Gestión de incidentes de seguridad informática

IFCT0109 – Seguridad informática

MF0488_3 (90 horas)

Sistemas de detección y prevención de intrusiones (IDS/IPS)

- Introducción
- Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
- Identificación y caracterización de los datos de funcionamiento del sistema
- Arquitecturas más frecuentes de los sistemas de detección de intrusos
- Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
- Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS
- Resumen

- IDS: detectan intrusos
- IPS: actúan

Introducción

En una economía donde las tecnologías de la información están cada vez más en auge y más extendidas, las organizaciones deben definir políticas de seguridad más exhaustivas en sus sistemas de información para evitar el acceso a ellos por personal no autorizado y para impedir un uso malintencionado de sus datos.

Motivaciones de los atacantes:

- Económicas: robo de información financiera, datos personales, etc.
- Diversión: "hackers" que buscan probar sus habilidades.
- Disconformidad: empleados descontentos con la empresa.
- Autorrealización personal: "hackers" que buscan reconocimiento.

A lo largo de este módulo, exploraremos diferentes tipos de ataques y aprenderemos cómo prevenirlos y combatirlos. En este capítulo en particular, nos centraremos en identificar y caracterizar los datos operativos del sistema, lo que nos permitirá localizar las incidencias que puedan surgir.

Además, analizaremos diversas técnicas para detectar y prevenir ataques de intrusos, utilizando herramientas como los sistemas de prevención de intrusiones (IPS) y los sistemas de detección de intrusos (IDS). Detallaremos sus características principales y funcionalidades.

Para concluir, proporcionaremos pautas específicas para elegir la ubicación adecuada de estos sistemas de prevención o detección de intrusos en función de las necesidades particulares de cada organización

Conceptos generales de incidentes, detección de intrusiones y su prevención

Antes de definir los conceptos de gestión de incidentes y sus relaciones, es imprescindible conocer tres conceptos básicos referentes a la información:

- Confidencialidad: La confidencialidad de la información es la propiedad mediante la que se garantiza el acceso a la misma solo a usuarios autorizados.
- Integridad: Propiedad de la información que garantiza que no ha sido alterada y que se ha mantenido intacto el documento original que contenía dicha información. La información solo puede ser modificada por los usuarios autorizados.
- Disponibilidad: Propiedad de la información en la que se garantiza que esté disponible para los usuarios cuando estos lo requieran.

En términos de seguridad informática, para que la información cumpla unos estándares de seguridad adecuados, debe contener las tres propiedades: integridad, confidencialidad y disponibilidad.

Un incidente de seguridad es cualquier evento que puede afectar a la integridad, confidencialidad y disponibilidad de la información. En otras palabras, y atendiendo a la norma ISO 27001:2013, un incidente de seguridad es un evento no deseado o no esperado que puede comprometer significativamente las operaciones de negocio y amenazar la seguridad de la información.

Conceptos generales de incidentes, detección de intrusiones y su prevención

Gestión de incidentes: La gestión de incidentes es un proceso que se encarga de identificar, contener, erradicar y recuperar los sistemas afectados por un incidente de seguridad. El objetivo principal es minimizar el impacto del incidente en el negocio y restaurar la normalidad lo antes posible. PREGUNTA EXAMEN

Detección de intrusiones: La detección de intrusiones es el proceso de identificar y monitorizar actividades no autorizadas en un sistema o red informática. Se utilizan diferentes técnicas para detectar intrusiones, como el análisis de tráfico de red, el análisis de archivos de registro y la monitorización de aplicaciones.

Prevención de intrusiones: La prevención de intrusiones es el proceso de impedir que se produzcan intrusiones en un sistema o red informática. Se utilizan diferentes técnicas para prevenir intrusiones, como el filtrado de paquetes, el uso de firewalls y la implementación de políticas de seguridad.

Relación entre los tres conceptos

La gestión de incidentes, la detección de intrusiones y la prevención de intrusiones son tres conceptos estrechamente relacionados.

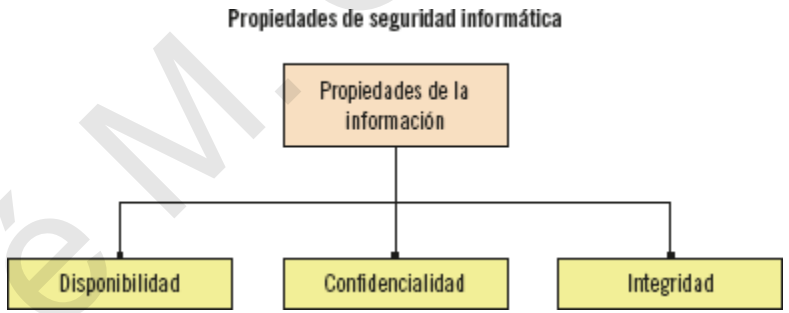
- La detección de intrusiones es el primer paso para la gestión de incidentes.
- Si no se detectan las intrusiones, no se podrán gestionar ni mitigar sus efectos.
- La prevención de intrusiones es una medida que puede ayudar a reducir el número de incidentes de seguridad que se producen.

Conceptos generales de incidentes, detección de intrusiones y su prevención

La gestión de incidentes, la detección de intrusiones y la prevención de intrusiones son importantes para proteger la información y los sistemas informáticos de las organizaciones.

Estas medidas pueden ayudar a:

- Minimizar el impacto de los incidentes de seguridad
- Reducir el número de incidentes de seguridad que se producen
- Cumplir con las normativas de seguridad
- Proteger la reputación de la organización



Conceptos generales de incidentes, detección de intrusiones y su prevención

Tipos de incidentes de seguridad

En el ámbito de la seguridad informática, la diversidad de incidentes que pueden afectar a un sistema es considerable. Una clasificación de estos incidentes:

Accesos No Autorizados. Engloba ingresos y operaciones no autorizadas en sistemas, ya sea con éxito o no. Comprende:

- Robo de Información: Extracción ilícita de datos sensibles.
- Borrado de Información: Eliminación indebida de datos almacenados.
- Alteración de la Información: Modificación malintencionada de datos.
- Asimismo, se incluyen intentos recurrentes y no recurrentes de acceso no autorizado, así como el abuso o mal uso de servicios informáticos, tanto internos como externos, que requieran autenticación.

