UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN CAMPUS 1 ING.

EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE NOMBRE DE

LA MATERIA: Análisis De Vulnerabilidades

TEMA (ACTIVIDAD). Realiza una investigación de los siguientes conceptos

NOMBRE DEL ALUMNO: Gabriel Omar Fuentes Chacon.

MATRICULA: A211120

SEMESTRE: 7 Séptimo.

GRUPO: M

DOCENTE: Mtro. Luis Gutiérrez Alfaro

LUGAR: Plataforma

Fecha de entrega: 08/02/2024

INDICE

Presentación

La seguridad informática es un campo dinámico y vital que aborda vulnerabilidades en sistemas, procesos y aplicaciones para salvaguardar la integridad, confidencialidad y disponibilidad de la información. Los pilares de confidencialidad, integridad, disponibilidad y autenticidad son fundamentales en la gestión de riesgos. Para proteger datos, sistemas, redes y usuarios, se emplean estrategias como firewalls, antivirus, actualizaciones y parches de seguridad. Se previenen amenazas como inyecciones, phishing y malware. En este contexto, nos protegemos contra una amplia gama de ataques, y las amenazas se materializan a menudo a través de vulnerabilidades. Estas vulnerabilidades incluyen errores de codificación y configuraciones incorrectas. El aumento de amenazas se atribuye a la expansión tecnológica, la complejidad de sistemas y la globalización. Las protecciones más usadas son firewalls, antivirus y actualizaciones de seguridad. La ingeniería social, ataques de fuerza bruta y denegación de servicio son desafíos constantes. Los mecanismos preventivos y correctivos en seguridad informática, junto con la gestión de vulnerabilidades, son esenciales. El aumento de privilegios, tanto en Windows como en Linux, requiere medidas específicas de protección. Estas prácticas se aplican en entornos empresariales, gubernamentales y personales para garantizar la seguridad digital y mitigar los riesgos asociados con posibles amenazas.

Contenido

La seguridad informática, un ámbito dinámico y vital, se enfoca en proteger la integridad, confidencialidad y disponibilidad de la información frente a diversas amenazas. Se basa en pilares como confidencialidad, integridad, disponibilidad y autenticidad. Para salvaguardar datos, sistemas y redes, se emplean estrategias como firewalls, antivirus y actualizaciones de seguridad, previniendo amenazas como inyecciones, phishing y malware.

Las vulnerabilidades, como errores de codificación y configuraciones incorrectas, son puntos débiles explotables. El aumento de amenazas se atribuye a la expansión tecnológica y complejidad de sistemas. Protecciones clave incluyen firewalls, antivirus y actualizaciones. Ingeniería social, ataques de fuerza bruta y denegación de servicio son desafíos persistentes. Mecanismos preventivos y correctivos, junto con la gestión de vulnerabilidades, son esenciales.

El aumento de privilegios, en Windows y Linux, requiere medidas específicas de protección para evitar accesos no autorizados. La seguridad informática no solo abarca tecnología, también la educación y concienciación del usuario son cruciales para fortalecer la postura de seguridad. La identificación de amenazas y la gestión de riesgos son prácticas proactivas fundamentales en entornos empresariales, gubernamentales y personales para garantizar la seguridad digital y mitigar riesgos asociados.

Desarrollo del tema

1.- ¿Qué es vulnerabilidad?

La vulnerabilidad se refiere a debilidades o fallos en sistemas, procesos, aplicaciones o componentes que pueden ser aprovechados por amenazas para comprometer la integridad, confidencialidad o disponibilidad de la información. Estas debilidades pueden manifestarse en diversas áreas, como el software, hardware, sistemas operativos, protocolos de red o incluso en el comportamiento humano. En el ámbito del software, los errores de codificación y las implementaciones deficientes de medidas de seguridad son factores críticos. Los sistemas operativos pueden volverse vulnerables debido a configuraciones inseguras o la falta de aplicar parches de seguridad. En hardware, problemas de diseño o defectos de fabricación pueden afectar la seguridad. Las redes y protocolos pueden ser vulnerables debido a protocolos inseguros o la falta de cifrado en las comunicaciones. Además, los factores humanos, como la ingeniería social y la falta de conciencia de seguridad, pueden contribuir a la vulnerabilidad. La gestión de identidad y acceso, con contraseñas débiles o no cambiadas, también representa un riesgo. La ciberseguridad implica la identificación y gestión proactiva de vulnerabilidades, utilizando parches, actualizaciones y herramientas de escaneo para corregir y descubrir posibles debilidades en sistemas. En resumen, la comprensión y mitigación de vulnerabilidades son esenciales para preservar la integridad y confidencialidad de los sistemas y datos, requiriendo enfoques proactivos de parte de organizaciones e individuos.

