1. WhatWeb

¿Qué es? Es una herramienta que escanea la web y permite detectar qué tecnologías están siendo utilizadas en esta, de esta forma podemos averiguar el CMS, el servidor, los diversos lenguajes de programación, bibliotecas… Es útil a la hora de recopilar información sobre una página web antes de realizar un proceso más exhaustivo de la ciberseguridad de esta.

¿Cómo se instala?

1. Necesitas tener instalado git y ruby, lo puedes hacer con el comando => sudo apt install git ruby.
2. Descargar whatweb desde el repositorio de github, con el comando => git clone https://github.com/urbanadventurer/WhatWeb.git

¿Cómo se utiliza?

1. Para usarla la herramienta, primeros debemos acceder a la carpeta con el comando => cd WhatWeb
2. Instalar la herramienta con el repositorio, esta se hace con el comando sudo ruby setup.rb.

Tras hacer estos pasos tendremos ya operativo el comando “whatweb dirección”, algunas de sus variantes son:

- Escaneo básico: whatweb ”dirección”
- Más detalles: whatweb -v “dirección”
- Escanear múltiples sitios desde un archivo: whatweb -i “nombredelarchivo.txt”

2. Dirb

¿Qué es? Es una herramienta de fuerza bruta que se usa para descubrir directorios y archivos ocultos en un servidor web. Se basa en diccionarios de palabras que contienen nombres comunes de directorios y archivos para intentar acceder a ellos.

¿Cómo se instala?

1. Necesitas tener instalado dirb, lo puedes hacer con el comando => sudo apt install dirb.
2. Descargar Dirb desde el repositorio de github, con el comando => git clone https://github.com/v0re/dirb.git

¿Cómo se utiliza?

1. Para usarla la herramienta, primeros debemos acceder a la carpeta con el comando => cd dirb
2. Para no tener que navegar a este directorio para ejecutar el comando podemos añadirlo al paht, con moverlo a /usr/local/bin con el comando export PATH=”$PATH:4~/direccion de dirb”, importante este comando se debe ejecutar desde el directorio a donde lo queramos mover.
3. Compilar la herramienta con el comando => make

4. Tras ejecutar make, nos saldrán las URLS “ocultas” y ya podremos ver si son accesibles.

3. Linux-exploit-suggester

¿Qué es? Linux Exploit Suggester (LES) es una herramienta que analiza la versión del kernel y otros componentes del sistema para recomendar posibles exploits que podrían usarse para escalar privilegios en una máquina Linux.

¿Cómo se instala?

1. Descargar desde el repositorio de github, con el comando => git clone https://github.com/The-Z-Labs/linux-exploit-suggester.git

¿Cómo se utiliza?

1. Para usarla la herramienta, primeros debemos acceder a la carpeta con el comando => cd linux-exploit-suggester.
2. Una vez dentro podemos darle más permisos al script, con el comando chmod 777 linux-exploit-suggester.
3. Ejecutamso el script “./linux-exploit-suggester.sh”

Tras ejecutar el script nos saldrán las vulnerabilidades con la probabilidad de que esta suceda. Haciendo una simple búsqueda en github con el nombre de la vulnerabilidad nos saldrá un repositorio, vemos las instrucciones que suelen poner en la página y nos lo descargamos y vemos si es vulnerable desde ahí.