

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

SUB1 - INTRODUCCIÓN AL PENTESTING

A. 1.3 INVESTIGACIÓN DE LOS SIGUIENTES CONCEPTOS

ALUMNO: **MARCO ANTONIO ZÚÑIGA MORALES – A211121**

DOCENTE: **DR. LUIS GUTIÉRREZ ALFARO**

TUXTLA GUTIÉRREZ, CHIAPAS
VIERNES, 9 DE FEBRERO DE 2024

Índice

Introducción	3
Desarrollo	4
1. ¿Qué es vulnerabilidad?	4
2. ¿Qué es seguridad?	4
3. ¿Escribe los pilares de la seguridad? (confidencialidad, integridad, disponibilidad, autenticidad.).....	5
4. ¿La seguridad en informática intenta proteger cuatro elementos cuáles son?	6
5. ¿Escribe algunos ataques sobre los datos?	6
6. ¿De qué nos protegemos?	7
7. ¿Menciona algunas amenazas que se concrete por medio de una vulnerabilidad? .	7
8. ¿Menciona los tipos de vulnerabilidades?	8
9. ¿Por qué aumentan las amenazas?	9
10. ¿Menciona tres protecciones más usadas?	10
11. ¿Qué es amenaza?	10
12. ¿Factores del riesgo de desastres desde el enfoque holístico?	11
13. ¿Qué es la ingeniería social?	11
14. ¿Que son los virus informáticos?	12
15. ¿Define el Concepto de autenticación?	13
16. ¿Mecanismos preventivos en seguridad informática?	13
17. ¿Mecanismos correctivos en seguridad informática?	14
18. ¿Qué es el aumento de privilegios?	15
19. ¿Técnicas de aumento de privilegios en Windows y/o Linux?	16
20. ¿Protección frente al aumento de privilegios?	17
Conclusión	18
Referencia Bibliográfica	19

Introducción

En la era digital actual, la seguridad informática se ha convertido en un pilar fundamental para la protección de la información y los sistemas que la procesan. A medida que avanzamos tecnológicamente, la complejidad y sofisticación de las amenazas cibernéticas también evolucionan, presentando desafíos únicos y constantes para individuos, organizaciones y gobiernos a nivel mundial. Este documento tiene como objetivo explorar de manera exhaustiva los conceptos clave, desafíos y estrategias relacionadas con la seguridad informática y el análisis de vulnerabilidades, proporcionando una visión integral sobre cómo proteger nuestros activos digitales en un panorama de amenazas en constante cambio.

Comenzaremos definiendo la naturaleza de las vulnerabilidades en sistemas informáticos y la importancia de la seguridad para mitigar los riesgos asociados a estas debilidades. Profundizaremos en los pilares fundamentales de la seguridad informática: confidencialidad, integridad, disponibilidad y autenticidad, y cómo estos principios guían la protección de los datos y los sistemas contra accesos no autorizados y ataques malintencionados.

Exploraremos los cuatro elementos esenciales que la seguridad informática intenta proteger: los datos, las aplicaciones, la infraestructura y los usuarios. Cada uno de estos elementos enfrenta amenazas específicas que requieren estrategias de defensa adaptadas. Se analizarán los ataques más comunes sobre los datos, incluyendo phishing, ransomware, inyecciones SQL y ataques de denegación de servicio distribuido (DDoS), para comprender mejor de qué nos protegemos y cómo las vulnerabilidades pueden ser explotadas.

Este documento también discutirá la naturaleza de las amenazas, su relación con las vulnerabilidades existentes y el aumento de estas amenazas en el contexto actual. Abordaremos los tipos de vulnerabilidades más comunes y las razones detrás del incremento en el número y sofisticación de las amenazas cibernéticas. Además, se presentarán las protecciones más utilizadas en la industria, incluyendo firewalls, soluciones antivirus y antimalware, y el cifrado de datos, como medios efectivos para mitigar los riesgos.

Profundizaremos en conceptos como la ingeniería social, los virus informáticos, la autenticación, y los mecanismos preventivos y correctivos en seguridad informática. Se examinará el desafío del aumento de privilegios, sus técnicas en sistemas operativos como Windows y Linux, y las estrategias de protección frente a estos ataques. Con un enfoque holístico, este documento pretende no solo informar sobre los desafíos y soluciones en la seguridad informática, sino también fomentar una cultura de seguridad consciente y proactiva, donde la prevención, detección y respuesta a incidentes sean componentes clave de una estrategia integral de seguridad.

