UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1

ING. EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

7 “M”

OPT.2 - ANÁLISIS DE VULNERABILIDADES

SUB2

ACTIVIDAD 2.1 HERRAMIENTAS PASIVAS

ALUMNO: MARCO ANTONIO ZÚÑIGA MORALES – A211121

DOCENTE: DR. LUIS GUTIÉRREZ ALFARO

TUXTLA GUTIÉRREZ, CHIAPAS
SÁBADO, 24 DE FEBRERO DE 2024

Índice

Introducción

La seguridad en la red constituye una piedra angular en la protección de la información y los recursos digitales en nuestra era tecnológicamente avanzada. A medida que la interconexión global se expande, también lo hace la complejidad y el alcance de los posibles ataques, vulnerabilidades y amenazas a los sistemas informáticos y las redes. En este contexto, conceptos fundamentales como la confidencialidad, la integridad, la disponibilidad y la autenticación emergen como pilares esenciales para salvaguardar la información contra accesos no autorizados y garantizar que los datos sean precisos, completos y accesibles cuando se necesiten.

Dentro de este marco, la elaboración y la implementación de políticas de seguridad robustas se vuelven críticas para establecer las normas, procedimientos y prácticas que regirán la defensa de los activos informáticos. Estas políticas no solo delinean las expectativas de seguridad dentro de una organización, sino que también proveen una guía clara para la gestión de riesgos y la respuesta ante incidentes. Además, destacan la importancia de mantener una postura de seguridad proactiva, adaptándose constantemente a las nuevas amenazas que emergen en un panorama digital en evolución.

Específicamente, la seguridad web merece una atención especial debido a su naturaleza expuesta y susceptible a una amplia variedad de ataques. La protección de aplicaciones y servicios web es crítica para preservar la confidencialidad de los datos del usuario, mantener la integridad de la información y asegurar la disponibilidad de los servicios en línea. Las vulnerabilidades en servicios como el DNS pueden ser explotadas para realizar ataques de envenenamiento de caché o amplificación, poniendo en riesgo la estabilidad y seguridad de las redes.

La utilización de herramientas como Maltego, para la inteligencia de fuentes abiertas, y la práctica de búsquedas de vulnerabilidades a través de motores de búsqueda, representan métodos innovadores para identificar riesgos y fortalecer las defensas. Sin embargo, estas técnicas también subrayan la necesidad de una ética sólida y un conocimiento profundo de las implicaciones legales y morales en la seguridad informática.

Finalmente, comprender y mitigar las amenazas en seguridad de la información no es solo una cuestión técnica, sino una prioridad estratégica que impacta directamente en la continuidad del negocio, la confianza del cliente y la reputación corporativa. A medida que avanzamos hacia un futuro cada vez más digitalizado, la seguridad en la red se posiciona como un desafío omnipresente, exigiendo una atención meticulosa, conocimiento especializado y una constante evolución de estrategias y herramientas para proteger nuestros activos digitales más valiosos.

Desarrollo

Explica que es network security o seguridad en la red.

La seguridad en la red, o network security, se refiere a las políticas, prácticas y herramientas diseñadas para proteger la integridad, confidencialidad y accesibilidad de las redes de computadoras y datos.

Su objetivo es asegurar la integridad, confidencialidad y disponibilidad de la información y los recursos de la red. Esto implica proteger tanto la infraestructura física como la digital, incluyendo hardware, software, y los datos que circulan por la red.

La seguridad en la red abarca una amplia gama de tecnologías, dispositivos y procesos. Incluye medidas preventivas como firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), cifrado de datos, y software antivirus. También involucra prácticas de gestión de seguridad, como la evaluación de vulnerabilidades, las pruebas de penetración, y la formación en concienciación sobre seguridad para los usuarios.

Explicar los tipos de ataques, vulnerabilidades y amenazas

- **Ataques:** Los ataques pueden ser pasivos, como la interceptación de datos (eavesdropping), o activos, como el acceso no autorizado a sistemas (hacking), la introducción de malware o el DoS (Denial of Service).

- **Ataques Pasivos:** Incluyen el espionaje o la interceptación de comunicaciones para recopilar datos sin afectar los recursos del sistema.

