Generación de reportes HTML en Nmap

Pedro Egea Ortega

Índice

Generación de reportes HTML a partir de escaneos Nmap

Introducción

Nmap es una herramienta ampliamente utilizada en auditorías de seguridad y análisis de redes para el descubrimiento de hosts, puertos y servicios activos. Si bien es común su uso para identificar puertos abiertos y servicios, su funcionalidad de exportación de resultados en formatos estructurados, como XML, suele ser subutilizada.

Este documento describe el procedimiento para generar un reporte en HTML a partir de un escaneo de Nmap, facilitando la visualización y documentación de los resultados.

1. Escaneo con Nmap

Para realizar un escaneo completo de puertos y detección de versiones de servicios, se puede utilizar el siguiente comando:

$ sudo nmap -p- -sV [IP] -oX archivo.xml

Descripción de los parámetros:

- -p-: Escanea todos los puertos TCP (1-65535).
- -sV: Detecta la versión de los servicios activos en cada puerto.
- -oX archivo.xml: Exporta los resultados del escaneo a un archivo en formato XML.

El archivo XML generado contiene información estructurada sobre cada puerto abierto, los servicios detectados y las versiones identificadas.

2. Conversión del XML a HTML

Nmap incluye una hoja de estilo XSLT dentro del XML generado, lo que permite transformar automáticamente el contenido en un reporte HTML legible en navegadores. Para realizar esta conversión, se utiliza el siguiente comando:

$ xsltproc archivo.xml -o archivo.html

Explicación del comando:

- xsltproc: Herramienta de línea de comandos para aplicar transformaciones XSLT a archivos XML.
- archivo.xml: Archivo XML generado por Nmap.
- -o archivo.html: Archivo de salida en formato HTML.

3. Resultado

La ejecución del proceso descrito genera un informe en HTML que permite:

- Visualizar puertos abiertos y servicios de forma clara y estructurada.
- Identificar versiones de software y servicios activos.
- Documentar los hallazgos para auditorías de seguridad, prácticas académicas o informes internos.

Este procedimiento facilita la presentación de resultados a perfiles tanto técnicos como no técnicos, mejorando la comunicación y la documentación de los escaneos de red.