FICHA DE CERTIFICADO DE PROFESIONALIDAD			
(IFCT0109) SEGURIDAD INFORMÁTICA (R. D. 686/2011, de 13 de mayo modificado por el R. D. 628/2013, de 2 de agosto)			
COMPETENCIA GENERAL: Garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y el interior de la organización.			
Cualificación profesional de referencia	**Unidades de competencia**		**Ocupaciones o puestos de trabajo relacionados:**
IFC153_3 SEGURIDAD INFORMÁTICA (R. D. 1087/2005, de 16 de septiembre)	UC0486_3	Asegurar equipos informáticos	▪ 3820.1017 Programador de Aplicaciones Informáticas ▪ 3812.1014 Técnico en Informática de Gestión ▪ Técnico en seguridad informática. ▪ Técnico en auditoría informática.
	UC0487_3	Auditar redes de comunicación y sistemas informáticos	
	UC0488_3	Detectar y responder ante incidentes de seguridad	
	UC0489_3	Diseñar e implementar sistemas seguros de acceso y transmisión de datos	
	UC0490_3	Gestionar servicios en el sistema informático	

Correspondencia con el Catálogo Modular de Formación Profesional		
Módulos certificado	Unidades formativas	Horas
MF0486_3: Seguridad en equipos informáticos		90
MF0487_3: Auditoría de seguridad informática		90
MF0488_3: Gestión de incidentes de seguridad informática		90
MF0489_3: Sistemas seguros de acceso y transmisión de datos		60
MF0490_3: Gestión de servicios en el sistema informático		90
MP0175: Módulo de prácticas profesionales no laborales		80

Índice

Capítulo 3

Control de código malicioso

Capítulo 4

Respuesta ante incidentes de seguridad

Capítulo 5

Proceso de notificación y gestión de intentos de intrusión

Capítulo 1

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

Contenido

1. 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.

Hay numerosas motivaciones por las que un atacante puede actuar en una organización: desde motivos económicos, por simple diversión, por disconformidad con sus directrices o valores o por la mera autorrealización personal, entre muchas otras.

A medida que avance el manual se irán comentando los distintos tipos de ataques y cómo prevenirlos y combatirlos y, en este capítulo en particular se van a identificar y caracterizar los distintos datos de funcionamiento del sistema donde localizar las incidencias que le suceden.

También se van a describir y analizar varias técnicas para detectar y prevenir el ataque de intrusos mediante una serie de herramientas como son los sistemas de prevención de intrusiones o IPS y los sistemas de detección de IDS, comentando detalladamente sus características principales y sus funcionalidades.

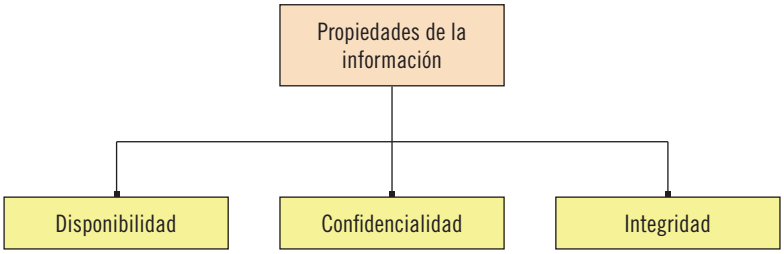
Para concluir el capítulo, una vez que ya se han descrito las herramientas necesarias para decidir qué sistema de prevención o detección de intrusos van a implantar las organizaciones en sus sistemas de información, se aportan una serie de pautas a tener en cuenta en el momento de elegir la ubicación de estos IDS y/o IPS atendiendo a las necesidades concretas de cada organización.

2. Conceptos generales de gestión 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.

Propiedades de seguridad informática



En términos de seguridad informática para que la información cumpla unos estándares de seguridad adecuados debe contener las tres propiedades mostradas en la imagen: 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 27001:2005, 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.

Nota

ISO es la Organización Internacional de Normalización. Esta organización elaboró una serie de normas internacionales que formulan recomendaciones de buenas prácticas para las empresas, entre ellas la ISO 2700:2005 que hace referencia a la seguridad de la información.

2.1. Tipos de incidentes de seguridad

Son numerosos los tipos de incidentes de seguridad que pueden ocurrir en un sistema. Una posible clasificación sería la siguiente:

- Accesos no autorizados: son ingresos y operaciones no autorizadas a los sistemas, con éxito o no. Forman parte de esta categoría:
  - Robo de información.
  - Borrado de información.
  - Accesos no autorizados exitosos.
  - Alteración de la información.
  - Intentos recurrentes y no recurrentes de acceso no autorizado.
  - Abuso o mal uso de los servicios informáticos (tanto internos como externos) que requieran autenticación.
- Código malicioso o *malware:* son incidentes que se infiltran en un sistema de información sin autorización del propietario. Son incidentes de código malicioso los siguientes:
  - Virus informáticos.
  - Troyanos: código malicioso que se introduce en el sistema informático como un programa aparentemente legítimo e inofensivo pero que, al ejecutarlo, permite el acceso remoto del sistema a usuarios no autorizados.

- Gusanos informáticos: código malicioso que, una vez ha accedido al sistema, se va duplicando a sí mismo. No altera los archivos ya instalados pero supone un consumo de recursos importante.

- Denegación del servicio: eventos que producen la pérdida de un servicio en particular, impidiendo su ejecución normal. Suelen ser incidentes de denegación del servicio cuando en el sistema se nota que hay tiempos de respuesta muy bajos y servicios internos y externos inaccesibles sin motivos aparentes.

- Pruebas, escaneos o intentos de obtención de información de un sistema de información: son eventos que intentan obtener información sobre las acciones que se producen en un sistema informático. Algunos de estos eventos son:

  - *Sniffers:* aplicaciones cuya función es obtener la información que envían los distintos equipos de una red.
  - Detección de vulnerabilidades: aplicaciones que buscan las vulnerabilidades de un sistema de información para aprovecharse de ello maliciosamente.

- Mal uso de los recursos tecnológicos: eventos que atacan a los recursos tecnológicos de un sistema de información a causa de un mal uso de los mismos. Forman parte de este tipo de eventos:

  - Violación de la normativa de acceso a internet.
  - Abuso o mal uso de los servicios informáticos externos o internos.
  - Abuso o mal uso del correo electrónico.
  - Violación de las políticas, normas y procedimientos de seguridad informática de una organización.

Incidentes de seguridad	
Tipo de incidente	**Incidente**
Acceso no autorizado	Accesos no autorizados con éxito.
	Robo de información.
	Alteración de la información.
	Borrado de la información.
	Intentos de acceso no autorizado recurrentes y no recurrentes.
	Mal uso o abuso de los servicios informáticos que necesitan autenticación.
Código malicioso	Virus informáticos.
	Troyanos.
	Gusanos informáticos.
Denegación del servicio o DoS	Ataques a páginas web o servidores para saturarlos.
Intentos de obtención de información	*Sniffers.*
	Detección de vulnerabilidades.
Mal uso de los recursos	Abuso o mal uso de los servicios informáticos (internos o externos).
	Violación de la normativa de acceso a internet.
	Abuso o mal uso del correo electrónico.
	Violación de políticas de seguridad informática.

2.2. Gestión y medidas de incidentes de seguridad

Ante la posibilidad de que haya algún tipo de incidente de seguridad en la organización hay que tomar una serie de medidas que pueden ser:

- Medidas preventivas: aquellas medidas que se aplican para evitar la ocurrencia de incidentes de seguridad. Algunos ejemplos son: utilización de contraseñas, cifrado de información, establecimiento de *firewalls,* etc.
- Medidas de detección: medidas que sirven para detectar y controlar los incidentes de seguridad. Por ejemplo: auditorías de seguridad, revisiones de seguridad, etc.

- Medidas correctivas: medidas implementadas una vez ya ha sucedido el incidente de seguridad que sirven para evitar que no vuelvan a ocurrir y para restaurar la situación inicial antes de la incidencia. Suelen ser procedimientos de restauración, eliminación de código malicioso y auditoría forense.

La gestión de incidentes tiene como objetivo calcular y utilizar adecuadamente los recursos necesarios para aplicar correctamente estas medidas de prevención, detección y corrección de incidentes de seguridad. Se establecen unas pautas generales a seguir para que esta gestión esté bien ejecutada:

- Prevención de los incidentes: aplicación de las medidas preventivas que eviten la producción de los incidentes.
- Detección y reporte de los incidentes: en caso de producirse el incidente hay que detectarlo y reportar el mismo a los responsables de su gestión.
- Clasificación del incidente: definición del tipo de incidente que ha ocurrido (acceso no autorizado, robo de información, etc.).
- Análisis del incidente: análisis de cómo se ha producido el incidente y de los daños que ha causado.
- Respuesta al incidente: aplicación de las medidas correctivas para restaurar el sistema a la situación inicial antes de producirse el incidente.
- Registro de incidentes: registro del incidente sucedido y de las medidas aplicadas para obtener un historial y un control de todos los registros que han ido ocurriendo.
- Aprendizaje: análisis de los posibles errores causantes de la incidencia para evitar que se vuelvan a producir.

Siguiendo estas fases de gestión de incidentes, las organizaciones pueden obtener numerosos beneficios, entre ellos:

- Rápida, eficiente y sistemática respuesta ante la aparición de incidentes.
- Rápida restauración del sistema informático garantizando la mínima pérdida de información posible.
- Generación de una base de datos con el histórico de los incidentes y de las medidas tomadas para una mayor rapidez ante próximos incidentes.
- Mejora continua de la gestión y tratamiento de incidentes.

- Eliminación de la aparición de incidentes repetitivos (gracias al registro histórico).
- Optimización de los recursos disponibles.
- Mayor productividad de los usuarios.
- Mayor control de los procesos del sistema de información y del proceso de monitorización del mismo.

Sin embargo, una gestión de incidentes deficiente puede llevar a efectos adversos importantes:

- Desperdicio y bajo rendimiento de los recursos.
- Pérdida de información valiosa para la organización.
- Pérdida de productividad en los servicios y, como consecuencia, peor calidad de servicio a los clientes.

2.3. Detección de intrusiones y su prevención

Los intentos de intrusión son aquellos intentos que pueden afectar negativamente a la confidencialidad, integridad y disponibilidad de la información de un equipo o que intentan evitar los mecanismos de seguridad que hay establecidos.

Estas intrusiones pueden producirse de varios modos: desde usuarios no autorizados que acceden al sistema a través de internet, usuarios que sí están autorizados pero que intentan acceder a privilegios para los que no tienen autorización, hasta usuarios autorizados que utilizan malintencionadamente los privilegios que les han sido otorgados.

Para evitar este tipo de intrusiones están los sistemas de prevención de intrusiones o IDS que son sistemas que permiten establecer una protección adicional a los equipos y redes de una organización ante las posibles amenazas que pueden aparecer debido al uso exhaustivo de las redes y de los sistemas de información externos.

Actividades

1. Ponga varios ejemplos de los distintos tipos de incidencias de seguridad.
2. Busque más información sobre las medidas correctivas, preventivas y de detección y proponga algún ejemplo de cada una de ellas.

Aplicación práctica

Su socio y usted están evaluando la seguridad de los equipos de su empresa y han detectado una serie de ataques de código malicioso y ataques de denegación de servicios. Para conseguir eliminar estos ataques y devolver los sistemas al estado original, ¿qué tipo de medidas deberán tomar? ¿Preventivas, de detección o correctivas?

SOLUCIÓN

Las medidas preventivas sirven para evitar que no ocurran los incidentes de seguridad. Las medidas de detección sirven para detectar los distintos tipos de incidentes.

En este caso, los incidentes ya se han producido y se pretende corregir la situación y restaurar los sistemas para minimizar el daño ocasionado e intentar volver a la situación original antes de la producción de las incidencias. Por ello, las medidas que se deberán tomar en esta ocasión son medidas de carácter correctivo que eliminen los ataques y restauren el sistema.

3. Identificación y caracterización de los datos de funcionamiento del sistema

Un *log* es un registro oficial de los eventos del sistema producidos a lo largo de un período de tiempo determinado. En los *logs* se registran datos de eventos referentes a:

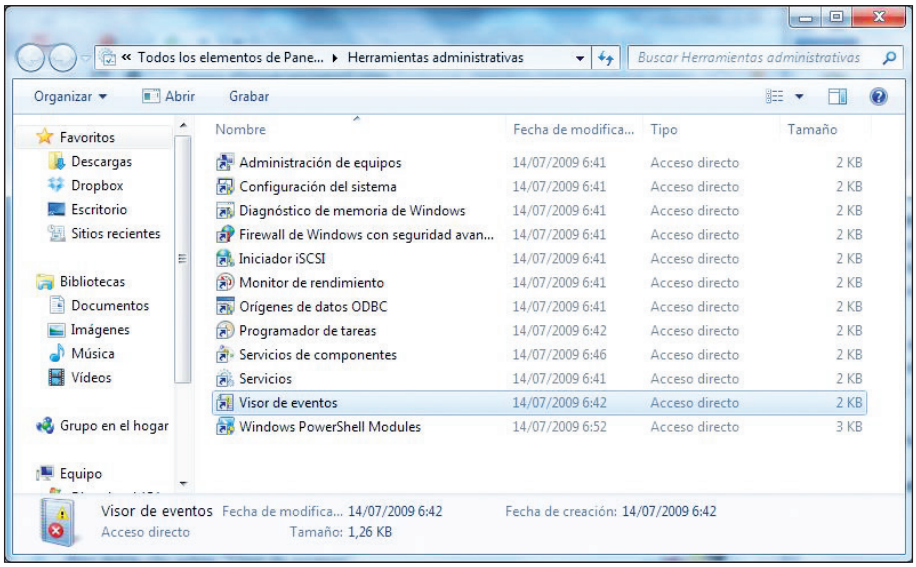
- Qué tipo de evento ha ocurrido.
- Quién ha originado el evento.
- Cuándo se ha producido el evento.
- Dónde se ha producido el evento.
- Por qué se ha producido el evento.

Así, para comprobar el correcto funcionamiento del sistema e identificar los distintos eventos sucedidos se recomienda evaluar los *logs* de los equipos, ya que se podrán detectar fallos y eventos como:

- Incidentes de seguridad.
- Funcionamientos anómalos.
- Cambios de configuración de aplicaciones o dispositivos.
- Utilización y rendimiento de los recursos.
- Intentos fallidos de acceso de usuarios no autorizados.

