Universidad Autónoma de Chiapas

Facultad: Contaduría y Administración

Licenciatura: Ingeniería en Desarrollo y Tecnologías de Software

Análisis de Vulnerabilidades

"Actividad 2.1 Herramientas Pasivas"

Alumno: Nango Ponce Manuel de Jesus

Grupo: 7M

Matrícula: A200338

Docente: Luis Gutiérrez Alfaro

Tuxtla Gutiérrez, Chiapas
02/09/2023

NETWORK SECURITY/SEGURIDAD DE RED

La **seguridad de red** es un conjunto de prácticas y tecnologías que se utilizan para proteger la integridad, confidencialidad y disponibilidad de los datos y recursos de una red. Incluye tecnologías de hardware y software, y está orientada a diversas amenazas, como ataques de hackers, virus, malware, phishing, entre otros.

La seguridad de red eficaz administra el acceso a la red y evita que ingresen o se propaguen por la red. Para ello, combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad.

La seguridad de red es importante porque la mayoría de las organizaciones actuales dependen en gran medida de las redes de computadoras para compartir información de manera eficiente y productiva dentro de la red definida. La digitalización ha transformado al mundo. Ha cambiado nuestra manera de vivir, trabajar, aprender y entretenernos. Todas las organizaciones que quieren prestar los servicios que exigen los clientes y los empleados deben proteger su red. La seguridad de red también ayuda a proteger la información confidencial de los ataques. En última instancia, protege su reputación.

TIPOS DE ATAQUES, VULNERABILIDADES Y AMENAZAS

Los **ataques informáticos** son acciones maliciosas que buscan explotar las **vulnerabilidades** de los sistemas informáticos. Las vulnerabilidades son debilidades en sistemas, redes o aplicaciones que pueden ser explotadas por atacantes. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento.

Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas). A continuación se presentan algunos tipos comunes de ataques, vulnerabilidades y amenazas:

- **Malware**: es un término que se usa para describir el software malicioso, que incluye spyware, ransomware, virus y gusanos. El malware infringe las redes mediante una vulnerabilidad, usualmente cuando un usuario hace clic en un enlace peligroso o en un archivo adjunto de correo electrónico que, luego, instala un software riesgoso. Una vez dentro del sistema, el malware puede hacer lo siguiente: bloquear el acceso a los componentes clave de la red (ransomware), instalar malware o software dañino adicional, obtener información furtivamente mediante la transmisión de datos del disco duro (spyware), alterar ciertos componentes y hacer que el equipo sea inoperable.
- **Phishing:** es la práctica de enviar comunicaciones fraudulentas que parecen provenir de fuentes confiables, habitualmente a través del correo electrónico. El objetivo es robar datos sensibles, como información de inicio de sesión y tarjetas de crédito, o instalar malware en la máquina de la víctima.
- **Ataque por denegación de servicio distribuido (DDoS)**: es un ataque que tiene como objetivo inundar un servidor con tráfico para que no pueda responder a las solicitudes legítimas. Los atacantes utilizan una red de dispositivos infectados para enviar tráfico al servidor objetivo.
- **Ingeniería social:** es una técnica utilizada por los atacantes para engañar a los usuarios y obtener información confidencial. Los atacantes pueden hacerse pasar por una persona o entidad confiable para engañar a los usuarios y obtener información confidencial como contraseñas o números de tarjetas de crédito.

CONCEPTOS BÁSICOS

La **tríada CID** (Confidencialidad, Integridad y Disponibilidad) es un modelo diseñado para guiar las políticas de seguridad de la información dentro de una organización. Estos conceptos son fundamentales para la seguridad de la información y se definen de la siguiente manera:

- **Confidencialidad:** es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. La confidencialidad protege la información de accesos no autorizados y usos indebidos. Las medidas de confidencialidad incluyen contraseñas, listas de control de acceso y procedimientos de autenticación.
- **Integridad:** significa que los datos están protegidos de cambios no autorizados para garantizar que son fiables y correctos. La integridad defiende que la información debe mantenerse fiel a como fue concebida en su momento salvo autorización expresa para su modificación.
- **Disponibilidad:** significa que los usuarios autorizados tienen acceso a los sistemas y recursos que necesitan. La disponibilidad es importante porque garantiza que los usuarios puedan acceder a los recursos necesarios cuando los necesiten.
- **Autenticación:** es el proceso mediante el cual se verifica la identidad del usuario o dispositivo que intenta acceder a un sistema o recurso. La autenticación se utiliza para garantizar que solo los usuarios autorizados tengan acceso a los recursos de red.