Desarrollo

1. ¿Qué es vulnerabilidad?

Una vulnerabilidad en el contexto de la seguridad informática se refiere a una debilidad, fallo o error en el diseño, implementación, operación o gestión de un sistema de información, que podría ser explotada por una amenaza para violar la seguridad del sistema. Esto incluye vulnerabilidades en el software, hardware o en los procesos y políticas de seguridad.

La explotación de una vulnerabilidad puede resultar en una amplia gama de impactos negativos, incluyendo, pero no limitado a:

- Acceso no autorizado a datos sensibles o personales.
- Denegación de servicio (DoS), donde los servicios legítimos se vuelven inaccesibles para los usuarios.
- Ejecución de código arbitrario por parte del atacante, lo que puede llevar a la toma de control total del sistema afectado.
- Escalada de privilegios, permitiendo a un atacante obtener mayores niveles de acceso de los que originalmente poseía.

Las vulnerabilidades son identificadas a través de varias metodologías, incluyendo análisis de código, pruebas de penetración, y el uso de herramientas automatizadas de escaneo de vulnerabilidades. Una vez identificadas, es crítico aplicar las medidas correctivas apropiadas, que pueden incluir la aplicación de parches de seguridad, cambios en la configuración del sistema, o incluso la sustitución de componentes del sistema vulnerables.

La gestión de vulnerabilidades es un aspecto crítico de la seguridad de la información y requiere un enfoque proactivo para identificar, clasificar, remediar y mitigar vulnerabilidades, con el fin de proteger los activos de información contra posibles amenazas.

2. ¿Qué es seguridad?

La seguridad, en términos generales, se refiere a la protección contra daños, pérdidas o ataques. En el contexto de la informática, se refiere específicamente a la protección de la información y los sistemas de información contra el acceso no autorizado, divulgación, alteración, destrucción o interrupción, ya sea de forma accidental o maliciosa.

La seguridad en TI también se enfoca en prevenir ataques de ciberdelincuentes y mitigar el impacto de cualquier brecha de seguridad.

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

Los pilares fundamentales de la seguridad informática son:

- **Confidencialidad:** Garantizar que la información es accesible solo para aquellos autorizados a tener acceso.

Se refiere a la protección de la información para que solo las personas o sistemas autorizados puedan acceder a ella. La confidencialidad asegura que la información sensible, como datos personales, secretos comerciales o información gubernamental clasificada, se mantenga privada y no sea accesible por individuos no autorizados. Técnicas como el cifrado, el control de acceso basado en roles y las políticas de privacidad ayudan a mantener la confidencialidad de los datos.

- **Integridad:** Asegurar la precisión y completitud de la información y los métodos de procesamiento.

Este principio se centra en asegurar que la información sea precisa y no haya sido alterada de forma no autorizada. La integridad garantiza que los datos sean confiables y se mantengan tal como fueron creados, enviados o almacenados, sin modificaciones, borrados o daños. Se puede mantener la integridad mediante el uso de sumas de verificación, firmas digitales y sistemas de control de versiones.

- **Disponibilidad:** Asegurar que la información y los recursos relacionados estén disponibles para los usuarios autorizados cuando sean necesarios.

La disponibilidad implica proteger los sistemas contra ataques que puedan interrumpir el servicio, como ataques de denegación de servicio (DoS), y también incluye medidas de redundancia, sistemas de respaldo y planes de recuperación ante desastres para garantizar que los servicios puedan continuar o ser restaurados rápidamente después de un incidente.

- **Autenticidad:** Verificación de que los usuarios son quienes dicen ser y que cada input llega de una fuente fiable.

La autenticidad es crucial para establecer confianza en las comunicaciones y transacciones electrónicas. Implica el uso de contraseñas, tokens de seguridad, certificados digitales y biometría para asegurar que solo los usuarios autorizados puedan acceder a los recursos y servicios.

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

La seguridad informática se enfoca en proteger:

- **Datos:** Información almacenada y procesada por los sistemas.
- **Aplicaciones:** Software que procesa los datos.
- **Infraestructura:** Componentes físicos y lógicos que soportan el procesamiento y almacenamiento de datos.
- **Usuarios:** Personas que acceden y usan los sistemas y datos.

5. ¿Escribe algunos ataques sobre los datos?

