# PRACTICA HACKING ÉTICO

## Objetivos

Para esta actividad final, realizará una prueba de penetración completa que comenzará con el reconocimiento y luego lanzará explotaciones contra las vulnerabilidades que haya descubierto. Por último, propondrá la corrección de las explotaciones.

Esta evaluación adopta la forma de un ejercicio de captura de indicadores de ciberseguridad. Utilizará sus habilidades de piratería ética para localizar archivos que contengan valores de marca. Luego, informará los valores de los indicadores que encontró como parte de la evaluación.

En esta simulación de un compromiso de piratería ética, utilizará herramientas para aprovechar las vulnerabilidades que descubra para alcanzar una meta. Esto puede implicar un enfoque de prueba y error que requiere persistencia y puede incluir cierto grado de dificultad. Para su propio desarrollo de habilidades, trabajar en esta lucha puede ser productivo. Si está completamente atascado, puede acceder a las respuestas y soluciones en cualquier momento durante esta evaluación.

- **Desafío 1**: Usar la inyección SQL para encontrar un archivo de indicador.
- **Desafío 2**: Utilizar las vulnerabilidades del servidor web para investigar directorios y encontrar un archivo de indicador.
- **Desafío 3**: Aprovechar los recursos compartidos abiertos de Samba para acceder a un archivo de indicadores.
- **Desafío 4**: Analizar un archivo de captura de Wireshark para encontrar la ubicación de un archivo que contenga información de los indicadores.

## Recursos necesarios

- **Kali VM personalizada para el curso Ethical Hacker.** Esta máquina virtual se encuentra https://drive.google.com/file/d/1h6uTC6aBd8p1sU8eB5r74ryWcyDsd6yf/view?usp=sharing. Solo se puede acceder al archivo compartido usando vuestra cuenta de educamadrid.
- **Las claves de acceso son:** usuario kali password kali

## Instrucciones para la realización de la práctica

**Trasfondo/Escenario**

Lo contrataron para realizar una prueba de penetración para un cliente. Al finalizar la prueba, el cliente solicitó un informe completo que incluya las vulnerabilidades descubiertas, las explotaciones exitosas y los pasos de corrección para proteger los sistemas vulnerables. Tiene acceso a los hosts en las redes 10.6.6.0/24 y 172.17.0.0/24.

## Desafío 1: Inyección de SQL

En esta parte, debe descubrir la información de la cuenta de usuario en un servidor y descifrar la contraseña de la cuenta de Gordon Brown. Luego, ubicará el archivo que contiene el código del Desafío 1 y usará las credenciales de la cuenta de Gordon Brown para abrir el archivo en 172.17.0.2 para ver su contenido.

Paso 1: Configuración preliminar.

1. Abra un navegador y vaya al sitio web en 10.6.6.100.
2. Nota: Si tiene problemas para acceder al sitio web, elimine el prefijo https: // de la dirección IP en el campo de dirección del navegador.
3. Inicie sesión con las credenciales admin / password.
4. Establezca el nivel de seguridad de DVWA en low y haga clic en Submit.

Paso 2: Recupere las credenciales de usuario para la cuenta de Gordon Brown.

1. Identifique la tabla que contiene los nombres de usuario y las contraseñas.
2. Busque un formulario de entrada vulnerable que le permita inyectar comandos SQL.
3. Recupere el nombre de usuario y el hash de contraseña de la cuenta de Gordon Brown.

Paso 3: Descifre la contraseña de la cuenta de Gordon Brown.

1. Utilice cualquier herramienta de descifrado de hash de contraseñas que desee para descifrar la contraseña de Gordon Brown.

**¿Cuál es la contraseña de la cuenta de Gordon Brown?**

Paso 4: Busque y abra el archivo con el código de desafío 1.

1. Inicie sesión en 172.17.0.2 como Gordon Brown.
2. Busque y abra el archivo de indicadores en el directorio de inicio del usuario.

**¿Cuál es el nombre del archivo con el código?**

**¿Cuál es el mensaje contenido en el archivo? Ingrese el código que encuentra en el archivo.**

Paso 5: Investigue y proponga la corrección de ataques de SQL.

**¿Cuáles son los cinco métodos de corrección para prevenir los ataques de inyección de SQL?**

## Desafío 2: Vulnerabilidades del servidor web

En esta parte, debe encontrar las vulnerabilidades en un servidor HTTP. La configuración incorrecta de un servidor web puede permitir la lista de archivos contenidos en directorios en el servidor. Puede utilizar cualquiera de las herramientas que aprendió en prácticas de laboratorio anteriores para realizar un reconocimiento y encontrar los directorios vulnerables.