POLÍTICA DE SEGURIDAD

La **política de seguridad** es un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de una organización. La política de seguridad es un documento indispensable para las organizaciones que deseen cumplir con la norma ISO 27001, la cual ayuda a incrementar la reputación de una empresa, proyecta una imagen de seguridad y confianza, mejora las relaciones con grupos de interés y disminuye los riesgos tecnológicos.

La política general de seguridad es un documento que se emite desde la alta dirección de una empresa, en el cual se definen los parámetros de los directivos para proteger la información. Su función principal es garantizar que los datos que se recolectan sean tratados de forma confidencial e íntegra y se mantengan disponibles. Además, establece el compromiso de mitigar los riesgos que pudieran afectar a la información. Por lo anterior, en dicha política se detallan las medidas que la organización llevará a cabo para todos los activos de información, los cuales hacen referencia a todo lo que es valioso para la empresa, por ejemplo: infraestructura de información; red de comunicación; instalaciones; equipos auxiliares; personas.

Las políticas de seguridad no solo van destinadas a los equipos técnicos e informáticos de una empresa, sino que van dirigidos a todos los puestos de trabajo que sean susceptibles de producir algún error o descuido de seguridad. Cabe destacar que muchos de los problemas de seguridad de las empresas se producen por errores humanos. Por ello, es necesario establecer cuáles son los mecanismos de seguridad que vamos a implantar en nuestra empresa. Estos tendrán que plantearse en tres ámbitos diferentes: prevención, detección y actuación.

CARACTERÍSTICAS DE UNA POLÍTICA DE SEGURIDAD

Las características de una política de seguridad pueden variar según la organización, pero aquí hay algunas características comunes:

- **Objetivos claros:** las políticas de seguridad deben tener objetivos claros y definidos para garantizar que se cumplan los requisitos de seguridad.
- **Alto nivel:** las políticas de seguridad deben ser definidas por la alta dirección y ser coherentes con los objetivos estratégicos de la organización.
- **Comunicación:** las políticas de seguridad deben ser comunicadas a todo el personal para garantizar que todos estén al tanto de las políticas y procedimientos.
- **Actualización:** las políticas de seguridad deben actualizarse regularmente para garantizar que sean efectivas y estén alineadas con los cambios en el entorno empresarial.

- **Controles técnicos y organizativos:** las políticas de seguridad deben incluir controles técnicos y organizativos para garantizar que se cumplan los objetivos de seguridad.
- **Política de uso aceptable:** las políticas de seguridad pueden incluir una política de uso aceptable que educa a los empleados sobre la seguridad informática y define lo que está permitido y lo que no está permitido en términos del uso del equipo informático.

¿POR QUÉ SE REQUIERE ATENCIÓN ESPECIAL A LA SEGURIDAD WEB?

La **seguridad web** es importante porque los sitios web desprotegidos están expuestos a sufrir ataques cibernéticos, entre otros. Los sitios web son muy propensos a ser atacados por los llamados 'piratas informáticos'. Los servidores de internet también tienden a recibir ciberataques, sin olvidar los riesgos creados por los propios empleados que desconocen los temas de ciberseguridad o usan inadecuadamente los recursos.

La seguridad web consiste en cada acción o herramienta adoptada para evitar que las informaciones sean expuestas o propensas a ataques por parte de cibercriminales. Esas medidas también sirven para proteger a los usuarios, como los clientes de ecommerce y los lectores de blogs, e incluso al host. La seguridad web es un proceso continuo y una parte esencial de administrar un sitio web. La ciberseguridad es importante porque garantiza que los usuarios puedan acceder a los recursos necesarios cuando los necesiten.

