Universidad Autónoma De Chiapas.

A 1.3 Investigación de conceptos.

Estudiante: José Gilberto Guzmán Gutiérrez.

LIDTS. 7ºM.

A200119.

Catedrático: DR. Luis Gutiérrez Alfaro.

Tuxtla Gutiérrez Chiapas. 27 de agosto del 2023.

Contenido

Desarrollo del tema.

1. ¿Qué es vulnerabilidad?

   Es una **debilidad o fallo** en un sistema, aplicación o proceso que podría ser explotada por un atacante para comprometer la seguridad del sistema, acceder a información sensible o causar daño.

2. ¿Qué es seguridad?

   Se refiere al **conjunto de medidas y prácticas implementadas para proteger sistemas**, datos, información y recursos de posibles amenazas y ataques. El objetivo es mantener la confidencialidad, integridad y disponibilidad de los activos digitales.

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

   - **Confidencialidad**: Garantiza que solo las personas autorizadas puedan acceder a la información.
   - **Integridad**: Asegura que los datos no sean modificados de manera no autorizada o accidental.
   - **Disponibilidad**: Garantiza que los sistemas y datos estén disponibles cuando se necesiten.
   - **Autenticidad**: Asegura que la identidad de los usuarios y los datos sean verificables y confiables.

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

   - **Datos**: Información almacenada en sistemas.
   - **Sistemas**: Hardware y software utilizados para procesar y almacenar datos.
   - **Redes**: Infraestructuras que permiten la comunicación entre sistemas.
   - **Usuarios**: Personas que utilizan los sistemas y acceden a los datos.

5. ¿Escribe algunos ataques sobre los datos?

   - **Ataques de inyección** (SQL injection, XSS).
   - **Robo de datos** (phishing, robo de identidad).
   - **Ataques de denegación de servicio** (DoS, DDoS).
   - **Malware** (virus, gusanos, troyanos).
   - **Ataques de fuerza bruta**.

6. ¿De qué nos protegemos?

- Acceso no autorizado a sistemas y datos.
- Robo o pérdida de información confidencial.
- Interrupción de servicios.
- Manipulación no autorizada de datos.
- Daños causados por malware y ataques maliciosos.

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

    - **Malware**: Aprovecha vulnerabilidades para infectar sistemas.
    - **Acceso no autorizado**: Explota debilidades para ganar acceso indebido.
    - **Robo de información**: Aprovecha fallos para extraer datos sensibles.
    - **Ataques de denegación de servicio**: Explota debilidades para saturar recursos.

8. ¿Menciona los tipos de vulnerabilidades?

    - De **software** (errores en código).
    - De **configuración** (ajustes incorrectos).
    - **Físicas** (acceso físico no autorizado).
    - De **red** (debilidades en comunicaciones).

9. ¿Por qué aumentan las amenazas?

    - Mayor **interconexión de sistemas**.
    - Mayor **dependencia de tecnologías**.
    - Mayor **valor de la información** digital.
    - Mayor **sofisticación** de los atacantes.

10. ¿Menciona tres protecciones más usadas?

    - **Cortafuegos** (firewalls).
    - **Antivirus y antimalware**.
    - **Autenticación de dos factores** (2FA).

11. ¿Qué es amenaza?

    Se refiere a cualquier **circunstancia o evento potencial que podría explotar una vulnerabilidad** para causar daño o pérdida a sistemas, datos o recursos.

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

    - **Físicos** (geológicos, climáticos, tecnológicos).
    - **Sociales** (vulnerabilidad de la población).

- **Económicos** (impacto en la economía).
- **Ambientales** (impacto en el entorno).

13. ¿Qué es la ingeniería social?

    Es una técnica en la que los atacantes **manipulan psicológicamente** a las personas para obtener información confidencial o acceso a sistemas.

14. ¿Qué son los virus informáticos?

    Son **programas maliciosos que se replican e insertan en otros archivos o programas**. Pueden causar daños al sistema, robar información o realizar acciones no autorizadas.

15. ¿Define el Concepto de autenticación?

    Proceso de **verificación la identidad** de un usuario, generalmente a través de credenciales como contraseñas, huellas dactilares o tokens, antes de permitir el acceso a sistemas o datos.

16. ¿Mecanismos preventivos en seguridad informática?

    - **Cortafuegos** (firewalls).
    - **Actualizaciones de software**.
    - **Políticas de seguridad**.
    - **Encriptación de datos**.

17. ¿Mecanismos correctivos en seguridad informática?

    - **Respuesta a incidentes**.
    - **Análisis forense**.
    - **Parches y actualizaciones de seguridad**.
    - **Restauración desde copias de seguridad**.

18. ¿Qué es el aumento de privilegios?

