venza®
Better Visibility. Better Defense.

Pruebas de Penetración y Análisis de Vulnerabilidades

Guía de Referencia Rápida

Versión: 1.0

Revisado: Junio 2023

Contenido

Introducción

Cuando se trata de evaluar la seguridad de los sistemas y redes de una organización, dos métodos comúnmente utilizados son las pruebas de penetración ("pen testing") y la exploración de vulnerabilidades.

Aunque comparten el objetivo de identificar las debilidades de un sistema, difieren en sus enfoques y objetivos. Esta guía pretende proporcionar una referencia rápida para entender la diferencia entre las pruebas de penetración y el escaneo de vulnerabilidades.

Definición de Pruebas de Penetración

Las pruebas de penetración, a menudo denominadas hacking ético o de "sombrero blanco", consisten en simular ataques reales a un sistema o red para identificar vulnerabilidades y determinar el impacto potencial de las mismas.

He aquí algunos puntos clave que conviene comprender:

- **Objetivo** - El objetivo principal de las pruebas de penetración es explotar las vulnerabilidades y obtener acceso no autorizado a los sistemas o datos sensibles para evaluar el nivel de riesgo y evaluar la eficacia de las medidas de seguridad.
- **Enfoque** - Los “Pen Testers” utilizan varias técnicas, herramientas y metodologías para imitar ataques del mundo real, simulando las acciones de un atacante real.
- **Alcance** - Las pruebas de penetración pueden realizarse desde perspectivas tanto internas como externas. El “pen testing” interno consiste en evaluar las medidas de seguridad dentro de una red, como servidores y estaciones de trabajo. El “pen testing” externo evalúa la seguridad de los sistemas accesibles desde Internet, como sitios web o infraestructuras en la nube.

Un “pen test” puede consistir en intentar obtener acceso no autorizado al sistema de reservas del hotel, manipular las reservas de los huéspedes o explotar las vulnerabilidades de la red Wi-Fi del hotel para interceptar los datos de los huéspedes.

Definición de Exploración de Vulnerabilidades

La exploración de vulnerabilidades es un proceso que identifica y notifica las vulnerabilidades potenciales de un sistema o red. Se centra en detectar puntos débiles de seguridad, configuraciones erróneas o versiones de software obsoletas.

Tenga en cuenta los siguientes aspectos:

- **Objetivo** - El escaneo de vulnerabilidades tiene como objetivo identificar vulnerabilidades conocidas que potencialmente podrían ser explotadas por un atacante. Proporciona una captura instantánea de la postura de seguridad del sistema en un momento determinado.
- **Enfoque** - Los escáneres de vulnerabilidades automatizan el proceso de exploración de sistemas o redes para descubrir vulnerabilidades comparándolas con una base de datos de vulnerabilidades y debilidades conocidas.
- **Alcance** - La exploración de vulnerabilidades puede realizarse tanto interna como externamente. La exploración de vulnerabilidades interna evalúa la postura de seguridad de los sistemas dentro de la red, mientras que la exploración de vulnerabilidades externa se centra en los sistemas expuestos a Internet, como los servidores web de cara al público.

En el sector de la hostelería, un análisis de vulnerabilidades podría consistir en analizar la red de un hotel en busca de versiones de software obsoletas, sistemas sin parches o cortafuegos mal configurados que podrían proporcionar un punto de entrada a un atacante.

Diferencias

Las pruebas de penetración y la exploración de vulnerabilidades tienen diferencias clave en varias áreas. Se resumen en la siguiente tabla.

Área	Pruebas de Penetración	Exploración de Vulnerabilidades

Actor	Humano (hackers éticos).	Herramientas o escáneres automatizados.
Profundidad	Análisis en profundidad para determinar el impacto de las vulnerabilidades y la cadena potencial de explotación.	Identificación superficial de vulnerabilidades sin un análisis detallado del impacto.
Enfoque	Hace hincapié en los fallos de seguridad y las vulnerabilidades centradas en el ser humano.	Hace hincapié en las vulnerabilidades técnicas y los errores de configuración.
Metodología	Enfoque sistemático y específico para explotar vulnerabilidades, escalar privilegios y obtener acceso no autorizado.	Utiliza firmas y patrones predefinidos para identificar vulnerabilidades.
En tiempo real	Tiene capacidad evolutiva para identificar nuevas vulnerabilidades que pueden no ser detectadas por los escáneres.	Capacidad limitada para identificar vulnerabilidades nuevas o de día cero no incluidas en la base de datos del escáner.
Objetivo	Sistemas, redes y dispositivos de la infraestructura de la organización.	Sistemas, redes, aplicaciones web y dispositivos conectados a la red o expuestos a Internet.