Tanto *Windows* como *Linux* ofrecen la posibilidad de visualizar estos *logs* y eventos para detectar y seguir los distintos eventos que han ido sucediendo en el equipo.

En *Windows* se puede utilizar el "Visor de eventos" accediendo a **Inicio -> Configuración -> Panel de control -> Herramientas administrativas -> Visor de eventos:**

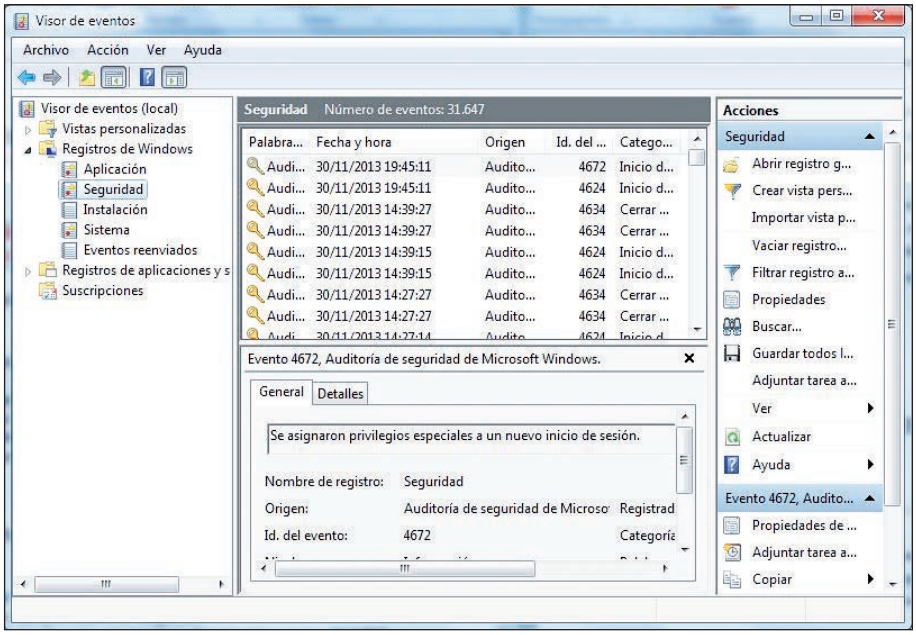


Panel de control, herramientas administrativas

Con esta herramienta se pueden visualizar distintos tipos de eventos sucedidos junto con la fecha y hora, el origen, su identificador, el usuario que lo ha generado y otras características:

- Registros de aplicación: eventos registrados por aplicaciones o programas.
- Registros de seguridad: eventos ocurridos en los accesos del sistema como los intentos de inicio de sesión (tanto exitosos como fallidos), las introducciones de contraseñas erróneas, la utilización de los recursos, etc.
- Registros de instalación: eventos que hacen referencia a la instalación de aplicaciones en el equipo. Se suelen utilizar para comprobar si se ha instalado algún código malicioso en el equipo.
- Registros de eventos reenviados: eventos que se han reenviado a este registro desde otros equipos.

En este caso, como se pretenden detectar las intrusiones y los distintos fallos de seguridad sucedidos en el equipo, el tipo de registros al que más atención habrá que prestar es a los registros de seguridad:



Visor de eventos de Windows

En cambio utilizando *Linux* no hay una aplicación gráfica que permita visualizar los eventos de un equipo. Para ello será necesario acceder a los archivos de registro iniciando la sesión como usuario *"root"* y utilizar una serie de comandos:

- Con el comando **tail –f** se ven las últimas líneas de un archivo y sus actualizaciones. Por ejemplo, utilizando **tail –f/var/log/auth.log** se mostrarán los últimos eventos de autenticación como sesiones nuevas.
- Con el comando **less +F** en lugar de acceder a las últimas líneas de un archivo de registro se accede a su totalidad, pudiéndose ver, incluso, las actualizaciones del mismo a tiempo real.

Para finalizar estos comandos se pulsa la combinación de teclas [Ctrl + C] y en el caso del comando **less +F** se pulsa además la tecla [Q].

Los principales archivos de registro que se utilizan para comprobar el funcionamiento del sistema y sus problemas de seguridad se pueden observar en la tabla siguiente:

Nombre de archivo	Funcionalidad
/var/log/auth.log	Eventos de autenticación de usuarios y permisos.
/var/log/boot.log	Eventos y servicios empezados cuando se inicia el sistema.
/var/log/daemon.log	Mensajes sobre permisos o servicios corriendo en el sistema.
/log/dmesg.log	Mensajes del núcleo Linux.
/var/log/errors.log	Errores del sistema.
/var/log/everything.log	Mensajes misceláneos no cubiertos por los 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	Muestra información acerca de los procesos usados por el usuario.

De este modo, tanto con *Windows* como con *Linux,* mediante las herramientas de visualización de *logs* y de eventos que se han visto hasta ahora, se pueden comprobar y evaluar los distintos parámetros de funcionamiento de un sistema o de un equipo. Así, se podrán detectar las distintas deficiencias de la gestión de recursos e incidentes de un sistema y analizar de dónde provienen y poder establecer una serie de medidas correctivas que permitan una eficiente gestión del equipo.

Asimismo, mediante el historial de *logs* y eventos también se pueden observar los eventos repetidos perjudiciales para el equipo y encontrar aquellas medidas que eviten que vuelvan a suceder mejorando significativamente el rendimiento del equipo y aumentando la seguridad del mismo.

Actividades

3. Según el sistema operativo que haya instalado en su equipo, explore con detenimiento el "Visor de eventos "de *Windows* o los archivos de registro en *Linux*.

Aplicación práctica

Ana, Carlos y usted pretenden definir la seguridad de los equipos de la organización y quieren observar los distintos eventos de seguridad que se han producido en la última semana. Teniendo en cuenta que en los equipos tienen instalado el sistema operativo *Windows,* ¿qué herramienta deben utilizar y cómo deben acceder a ella y a los registros de seguridad del sistema?

SOLUCIÓN

En *Windows,* para visualizar los distintos eventos de seguridad producidos en un determinado tiempo hay que acceder al **Visor de eventos** mediante **Inicio -> Configuración -> Panel de control -> Herramientas administrativas -> Visor de eventos.**

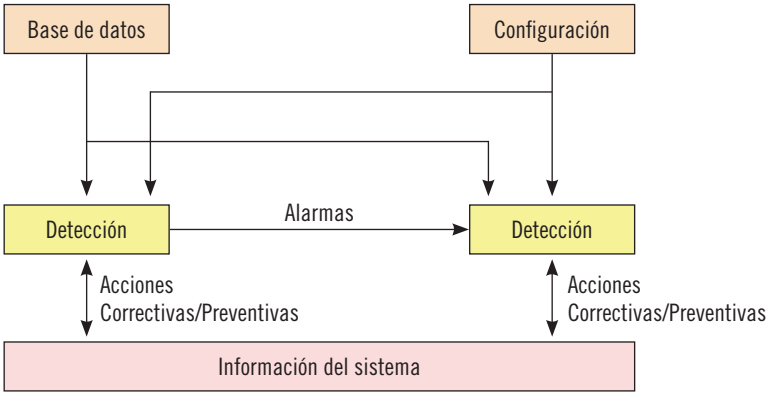
Una vez se ha accedido al "Visor de eventos" para ver el historial de los registros de seguridad de cada equipo bastará con hacer *clic* sobre la pestaña **Registros de seguridad** y ahí aparecerán los eventos con detalles como su identificador, fecha y hora y usuario, entre otros.

4. Arquitecturas más frecuentes de los sistemas de detección de intrusos

Los sistemas de detección de intrusos o IDS *(Intrusion Detection System)* son programas cuya utilidad es detectar las intrusiones que se pueden producir en la red o en un equipo. Se encargan de monitorizar los eventos del equipo para buscar intentos de intrusión.

Los IDS son una especie de proceso de auditoría. Son aplicaciones que mediante una amplia base de datos y una serie de configuraciones consiguen prevenir y detectar los posibles ataques que pueden producirse en un sistema. Una visión gráfica del funcionamiento de un IDS podría ser la siguiente:

Funcionamiento de un IDS



Las ventajas que proporcionan los sistemas de detección de intrusos son numerosas. No obstante, son varios los motivos que justifican la utilización de IDS en las organizaciones:

- Previenen de posibles problemas porque disuaden individuos hostiles: los IDS posibilitan el descubrimiento de atacantes al sistema, lo que resulta un elemento disuasorio ante la posibilidad de ser descubiertos y penalizados.
- Detectan ataques y otras vulneraciones de la seguridad que otros sistemas de protección no previenen: en numerosas ocasiones los atacantes acceden sin autorización a los equipos aprovechando sus vulnerabilidades. Mediante los IDS se pueden detectar estos intentos de acceso y reportarlos de inmediato al administrador, de modo que puedan aplicarse medidas correctivas lo antes posible y minimizar el daño.
- Detectan preámbulos de ataques: normalmente, antes de intentar acceder y atacar a un sistema, los atacantes suelen examinarlo y hacer pruebas para tantear el ataque. Los IDS detectan estas pruebas de red

y accesos al sistema lo que permite aumentar la seguridad cuando hay este tipo de detecciones para poder evitar futuros ataques.

- Justifican y documentan el riesgo de la organización: en el momento en el que se elaboran las políticas de seguridad de la empresa es necesario realizar una evaluación de los riesgos justificada con indicadores y datos. Los IDS permiten conocer estos riesgos y documentarlos, de modo que la política de seguridad establecida y las decisiones que se tomen en relación a esta estarán correctamente justificadas.
- Aportan información útil sobre las intrusiones y ataques que se producen en el equipo: aparte de bloquear los ataques e intentos de ataque del sistema, los IDS también recogen información útil de estos ataques que puede utilizarse como prueba de delito en el momento de querer emprender acciones legales.

Arquitectura de los IDS

Actualmente hay varias propuestas en el mercado sobre la arquitectura de IDS y no hay ninguna de ellas que se utilice de modo estándar, lo que provoca que las organizaciones que trabajan con distinta arquitectura IDS tengan dificultades para interoperar entre sí.

No obstante, hay ciertas peculiaridades comunes en las distintas arquitecturas de IDS:

- La fuente de recogida de datos. Las fuentes pueden ser *logs,* dispositivos de red o el mismo sistema de información.
- Las reglas que definen los patrones y directrices para detectar las anomalías de seguridad de un sistema.
- Los filtros que comparan los datos o los *logs* que se han obtenido con los patrones definidos en las reglas.
- Los detectores de los eventos anormales que suceden en el tráfico de la red.
- El sistema que genera los informes y las alarmas en caso de encontrar alguna intrusión o ataque.

Nota

La seguridad de la información en las organizaciones es un asunto primordial para garantizar su éxito. A pesar de que es imposible conocer todas las vulnerabilidades de un sistema y que cada día surgen vulnerabilidades nuevas, los IDS son una herramienta muy útil para detectarlas y solucionarlas. Aún así, como única medida de seguridad no son suficientes: es necesario establecer medidas adicionales como cortafuegos o IPS, entre otras.

A pesar de estos rasgos comunes son muchas las diferencias que hay entre las arquitecturas de los IDS. A continuación se describirán las arquitecturas de IDS más importantes en el mercado actual.

Arquitectura CIDF *(Common Intrusion Detection Framework)*

La arquitectura CIDF *(Common Intrusion Detection Framework)* fue promovida por la Agencia Federal de Estados Unidos DARPA *(Defense Advanced Research Projects Agency)* y, aunque no logró establecerse como un estándar, determinó un modelo y un vocabulario general para tratar las intrusiones.

Esta arquitectura contempla cuatro tipos básicos de equipos:

- Equipos generadores de eventos o Equipos E: equipos cuya función principal es la detección de eventos y la emisión de informes.
- Analizadores de eventos o Equipos A: equipos que reciben los informes emitidos y se encargan de realizar los análisis pertinentes.
- Base de datos de eventos o Equipos D: componentes de bases de datos que permiten ver el historial de los eventos sucedidos en el sistema.
- Equipos de respuesta o Equipos R: obtienen los datos de los demás tipos de equipos (E, A y D) y responden a los eventos sucedidos en el sistema.

Arquitectura CISL *(Common Intrusion Specification Language)*

La arquitectura CISL *(Common Intrusion Specification Language)* o lenguaje de especificación de intrusiones común surge por la necesidad de unir los cuatro tipos de equipos que se definieron en la arquitectura CISL. En esta arquitectura deben poder transmitirse los siguientes tipos de información:

- Información de eventos en grupo: une los equipos C y A definidos en la arquitectura CIDF. Proporciona información sobre el tráfico de red del sistema y sobre la auditoría de registros.
- Resultados de los análisis: une los equipos A y D y facilita información como las características de las anomalías sucedidas en el sistema y de los ataques que se han detectado.
- Prescripciones de respuestas: une los equipos A y R y se encarga de detener ciertas actividades y de modificar los parámetros de seguridad de componentes para responder a posibles ataques.

Arquitectura AusCERT

La arquitectura AusCERT (CERT australiano) es mucho más simple que las dos anteriores (CIDF y CISL) y facilita en unas pocas líneas un informe en una base de datos de un incidente sucedido en el sistema.

Un ejemplo de informe que proporciona AusCERT podría ser el siguiente:

Ejemplo de informe AusCERT

```
Source: 216.37.42.84
Ports: tcp 111
Incident type: Network_scan
Re-distribute: yes
Timezone: GMT -1
Reply: yes
Time: Sat 14 November 2013 at 15:30 (UTC)
```

La ventaja principal de esta arquitectura es que es muy sencilla para construirla y analizarla. Eso sí, en el momento en el que se requiera una información detallada de los eventos e incidencias sucedidos en el sistema se deberá tener en cuenta que AusCERT es muy limitada ya que su nivel de detalle es mínimo.

Arquitectura IDWG *(Instrusion Detection Working Group)*

La arquitectura IDWG *(Intrusion Detection Working Group)* propone un nuevo formato (el formato IDEF o *Instrusion Detection Exchange Format)* cuya función principal es la definición de formatos y procedimientos de intercambio de información entre los diversos subsistemas del IDS. Facilita el intercambio de información acerca de los incidentes de seguridad.