2.- ¿Qué es seguridad?

La seguridad informática es un campo dinámico y vital que busca proteger los activos digitales en el ámbito tecnológico. Este campo multidimensional abarca diversos aspectos, incluyendo la integridad, confidencialidad, disponibilidad y autenticidad de datos y recursos digitales. La implementación de tecnologías como firewalls, medidas de cifrado y sistemas de autenticación son esenciales para crear una barrera efectiva contra amenazas externas e internas.

Además de las soluciones tecnológicas, se destaca la importancia de la educación y concienciación de los usuarios. La capacitación de empleados y la aplicación de políticas de seguridad son aspectos cruciales para fortalecer el eslabón humano en la cadena de seguridad. Por ejemplo, enseñar a los empleados a reconocer correos electrónicos de phishing o a utilizar contraseñas seguras puede reducir significativamente los riesgos de amenazas internas y mejorar la postura de seguridad global de una organización.

En un entorno donde las amenazas evolucionan constantemente, la seguridad informática no es solo una cuestión de tecnología, sino también de cultura organizacional y comportamiento de los usuarios. La implementación de estrategias holísticas que incluyan tanto soluciones tecnológicas avanzadas como la concienciación continua de los usuarios es esencial para enfrentar los desafíos actuales y futuros en el ámbito de la seguridad digital.

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

En el contexto de la seguridad informática, los pilares de confidencialidad, integridad, disponibilidad y autenticidad son fundamentales para la gestión efectiva de riesgos y la protección de activos digitales.

Confidencialidad: Implica garantizar que la información solo esté disponible para aquellos que tienen la autorización adecuada. Ejemplos de medidas de confidencialidad incluyen el cifrado de datos sensibles y el acceso restringido a información confidencial.

Integridad: Se refiere a la garantía de que los datos no se han alterado de manera no autorizada. Un ejemplo específico sería el uso de firmas digitales para verificar que un archivo no ha sido modificado desde su creación.

Disponibilidad: Asegura que los recursos y servicios digitales estén disponibles cuando se necesiten. Ejemplos prácticos incluyen la implementación de redundancia en servidores y la planificación de recuperación ante desastres.

Autenticidad: Verifica la legitimidad de las comunicaciones y la identidad de los usuarios. La aplicación de certificados digitales en comunicaciones en línea es un ejemplo que garantiza la autenticidad y evita ataques de suplantación de identidad.

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

Para proteger los datos, sistemas, redes y usuarios, las organizaciones emplean diversas estrategias. Un ejemplo adicional sería el uso de redes privadas virtuales (VPN) para cifrar el tráfico de red y garantizar la confidencialidad de la información transmitida, especialmente cuando se accede a datos sensibles desde ubicaciones remotas.

5.- ¿Escribe algunos ataques sobre los datos?

Ataques de Inyección: Más allá de la inyección SQL, los ataques de inyección también pueden involucrar scripts maliciosos en campos de entrada de datos, poniendo en riesgo la integridad y la autenticidad de las interacciones en línea.

Ataques de Phishing: Además de correos electrónicos, los ataques de phishing pueden manifestarse a través de mensajes de texto o llamadas telefónicas, ilustrando la necesidad de concientización continua para proteger la autenticidad y confidencialidad de la información personal.

Malware: Aparte de virus y troyanos, el adware, que muestra anuncios no deseados y recopila datos de navegación, sirve como ejemplo de amenaza que compromete la confidencialidad y disponibilidad de la información.