Malware. Estos incidentes son provocados de manera autónoma por programas o códigos maliciosos sin la autorización del propietario. Algunos tipos relevantes son:

- Virus Informáticos: Se adhieren a programas o archivos para propagarse y ejecutar acciones dañinas. Dependientes de la activación por parte de un usuario.
- Gusanos Informáticos: Similar a los virus, pero se replican sin necesidad de la acción del usuario, aprovechando funciones de transferencia de archivos o información del sistema.
- Troyanos: Se disfrazan como programas auténticos, creando una puerta trasera para acceso no autorizado.
- Ransomware: Cifran archivos exigiendo un rescate para desbloquearlos. Pueden replicarse en la red, comportándose de manera similar a los virus.

Conceptos generales de incidentes, detección de intrusiones y su prevención

Tipos de incidentes de seguridad

Denegación del Servicio. Eventos que provocan la pérdida de un servicio, dificultando su ejecución normal. Se considera denegación del servicio cuando se experimentan tiempos de respuesta extremadamente altos y servicios inaccesibles sin razón aparente.

Pruebas, Escaneos o Intentos de Obtención de Información. Eventos que buscan obtener información sobre las acciones en un sistema, como:

- Sniffers: Aplicaciones que interceptan y recopilan información enviada por los equipos de una red.
- Detección de Vulnerabilidades: Aplicaciones que buscan debilidades en un sistema para explotarlas maliciosamente.

Mal Uso de Recursos Tecnológicos: Eventos que atacan los recursos tecnológicos de un sistema debido a un uso inadecuado, incluyendo:

- Violación de la Normativa de Acceso a Internet.
- Abuso o Mal Uso de Servicios Informáticos Externos o Internos.
- Abuso o Mal Uso del Correo Electrónico.
- Violación de Políticas, Normas y Procedimientos de Seguridad Informática de una Organización.

Esta clasificación proporciona una visión integral de los incidentes de seguridad, abordando diversas amenazas que pueden afectar la integridad y confidencialidad de la información en un sistema. Es fundamental para el diseño y la implementación efectiva de estrategias de seguridad informática.

Conceptos generales de incidentes, detección de intrusiones y su prevención

Gestión y medidas de incidentes de seguridad

Ante la posibilidad de que ocurra algún tipo de incidente de seguridad en la organización, es esencial implementar un conjunto de medidas para prevenir, detectar y corregir dichos eventos. Estas medidas se dividen en:

- Medidas Preventivas: Son aquellas acciones diseñadas para evitar la ocurrencia de incidentes de seguridad. Ejemplos incluyen el uso de contraseñas seguras, el cifrado de información, la implementación de firewalls y la creación de honeypots.

- Medidas de Detección: Estas medidas se centran en identificar y controlar los incidentes de seguridad. Incluyen sistemas de detección de intrusiones y revisiones de seguridad periódicas, entre otros.

- Medidas Correctivas: Una vez que ha ocurrido un incidente de seguridad, se implementan medidas correctivas para prevenir su recurrencia y restaurar el sistema a su estado inicial. Esto puede involucrar procedimientos de restauración, eliminación de código malicioso y auditorías de seguridad.

Conceptos generales de incidentes, detección de intrusiones y su prevención

Gestión y medidas de incidentes de seguridad

La gestión de incidentes busca calcular y utilizar eficientemente los recursos necesarios para aplicar estas medidas de prevención, detección y corrección. Se establecen pautas generales para una ejecución efectiva de la gestión de incidentes:

- Prevención de Incidentes: Aplicación de medidas preventivas para evitar la ocurrencia de incidentes.
- Detección y Reporte de Incidentes: Identificación y notificación de incidentes a los responsables de la gestión.
- Clasificación del Incidente: Definición del tipo de incidente que ha ocurrido (acceso no autorizado, robo de información, etc.).
- Análisis del Incidente: Evaluación de cómo se produjo el incidente y los daños causados.
- Respuesta al Incidente: Aplicación de medidas correctivas para restaurar el sistema a su estado inicial.
- Registro de Incidentes: Documentación de incidentes y medidas aplicadas para mantener un historial y control.
- Aprendizaje: Análisis de posibles errores causantes de la incidencia para evitar repeticiones.

Conceptos generales de incidentes, detección de intrusiones y su prevención

Gestión y medidas de incidentes de seguridad

Siguiendo estas fases, las organizaciones obtienen beneficios significativos:

- Rápida, Eficiente y Sistemática Respuesta: Actuación rápida ante incidentes.
- Restauración Rápida del Sistema: Garantiza la mínima pérdida de información posible.
- Base de Datos Histórico: Generación de un registro para agilizar futuros incidentes.
- Mejora Continua: Optimización constante de la gestión de incidentes, eliminando repeticiones.

Sin embargo, una gestión deficiente puede tener consecuencias adversas:

- Desperdicio y Bajo Rendimiento de Recursos: Ineficiencia en la utilización de recursos.
- Pérdida de Información Valiosa: Consecuencias negativas para la organización.
- Pérdida de Productividad y Calidad de Servicio: Impacto en la calidad del servicio a los clientes.

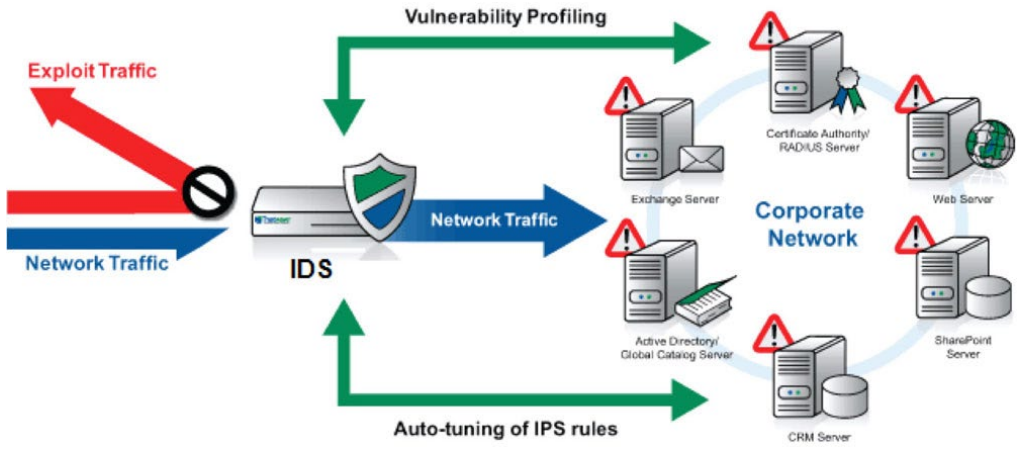
Conceptos generales de incidentes, detección de intrusiones y su prevención

