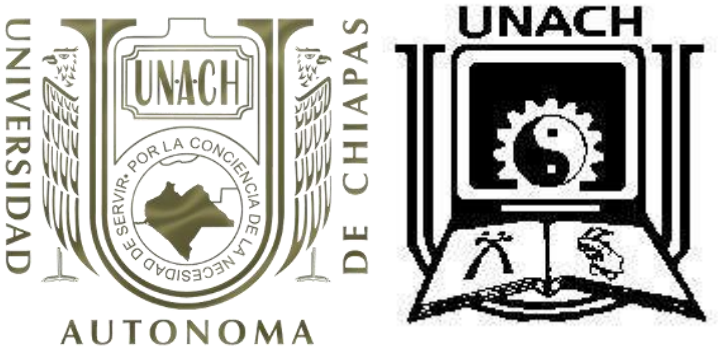
UNIVERSIDAD AUTÓNOMA DE CHIAPAS



FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1
Licenciatura en Ingeniería en Desarrollo y Tecnologías de Software

Actividad. 2.1 Herramientas pasivas

6 “M”

Materia: Análisis De Vulnerabilidades
Docente: Luis Gutiérrez Alfaro

ALUMNOS:
A 211387
Steven de Dios Montoya Hernández
Git:https://github.com/StevenMontoya12

TUXTLA GUTIÉRREZ, CHIAPAS
Sábado, 24 de febrero de 2024

Explica que es network security o seguridad en la red.

La seguridad en la red, también conocida como seguridad informática o network security en inglés, se refiere a las medidas y prácticas diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información que se encuentra en una red de computadoras.

Algunos aspectos clave de la seguridad en la red incluyen:

Confidencialidad: Garantizar que la información sensible solo sea accesible por aquellos autorizados para verla. Esto puede lograrse mediante técnicas de cifrado y control de acceso.

Integridad: Asegurar que la información no sea alterada de manera no autorizada durante su transmisión o almacenamiento. Los mecanismos de integridad incluyen firmas digitales y checksums.

Disponibilidad: Asegurar que los recursos de la red estén disponibles cuando sea necesario. Esto implica proteger contra ataques de denegación de servicio (DoS) y planificación de la capacidad adecuada.

Autenticación: Verificar la identidad de usuarios, sistemas y dispositivos que acceden a la red. Esto se logra mediante contraseñas, certificados digitales, biometría y otros métodos.

Control de Acceso: Limitar el acceso a recursos de red solo a aquellos usuarios o sistemas autorizados. Esto se puede lograr mediante políticas de acceso y tecnologías como firewalls y listas de control de acceso (ACL).

Monitoreo y Detección de Intrusiones: Implementar herramientas y sistemas para monitorear la actividad de la red y detectar comportamientos inusuales que puedan indicar un posible ataque o violación de seguridad.

Actualizaciones y Parches: Mantener actualizados los sistemas y aplicaciones con las últimas correcciones de seguridad para mitigar vulnerabilidades conocidas.

Educación y Concientización: Sensibilizar a los usuarios y administradores de la red sobre las prácticas de seguridad, la importancia de contraseñas fuertes, y cómo reconocer posibles amenazas y ataques de ingeniería social.

Explicar los tipos de ataques, vulnerabilidades y amenazas.

Tipos de Ataques:

Ataques de Fuerza Bruta:

Intentos repetitivos de adivinar credenciales de acceso mediante la prueba sistemática de todas las combinaciones posibles de contraseñas.

Ataques de Inyección:

Se introducen datos maliciosos en una aplicación para manipular su comportamiento. Ejemplos comunes incluyen ataques de SQL injection y de Cross-Site Scripting (XSS).

Ataques de Denegación de Servicio (DoS) y Distribuidos (DDoS):

Buscan saturar los recursos de un sistema o red, haciendo que sea inaccesible para los usuarios legítimos. En los ataques DDoS, se utiliza una red de sistemas comprometidos para amplificar el impacto.