Ataques de Fuerza Bruta: Además de contraseñas, los ataques de fuerza bruta pueden dirigirse a códigos de autenticación, resaltando la necesidad de políticas de bloqueo de cuentas y medidas de seguridad adicionales para preservar la autenticidad y disponibilidad de los sistemas.

Ataques de Denegación de Servicio (DoS/DDoS): Más allá de saturar recursos, los ataques DDoS pueden involucrar técnicas avanzadas, como ataques de amplificación, que impactan la disponibilidad de servicios de manera más efectiva, destacando la necesidad de soluciones de mitigación de DDoS para garantizar la continuidad operativa.

6. ¿De qué nos protegemos?

En el ámbito de la seguridad informática, nos protegemos contra una amplia gama de amenazas que buscan comprometer la integridad, confidencialidad y disponibilidad de datos y sistemas digitales. Estas amenazas incluyen, pero no se limitan a, ataques de malware, intrusiones de red, robo de información confidencial, suplantación de identidad, pérdida de datos y más. La protección se extiende a salvaguardar tanto los aspectos técnicos, como los sistemas y redes, como los factores humanos, como la ingeniería social.

Ejemplo de Aplicación: Un ejemplo concreto sería la protección contra malware mediante el uso de software antivirus que escanea y elimina amenazas potenciales, evitando así la pérdida de datos y la comprometida integridad de los sistemas.

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

Las amenazas se materializan a menudo a través de vulnerabilidades en sistemas y aplicaciones. Algunos ejemplos incluyen:

Ataques de Inyección: Un atacante podría aprovechar vulnerabilidades en formularios web para inyectar código malicioso, comprometiendo la integridad y seguridad de la aplicación.

Explotación de Fallos de Software: Mediante vulnerabilidades en el código, un atacante podría ganar acceso no autorizado a sistemas y realizar acciones maliciosas como robo de datos.

Ejemplo de Aplicación: Para prevenir ataques de inyección, se implementan prácticas seguras de codificación y validación de entrada en las aplicaciones web.

8. ¿Menciona los tipos de vulnerabilidades?

Errores de Codificación: Fallos en el desarrollo de software que pueden ser aprovechados por atacantes.

Configuración Incorrecta: Ajustes de sistemas o aplicaciones que dejan abiertas puertas para posibles ataques.

Ejemplo de Aplicación: Evitar configuraciones predeterminadas no seguras en servidores y aplicaciones para prevenir accesos no autorizados.

9.- ¿Por qué aumentan las amenazas?

Las amenazas en el ámbito digital aumentan debido a varios factores.

Expansión Tecnológica: La creciente adopción de tecnologías digitales proporciona más oportunidades para ataques.

Complejidad de Sistemas: Sistemas más complejos a menudo presentan más vulnerabilidades que pueden ser explotadas.

Complejidad de Sistemas: Sistemas complejos a menudo tienen más vulnerabilidades que pueden ser explotadas.

Globalización: La conectividad global aumenta el alcance de los ataques, permitiendo a los atacantes operar desde cualquier parte del mundo.

Ingeniería Social Avanzada: Técnicas más sofisticadas para engañar a los usuarios y obtener información confidencial.

Ejemplo de Aplicación: La implementación de protocolos de seguridad robustos en sistemas complejos ayuda a mitigar amenazas derivadas de su complejidad.

10.- ¿Menciona tres protecciones más usadas ?

Firewalls:

Los firewalls son como guardianes digitales que protegen nuestras redes. Funcionan como filtros, permitiendo o bloqueando el tráfico según reglas establecidas. Imagina un firewall como el portero de una fiesta: decide quién entra y quién no. Puede bloquear intentos de acceso no autorizado y proporciona registros detallados para que los administradores puedan estar al tanto de lo que sucede en la red. Un ejemplo sería configurar el firewall para permitir solo el tráfico a través de ciertos puertos, evitando así que personas no invitadas entren a lugares no deseados.