En esta arquitectura se distinguen tres módulos distintos:

- Sensor: recoge los datos de la fuente de datos, datos que el IDS utiliza para detectar las actividades no autorizadas. Son ejemplos de este tipo de datos los paquetes de red, *logs* de aplicaciones, *logs* del sistema operativo, etc.
- Analizador: analiza los datos recopilados por el sensor para detectar los accesos y/o actividades no autorizados.
- Manager: componente que gestiona y administra los demás elementos del IDS. Configura los sensores y analizadores, consolida los datos obtenidos, genera los informes mediante los datos facilitados por el analizador, etc.

Con estos tres módulos de la arquitectura IDWG se obtienen resultados como los siguientes:

- Lenguaje común que describe el formato de los datos.
- Documentos que recogen los distintos requerimientos funcionales de alto nivel que permiten la comunicación entre los IDS y entre los IDS y sus sistemas de gestión de incidentes.
- Identificación y definición de los protocolos más apropiados para la comunicación entre IDS y para el establecimiento del formato de los datos.

Como resumen, en la siguiente tabla se muestran las distintas arquitecturas IDS y sus características principales:

Tipo de arquitectura IDS	Características
CIDF (Common Intrusion Detection Framework)	Consta de generador, analizador y base de datos de eventos además de unidades de respuesta ante la aparición de incidentes. Tuvo escasa aceptación en el mercado.
CISL (Common Intrusion Specification Language)	Une los distintos equipos que forman parte de la arquitectura CIDF y facilita información sobre información de eventos en bruto, resultados de los análisis y prescripciones de respuestas.
AusCERT	Arquitectura simple que facilita la información de las incidencias en muy pocas líneas. Es muy limitada si se pretende obtener información detallada de las incidencias.
IDWG (Intrusion Detection Working Group)	Facilita el intercambio de información sobre los incidentes de seguridad y permite definir los protocolos y formatos de intercambio de información entre los IDS.

Actividades

4. Busque información adicional sobre las distintas arquitecturas de sistemas de detección de intrusos. ¿Cuál de ellas considera más adecuada para las organizaciones? Justifique su respuesta.
5. En este epígrafe se han mencionado varios motivos por los que se recomienda la implantación de un IDS en las organizaciones. ¿Echa en falta algún motivo adicional? Propóngalo y justifíquelo.

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

En este epígrafe se van a describir los distintos tipos de IDS/IPS por ubicación y funcionalidad distinguiendo entre los sistemas de detección de intrusiones (o IDS) y los sistemas de prevención de intrusiones (IPS).

5.1. Tipos de IDS

Atendiendo a su ubicación hay varios tipos de sistemas de detección de intrusos o IDS que se especificarán a continuación.

IDS basados en red (NIDS)

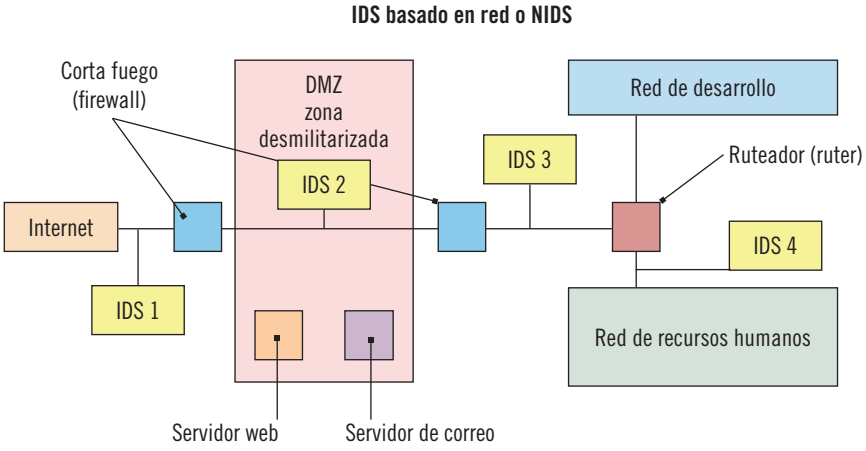
Los IDS basados en red detectan los ataques mediante la captura y análisis de los paquetes de la red. La gran mayoría de los IDS están basados en red. Una vez capturados y analizados los paquetes de la red, los IDS se encargan de buscar patrones que supongan algún tipo de ataque.

Los NIDS analizan el tráfico de toda la red examinando paquetes para buscar opciones no permitidas y diseñadas para no ser detectadas por los cortafuegos. Además, emite alertas cuando hay intentos de acceso o análisis externo de alguna vulnerabilidad del sistema.

Su funcionamiento consiste en:

- Unos sensores o agentes que se sitúan en varios puntos de la red para monitorizar el tráfico buscando tráfico sospechoso. Lo habitual es que estos sensores analicen los paquetes en modo oculto para no ser descubiertos.
- Una consola que recibe las alarmas emitidas por los sensores y que, atendiendo al tipo de alarma, producirá algún tipo de respuesta.

Un ejemplo de NIDS está reflejado en la imagen siguiente:



Como se puede observar, hay IDS (sensores) situados en varios puntos de la red que se encargan de monitorizar el tráfico que hay entre ellos. De este modo se pueden detectar las incidencias sucedidas a lo largo de toda la red del sistema y reaccionar ante ellas.

Hay una serie de ventajas de este tipo de IDS:

- Detectan accesos no deseados en la red.
- No requieren la utilización de un *software* adicional en los servidores para poder funcionar.
- Son sistemas de fácil instalación y actualización.
- Tienen un bajo impacto en la red al no intervenir en sus operaciones habituales.
- Pueden monitorizar redes de grandes dimensiones siempre que haya capacidad suficiente para analizar todo su tráfico.

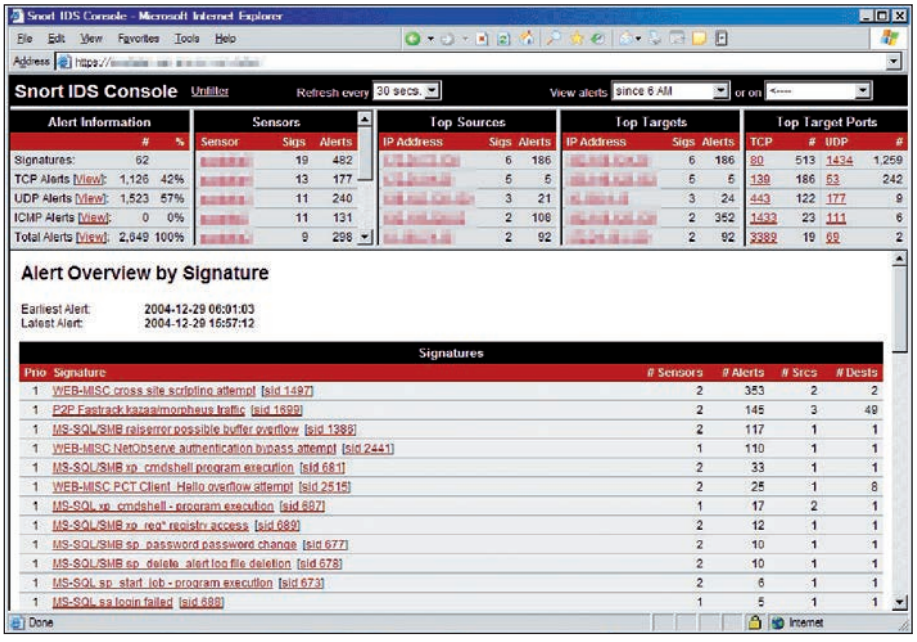
No obstante, los NIDS también conllevan una serie de desventajas:

- A pesar de poder monitorizar redes grandes pueden presentar dificultades en su procesamiento y fallar en el reconocimiento de ataques producidos en momentos de elevado nivel de tráfico de red.
- Los NIDS tienen dificultades para detectar los ataques con información cifrada.

- Los NIDS se limitan a detectar los ataques lanzados, independientemente de si han tenido éxito o no, lo que implica que ante cada ataque detectado los administradores deben analizarlo uno a uno para comprobar el éxito o fracaso del mismo.
- Pueden presentar problemas cuando tienen que detectar ataques que viajan en paquetes fragmentados.

Uno de los NIDS más utilizados es *Snort,* una herramienta que, además de facilitar la información de los paquetes de red, es diferenciada de las demás por suministrar información completa y precisa en el registro de actividades maliciosas de la red. Además, notifica a los administradores la detección de potenciales violaciones de la red. Como características principales destacan:

- Dispone de más de 700 firmas en su base de datos.
- Es de distribución gratuita.
- Analiza el tráfico de la red en tiempo real.
- Permite la utilización de filtros en la detección de ataques.



NIDS Snort

IDS basados en host (HIDS)

Los IDS basados en *host* o HIDS detectan las intrusiones a nivel de un equipo informático, analizando su tráfico para comprobar si ha habido algún tipo de alteración de los archivos del sistema operativo y para localizar actividades sospechosas. Fueron el primer tipo de IDS desarrollado e implementado.

Al trabajar sobre un equipo y no sobre el tráfico de la red ofrece una gran precisión en el análisis de las actividades, pudiendo detectar de un modo exacto los procesos y usuarios que han estado involucrados en un ataque en concreto dentro de un sistema operativo.

A diferencia de los NIDS, los IDS basados en *host* informan del resultado del ataque en cuanto a su éxito o fracaso. Además, también monitorizan los ficheros y los procesos del sistema atacado para una mejor detección y respuesta ante los ataques.

Sus funcionalidades principales se concretan en:

- Análisis del tráfico sobre un servidor o sobre un equipo concreto.
- Detección de los intentos de acceso, tanto fallidos como exitosos.
- Detección de las modificaciones realizadas en archivos críticos.

Como ventajas importantes, los HIDS destacan por:

- Detectan ataques que no pueden descubrir los NIDS al poder monitorizar los eventos locales del equipo o *host.*
- Pueden operar y detectar ataques ante datos cifrados que circulan por la red porque analizan los datos en el *host* de origen antes de ser cifrados o los datos en el *host* de destino una vez ya han sido descifrados.
- Facilitan información sobre el éxito o fracaso de los intentos de ataque.

Sin embargo, los IDS basados en *host* también cuentan con una serie de desventajas:

- Suponen un coste mayor que los NIDS ya que hay que gestionarlos y configurarlos en cada *host* que se quiere monitorizar.

- No son útiles cuando se pretende detectar ataques a toda una red, ya que los HIDS solo analizan los paquetes de red que entran en el *host* en el que están instalados.
- Suponen un consumo de recursos del *host* al que monitorizan, lo que implica una disminución del rendimiento del sistema.
- Los HIDS corren el peligro de ser deshabilitados por algunos DoS.

Recuerde

Los DoS son ataques de denegación del servicio. Estos ataques se realizan a equipos o a redes e impiden al usuario el acceso a un servicio o recurso determinado para el que está legitimado.

Además, los IDS también se pueden clasificar atendiendo a su funcionalidad fundamental:

- IDS de detección de abusos o firmas.
- IDS de detección de anomalías.

IDS de detección de abusos o firmas

Los IDS de detección de abusos o firmas tienen como funcionalidad principal buscar eventos que coincidan con un patrón predefinido o con una firma que describa un ataque conocido.

Entre las ventajas de este tipo de IPS destacan:

- Elevado grado de efectividad sin generar en exceso falsas alarmas.
- Rápido diagnóstico del uso de un ataque determinado.

Sin embargo, también tiene como desventaja la constante necesidad de actualización continua para que la detección de los abusos o firmas sea eficaz.

IDS de detección de anomalías

Este tipo de IDS, en lugar de buscar abusos conforme a unos patrones, tiene como función principal la detección de comportamientos inusuales que sucedan en un *host* de una red. Sus ventajas principales son:

- La elevada capacidad de detectar ataques de los que no hay un conocimiento determinado.
- La posibilidad de definir firmas en la detección de abusos con la información que obtienen.

Sin embargo, al contrario que con los IPS de detección de abusos o firmas, este tipo de IPS genera un elevado número de falsas alarmas (al no haber ningún patrón definido).

Actividades

8. Busque más información sobre los distintos *software* de los tipos de IPS diferenciando entre IPS de filtrado de paquetes, IPS de bloqueo e IPS de decepción.
9. Señale qué desventajas puede suponer para una organización la implantación de un sistema IDS en lugar de un sistema IPS. Justifique su respuesta.

5.2. Tipos de IPS

Los sistemas de prevención de intrusiones o IPS se desarrollaron en 1990 con la finalidad de monitorizar el tráfico de una red en tiempo real y conseguir prevenir las intrusiones al sistema. Se consideran una evolución de los sistemas de detección de intrusiones (IDS).

Los IPS tratan de prevenir que se filtre cualquier intrusión: en cuanto se produce la caída de algún paquete o se detecta que está dañado o incompleto,

la red bloquea la transmisión de este paquete con el fin de prevenir un posible ataque.

Las características fundamentales que tienen en común los distintos tipos de IPS son las siguientes:

- Tienen una capacidad de respuesta automática en cuanto se produce un incidente.
- Aplican filtros nuevos conforme se van detectando ataques en progreso.
- Reducen las falsas alarmas de ataques producidos en la red.
- Bloquean automáticamente los ataques a la red en tiempo real.
- Optimizan el rendimiento del tráfico de la red al bloquear de un modo automático los ataques.

Además, los IPS conllevan una serie de ventajas:

- Ofrecen una protección preventiva antes de que se produzca el ataque.
- Ofrecen una protección y defensa completa de varios tipos de ataques como: vulnerabilidades del sistema, tráfico de red, códigos maliciosos, intrusiones, etc.
- Optimiza la seguridad y la eficiencia en la prevención de intrusiones y/o ataques a una red o sistema.
- Son fáciles de instalar, configurar y administrar.
- Son escalables, por lo que se pueden ir actualizando según las necesidades de la organización.
- En comparación con un IDS requieren de menos inversión en recursos para entrar en funcionamiento.

Los IPS se pueden distinguir en tres categorías atendiendo a la acción que realizan:

- IPS de filtrado de paquetes.
- IPS de bloqueo de IP.
- IPS con acción de decepción.