Los ataques sobre los datos representan una de las principales preocupaciones en el ámbito de la ciberseguridad, ya que buscan comprometer la confidencialidad, integridad y disponibilidad de la información.

Algunos ataques comunes incluyen:

- **Phishing:** Engañar a los usuarios para que entreguen información confidencial.
- **Ransomware:** Encriptar datos y exigir un rescate para su liberación.
- **SQL Injection:** Insertar o "inyectar" código malicioso en bases de datos a través de aplicaciones web.
- **DDoS (Distributed Denial of Service):** Sobrecargar un sistema con tráfico para hacerlo inaccesible.
- **Intercepción o Espionaje Electrónico (Eavesdropping):** Este tipo de ataque implica la captura no autorizada de datos que se están transmitiendo a través de una red. Los atacantes pueden interceptar comunicaciones para robar información sensible, como contraseñas, datos financieros o secretos comerciales.

6. ¿De qué nos protegemos?

Nos protegemos de:

- Accesos no autorizados.
- Robo de información.
- Daños o alteraciones de datos.
- Interrupciones del servicio.
- Malware
- Ataques de ingeniería social
- Ataques de red
- Vulnerabilidades del software y del hardware
- Errores humanos
- Amenazas internas

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

Las amenazas que se materializan a través de vulnerabilidades en sistemas informáticos pueden adoptar diversas formas, explotando debilidades específicas para comprometer la seguridad de los datos, sistemas y redes.

Algunas de estas amenazas incluyen:

- **Exploits:** Código, secuencias de comandos o comandos que aprovechan una vulnerabilidad.
- **Malware:** Software malicioso diseñado para dañar o realizar acciones no autorizadas.
- **Ataques de fuerza bruta:** Intentos de adivinar contraseñas o claves mediante la repetición de intentos.
- **Ejecución de código remoto:** Permite a un atacante ejecutar código arbitrario en un sistema afectado desde una ubicación remota.
- **Inyección de SQL:** Explota vulnerabilidades en aplicaciones que interactúan con bases de datos SQL, permitiendo a los atacantes manipular o robar datos.
- **Cross-Site Scripting (XSS):** Permite inyectar scripts maliciosos en páginas web para robar información de sesión o acceder a cuentas de usuario.

- **Desbordamiento de búfer:** Ocurre cuando se escribe más información en un búfer de lo que puede contener, lo que puede llevar a la ejecución de código arbitrario.
- **Ataques de día cero:** Explotan vulnerabilidades desconocidas para los desarrolladores y el público hasta el momento del ataque.
- **Elevación de privilegios:** Permite a un atacante obtener mayores niveles de acceso en el sistema, a menudo control total sobre este.
- **Ataques de reinyección:** Involucran la captura y retransmisión de datos legítimos para realizar acciones no autorizadas.
- **Ataques Man-in-the-Middle (MitM):** Interceptan, modifican o reenvían datos entre dos partes sin su conocimiento.
- **Ransomware:** Cifra archivos del usuario y exige un rescate para su descifrado, aprovechando software no actualizado.
- **Ataques de phishing:** Utilizan ingeniería social y pueden explotar vulnerabilidades de software para robar credenciales.

8. ¿Menciona los tipos de vulnerabilidades?

- **Vulnerabilidades de software:** Errores de código que pueden ser explotados.

Ejemplo: Una vulnerabilidad de inyección SQL en una aplicación web que permite a un atacante ejecutar comandos SQL arbitrarios en la base de datos de la aplicación.

- **Vulnerabilidades de configuración:** Configuraciones incorrectas o inseguras de sistemas o aplicaciones.

Ejemplo: Un servidor web configurado para permitir el listado de directorios, lo que podría exponer archivos y carpetas sensibles a un atacante.

- **Vulnerabilidades físicas:** Acceso físico no autorizado a instalaciones o hardware.

Ejemplo: Falta de protección adecuada contra el acceso físico a servidores en un centro de datos, permitiendo a alguien robar o dañar hardware crítico.

- **Vulnerabilidades de diseño:** Deficiencias en la arquitectura de sistemas o protocolos de comunicación.

Ejemplo: Un protocolo de autenticación que transmite credenciales en texto plano, susceptible a interceptación.

- **Vulnerabilidades de autenticación:** Debilidades en mecanismos de autenticación que pueden permitir a un atacante eludir la autenticación o suplantar a otro usuario.

Ejemplo: Uso de contraseñas predeterminadas o débiles que pueden ser fácilmente adivinadas o crackeadas.