Antivirus y Antimalware:

Estas herramientas actúan como detectives digitales, buscando y eliminando software malicioso que podría dañar nuestros sistemas. Son como los guardias de seguridad de un edificio, inspeccionando cada rincón para detectar comportamientos sospechosos. Los programas antivirus escanean archivos y aplicaciones en busca de patrones maliciosos, protegiendo nuestros sistemas

contra virus, gusanos y otros tipos de malware. Un ejemplo sería un antivirus que detecta y elimina un archivo adjunto de correo electrónico que podría contener un virus, manteniendo nuestros sistemas a salvo de infecciones no deseadas.

Actualizaciones y Parches de Seguridad:

Imagina que tu software es como un castillo, y las actualizaciones son las mejoras que refuerzan sus defensas. Las actualizaciones y parches de seguridad son como los arreglos que mantienen el castillo fuerte y resistente. Mantener nuestro software actualizado es crucial, ya que cada actualización corrige posibles vulnerabilidades y errores. Sin estas actualizaciones, nuestro castillo estaría expuesto a ataques. Un ejemplo sería aplicar un parche de seguridad en nuestro sistema operativo para cerrar una brecha que podría ser aprovechada por malware, asegurando así que nuestro castillo digital esté protegido contra las amenazas modernas.

11.-¿Que es amenaza?

En el ámbito de la seguridad informática, las amenazas pueden manifestarse de diversas maneras. Imagina un escenario donde un empleado recibe un correo electrónico no deseado que aparenta ser legítimo. Este correo electrónico contiene un virus informático oculto que, al ser activado al hacer clic en un enlace, puede comprometer la integridad de los archivos en la computadora y afectar el funcionamiento del sistema.

Además, considera a un atacante que intenta obtener acceso no autorizado a la red de una empresa. Utilizando técnicas de ingeniería social, el atacante podría hacerse pasar por un empleado legítimo y persuadir a otro empleado para que revele información confidencial o proporcione acceso a la red. Este tipo de amenaza pone en riesgo la confidencialidad de los datos empresariales y la seguridad de la red.

En este contexto, la identificación y comprensión de estas amenazas permiten implementar medidas de seguridad efectivas. Por ejemplo, la empresa podría proporcionar capacitación a los empleados sobre la detección de correos electrónicos fraudulentos y la importancia de no compartir información confidencial sin la verificación adecuada. Además, se podrían implementar soluciones de seguridad avanzadas, como software antivirus y sistemas de prevención de intrusiones, para proteger contra amenazas cibernéticas.

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

Geográficos y climáticos:

La ubicación geográfica y el clima pueden aumentar la susceptibilidad a ciertos desastres naturales, como terremotos, inundaciones, huracanes, etc.

Ejemplo: Una comunidad ubicada en una región propensa a huracanes implementa construcciones resistentes y planes de evacuación anticipados para mitigar los efectos de los eventos climáticos extremos.

Sociales y Económicos:

Factores como la densidad poblacional, pobreza, acceso a recursos y estructuras socioeconómicas afectan la capacidad de una comunidad para prepararse y recuperarse de desastres.

Ejemplo: Una zona con altos índices de pobreza invierte en programas de educación sobre preparación para desastres y acceso a recursos esenciales para fortalecer la resiliencia de la comunidad.

Infraestructura y Tecnología:

La calidad de la infraestructura y el acceso a tecnologías influyen en la capacidad de una región para resistir y recuperarse de eventos catastróficos.

Ejemplo: Una ciudad vulnerable a terremotos invierte en tecnologías de construcción sísmica y sistemas de alerta temprana para minimizar los daños y maximizar la capacidad de recuperación.

Gestión del Riesgo:

La efectividad de las estrategias y medidas de gestión del riesgo, incluyendo sistemas de alerta temprana y planes de evacuación, es esencial para reducir el impacto de los desastres.

Ejemplo: Un país con riesgo de incendios forestales implementa medidas preventivas, como cortafuegos y planes de evacuación, para gestionar de manera proactiva la amenaza de incendios.

Capacidades Comunitarias:

El nivel de conciencia, preparación y resiliencia de la comunidad juega un papel crucial en la respuesta y recuperación después de un desastre.

Ejemplo: Una comunidad costera con historial de tsunamis realiza simulacros regulares, educando a los residentes sobre las acciones a tomar en caso de emergencia y fortaleciendo así su capacidad de respuesta.