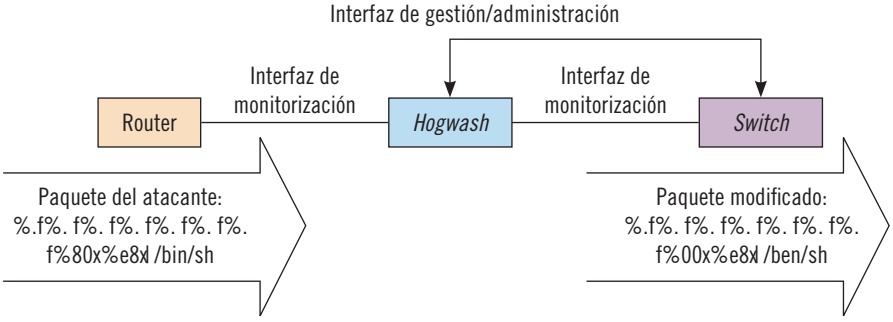
IPS de filtrado de paquetes

Los IPS de filtrado de paquetes tienen como función principal determinar el tipo de tráfico que puede entrar y salir de un equipo o servidor.

En el mercado hay varias soluciones de IPS de filtrado de paquetes, las más importantes se describen a continuación:

- ***Hogwash:*** es un sistema que funciona tanto como IDS, como IPS (es un IDS/IPS). Monitoriza el tráfico de una o varias redes y genera alertas. Además, puede detectar los ataques de la red y filtrarlos. Aunque es imposible que evite todos los ataques a una red, sí que descarta un elevado porcentaje de los mismos.

Funcionamiento del IDS/IPS *Hogwash*



- ***Dragon IPS:*** herramienta cuya funcionalidad principal es bloquear a los atacantes, reducir los ataques DoS y prevenir el acceso a la información del sistema convirtiendo la red en una red invisible.

Herramienta Dragon IPS

- ***Snort_Inline:*** está basado y construido sobre el IDS *Snort* mencionado anteriormente, y con la función añadida de la capacidad de cambiar o descartar paquetes mientras circulan por el *host.* Es uno de los IPS de red más conocidos y utilizados.

IPS de bloqueo de IP

Este tipo de IPS tiene como funcionalidad principal bloquear direcciones IP que puedan ser causantes de algún tipo de ataque.

Del mismo modo que con los IPS de filtrado de paquetes, son numerosas las herramientas que hay en el mercado:

- ***Snortsam:*** herramienta gratis y de código abierto que bloquea las direcciones IP por periodos de tiempo que pueden ir desde segundos hasta tiempo indefinido. Además, también permite determinar una serie de di-

recciones individuales o redes enteras que el usuario no quiere que sean bloqueadas de ningún modo aunque en ellas se genere alguna alerta.

- ***Portsentry:*** herramienta de libre distribución desarrollada por *Cisco.* Su función principal es rastrear las conexiones sobre el *host* donde es ejecutada e identificar los intentos de exploración contra dicho *host.* En cuanto se detecta algún intento *Portsentry* niega el acceso a la exploración del *host.*

IPS con acción de decepción

Los IPS con acción de decepción están basados en la decepción o en el engaño hacia el atacante, de modo que cuando se produce algún ataque el IPS remite al atacante información errónea del *host.*

Las principales soluciones de IPS con acción de decepción son las siguientes:

- **DTK o *Toolkit Deception:*** conjunto de herramientas cuya función principal es emitir respuestas falsas al atacante para que este entienda que hay un número muy elevado de vulnerabilidades en el sistema al que está atacando.
- ***Honeyd:*** herramienta que crea *hosts* virtuales sobre una red con el fin de crear una simulación de la misma y engañar a los atacantes.
- ***Specter:*** es un *honeypot* o sistema de engaño que realiza la simulación de un equipo completo para atraer a los atacantes y alejarlos de los equipos reales. Además, en el momento en el que se produce algún ataque *Specter* investiga el rastro de los atacantes.

A modo de resumen se puede observar en la siguiente tabla los distintos tipos de IPS y las principales herramientas que actualmente se comercializan:

Nombre	Acción	Funciones
Hogwash	Filtrado de paquetes	Filtra y descarta paquetes que pueden provocar ataques en el sistema.
Dragon IPS	Filtrado de paquetes	Palía los efectos de los ataques de denegación de servicio.
Snort_Inline	Filtrado de paquetes	Modifica los paquetes que circulan por la red. Basado en el IDS Snort.
Snortsam	Bloqueo de IP	Bloquea direcciones IP por un período determinado o indefinidamente.
Portsentry	Bloqueo de IP	Detecta intentos de escaneo al host y bloquea el acceso al escaneo.
DTK	Decepción	Emite una respuesta falsa al atacante haciéndole ver que el equipo tiene un número elevado de vulnerabilidades.
Honeyd	Decepción	Crea hosts virtuales sobre una red.
Specter	Decepción	Realiza una simulación de un equipo completo para atraer a los atacantes.

Actividades

8. Busque más información sobre los distintos *software* de los tipos de IPS diferenciando entre IPS de filtrado de paquetes, IPS de bloqueo e IPS de decepción.
9. Señale qué desventajas puede suponer para una organización la implantación de un sistema IDS en lugar de un sistema IPS. Justifique su respuesta.

Aplicación práctica

Usted, como responsable de seguridad de su organización, se encuentra en pleno proceso de definición de su política de seguridad. Ha estado evaluando las necesidades de la empresa y los requerimientos establecidos por la dirección y, finalmente, se ha decidido por un sistema que sea capaz de monitorizar el tráfico de red a tiempo real y que aplique medidas preventivas de modo automático. No le sirve la simple detección de las incidencias de seguridad. ¿Qué tipo de sistema utilizaría: sistema de prevención de intrusiones o sistema de detección de intrusiones? ¿Por qué?

SOLUCIÓN

La herramienta que es capaz de monitorizar el tráfico de la red a tiempo real es el sistema de prevención de intrusos. Mientras que los IDS o sistemas de detección de intrusos se limitan a la simple detección de ataques (exitosos y no exitosos, según el tipo de IDS implantado), los IPS o sistemas de prevención de intrusos pueden aplicar medidas preventivas que eviten la entrada de ataques a tiempo real gracias a la monitorización de la red.

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

Una vez decidido el tipo de IDS/IPS que se quiere implantar, una de las preguntas más importantes que deben realizarse las organizaciones es dónde localizarlo. La ubicación de los sistemas IDS/IPS dependerán del equipo que se va a utilizar y del *software* IDS/IPS que se va a implantar.

Atendiendo a los criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS se distinguen tres zonas en las que se puede ubicar un sistema IDS/IPS:

- **Zona roja:** es una zona de riesgo elevado. En esta zona el sistema IDS/IPS debe configurarse de modo que tenga poca sensibilidad, ya que observará todo el tráfico de la red y habrá una elevada posibilidad de falsas alarmas.

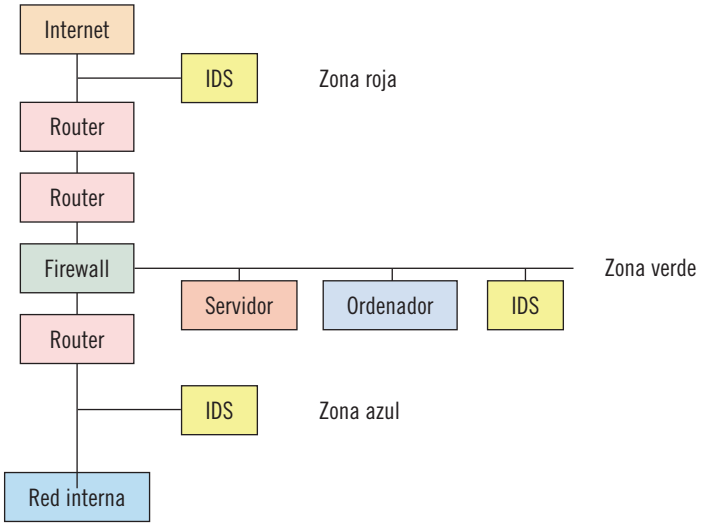
- **Zona verde:** esta zona tiene menos riesgo que la zona roja y en ella el IDS/IPS debe configurarse de modo que tenga mayor sensibilidad que en la zona roja porque aquí el firewall o cortafuegos realiza un filtrado de accesos predefinidos por la organización. En esta zona hay menos falsas alarmas que en la zona roja.
- **Zona azul:** es la zona de confianza. En esta zona cualquier tipo de acceso anómalo que haya en la red hay que considerarlo como acceso hostil. Al haber un número inferior de accesos también se reduce considerablemente el número de falsas alarmas, por lo que es necesario que cualquier falsa alarma detectada por el sistema IDS/IPS sea analizada con detenimiento.

Nota

Aunque la zona azul se considere zona de confianza y el tráfico analizado sea muy limitado, los IDS/IPS ubicados en esta zona no forman parte de la red interna del sistema, por lo que no se analizará el tráfico interno de la red.

En la siguiente imagen se pueden observar las distintas ubicaciones de los IDS/IPS, distinguiendo entre zona roja, azul y verde:

Ubicación de los sistemas IDS/IPS



Así, atendiendo al nivel de riesgo, al grado de falsas alarmas que se está dispuesto a asumir y al tráfico de datos que se pretenda analizar (según las preferencias de la organización) se elegirá una zona u otra para ubicar un sistema IDS/IPS en una organización.

Actividades

10. Proponga ejemplos por los que resultaría interesante ubicar los IDS/IPS en zona azul, roja o verde.

Aplicación práctica

Usted, como responsable de seguridad de su organización, está decidiendo dónde ubicar un sistema IDS/IPS. Le han dado directrices específicas de que el número de falsas alarmas que facilite el sistema implantado sea muy reducido (prácticamente nulo) y que esté situado en una zona de riesgo mínimo para garantizar que las alarmas que se generen por algún acceso se correspondan casi siempre con un acceso hostil. ¿En qué ubicación situaría el IDS/IPS? ¿Por qué?

SOLUCIÓN

En esta ocasión hay que ubicar el sistema IDS/IPS en zona azul, ya que es la zona de confianza y menor riesgo del sistema. Además, es la zona donde se genera el menor número de falsas alarmas y donde todos los accesos se deben considerar como hostiles por el reducido volumen de alarmas por accesos que genera.

7. Resumen

Un incidente de seguridad es cualquier evento que puede afectar a la integridad, confidencialidad y disponibilidad de la información. En otros términos, también se puede definir como un evento no deseado que puede comprometer significativamente las operaciones de una organización y amenazar su seguridad.

Hay numerosos tipos de incidentes de seguridad: accesos no autorizados, código malicioso, denegación de servicio, intentos de información de un sistema, uso deficiente de los recursos tecnológicos, etc. Para cada uno de ellos las organizaciones deben tomar una serie de medidas que los corrijan, los prevengan o, como mínimo, los detecten. La gestión de incidentes tiene como objetivo la organización de los recursos para que estas medidas sean aplicadas de un modo eficiente. Para ello se puede utilizar el "Visor de eventos" de *Windows* o una serie de comandos en *Linux* que ofrecen una visión de los diferentes archivos de registro de eventos.

Una vez ya se conoce cómo localizar los eventos que ocurren en un sistema, es básica la implantación de sistemas de prevención de intrusiones o de sistemas de detección de intrusiones como complemento a las demás medidas de seguridad de la organización.

Una vez decidido el sistema IDS/IPS a implantar, otra de las decisiones fundamentales que influirán en el sistema de seguridad de una organización es elegir la ubicación de estos sistemas. Atendiendo a criterios de asunción de riesgos, grado donfianza donde el riesgo es mínimo y el número de falsas alarmas es muy limitado).

Ejercicios de repaso y autoevaluación

1. **Indique a qué propiedad de la información se refieren las siguientes definiciones (integridad, disponibilidad y confidencialidad).**

    a. Propiedad de la información que garantiza que no ha sido alterada y que se ha mantenido intacto el documento original de la misma.
    b. Propiedad de la información en la que se garantiza que esté disponible para los usuarios cuando estos lo requieran.
    c. Propiedad mediante la que se garantiza el acceso a la misma solo a usuarios autorizados.

2. **Clasifique los siguientes incidentes de seguridad según el tipo de incidente al que hacen referencia.**

    a. Borrado de la información.
    b. Troyanos.
    c. Ataques a páginas web o servidores para saturarlos.
    d. Detección de vulnerabilidades.
    e. Violación de la normativa de acceso a internet.
    f. Intentos de acceso no autorizados recurrentes.
    g. Violación de políticas de seguridad informática.

3. **Indique a qué categoría pertenecen las siguientes medidas (preventivas, de detección o correctivas).**

    a. Medidas que sirven para detectar y controlar los incidentes de seguridad.
    b. Medidas implementadas una vez sucedido el incidente de seguridad que se utilizan para evitar que no vuelva a ocurrir y para restaurar el sistema a la situación anterior a la incidencia.
    c. Medidas que se aplican para evitar la ocurrencia de incidentes de seguridad.

4. **Complete los espacios libres de la siguiente oración:**

    La gestión de incidentes tiene como objetivo calcular y utilizar adecuadamente los _____ necesarios para aplicar correctamente estas medidas de prevención, _____y corrección de incidentes de _____.

5. **Indique cuál de las siguientes opciones no se corresponde con los beneficios que aporta una correcta gestión de incidentes en las organizaciones.**

   a. Rápida restauración del sistema informático garantizando la mínima pérdida de información posible.
   b. Mejora continua de la gestión y tratamiento de incidentes.
   c. Menor control de los procesos del sistema de información.
   d. Optimización de los recursos disponibles.

6. **¿Qué es un log? ¿Qué datos referentes a los eventos quedan registrados en los logs?**

   _____
   _____
   _____
   _____

7. **Indique a qué tipo de eventos/registros del "Visor de eventos" de Windows se refieren las siguientes definiciones:**

   a. Eventos ocurridos en los accesos del sistema, como los intentos de inicio de sesión (tanto exitosos como fallidos).
   b. Eventos registrados por aplicaciones o programas.
   c. Eventos que se han reenviado a este registro desde otros equipos.
   d. Eventos que hacen referencia a la instalación de aplicaciones en el equipo.

8. **Complete los espacios libres de la siguiente oración:**

   Los sistemas de _____ de intrusos o IDS (Intrusion Detection System) son programas cuya utilidad es detectar las _____ que se pueden producir en la red o en un equipo. Se encargan de monitorizar los _____ del equipo para buscar intentos de intrusión.