- **Vulnerabilidades de autorización:** Fallos en los controles que determinan qué acciones pueden realizar los usuarios autenticados.

Ejemplo: Una aplicación web que permite a un usuario sin privilegios acceder a funciones administrativas debido a controles de autorización inadecuados.

- **Vulnerabilidades criptográficas:** Debilidades en la implementación de algoritmos criptográficos o en su uso.

Ejemplo: Uso de cifrado débil que puede ser roto con técnicas de fuerza bruta o explotando vulnerabilidades conocidas en algoritmos específicos.

- **Vulnerabilidades de denegación de servicio (DoS):** Debilidades que pueden ser explotadas para hacer que un recurso de sistema o red sea inaccesible a los usuarios legítimos.

Ejemplo: Una vulnerabilidad en un servidor web que permite a un atacante enviar solicitudes especialmente diseñadas que consumen todos los recursos disponibles, causando un colapso del servicio.

9. ¿Por qué aumentan las amenazas?

El aumento de las amenazas en el ámbito de la seguridad informática se debe a una combinación de factores tecnológicos, económicos y sociales.

Las amenazas aumentan debido a:

- Avances tecnológicos que crean nuevas vulnerabilidades.
- Mayor dependencia de sistemas digitales, lo que aumenta el valor de los objetivos.

- Crecimiento de la superficie de ataque con más dispositivos conectados.
- Mayor sofisticación de los atacantes.
- Ataques automatizados y herramientas de hacking accesibles.
- Lagunas en la aplicación de parches y mantenimiento de seguridad.

10. ¿Menciona tres protecciones más usadas?

En el ámbito de la seguridad informática, hay varias medidas de protección clave que son ampliamente utilizadas por organizaciones y usuarios individuales para defenderse contra amenazas y vulnerabilidades.

Tres de las protecciones más comunes son las siguientes:

- **Firewalls:** Para filtrar el tráfico de red no deseado.
- **Antivirus y antimalware:** Para detectar y eliminar software malicioso.
- **Cifrado de datos:** Para proteger la confidencialidad e integridad de los datos durante su almacenamiento y transmisión.

11. ¿Qué es amenaza?

Una amenaza es cualquier circunstancia o evento con el potencial de causar daño a un sistema de información a través de la destrucción, divulgación, modificación de datos, o denegación de servicios. Las amenazas pueden ser intencionales (como los ataques cibernéticos) o accidentales (como un error humano o fallos de software).

Las amenazas se clasifican generalmente según su naturaleza y origen en categorías como:

- **Amenazas internas:** Proviene de individuos dentro de la organización, como empleados, contratistas o socios de negocio, que tienen acceso legítimo a los sistemas y datos pero pueden actuar con intenciones maliciosas o cometer errores que comprometan la seguridad.
- **Amenazas externas:** Originadas por individuos o grupos fuera de la organización, como hackers, espías cibernéticos, y grupos de ciberdelincuencia, que buscan acceder a sistemas y datos de manera no autorizada para robar, alterar o destruir información.
- **Malware:** Software malicioso diseñado específicamente para dañar, interrumpir o realizar acciones no autorizadas en un sistema informático.

- **Amenazas naturales:** Desastres naturales como terremotos, inundaciones o incendios que pueden dañar la infraestructura física de TI.
- **Errores y fallos técnicos:** Incluyen fallos de software o hardware, así como errores de configuración o de operación cometidos por empleados, que pueden llevar a vulnerabilidades de seguridad.

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

Desde un enfoque holístico, los factores de riesgo de desastres incluyen:

- **Amenazas naturales y humanas:** Como terremotos, inundaciones, ataques cibernéticos.
- **Vulnerabilidades:** Fallos en sistemas, infraestructuras o en la preparación de la comunidad.
- **Exposición:** Elementos en riesgo, como personas, bienes, servicios.
- **Capacidad de respuesta y adaptación:** Habilidad de una comunidad o sistema para gestionar y recuperarse de los efectos de un desastre.
- **Gestión de Riesgos y Políticas Públicas:** Estrategias y medidas implementadas para reducir el riesgo de desastres, incluyendo planificación, infraestructura resiliente y educación.
- **Cambio Climático y Degradación Ambiental:** Factores que aumentan la frecuencia e intensidad de algunos desastres naturales y afectan la vulnerabilidad de las comunidades.
- **Factores Socioeconómicos y Culturales:** Incluyen la distribución de recursos, desigualdad social y prácticas culturales que afectan la capacidad de las comunidades para enfrentar desastres.

