Centro Universitario De Ciencias Exactas e ingenierías

Sistemas Operativos

Becerra Velázquez Violeta del Rocío

De Santiago Rodríguez Armando

Código: 222362658

Ingeniería en Computación (ICOM)

Sección: D04

Actividad de Aprendizaje 15

12/05/2024

Actividad de Aprendizaje 15

Índice

Tabla de contenido

Índice 2
Esteganografía: 3
Ensayo el tema de seguridad y protección tanto en el sistema operativo como en la red 3
Seguridad en Sistemas Operativos: 3
Seguridad en Redes: 4
El Papel del Usuario: 5
Resumen película Blackhat 5
Conclusiones: 6
Referencias: 6

Criptografía:

La criptografía es el estudio de técnicas para asegurar la comunicación y el almacenamiento de información frente a adversarios. Se basa en algoritmos matemáticos que transforman los datos en un formato ilegible (cifrado) y que solo pueden ser decodificados por aquellos que poseen la clave de descifrado correspondiente.

- **Aplicaciones en sistemas operativos:** La criptografía se utiliza en sistemas operativos para proteger la confidencialidad de los datos almacenados y transmitidos. Por ejemplo, sistemas operativos modernos como Windows, macOS y Linux ofrecen herramientas integradas para cifrar unidades de almacenamiento, archivos individuales y comunicaciones de red.
- **Aplicaciones en redes:** En redes, la criptografía se utiliza para garantizar la confidencialidad y la integridad de la información transmitida a través de canales inseguros, como Internet. Protocolos como HTTPS (HTTP seguro), SSL/TLS, IPsec y VPN utilizan técnicas criptográficas para proteger las comunicaciones entre clientes y servidores.

Esteganografía:

La esteganografía es el arte y la ciencia de ocultar información dentro de otros datos, de modo que la presencia de la información oculta sea imperceptible para un observador externo. A diferencia de la criptografía, que se centra en hacer que los mensajes sean incomprensibles, la esteganografía se centra en hacer que los mensajes sean invisibles.

- **Aplicaciones en sistemas operativos:** En sistemas operativos, la esteganografía se puede utilizar para ocultar datos sensibles dentro de archivos multimedia, como imágenes, audio o video. También se pueden utilizar técnicas esteganográficas para ocultar información en el espacio no utilizado de archivos de sistema.
- **Aplicaciones en redes:** En redes, la esteganografía puede utilizarse para ocultar mensajes dentro de archivos multimedia que se comparten a través de la red. Esto puede permitir la comunicación encubierta entre partes interesadas sin despertar sospechas.

Ensayo el tema de seguridad y protección tanto en el sistema operativo como en la red

En la era digital actual, donde la información es un activo invaluable, la seguridad y protección en los sistemas operativos y redes se han convertido en pilares fundamentales para garantizar la integridad, confidencialidad y disponibilidad de los datos. Tanto en el ámbito personal como empresarial, la vulnerabilidad a ciberataques es una preocupación constante. En este ensayo, exploraremos la importancia de la seguridad en los sistemas operativos y redes, así como el papel crucial que desempeña el usuario para garantizar su cumplimiento.

Seguridad en Sistemas Operativos:

Los sistemas operativos actúan como el puente entre el hardware y el software, gestionando recursos y ejecutando programas. Por lo tanto, asegurar la seguridad en

estos sistemas es esencial para proteger toda la información y funcionalidad que operan sobre ellos.

- **Actualizaciones y Parches**: Los desarrolladores constantemente identifican y corrigen vulnerabilidades en los sistemas operativos a través de actualizaciones y parches de seguridad. Es responsabilidad del usuario asegurarse de aplicar estas actualizaciones de manera oportuna para mantener su sistema protegido.

- **Firewalls y Antivirus:** Implementar firewalls y software antivirus ayuda a prevenir intrusiones no autorizadas y a detectar y eliminar malware que pueda comprometer la seguridad del sistema.
- **Políticas de Acceso:** Establecer políticas de acceso que limiten los privilegios de los usuarios y controlen el acceso a recursos sensibles es crucial para prevenir brechas de seguridad.