9. A pesar de haber varias arquitecturas de sistemas de detección de intrusos, hay ciertas peculiaridades que son comunes a todas ellas. ¿Cuáles son estas peculiaridades?

_____
_____
_____
_____

10. Rellene la siguiente tabla indicando a qué tipo de arquitectura IDS se corresponden las características situadas en la zona derecha de la misma.

Tipo de arquitectura IDS	Características
	Consta de generador, analizador y base de datos de eventos además de unidades de respuesta ante la aparición de incidentes. Tuvo escasa aceptación en el mercado.
	Une los distintos equipos que forman parte de la arquitectura CIDF y facilita información sobre información de eventos en bruto, resultados de los análisis y prescripciones de respuestas.
	Arquitectura simple que facilita la información de las incidencias en muy pocas líneas. Es muy limitada si se pretende obtener información detallada de las incidencias.
	Facilita el intercambio de información sobre los incidentes de seguridad y permite definir los protocolos y formatos de intercambio de información entre los IDS.

11. Indique cuál de las siguientes oraciones no se corresponde con las ventajas de los sistemas de detección de intrusos basados en red o NIDS.

a. Son sistemas de fácil instalación y actualización.
b. Detectan accesos no deseados en la red.
c. Pueden operar y detectar ataques ante datos cifrados que circulan por la red.
d. Tienen un bajo impacto en la red al no intervenir en sus operaciones habituales.

12. Complete los espacios libres de la siguiente oración:

Los IDS basados en _____ o HIDS detectan las _____ a nivel de un equipo informático, analizando su _____ para comprobar si ha habido algún tipo de alteración de los archivos del _____, y para localizar actividades sospechosas. Fueron el _____ tipo de IDS desarrollado e implementado.

13. ¿Qué diferencia los IDS de detección de abusos o firmas de los IDS de detección de anomalías?

_____

_____

14. Complete la siguiente tabla indicando qué tipo de acción (filtrado de paquetes, bloqueo de IP o acción de decepción) realizan los distintos IPS atendiendo a sus características fundamentales.

Nombre	Acción	Funciones
Hogwash		Filtra y descarta paquetes que pueden provocar ataques en el sistema.
Dragon IPS		Palía los efectos de los ataques de denegación de servicio.
Snort_Inline		Modifica los paquetes que circulan por la red. Basado en el IDS Snort.
Snortsam		Bloquea direcciones IP por un período determinado o indefinidamente.
Portsentry		Detecta intentos de escaneo al host y bloquea el acceso al escaneo.
DTK		Emite una respuesta falsa al atacante haciéndole ver que el equipo tiene un número elevado de vulnerabilidades.
Honeyd		Crea hosts virtuales sobre una red.
Specter		Realiza una simulación de un equipo completo para atraer a los atacantes.

15. Determine a qué zona hace referencia cada una de las siguientes definiciones.

a. Esta zona tiene menos riesgo que la zona roja y en ella el IDS/IPS tiene que configurarse de modo que tenga mayor sensibilidad que en la zona roja porque aquí el firewall o cortafuegos realiza un filtrado de accesos predefinidos por la organización. En esta zona hay menos falsas alarmas que en la zona roja.
b. Es la zona de confianza. En esta zona cualquier tipo de acceso anómalo que haya en la red hay que considerarlo como acceso hostil. Al haber un número inferior de accesos también se reduce considerablemente el número de falsas alarmas, por lo que es necesario que cualquier falsa alarma detectada por el sistema IDS/IPS sea analizada con detenimiento.
c. Es una zona de riesgo elevado. En esta zona el sistema IDS/IPS debe configurarse de modo que tenga poca sensibilidad ya que observará todo el tráfico de la red y habrá una elevada posibilidad de falsas alarmas.

Capítulo 2

Implantación y puesta en producción de sistemas IDS/IPS

Contenido

1. Introducción

Cuando las organizaciones toman la decisión de implantar un sistema de detección y prevención de intrusos o IDS/IPS deben realizar una serie de análisis y comprobaciones previas para garantizar que la implementación se realice correctamente y sea lo más eficaz posible.

En el primer apartado de este capítulo se describen con profundidad los distintos elementos que hay que tener en consideración cuando se deben tomar las decisiones de ubicación del sistema, equipos que van a funcionar y se van a utilizar bajo los IDS/IPS y los protocolos y servicios que emplea la organización en su actividad diaria y en la transferencia y utilización de datos.

Una vez decidida la ubicación y las características de los sistemas de detección y prevención de intrusiones, en el apartado siguiente se mencionan una serie alternativas de políticas de seguridad que pueden utilizar estos sistemas en el momento en el que se detecta algún tipo de actividad sospechosa.

Aunque la detección de las intrusiones es fundamental para garantizar la eficacia del IDS/IPS hay que tener en cuenta que no todas las intrusiones detectadas tienen que ser intrusiones reales y que también puede ser que haya alguna intrusión no detectada. Por ello, en otro apartado se profundiza en estos conceptos y se formulan una serie de recomendaciones que permitan a las organizaciones configurar sus sistemas IDS/IPS para reducir las intrusiones no detectadas y las falsas detecciones.

Además, también se describen en profundidad las informaciones detalladas que deben facilitar los sistemas IDS/IPS cuando detectan alguna intrusión para que se realice una correcta monitorización de los eventos y se pueda comprobar el funcionamiento correcto del equipo y sus dispositivos.

Para finalizar el capítulo se formula una serie de recomendaciones que pueden ayudar a las organizaciones a definir los niveles adecuados de monitorización, actualización y pruebas a realizar antes de la implantación y una vez implantado el sistema de detección y prevención de intrusiones.

2. Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio

Los sistemas de detección y prevención de intrusiones (IDS/IPS) cada vez resultan más imprescindibles para cualquier empresa que trabaje con alguna infraestructura de red. Los intentos de intrusión y de utilización malintencionada de los datos de una organización siguen aumentando a niveles cada vez más elevados.

Aunque estos sistemas resultan muy útiles para evitar posibles intrusiones, no son suficientes: las organizaciones deben establecer una serie de medidas de seguridad adicionales que sirvan de apoyo en el momento que ocurra cualquier fallo de seguridad.

Además, suele ocurrir que los responsables de la infraestructura de la red no tengan muchos conocimientos específicos y concretos de estos sistemas.

Debido a ello es necesario que las organizaciones realicen previamente un estudio de sus infraestructuras, servicios, equipos, zonas y protocolos, entre otros muchos elementos, para que la implantación del sistema IDS/IPS y de las demás medidas de seguridad se realicen de un modo correcto y efectivo.

Por esto, el establecimiento de estos sistemas y medidas requiere un proceso previo de planificación, preparación, pruebas y formación especializada de los administradores de modo que cuando ya esté la implementación completada se pueda funcionar a pleno rendimiento y con la certeza de que el nivel de seguridad de la infraestructura de la organización es el adecuado.

La implementación de los sistemas IDS/IPS dependen en mayor parte de los recursos y políticas de la organización y debe realizarse escalonadamente para que el proceso de aprendizaje de los administradores sea profundo y basado en la experiencia que vaya adquiriendo a medida que se completa la implementación.

Recuerde

Los sistemas de detección de intrusiones (IDS) tienen como función principal detectar accesos no autorizados en los equipos o redes de una organización. Sin embargo, los sistemas de prevención de intrusiones (IPS) tienen como objetivo evitar estos accesos no autorizados.

A continuación se describirán las distintas opciones de localización de los sistemas IPS/IDS y sus características, ventajas e inconvenientes principales que deberán tener en cuenta las organizaciones en el momento de decidir qué sistema implantar en su infraestructura.

2.1. Sistemas de detección y prevención de intrusiones en red o NIDPS

Como ya se ha comentado en el capítulo anterior y a modo de recordatorio, los sistemas de detección y prevención de intrusiones en red o NIDPS son sistemas que trabajan con los datos que circulan en una red, monitorizándola para buscar posibles accesos no autorizados y filtrando el tráfico de la red.

Son muy útiles porque proporcionan alertas cuando se produce un ataque en la red y pueden reaccionar para evitarla o para intentar que los daños sean mínimos. Además, facilitan un análisis de las intrusiones exitosas, lo que ayuda a las organizaciones a prevenir estas intrusiones en momentos futuros. No obstante, nunca deben ser sustitutos de una política de seguridad, sino que deben ser accesorios.

Estos sistemas pueden colocarse en varias ubicaciones de la infraestructura de red de una organización. Estos se mencionan a continuación.

Delante del cortafuegos o firewall

La colocación de los sistemas NIDPS delante del cortafuegos externo permite una monitorización de los ataques (tanto en tipo de ataque como en

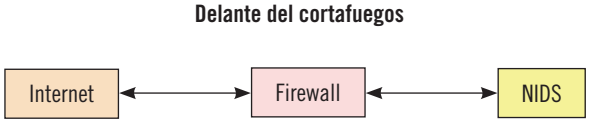
número de ataques) contra la infraestructura de una organización y detecta principalmente aquellos ataques que van dirigidos contra el *firewall* de la red.

Esta ubicación también implica una serie de desventajas:

- No detecta ataques con información encriptada.
- El NIDPS, si está mal diseñado, se puede saturar debido al elevado tráfico de red que acontece en esta zona de la infraestructura de la red.
- El exceso de información producido por el elevado tráfico de red puede ser contraproducente, ya que puede ser más difícil localizar la información importante y, por lo tanto, los ataques efectivos.
- No ofrece un elevado grado de protección ya que si algún intruso lo localiza puede dirigir sus ataques directamente a él.

Detrás del cortafuegos o firewall

El sistema NIDPS se sitúa entre la red externa y la red interna en una zona llamada DMZ (zona desmilitarizada).



Esta localización permite comprobar la totalidad de los ataques que se producen en la red de la organización, tanto exitosos como no exitosos. Como ventajas de localizar los sistemas en esta zona destacan:

- En esta ubicación se monitorizan aquellas intrusiones que consiguen atravesar el cortafuegos o *firewall.*

- Los ataques detectados son potencialmente mucho más peligrosos que los detectados en otras ubicaciones, por lo que el riesgo de ataques exitosos disminuye considerablemente.
- Al poder identificar los ataques más comunes permite una configuración más efectiva del cortafuegos principal.
- La cantidad de logs es inferior, pero la información facilitada por estos sistemas está mejor seleccionada y es más relevante.

No todo son ventajas, también hay que tener en cuenta una serie de desventajas:

- Solo se monitoriza el tráfico que haya entrado realmente en la red. Al estar situado posteriormente al cortafuegos, los datos que le llegan han sido previamente filtrados por la barrera del *firewall*.
- En esta ubicación tampoco se pueden identificar los ataques con información encriptada.
- Aunque la seguridad del NIDPS mejora considerablemente al estar situado a continuación del cortafuegos, esta sigue sin ser suficiente: hay que utilizar medidas de seguridad adicionales.

Combinación de los dos anteriores

Una opción muy válida que contrarresta las desventajas de la ubicación del sistema de detección y prevención de intrusiones antes o después del cortafuegos es la combinación de ambas: situar sistemas antes y después del cortafuegos.

Delante y detrás del cortafuegos

Esta combinación reúne las ventajas de las dos ubicaciones y además, proporciona otras adicionales:

- Hay un mayor control de las posibles intrusiones en la red.

- En el supuesto de que se deje pasar tráfico que no se debe, esta combinación permite ir mejorando la seguridad a través del aprendizaje.
- Permite una correlación entre los ataques detectados antes y después del cortafuegos.

Como desventaja principal destaca el coste que implica la colocación de dos máquinas para implementar estos sistemas en dos ubicaciones.

Combinación firewall/NIDPS

Cuando la organización no dispone de máquinas suficientes para que haya una de ellas destinada exclusivamente a la detección y prevención de intrusiones, una buena alternativa es utilizar un equipo que funcione como cortafuegos y NIDPS a la vez.

Con esta opción se monitoriza todo el tráfico de la red con las ventajas y desventajas que ello implica, pero se reduce el gasto al ser necesaria una inversión menor por un solo equipo.

Equipo utilizado como cortafuegos y NIDS

Ubicación en las redes principales de la organización

Otra opción, independientemente de si se ubica el IDS/IPS antes o después del cortafuegos, es decidir entre ubicarlo en las redes principales de la organización o bien situarlo solo en las redes más críticas y valiosas.

La ubicación en las redes generales de la organización monitoriza una cantidad más elevada de tráfico, lo que aumenta las posibilidades de encontrar posibles ataques. Además, también permite detectar aquellos ataques que se producen dentro de la misma red interna de la organización, normalmente ocasionada por empleados y otro personal interno.

Aun así, también presenta una serie de desventajas:

- Tampoco se detectan ataques con información encriptada.
- Los sistemas situados en las redes generales pueden hacerlas más vulnerables ante ataques internos producidos dentro de la misma red.

Ubicación en las redes críticas de la organización

En numerosas ocasiones la información más valiosa de una organización no se almacena en sus redes generales, sino que utilizan otras subredes separadas para aumentar su nivel de seguridad y ser tratados de un modo acorde con su valor.

De este modo, la ubicación de los IDS/IPS en estas redes permite la detección y prevención de los ataques realizados específicamente contra los datos críticos y añaden un nivel de seguridad adicional a los mismos, minimizando aún más los posibles riesgos de ataques.

Aun así, no evitan los ataques contra las redes generales y serán necesarias más medidas adicionales que protejan a la infraestructura de red general de la organización.

2.2. Sistemas de detección y prevención de intrusiones en equipos (hosts) o HIDPS

Los sistemas de detección y prevención de intrusiones basados en *hosts* son los que residen en el mismo equipo que monitorizan y solo se preocupan de proteger a dicho equipo sin necesitad de monitorizar todo el tráfico de la red de una organización. Consumen menos recursos que los NIDS o NIDPS y no impiden un buen rendimiento del sistema.

Aunque implican un mejor rendimiento del sistema, estos tipos de sistema combaten las intrusiones una vez que el equipo ya está en peligro, lo que el riesgo es bastante mayor. Además, implica unas mayores medidas de seguridad en el equipo para combatir los ataques.

Los IDPS basados en *hosts* monitorizan con más profundidad los datos del equipo (que puede ser un servidor, ordenador o, incluso, alguna aplicación específica) que los IDPS basados en red como, el tráfico inalámbrico, el tráfico de red, los accesos a los archivos, los cambios de configuración en el equipo o en alguna aplicación, etc.