13. ¿Qué es la ingeniería social?

La ingeniería social es una técnica de manipulación que explota las debilidades humanas para obtener información confidencial, acceso no autorizado o para inducir a los usuarios a realizar acciones que podrían comprometer la seguridad. Se basa en engañar a las personas en lugar de hackear sistemas informáticos directamente.

Los atacantes que emplean la ingeniería social a menudo se presentan como una fuente confiable o autorizada, como un colega, un departamento de TI, una entidad bancaria o una organización gubernamental, para persuadir a sus víctimas de que proporcionen información sensible, como contraseñas, datos de tarjetas de crédito o información personal identificable.

También pueden convencer a los usuarios para que realicen acciones específicas, como descargar un archivo adjunto malicioso, visitar un sitio web fraudulento o realizar una transferencia de dinero.

Algunos ejemplos comunes de ataques de ingeniería social son:

- **Phishing:** Envío de correos electrónicos que parecen provenir de fuentes legítimas solicitando a los destinatarios que revelen información personal o financiera.
- **Pretexto:** Creación de un escenario falso o una historia convincente para obtener información sensible o acceso físico a instalaciones.
- **Baiting:** Ofrecimiento de algo tentador, como la descarga gratuita de software, para engañar a los usuarios para que instalen malware o revelen información confidencial.
- **Tailgating o Piggybacking:** Acceder físicamente a un área restringida siguiendo a alguien con acceso legítimo sin ser detectado.
- **Quid pro quo:** Ofrecer un beneficio, como asistencia técnica gratuita, a cambio de información o acceso.

14. ¿Que son los virus informáticos?

Los virus informáticos son programas maliciosos diseñados para replicarse y propagarse de un dispositivo a otro, interfiriendo con el funcionamiento del software. Pueden dañar archivos, robar información, o incluso tomar el control de dispositivos afectados.

Los virus pueden ser programados para realizar una amplia gama de acciones maliciosas como las siguientes:

- **Corrupción de Datos:** Pueden dañar o eliminar archivos, afectando la operación del sistema o la disponibilidad de datos importantes.
- **Ralentización de Sistemas:** Consumen recursos del sistema, lo que puede ralentizar o incluso colapsar el sistema infectado.

- **Robo de Información:** Algunos están diseñados para robar información sensible del usuario, como contraseñas, números de tarjetas de crédito y otros datos personales.
- **Creación de Backdoors:** Pueden crear puertas traseras en el sistema infectado, permitiendo a los atacantes un acceso remoto al dispositivo.
- **Propagación:** Se replican y se propagan a otros dispositivos a través de la red, correos electrónicos, programas de software o archivos compartidos.

15. ¿Define el Concepto de autenticación?

La autenticación es el proceso de verificar la identidad de un usuario o dispositivo, usualmente antes de conceder acceso a recursos o servicios. Se basa en la presentación de credenciales, como contraseñas, tokens, huellas digitales, o cualquier forma de identificación que confirme que el usuario es quien dice ser.

La autenticación es un componente fundamental de la seguridad informática y se emplea para proteger contra accesos no autorizados y asegurar que solo los usuarios legítimos puedan acceder a los datos y funciones relevantes.

16. ¿Mecanismos preventivos en seguridad informática?

Los mecanismos preventivos son estrategias y herramientas diseñadas para prevenir incidentes de seguridad antes de que ocurran, protegiendo los sistemas, redes y datos contra accesos no autorizados, ataques, malwares y otras amenazas.

Algunos de los mecanismos preventivos en la seguridad informática son los siguientes:

- **Políticas de seguridad:** Directrices y procedimientos para proteger los recursos.
- **Control de acceso:** Limitar el acceso a información y recursos a usuarios autorizados.
- **Educación y concienciación en seguridad:** Entrenar a usuarios en buenas prácticas de seguridad.
- **Actualizaciones y parches:** Mantener software y sistemas operativos actualizados.
- **Software Antivirus y Antimalware:** Detectar y eliminar malware.