En este desafío, ubicará el archivo de indicadores en un directorio vulnerable de un servidor web.

Paso 1: Configuración preliminar.

1. Si aún no lo ha hecho, inicie sesión en el servidor en 10.6.6.100 con las credenciales admin / password.
2. Establezca el nivel de seguridad de la aplicación en bajo.

Paso 2: A partir de los resultados del reconocimiento, determine qué directorios se pueden ver mediante un navegador web y la manipulación de URL.

1. Realice un reconocimiento en el servidor para encontrar los directorios donde se encontró la indexación.

**¿A qué directorios se puede acceder a través de un navegador web para enumerar los archivos y subdirectorios que contienen?**

Paso 3: Vea los archivos contenidos en cada directorio para encontrar el archivo que contiene el indicador.

1. Cree una URL en el navegador web para acceder a los subdirectorios visibles. Busque el archivo con el código del desafío 2 en uno de los subdirectorios.

**¿En qué dos subdirectorios pueden buscar el archivo?**

**¿Cuál es el nombre del archivo con el código del Desafío 2?**

**¿Qué subdirectorio contenía el archivo?**

**¿Cuál es el mensaje contenido en el archivo de indicador? Ingrese el código que encuentra en el archivo.**

Paso 4: Investigue y proponga la corrección de explotaciones de listas de directorios.

**¿Cuáles son los dos métodos de corrección para evitar explotaciones en las listas de directorios?**

## Desafío 3: Aprovechar los recursos compartidos del servidor SMB abierto

En esta parte, querrá descubrir si hay directorios compartidos no seguros ubicados en un servidor SMB en la red 10.6.6.0/24. Puede utilizar cualquiera de las herramientas que aprendió en prácticas de laboratorio anteriores para encontrar las unidades compartidas disponibles en los servidores.

Paso 1: Busque posibles destinos que ejecuten SMB.

1. Utilice herramientas de análisis para analizar la LAN 10.6.6.0/24 en busca de posibles objetivos para la enumeración de SMB.

**¿Qué host de la red 10.6.6.0/24 tiene puertos abiertos que indican que es probable que ejecute servicios SMB?**

Paso 2: Determine qué directorios de SMB se comparten y pueden acceder a ellos usuarios anónimos.

1. Utilice una herramienta para escanear el dispositivo que ejecuta SMB y ubicar los recursos compartidos a los que pueden acceder los usuarios anónimos.

**¿Qué recursos compartidos se enumeran en el servidor SMB? ¿Cuáles son accesibles sin un inicio de sesión de usuario válido?**

Paso 3: Investigue cada directorio compartido para encontrar el archivo.

1. Utilice el cliente nativo de SMB para acceder a las unidades compartidas en el servidor SMB. Utilice dir, ls, cd y otros comandos para buscar subdirectorios y archivos.
2. Busque el archivo con el código del desafío 3. Descargue el archivo y ábralo localmente.

**¿En qué recurso compartido se encuentra el archivo?**

**¿Cuál es el nombre del archivo con el código del desafío 3?**

**Ingrese el código para el Desafío 3 a continuación.**

Paso 4: Investigue y proponga la corrección del ataque de SMB.

**¿Cuáles son los dos métodos de corrección para evitar el acceso a servidores SMB?**

## Desafío 4: Analizar un archivo PCAP para encontrar información.

Como parte de su esfuerzo de reconocimiento, su equipo capturó el tráfico con Wireshark. El archivo de captura, SA.pcap, se encuentra en el subdirectorio OTHER dentro del directorio principal del usuario kali.

Paso 1: Busque y analice el archivo SA.pcap.

1. Analice el contenido del archivo PCAP para determinar la dirección IP de la computadora de destino y la ubicación URL del archivo con el código del Desafío 4.

**¿Cuál es la dirección IP del ordenador objetivo?**

**¿Qué directorios del destino se revelan en el PCAP?**

Paso 2: Utilice un navegador web para mostrar el contenido de los directorios en la computadora de destino.

1. Utilice un navegador web para investigar las URL enumeradas en el resultado de Wireshark. Busque el archivo con el código para el desafío 4.

**¿Cuál es la URL del archivo?**

**¿Cuál es el contenido del archivo?**

**¿Cuál es el código del desafío 4?**

Paso 3: Investigue y proponga una corrección que evitaría que el contenido del archivo se transmita en texto sin cifrar.

**¿Cuáles son los dos métodos de corrección que pueden evitar que personas no autorizadas vean el contenido de los archivos?**