Detección de Intrusiones y su Prevención

Los intentos de intrusión representan acciones que pueden tener un impacto adverso en la confidencialidad, integridad y disponibilidad de la información de un sistema, o que buscan eludir los mecanismos de seguridad establecidos.

Estos intentos de intrusión pueden manifestarse de diversas maneras, desde accesos no autorizados por parte de usuarios externos a través de internet, hasta usuarios autorizados que intentan obtener privilegios para los cuales no tienen autorización. Incluso, puede incluir a usuarios con permisos legítimos que emplean maliciosamente los privilegios otorgados.

Con el objetivo de prevenir este tipo de intrusiones, se implementan sistemas de prevención de intrusiones, conocidos como IPS (Intrusion Prevention Systems). Estos sistemas proporcionan una capa adicional de protección a los equipos y redes de una organización frente a posibles amenazas originadas por un uso intensivo de las redes y sistemas de información externos.



Identificación y caracterización de los datos de funcionamiento del sistema

Registro de Eventos y Logs en Sistemas Windows y Linux: Análisis y Evaluación

Un log, o registro, constituye una documentación oficial de los eventos del sistema ocurridos durante un periodo específico. Estos registros detallan información crucial sobre:

- Tipo de Evento: Descripción específica del evento en cuestión.
- Origen del Evento: Identificación del individuo o sistema responsable del evento.
- Fecha y Hora del Evento: Registro temporal del momento en que tuvo lugar el evento.
- Ubicación del Evento: Indicación del lugar o contexto donde ocurrió el evento.
- Motivo del Evento: Descripción de la razón o circunstancia que provocó el evento.

De lo más importante a la hora de hacer un analisis forense

La evaluación de los logs de los equipos se recomienda para verificar el correcto funcionamiento del sistema y detectar diversos eventos, como incidentes de seguridad, comportamientos inusuales, cambios en la configuración de aplicaciones o dispositivos, y la utilización y rendimiento de los recursos.

Es posible identificar eventos como intentos fallidos de acceso por parte de usuarios no autorizados.

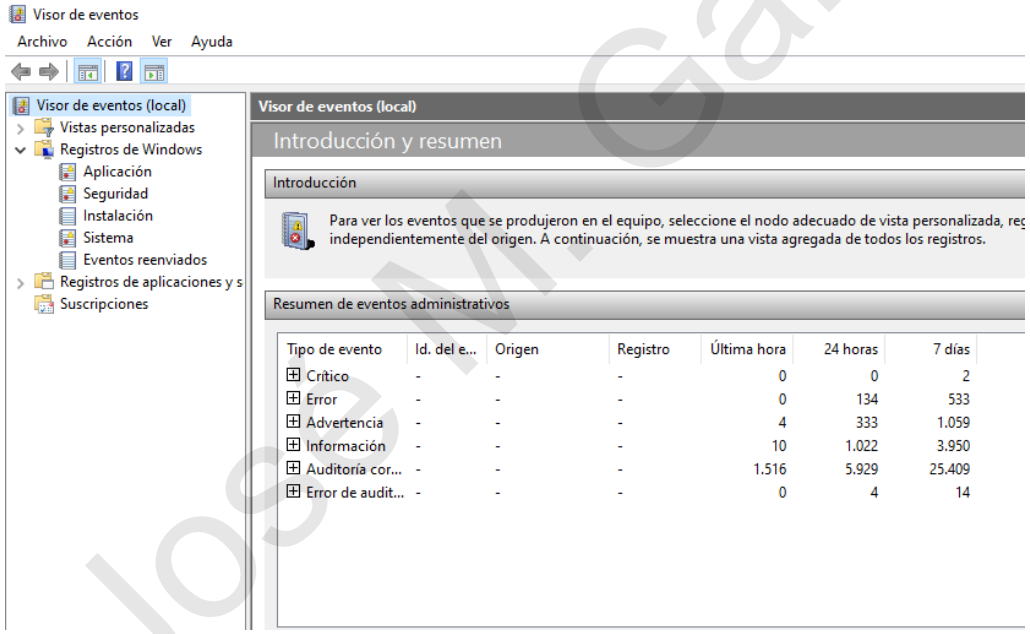
Identificación y caracterización de los datos de funcionamiento del sistema

Registro de Eventos y Logs en Sistemas Windows y Linux: Análisis y Evaluación

Tanto en entornos Windows como Linux, se puede acceder y visualizar estos logs para un análisis detallado de la actividad del sistema.

En Windows:

En el sistema operativo Windows, se emplea el "Visor de eventos". Esta herramienta proporciona una interfaz gráfica accesible a través de Inicio -> Configuración -> Panel de control -> Herramientas administrativas -> Visor de eventos. El Visor de eventos permite visualizar diversos tipos de eventos, como registros de aplicación, seguridad, instalación y eventos reenviados. Para detectar intrusiones y fallas de seguridad, es crucial prestar atención a los registros de seguridad.



Identificación y caracterización de los datos de funcionamiento del sistema

Registro de Eventos y Logs en Sistemas Windows y Linux: Análisis y Evaluación

En Windows:

En sistemas Windows, se generan diversos tipos de eventos que son registrados en el "Visor de eventos". Estos eventos proporcionan información valiosa sobre el estado, la seguridad y el rendimiento del sistema. Aquí tienes una descripción de algunos tipos comunes de eventos en Windows:

- Registros de Aplicación: Registra eventos generados por aplicaciones o programas instalados en el sistema.

