**Métodos para el escaneo de vulnerabilidades**

Previamente, aprendiste sobre una **evaluación de vulnerabilidad**, que es el proceso de revisión interna de los sistemas de seguridad de una organización. Las evaluaciones de vulnerabilidad se llevan a cabo con el fin de identificar debilidades y prevenir ataques. Por lo general, las herramientas de análisis de vulnerabilidades se utilizan para simular amenazas mediante la búsqueda de vulnerabilidades en una superficie de ataque. También ayudan a los equipos de seguridad a tomar medidas proactivas para implementar su estrategia de remediación.

Los escáneres de vulnerabilidades son herramientas importantes que muy probablemente utilizarás en el campo. En esta lectura, explorarás cómo funcionan y los tipos de escaneos que pueden realizar.

**¿Qué es un escáner de vulnerabilidades?**

Un **escáner de vulnerabilidades** es un software que compara automáticamente las vulnerabilidades y exposiciones conocidas con las tecnologías de la red. En general, estas herramientas analizan los sistemas para encontrar configuraciones erróneas o fallas de programación.

Las herramientas de escaneo se utilizan para analizar cada una de las cinco superficies de ataque que aprendiste en [el video sobre la estrategia de defensa en profundidad](https://www.coursera.org/learn/activos-amenazas-y-vulnerabilidades/lecture/IdvXj/estrategia-de-defensa-en-profundidad):

1. **Capa perimetral**,como los sistemas de autenticación que validan el acceso del usuario.
2. **Capa de red**,que se compone de tecnologías como firewalls de red y otros.
3. **Capa de punto de conexión (endpoint)**,que describe los dispositivos en una red, como computadoras portátiles yde escritorio o servidores.
4. **Capa de aplicación**,que involucra el software con el que interactúan los usuarios.
5. **Capa de datos**, que incluye cualquier información almacenada, en tránsito o en uso.

Cuando comienza un escaneo de cualquiera de las capas, la herramienta de escaneo compara los hallazgos con las bases de datos de amenazas de seguridad. Al final del escaneo, la herramienta marca cualquier vulnerabilidad que encuentra y la agrega a su base de datos de referencia. Cada escaneo agrega más información a la base de datos, lo cual ayuda a que la herramienta sea más precisa en su análisis.

**Nota:** La empresa que diseñó el software de escaneo también actualiza las bases de datos de vulnerabilidades de forma rutinaria.

**Realización de escaneos**

Los escáneres de vulnerabilidad no son intrusivos. Es decir, no rompen ni se aprovechan de un sistema como lo haría un atacante, sino que simplemente escanean una superficie y te alertan sobre cualquier puerta potencialmente desbloqueada en tus sistemas.

**Nota:** Si bien los escáneres de vulnerabilidades no son intrusivos, existen casos en los que un análisis puede causar problemas inadvertidamente, como colapsar un sistema.

Existen varias maneras de utilizar estas herramientas para escanear una superficie. Cada una contempla uno de los caminos posibles que un agente de amenaza podría tomar. A continuación, puedes explorar cada tipo de escaneo para obtener una imagen más clara de esto.

**Externo versus interno**

Los escaneos externos e internos simulan la estrategia de un atacante.

Los *escaneos externos* prueban la capa perimetral fuera de la red interna. Analizan sistemas externos, como sitios web y cortafuegos (firewalls). Este tipo de análisis puede descubrir, por ejemplo, puertos de red o servidores vulnerables.

Los *escaneos internos* comienzan desde el extremo opuesto, ya que examinan los sistemas internos de una organización. Por ejemplo, este tipo de escaneo podría analizar software de aplicación, en busca de debilidades en la manera en que gestiona las entradas de usuarios.

**Autenticado versus no autenticado**

Los escaneos autenticados y no autenticados simulan si un usuario tiene o no acceso a un sistema.

Los *escaneos autenticados* pueden testear un sistema iniciando sesión con una cuenta de usuario real o incluso con una cuenta de administrador. Estas cuentas de servicio se utilizan para verificar vulnerabilidades, como controles de acceso rotos.

Los *análisis no autenticados* simulan agentes de amenaza externos que no tienen acceso a los recursos de tu empresa. Por ejemplo, un escaneo podría analizar los recursos compartidos de archivos dentro de la organización que se utilizan para alojar documentos internos solamente. Los usuarios no autenticados deberían recibir resultados de “acceso denegado” si intentan abrir estos archivos. Si es posible acceder a un archivo, se identificará una vulnerabilidad.

**Limitado versus completo**

Los escaneos limitados y completos se centran en dispositivos particulares a los que acceden usuarios internos y externos.

Los *escaneos limitados* analizan dispositivos particulares en una red, como la búsqueda de configuraciones erróneas en un firewall.

Los *análisis exhaustivos* analizan todos los dispositivos conectados a una red. Esto incluye sistemas operativos, bases de datos de usuarios y más.

**Consejo profesional:** antes de los escaneos limitados o completos debe realizarse un escaneo de descubrimiento. Este se utiliza para conocer las computadoras, dispositivos y puertos abiertos que se encuentran en una red.

**Conclusiones clave**

Para encontrar vulnerabilidades, hay que pensar en todas las posibilidades. Los escaneos de vulnerabilidad varían de acuerdo a las superficies que una organización está evaluando. Por lo general, los profesionales de seguridad con más experiencia son quienes están al frente, a la hora configurar y llevar a cabo este tipo de escaneos con el fin de crear un perfil de la postura de seguridad de una empresa. Aun así, los analistas también juegan un papel importante en el proceso. A menudo, los resultados de un análisis de vulnerabilidades conducen a intentos renovados de cumplimiento, cambios en los procedimientos e implementación de parches en el sistema. Comprender los objetivos de los tipos comunes de escaneos de vulnerabilidades te ayudará a participar en estos ejercicios de seguridad proactivos cuando sea posible.