La seguridad web requiere vigilancia en todos los aspectos del diseño y uso de un sitio web. La seguridad web eficaz requiere de esfuerzos de diseño a lo largo de la totalidad del sitio web: en tu aplicación web, en la configuración del servidor web, en tus políticas para crear y renovar contraseñas, y en el código del lado cliente.

LA SEGURIDAD WEB ES IMPORTANTE PORQUE:

- Previene ataques y protege sitios web del acceso, uso, modificación, destrucción o interrupción no autorizados.
- Afecta directamente al posicionamiento SEO de la página web.
- Evita la pérdida de visibilidad en buscadores.
- Protege la información personal de los usuarios.
- Mejora el SEO de la página web.
- Aumenta la confiabilidad y seguridad de la página web.
- Evita la disminución de las conversiones.
- Evita la disminución del tráfico.
- Evita dañar la reputación online.
- Evita la disminución de los ingresos y las ventas.

¿QUÉ SON LAS VULNERABILIDADES EN SERVICIO DNS A TRAVÉS DE HERRAMIENTAS WEB?

El **Sistema de Nombres de Dominio (DNS)** es un sistema que se utiliza para traducir nombres de dominio legibles por humanos en direcciones IP que las computadoras pueden entender. El DNS es una parte integral de la mayoría de las solicitudes de Internet y, por lo tanto, es un objetivo principal de los ataques.

Las vulnerabilidades del DNS pueden ser explotadas por los ciberdelincuentes para realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento. Algunas formas en que el DNS puede convertirse en una vulnerabilidad para su empresa son:

1. Las cachés DNS pueden estar "envenenadas".

2. El DNS se puede utilizar para realizar ataques de "usurpación" de dominio como pueden ser "typo cons" y "domain squatting".

3. El DNS se puede usar en ataques de phishing.

4. El DNS se puede aprovechar para ataques de malware Command and Control (C2).

5. El DNS no discrimina.

Las herramientas web pueden ser utilizadas para identificar vulnerabilidades en el servicio DNS. Por ejemplo, los escáneres de vulnerabilidades web pueden detectar problemas como la suplantación de identidad, la amplificación, DoS (denegación de servicio) o la interceptación de información personal privada.

BÚSQUEDAS DE VULNERABILIDADES A TRAVÉS DE GOOGLE

Las **búsquedas de vulnerabilidad a través de Google** son una técnica de hacking que se utiliza para buscar servidores desactualizados y vulnerables, así como para realizar búsquedas de usuario y contraseña de sitios webs, servidores y bases de datos. Los hackers utilizan la búsqueda avanzada de Google para encontrar agujeros de seguridad en la configuración y el código de un sitio web.

Google también tiene un programa de recompensa llamado Vulnerability Reward Program (VRP), que invita a investigadores a reportar vulnerabilidades y bugs que tengan el potencial de afectar su ecosistema de proyectos Open Source.

Para realizar búsquedas en Google de manera más precisa, se pueden utilizar una serie de operadores. Estos operadores se utilizan para filtrar los resultados y encontrar resultados relevantes para las búsquedas de forma más rápida y precisa. Algunos ejemplos son:

- **site**: Buscar resultados dentro de un sitio específico.
- **related**: Buscar sitios relacionados.
- **cache**: Buscar la versión del sitio en caché.
- **intitle**: Buscar en el título de la página.
- **inurl**: Buscar una palabra contenida en una URL.

- **filetype**: Buscar por tipos de archivo específicos.
- **intext**: Buscar en el texto del sitio web solamente.
- **""**: Buscar palabra por coincidencia exacta.
- **+**: Buscar más de una palabra clave.
- **-**: Excluir palabras de la búsqueda.
- **OR**: Combinar dos palabras.
- ***: Operador de comodín.

