP\_de\_Ubuntu\_Server>/mutillidae

* + Asegúrate de reemplazar <IP\_de\_Ubuntu\_Server> con la dirección IP de tu Ubuntu Server.

### Analizar los Resultados

1. **Revisa los resultados del escaneo**:
   * WPScan proporcionará información sobre las vulnerabilidades detectadas, plugins instalados, temas, y versiones.
   * Aunque WPScan está optimizado para WordPress, puede identificar otras vulnerabilidades web genéricas que pueden ser útiles.

### Consideraciones Adicionales

* **Configurar el Firewall**:
  + Asegúrate de que el firewall en Ubuntu Server no esté bloqueando las conexiones entrantes en el puerto 80 (HTTP):

bash

Copy code

sudo ufw allow 80/tcp

sudo ufw enable

* **Herramientas Adicionales**:
  + Si WPScan no proporciona suficiente información para Mutillidae, considera usar herramientas adicionales como nikto, burpsuite, o nmap para un análisis más detallado.

### Ejemplo de Uso de WPScan

bash

Copy code

wpscan --url http://192.168.x.x/mutillidae --enumerate vp

* --url: Especifica la URL del sitio web a escanear.
* --enumerate vp: Enumera los plugins vulnerables.

### Ejemplo de Uso de Nikto para Mayor Cobertura

1. **Instalar Nikto (si no está ya instalado)**:

bash

Copy code

sudo apt install nikto

1. **Ejecutar Nikto**:

bash

Copy code

nikto -h http://<IP\_de\_Ubuntu\_Server>/mutillidae

Esto te proporcionará un análisis más amplio de posibles vulnerabilidades en la aplicación web.

Si necesitas ayuda adicional, no dudes en preguntar.

4o