Escaneo de puertos

En este proyecto se escanea la maquina Debian utilizando la maquina Kali como atacante mediante un escaneo de puertos con la herramienta NMAP para detectar vulnerabilidades y posteriormente consultarlas en bases de datos públicas.

En primer lugar, se escanea la maquina debían mediante el comando nmap –Sv –script=vuln <IP> y este nos muestra como resultado tanto los programas como su versión y vulnerabilidades.

En este caso la maquina Debian no muestra vulnerabilidades en los archivos “http-stored-xss”, “http-dom-based-xss” ni “http-csrf”. Sin embargo, muestra la versión Apache 2.4.62.

Esta versión de Apache es reciente y no muestra ninguna vulnerabilidad aparente, de hecho, soluciona la vulnerabilidad CVE-2024-39884 de su versión anterior.

Sin embargo, sí que existe un fallo de seguridad en la maquina debían pues con el escaneo podemos encontrar un archivo info.php, el cual puede contener información sensible acerca de la máquina. Para acceder a este archivo simplemente se debe buscar en cualquier buscador la dirección http://<IP>/info.php , dirección que nos abre toda la información acerca de todos los pluggings instalados, versiones y vulnerabilidades.

Gracias a este archivo podemos ver, entre otros muchos programas, la versión de mysqlnd; 8.2.28, que presenta las siguientes vulnerabilidades.

CVE-2025-1861	Cuando se analiza la redirección HTTP en la respuesta a una solicitud HTTP, actualmente hay un límite en el tamaño del valor de ubicación causado por el tamaño limitado del búfer de ubicación a 1024. Esto puede dar lugar a un truncamiento incorrecto de la URL y redirigir a una ubicación incorrecta.
CVE-2025-1219	Cuando se solicita un recurso HTTP utilizando las extensiones DOM o SimpleXML, se utiliza la cabecera content-type incorrecta para determinar el conjunto de caracteres cuando el recurso solicitado realiza una redirección. Esto puede provocar que el documento resultante se analice de forma incorrecta o se salte las validaciones.
CVE-2010-3063	La función php_mysqlnd_read_error_from_line de la extensión Mysqlnd de PHP 5.3 a 5.3.2 no calcula correctamente la longitud del búfer, lo que permite a los atacantes dependientes del contexto provocar un desbordamiento de búfer basado en la pila a través de entradas manipuladas que hacen que se utilice un valor de longitud negativo.