Universidad Autonoma de Chiapas

Facultad de contaduría y administración | Campus 1

Alumno: Diego González Carpio

Matricula: A200240

Actividad: 1.3 Investigación de los siguientes conceptos está en fecha de entrega

Materia:

-Optativa 2- Análisis de Vulnerabilidades

Profesor:

-Gutiérrez Alfaro Luis

En Tuxtla Gutiérrez Chiapas

1.- ¿Qué es vulnerabilidad?

Una vulnerabilidad de seguridad es una debilidad en un sistema que puede ser explotada para violar su política de seguridad. Incluye fallos en diseño, implementación, operación o gestión que pueden ser aprovechados maliciosamente. La seguridad comienza identificando estas vulnerabilidades, que son el punto de partida para proteger sistemas de información, que abarcan desde dispositivos personales hasta infraestructuras de comunicación y usuarios.

2.- ¿Qué es seguridad?

La seguridad informática, también conocida como ciberseguridad, se enfoca en la protección de la información y su procesamiento para prevenir la manipulación por parte de ciberdelincuentes o accesos no autorizados. Cubre áreas como la confidencialidad, integridad, disponibilidad y autenticación de la información y los sistemas. Es esencial para proteger a usuarios y equipos informáticos de daños y amenazas externas. La creciente digitalización y el auge del teletrabajo han incrementado la importancia de la ciberseguridad en el ámbito empresarial.

3.- ¿Escribe los pilares de la seguridad? (confidencialidad, integridad, disponibilidad, autenticidad.)

Los pilares de la seguridad informática, fundamentales para proteger la información y los sistemas, incluyen:

- Confidencialidad: Asegura que solo las personas autorizadas pueden acceder a la información.

- Integridad: Garantiza que la información es precisa y completa, y solo puede ser modificada por quienes tienen el derecho de hacerlo.

- Disponibilidad: Asegura que la información y los sistemas están accesibles para los usuarios autorizados cuando lo necesiten.

- Autenticidad: Verifica que la información y las transacciones son genuinas, confirmando la identidad de los usuarios y la validez de la información.

4.- ¿La seguridad en informática intenta proteger cuatro elementos cuáles son?

La seguridad informática se centra en proteger cuatro elementos clave: datos, hardware, software y usuarios. Estos componentes son fundamentales para el funcionamiento seguro de cualquier sistema informático. Los datos representan la información almacenada y procesada por los sistemas. El hardware y el software forman la infraestructura tecnológica que permite el almacenamiento, procesamiento y transmisión de datos. Los usuarios, tanto individuos como

organizaciones, interactúan con estos sistemas y son tanto beneficiarios de la seguridad como potenciales vectores de riesgo.

5.- ¿Escribe algunos ataques sobre los datos?

Algunos ataques comunes sobre los datos incluyen inyección SQL, donde se inserta código malicioso en bases de datos a través de formularios web; phishing, engañando a usuarios para obtener información confidencial; ransomware, cifrando datos y exigiendo rescate por su liberación; y ataques de Man-in-the-Middle (MitM), interceptando comunicaciones entre dos partes para robar o manipular la información transmitida. Estos ataques buscan explotar vulnerabilidades en sistemas y redes para acceder, alterar, robar o destruir datos.

6.- ¿De qué nos protegemos?

Nos protegemos de una amplia gama de amenazas informáticas, que incluyen ataques cibernéticos como el malware, phishing, y ransomware; vulnerabilidades en software y hardware; errores humanos que pueden comprometer la seguridad de los datos; y desastres naturales que pueden dañar la infraestructura física. La seguridad informática busca mitigar estos riesgos para proteger la confidencialidad, integridad y disponibilidad de la información y los sistemas.

7.- ¿Menciona algunas amenazas que se concrete por medio de una vulnerabilidad?

Algunas amenazas que pueden concretarse por medio de una vulnerabilidad incluyen:

- Ataques de inyección, como SQL Injection, que explotan vulnerabilidades en el manejo de entradas de datos para ejecutar comandos no autorizados.

- Ataques de ejecución de código remoto, permitiendo a un atacante ejecutar código malicioso en un sistema objetivo.