- **Firewalls:** Controlar el tráfico de red y prevenir accesos no autorizados.
- **Autenticación Multifactor (MFA):** Añadir capas adicionales de seguridad en la autenticación.
- **Cifrado:** Proteger datos en reposo y en tránsito.
- **Educación en Conciencia de Seguridad:** Capacitar a usuarios sobre prácticas seguras.
- **Gestión de Accesos:** Restringir el acceso a datos y recursos a usuarios autorizados.
- **Copias de Seguridad (Backups):** Garantizar la recuperación de datos ante incidentes.
- **Análisis de Vulnerabilidades y Pruebas de Penetración:** Identificar y mitigar debilidades.
- **Seguridad Física:** Proteger la infraestructura de TI contra amenazas físicas.

17. ¿Mecanismos correctivos en seguridad informática?

Los mecanismos correctivos en seguridad informática son acciones y procedimientos implementados después de que se ha detectado un incidente de seguridad, con el objetivo de remediar el daño causado y restaurar la operatividad y seguridad de los sistemas afectados.

Estos mecanismos se centran en la recuperación y reparación, así como en la prevención de futuras brechas o ataques similares.

Algunos de los mecanismos correctivos son los siguientes:

- **Respuesta a incidentes:** Procedimientos para responder a violaciones de seguridad.
- **Recuperación de desastres:** Planes para restaurar sistemas y datos después de un incidente.
- **Forense digital:** Investigación de violaciones de seguridad para entender cómo ocurrieron y prevenir incidentes futuros.
- **Erradicación del Malware:** Eliminar software malicioso de los sistemas afectados.

- **Parcheo y Actualización:** Corregir vulnerabilidades explotadas y actualizar sistemas.
- **Restauración de Datos:** Recuperar datos desde copias de seguridad.
- **Revisión de Políticas de Seguridad:** Ajustar políticas y prácticas de seguridad basándose en el análisis del incidente.
- **Fortalecimiento de la Infraestructura:** Mejorar la seguridad de la infraestructura de TI.
- **Capacitación y Concienciación:** Reforzar la formación en seguridad para empleados.
- **Comunicación y Notificación:** Informar a las partes afectadas sobre el incidente.
- **Monitoreo Mejorado:** Incrementar la vigilancia de sistemas y redes para detectar y prevenir futuros incidentes.

18. ¿Qué es el aumento de privilegios?

El aumento de privilegios es una técnica que permite a un usuario, proceso o aplicación obtener un nivel de acceso más elevado del que originalmente se le concedió, normalmente para ejecutar acciones que están restringidas a usuarios, procesos o aplicaciones con mayores privilegios.

El aumento de privilegios es considerado una vulnerabilidad crítica porque permite a los atacantes, una vez que han ingresado al sistema con privilegios limitados, acceder a recursos, datos o funcionalidades de seguridad sensibles que de otro modo estarían fuera de su alcance.

Tipos principales de aumento de privilegios

- **Vertical:** El atacante pasa de un nivel de privilegio bajo a uno más alto, como de usuario común a administrador.
- **Horizontal:** El atacante extiende sus privilegios dentro del mismo nivel de acceso para usar recursos no autorizados.

Puede explotarse mediante vulnerabilidades de software, ingeniería social, phishing, o instalación de malware.

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

Las técnicas de aumento de privilegios en sistemas operativos como Windows y Linux explotan vulnerabilidades, configuraciones incorrectas o debilidades en los procesos de seguridad para obtener privilegios más elevados que los inicialmente asignados.

Windows

- **Explotación de Vulnerabilidades en el Software:** Aprovechar bugs en el sistema operativo o en aplicaciones instaladas para ejecutar código con privilegios de administrador.
- **Pass-the-Hash / Pass-the-Ticket:** Técnicas para usar hashes de contraseñas o tickets de autenticación robados para autenticarse como un usuario diferente sin conocer la contraseña real.
- **DLL Hijacking:** Reemplazar o modificar bibliotecas dinámicas de enlace (DLL) que son cargadas por aplicaciones legítimas para ejecutar código malicioso con los privilegios de la aplicación.
- **Token Manipulation:** Atacantes que ya tienen acceso a un sistema pueden manipular tokens de seguridad de Windows para asignarse privilegios de administrador.
- **Uso de Cuentas de Servicio:** Explotar configuraciones débiles en cuentas de servicio (por ejemplo, servicios que se ejecutan con privilegios elevados) para ejecutar código malicioso.

