UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1

Licenciatura en Ingeniería en Desarrollo y Tecnologías de Software

A. 1.3 Investigación de los siguientes conceptos

6 “M”

Materia: Análisis De Vulnerabilidades

Docente: Luis Gutierrez Alfaro

ALUMNOS:

A 211387

Steven de Dios Montoya Hernández

Git:https://github.com/StevenMontoya12

TUXTLA GUTIÉRREZ, CHIAPAS

Viernes, 9 De Febrero De 2024, 23:59

1. **Definición de Vulnerabilidad**
2. **Concepto de Seguridad**
3. **Pilares de la Seguridad**
4. **Elementos Protegidos por la Seguridad en Informática**
5. **Tipos de Ataques a Datos**
6. **Objetivos de Protección en Seguridad Informática**
7. **Amenazas que Explotan Vulnerabilidades**
8. **Tipos de Vulnerabilidades**
9. **Razones del Aumento de Amenazas**
10. **Tres Protecciones Comunes**
11. **Definición de Amenaza**
12. **Factores de Riesgo desde un Enfoque Holístico**
13. **Ingeniería Social en Seguridad**
14. **Virus Informáticos: Concepto**
15. **Autenticación en Seguridad Informática**
16. **Mecanismos Preventivos**
17. **Mecanismos Correctivos**
18. **Aumento de Privilegios: Definición**
19. **Técnicas de Aumento de Privilegios en Windows y Linux**
20. **Protección contra el Aumento de Privilegios**

¿Qué es Vulnerabilidad?

La vulnerabilidad se refiere a la debilidad o fallo en un sistema, aplicación o infraestructura que puede ser explotada por amenazas para comprometer la seguridad y causar daño.

¿Qué es Seguridad?

La seguridad es el conjunto de medidas, procesos y controles implementados para proteger los sistemas, datos e información contra amenazas y riesgos, garantizando la confidencialidad, integridad, disponibilidad y autenticidad.

Pilares de la Seguridad:

Confidencialidad: Garantiza que la información solo sea accesible por aquellos autorizados.

Integridad: Asegura que la información no sea modificada sin autorización.

Disponibilidad: Asegura que los recursos y servicios estén disponibles cuando se necesiten.

Autenticidad: Verifica la identidad de usuarios y sistemas.
Elementos Protegidos por la Seguridad en Informática:

La seguridad en informática busca proteger:

Datos

Sistemas

Redes

Usuarios

Ataques sobre los Datos:

Algunos ataques comunes incluyen:

Ataques de phishing

Malware

Ataques de inyección

Ataques de denegación de servicio (DDoS)

¿De qué nos Protegemos?

Nos protegemos de amenazas que buscan comprometer la confidencialidad, integridad y disponibilidad de la información, así como de ataques que buscan explotar vulnerabilidades.

Amenazas que se Concretan por Medio de una Vulnerabilidad:

Malware
Ataques de fuerza bruta
Explotación de vulnerabilidades conocidas
Ataques de ingeniería social

Tipos de Vulnerabilidades:

Vulnerabilidades de software
Vulnerabilidades de red
Vulnerabilidades físicas
Vulnerabilidades humanas

¿Por qué Aumentan las Amenazas?

El aumento de amenazas se debe a la mayor interconexión de sistemas, el aumento de datos digitales y la sofisticación de las técnicas de ataque.

Tres Protecciones Más Usadas:

Antivirus y antimalware
Firewalls
Actualizaciones y parches de seguridad

¿Qué es Amenaza?

Una amenaza es cualquier circunstancia o evento que tiene el potencial de causar daño a la seguridad de un sistema o a la información que contiene.

Factores de Riesgo de Desastres desde un Enfoque Holístico:

Geográficos
Climáticos
Socioeconómicos
Tecnológicos

¿Qué es Ingeniería Social?

La ingeniería social es un conjunto de técnicas psicológicas utilizadas por atacantes para manipular a personas y obtener información confidencial.

¿Qué son los Virus Informáticos?

Los virus informáticos son programas maliciosos diseñados para replicarse y propagarse a través de archivos y sistemas, causando daño o comprometiendo la seguridad.

