Fecha límite para la entrega: 24 de diciembre de 2024

1. OBJETIVO

En esta práctica evaluaremos diferentes herramientas que nos ayudan a la hora de realizar auditorías de seguridad. Las pruebas se realizarán en un **entorno virtual controlado**, construido exclusivamente para uso docente. Usaremos Kali Linux como distribución de referencia, aunque no todas las herramientas a evaluar se encuentran disponibles en esta distribución (en ese caso será necesaria su instalación).

2. ENTORNO DE TRABAJO

En primer lugar, construiremos un entorno virtual para la realización de la práctica. Usaremos una red virtual que ofrezca a las VM visibilidad entre ellas y conectividad exterior (por ejemplo, la red NAT de *VMWare* o la red **NAT Network** de *Virtualbox*). Levantaremos al menos las siguientes máquinas virtuales:

- VM con Kali Linux
- VM con Metasploitable 2 (Linux)
- VM Linux genérica (RockyLinux, Ubuntu, Debian, …) con algún servicio arrancado.

Opcionalmente, se podrá incorporar al entorno un equipo con MS Windows (Metasploitable 3 o una VM genérica).

Se recomienda tomar instantáneas o realizar copias con la configuración de las VM, para poder recuperar este estado rápidamente si es necesario regresar al punto de partida o a algún otro punto que se considere.

3. TAREAS Y HERRAMIENTAS

a. Extracción de información de DNS (una herramienta)
b. Dorking con ATSCAN
c. Exploración de red con nmap (al menos 5 escaneos + 5 scripts, estos últimos preferiblemente distintos de los descritos en la documentación de clase)
d. Escaneo web (dos herramientas)
e. Auditoría de host (una herramienta no descrita en la documentación)
f. Análisis de Vulnerabilidades (GVM/OpenVAS o Nessus Essentials)
g. Inyección SQL (sqlmap)
h. Ataques a contraseñas online (una herramienta)
i. Ataques a contraseñas offline (una herramienta)
j. Metasploit (enumeración, identificación de vulnerabilidades y explotación)

4. REALIZACIÓN DE LA PRÁCTICA

Seleccionar **al menos cinco** de las tareas propuestas (la última, Metasploit, es **obligatoria**). Cuando sea necesario, se indicarán posibles herramientas disponibles y se seleccionará una de ellas para su uso. En cada tarea se evaluará la herramienta elegida con ejemplos de uso. Las dos propuestas iniciales (extracción DNS y Dorking) podrán realizarse sobre recursos externos. El resto se realizará sobre equipos de nuestro entorno de pruebas.

5. PARTES OPCIONALES

Se consideran partes opcionales todas las tareas realizadas que exceden las cinco obligatorias. La máxima puntuación en esta parte opcional se alcanza realizando al menos otras tres tareas propuestas, además de las cinco obligatorias.

6. FORMA DE ENTREGA

Una vez finalizada la práctica, se entregará una memoria justificativa **en formato PDF**. Deberá incluir los pasos seguidos para la realización de cada tarea planteada, comandos utilizados y dificultades encontradas.

La memoria será ordenada, clara y legible, e irá encabezada con el nombre de los autores. Se deberán evitar los "listados" innecesarios. Si se considera de interés, podrán incorporarse como anexos a la memoria, debidamente reseñados.

El resultado será un documento único denominado **practica3-SPD.pdf** que se enviará antes de la fecha de cierre a la dirección de correo electrónico teo.rojo@ceu.es.

Se podrá requerir la defensa individual de la práctica. Se deberá guardar una copia del entorno virtual utilizado en el desarrollo de la práctica, para poder verificar, si fuera necesario, su correcto funcionamiento.

7. REFERENCIAS

Kali Linux VM
https://www.kali.org/get-kali/#kali-virtual-machines

Official Kali Linux Documentation
https://www.kali.org/kali-linux-documentation/

Metasploitable 2
https://sourceforge.net/projects/metasploitable/

Metasploitable 3
https://github.com/rapid7/metasploitable3