- Cross-Site Scripting (XSS), que inserta scripts maliciosos en páginas web vistas por otros usuarios.

- Desbordamiento de búfer, que ocurre cuando un programa escribe más datos en un búfer de lo que este puede almacenar.

8.- ¿Menciona los tipos de vulnerabilidades?

Los tipos de vulnerabilidades en sistemas informáticos incluyen:

1. Vulnerabilidades de software: Errores de programación que pueden ser explotados para realizar ataques.

2. Vulnerabilidades de hardware: Defectos físicos o diseño inseguro de componentes electrónicos.

3. Vulnerabilidades de configuración: Configuraciones incorrectas o inseguras en sistemas y aplicaciones.

4. Vulnerabilidades de seguridad de red: Debilidades en los protocolos de red o la infraestructura que permiten accesos no autorizados o interceptaciones.

5. Vulnerabilidades humanas: Errores humanos, como el uso de contraseñas débiles o caer en engaños de phishing.

9.- ¿Por qué aumentan las amenazas?

Las amenazas aumentan debido a varios factores: la creciente digitalización de procesos y servicios, la mayor conectividad e interconexión de dispositivos a través de Internet, la sofisticación y la innovación constante en las técnicas de ataque por parte de los ciberdelincuentes, y la valiosa información almacenada en sistemas digitales que atrae a actores maliciosos. Además, la rápida evolución tecnológica a menudo supera las medidas de seguridad implementadas, dejando vulnerabilidades no detectadas o sin parchear.

10.- ¿Menciona tres protecciones más usadas?

Tres de las protecciones más utilizadas en seguridad informática son:

1. Firewalls: Controlan el tráfico entrante y saliente de una red basándose en un conjunto de reglas de seguridad, ayudando a bloquear accesos no autorizados.

2. Software Antivirus: Detecta, previene y elimina software malicioso como virus, gusanos y troyanos de computadoras y redes.

3. Autenticación Multifactor (MFA): Aumenta la seguridad al requerir dos o más métodos de verificación de la identidad del usuario antes de otorgar acceso a recursos y servicios.

11.- ¿Que es amenaza?

Una amenaza en el contexto de la seguridad informática es cualquier circunstancia, capacidad, acción o evento potencial que pueda causar daño al sistema informático, la red o los datos. Las amenazas pueden ser intencionadas, como los ataques perpetrados por ciberdelincuentes, o no intencionadas, como los

errores de software o fallas de hardware, y pueden afectar la confidencialidad, integridad o disponibilidad de la información.

12.- ¿Factores del riesgo de desastres desde el enfoque holístico?

Los factores del riesgo de desastres desde un enfoque holístico incluyen la vulnerabilidad (la susceptibilidad a ser dañado), la exposición (los elementos presentes en áreas propensas a desastres), los peligros (eventos que pueden causar daño) y la capacidad de respuesta y adaptación de las comunidades y sistemas afectados. Este enfoque considera la interacción entre estos elementos y cómo contribuyen al riesgo de desastres, buscando estrategias integrales que aborden no solo la emergencia inmediata sino también la reducción de la vulnerabilidad y el aumento de la resiliencia a largo plazo.

13.- ¿Que es la ingeniería social?

La ingeniería social es una técnica de manipulación psicológica utilizada para obtener información confidencial, acceso no autorizado o realizar fraudes, engañando a las personas para que rompan los procedimientos de seguridad normales. Se basa en la explotación de la confianza humana, más que en fallos técnicos o vulnerabilidades de software, para engañar a los usuarios y hacer que divulguen datos sensibles, como contraseñas o información bancaria.

14.- ¿Que son los virus informáticos?

Los virus informáticos son programas maliciosos diseñados para infectar y dañar computadoras y sistemas, replicándose y extendiéndose a otros equipos. Estos pueden alterar el funcionamiento normal de los sistemas, robar información, generar pérdidas de datos, o facilitar ataques adicionales. Los virus requieren la intervención del usuario para ejecutarse, a menudo disfrazados como archivos legítimos o adjuntos en correos electrónicos.

15.- ¿Define el Concepto de autenticación?