    Un ejemplo sería el sniffing de red, donde un atacante recopila datos que se transmiten a través de la red sin alterarlos.

- **Ataques Activos:** Son aquellos que alteran o destruyen los datos, o afectan negativamente las operaciones de la red. Esto puede incluir ataques de denegación de servicio (DoS), donde el objetivo es hacer que un recurso de la red sea inaccesible a los usuarios legítimos.

- **Vulnerabilidades:** Son debilidades en el sistema que pueden ser explotadas por un atacante para comprometer la seguridad. Esto incluye configuraciones incorrectas, software desactualizado, y fallos en el diseño del sistema o de la red.

- **Amenazas:** Son potenciales violaciones de seguridad que podrían explotar una vulnerabilidad para causar daño. Las amenazas pueden ser internas (originadas dentro de la organización) o externas (originadas fuera de la organización), e incluyen a actores maliciosos como hackers, malware, y ataques dirigidos.

Explica los conceptos básicos como confidencialidad, integridad, disponibilidad y autenticación

- **Confidencialidad:** Se refiere a la protección de la información para que solo las personas autorizadas puedan acceder a ella. El cifrado es una técnica común utilizada para mantener la confidencialidad de los datos.

- **Integridad:** Asegura que la información es fiable y precisa, y que no ha sido modificada de forma no autorizada. Los mecanismos de control de integridad, como las sumas de verificación y los hash criptográficos, ayudan a detectar alteraciones en los datos.

- **Disponibilidad:** Implica asegurar que los datos y los recursos de la red estén disponibles para los usuarios legítimos cuando los necesiten. Esto incluye protegerse contra ataques que buscan interrumpir los servicios, como los ataques de denegación de servicio.

- **Autenticación:** Es el proceso de verificar la identidad de un usuario, dispositivo o entidad antes de permitirle acceso a los recursos de la red. La autenticación puede basarse en algo que el usuario sabe (una contraseña), algo que el usuario tiene (un token de seguridad o un teléfono móvil), o algo que el usuario es (biometría).

Política de seguridad

Una política de seguridad es un documento formal que establece las reglas, directrices y prácticas a seguir para proteger los activos de información de una organización.

Su propósito es minimizar el riesgo de seguridad y asegurar que los datos se manejen de manera segura y consistente, para proteger la integridad, confidencialidad y disponibilidad de la información.

La política de seguridad sirve como un marco para la gestión de la seguridad de la información y establece las expectativas para el comportamiento de los empleados, los procedimientos operativos y el uso de los sistemas y recursos de TI.

Presenta las características de una política de seguridad

- **Claridad y Comprensibilidad:** Debe estar escrita en un lenguaje claro y comprensible para todos los destinatarios, independientemente de su conocimiento técnico.

- **Alcance y Aplicabilidad:** Debe definir claramente su alcance y ser aplicable a toda la organización, incluyendo empleados, contratistas y cualquier otra parte interesada.

- **Responsabilidades y Roles Definidos:** Debe asignar claramente responsabilidades y roles específicos en lo que respecta a la seguridad de la información.

- **Directrices Específicas:** Debe proporcionar directrices específicas sobre cómo proteger los activos de información, incluyendo procedimientos para el manejo de datos sensibles, gestión de contraseñas y acceso a redes.

- **Cumplimiento de Normativas y Leyes:** Debe asegurar el cumplimiento de todas las leyes, regulaciones y estándares de la industria relevantes.

- **Evaluación de Riesgos y Gestión:** Debe establecer un proceso para la evaluación y gestión de riesgos de seguridad de la información.

- **Mecanismos de Revisión y Actualización:** Debe incluir procedimientos para su revisión periódica y actualización, asegurando que siga siendo relevante ante el cambiante panorama de amenazas.

- **Medidas Disciplinarias:** Debe describir las acciones que se tomarán en caso de incumplimiento de la política.

Por qué se requiere atención especial la seguridad web

La seguridad web requiere atención especial debido a la naturaleza pública e interconectada de la web, lo que la hace particularmente vulnerable a una amplia gama de ataques. Esto incluye la exposición de datos sensibles, el robo de identidad, y ataques a la infraestructura web.