Seguridad en Redes:

Las redes de computadoras son el medio a través del cual los sistemas operativos intercambian datos y recursos. Garantizar la seguridad en las redes es fundamental para proteger la comunicación y prevenir ataques externos e internos.

- **Cifrado de Datos:** Utilizar protocolos de cifrado como SSL/TLS en la comunicación de red ayuda a proteger la confidencialidad de los datos transmitidos, evitando que sean interceptados por terceros no autorizados.
- **Segmentación de Redes:** Dividir la red en segmentos separados con acceso controlado ayuda a limitar el alcance de posibles ataques, mitigando el impacto en caso de intrusión.

- **Monitoreo de Tráfico:** Implementar sistemas de monitoreo de tráfico de red permite detectar actividades sospechosas y responder rápidamente ante posibles amenazas.

El Papel del Usuario:

Aunque las medidas técnicas son esenciales, el usuario desempeña un papel igualmente crucial en la garantía de la seguridad en sistemas operativos y redes.

- **Conciencia de Seguridad:** Estar informado sobre las últimas amenazas y mejores prácticas de seguridad ayuda a los usuarios a tomar decisiones más seguras al utilizar sus sistemas y navegar por la red.
- **Buena Higiene Digital:** Adoptar prácticas de seguridad básicas, como la creación de contraseñas fuertes y únicas, evitar hacer clic en enlaces sospechosos y no compartir información confidencial, contribuye significativamente a proteger los sistemas y datos personales.
- **Educación y Formación:** Capacitar a los usuarios sobre la importancia de la seguridad cibernética y proporcionarles capacitación regular sobre cómo identificar y responder a posibles amenazas mejora su capacidad para protegerse a sí mismos y a sus sistemas.

Resumen película Blackhat

La película comienza con un ciberataque masivo a una instalación nuclear china que hace que explote. Las autoridades chinas trabajaron con el FBI para localizar al responsable del ataque y descubrieron que el código malicioso utilizado fue creado por un hacker.

Nicholas Hathaway es un ladrón que cumple condena de prisión por delitos cibernéticos. Hathaway fue liberado temporalmente para que ayudara al FBI a atrapar al ladrón responsable del ataque. Los agentes del FBI y expertos en seguridad informática, Hathaway inició una búsqueda de pruebas que los llevó a varios países.

Actividad de Aprendizaje 15

A medida que avanza su investigación, descubren que el ataque nuclear es sólo el comienzo de una serie de ciberataques orquestados por un grupo criminal. Hathaway y su equipo enfrentan desafíos cada vez mayores mientras intentan detener al hacker y evitar nuevos ataques.

Conclusiones:

La criptografía y la esteganografía representan pilares fundamentales en la protección de la información, cada una con enfoques distintos para garantizar la seguridad de los datos. En el ámbito de los sistemas operativos y las redes, la seguridad se convierte en un aspecto crucial, requiriendo medidas técnicas como actualizaciones regulares, firewalls y cifrado de datos, así como una participación del usuario a través de la conciencia de seguridad y prácticas de higiene digital. Esta combinación de enfoques técnicos y comportamientos responsables se convierte en la clave para mantener la integridad, confidencialidad y disponibilidad de la información en el entorno digital actual.

Referencias:

"Applied Cryptography: Protocols, Algorithms, and Source Code in C" de Bruce Schneier.

"Cryptography Engineering: Design Principles and Practical Applications" de Bruce Schneier, Niels Ferguson y Tadayoshi Kohno.

"Disappearing Cryptography: Information Hiding: Steganography & Watermarking" de Peter Wayner.

"Information Hiding Techniques for Steganography and Digital Watermarking" de Stefan Katzenbeisser y Fabien A. P. Petitcolas.

Bejtlich, R. (2013). "The Practice of Network Security Monitoring: Understanding Incident Detection and Response." No Starch Press.

Stallings, W. (2017). "Operating Systems: Internals and Design Principles." Pearson.

Whitman, M. E., & Mattord, H. J. (2018). "Management of Information Security." Cengage Learning.

Blackhat - Amenaza en la red