Linux

- **Explotación de Vulnerabilidades del Kernel:** Utilizar bugs en el kernel de Linux para ejecutar código con privilegios root.
- **Sudo y SUID/GUID Misconfigurations:** Aprovechar configuraciones incorrectas en sudo o en binarios con los bits SUID/SGID establecidos incorrectamente para ejecutar comandos como root o otro usuario privilegiado.
- **Crontab Abuse:** Modificar tareas programadas (crontab) para ejecutar comandos maliciosos con privilegios elevados.
- **Dirty COW y otras vulnerabilidades específicas del kernel:** Explotar vulnerabilidades conocidas del kernel como Dirty COW para escribir en archivos a los que un usuario normal no tendría acceso y elevar privilegios.

- **Abuso de Servicios y Daemons:** Identificar servicios o daemons que se ejecutan como root y tienen configuraciones inseguras o vulnerabilidades que pueden ser explotadas.

20. ¿Protección frente al aumento de privilegios?

Para proteger los sistemas frente al aumento de privilegios, es crucial implementar una serie de prácticas y controles de seguridad diseñados para minimizar las vulnerabilidades y limitar las oportunidades para que los atacantes exploten estos fallos.

Algunas de las estrategias efectivas para la protección frente al aumento de privilegios son las siguientes:

- **Principio de Menor Privilegio:** Limitar los privilegios de usuarios y aplicaciones al mínimo necesario.
- **Parcheo y Actualización Regular:** Mantener actualizados los sistemas y aplicaciones con los últimos parches de seguridad.
- **Control de Acceso y Autenticación Multifactor (MFA):** Reforzar la verificación de identidades y restringir accesos no autorizados.
- **Auditoría y Monitoreo:** Vigilar comportamientos sospechosos y revisar registros de actividad.
- **Segmentación de Red y Aislamiento de Sistemas:** Limitar la propagación de ataques mediante la división de redes y el aislamiento de sistemas críticos.
- **Detección de Vulnerabilidades y Análisis de Seguridad:** Identificar y corregir vulnerabilidades potenciales.
- **Educación en Seguridad:** Capacitar a usuarios y administradores en prácticas de seguridad.
- **Restricciones de Software y Control de Aplicaciones:** Controlar qué aplicaciones pueden ejecutarse en los sistemas.
- **Configuraciones de Seguridad Fortalecidas:** Aplicar configuraciones de seguridad óptimas y deshabilitar servicios innecesarios.
- **Respuesta a Incidentes:** Tener un plan establecido para responder y recuperarse de incidentes de seguridad.

Conclusión

En conclusión, la seguridad informática y el análisis de vulnerabilidades constituyen fundamentos críticos en la protección de nuestros activos digitales frente a una variedad de amenazas en constante evolución. A lo largo de este documento, hemos explorado exhaustivamente los conceptos clave, desafíos y estrategias en el ámbito de la seguridad cibernética, destacando la importancia de comprender las vulnerabilidades, los pilares de la seguridad, los tipos de ataques y las medidas de protección más efectivas.

Hemos visto cómo la confidencialidad, integridad, disponibilidad y autenticidad sirven como principios rectores en la salvaguarda de la información y los sistemas informáticos. Estos pilares no solo son esenciales para diseñar sistemas seguros, sino también para implementar prácticas y políticas que aseguren la protección de datos, aplicaciones, infraestructura y usuarios contra una amplia gama de amenazas.

La discusión sobre los ataques comunes, como el phishing, ransomware, inyecciones SQL y DDoS, subraya la necesidad de una vigilancia constante y adaptación a las nuevas técnicas empleadas por los actores maliciosos. Asimismo, hemos destacado la importancia de entender las amenazas en el contexto de vulnerabilidades existentes y cómo el paisaje de amenazas sigue expandiéndose debido a factores como los avances tecnológicos y la creciente dependencia de sistemas digitales.

Las estrategias de defensa, incluyendo firewalls, soluciones antivirus/antimalware y cifrado de datos, son indispensables para mitigar los riesgos asociados a las vulnerabilidades. Sin embargo, es fundamental adoptar un enfoque holístico que también incorpore mecanismos preventivos y correctivos, educación en seguridad, y una cultura de seguridad consciente entre los usuarios.

Enfrentar el desafío del aumento de privilegios y otras técnicas avanzadas requiere no solo de tecnologías robustas, sino también de prácticas de seguridad informática bien definidas y constantemente actualizadas. La protección eficaz frente al aumento de privilegios, por ejemplo, destaca la necesidad del principio de mínimo privilegio, segmentación de red, actualizaciones regulares de seguridad, y monitoreo y auditoría continuos.