La seguridad web merece una atención especial por varias razones críticas:

- **Crecimiento Exponencial de Amenazas:** El número y la sofisticación de los ataques dirigidos a aplicaciones y servicios web están en aumento, incluyendo inyecciones SQL, cross-site scripting (XSS), y ataques de fuerza bruta.

- **Datos Sensibles:** Las aplicaciones web a menudo procesan y almacenan datos sensibles, como información financiera y personal, lo que las convierte en un objetivo atractivo para los ciberdelincuentes.

- **Visibilidad Pública:** Dado que las aplicaciones web están accesibles públicamente, son más susceptibles a ser exploradas y atacadas por actores maliciosos de todo el mundo.

- **Reputación y Confianza:** Los incidentes de seguridad web pueden dañar seriamente la reputación de una organización y erosionar la confianza de los clientes y usuarios.

- **Requisitos de Cumplimiento:** La seguridad web es también un requisito para cumplir con diversas normativas y estándares de protección de datos, como el GDPR en Europa.

Por qué preocuparse sobre la seguridad web

La preocupación sobre la seguridad web es primordial por varias razones críticas en el entorno digital actual:

1. **Protección de Datos Sensibles:** Las páginas web y las aplicaciones suelen manejar datos sensibles, incluyendo información financiera, personal, y de salud. Una brecha en la seguridad puede resultar en el acceso no autorizado, robo, o exposición de estos datos, afectando tanto a individuos como a organizaciones.

2. **Confianza del Usuario:** La seguridad web es fundamental para mantener y construir la confianza de los usuarios. Los incidentes de seguridad pueden erosionar esta confianza, llevando a la pérdida de clientes y dañando la reputación de una marca o institución.

3. **Cumplimiento Normativo:** Existen diversas regulaciones y leyes que exigen a las organizaciones proteger la información personal de los usuarios. La falta de seguridad web puede resultar en violaciones de estas normativas, acarreando sanciones económicas y legales significativas.

4. **Ataques Cibernéticos en Aumento:** Con el crecimiento del comercio electrónico y la presencia digital, las amenazas cibernéticas se han vuelto más sofisticadas y frecuentes. Esto incluye ransomware, phishing, y otros tipos de malware diseñados específicamente para explotar vulnerabilidades web.

5. **Costos Asociados a Brechas de Seguridad:** Las brechas de seguridad pueden tener un costo económico directo significativo, incluyendo la necesidad de implementar medidas correctivas, pagar compensaciones y enfrentar posibles demandas legales.

6. **Infraestructura Crítica:** Muchas infraestructuras críticas dependen de sistemas web para su operación. Un ataque o fallo en la seguridad web puede tener consecuencias devastadoras para servicios esenciales como hospitales, sistemas de energía y servicios financieros.

Que son las vulnerabilidades en servicio DNS a través de herramientas web

Las vulnerabilidades en el servicio DNS pueden incluir envenenamiento de caché (DNS poisoning), donde los atacantes desvían el tráfico web a sitios maliciosos, y ataques de amplificación DNS, que pueden causar denegaciones de servicio. Las herramientas web, como los escáneres de vulnerabilidades, pueden ayudar a identificar y mitigar estas vulnerabilidades.

El DNS es fundamental para la funcionalidad de Internet, traduciendo nombres de dominio fáciles de recordar en direcciones IP necesarias para la localización de servicios y páginas web.

Las vulnerabilidades pueden incluir:

- **Envenenamiento de caché DNS:** Donde los atacantes insertan información falsa en la caché DNS de un servidor, redirigiendo a los usuarios a sitios maliciosos.

- **DNS Amplification Attacks:** Ataques de amplificación que utilizan servidores DNS públicamente accesibles para inundar un objetivo con tráfico de respuesta DNS, efectivamente realizando un ataque de denegación de servicio distribuido (DDoS).

- **Secuestro de DNS:** Cambiar la configuración de DNS de un sitio web para redirigir el tráfico a un servidor bajo control del atacante.

Herramientas web específicas, como escáneres de vulnerabilidades DNS y evaluadores de configuración, pueden ayudar a identificar estas vulnerabilidades, permitiendo a los administradores de sistemas tomar medidas correctivas antes de que sean explotadas.