13.- ¿Que es la ingeniería social?

La ingeniería social es una táctica astuta empleada por ciberdelincuentes para aprovechar la psicología humana y obtener acceso no autorizado a información confidencial o sistemas. En lugar de atacar directamente sistemas informáticos, esta estrategia se enfoca en la manipulación psicológica y social. Ejemplos incluyen la suplantación de identidad, donde los atacantes se hacen pasar por individuos confiables, y el phishing, que implica el envío de mensajes fraudulentos para engañar a las personas y obtener información sensible.

Como se aplica:

Visualiza recibir un correo electrónico aparentemente legítimo de tu banco solicitando información urgente. Aunque el mensaje parece genuino, podría tratarse de un intento de phishing, donde los atacantes buscan obtener datos bancarios aprovechando la urgencia percibida.

14.- ¿Que son los virus informáticos?

Los virus informáticos son programas maliciosos diseñados para infiltrarse en sistemas y replicarse, propagándose de un archivo a otro. Estos programas pueden causar daños significativos corrompiendo archivos, robando información o afectando el rendimiento del sistema. La propagación de virus puede ocurrir a través de archivos adjuntos, descargas en línea o dispositivos extraíbles, y a menudo requieren la intervención del usuario para activarse.

Donde se aplica:

Imagina descargar un archivo desde un sitio web aparentemente seguro. Sin saberlo, el archivo contiene un virus que se instala en tu computadora, dañando archivos importantes y afectando el rendimiento del sistema.

15.- ¿Define el Concepto de autenticación?

La autenticación es el proceso esencial de verificar la identidad de un usuario, dispositivo o entidad para asegurar el acceso autorizado a recursos específicos. Se realiza mediante la presentación de credenciales como contraseñas, tarjetas de identificación, huellas dactilares o certificados digitales. Este procedimiento es crucial en la seguridad informática para prevenir accesos no autorizados y proteger la confidencialidad de la información.

Ejemplo de cómo se utiliza:

Cuando intentas acceder a tu cuenta en línea, proporcionas un nombre de usuario y una contraseña. Si estos datos coinciden con la información almacenada, el sistema autentica tu identidad y te

concede acceso a la cuenta. La autenticación garantiza que solo las personas autorizadas tengan acceso a recursos protegidos.

16.- ¿Mecanismos preventivos en seguridad informática?

Los mecanismos preventivos en seguridad informática constituyen estrategias diseñadas para prevenir activamente la ocurrencia de amenazas y salvaguardar los sistemas contra potenciales ataques. Estas medidas se implementan en diversas capas de seguridad, fortaleciendo la resistencia frente a posibles vulnerabilidades.

Firewalls:

Descripción: Firewalls actúan como barreras de seguridad, supervisando y controlando el flujo de tráfico de red mediante reglas predefinidas.

Aplicación: Su implementación en redes corporativas previene intrusiones no autorizadas desde el exterior.

Sistemas de Detección de Intrusiones (IDS):

Descripción: IDS monitorizan actividades en tiempo real, identificando comportamientos sospechosos o patrones de ataques conocidos.

Aplicación: Utilizados en servidores y redes para detectar y responder a posibles intrusiones.

Actualizaciones y Parches de Seguridad:

Descripción: Consiste en mantener actualizado el software, sistemas operativos y aplicaciones con los últimos parches de seguridad para corregir vulnerabilidades conocidas.

Aplicación: Aplicado a nivel de sistemas y software en todos los dispositivos conectados a la red.

Educación y Concientización del Usuario:

Descripción: Programas de formación orientados a usuarios sobre prácticas seguras en línea y reconocimiento de posibles amenazas.

Aplicación: Implementados en entornos empresariales y educativos para mitigar el riesgo de ataques por factores humanos.

17.- ¿Mecanismos correctivos en seguridad informática?

Los mecanismos correctivos en seguridad informática se concentran en responder y mitigar los impactos una vez que ha ocurrido un incidente de seguridad.

Sistemas de Respuesta a Incidentes (IR):

Descripción: Establecimiento de procedimientos y protocolos para gestionar y responder efectivamente a incidentes de seguridad.