  Ejemplos de Eventos: Errores en la ejecución de aplicaciones, advertencias de rendimiento, información sobre actualizaciones de software.

- Registros de Seguridad: Registra eventos relacionados con la seguridad del sistema, como intentos de inicio de sesión, cambios en permisos y políticas de seguridad.

  Ejemplos de Eventos: Intentos de inicio de sesión exitosos o fallidos, cambios en la configuración de seguridad, actividades de cuentas de usuario.

- Registros de Instalación: Registra eventos relacionados con la instalación y desinstalación de programas y aplicaciones en el sistema. (SYSmon)

  Ejemplos de Eventos: Instalación o desinstalación de software, cambios en configuraciones del sistema.

- Registros del Sistema: Registra eventos del sistema operativo, incluyendo mensajes de error y advertencias generales.

  Ejemplos de Eventos: Fallos en hardware, errores del sistema operativo, advertencias sobre recursos insuficientes.

Identificación y caracterización de los datos de funcionamiento del sistema

Registro de Eventos y Logs en Sistemas Windows y Linux: Análisis y Evaluación

En Windows:

Aquí tienes una descripción de algunos tipos comunes de eventos en Windows: (continuación)

- Registros de Seguridad del Directorio Activo: Registra eventos específicos del Directorio Activo en entornos de red.

  Ejemplos de Eventos: Cambios en objetos del Directorio Activo, intentos de acceso no autorizado a recursos compartidos.

- Registros de Hardware: Registra eventos relacionados con el hardware del sistema, como errores de hardware, problemas de dispositivos.
  - Ejemplos de Eventos: Fallos en discos duros, problemas con controladores de dispositivos, cambios en la configuración de hardware.

- Registros de Red: Registra eventos relacionados con la actividad de red y la conectividad.
  - Ejemplos de Eventos: Cambios en la configuración de red, problemas de conectividad, eventos de firewall.

- Registros de Aplicaciones y Servicios: Registra eventos generados por aplicaciones y servicios específicos.
  - Ejemplos de Eventos: Registro detallado de eventos específicos de aplicaciones, errores de servicios.

Identificación y caracterización de los datos de funcionamiento del sistema

Registro de Eventos y Logs en Sistemas Windows y Linux: Análisis y Evaluación

Tanto en entornos Windows como Linux, se puede acceder y visualizar estos logs para un análisis detallado de la actividad del sistema.

En Linux:

Por otro lado, Linux no dispone de una aplicación gráfica equivalente para visualizar eventos. Para esta tarea, es necesario acceder a los archivos de registro como usuario "root" mediante comandos. Algunos comandos útiles incluyen:

- **tail -f /var/log/auth.log**: Muestra las últimas líneas y actualizaciones de eventos de autenticación.
- **less +F /var/log/auth.log**: Permite visualizar la totalidad del archivo con actualizaciones en tiempo real.

Además, es posible revisar varios archivos de registro importantes, como:

/var/log/auth.log, /var/log/boot.log, /var/log/daemon.log, /var/log/dmesg.log, y otros, para evaluar el funcionamiento y los problemas de seguridad del sistema.

Identificación y caracterización de los datos de funcionamiento del sistema

Registro de Eventos y Logs en Sistemas Windows y Linux: Análisis y Evaluación

Logs en Linux, algunos:

Nombre de Archivo	Funcionalidad
/var/log/auth.log	Eventos de autenticación de usuarios y permisos.
/var/log/boot.log	Eventos y servicios iniciados al iniciar el sistema.
/var/log/daemon.log	Mensajes sobre permisos o servicios en ejecución.
/log/dmesg.log	Mensajes del núcleo Linux.
/var/log/errors.log	Errores del sistema.
/var/log/everything.log	Mensajes misceláneos no cubiertos por otros archivos.
/var/log/httpd.log	Mensajes y errores de Apache.
/var/log/mail.log	Mensajes del servidor de correo electrónico.
/var/log/messages.log	Alertas generales del sistema.
/var/log/secure	Registro de seguridad.
/var/log/syslog.log	Registro del sistema de registro.
/var/log/user.log	Información sobre los procesos utilizados por el usuario.

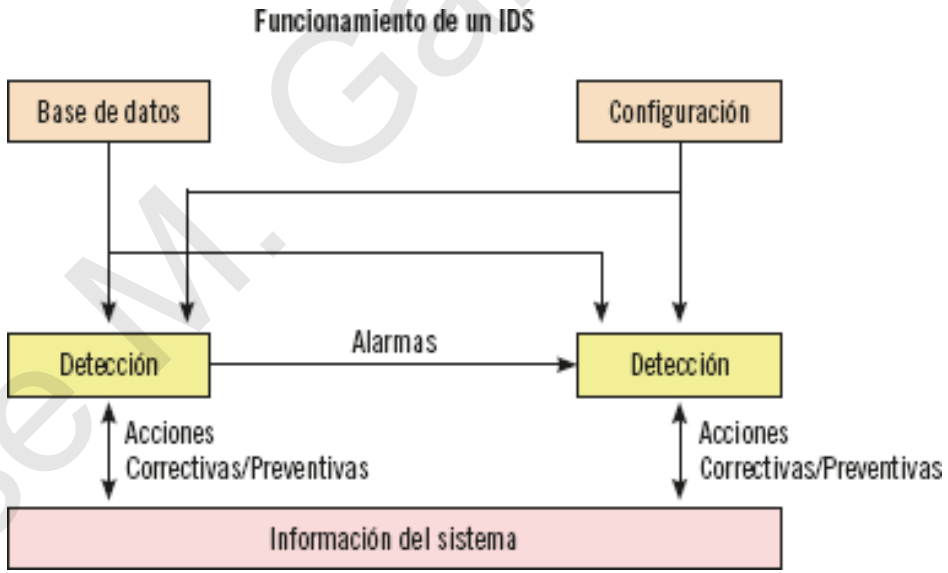
Arquitecturas más frecuentes de los sistemas de detección de intrusos

Introducción

Los Sistemas de Detección de Intrusos (IDS), también conocidos como Intrusion Detection Systems, son programas diseñados para detectar intrusiones en redes o sistemas informáticos, monitorizando activamente los eventos del sistema en busca de posibles intentos de intrusión.