Que son las búsquedas vulnerabilidades a través de Google

Las búsquedas de vulnerabilidades a través de Google, conocidas como "Google hacking", utilizan operadores de búsqueda avanzados para encontrar información sensible expuesta en la web o vulnerabilidades en sistemas y redes.

Este método puede revelar:

- Información confidencial expuesta accidentalmente en la web (como archivos de configuración, bases de datos expuestas y backups).
- Páginas de administración de sitios web sin proteger.
- Vulnerabilidades conocidas en software específico, a través de la búsqueda de versiones de software y los errores asociados a ellas.

Aunque esta técnica puede ser utilizada por atacantes para identificar objetivos vulnerables, también es una herramienta valiosa para los profesionales de seguridad para auditar y mejorar la postura de seguridad de sus propias organizaciones.

Que es la herramienta maltego

Maltego es una herramienta avanzada de análisis e inteligencia que permite a los usuarios recopilar, integrar y analizar información de diversas fuentes abiertas, así como realizar enlaces gráficos de relaciones entre piezas de información. Es especialmente útil en el campo de la seguridad informática y la inteligencia de fuentes abiertas (OSINT) para:

- Identificación de vulnerabilidades.
- Recopilación de información sobre personas o empresas.
- Mapeo de la infraestructura de red de un objetivo.
- Análisis de relaciones sociales y redes.

Maltego se destaca por su capacidad para visualizar complejas redes de información, lo que ayuda en la identificación de patrones ocultos o conexiones que pueden ser indicativos de vulnerabilidades de seguridad o amenazas potenciales.

Que son las amenazas en seguridad de la información

Las amenazas en seguridad de la información se refieren a cualquier potencial de daño que pueda afectar la confidencialidad, integridad o disponibilidad de la información. Incluyen malware, phishing, ataques de ingeniería social, ataques de denegación de servicio, entre otros.

- **Malware:** Software malicioso diseñado para dañar o realizar acciones no autorizadas en un sistema informático.

- **Phishing:** Tácticas de engaño para obtener información sensible, como contraseñas y datos de tarjetas de crédito, a través de la suplantación de entidades confiables.

- **Ataques de Fuerza Bruta:** Intentos repetitivos de adivinar contraseñas o claves criptográficas.

- **Insider Threats:** Amenazas internas de empleados o contratistas que abusan de su acceso para dañar a la organización.

- **Ataques de Denegación de Servicio (DDoS):** Intentos de hacer que los recursos de la red sean inaccesibles a sus usuarios previstos.

Entender y mitigar estas amenazas es crucial para proteger la información y los sistemas críticos de una organización. Esto requiere una combinación de tecnologías de seguridad, políticas robustas, y una cultura de concienciación sobre seguridad entre los usuarios.

Conclusión

En conclusión, la exploración de los temas relacionados con la seguridad en la red ha revelado la complejidad y la importancia crítica de proteger nuestras infraestructuras digitales en un mundo cada vez más interconectado. Hemos aprendido que la seguridad de la información no se limita a la implementación de tecnologías avanzadas, sino que también abarca la comprensión profunda de conceptos fundamentales como la confidencialidad, la integridad, la disponibilidad y la autenticación. Estos principios forman la base sobre la cual se construyen políticas de seguridad efectivas, diseñadas para salvaguardar los activos digitales contra un espectro cada vez mayor de amenazas y vulnerabilidades.

Una lección particularmente importante extraída de esta discusión es la necesidad imperativa de prestar atención especial a la seguridad web. Dado el volumen y la sensibilidad de los datos manejados a través de aplicaciones y servicios web, la protección contra ataques y explotaciones en este ámbito se ha convertido en una prioridad absoluta. Las vulnerabilidades en servicios críticos como el DNS resaltan la sofisticación de las amenazas actuales y la necesidad de herramientas avanzadas y estrategias proactivas para detectar y mitigar riesgos potenciales.

La utilización de herramientas como Maltego para inteligencia de fuentes abiertas y las técnicas de búsqueda de vulnerabilidades evidencian la evolución constante de las metodologías de seguridad. Estas prácticas no solo mejoran nuestra capacidad para identificar y abordar debilidades antes de que sean explotadas, sino que también refuerzan la importancia de una ética de seguridad informática rigurosa y un compromiso con la legalidad y la responsabilidad.