HERRAMIENTA MALTEGO

Maltego es un software utilizado para la Inteligencia de fuentes abiertas y forense, desarrollado por Paterva. Maltego se enfoca en proporcionar una biblioteca de transformaciones para el descubrimiento de datos de fuentes abiertas y visualizar esa información en un formato gráfico, adecuado para análisis de enlaces y minería de datos. Maltego permite crear entidades personalizadas, lo que le permite representar cualquier tipo de información además de los tipos básicos de entidades que forman parte del software. El enfoque básico de la aplicación es analizar las relaciones del mundo real (red social y red de computadoras entre personas, grupos, páginas web, dominios, redes, infraestructura de Internet y afiliaciones con servicios de línea nodos de redes informáticas como Twitter y Facebook. Entre sus fuentes de datos se encuentran el sistema de nombres de dominio, entre otros. Es usado para la seguridad de la información y detectives privados.

AMENAZAS EN SEGURIDAD DE LA INFORMACIÓN

Las **amenazas en seguridad de la información** son cualquier evento o acción que compromete la confidencialidad, integridad o disponibilidad de la información. Las amenazas pueden ser internas o externas y pueden ser causadas por personas, procesos o tecnología. Algunos ejemplos de amenazas en seguridad de la información incluyen:

Malware: software malicioso que se utiliza para dañar, interrumpir o tomar el control de un sistema informático.

Phishing: un tipo de ataque de ingeniería social que se utiliza para engañar a los usuarios para que revelen información confidencial, como contraseñas y números de tarjetas de crédito.

Ataques de denegación de servicio (DoS): ataques que tienen como objetivo inundar un servidor con tráfico para que no pueda responder a las solicitudes legítimas.

Ataques de fuerza bruta: ataques que intentan adivinar contraseñas mediante la prueba de todas las combinaciones posibles.

Ataques de inyección: ataques que aprovechan las vulnerabilidades en el software para insertar código malicioso en una aplicación web.

Ataques de suplantación: ataques que se utilizan para hacerse pasar por otra persona o entidad con el fin de obtener información confidencial.

Robo de identidad: el robo de información personal, como nombres, direcciones y números de seguridad social, con el fin de cometer fraude.

CONCLUSIÓN:

En este chat hemos hablado sobre seguridad de la información, la importancia de la seguridad web, las amenazas en seguridad de la información, la política de seguridad, el sistema de nombres de dominio (DNS), las búsquedas de vulnerabilidades a través de Google y la herramienta Maltego. La seguridad de la información es importante para proteger los datos y recursos de una organización. Las amenazas en seguridad de la información pueden ser internas o externas y pueden ser causadas por personas, procesos o tecnología. La política de seguridad es un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de una organización. El DNS es un sistema que se utiliza para traducir nombres de dominio legibles por humanos en direcciones IP que las computadoras pueden entender. Las búsquedas de vulnerabilidad a través de Google son una técnica de hacking que se utiliza para buscar servidores desactualizados y vulnerables, así como para realizar búsquedas de usuario y contraseña de sitios webs, servidores y bases de datos. Maltego es un software utilizado para la Inteligencia de fuentes abiertas y forense.

FUENTES DE INFORMACIÓN

1. Wikipedia. (2022). Vulnerabilidad (seguridad informática). Recuperado de https://es.wikipedia.org/wiki/Vulnerabilidad_(seguridad_inform%C3%A1tica)

2. Sánchez, J. (2019). Análisis de vulnerabilidades: qué es, tipos y herramientas. Recuperado de URL

3. NortonLifeLock. (2022). Common types of cyberattacks. Recuperado de https://www.nortonlifelock.com/cybersecurity/what-is-cybersecurity/common-types-of-cyberattacks

4. Kaspersky. (2022). What is cybersecurity? Recuperado de https://www.kaspersky.com/resource-center/definitions/what-is-cybersecurity

5. Palo Alto Networks. (2022). What is cybersecurity? Recuperado de https://www.paloaltonetworks.com/cyberpedia/what-is-cybersecurity

6. Sánchez, J. (2019). Análisis de vulnerabilidades: qué es, tipos y herramientas.

7. Kaspersky. (2022). What is social engineering? Recuperado de https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering