HACKING ÉTICO

PRÁCTICA UD1
FUNDAMENTOS DE HE

PRÁCTICA UD1 – FUNDAMENTOS DE HE

Autor: Pedro Manuel García Álvarez

Fecha: 07/02/2024

Índice

PRÁCTICA UD1 – FUNDAMENTOS DE HE

1.- Define cada uno de los principios de seguridad e ilustra la importancia de cada uno con un ejemplo real.

1.1.- Confidencialidad

La confidencialidad asegura que la información sensible esté protegida contra el acceso no autorizado. Solo las personas autorizadas pueden acceder a la información confidencial.

La confidencialidad es crucial para proteger datos sensibles, como información personal, financiera o de negocios, de ser divulgados a personas no autorizadas.

En una empresa de servicios financieros, los registros de los clientes, incluidos los números de cuenta y la información financiera, están protegidos mediante sistemas de autenticación y cifrado para garantizar que solo el personal autorizado tenga acceso a ellos.

1.2.- Integridad

La integridad asegura que la información no se modifique ni altere de manera no autorizada. La información debe permanecer precisa y completa durante todo su ciclo de vida.

La integridad garantiza que los datos no se manipulen de forma no deseada, lo que podría llevar a decisiones erróneas o pérdida de confianza en la información.

En un sistema de gestión de bases de datos, se implementan controles de integridad para garantizar que los datos almacenados no se corrompan. Se pueden utilizar técnicas como la firma digital o el control de versiones para garantizar que los datos se mantengan íntegros.

1.3.- Disponibilidad

La disponibilidad garantiza que los sistemas y recursos de información estén disponibles y accesibles cuando sea necesario por parte de los usuarios autorizados.

La disponibilidad es esencial para garantizar que los usuarios puedan acceder a la información y los servicios de manera oportuna y sin interrupciones, lo que asegura la continuidad del negocio.

Un proveedor de servicios en la nube utiliza redundancia de servidores y sistemas de copia de seguridad para garantizar que los datos estén disponibles incluso en caso de fallos de hardware o desastres naturales.

1.4.- Autenticidad

La autenticidad verifica la identidad de los usuarios y la autenticidad de los datos. Garantiza que los usuarios sean quienes dicen ser y que los datos no sean falsificados.

La autenticidad ayuda a prevenir el acceso no autorizado y el uso de datos falsificados, lo que protege la integridad y la confidencialidad de la información.

En un sistema de autenticación de dos factores, los usuarios deben proporcionar una combinación de contraseña y un código de verificación único enviado a su dispositivo móvil para acceder a sus cuentas en línea. Esto garantiza que solo los usuarios legítimos puedan acceder a los sistemas.

Estos son solo algunos de los principios básicos de seguridad de la información, y cada uno juega un papel crucial en la protección de los datos y los sistemas contra amenazas y riesgos.

2.- Elabora una comparativa entre los siguientes conceptos: activos, vulnerabilidades, amenazas, ataques y riesgos. Debe quedar claro cómo se relacionan entre sí y sus diferencias. Cita las fuentes que hayas utilizado para encontrar el significado de dichos términos.

2.1.- Activos

Los activos son recursos valiosos de una organización, que pueden ser tangibles (como hardware, software, datos físicos) o intangibles (como datos digitales, propiedad intelectual).

Los activos son el objeto de protección en un entorno de seguridad de la información. Las organizaciones identifican y valoran sus activos para determinar su importancia y aplicar medidas de seguridad adecuadas.

Para la definición de activos, se ha consultado https://peritoinformatico.es/que-es-un-activo-informatico-y-como-se-valoran/.

2.2.- Vulnerabilidades:

Las vulnerabilidades son debilidades o fallos en los activos de una organización que podrían ser explotados por amenazas para comprometer la seguridad.

Las vulnerabilidades representan el punto débil de los activos y pueden ser explotadas por amenazas mediante ataques para causar daño o pérdida.

La definición de vulnerabilidades se ha obtenido del https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

2.3.- Amenazas:

Las amenazas son cualquier evento o acción que pueda causar daño o poner en peligro los activos de una organización. Pueden ser internas o externas, naturales o provocadas.

Las amenazas representan el riesgo potencial para los activos de una organización al explotar sus vulnerabilidades mediante ataques.

Se ha consultado web https://es.linkedin.com/pulse/gesti%C3%B3n-de-riesgos-terminolog%C3%ADa-pedro.

2.4.- Ataques

Los ataques son acciones deliberadas o intencionadas para explotar las vulnerabilidades de los activos y comprometer su seguridad. Pueden ser llevados a cabo por personas, malware o desastres naturales.

Los ataques son la forma en que las amenazas explotan las vulnerabilidades para comprometer los activos de una organización.

La definición de ataques se ha obtenido web https://www.linkedin.com/pulse/ciberseguridad-ataques-conceptos-y-t%C3%A9cnicas-adrian-arguello

2.5.- Riesgos

Los riesgos son la posibilidad de pérdida, daño o interrupción de los activos de una organización debido a la explotación de vulnerabilidades por parte de amenazas.

Los riesgos son el resultado de la combinación de la probabilidad de que ocurra un ataque y el impacto que tendría en los activos.

Se ha consultado la web https://es.linkedin.com/pulse/gesti%C3%B3n-de-riesgos-terminolog%C3%ADa-pedro.

En resumen, los activos son los recursos valiosos de una organización, las vulnerabilidades son sus puntos débiles, las amenazas representan el riesgo potencial, los ataques son las acciones para explotar las vulnerabilidades y los riesgos son la posibilidad de pérdida debido a los ataques.

3.- Indica los repositorios o bases de vulnerabilidades que conozcas.

3.1.- Common Vulnerabilities and Exposures (CVE)

Es un diccionario público de información de ciberseguridad que proporciona identificadores únicos para todas las vulnerabilidades conocidas. Las organizaciones y proveedores de seguridad suelen referenciar los CVE en sus informes y productos. https://cve.mitre.org/

3.2.- National Vulnerability Database (NVD)

Mantenido por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., el NVD es una base de datos que ofrece información detallada sobre vulnerabilidades de software, incluyendo descripciones, puntuaciones de gravedad y referencias CVE. https://nvd.nist.gov/

3.3.- Exploit Database (Exploit-DB)

Es un repositorio de exploits y técnicas de penetración que recopila exploits, shellcodes y scripts utilizados por investigadores de seguridad y profesionales de la ciberseguridad para probar la seguridad de sistemas y aplicaciones. https://www.exploit-db.com/

3.4.- Vulnerability Notes Database (VulnDB)

Mantenido por Risk Based Security, VulnDB es una base de datos de vulnerabilidades que ofrece detalles sobre vulnerabilidades publicadas y no publicadas, incluyendo información de parches, referencias CVE y detalles de impacto. https://vuldb.com/

3.5.- Open Sourced Vulnerability Database (OSVDB)

Aunque ya no está activamente mantenido, OSVDB fue un proyecto que recopilaba y catalogaba información sobre vulnerabilidades de software de código abierto y proporcionaba acceso a una amplia gama de datos relacionados con la seguridad. https://osv.dev/

4.- ¿Existe algún sistema para evaluar la gravedad de una vulnerabilidad?

Sí, existen varios sistemas para evaluar la gravedad de una vulnerabilidad. Uno de los sistemas más utilizados es el Sistema de Puntuación de Vulnerabilidades

Comunes (CVSS, por sus siglas en inglés), desarrollado por el Foro de Proveedores de Seguridad (Forum of Incident Response and Security Teams - FIRST).

El CVSS proporciona una puntuación numérica que representa la gravedad de una vulnerabilidad en función de diferentes métricas, como el impacto de la vulnerabilidad en la confidencialidad, integridad y disponibilidad de los datos, así como la complejidad de explotación y los privilegios necesarios para llevar a cabo el ataque. La puntuación CVSS ayuda a las organizaciones a priorizar y gestionar eficazmente las vulnerabilidades en sus sistemas.

El CVSS asigna una puntuación entre 0.0 y 10.0 a una vulnerabilidad, donde 10.0 representa el impacto más grave. Además, el CVSS proporciona vectores de puntuación que describen las características específicas de la vulnerabilidad para ayudar a comprender mejor su impacto y contexto.

Otros sistemas de puntuación de vulnerabilidades incluyen el Sistema de Puntuación de Vulnerabilidades Exploitability (EVS), el Sistema de Puntuación de Riesgo de Vulnerabilidad (VRS), entre otros. Sin embargo, el CVSS es el más ampliamente utilizado y reconocido en la comunidad de seguridad informática.

5.- Enumera los tipos de vulnerabilidades y de ataques que existen (no es necesario que los definas).

Tipos de Vulnerabilidades:

1.- Inyección de código (SQL Injection, XSS)

2.- Cross-Site Scripting (XSS)

3.- Secuencias de escape (Escape Sequences)

4.- Ejecución remota de código (Remote Code Execution)

5.- Desbordamiento de búfer (Buffer Overflow)

6.- Inclusión de archivos (File Inclusion)

7.- Ejecución de comandos (Command Execution)

8.- Fugas de información (Information Leakage)

9.- Inyección de código HTML (HTML Injection)

10.- Falsificación de solicitudes entre sitios (Cross-Site Request Forgery - CSRF)

11.- Desbordamiento de enteros (Integer Overflow)

12.- Fallos de autenticación y gestión de sesiones

13.- Uso de componentes con vulnerabilidades conocidas

14.- Vulnerabilidades de seguridad en la configuración

Tipos de Ataques:

1.- Denegación de servicio (DoS)

2.- Ataques de fuerza bruta

3.- Ataques de diccionario

4.- Ataques de intermediarios (Man-in-the-Middle - MitM)

5.- Ataques de suplantación de identidad (Spoofing)

6.- Ataques de inundación (Flood Attacks)

7.- Ataques de envenenamiento de DNS (DNS Spoofing)

8.- Ataques de phishing

9.- Ataques de ransomware

10.- Ataques de sniffing de red

11.- Ataques de inyección de código

12.- Ataques de ingeniería social

13.- Ataques de phishing de ingeniería social

14.- Ataques de explotación de vulnerabilidades conocidas

6.- ¿Qué es un vector de ataque? Enumera los principales vectores.

Un vector de ataque es un camino o método utilizado por un atacante para explotar una vulnerabilidad en un sistema y lograr su objetivo malicioso. Los vectores de ataque pueden variar dependiendo del tipo de vulnerabilidad y del sistema objetivo. Aquí tienes una lista de algunos de los principales vectores de ataque:

1.- Inyección de código (por ejemplo, SQL Injection, XSS)

2.- Ingeniería social

3.- Explotación de vulnerabilidades de software (por ejemplo, exploits)

4.- Ataques de fuerza bruta

5.- Ataques de phishing

6.- Ataques de suplantación de identidad (Spoofing)

7.- Ataques de denegación de servicio (DoS)

8.- Ataques de intermediarios (Man-in-the-Middle - MitM)

9.- Ataques de envenenamiento de DNS (DNS Spoofing)

10.- Ataques de sniffing de red

7.- ¿Cuál es la finalidad de la gestión de riesgos de ciberseguridad? Enumera las fases principales.

La finalidad de la gestión de riesgos de ciberseguridad es identificar, evaluar y mitigar los riesgos asociados con las amenazas cibernéticas que pueden afectar a una organización. Esto implica proteger los activos de información y sistemas de información contra posibles ataques, asegurando la continuidad del negocio y la integridad de los datos. Las fases principales de la gestión de riesgos de ciberseguridad son:

7.1.- Identificación de activos

Esta fase consiste en identificar y clasificar los activos de información y sistemas de información que son críticos para la organización.

7.2.- Evaluación de riesgos

En esta fase se evalúan los riesgos identificados, considerando la probabilidad de ocurrencia y el impacto potencial en caso de que se materialicen. Se utilizan diferentes técnicas, como análisis cualitativos y cuantitativos, para evaluar los riesgos.

7.3.- Mitigación de riesgos

Una vez que los riesgos han sido evaluados, se desarrollan estrategias y medidas para mitigarlos. Esto puede incluir la implementación de controles de seguridad, la aplicación de parches de seguridad, la adopción de políticas y procedimientos, entre otras medidas.

7.4.- Monitoreo y revisión

La gestión de riesgos de ciberseguridad es un proceso continuo que requiere monitoreo constante y revisión periódica. Se deben realizar auditorías de seguridad, pruebas de penetración y análisis de vulnerabilidades de forma regular para asegurar que los controles de seguridad sean efectivos y estén actualizados.

Estas fases ayudan a las organizaciones a identificar y abordar proactivamente los riesgos de ciberseguridad, protegiendo así sus activos y garantizando la continuidad del negocio.

Índice Alfabético

H

I

L

M

N

O

P

R

S

T

U

V