Funcionan como procesos de auditoría, utilizando una amplia base de datos y configuraciones específicas para prevenir y detectar posibles ataques.

Una representación gráfica del funcionamiento de un IDS podría describirse de la siguiente manera:



Arquitecturas más frecuentes de los sistemas de detección de intrusos

Introducción

Estos sistemas ofrecen numerosas ventajas, y su implementación en organizaciones se justifica por varios motivos:

- Prevención de Problemas mediante Disuasión: Los IDS actúan como elementos disuasorios al descubrir a posibles atacantes. La posibilidad de ser detectados y sancionados disuade a individuos hostiles de llevar a cabo acciones maliciosas.
- Detección de Ataques no Prevenidos por Otros Sistemas: Los IDS son capaces de detectar ataques y violaciones de seguridad que otros sistemas de protección no pueden prevenir. Identifican intentos de acceso no autorizado y alertan al administrador para que se tomen medidas correctivas de inmediato, minimizando el impacto.
- Identificación de Preámbulos de Ataques: Antes de lanzar un ataque, los intrusos suelen examinar y probar el sistema. Los IDS detectan estas pruebas y accesos no autorizados, aumentando la seguridad al identificar estos preámbulos y permitiendo la prevención de futuros ataques.
- Justificación y Documentación del Riesgo Organizacional: Al elaborar políticas de seguridad, es crucial evaluar los riesgos respaldados con indicadores y datos. Los IDS permiten identificar y documentar estos riesgos, garantizando que las políticas de seguridad y las decisiones relacionadas estén debidamente justificadas.
- Aportación de Información Útil sobre Intrusiones y Ataques: Además de bloquear ataques, los IDS recopilan información valiosa sobre estos eventos, que puede utilizarse como evidencia en acciones legales contra los perpetradores. Además de salvaguardar el sistema, aportan datos útiles para posibles acciones legales.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

En la actualidad, existe una diversidad de propuestas en el mercado con respecto a la arquitectura de los Sistemas de Detección de Intrusos (IDS). Sin embargo, la falta de estandarización en estas arquitecturas presenta un desafío para la interoperabilidad entre organizaciones que adoptan diferentes enfoques en sus IDS.

A pesar de esta variabilidad, hay características comunes en las distintas arquitecturas de IDS:

Fuente de Recogida de Datos: Las fuentes de datos pueden ser logs, dispositivos de red o el propio sistema de información. Estas sirven como la base para la detección de anomalías de seguridad.

Reglas Definitorias: Establecen patrones y directrices que permiten la detección de anomalías de seguridad en un sistema. Estas reglas actúan como la brújula que guía la identificación de posibles intrusiones.

Filtros: Comparan los datos o logs obtenidos con los patrones definidos en las reglas. Funcionan como un tamiz que separa eventos normales de posibles amenazas.

Detectores de Eventos Anormales: Identifican eventos anómalos que ocurren en el tráfico de la red. Este componente es esencial para la detección temprana de actividades sospechosas.

Sistema de Generación de Informes y Alarmas: Responsable de generar informes detallados y alarmas en caso de detectar alguna intrusión o ataque. Proporciona la capacidad de respuesta necesaria ante posibles amenazas.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

Es importante destacar que, aunque los IDS son herramientas valiosas para la detección y mitigación de vulnerabilidades, no deben considerarse como la única medida de seguridad. Para garantizar una defensa completa, se requiere la implementación de medidas adicionales como cortafuegos o Sistemas de Prevención de Intrusiones (IPS), entre otras.

A pesar de las similitudes, las diferencias entre las arquitecturas de IDS son notables. A continuación, se explorarán las arquitecturas de IDS más relevantes en el mercado actual, destacando la diversidad de enfoques adoptados por los desarrolladores y las organizaciones.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

Arquitectura CIDF (Common Intrusion Detection Framework) Intento de establecer un estándar para el diseño de sistemas de detección de intrusiones (IDS). Aunque no logró convertirse en un estándar universalmente adoptado.

Esta arquitectura se promovió inicialmente por la Agencia Federal de Estados Unidos DARPA (Defense Advanced Research Projects Agency). Y la CIDF define cuatro tipos fundamentales de equipos que trabajan de manera conjunta para lograr una detección efectiva de intrusiones:

- Equipos Generadores de Eventos (Equipos E): Su función principal es detectar eventos y emitir informes relacionados con la seguridad. Estos eventos pueden incluir actividades sospechosas o comportamientos inusuales que podrían indicar una posible intrusión.
- Analizadores de Eventos (Equipos A): Estos equipos reciben los informes generados por los Equipos E y llevan a cabo análisis más detallados. Su tarea es examinar la información proporcionada, evaluar la gravedad de la situación y determinar si hay signos de intrusiones o amenazas a la seguridad.
- Base de Datos de Eventos (Equipos D): Los componentes de base de datos almacenan el historial de eventos ocurridos en el sistema. Este almacenamiento es esencial para tener un registro completo de las actividades pasadas, lo que facilita la detección de patrones y la identificación de posibles amenazas.
- Equipos de Respuesta (Equipos R): Estos equipos se encargan de responder a los eventos detectados. Obtienen datos de los Equipos E, A y D, y ejecutan acciones específicas para mitigar o contener la amenaza. Esto podría incluir la implementación de medidas de seguridad adicionales o la detención de actividades sospechosas.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

La Arquitectura CISL (Common Intrusion Specification Language), o Lenguaje Común de Especificación de Intrusiones, surge como una extensión y complemento de la Arquitectura CIDF (Common Intrusion Detection Framework). Es una extensión de la Arquitectura CIDF (Common Intrusion Detection Framework). Su objetivo principal es facilitar la comunicación y coordinación entre los componentes de un sistema de detección de intrusiones.

CISL permite:

- Información de Eventos en Grupo: Une los Equipos Generadores de Eventos (Equipos E) y Analizadores de Eventos (Equipos A), proporcionando detalles sobre el tráfico de red y la auditoría de registros.