    Se refiere a **la elevación de los permisos de acceso y control** de un usuario o proceso, permitiéndole acceder a recursos o realizar acciones que normalmente no estarían autorizados.

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

    - **Explotación de vulnerabilidades del sistema**.
    - **Uso de contraseñas débiles**.

- **Ataques de fuerza bruta**.
- **Explotación de configuraciones inseguras**.

20. ¿Protección frente al aumento de privilegios?

- **Aplicar parches y actualizaciones**.
- **Usar contraseñas seguras y políticas de autenticación sólidas**.
- **Aplicar el principio de "menos privilegios"**.
- **Utilizar soluciones de monitoreo y detección de anomalías**.

Conclusión.

Posterior a la realización de esta investigación, se pudo comprender que la seguridad informática es un concepto muy basto y complejo, el cual busca prevenir diversos tipos de vulnerabilidades, ya sean por errores de programación, falta de conocimientos u manipulación psicológica hacia los usuarios, una mala gestión de privilegios, entre otros.

Fuentes de información.

1. What is a vulnerability? Definition + examples. (s/f). Upguard.com. Recuperado el 27 de agosto de 2023, de https://www.upguard.com/blog/vulnerability
2. Bacon, M. (2021, junio 22). What is security? Security; TechTarget. https://www.techtarget.com/searchsecurity/definition/security
3. Zorio, L., & Chief Information Security Officer. (2022, junio 21). 3 pillars of data security: Confidentiality, integrity & availability. Mark43. https://mark43.com/resources/blog/3-pillars-of-data-security-confidentiality-availability-integrity/
4. Forsyth, C. (s/f). The four elements which form an effective security system. Detection-technologies.com. Recuperado el 27 de agosto de 2023, de https://blog.detection-technologies.com/the-four-elements-which-form-an-effective-security-system
5. Types of cyber attacks. (s/f). Rapid7. Recuperado el 27 de agosto de 2023, de https://www.rapid7.com/fundamentals/types-of-attacks/
6. 10 ways to prevent cyber attacks. (2020, febrero 11). Leaf. https://leaf-it.com/10-ways-prevent-cyber-attacks/
7. Dosal, E. (2020, febrero 13). Top 9 Cybersecurity Threats and Vulnerabilities - Compuquip. Compuquip.com. https://www.compuquip.com/blog/cybersecurity-threats-vulnerabilities
8. Raza, M. (2023, abril 10). Vulnerability types: 5 types of vulnerabilities you need to know. Splunk-Blogs. https://www.splunk.com/en_us/blog/learn/vulnerability-types.html
9. Reed, J. (2023, enero 4). 7 reasons global attacks will rise significantly in 2023. Security Intelligence. https://securityintelligence.com/articles/7-reasons-global-attacks-will-soar-2023/

10. Common cyber security measures. (s/f). Nibusinessinfo.co.uk; NI Business Info. Recuperado el 27 de agosto de 2023, de https://www.nibusinessinfo.co.uk/content/common-cyber-security-measures
11. Cyber threat - glossary. (s/f). Nist.gov. Recuperado el 27 de agosto de 2023, de https://csrc.nist.gov/glossary/term/cyber_threat
12. Adams, M. (2022, septiembre 22). The Importance of developing a Holistic Cyber Security Approach for your Business. Businesstechweekly.com. https://www.businesstechweekly.com/cybersecurity/risk-management/cyber-security-approach/
13. What is social engineering? (2023, junio 30). Usa.kaspersky.com. https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering
14. Computer Virus: What are Computer Viruses? (s/f). Malwarebytes. Recuperado el 27 de agosto de 2023, de https://www.malwarebytes.com/computer-virus
15. Shacklett, M. E., & Rosencrance, L. (2021, septiembre 27). What is authentication? Security; TechTarget. https://www.techtarget.com/searchsecurity/definition/authentication
16. Developing network security strategies. (s/f). Ciscopress.com. Recuperado el 28 de agosto de 2023, de https://www.ciscopress.com/articles/article.asp?p=1626588&seqNum=2
17. (S/f). Drata.com. Recuperado el 28 de agosto de 2023, de https://drata.com/blog/security-controls
18. Privilege escalation attack and defense explained. (2023, junio 19). BeyondTrust. https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained
19. Privilege escalation. (2023, febrero 23). Aqua; Aqua Security. https://www.aquasec.com/cloud-native-academy/supply-chain-security/privilege-escalation/
20. Arun, K. L. (2022, enero 31). What is A privilege escalation attack? How to prevent privilege escalation attacks? The Sec Master. https://thesecmaster.com/what-is-a-privilege-escalation-attack-how-to-prevent-privilege-escalation-attacks/