Este viaje a través de los diversos aspectos de la seguridad en la red subraya el hecho de que, en el ámbito de la ciberseguridad, el conocimiento y la preparación son tan importantes como las soluciones tecnológicas mismas. La continua evolución de las amenazas requiere una actualización constante de nuestras habilidades y estrategias para proteger eficazmente la información y los sistemas.

En última instancia, la seguridad en la red es una responsabilidad compartida que exige la colaboración entre individuos, organizaciones y gobiernos para desarrollar un entorno digital seguro y resiliente.

La comprensión de la seguridad en la red y sus múltiples dimensiones nos equipa mejor para enfrentar los desafíos actuales y futuros en el ciberespacio. Al priorizar la educación, la conciencia y la implementación de políticas de seguridad robustas, podemos aspirar a un futuro digital más seguro para todos.

Referencia bibliográfica

Avi. (2023, 6 julio). *Seguridad de red: conceptos básicos y 12 recursos de aprendizaje*. Geekflare. https://geekflare.com/es/learn-network-security/

Cruzito. (2022, 7 octubre). *¿Qué es una política de seguridad de red? - Procedimientos y ejemplos* | *Estudyando*. Estudyando. https://estudyando.com/que-es-una-politica-de-seguridad-de-red-procedimientos-y-ejemplos/

Inga. (2022, 26 octubre). *Política de seguridad de la red*. TechEdu. https://techlib.net/techedu/politica-de-seguridad-de-la-red/

López, A. (2023, 23 octubre). Estos son todos los ataques a las redes que existen y cómo evitarlos. *RedesZone*. https://www.redeszone.net/tutoriales/seguridad/listado-completo-ataques-redes-como-evitarlos/

ManageEngine. (s. f.). *Políticas de seguridad de la red* | *ManageEngine Firewall Analyzer*. https://www.manageengine.com/latam/firewall/politica-de-seguridad-de-la-red.html

¿Qué es DNS? (2023, 19 abril). www.kaspersky.es. https://www.kaspersky.es/resource-center/definitions/dns

¿Qué es la seguridad de la red? (2018, 4 julio). IDG Communications S.A.U. https://www.computerworld.es/seguridad/que-es-la-seguridad-de-la-red

¿Qué es la seguridad de red? | *Seguridad de redes empresariales* | *Cloudflare*. (s. f.). Cloudflare. https://www.cloudflare.com/es-es/learning/network-layer/network-security/

¿Qué es una política de seguridad de red? - Spiegato. (2021, 28 julio). *Spiegato*. https://spiegato.com/es/que-es-una-politica-de-seguridad-de-red

Seguridad web: Importancia, amenazas que debes evitar y consejos clave. (s. f.). https://blog.akky.mx/seguridad-web-importancia-amenazas-que-debes-evitar-y-consejos-clave

Stic. (2023, 8 mayo). *Confidencialidad, Integridad y Disponibilidad*. Ciberseguridad. https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/

Team, A. (s. f.). *Tipos de Vulnerabilidades y Amenazas informáticas*. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Unir, V. (2023, 11 octubre). Los 4 principios de la seguridad informática y su implementación. *UNIR FP*. https://unirfp.unir.net/revista/ingenieria-y-tecnologia/principios-seguridad-informatica/

Stallings, W. (2020). Network Security Essentials: Applications and Standards (7th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th ed.). Cengage Learning.

Pfleeger, C. P., & Pfleeger, S. L. (2017). Security in Computing (5th ed.). Pearson.

Easttom, C. (2019). Computer Security Fundamentals (4th ed.). Pearson.

Shema, M. (2020). Hacking Web Applications: The Art of Hacking Series (2nd ed.). Pearson IT Certification.

Aitchison, R. (2019). Pro DNS and BIND 10. Apress.

Long, J., & Gardner, T. (2020). Google Hacking for Penetration Testers (3rd ed.). Syngress.

Chappell, P. (2018). Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information (6th ed.). CreateSpace Independent Publishing Platform.

Andress, J., & Winterfeld, S. (2021). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (3rd ed.). Syngress.