Aun así, y del mismo modo que en los demás sistemas mencionados, tampoco detecta los ataques con información encriptada.

2.3. IDS/IPS en ambientes virtuales

La utilización de ambientes virtuales (información en "la nube") es cada vez mayor debido a sus numerosas ventajas:

- Hay un ahorro de energía al ser necesaria una infraestructura menor en la organización para almacenar datos.
- Suponen un coste reducido de mantenimiento, permitiendo así que los equipos tengan mayor capacidad de almacenamiento y reduciendo también el espacio físico y la reducción de costes que ello implica (menos gastos de electricidad, menos gastos de alquiler de local, etc.).

Definición

Ambientes virtuales
Son un conjunto de herramientas de *software* que facilitan a los usuarios y organizaciones el almacenamiento de aplicaciones y datos en infraestructuras externas de la organización por un reducido coste de servicio.

El nivel de seguridad en este tipo de sistemas es bastante elevado al estar las estructuras físicas situadas fuera de la organización. Además, al utilizar soluciones de detección y prevención de ataques facilitadas por proveedores que

ofrecen servicio a muchas otras organizaciones, la base de datos de posibles vulnerabilidades y ataques es mucho mayor y hay más posibilidad de detección y reacción.

2.4. IDS/IPS inalámbricos o wireless IDS/IPS

Este tipo de sistemas analizan los protocolos inalámbricos para detectar las actividades sospechosas.

Su funcionamiento es igual a los IDPS basados en red, con servidor, consola y base de datos y permite la monitorización del tráfico de red que circula por la red inalámbrica de la organización.

Como desventaja principal cabe señalar que los análisis de estos sistemas se limitan a un solo canal, por lo que si la organización utiliza varios canales inalámbricos no podrán realizarse análisis de todos los canales simultáneamente.

2.5. Decisiones de la organización para ubicar un sistema de detección y prevención de intrusiones

Una vez vistas varias opciones de ubicación de los sistemas de detección y prevención de intrusiones queda bastante claro que en el momento de decidir cuál de ellos implantar en la organización es necesario realizar un análisis previo y profundo que incluya varios aspectos:

- Análisis de los procesos de negocio e identificación de la información valiosa en cada uno de los procesos.
- Análisis de los protocolos de red utilizados para transferir datos entre los equipos de la organización y al exterior.
- Análisis de los protocolos y políticas de la organización para ser coherentes con su política de seguridad y su política de costes en el momento de implantar el sistema IDS/IPS apropiado.

- Análisis de las distintas zonas que forman parte de la organización y la ubicación de sus equipos y servidores para ver qué ubicación del IDS/IPS puede ser más conveniente según sus características.
- Análisis de los servicios que ofrece la organización para averiguar cuáles de ellos necesitan un nivel de seguridad especial debido a la tipología de información con la que trabajan.

Una vez realizados todos estos análisis ya se puede planificar el proceso de implantación de los sistemas de seguridad. No obstante, y como se ha repetido ya varias veces, los sistemas IDS/IPS no deben ser los únicos sistemas de seguridad implantados siendo necesarias otras medidas como antivirus, *firewalls,* etc.

Aplicación práctica

Ana, Daniel y usted acaban de crear una empresa de asesoramiento financiero y disponen de pocos recursos y de poca financiación. No por ello quieren dejar de establecer un sistema de seguridad que garantice la integridad, confidencialidad y disponibilidad de los datos de la empresa, ya que se trata de datos delicados que requieren toda la protección posible. Disponen de cortafuegos y de otras medidas de seguridad adicionales, pero también han decidido instalar un sistema IDS/IPS que minimice los riesgos. Teniendo en cuenta que disponen de pocos equipos, de poca financiación y que ya cuentan con un cortafuegos, ¿dónde ubicaría el IDS/IPS? ¿Por qué?

SOLUCIÓN

Considerando que la empresa está recién creada, que dispone de equipos limitados y que ya tiene un cortafuegos, la mejor opción para instalar un sistema de detección y prevención de intrusiones es ubicarlo en el mismo equipo en el que está el cortafuegos. De este modo se ahorra la utilización de un equipo adicional y permite utilizarlo en otras funciones que pueden ser también fundamentales para la empresa. Al usar un equipo ya adquirido también se reduce la inversión requerida para instalar el sistema, lo que es completamente acorde para la financiación limitada de la empresa.

Actividades

1. Explique qué es un cortafuegos o *firewall* y para qué se utiliza. ¿Por qué es tan determinante a la hora de decidir la ubicación del IDS/IPS? Justifique su respuesta.
2. Señale qué diferencia hay entre los IDS/IPS inalámbricos y los IDS/IPS en ambientes virtuales. Establezca en qué ocasiones es preferente la utilización de cada tipo de IDS/IPS.

3. Definición de políticas de corte de intentos de intrusión en los IDS/IPS

Una vez tomada la decisión sobre el sistema IDS/IPS que se va a implantar en la organización hay que definir una serie de políticas sobre el tipo de respuesta que debe tomar cuando haya algún intento de intrusión o ataque.

Antes de comentar las distintas políticas de corte de intentos de intrusión en los IDS/IPS es fundamental conocer los diversos tipos de análisis que realizan estos sistemas para entender sus diferentes modos de funcionamiento.

Hay dos tipos fundamentales de análisis:

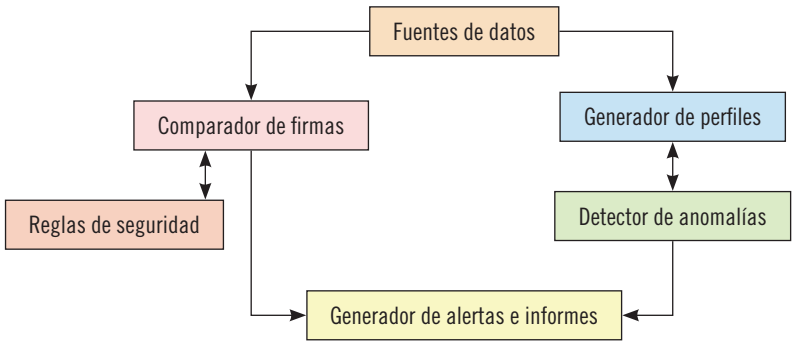
- **Detección de usos indebidos *(misuse):*** los IDS/IPS utilizan una base de datos para encontrar usos indebidos mediante la comparación de las firmas de la base de datos con la información recogida previamente.
- **Detección de anomalías:** en este caso no se utiliza una base de datos como elemento de comparación, sino que se emplean técnicas estadísticas para definir y aproximar los patrones que se corresponden con un comportamiento normal.

Nota

Las firmas en IDS/IPS se refieren a los patrones de ataques conocidos, patrones que se han repetido en varias ocasiones y que se han confirmado como comportamientos maliciosos.

En la siguiente figura se puede observar el funcionamiento de los dos tipos de análisis en los sistemas de detección de intrusiones.

Tipos de análisis de detección de intrusiones



Lo habitual en las organizaciones es que se utilice una combinación de ambos tipos de análisis para minimizar el riesgo y poder detectar todo tipo de ataques, tanto los más comunes como los más inusuales.

Otra manera de distinguir los tipos de análisis de los sistemas de detección y prevención de intrusiones es teniendo en cuenta el tiempo de realización de los análisis, distinguiendo entre:

- **Análisis por lotes *(batch mode):*** el análisis de los datos para detectar intrusiones se realiza cada cierto intervalo de tiempo definido. Al finalizar cada período de tiempo el sistema realiza el análisis de los datos recibidos en ese período. Tiene como inconveniente principal que las

posibles alarmas de las intrusiones sucedidas no se hacen en tiempo real, sino que se originan después de haberse producido las intrusiones.

- **Análisis en tiempo real:** en este tipo de análisis se examinan los datos conforme se van recibiendo a tiempo real o con un retardo mínimo de tiempo. Son más utilizados ya que posibilitan responder a las posibles intrusiones a la misma vez que se van detectando.

En la siguiente tabla se resumen los distintos tipos de análisis de un sistema de detección y prevención de intrusiones:

Análisis de los datos obtenidos por los IDS/IPS	
Clasificación del análisis	**Tipo de análisis**
Según el procedimiento de análisis de los datos	Detección de usos indebidos
	Detección de anomalías
Según el tiempo del análisis	Análisis por lotes
	Análisis a tiempo real

Ante estos tipos de análisis las organizaciones pueden definir cuándo quieren que se realice la detección y qué tipo de detección se quiere implementar.

El siguiente paso consiste en definir las políticas de actuación del sistema IDS/IPS cuando se detecta algún intento de intrusión.

En general, una política de seguridad define las directrices de lo que se va a permitir y lo que se va a prohibir en un sistema de información. De este modo se puede distinguir entre dos líneas actuación en cuanto a políticas de seguridad:

- **Política prohibitiva:** política en la que se prohíbe todo lo que no se ha definido como permitido expresamente.
- **Política permisiva:** esta política es todo lo contrario. En la política permisiva se define todo lo que se va a prohibir y todo lo demás se considera permitido.

Lo más habitual en las organizaciones en cuanto a políticas de seguridad es utilizar políticas permisivas, ya que las prohibitivas son demasiado restrictivas y pueden ocasionar bloqueos de acciones rutinarias o básicas que se pueden haber pasado por alto en la definición de las permisiones.

3.1. Políticas de corte de intrusiones en sistemas IDS/IPS

En cuanto a los sistemas de detección y prevención de intrusiones, cuando se detecta alguna intrusión se pueden definir dos tipos de políticas de corte de intrusiones:

- Políticas de respuesta pasiva.
- Políticas de respuesta activa.

Políticas de respuesta pasiva

En estas políticas, cuando se detecta una intrusión, el sistema se limita a registrar y a emitir una alarma del ataque detectado. No se realiza ninguna acción para cambiar el curso del ataque.

Algunos ejemplos de políticas de respuesta pasiva son los siguientes:

- **Envío de un correo electrónico a uno o varios usuarios:** cuando se detecta una intrusión se envía un correo electrónico a uno o varios usuarios informando de esta intrusión.
- **Registro del ataque:** se almacenan los detalles de la alerta (fecha del ataque, hora, IP del intruso, IP del destino, protocolo utilizado, etc.) en una base de datos.
- **Almacenamiento de paquetes sospechosos:** se almacenan todos los paquetes de datos que originaron la alerta.
- **Apertura de una aplicación:** cuando hay algún intento de intrusión se abre una aplicación que realiza una acción específica como el envío de mensajes de texto o la emisión de algún sonido, entre otras.
- **Notificación visual:** cuando se produce un intento de intrusión se emite una notificación visual en las consolas de administración.

- **Envío de una trampa SNMP a un hipervisor externo:** se emite un mensaje de alerta (trampa) en protocolo SNMP a una consola externa.

Políticas de respuesta activa

El sistema de detección y prevención cuando detecta una intrusión, además de generar una alarma y remitirla al responsable, modifica el entorno para evitar que la intrusión tenga éxito.

Algunos ejemplos de políticas de respuesta activa ante ataques se describen a continuación:

- **Envío de un *ResetKill:*** en el momento de la detección de la intrusión se envía un paquete de alerta que fuerza la finalización de la conexión evitando que el atacante consiga entrar en el equipo.
- **Reconfiguración de dispositivos externos:** al detectarse el ataque se envía un comando para que el dispositivo externo se reconfigure de inmediato y pueda bloquear el intento de ataque.

En la tabla siguiente se pueden observar los distintos tipos de políticas de corte de intrusiones con sus respectivos ejemplos:

Políticas de corte de intrusiones	
Políticas de respuesta pasiva: se limitan a registrar los datos del intento de intrusión.	**Políticas de respuesta activa:** registran los datos del intento de intrusión e intentan evitarlo.
Envío de correo electrónico.	Envío de un *ResetKill.*
Envío de trampas SNMP a consolas externas.	Reconfiguración de los dispositivos externos.
Registro del ataque.	
Almacenamiento de los paquetes de datos sospechosos.	
Apertura de una aplicación.	
Notificación visual de una alerta.	

Actividades

3. Busque más ejemplos de políticas de corte de intrusiones de respuesta pasiva y activa.
4. Explique por qué se recomienda utilizar una combinación de IDS/IPS de detección de usos indebidos y de detección de anomalías. ¿Su utilización combinada ofrece alguna ventaja adicional?

Aplicación práctica

Usted, como administrador de la infraestructura de red de su empresa, está definiendo las políticas de corte de ataques ante detecciones de intrusiones del sistema IDS/IPS que pretende implantar. Quiere que el sistema, en cuanto detecte alguna intrusión, le envíe un SMS a su móvil indicando con detalle las características de la intrusión pero que no realice ninguna acción adicional automáticamente porque prefiere ser usted el que decida qué medida tomar en cada intrusión. ¿De qué tipo de política de respuesta se está hablando en este caso? ¿Qué otras opciones de notificación de intrusión podrían establecerse?

SOLUCIÓN

Las políticas de respuesta ante detecciones de ataques que se limitan a notificar y a facilitar información detallada del ataque son las llamadas políticas de respuesta pasiva.

Otras opciones de notificación que se podrían establecer pueden ser el envío de correo electrónico, la apertura de una aplicación que genere una alerta o la notificación visual de una alerta, entre otras.

4. Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS

El análisis de los distintos eventos registrados en el sistema por los IDS/IPS no es impecable: es habitual que la base de datos de firmas esté desactualizada y que los métodos estadísticos de detección de comportamientos indebidos no sean perfectos.

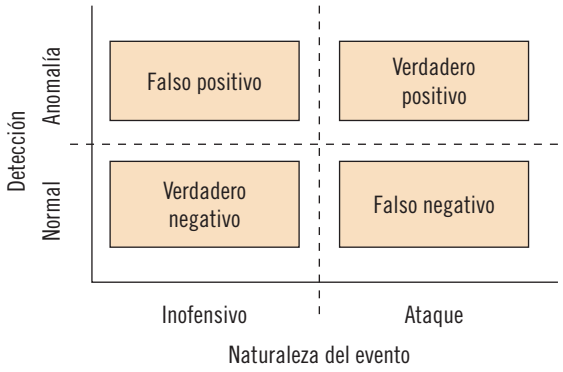
Por ello es común que cuando los sistemas de detección y prevención de intrusiones toman decisiones sobre si un evento debe considerarse o no un ataque, se equivoquen.