Aplicación: Implementados en organizaciones para coordinar acciones cuando se detecta una amenaza.

Copias de Seguridad y Recuperación de Datos:

Descripción: Implica realizar copias de seguridad periódicas de datos críticos y establecer procesos para su recuperación rápida en caso de pérdida.

Aplicación: Utilizado en servidores y sistemas críticos para asegurar la continuidad del negocio.

Análisis Forense Digital:

Descripción: Investigación exhaustiva para determinar el alcance y origen de un incidente de seguridad.

Aplicación: Se utiliza después de un ataque para comprender su desarrollo y tomar medidas correctivas.

Gestión de Vulnerabilidades:

Descripción: Implica la identificación y corrección proactiva de vulnerabilidades en sistemas y aplicaciones.

Aplicación: Realizado de forma continua para garantizar la protección de los sistemas contra las últimas amenazas.

Estos enfoques son fundamentales no solo para la seguridad de la información, sino que también se aplican en entornos empresariales, gubernamentales y personales, asegurando la protección y disponibilidad de los recursos digitales.

18.- ¿Qué es el aumento de privilegios?

El aumento de privilegios, también conocido como elevación de privilegios, es un proceso mediante el cual un usuario o aplicación adquiere permisos o privilegios mayores de los que originalmente poseía en un sistema informático. Esto puede permitir realizar acciones que, de otra manera,

estarían restringidas. La finalidad del aumento de privilegios puede variar, desde mejorar la funcionalidad de una aplicación hasta facilitar acciones maliciosas. Este concepto es crítico en seguridad informática, ya que el acceso no autorizado a privilegios elevados representa un riesgo significativo para la integridad y seguridad de un sistema.

Aplicación del Aumento de Privilegios:

La aplicación del aumento de privilegios se refiere a maniobras maliciosas realizadas por atacantes con el objetivo de obtener un mayor nivel de acceso o control del que normalmente les ha sido asignado en un sistema. Este proceso implica que los atacantes buscan elevar sus permisos para llevar a cabo acciones que, de otra manera, estarían restringidas, puede manifestarse mediante la explotación de debilidades en sistemas operativos, aplicaciones, redes empresariales, entornos web, o incluso mediante tácticas internas como el escalamiento de privilegios por parte de empleados malintencionados.

Sistemas Operativos:

En sistemas operativos como Windows y Linux, los ataques de aumento de privilegios son un objetivo común. Los atacantes buscan vulnerabilidades para elevar sus privilegios y ganar un mayor control sobre el sistema, el aumento de privilegios es un componente clave en la gestión de la seguridad informática, y la implementación de prácticas sólidas, como la limitación de privilegios a niveles estrictamente necesarios, es fundamental para mitigar riesgos y proteger la integridad de los sistemas.

Aplicaciones y Servicios:

Algunas aplicaciones y servicios requieren privilegios específicos para funcionar correctamente. Los usuarios pueden necesitar elevar sus privilegios para realizar tareas de administración o configuración.

Escenarios de Ataque:

Los ciberdelincuentes utilizan técnicas de aumento de privilegios en escenarios de ataque, como la explotación de vulnerabilidades en el kernel del sistema operativo o la manipulación de configuraciones débiles de servicios.

Desarrollo de Software: En el desarrollo de software, los programadores pueden requerir privilegios elevados para compilar, depurar o realizar otras tareas críticas. Sin embargo, es esencial gestionar estos privilegios de manera segura.

Administración de Sistemas:

Los administradores de sistemas pueden necesitar aumentar sus privilegios para llevar a cabo tareas de mantenimiento, instalación de software o solución de problemas.

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

Es esencial para la seguridad de sistemas en entornos Windows y Linux aplicar medidas sólidas, como mantener actualizados los sistemas, configurar adecuadamente los permisos, utilizar contraseñas robustas y monitorear activamente posibles intentos de aumento de privilegios. Estas prácticas contribuyen eficazmente a prevenir ataques que buscan obtener privilegios no autorizados y salvaguardar la integridad de los sistemas.