- Resultados de los Análisis: Conecta los Analizadores de Eventos (Equipos A) y la Base de Datos de Eventos (Equipos D), facilitando información sobre anomalías y ataques detectados.

- Prescripciones de Respuestas: Establece la conexión entre los Analizadores de Eventos (Equipos A) y los Equipos de Respuesta (Equipos R), permitiendo detener actividades y modificar parámetros de seguridad para contrarrestar posibles ataques.

A través de un lenguaje común de especificación de intrusiones, CISL mejora la interoperabilidad de los sistemas de detección de intrusiones, contribuyendo a las mejores prácticas en ciberseguridad. Aunque no es un estándar ampliamente adoptado, su enfoque en la estandarización promueve el intercambio eficiente de información en el ámbito de la seguridad informática.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

Arquitectura AusCERT es un enfoque simplificado de detección de intrusiones que se destaca por su simplicidad y eficacia para informar sobre incidentes de seguridad. Aunque carece de la complejidad de arquitecturas como CIDF o CISL, ofrece una manera rápida y directa de documentar eventos en una base de datos de incidentes.

Principales Características:

- Simplicidad: AusCERT se distingue por su diseño minimalista, que simplifica la construcción y el análisis de informes. Está orientada a proporcionar información esencial sobre incidentes de seguridad en pocas líneas.

- Informes Directos: La arquitectura se centra en generar informes concisos y directos sobre incidentes ocurridos en el sistema. Aunque limitada en detalles, brinda una visión rápida de la naturaleza y el alcance de un incidente.

- Eficiencia en el Análisis: AusCERT se destaca en situaciones donde la rapidez y la simplicidad son prioritarias. Es ideal para casos en los que se necesita una respuesta inmediata y el nivel de detalle no es crítico.

Aunque AusCERT puede carecer de la profundidad necesaria para investigaciones exhaustivas, su enfoque simplificado la convierte en una herramienta eficaz para la identificación y respuesta rápidas a incidentes de seguridad.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

Ejemplo de Informe AusCERT

Incidente: Ataque de Denegación de Servicio (DoS)

Fecha: 03/05/2024

Hora: 14:30

Descripción: Se detectaron múltiples intentos de saturar el tráfico en la red, resultando en la pérdida temporal de servicio.

Acciones Tomadas: Se aplicaron filtros para mitigar el ataque y se restableció el servicio.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

Arquitectura IDWG (Intrusion Detection Working Group) es un enfoque integral para la detección de intrusiones que busca establecer un intercambio efectivo de información entre los distintos subsistemas de un Sistema de Detección de Intrusiones (IDS).

A través de sus tres módulos fundamentales, IDWG busca mejorar la coordinación y la eficiencia en la detección y respuesta a amenazas de seguridad.

- Sensor:

  Recoge datos de la fuente, como paquetes de red, logs de aplicaciones y del sistema operativo y proporciona información vital para la detección de actividades no autorizadas.

- Analizador:

  Analiza los datos recopilados por el sensor y detecta accesos y/o actividades no autorizadas a través de la comparación con patrones y reglas predefinidas.

- Manager:

  Gestiona y administra los componentes del IDS, incluyendo sensores y analizadores. Su propósito es configurar los sensores y analizadores, consolidar datos, generar informes y facilitar la comunicación entre subsistemas.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

Arquitectura IDWG (Intrusion Detection Working Group)

Qué se obtiene con esta arquitectura:

- Lenguaje Común: Se establece un lenguaje común que describe el formato de los datos intercambiados entre los subsistemas.

- Documentos de Requerimientos Funcionales: Se crean documentos que especifican los requisitos funcionales, permitiendo una comunicación efectiva entre los IDS y sus sistemas de gestión de incidentes.

- Protocolos de Comunicación: Se identifican y definen los protocolos más apropiados para facilitar la comunicación entre los diferentes componentes del IDS y para establecer el formato de los datos intercambiados.

La arquitectura IDWG busca promover la interoperabilidad y la comunicación eficiente entre los elementos clave de un IDS, mejorando así la capacidad de detección y respuesta ante amenazas de seguridad. Su enfoque integral busca abordar la complejidad de los entornos de seguridad cibernética mediante la coordinación efectiva de sus componentes.

Arquitecturas más frecuentes de los sistemas de detección de intrusos

Arquitectura de los IDS

Tipo de Arquitectura IDS	Características
CIDF (Common Intrusion Detection Framework)	Constelación de generadores, analizadores y base de datos de eventos con unidades de respuesta. Escasa aceptación en el mercado.
CISL (Common Intrusion Specification Language)	Conecta los equipos de CIDF, facilita información sobre eventos, resultados de análisis y prescripciones de respuestas.
AusCERT	Arquitectura simple que proporciona información de incidentes de manera concisa. Limitada para obtener detalles detallados de las incidencias.
IDWG (Intrusion Detection Working Group)	Facilita el intercambio de información sobre incidentes de seguridad y define protocolos y formatos para la comunicación entre IDS.

Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad

Tipos de IDS

IDS basados en red (NIDS)

- Estos sistemas detectan ataques mediante la captura y análisis de los paquetes de la red.
- La mayoría de los IDS se ubican en la red, analizando el tráfico para identificar patrones que puedan indicar un ataque.
- Los NIDS examinan todo el tráfico de la red, emitiendo alertas ante intentos de acceso no autorizado o análisis de vulnerabilidades.
- Su estructura incluye sensores o agentes que monitorean el tráfico y una consola que recibe y responde a las alarmas. Ejemplos son Snort o Suricata reconocido por su distribución gratuita, capacidad de análisis en tiempo real, y su extensa base de datos con más de 700 firmas.

Ventajas:

- Detectan accesos no deseados.
- No requieren software adicional en servidores.
- Fácil instalación y actualización.
- Bajo impacto en la red.

Desventajas:

- Pueden tener dificultades en momentos de tráfico elevado.
- Limitaciones para detectar ataques cifrados.
- Requieren análisis manual ante cada detección.

Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad

Tipos de IDS

IDS basados en red (NIDS)

Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad

Tipos de IDS

IDS basados en host (HIDS)

- Estos sistemas operan a nivel de un equipo, analizando el tráfico local para identificar alteraciones en archivos del sistema o actividades sospechosas.
- Informan sobre el éxito o fracaso de los ataques y monitorizan archivos y procesos para mejorar la detección.
- Aunque más precisos, requieren gestión y configuración en cada host, suponiendo un costo mayor.
- Detectan ataques no descubiertos por NIDS, pueden operar con datos cifrados y proporcionan información sobre el éxito o fracaso de los intentos de ataque.

Ventajas:

- Detectan ataques no descubiertos por NIDS.
- Operan con datos cifrados.
- Informan sobre el éxito o fracaso de los intentos de ataque

Desventajas:

- Mayor costo y gestión que los NIDS.
- No son útiles para detectar ataques en toda la red.
- Consumen recursos del host, afectando el rendimiento

Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad

Tipos de IDS

NIDS (Network Intrusion Detection System) vs. HIDS (Host Intrusion Detection System):

Aspecto	NIDS (Sistema de Detección de Intrusiones Basado en Red)	HIDS (Sistema de Detección de Intrusiones Basado en Host)
Definición	Monitorea y analiza el tráfico en una red completa.	Se centra en la seguridad de un host o sistema individual.
Enfoque	Analiza el tráfico de red en busca de patrones sospechosos.	Examina actividades en un host específico para detectar intrusiones.
Ubicación	Colocado en puntos estratégicos de la red.	Instalado directamente en el host que se va a proteger.
Alcance	Puede detectar amenazas que afectan a múltiples hosts.	Se centra en amenazas dirigidas al host en el que está instalado.
Precisión	Puede generar falsos positivos al analizar el tráfico de red.	Mayor precisión al analizar actividades en el host, reduciendo falsos positivos.
Visibilidad	Tiene una visión general del tráfico de red.	Tiene una visión detallada de las actividades en el host.
Detección	Detecta amenazas mientras atraviesan la red.	Detecta amenazas que afectan directamente al host.
Implementación	Se implementa en dispositivos de red como sensores.	Se implementa en servidores individuales o sistemas finales.
Ejemplos	Snort, Suricata.	Tripwire, OSSEC.
Escalabilidad	Más escalable para redes grandes.	Escalabilidad puede ser un desafío en grandes entornos.

Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad

Tipos de IDS

Los IDS, además, se clasifican según su funcionalidad esencial en dos categorías principales: IDS de detección de abusos o firmas y IDS de detección de anomalías.

IDS de detección de abusos o firmas:

- Estos IDS tienen como función principal identificar eventos que coincidan con patrones predefinidos o firmas que describan ataques conocidos.
- Algunas de sus ventajas incluyen un alto grado de efectividad sin generar muchas falsas alarmas y un diagnóstico rápido del uso de un ataque específico.
- Sin embargo, presentan la desventaja de requerir una actualización constante para mantener su eficacia, ya que deben adaptarse a las nuevas firmas y patrones de ataques.

IDS de detección de anomalías:

- Este tipo de IDS, en contraste con los de detección de abusos, se centra en la identificación de comportamientos inusuales en un host de una red.
- Ventajas: incluyen la capacidad para detectar ataques desconocidos y la posibilidad de definir firmas en la detección de abusos con la información obtenida.
- No obstante, a diferencia de los IDS de detección de abusos, tienden a generar un número elevado de falsas alarmas, ya que no se basan en patrones definidos, lo que puede dificultar la interpretación de la relevancia de cada alerta.

Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad

Tipos de IPS

Los Sistemas de Prevención de Intrusiones (IPS), desarrollados en la década de 1990, tienen como objetivo monitorizar el tráfico en tiempo real y prevenir intrusiones al sistema, considerándose una evolución de los Sistemas de Detección de Intrusiones (IDS). A continuación, se detallan los tipos de IPS:

Características comunes de los IPS:

- Respuesta automática: Actúan automáticamente al producirse un incidente.
- Filtros dinámicos: Aplican nuevos filtros a medida que detectan ataques en curso.
- Reducción de falsas alarmas: Minimizan las alertas erróneas.
- Bloqueo automático: Detienen ataques en tiempo real.
- Optimización del tráfico: Mejoran el rendimiento bloqueando automáticamente ataques.

Ventajas de los IPS:

- Protección preventiva: Actúan antes de que ocurra un ataque.
- Defensa completa: Protegen contra diversas amenazas como vulnerabilidades, tráfico malicioso, códigos dañinos, etc.
- Fácil instalación y gestión: Son simples de configurar y administrar.
- Escalabilidad: Pueden actualizarse según las necesidades de la organización.
- Menor inversión en recursos: Requieren menos recursos que un IDS para su funcionamiento.

Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad

Tipos de IPS

Categorías de IPS según la acción:

IPS de Filtrado de Paquetes: Determinar el tráfico permitido en un equipo o servidor. Ejemplos:

- **Zeek**: Zeek es un marco flexible y adaptable que ofrece análisis profundos de protocolos. Permite un análisis semántico avanzado en la capa de aplicación y se utiliza para monitorear redes de alto rendimiento. Además, Zeek crea registros de transacciones compactos y seguros, lo que facilita su visualización en herramientas como SIEM (Gestión de eventos de información y seguridad)
- **Snort**: Snort es un potente software de detección de código abierto. Utiliza un conjunto de reglas para definir actividades maliciosas en la red y genera alertas para los usuarios.

IPS de Bloqueo de IP: Bloquean direcciones IP causantes de ataques. Ejemplos:

- **SolarWinds Log & Event Manager**: Este software ofrece una prueba gratuita y se enfoca en la gestión de registros y eventos. Además de la detección de intrusiones, también permite bloquear o detener actividades sospechosas.
- **Fail2Ban**: Aunque no es exclusivamente un IPS, Fail2Ban es una herramienta de seguridad que monitorea los registros del sistema en busca de fallos de autenticación. Cuando detecta intentos de intrusión, bloquea las direcciones IP de los atacantes utilizando iptables.

Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad

Tipos de IPS

Categorías de IPS según la acción:

IPS con Acción de Decepción: Engañan al atacante emitiendo información falsa. Ejemplos:

- **Sagan**: Sagan es un sistema de detección de intrusiones que se integra bien con Snort. Además de detectar actividades sospechosas, Sagan puede enviar su salida a Snort, lo que le brinda a la herramienta algunas capacidades de detección de intrusos basadas en la red.

Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

Una vez que se ha definido el tipo de IDS/IPS a implementar, surge una pregunta crucial para las organizaciones: ¿dónde colocarlo? La elección de la ubicación de los sistemas IDS/IPS dependerá del hardware seleccionado y del software que se va a desplegar.

Siguiendo criterios de seguridad, se pueden identificar tres zonas para situar un sistema IDS/IPS:

- **Zona Roja**: Esta área representa un riesgo elevado. En la Zona Roja, el IDS/IPS debe configurarse con baja sensibilidad, ya que supervisará todo el tráfico de la red, lo que podría generar un número significativo de falsas alarmas.

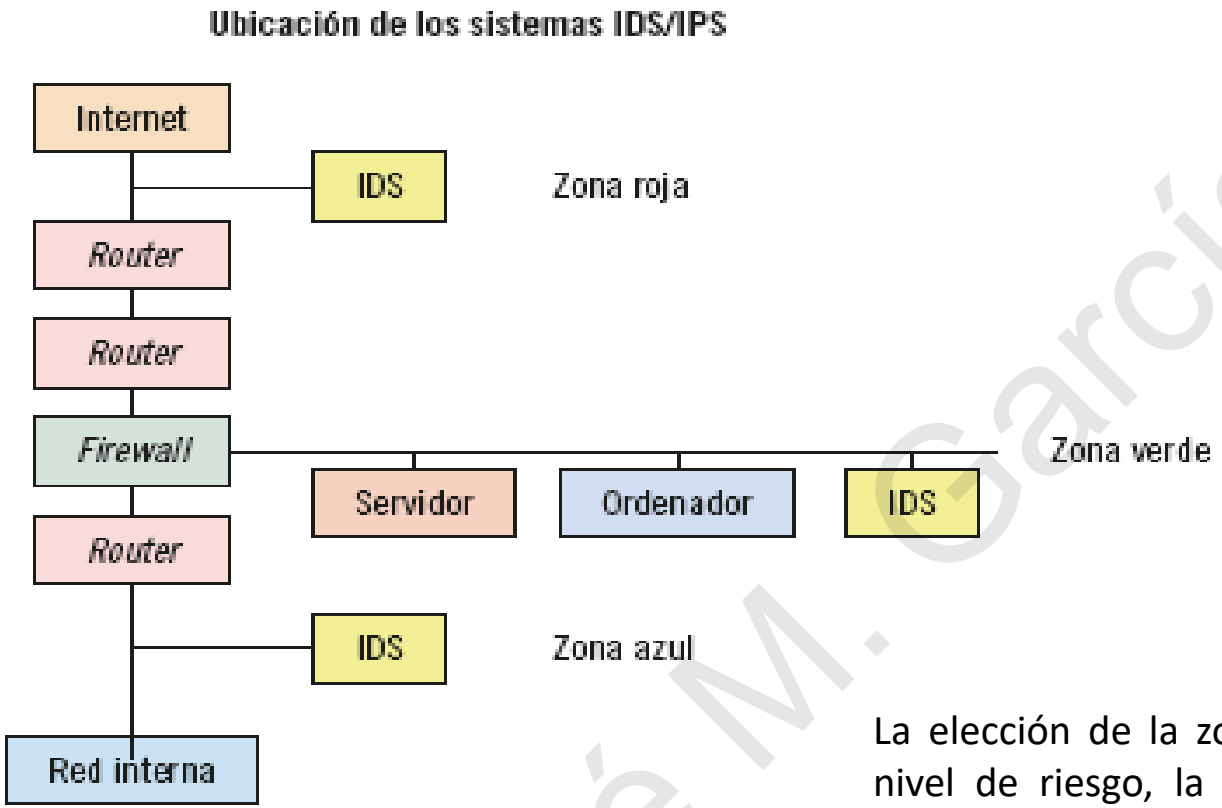
- **Zona Verde**: Con un riesgo menor que la Zona Roja, aquí el IDS/IPS debe configurarse con mayor sensibilidad, ya que el cortafuegos realiza un filtrado de accesos predefinidos por la organización. La Zona Verde experimenta menos falsas alarmas en comparación con la Zona Roja.

- **Zona Azul**: Designada como la zona de confianza, cualquier acceso anómalo en esta área se considera hostil. Aunque hay menos accesos en esta zona, también se reduce considerablemente el número de falsas alarmas. Es imperativo analizar con detenimiento cualquier falsa alarma detectada por el sistema IDS/IPS.

A pesar de considerarse una zona de confianza con tráfico limitado, los IDS/IPS en la Zona Azul no forman parte de la red interna del sistema, y por ende, no analizan el tráfico interno de la red.

se refiere a que son IDS/IPS de host

Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS



La elección de la zona para situar un sistema IDS/IPS dependerá del nivel de riesgo, la tolerancia a falsas alarmas y las preferencias de análisis de datos de la organización.

Este enfoque estratégico garantiza una implementación efectiva y personalizada de los sistemas IDS/IPS en la organización.

Resumen

Un incidente de seguridad abarca cualquier evento que ponga en riesgo la integridad, confidencialidad y disponibilidad de la información de una organización, lo que puede tener graves consecuencias para sus operaciones y seguridad.

Estos incidentes pueden manifestarse de diversas formas, como accesos no autorizados, ataques de código malicioso, denegación de servicio, entre otros, lo que requiere que las organizaciones implementen medidas para corregir, prevenir o detectar estos eventos.

La gestión de incidentes busca organizar los recursos de manera eficiente para aplicar estas medidas, utilizando herramientas como el Visor de eventos de Windows o comandos en Linux para monitorear los registros de eventos.

Una vez que se comprende cómo localizar estos eventos, es crucial establecer sistemas de prevención o detección de intrusiones como parte integral de la estrategia de seguridad de la organización.

La elección de la ubicación de estos sistemas, basada en criterios de riesgo y confianza, es otra decisión crítica que afectará la efectividad del sistema de seguridad de la organización, minimizando el riesgo y las falsas alarmas.