La autenticación es el proceso mediante el cual se verifica la identidad de un usuario o dispositivo antes de otorgar acceso a sistemas y datos. Este proceso puede basarse en algo que el usuario sabe (como una contraseña), algo que el usuario tiene (como un token de seguridad o un teléfono móvil), o algo que el usuario es (como huellas dactilares o reconocimiento facial). La autenticación es fundamental para asegurar que solo los usuarios autorizados puedan acceder a recursos y servicios sensibles.

16.- ¿Mecanismos preventivos en seguridad informática?

Los mecanismos preventivos en seguridad informática son estrategias y herramientas diseñadas para evitar incidentes de seguridad antes de que ocurran.

Incluyen la implementación de software antivirus y antimalware, el uso de firewalls para controlar el tráfico de red, la actualización regular de sistemas y aplicaciones para corregir vulnerabilidades, la realización de copias de seguridad de datos importantes, la educación y capacitación de usuarios en buenas prácticas de seguridad, y la adopción de políticas de seguridad fuertes como el principio de menor privilegio y la autenticación multifactor.

17.- ¿Mecanismos correctivos en seguridad informática?

Los mecanismos correctivos en seguridad informática son acciones y procedimientos implementados después de que un incidente de seguridad ha ocurrido, con el objetivo de mitigar el daño, restaurar los sistemas y servicios afectados a su estado operativo normal, y prevenir futuros incidentes. Incluyen la identificación y eliminación de malware, la reparación de sistemas dañados, la recuperación de datos a partir de copias de seguridad, la actualización de sistemas y aplicaciones para corregir vulnerabilidades explotadas, y la revisión y mejora de políticas y procedimientos de seguridad.

18.-¿Qué es el aumento de privilegios?

El aumento de privilegios es un ataque o vulnerabilidad que permite a un usuario o proceso obtener un nivel de acceso más elevado en un sistema del que originalmente se le había concedido, violando las políticas de seguridad. Este tipo de ataque se utiliza para ganar acceso no autorizado a funciones restringidas o datos sensibles, permitiendo al atacante realizar acciones que normalmente estarían fuera de su alcance, como modificar configuraciones del sistema, acceder a datos confidenciales o ejecutar comandos arbitrarios.

19.- ¿Técnicas de aumento de privilegios en Windows y/o Linux?

Las técnicas de aumento de privilegios en sistemas Windows y Linux pueden incluir la explotación de vulnerabilidades de software no parcheadas, el uso de contraseñas por defecto o débiles, la ingeniería social para obtener credenciales de administrador, y el abuso de configuraciones de sistema mal configuradas o servicios vulnerables. En Windows, esto podría involucrar manipular el Registro o usar herramientas de terceros para escalada. En Linux, podría incluir explotar vulnerabilidades en el kernel o servicios de sistema para obtener acceso root. Estas técnicas requieren que los administradores mantengan los sistemas actualizados y sigan las mejores prácticas de seguridad.

20.- ¿Protección frente al aumento de privilegios??

Para protegerse contra el aumento de privilegios, es fundamental aplicar regularmente parches y actualizaciones de seguridad para corregir vulnerabilidades conocidas. Además, se deben seguir las mejores prácticas de seguridad como el principio de menor privilegio, asegurando que los usuarios tengan solo los permisos necesarios para sus tareas. La implementación de

soluciones de seguridad, como sistemas de detección de intrusiones y antivirus, junto con una monitorización constante de los sistemas para detectar actividades sospechosas, también es crucial. Finalmente, la capacitación y concienciación de los usuarios sobre los riesgos de seguridad informática puede ayudar a prevenir ataques que buscan explotar vulnerabilidades humanas.

Bibliografía

Bishop, M. (2002). *Computer Security: Art and Science*. Boston: Addison Wesley

Mell, P.; Scarfone, K.; Romanosky, S. (2007). *A Complete Guide to the Common Vulnerability Scoring System Version 2.0* [artículo en línea] <http://www.first.org/cvss/cvss-guide.html>

Shirey, R. (2000). *Internet Security Glossary*. RFC 2828, IETF

Benito, M. (2022, 4 febrero). *¿Qué es la seguridad informática y por qué es tan importante? - FP Online*. FP Online. https://fp.uoc.fje.edu/blog/que-es-la-seguridad-informatica-y-por-que-es-tan-importante/