Ataques de Man-in-the-Middle (MitM):

El atacante se sitúa entre la comunicación de dos partes y puede interceptar o alterar los datos que se transmiten. Esto puede ocurrir en redes Wi-Fi no seguras o a través de ataques ARP spoofing.

Ataques de Phishing:

Intentan engañar a los usuarios para que revelen información confidencial, como contraseñas o información financiera, mediante el uso de correos electrónicos, mensajes o sitios web falsos.

Ataques de Ransomware:

Malware que cifra los archivos de la víctima y exige un rescate para restaurar el acceso. Los ataques de ransomware son una forma de extorsión digital.

Tipos de Vulnerabilidades:

Vulnerabilidades de Software:

Errores en el código de software que pueden ser explotados por un atacante para comprometer la seguridad del sistema. Esto incluye bugs, fallas de diseño y vulnerabilidades de día cero.

Vulnerabilidades de Configuración:

Configuraciones incorrectas o débiles en sistemas, aplicaciones o dispositivos que pueden ser aprovechadas por un atacante para obtener acceso no autorizado.

Vulnerabilidades en Sistemas Operativos:

Fallas en los sistemas operativos que podrían ser explotadas para comprometer la integridad y seguridad del sistema.

Vulnerabilidades en Red:

Debilidades en la infraestructura de red, como configuraciones incorrectas de firewalls o routers, que podrían permitir a un atacante acceder a la red de manera no autorizada.

Vulnerabilidades en Protocolos:

Debilidades en los protocolos de comunicación utilizados en redes, como el protocolo SSL/TLS, que podrían ser explotadas para interceptar o manipular datos.

Tipos de Amenazas:

Malware:

Software malicioso diseñado para dañar o explotar sistemas. Incluye virus, gusanos, troyanos y ransomware.

Ingeniería Social:

Engañar a las personas para obtener información confidencial o persuadirlas para que realicen acciones que comprometan la seguridad.

Atacantes Internos:

Individuos dentro de una organización que abusan de sus privilegios para acceder, robar o dañar información.

Hacktivismo:

Ataques realizados con motivaciones políticas o sociales, donde los atacantes buscan expresar sus opiniones o causar impacto.

Amenazas Persistentes Avanzadas (APTs):

Ataques a largo plazo y altamente dirigidos, donde los atacantes buscan mantenerse ocultos mientras roban información valiosa.

Botnets:

Redes de dispositivos comprometidos que son controlados de manera remota por un atacante. Se utilizan para realizar actividades maliciosas, como ataques DDoS.

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

1. Confidencialidad:

Definición: La confidencialidad se refiere a la protección de la información contra el acceso o divulgación no autorizados. Garantiza que solo aquellos con permisos adecuados puedan acceder a la información sensible.

Ejemplo: El cifrado de datos es una medida común para mantener la confidencialidad. Solo las personas con la clave adecuada pueden descifrar y acceder a la información.

2. Integridad:

Definición: La integridad se relaciona con la protección de la precisión y la confiabilidad de la información. Asegura que los datos no sean alterados de manera no autorizada durante su almacenamiento, procesamiento o transmisión.

Ejemplo: El uso de firmas digitales en mensajes o archivos garantiza que no se hayan modificado desde la firma. Si se altera el contenido, la firma ya no coincidirá.

3. Disponibilidad:

Definición: La disponibilidad se refiere a garantizar que los recursos de la información estén disponibles y accesibles cuando se necesiten. Implica prevenir o mitigar interrupciones en el acceso a la información.

Ejemplo: Implementar medidas de redundancia, como tener servidores duplicados en ubicaciones geográficas diferentes, para garantizar que los servicios estén disponibles incluso en caso de fallos.

4. Autenticación:

Definición: La autenticación verifica la identidad de un usuario, sistema o dispositivo. Asegura que solo aquellos con credenciales válidas tengan acceso a recursos protegidos.

Ejemplo: El uso de contraseñas, tarjetas de acceso, huellas dactilares o certificados digitales son métodos comunes de autenticación. Un usuario debe demostrar su identidad antes de acceder a un sistema.