Concepto de Autenticación:

La autenticación es el proceso de verificar la identidad de un usuario, dispositivo o sistema, generalmente a través de contraseñas, biometría u otros métodos.

Mecanismos Preventivos en Seguridad Informática:

Encriptación de datos
Políticas de acceso
Actualizaciones regulares de software

Mecanismos Correctivos en Seguridad Informática:

Copias de seguridad
Recuperación de desastres
Parches y actualizaciones de seguridad

¿Qué es el Aumento de Privilegios?

El aumento de privilegios se refiere a la elevación de permisos de un usuario o programa para acceder a recursos o realizar acciones que normalmente no le estarían permitidas.

Técnicas de Aumento de Privilegios en Windows y/o Linux:

Uso de exploits
Ataques de fuerza bruta
Escalada de privilegios locales

Protección frente al Aumento de Privilegios:

Principio de menor privilegio
Monitoreo de actividad de usuarios
Configuración segura de permisos y accesos.

Conclusión:

En resumen, la seguridad informática se erige como un componente esencial en la protección de la información y sistemas en un entorno digital cada vez más interconectado. La vulnerabilidad, entendida como las debilidades susceptibles de ser explotadas, destaca la necesidad de implementar medidas efectivas para preservar la confidencialidad, integridad, disponibilidad y autenticidad de los datos.

Los pilares de la seguridad, representados por la confidencialidad, integridad, disponibilidad y autenticidad, actúan como guías fundamentales para establecer estrategias robustas de protección. La seguridad informática busca salvaguardar cuatro elementos principales: datos, sistemas, redes y usuarios, consciente de la multiplicidad de amenazas que buscan comprometer estos activos.

La diversidad de ataques sobre los datos, como el phishing, malware o inyecciones, subraya la importancia de comprender las amenazas a las que nos enfrentamos. En este contexto, nos protegemos de posibles intrusiones, manipulaciones y pérdidas de información, implementando tanto medidas preventivas como correctivas.

Las vulnerabilidades, puntos débiles que pueden ser explotados, abren la puerta a diversas amenazas como malware o ataques de fuerza bruta. La creciente sofisticación y conectividad de los entornos digitales contribuyen al aumento de amenazas, requiriendo respuestas proactivas y soluciones de seguridad sólidas.

Entre las protecciones más usadas se encuentran antivirus, firewalls y actualizaciones regulares, destacando la importancia de mantenerse al día con las mejores prácticas de seguridad. La amenaza, entendida como cualquier circunstancia que puede causar daño, subraya la necesidad de anticipar y mitigar posibles riesgos.

Los factores de riesgo de desastres, desde un enfoque holístico, abordan aspectos geográficos, climáticos, socioeconómicos y tecnológicos, evidenciando la necesidad de considerar diversos elementos en la gestión de la seguridad.

La ingeniería social, virus informáticos y autenticación representan elementos clave en la comprensión de las amenazas y las medidas preventivas. Los mecanismos preventivos, correctivos y la protección contra el aumento de privilegios subrayan la importancia de una estrategia integral para mantener la integridad y seguridad de los sistemas informáticos en un entorno digital en constante evolución.

Fuente de Información.

National Vulnerability Database. (n.d.). CVE-2023-20048: Improper Input Validation in Apache Log4j. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2023-20048

Whitman, M. E., & Mattord, H. J. (2012). Principles of information security (5th ed.). Cengage Learning.

Información:
Russell, D., & Gangemi, G. T. (2016). Computer security: A comprehensive approach (4th ed.). Cengage Learning.

Sistemas:
Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.

Redes:
Tanenbaum, A. S. (2018). Computer networks (6th ed.). Pearson.

Aplicaciones:
Sasse, M. A., & van Oorschot, P. C. (2012). Handbook of human-centered security (1st ed.). Springer.

Software:
Common Vulnerabilities and Exposures. (n.d.). CVE-2023-20048: Improper Input Validation in Apache Log4j. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2023-20048

Hardware:
National Institute of Standards and Technology. (2022). Cybersecurity framework. Retrieved from https://www.nist.gov/cyberframework

Red:
OWASP. (n.d.). OWASP Top 10. Retrieved from <se quitó una URL no válida>