Universidad Autónoma de Chiapas
Facultad de contaduría y administración C-I

Carrera:
Lic. En ing en desarrollo y tecnologías de software.

Materia:
Análisis de vulnerabilidades.

Catedrático:
Mtro. Luis Gutiérrez Alfaro.

Nombre del alumno:
González Aguilar Eduardo - A211154

Semestre: 7. **Grupo:** M.

Nombre de la actividad:
Investigación de conceptos.

Link Github:
AguilarEduardo/AnalisisDeVulnerabilidades (github.com)

Fecha de entrega:
09/02/2024.

1.- ¿Qué es vulnerabilidad?

Una vulnerabilidad es una debilidad o fallo en un sistema de seguridad que puede ser explotado por un atacante para comprometer la integridad, confidencialidad o disponibilidad de un sistema o de la información que contiene.

2.- ¿Qué es seguridad?

La seguridad se refiere al conjunto de medidas y procedimientos diseñados para proteger los activos de una organización o individuo, como la información, los sistemas informáticos, la infraestructura física, entre otros, contra amenazas y riesgos potenciales.

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

- Confidencialidad: Garantizar que la información solo sea accesible para aquellos autorizados.

- Integridad: Asegurar que la información sea precisa, completa y no se haya alterado de manera no autorizada.

- Disponibilidad: Asegurar que los recursos de información estén disponibles y accesibles cuando sea necesario.

- Autenticidad: Verificar la identidad de usuarios y recursos para asegurar que sean quienes dicen ser.

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

Los sistemas, los datos, las redes y los usuarios.

5.- ¿Escribe algunos ataques sobre los datos ?

Robo de datos, la modificación no autorizada de datos, la suplantación de identidad y el secuestro de dato(ransomware).

6.¿De que nos protegemos?

Nos protegemos de amenazas y riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información y los sistemas.

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

Malware, ataques de denegación de servicio (DDoS), intrusos, robo de datos, entre otros.

8.¿Menciona los tipos de vulnerabilidades?

Vulnerabilidades de software, vulnerabilidades de red, vulnerabilidades físicas y vulnerabilidades humanas.

9.-¿Por qué aumentan las amenazas ?

Las amenazas aumentan debido a la creciente interconexión de sistemas, el aumento del valor de la información, la evolución de las tecnologías y la sofisticación de los ataques.

10.- ¿Menciona tres protecciones más usadas ?

- Cortafuegos (firewalls).

- Antivirus.

- Software de detección de intrusiones (IDS).

- Software de prevención de intrusiones (IPS).

- Cifrado de datos.

- Autenticación de dos factores.

11.-¿Que es amenaza?

Una amenaza es cualquier evento, acción o potencialidad que pueda causar daño, pérdida o interrupción en un sistema o en la información que contiene.

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

Los factores del riesgo de desastres desde un enfoque holístico incluyen aspectos como la ubicación geográfica, la vulnerabilidad de las infraestructuras, la capacidad de respuesta de las autoridades y la preparación de la comunidad.

13.- ¿Que es la ingeniería social?

La ingeniería social es una técnica utilizada por atacantes para manipular a las personas y obtener información confidencial o acceso no autorizado a sistemas mediante el engaño psicológico.

14.- ¿Que son los virus informáticos?

Los virus informáticos son programas maliciosos diseñados para replicarse y propagarse a través de sistemas informáticos, con el objetivo de causar daño, robar información o realizar otras acciones no autorizadas.

15.- ¿Define el Concepto de autenticación?

La autenticación es el proceso de verificar la identidad de un usuario o recurso, generalmente mediante el uso de credenciales como contraseñas, certificados digitales, tokens o biometría.

16.- ¿ Mecanismos preventivos en seguridad informática?

Algunos mecanismos preventivos incluyen cortafuegos, antivirus, sistemas de detección de intrusiones, políticas de seguridad, educación y concientización de usuarios, entre otros.

17.- ¿ Mecanismos correctivos en seguridad informática?

Los mecanismos correctivos en seguridad informática incluyen la aplicación de parches de seguridad, la restauración de sistemas desde copias de seguridad, la investigación forense digital y la implementación de contramedidas para mitigar el impacto de un incidente de seguridad.

18.-¿Qué es el aumento de privilegios?

El aumento de privilegios se refiere al proceso mediante el cual un atacante obtiene acceso a recursos o funcionalidades para los cuales no tiene autorización inicialmente, incrementando sus privilegios en el sistema.

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

Algunas técnicas de aumento de privilegios incluyen la explotación de vulnerabilidades de software, el uso de herramientas de escalada de privilegios, la manipulación de permisos y configuraciones incorrectas, entre otras.

20.-¿Protección frente al aumento de privilegios?

Para protegerse contra el aumento de privilegios, es importante implementar políticas de seguridad sólidas, mantener actualizado el software con parches de seguridad, utilizar mecanismos de control de acceso adecuados y realizar auditorías de seguridad regulares para detectar y mitigar posibles vulnerabilidades.

Conclusión.

En conclusión, la seguridad informática es un aspecto crítico en el mundo actual, donde la información y los sistemas digitales son fundamentales para las operaciones de organizaciones y la vida cotidiana de las personas. Para proteger estos activos, es esencial entender y aplicar los principios de seguridad, como confidencialidad, integridad, disponibilidad y autenticidad, así como implementar medidas preventivas y correctivas contra amenazas y vulnerabilidades. Desde la gestión de riesgos hasta la aplicación de tecnologías y políticas de seguridad, es necesario un enfoque integral y proactivo para salvaguardar la información y los sistemas contra ataques, aumentando así la resiliencia y la confianza en el entorno digital. La educación y concientización de usuarios también juegan un papel fundamental en la protección contra ataques de ingeniería social y en la promoción de una cultura de seguridad cibernética. En resumen, la seguridad informática es un proceso continuo y colaborativo que requiere la participación de todos los actores involucrados para mantener la integridad, confidencialidad y disponibilidad de la información en un mundo cada vez más interconectado y digitalizado.

Fuente de información.

Autor Desconocido, (08 de febrero del 2024), “Que es la Vulnerabilidad”. Qué es Vulnerabilidad: Significado, Tipos y Ejemplos - Enciclopedia Significados

Autor Desconocido, (08 de febrero del 2024), “Virus informático, ¿Qué son los virus informáticos? ¿Cómo funcionan los virus informáticos?”. Virus informáticos - Definición, tipos y función explicada (hornetsecurity.com)

DocuSing, (24 de Agosoto 2021), “¿Cuáles son los pilares de la seguridad de la infromacion?”- ¿Cuáles son los pilares de la seguridad de la información? (docusign.com)