Política de seguridad.

La elaboración de una política de seguridad es crucial para proteger los sistemas y datos sensibles de una organización contra posibles amenazas y riesgos.

Objetivo y Alcance:

Define el propósito de la política, que en este caso sería establecer directrices para la identificación y mitigación de vulnerabilidades.

Especifica el alcance de la política, indicando los sistemas, aplicaciones o redes que están sujetos a las evaluaciones de vulnerabilidades.

Responsabilidades:

Establece las responsabilidades de los equipos de seguridad, administradores de sistemas y personal encargado de realizar análisis de vulnerabilidades.

Define claramente quiénes son responsables de implementar parches y soluciones para las vulnerabilidades identificadas.

Procedimientos de Análisis de Vulnerabilidades:

Describe los métodos y herramientas que se utilizarán para realizar análisis de vulnerabilidades.

Detalla la frecuencia con la que se llevarán a cabo las evaluaciones.

Notificación de Vulnerabilidades:

Establece un proceso claro para la notificación de vulnerabilidades descubiertas, tanto internamente como externamente.

Define límites de tiempo para la divulgación responsable de vulnerabilidades a terceros.

Gestión de Parches:

Especifica los procedimientos para la gestión de parches y actualizaciones.

Define cómo se priorizarán y aplicarán los parches, especialmente para las vulnerabilidades críticas.

Segregación de Redes y Datos Sensibles:

Indica cómo se deben segmentar y proteger las redes que contienen datos sensibles o sistemas críticos.

Establece políticas de control de acceso y medidas para limitar la exposición de vulnerabilidades.

Auditoría y Seguimiento:

Describe cómo se llevarán a cabo auditorías de seguridad para verificar el cumplimiento de la política.

Especifica las medidas de seguimiento para garantizar que las vulnerabilidades identificadas se aborden y resuelvan en un tiempo adecuado.

Educación y Concientización:

Fomenta la conciencia sobre la importancia del análisis de vulnerabilidades entre el personal.

Proporciona capacitación continua sobre las mejores prácticas de seguridad.

Colaboración con Terceros:

Establece pautas para la colaboración con proveedores externos o expertos en seguridad para realizar análisis de vulnerabilidades.

Define cómo se compartirán los resultados y se gestionarán las relaciones con terceros.

Política de Respuesta a Incidentes:

Especifica cómo se responderá a incidentes relacionados con vulnerabilidades.

Define roles y responsabilidades durante la gestión de incidentes de seguridad.

Actualización y Revisión:

Indica cómo se mantendrá y actualizará la política para adaptarse a cambios en las amenazas o en la infraestructura tecnológica.

Establece intervalos para la revisión de la política.

Cumplimiento y Sanciones:

Describe las consecuencias por no cumplir con las directrices de seguridad establecidas.

Define las sanciones correspondientes para garantizar la responsabilidad.

Por qué se requiere atención especial la seguridad web.

La seguridad web es fundamental debido a la creciente dependencia de las actividades en línea y el intercambio de información a través de la World Wide Web. Aquí hay varias razones por las cuales la seguridad web requiere atención especial:

Volumen de Datos Sensibles:

La web almacena y procesa grandes cantidades de datos sensibles, incluyendo información personal, datos financieros y comerciales. La pérdida o compromiso de esta información puede tener consecuencias graves.

Aumento de Ataques Cibernéticos:

El número y la sofisticación de los ataques cibernéticos dirigidos a aplicaciones web han aumentado significativamente. Los ciberdelincuentes buscan explotar vulnerabilidades para robar datos, realizar fraudes o interrumpir servicios.

Evolución de las Amenazas:

Las amenazas en línea evolucionan constantemente. Nuevas formas de malware, técnicas de phishing y ataques de inyección son desarrolladas para eludir las medidas de seguridad tradicionales.

Importancia de la Reputación:

La seguridad web afecta directamente la reputación de una organización. Una brecha de seguridad puede socavar la confianza de los usuarios y clientes, lo que puede llevar a pérdidas financieras y daño a la marca.