En el momento de la toma de decisión de si un evento es efectivamente un ataque o no puede haber cuatro posibilidades:

- **Detección de falso positivo o falsa alarma:** cuando el IDS/IPS detecta como ataque el tráfico de datos que en verdad es inofensivo.
- **Falso negativo:** ataque que no es detectado por el IDS/IPS.
- **Verdadero positivo:** evento inofensivo que el IDS/IPS ha detectado como tráfico de red normal.
- **Verdadero negativo:** ataque detectado correctamente por el IDS/IPS.

Así, en la siguiente figura se muestran las distintas posibilidades en cuanto a la detección de ataques en los IDS/IPS.

Posibilidades de detección de ataques



Ante estas posibilidades el objetivo que debe establecerse en un IDS/IPS es minimizar el número de errores (falsos positivos y falsos negativos) en la detección y maximizar el número de aciertos (verdaderos positivos y verdaderos negativos) por varios motivos:

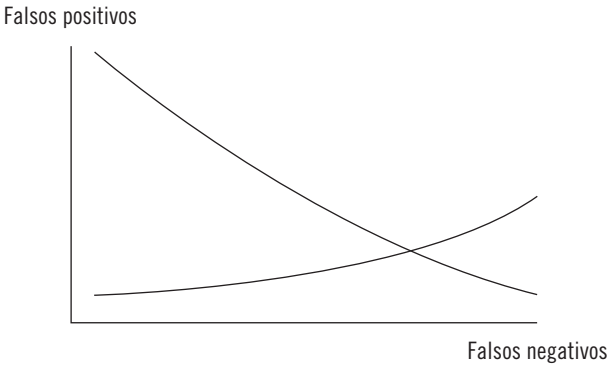
- Un elevado nivel de falsos positivos y negativos puede difuminar los motivos por los que se implantó el IDS/IPS, obteniendo bajos niveles de efectividad del sistema.
- Los falsos positivos ocupan tiempo y recursos cuando el IDS/IPS genera alarmas cuando no debe.
- La no detección de ataques (falsos negativos) puede tener graves consecuencias en la información de la organización.

Así, viendo los efectos que tiene la configuración establecida en el sistema de detección y prevención de intrusos y viendo los falsos positivos y los falsos negativos que se generan, se pueden realizar modificaciones en la configuración para conseguir la más adecuada y que trabaje con un mayor rendimiento según las características de la infraestructura de red y sus necesidades.

Para comprobar las configuraciones hay que realizar varias pruebas de referencia sobre distintas configuraciones para que se puedan hacer comparaciones de los resultados: con el análisis de las diferencias de los resultados obtenidos con las diversas configuraciones se puede detectar y eliminar la causa que provoca los falsos positivos y negativos.

Por ejemplo, de las alarmas generadas por las distintas configuraciones se puede obtener información sobre si estas se producen por un ataque real, un falso positivo o si puede determinar algún falso negativo.

El objetivo a perseguir con la configuración del IDS/IPS es conseguir un equilibrio entre los falsos positivos y los falsos negativos, consiguiendo localizarse en el cruce de las tasas de falsos positivos y negativos mostrado en el gráfico siguiente:



El gráfico de la imagen es un modelo de la tasa de error en un IDS/IPS, representando lo que ocurre cuando se reduce la sensibilidad del sistema para emitir alertas y cuando se incrementa la cantidad de paquetes inspeccionados:

- A mayor sensibilidad del sistema, mayor posibilidad de detección de falsos positivos y menor aparición de falsos negativos.
- A menor sensibilidad, menor detección de falsos positivos y mayor aparición de falsos negativos.
- A mayor cantidad de paquetes inspeccionados, mayor posibilidad de detectar falsos positivos y menor aparición de falsos negativos.
- A menor cantidad de paquetes inspeccionados, menor posibilidad de detección de falsos positivos y mayor aparición de falsos negativos.

En conclusión, en el momento de decidir la configuración de un IDS/IPS hay que encontrar a través de varias pruebas el equilibrio entre la sensibilidad del sistema y la cantidad de datos a inspeccionar, atendiendo a las necesidades de cada organización e intentando conseguir el mayor rendimiento posible.

Como recomendación, en el momento de realizar las pruebas de configuración hay que tener en cuenta algunas de las causas más frecuentes de falsos positivos:

1. **Actividad del sistema de supervisión de red:** en ocasiones, las empresas utilizan sistemas de supervisión de redes para obtener registros de la actividad que hay en sus sistemas. Muchos sistemas de detección

y prevención de intrusos suelen clasificar esta actividad como hostil o sospechosa cuando en verdad es inofensiva. Como solución se recomienda configurar el IDS/IPS eliminando las alertas de este tipo de la base de datos.

2. **Escaneo de vulnerabilidad y escáneres de puertos de red:** cuando se pretende realizar una prueba de vulnerabilidad de la red o un escáner de sus puertos el IDS/IPS lo suele detectar como ataque, ya que su funcionamiento es muy similar al utilizado por los piratas informáticos en sus ataques. Se recomienda desactivar el IDS/IPS momentáneamente cuando se realiza este tipo de actividades.
3. **Actividad del usuario:** en muchos IDS/IPS viene configurado por defecto la emisión de alarmas ante comportamientos del usuario que considera como "peligrosas": compartir archivos punto a punto o utilización de mensajería instantánea, entre otras. Para evitar que se generen estas alertas es recomendable configurar específicamente las alarmas eliminando estas casuísticas.
4. **Comportamientos similares a troyanos o gusanos:** en ocasiones, la misma organización realiza acciones que son similares a las que ejecutan los gusanos o los troyanos y emite alarmas cuando realmente son acciones inofensivas. En este caso no se recomienda desactivar las alarmas, ya que dejaría al equipo desprovisto de mecanismos de detección de ataques reales de troyanos y gusanos.
5. **Cadenas largas de registro web:** hay alertas que se generan por la detección de cadenas de registro web largas, ya que algunos ataques las utilizan para desbordar la memoria del equipo y así poder acceder a su sistema. Aunque en la actualidad hay muchas webs que utilizan cadenas largas de un modo habitual no se recomienda desactivar las alertas de su detección, ya que permitiría el acceso de ataques potencialmente dañinos.
6. **Actividad de autenticación de base de datos:** los sistemas de detección y prevención de intrusiones suelen analizar la actividad administrativa de las bases de datos porque consideran que una elevada actividad puede ser un indicio de estar sufriendo algún ataque. Si la organización utiliza bases de datos en continua actualización y con un elevado nivel de actividad administrativa, se recomienda desactivar estas alertas para reducir el número de falsos negativos.

Si aun así se siguen teniendo dudas sobre la configuración ideal para el sistema de detección y prevención de intrusiones, hay dos metodologías de libre configuración que se utilizan para evaluar y realizar test de los distintos elementos de seguridad de una organización, entre ellos los sistemas IDS/IPS:

- **Metodología OSSTM *(Open Source Security Testing Methodology):*** la metodología de testeo de seguridad de código abierto ha sido elaborada por el Instituto para la Seguridad y Código Abierto (ISECOM) y ofrece una metodología de evaluación de sistemas de seguridad, sobretodo de cortafuegos e IDS/IPS.
- **Metodología OSEC *(Open Security Evaluation Criteria):*** el Criterio de Evaluación de Código Abierto es similar al OSSTM pero está concentrado fundamentalmente en estandarizar productos de seguridad relativos a los NIDS y a los cortafuegos.

Aparte de estas metodologías también se pueden encontrar varias herramientas de libre distribución capaces de generar elevadas cantidades de falsos ataques que pueden facilitar a la organización la configuración de los sistemas IDS/IPS. Muchas de ellas también son capaces de utilizar las propias reglas del IDS/IPS para realizar la evaluación de su capacidad de detección. Algunas de estas herramientas se muestran a continuación:

- ***IDSWakeup:*** genera falsos ataques desde direcciones IP que pueden ser tanto aleatorias como específicas para comprobar si el sistema IDS/IPS los detecta correctamente.
- ***Sneeze:*** también es un generador de falsos positivos, en este caso diseñado específicamente para Snort.
- ***Stick:*** herramienta que se utiliza para evaluar la capacidad del sistema para detectar intrusiones y testear las reglas del IDS y del cortafuegos.
- ***Ftester:*** esta herramienta envía ataques de red a equipos remotos.

```
#. / IDSwakeup 0 127.0.0.1 1 1

- = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - =
- IDSwakeup: generador de falsos positivos
- Stephane Aubert
- Hervé Schauer Consultants (c) 2000
- = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - = - =


  src_addr: 0 dst_addr: 127.0.0.1 nb: 1 ttl: 1

  enviando: lágrima ...
  enviando: la tierra ...
  enviando: get_phf ...
  enviando: bind_version ...
  enviando: get_phf_syn_ack_get ...
  enviando: ping_of_death ...
  enviando: syndrop ...
  enviando: newtear ...
  enviando: X11 ...
  enviando: SMBnegprot ...
  enviando: smtp_expn_root ...
  enviando: finger_redirect ...
  enviando: ftp_cwd_root ...
  enviando: ftp_port ...
  enviando: trin00_pong ...
  enviando: back_orifice ...
  enviando: msadcs ...
            245.146.219.144 -> 127.0.0.1 80/tcp   GET / msadc / msadcs.dll HTTP/1.0
  envío: www_frag ...
            225.158.207.188 -> 127.0.0.1 80/fragmented-tcp
              GET / .. ..................................... HTTP/1.0
            181.114.219.120 -> 127.0.0.1 80/fragmented-tcp
              GET / AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
             AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
             AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA \
             .. AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA / / cgi-bin / phf HTTP/1.0
  envío: www_bestof ...
     137.78.167.188 -> 127.0.0.1 80/tcp   GET / HTTP/1.0
     165.90.83.96 -> 127.0.0.1 80/tcp   GET / / / / / / / / HTTP/1.0
            249.174.111.124 -> 127.0.0.1 80/tcp   CABEZA / HTTP/1.0
            101.146.51.80 -> 127.0.0.1 80/tcp CABEZA / /.
            137.126.215.76 -> 127.0.0.1 80/tcp   / cgi-bin \ \ manejador
            101.226.235.216 -> 127.0.0.1 80/tcp   / cgi-bin \ \ webdist.cgi
            241.70.55.180 -> 127.0.0.1 80/tcp   / mlog.phtml
            69.138.75.176 -> 127.0.0.1 80/tcp   / mylog.phtml
            137.86.207.116 -> 127.0.0.1 80/tcp   / CFIDE \ \ administrator \ \ startstop.html
            53.90.147.104 -> 127.0.0.1 80/tcp   / cfappman \ \ index.cfm
            201.110.175.156 - > 127.0.0.1 80/tcp   / mall_log_files \ \ order.log
            221.226.155.208 -> 127.0.0.1 80/tcp   / admin_files \ \ order.log
            137.222.71.244 -> 127.0.0.1 80/tcp   / cgi-bin \ \ wrap
            85.82.147.96 -> 127.0.0.1 80/tcp   GET / cgi-bin/ph% 66 HTTP/1.0
            57.230.199.52 -> 127.0.0.1 80/tcp   GET / HTTP/1.0 sahsc.lnk
            221.74.227.112 -> 127.0.0.1 80/tcp GET / HTTP/1.0 sahsc.bat
            201.206.207.124 -> 127.0.0.1 80/tcp GET / HTTP/1.0 sahsc.url
            69.138.171.192 -> 127.0.0.1 80/tcp GET / HTTP/1.0 sahsc.ida
            145.94 .199.68 -> 127.0.0.1 80/tcp GET / default.asp :: $ HTTP/1.0 DATOS
            69.218.155.216 -> 127.0.0.1 80/tcp GET / HTTP/1.0
            65.166.87.92 -> 127.0.0.1 80/tcp PUT / scripts / cmd.exe HTTP/1.0
            133.186.155.192 -> 127.0.0.1 80/tcp GET / scripts / cmd.exe HTTP/1.0
```

Alertas generadas por IDSWakeup

Actividades

5. Explique por qué las organizaciones deben encontrar el equilibrio entre la sensibilidad de un IDS/IPS y la cantidad de datos a analizar. ¿Qué influencia tienen en los falsos positivos y los falsos negativos?
6. Busque más información sobre las metodologías para evaluar y testear IDS/IPS que se han propuesto en este capítulo. ¿Cuáles son sus recomendaciones más importantes?

5. Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión

Los registros de auditoría son aquellos en los que se registran las acciones realizadas por los usuarios en un sistema. Estos registros son vitales para las organizaciones, ya que cuando se produce un incidente de seguridad facilitan información sobre el usuario que haya podido cometer la infracción. El registro de auditoría no solo contiene información de los usuarios, sino que también contiene información importante sobre las infracciones de seguridad sucedidas en el sistema.

Los administradores de seguridad, por tanto, deben realizar análisis periódicos de los registros de auditoría para comprobar si la seguridad de la infraestructura de red o del equipo es la adecuada y tomar medidas al respecto en caso de no serlo. De este modo se pueden ir ajustando los niveles de seguridad e ir detectando los defectos de seguridad que suceden en el equipo.

No obstante, hay que remarcar que no todos los registros de auditoría ponen de manifiesto fallos de seguridad. La gran mayoría de estos son meramente informativos. Por ejemplo, cuando un usuario ha intentado acceder al sistema sin éxito se genera un registro de error pero no significa que haya un fallo de seguridad, simplemente informa del intento de acceso del usuario sin más.

En el momento de establecer la política de auditoría hay que realizar un análisis previo para que la política implantada sea la adecuada. Si se auditan demasiados tipos de eventos puede sobrecargarse el sistema y reducir su rendimiento, por ello se recomienda la auditoría de solo aquellos eventos que faciliten información útil para evaluar la seguridad del sistema.

Así, para la definición de la política de auditoría se plantean una serie de recomendaciones:

- Determinar los equipos y dispositivos en los que se va a configurar la auditoría.
- Determinar los eventos que se quieren auditar (por ejemplo los accesos a archivos y carpetas, el inicio de sesión de los usuarios, el encendido del servidor, etc.).
- Determinar si se quiere auditar el éxito del evento, el fallo del evento o ambos casos.
- Determinar la necesidad real de auditar las tendencias de uso del sistema.
- Determinar la periodicidad de las revisiones de los registros de seguridad.

