UNIVERSIDAD AUTÓNOMA
DEL ESTADO DE MÉXICO

Facultad de Ingeniería

MATERIA: Seguridad de la información

ANÁLISIS DE AMENAZAS, VULNERABILIDADES Y ATAQUES A LA SEGURIDAD DE LA INFORMACIÓN

Docente: Alejandro Hernández Arriaga

Alumno:
Ulises Becerril Valdés

Grupo: 01

Ciclo escolar 2023B

23 de febrero de 2023

Sumario

Vulnerabilidades

Las vulnerabilidades en la seguridad de la información se refieren a debilidades o huecos en los sistemas de información que pueden ser explotados por amenazas para ganar acceso no autorizado, causar daño o realizar acciones maliciosas. Estas vulnerabilidades pueden existir en diferentes componentes del sistema de información, como el hardware, el software, la red y los procesos o prácticas de los usuarios. La identificación y mitigación de estas vulnerabilidades es fundamental para proteger la integridad, confidencialidad y disponibilidad de la información.

1. **Vulnerabilidades de software**: Errores de programación, fallas de diseño o configuraciones inseguras en el software que pueden ser explotadas. Ejemplos comunes incluyen inyección SQL, cross-site scripting (XSS) y desbordamiento de búfer.
2. **Vulnerabilidades de hardware**: Defectos físicos o fallos de diseño en los componentes del hardware que pueden ser explotados para comprometer la seguridad del sistema. Aunque menos comunes que las vulnerabilidades de software, pueden ser muy críticas (por ejemplo, vulnerabilidades en chips o procesadores).
3. **Vulnerabilidades de red**: Debilidades en los protocolos de red, configuraciones inseguras o malas prácticas de gestión de red que permiten ataques como el hombre en el medio (MitM), denegación de servicio (DoS) o ataques distribuidos de denegación de servicio (DDoS).
4. **Vulnerabilidades humanas**: Errores o acciones negligentes de los usuarios, como el uso de contraseñas débiles, el phishing o la ingeniería social, que pueden ser explotadas para acceder a sistemas o información de manera no autorizada.
5. **Vulnerabilidades de configuración**: Configuraciones inadecuadas de sistemas, aplicaciones o dispositivos que dejan abiertas brechas de seguridad. Esto incluye permisos excesivos, servicios innecesarios activos o el uso de configuraciones predeterminadas inseguras.

Para mitigar estas vulnerabilidades, las organizaciones adoptan una variedad de estrategias y herramientas, incluyendo la realización de auditorías de seguridad y evaluaciones de vulnerabilidad, la aplicación de parches y actualizaciones de seguridad, el fortalecimiento de las políticas de seguridad y la formación continua de los usuarios en buenas prácticas de seguridad. La gestión de vulnerabilidades es un proceso continuo que requiere vigilancia y actualización constantes para protegerse contra las amenazas emergentes.

Amenazas

Las amenazas en seguridad de la información son numerosas y constantemente evolucionan.

1. **Ataques de malware**: Software malicioso diseñado para infiltrarse en sistemas y causar daño, robar información o interrumpir operaciones. Ejemplos incluyen virus, gusanos, troyanos y ransomware.
2. **Phishing**: Intentos de engañar a los usuarios para que revelen información confidencial, como contraseñas o información financiera, a menudo a través de correos electrónicos, mensajes de texto o llamadas telefónicas fraudulentas.
3. **Ataques de ingeniería social**: Manipulación psicológica de personas para obtener información confidencial o acceso a sistemas. Puede incluir pretexting, donde un atacante inventa una historia para obtener información, o spear phishing, que es phishing dirigido a individuos específicos.
4. **Vulnerabilidades de software y sistemas**: Agujeros de seguridad en programas, aplicaciones o sistemas operativos que pueden ser explotados por atacantes para acceder ilegalmente a sistemas o datos.
5. **Fugas de datos**: Divulgación no autorizada de información sensible o confidencial, ya sea debido a una violación de seguridad, errores de configuración o acciones maliciosas.
6. **Ataques de denegación de servicio (DDoS)**: Intentos de sobrecargar un sistema, red o servicio con tráfico falso o inundaciones de solicitudes legítimas, lo que resulta en una interrupción del servicio para usuarios legítimos.
7. **Ataques de fuerza bruta**: Intentos repetidos y automáticos de adivinar contraseñas o claves de cifrado mediante la generación de combinaciones posibles hasta que se encuentre la correcta.
8. **Fugas internas**: Acciones maliciosas o negligentes por parte de empleados, contratistas o socios comerciales que resultan en la divulgación no autorizada de información.
9. **Ataques a la cadena de suministro**: Ataques dirigidos a proveedores de servicios o fabricantes de software para comprometer indirectamente los sistemas de sus clientes.
10. **Amenazas emergentes**: Con el avance de la tecnología, surgen nuevas amenazas como el ransomware-as-a-service, donde los ciberdelincuentes alquilan acceso a plataformas de ransomware, o ataques a dispositivos IoT que pueden comprometer la seguridad de redes domésticas o empresariales.