Comercio Electrónico y Transacciones en Línea:

El auge del comercio electrónico y las transacciones en línea implica la transmisión de datos financieros y personales. La seguridad web es esencial para proteger esta información durante su procesamiento y almacenamiento.

Privacidad del Usuario:

Los usuarios esperan que sus datos personales estén seguros al interactuar con sitios web. La falta de seguridad puede resultar en violaciones de privacidad y en la pérdida de la confianza del usuario.

Cumplimiento Normativo:

Muchas industrias están sujetas a regulaciones estrictas que exigen medidas de seguridad web. No cumplir con estas normativas puede llevar a sanciones legales y multas.

Ataques Dirigidos a Aplicaciones Web:

Las aplicaciones web son a menudo el blanco de ataques específicos, como inyecciones SQL, Cross-Site Scripting (XSS) y Cross-Site Request Forgery (CSRF). Proteger las aplicaciones web es esencial para prevenir estas amenazas.

Por qué preocuparse de la seguridad web.

La seguridad web es crítica en la era digital debido a la abundancia de datos sensibles y la creciente amenaza de ataques cibernéticos. Garantizar la protección de información personal, financiera y empresarial, así como prevenir la explotación de vulnerabilidades, es esencial para construir y mantener la confianza del usuario. Además, el cumplimiento normativo, la preservación de la privacidad, la gestión de la reputación y la garantía de la disponibilidad de servicios en línea son razones clave por las cuales la seguridad web debe ser una prioridad para individuos y organizaciones en el entorno digital actual.

La protección contra amenazas como ransomware y extorsión digital se vuelve esencial para evitar no solo pérdidas financieras, sino también posibles daños a la reputación y a la continuidad de las operaciones. La seguridad web no solo es una medida preventiva, sino que también implica una preparación constante para responder a incidentes, asegurando la integridad de la información y la confianza en un entorno digital dinámico y desafiante.

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

Las vulnerabilidades en servicios DNS a través de herramientas web implican debilidades en la seguridad de los sistemas DNS que pueden ser explotadas mediante el uso de herramientas y técnicas basadas en la web. Un ejemplo de vulnerabilidad común es la inyección de datos en zonas DNS, donde un atacante puede manipular registros DNS para dirigir el tráfico a servidores controlados por ellos. Otro riesgo es la posibilidad de ataques de transferencia de zona, que explotan configuraciones débiles para obtener información completa sobre la infraestructura DNS.

Además, el envenenamiento de caché DNS es una amenaza donde los atacantes introducen información falsa en la caché DNS del servidor, influyendo en la resolución de nombres de dominio. Los ataques de amplificación DNS buscan aprovechar servicios mal configurados para amplificar el tráfico dirigido a un objetivo específico. Finalmente, el spoofing de respuestas DNS implica falsificar respuestas para redirigir usuarios a sitios maliciosos o interceptar tráfico.

Estas vulnerabilidades pueden ser exploradas mediante herramientas web que automatizan ataques DNS, como dnsrecon. La mitigación de estos riesgos implica implementar buenas prácticas de configuración, mantener actualizaciones de software y realizar auditorías regulares para detectar y corregir posibles vulnerabilidades, garantizando así la integridad y seguridad del sistema DNS.

Que son las búsquedas vulnerabilidades a través de Google

Las búsquedas de vulnerabilidades a través de Google, conocidas como "Google hacking" o "dorks", involucran la utilización de consultas específicas en el motor de búsqueda para identificar información sensible o descubrir posibles puntos débiles en sistemas y redes. Estas búsquedas pueden exponer datos que no deberían ser públicamente accesibles y pueden ser empleadas tanto con fines legítimos, como la evaluación de seguridad, como de manera malintencionada.

Por ejemplo, al realizar consultas específicas, se pueden descubrir documentos desactualizados de software que contienen información sobre vulnerabilidades conocidas. Asimismo, estas búsquedas pueden revelar archivos de configuración mal protegidos, como configuraciones de servidores web, que podrían contener información sensible o revelar configuraciones incorrectas. Otros casos incluyen la identificación de dispositivos IoT o cámaras de seguridad con configuraciones inseguras y la expo

Que es la herramienta maltego

Maltego es una herramienta de inteligencia de código abierto utilizada en el campo de la ciberseguridad y la investigación de amenazas. Su objetivo principal es recopilar y visualizar información de manera gráfica para facilitar la comprensión de las relaciones entre diferentes entidades en el mundo digital. Maltego se utiliza comúnmente para realizar análisis de redes, investigaciones de amenazas y recopilación de información.

La herramienta permite a los usuarios realizar búsquedas en diversas fuentes de datos en línea, como bases de datos públicas, redes sociales, registros DNS y más. Utiliza técnicas de transformación para convertir y visualizar esta información de manera gráfica, presentando las conexiones entre entidades, como direcciones IP, nombres de dominio, correos electrónicos y organizaciones.

Maltego puede ser una herramienta valiosa para profesionales de la ciberseguridad y analistas de inteligencia, ya que simplifica el proceso de recopilación de datos y ayuda a identificar patrones y conexiones en el ciberespacio. Sin embargo, es esencial utilizar Maltego de manera ética y respetar la privacidad y las leyes aplicables, ya que el mal uso de la información recopilada podría tener consecuencias legales.

Que son las amenazas en seguridad de la información

Las amenazas en seguridad de la información son eventos o situaciones que potencialmente pueden causar daño o comprometer la integridad, confidencialidad y disponibilidad de los datos y sistemas de una organización. Estas amenazas pueden manifestarse de diversas maneras, siendo una de las más prominentes los ataques cibernéticos. Estos incluyen tácticas como el hacking, malware, ransomware y phishing, que buscan explotar vulnerabilidades en sistemas y redes.

Además, amenazas como el acceso no autorizado a sistemas, la pérdida o robo de dispositivos que contienen información sensible y desastres naturales o errores humanos también representan riesgos significativos. Las amenazas internas, derivadas de acciones malintencionadas o negligentes de individuos dentro de la organización, así como las vulnerabilidades en la infraestructura, los ataques de ingeniería social y la interceptación de comunicaciones, contribuyen a la complejidad del panorama de amenazas.

La gestión efectiva de riesgos implica comprender y evaluar constantemente estas amenazas. Esto incluye abordar problemas como fallos de seguridad en el software, robo de identidad y, crucialmente, la implementación de medidas de seguridad proactivas. La conciencia y la adopción de buenas prácticas de seguridad son esenciales para mitigar las amenazas en seguridad de la información y proteger la vitalidad y confiabilidad de los activos digitales de una organización.

Referencias Bibliográficas

Forouzan, B. A. (2022). Fundamentos de seguridad en redes. McGraw-Hill Education.

Stallings, W. (2021). Criptografía y seguridad en redes. Pearson Educación.

Northcutt, S., & Novak, J. (2020). Detección de intrusiones en redes. McGraw-Hill Education. [se quitó una URL no válida]

Scarfone, K., & Souppaya, M. (2017). Guía de seguridad de redes y sistemas. NIST Special Publication 800-82. https://doi.org/10.6028/NIST.SP.800-82r2

ISO/IEC 27001:2013. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos. International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

NIST Cybersecurity Framework. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Anderson, R. (2008). Seguridad informática: un enfoque de ingeniería. John Wiley & Sons.

Pfleeger, C. P., & Pfleeger, S. L. (2018). Seguridad en computación y redes. Pearson Educación.

OWASP Foundation. Open Web Application Security Project. https://owasp.org/

Cloudflare. Web Application Firewall. https://www.cloudflare.com/waf/

DNSSEC. Domain Name System Security Extensions. https://www.dnssec.net/

Microsoft. DNS Security Best Practices.

Google Hacking Database.

Shodan. https://shodan.io/

Maltego Technologies. Maltego. https://www.maltego.com/

ENISA. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/

MITRE ATT&CK Framework. https://attack.mitre.org/