Windows:

Explotación de Vulnerabilidades:

Malwares aprovechan debilidades en el sistema operativo para obtener permisos más altos, accediendo a funciones críticas del sistema.

Uso de Herramientas Específicas:

Herramientas como Mimikatz se utilizan para extraer credenciales almacenadas, lo que posibilita a los atacantes elevar sus privilegios y obtener control sobre el sistema.

Ataques a Servicios y Configuraciones Débiles:

Explotar servicios mal configurados proporciona a los atacantes acceso a niveles de privilegios superiores, facilitando el movimiento lateral en la red.

Linux:

Explotación de Vulnerabilidades del Kernel:

Atacantes buscan debilidades en el núcleo de Linux para obtener privilegios elevados, lo que les concede un control más profundo sobre el sistema.

Uso de Sudo y Escalamiento de Privilegios:

Aprovechar configuraciones de sudo débilmente protegidas permite a los atacantes obtener acceso con privilegios adicionales, comprometiendo la seguridad del sistema.

Manipulación de Archivos de Configuración:

Modificar archivos de configuración brinda a los atacantes la capacidad de ejecutar comandos con mayores privilegios, lo que puede conducir a la toma completa del sistema.

Ataques a Servicios y Usuarios Débiles:

Explotar servicios débiles o contraseñas de usuario facilita el escalamiento de privilegios, siendo una táctica común en los vectores de ataque.

20.- ¿Protección frente al aumento de privilegios?

Esta información y las prácticas asociadas para la protección frente al aumento de privilegios son aplicadas en diversos entornos, tanto empresariales como personales, con el objetivo de salvaguardar la integridad y seguridad de los sistemas informáticos, la protección frente al aumento de privilegios se aplica en cualquier entorno donde la seguridad de la información y la integridad de los sistemas son fundamentales. Desde entornos empresariales hasta dispositivos personales, estas prácticas son esenciales para mitigar los riesgos asociados con posibles ataques que buscan obtener privilegios no autorizados.

Entornos Empresariales y Organizaciones:

Las empresas implementan estas medidas para proteger sus redes, sistemas y datos empresariales críticos.

La aplicación del principio de menor privilegio y la auditoría de permisos son fundamentales en entornos corporativos para gestionar el acceso a la información confidencial.

El monitoreo continuo y la respuesta proactiva a posibles intentos de aumento de privilegios son esenciales para la seguridad de la red empresarial.

Infraestructuras Gubernamentales:

Organizaciones gubernamentales adoptan estas prácticas para asegurar la confidencialidad y la integridad de la información gubernamental sensible.

El control de acceso basado en roles se implementa para gestionar los privilegios de los usuarios de manera estructurada y conforme a las responsabilidades laborales en instituciones gubernamentales.

Entornos de Servidores y Nubes:

En entornos de servidores y servicios en la nube, estas prácticas son aplicadas para proteger los recursos y datos almacenados.

La segregación de redes y la protección contra malware son cruciales en servidores para prevenir la propagación de amenazas y limitar el impacto de posibles ataques.

Ambientes Personales y de Usuarios Finales:

Los individuos aplican estas medidas para proteger sus dispositivos personales, como computadoras y dispositivos móviles, la concientización del usuario sobre prácticas seguras en línea y la gestión de contraseñas robustas son esenciales para prevenir ataques dirigidos a usuarios finales.

Sistemas Críticos y de Infraestructura Nacional: En sectores críticos, como el energético o de transporte, estas prácticas se implementan para garantizar la seguridad y operatividad continua de infraestructuras esenciales.

Conclusión

En conclusión, la seguridad informática es un campo integral y dinámico que aborda la protección de sistemas, datos y usuarios contra amenazas digitales, se centra en la gestión proactiva de vulnerabilidades y la aplicación de medidas preventivas y correctivas. Los pilares de confidencialidad, integridad, disponibilidad y autenticidad guían las estrategias de seguridad, las amenazas, que van desde ataques de malware hasta ingeniería social avanzada, buscan comprometer la seguridad de la información, las vulnerabilidades, como errores de codificación o configuraciones incorrectas, son explotadas por estas amenazas, el aumento de privilegios representa un riesgo crítico, y su prevención es esencial para salvaguardar la integridad de sistemas operativos y aplicaciones.