Ataques

Se consiera a un ataquecomo cualquier acción que comprometa la seguridad de la información dentro de una organización.

Deacuerdo a los estándares internacionales, podemos clasificar a los ataques en dos grandes categorías:

Ataques pasivos

Este tipo de ataques se dan en forma de escucha o de observacines no autorizadas de las transmisiones. El objetivo de este ataque es obtener información que se esté transmitiendo.

Dentro de este tipo de ataques encontramos la obtención de contenido de mensajes, en los que un tercer sujeto, conocido com el oponente, ajeno a la comunicación entre dos o más equipos de computo, tiene acceso a la conversación que existe entre estos equipos.

Otro tipo de ataque pasivo es el análisis de tráfico, en este tipo de ataque existe un enmascarado de los datos que están siendo intercambiados, sin embargo, el oponente observa el patrón del tráfico de mensajes, de esta manera puede tener acceso a la información que se está intercambiando entre los equipos de cómputo.

Ataques activos

Los ataques activos implican que la información que está siendo intercambiada entre los equipos de cómputo sea modificada de alguna manera

Dentro de los ataques activos más comunes encontramos la repetición que implica la captura pasiva de datos y su retrasmisión sin producir un efecto no autorizado, la modificación de mensajes que implica alterar una parte del mensaje original, retrasar o reordenar los mensajes.

La interrupción del servicio impide el uso o gestión normal del uso de las utilidades de comunicación.

Servicios de seguridad

Un servicio de seguridad se define como un servcio proporcionado por una capa de protocolo de sistemas abiertos de comunicación, que garantiza la seguridad adecuada de los sistemas o de las transferencias de los datos.

Se considera como un servicio de procesamiento o comunicación proporcionado por un sistema para dar un tipo de protección especial a los resursos del sistema.

Estos servicios están clasificados en 5 categorías y 14 servicios específicos:

Autentificación

Seguridad en que la entidad con la que se comunica es quien dice ser.

Autentificación de entidades origen/destino

Autentificación del origen de los datos

Control de acceso

Prevención del uso no autorizado de una fuente.

Controla quien puede tener acceso a una fuente de información, a un recurso en particular, en que condiciones y que efecto puede producir en dichos recursos.

Confidencialidad de los datos

Evita revelaciones no autorizadas de los datos.

Confidencialidad de conexión

Confidencialidad no orientada a la conexión

Confidencialidad de campos seleccionados

Confidencialidad del flujo de tráfico

Integridad de los datos

Asegura que los datos son recibidos extactamente como los envió la entidad autorizada.

Integridad de la conexión con recuperación

Integridad de la conexión sin recuperación

Integridad de la conexión de campos seleccionados

Integridad no orientada a la conexión

Integridad no orientada a la conexión de campos selecionados

No repudio

Evita la interrupción por parte de cualquiera de las partes implicadas en la comunicación.

No repudio, origen

No repudio, destino

Mecanismos de seguridad

Un mecanismo de seguridad es una medida de seguridad diseñada para detectar un ataque a la seguridad, prevenirlo o restablecerse de él.

Existen mecanismos de seguridad que existen para poder proteger una capa en específico y existen mecanismos de seguridad para proteger la información de manera general.

Mecanismos específicos de seguridad

Se incorporan en la capa de protocolo adecuada para proporcionar servicios de seguridad.

Cifrado

Firma digital

Control de acceso

Integridad de los datos

Intercambio de autentificación

Relleno del tráfico

Control de enrutamiento

Notarización

Mecanismos generales de seguridad

No están incorporados a ninguna capa de protocolo en específico.

Funcionalidad fiable

Etiquetas de seguridad

Detección de acciones

Informe para la auditoría de seguridad

Recuperación de la seguridad