Finalmente, este documento subraya que la seguridad informática no es una tarea estática, sino un proceso dinámico y continuo que exige atención constante, adaptación y mejora. La colaboración entre individuos, organizaciones y gobiernos, junto con la adopción de buenas prácticas y tecnologías avanzadas, es esencial para construir un entorno digital más seguro y resiliente. A medida que avanzamos hacia un futuro cada vez más interconectado, la importancia de una seguridad informática efectiva y proactiva nunca ha sido tan crítica.

Referencia Bibliográfica

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.

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.

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.

Abanca. (2023, 3 abril). Tipos de vulnerabilidades informáticas y cómo evitarlas | ABANCA Blog. Cuentas Claras by ABANCA | Ahorro, finanzas personales y actualidad. <https://www.cuentasclaras.es/ciberseguridad/tipos-de-vulnerabilidades-informaticas/#:~:text=Vulnerabilidad%20baja%3A%20su%20impacto%20es%20m%C3%ADnimo%20y%20se, en%20riesgo%20la%20informaci%C3%B3n%20y%20se%20propaga%20libremente>.

Asale, R.-. (s. f.). Autenticación | Diccionario de la Lengua Española. «Diccionario de la lengua española» - Edición del Tricentenario. <https://dle.rae.es/autenticaci%C3%B3n>

Chavez, J. J. S. (2024, 22 enero). ¿Qué es una vulnerabilidad informática y cómo protegerse? <https://www.deltaprotect.com/blog/vulnerabilidad-informatica/#:~:text=Una%20vulnerabilidad%20inform%C3%A1tica%20es%20cualquier%20fallo%20o%20error,aprovechado%20por%20un%20hacker%20para%20comprometer%20su%20seguridad>.

Ciberseg. (2019, 18 noviembre). Aumento de privilegios. Ciberseguridad. <https://ciberseguridad.com/amenazas/aumento-privilegios/#:~:text=T%C3%A9cnicas%20de%20aumento%20de%20privilegios%20en%20Windows%201,3.%20Secuestro%20de%20orden%20de%20b%C3%BAscueda%20de%20DLL>

Durán, M. (2023, 12 junio). 10 herramientas de seguridad informática para tu empresa. HubSpot. <https://blog.hubspot.es/website/herramientas-de-seguridad-informatica/#:~:text=Las%2010%20herramientas%20de%20seguridad%20inform>

[C3%A1tica%20m%C3%A1s%20utilizadas,7%20Almacenamientos%20de%20respaldo.%208%20Antispyware.%20M%C3%A1s%20elementos](#)


KeepCoding, R. (2023, 21 julio). ¿Qué es la escalada de privilegios? | KeepCoding Bootcamps. KeepCoding Bootcamps. <https://keepcoding.io/blog/que-es-la-escalada-de-privilegios/#:~:text=%C2%BFQu%C3%A9%20es%20la%20escalada%20de%20privilegios%3F%20Un%20ataque,administrador%20%28root%29%20en%20el%20sistema%20de%20una%20organizaci%C3%B3n.>

¿Qué es la ingeniería social? | IBM. (s. f.). <https://www.ibm.com/es-es/topics/social-engineering>

¿Qué es la seguridad informática? | Glosario. (s. f.). HPE México. <https://www.hpe.com/mx/es/what-is/it-security.html#:~:text=La%20seguridad%20inform%C3%A1tica%20es%20esencial%20para%20prevenir%20ataques,vulneraciones%20de%20seguridad%20y%20de%20strucci%C3%B3n%20de%20la%20propiedad.>

¿Qué es un virus informático? - Tipos, ejemplos y más | ProofPoint ES. (2024, 26 enero). Proofpoint. <https://www.proofpoint.com/es/threat-reference/computer-virus>

SensorsTech. (2023, 26 septiembre). Qué es una amenaza informática: ejemplos y concepto - SensorsTech. SensorsTech. <https://sensorstechforum.es/que-es-una-amenaza-informatica-y-ejemplos/>

Webmaster, & Webmaster. (2023, 11 diciembre). Concepto de amenaza informática  Significado y definición. SignificadosWeb.com. <https://significadosweb.com/concepto-de-amenaza-informatica-definicion-y-que-es/>

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

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 de la data center de la escuela politécnica del ejército. SANGOLQUI/ESPE/2011, SANGOLQUI.

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.