Puntos en común

Aunque las pruebas de penetración y la exploración de vulnerabilidades tienen muchas diferencias, comparten similitudes significativas. Estos puntos en común incluyen:

- **Ayudar a las organizaciones a mejorar su postura de seguridad**. Ambos ayudan a las organizaciones a mejorar su postura general de seguridad mediante la identificación de puntos débiles que podrían ser explotados por los atacantes. Al abordar estos

problemas, las organizaciones mitigan las amenazas potenciales y mejoran sus defensas.

- **Contribuyen a una estrategia global de evaluación de la seguridad**. Mientras que las pruebas de penetración se centran en la explotación activa de vulnerabilidades mediante ataques simulados, la exploración de vulnerabilidades proporciona un enfoque sistemático y automatizado para identificar vulnerabilidades conocidas. Juntos, proporcionan una comprensión más completa del panorama de seguridad de una organización.
- **Cumplimiento de PCI DSS**. Las pruebas de penetración y el escaneo de vulnerabilidades son requisitos explícitos de PCI DSS para las organizaciones que manejan datos de tarjetas de pago. El Requisito 11.2 exige escaneos regulares de vulnerabilidades internas y externas para identificar vulnerabilidades potenciales, y el Requisito 11.2.1 establece que las organizaciones deben realizar escaneos trimestrales de vulnerabilidades externas por un Proveedor de Escaneo Aprobado (ASV). Además, el requisito 11.3 exige que las organizaciones realicen "pen tests" anualmente o después de cambios significativos en la red o las aplicaciones.
- **Exigir evaluaciones periódicas**. Tanto las pruebas de penetración como el escaneo de vulnerabilidades requieren evaluaciones regulares y periódicas para garantizar la seguridad continua. El panorama de las amenazas evoluciona constantemente, con la aparición de nuevas vulnerabilidades y la actualización de los sistemas. Las evaluaciones periódicas ayudan a las organizaciones a anticiparse a los riesgos potenciales.
- **Ayuda en la identificación de vulnerabilidades**. Ambos métodos son eficaces para identificar vulnerabilidades antes de que sean explotadas por agentes malintencionados. Las pruebas de penetración aprovechan diversas técnicas para identificar y explotar vulnerabilidades, mientras que la exploración de vulnerabilidades utiliza herramientas y bases de datos automatizadas para detectar vulnerabilidades conocidas.
- **Proporcionan informes con propuestas de corrección**. En ambos casos se elaboran informes en los que se describen las vulnerabilidades detectadas y se sugieren medidas correctivas. Estos informes proporcionan información sobre las vulnerabilidades específicas descubiertas y ofrecen orientación sobre cómo mitigarlas o eliminarlas.

- **Requieren acciones de seguimiento**. Tanto las pruebas de penetración como la exploración de vulnerabilidades pueden requerir acciones de seguimiento para abordar las vulnerabilidades identificadas. No basta con identificar las vulnerabilidades; las organizaciones deben tomar medidas para remediar y mitigar estos riesgos. Las acciones de seguimiento pueden incluir la aplicación de parches, la actualización de configuraciones, la mejora de los controles de seguridad o la aplicación de salvaguardias adicionales para hacer frente a las vulnerabilidades identificadas.

Aprovechando estos puntos en común, las organizaciones pueden utilizar tanto las pruebas de penetración como la exploración de vulnerabilidades como enfoques complementarios para protegerse contra las amenazas.

Conclusión

Tanto las pruebas de penetración como la exploración de vulnerabilidades son componentes esenciales de una estrategia integral de evaluación de la seguridad.

Mientras que las pruebas de penetración tienen como objetivo imitar ataques del mundo real y explotar vulnerabilidades para evaluar el riesgo y la eficacia de la seguridad, la exploración de vulnerabilidades se centra en identificar debilidades conocidas y configuraciones erróneas.

Ambos métodos desempeñan un papel crucial en la protección proactiva de sistemas y redes, permitiendo a las organizaciones del sector de la hostelería, como los hoteles, identificar y abordar posibles vulnerabilidades antes de que sean explotadas por agentes malintencionados.

Acerca de VENZA

VENZA es un proveedor líder de soluciones de protección de datos de seguridad que permiten al sector hotelero mitigar las vulnerabilidades y garantizar el cumplimiento de las normativas. VENZA presta asistencia a más de 2.000 hoteles en todo el mundo, manteniendo a los huéspedes y sus datos a salvo de infracciones con una visibilidad de 360 grados para una gestión proactiva de los riesgos. Esto permite a los gestores de los establecimientos centrarse en el servicio a los huéspedes y en fomentar la confianza en su marca.

Visite www.VENZAGroup.com para obtener más información.

Contacte con Nosotros

Ventas: sales@venzagroup.com

Atención al cliente: success@venzagroup.com