La implementación de mecanismos preventivos, como firewalls y sistemas de detección de intrusiones, junto con prácticas educativas y de concientización del usuario, contribuyen a fortalecer la postura de seguridad. Por otro lado, los mecanismos correctivos, como la respuesta a incidentes y análisis forense digital, son esenciales para mitigar los impactos de posibles violaciones de seguridad, la protección frente al aumento de privilegios se extiende a diversos entornos, desde empresas hasta sistemas críticos y dispositivos personales. La aplicación del principio de menor privilegio, la auditoría de permisos y la concientización del usuario son elementos clave en la prevención de intentos maliciosos de obtener privilegios no autorizados, la seguridad informática requiere enfoques holísticos y la colaboración de tecnologías avanzadas, políticas organizacionales sólidas y la participación activa de los usuarios para hacer frente a las crecientes amenazas en el ámbito digital.

BIBLIOGRAFIAS:

Cano, J. (2015). *Computación forense*. Alpha Editorial.

GABRIELA, G. V. M., & PATRICIO, O. V. D. (2015). DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN.

JUMBO DELGADO, R. V. (2019). *ANÁLISIS DE VULNERABILIDADES DE REDES INALÁMBRICAS PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS EN EL LABORATORIO DE TELECOMUNICACIONES DE LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES* (Bachelor's thesis, Jipijapa-UNESUM).

Amaro López, J. A., & Rodríguez Rodríguez, C. R. (2017). Seguridad en internet. *PAAKAT: revista de tecnología y sociedad*, *6*(11).

Vega, G., Napoleón, R., & Moscoso Montalvo, P. E. (2011). *Evaluación técnica de la seguridad informática del data center de la escuela politécnica del ejército*. SANGOLQUI/ESPE/2011, SANGOLQUI.

Urbina, G. B. (2017). *Introducción a la seguridad informática*. Grupo editorial PATRIA.

Gómez Vieites, Á. (2011). Enciclopedia de la seguridad informática.

Tandazo Tipan, A. A. (2022). *Plan de seguridad informática aplicando la norma iso-27001 para la protección de activos informáticos en la empresa "Rav"* (Bachelor's thesis).

Mieres, J. (2009). Buenas prácticas en seguridad informática. *ESET, LLC. Disponible en: http://www. esetla. com/pdf/prensa/informe/buenas_practicas_seguridad_informatica. pdf*.

López Grande, C. E. (2015). Ingeniería social: el ataque silencioso. *Revista Tecnológica: no. 8*.

Huerta, D. (2010). Ingeniería social. *Revista de Derecho Informático*, *43*.

Canes Fauces, D. M., Pérez Infante, Y., & Callis Fernández, S. (2011). Acerca de los virus informáticos: una amenaza persistente. *Medisan*, *15*(2), 257-260.

de Colmenares, F. D. L. C. (2002). Virus informáticos. *Informática y derecho: revista iberoamericana de derecho informático*, (34), 67-88.

Torres Crego, A. (2016). *Desarrollo de un mecanismo de autenticación centralizada para el entorno de aplicaciones de la UCI* (Bachelor's thesis, Universidad de las Ciencias Informáticas. Facultad-5).

Ríos, N. R. T., í lvarez Morales, E. L., & Sandoya, S. D. C. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista Publicando*, *4*(10 (2)), 462-473.

Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (Vol. 46). 3Ciencias.

Romero, M. I., Figueroa, G. L., Vera, D. S., Álava, J. E., Parrales, G. R., Álava, C. J., ... & Castillo, M. A. (2018). Mecanismo Correctivos en seguridad informática. *Introducción a la seguridad informática y el análisis de vulnerabilidades*.

Giraldo Ramírez, J. J. (2022). Herramienta de Ciberseguridad para la auditoría de una línea base de buenas prácticas de seguridad informática en Pymes a través de un prototipo funcional de Chatbot que ofrezca recomendaciones para la mitigación de vulnerabilidades en servidores Windows y Linux.