Un registro de auditoría puede clasificarse en una de las categorías mostradas en la tabla siguiente:

Categoría del registro	Descripción
Error	Para eventos de seguridad importantes.
Advertencia	Para eventos que no son importantes pero que pueden causar algún problema en un futuro.
Información	Para operaciones realizadas con éxito.
Auditoría correcta	En eventos ocurridos cuando la auditoría se ha realizado correctamente.
Auditoría incorrecta	En eventos ocurridos cuando ha habido algún fallo de auditoría.

Sea de la categoría que sea, un evento en el registro de auditoría contiene información sobre:

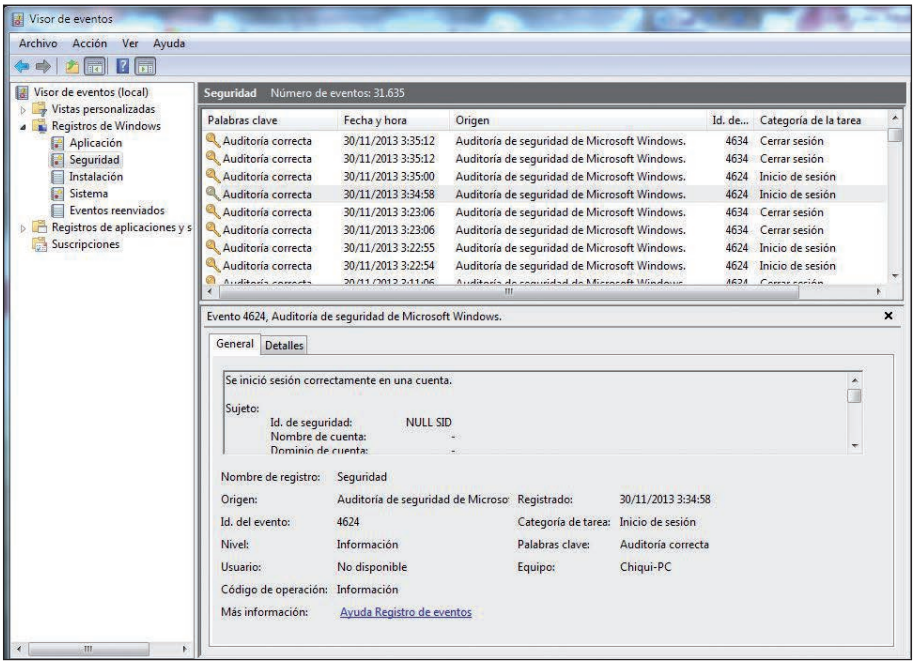
- La acción realizada.
- El usuario que ha realizado la acción.
- El éxito o fracaso del evento.
- Cuándo se ha producido el evento.
- Información adicional como, por ejemplo, el sistema desde el que se realiza la acción.

Como ya se ha comentado en el capítulo anterior, el acceso a los registros del sistema (tanto de seguridad como otros) en *Linux* se hace a través de varios comandos dependiendo del tipo de información del evento que se pretende obtener.

Para ver los registros de seguridad del sistema hay que acceder al archivo de registro de seguridad con el comando **tail-f/var/log/secure** (si solo se quieren ver las últimas líneas del registro) o con el comando ***less +F/var/log/secure*** (si se quiere ver el archivo de registro completo).

En *Windows* esta información se obtiene a través del "Visor de eventos" accediendo a **Inicio -> Panel de Control -> Herramientas administrativas -> Visor de eventos.**

En la pestaña **Seguridad** dentro de **Registros de Windows** se pueden ver específicamente los registros de seguridad con toda la información detallada.



Visor de eventos en Windows, registros de seguridad

5.1. Relación de los registros de auditoría del IDS/IPS necesarios para un correcto control de intrusiones

Una vez visto el modo en el que están monitorizados los eventos de auditoría es imprescindible conocer cuáles son los eventos fundamentales que las organizaciones deben auditar para que la detección y prevención de intrusiones en un IDS/IPS sea lo más eficiente posible.

A continuación se describen los elementos imprescindibles que deben ser sometidos a auditoría.

Sucesos de inicio de sesión de cuenta

Es necesario configurar los IDS/IPS para que auditen los intentos de inicio de sesión de cuenta, tanto exitosos como no exitosos. Eso sí, en el momento de su configuración hay que decidir en la política de corte de ataques si se

quieren auditar solo los intentos exitosos, los intentos fracasados, ambos o si directamente se decide omitir esta auditoría.

Las auditorías de inicios de sesión con éxito sirven sobre todo para poder comprobar qué ha realizado cada usuario y descubrir quién es el responsable de cualquier incidente de seguridad en el momento de su investigación: se puede comprobar quién accedió, cómo consiguió acceder y en qué equipo accedió.

Las auditorías de inicios de sesión sin éxito también resultan muy útiles para detectar intentos de intrusiones y prevenir futuros intentos.

Administración de cuentas

En estos registros de auditoría se reflejan los distintos sucesos de administración de cuentas de un equipo como, por ejemplo:

- Cuando se crea, modifica o se elimina alguna cuenta de usuario.
- Cuando se modifica alguna contraseña.
- Cuando se activa o desactiva alguna cuenta de usuario.
- Cuando se modifica el nombre de alguna cuenta de usuario.

Del mismo modo que en los registros de auditoría de inicio de sesión, también se puede decidir que el IDS/IPS elabore registros sobre los intentos exitosos, no exitosos o ambos.

Las auditorías de sucesos exitosos de administración de cuentas son muy útiles para comprobar todos los cambios producidos en las cuentas de usuario del sistema y deberían estar siempre habilitados para llevar un seguimiento de la evolución de las cuentas y de los usuarios responsables.

Sucesos de inicio de sesión

Los registros de auditoría de sucesos de inicio de sesión facilitan información de los eventos generados cada vez que un usuario inicia o cierra una sesión, además de cada vez que se realiza alguna conexión de red al equipo.

La decisión de registrar los eventos de inicio de sesión exitosos puede ser de gran utilizad, ya que se obtiene información sobre el usuario que consigue registrarse en cada equipo en el momento de investigar algún incidente de seguridad. Los registros de inicios de sesión sin éxito también son útiles (al igual que en los sucesos de inicio de sesión de cuenta) para detectar intentos de acceso de intrusos.

Nota

Hay que diferenciar los sucesos de inicio de sesión de cuenta con los sucesos de inicio de sesión. Los sucesos de inicio de sesión de cuenta hacen referencia a los intentos de acceso al equipo local a través de la red. Sin embargo, los sucesos de inicio de sesión son aquellos registrados cuando un usuario intenta iniciar la sesión desde el mismo equipo local.

Acceso a objetos

Los registros de auditoría de acceso a objetos contienen información sobre los accesos de un usuario a cualquier tipo de objeto del sistema (como carpetas, archivos, dispositivos, etc.) que esté incluido en una lista de control predefinida por el administrador.

Del mismo modo que en las anteriores, la organización también puede decidir si registrar los accesos con éxito, los intentos fracasados, ambos o, directamente, no auditar este tipo de sucesos.

Uso de privilegios

Los registros de auditoría sobre el uso de privilegios contienen información de cada evento sucedido cuando un usuario realiza alguna acción bajo unos privilegios que le han sido otorgados previamente.

Algunos de los ejemplos en los que se puede definir la generación de registros de auditoría pueden ser:

- Cuando un administrador realiza copias de seguridad de algún archivo o directorio.
- Cuando un usuario sin privilegios intenta realizar alguna acción para la que no tiene permiso (se genera un registro de error).
- Cuando el usuario con privilegios de administrador restaura algún archivo o directorio.

Seguimiento de procesos

En cuanto al seguimiento de procesos, sus registros de auditoría contienen información detallada de los sucesos ocurridos en el sistema como pueden ser: la activación de alguna aplicación, el acceso o salida a un proceso, etc.

No se recomienda la activación de este tipo de registro de auditoría, ya que debido al elevado número de procesos que acontecen en el sistema puede ser difícil localizar la información de los sucesos más valiosos.

Sucesos del sistema

Los registros de auditoría de los sucesos del sistema facilitan información sobre el reinicio o cierre de un equipo por parte de un usuario o generado por algún suceso que haya afectado a la seguridad del sistema.

Es de gran utilidad activar la generación de este tipo de registros, ya que los sucesos que acontecen son pocos y la información que se puede obtener puede ser de gran valor: siempre es útil conocer por qué se ha reiniciado o apagado el equipo para detectar qué fue lo que falló y poder evitarlo en otras ocasiones.

A modo de resumen, en la siguiente tabla se establecen los registros de auditoría de los IDS/IPS que se recomiendan para que la monitorización y evaluación de su funcionamiento sea la correcta y se pueda realizar un control eficiente de los eventos generados por intentos de intrusión:

Registro de auditoría	Breve descripción
Sucesos de inicio de sesión de cuenta	En eventos de inicio o cierre de sesión de cuenta a través de la red.
Administración de cuentas	En eventos de modificaciones de las cuentas de usuario.
Sucesos de inicio de sesión	En eventos de inicio o cierre de sesión en equipos locales.
Acceso a objetos	En eventos de acceso a objetos predefinidos en una lista de control.
Uso de privilegios	En eventos de acciones de un usuario bajo unos privilegios asignados.
Seguimiento de procesos	En eventos referentes a cualquier proceso ejecutado en el sistema.
Sucesos del sistema	En eventos de reinicio o cierre de sesión provocados por algún usuario o por algún fallo de seguridad.

Aplicación práctica

Usted se encuentra en pleno proceso de revisión del sistema IDS/IPS implantado en su equipo y quiere comprobar los distintos eventos de seguridad que han sucedido en las dos últimas semanas para ver si ha habido algún ataque no detectado en el sistema. Teniendo en cuenta que utiliza Linux como sistema operativo y que quiere ver el archivo de registro de seguridad completo para que no se le escape nada, ¿qué comando debe utilizar? En el caso de querer ver solo las últimas líneas del archivo de registro, ¿qué otro comando utilizaría?

SOLUCIÓN

Utilizando el sistema operativo *Linux,* para ver el archivo de registro de seguridad al completo hay que utilizar el comando **less +F/var/log/secure.** Si solo se quisieran visualizar las últimas líneas del archivo de registro habría que utilizar otro comando: **tail -/var/log/secure.**

Actividades

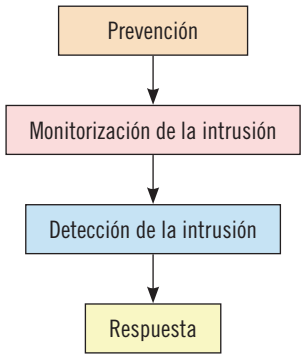
7. Dependiendo del sistema operativo que tiene en su ordenador personal, profundice en las herramientas de visualización de registros de seguridad y sus funcionalidades principales.
8. Busque más información sobre los registros de auditoría necesarios para conseguir un control adecuado de las intrusiones de un sistema. Proponga otros tipos de registros de auditoría que contengan eventos que considere básicos para efectuar este control.

6. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

Los sistemas de detección y prevención de intrusiones siguen una serie de fases en sus procesos:

- **Prevención:** en un momento inicial, los IDS/IPS intentan evitar los ataques mediante mecanismos que dificulten el acceso de intrusos.
- **Monitorización de la intrusión:** si, a pesar de todas las medidas preventivas ha habido una intrusión o actividad sospechosa, los IDS/IPS detectan esta actividad y monitorizan el tráfico de datos sospechoso para que pueda ser analizado y revisado por el administrador del sistema.
- **Detección de la intrusión:** cuando se ha analizado el tráfico, si el IDS/IPS determina que la actividad sospechosa es efectivamente una intrusión, el sistema genera una alarma para notificar esta intrusión al administrador.
- **Respuesta:** determinada la intrusión como ataque los sistemas IDS/IPS pueden adoptar una serie de medidas que intenten bloquear el acceso del atacante al sistema.

Fases de los procesos de detección y prevención de instrucciones



Para que la implantación se realice correctamente y el funcionamiento del IDS/IPS sea realmente efectivo es necesaria la inclusión de una base de datos de firmas que permita la monitorización de los eventos y su clasificación entre actividades sospechosas, actividades no sospechosas e intrusiones reales.

Cuando la implantación ya está completada es posible que el funcionamiento del sistema no sea el adecuado debido al elevado número de falsos positivos detectados como amenaza o a ciertas intrusiones no detectadas como tal. Para solucionarlo hay que realizar una serie de pruebas (ya descritas en apartados anteriores) que permitan comparar los resultados de varias configuraciones y así conseguir definir la configuración más adecuada a las necesidades de seguridad de la organización.

Aunque ya se haya verificado que el IDS/IPS funciona correctamente, no hay que olvidar realizar comprobaciones y actualizaciones periódicas para detectar la posible obsolescencia de la base de datos de intrusiones o la pérdida de efectividad del sistema implantado.

Aunque la determinación de los niveles adecuados de monitorización, prueba y actualización de los sistemas de detección y prevención de intrusiones dependa de las directrices y requerimientos de cada organización, para medir la eficiencia del sistema IDS/IPS y establecer estos niveles se deben tener en cuenta las características siguientes:

- **Precisión:** la precisión de un sistema IDS/IPS es su capacidad para detectar ataques y diferenciarlos del tráfico normal de una red. Para medir la precisión se utiliza el porcentaje de falsos positivos (el número de veces que se detecta un ataque que es una actividad normal) y el porcentaje de falsos negativos (número de ataques no detectados por el sistema) con la fórmula siguiente:

$$\text{Precisión} = \frac{\text{Ataques reales detectados}}{\text{Ataques reales detectados} + \text{Falsos positivos}}$$

  Debido a que minimizar a la vez los porcentajes de falsos positivos y falsos negativos es prácticamente imposible (ya que cuando se quieren minimizar los falsos negativos se produce un aumento de los falsos positivos al aumentar la sensibilidad del sistema y viceversa), lo ideal es encontrar el equilibrio entre ambos.

  En cuanto a la fórmula, la precisión será mayor cuando el ratio obtenido sea 1 o lo más cercano a 1 posible, lo que significará que la gran mayoría de ataques reales detectados son realmente ataques.
- **Rendimiento:** el rendimiento de un sistema de detección y prevención de intrusiones consiste en la cantidad de eventos que el sistema puede analizar. Aunque lo ideal sería que el sistema pudiese analizar todo el tráfico de la red habrá que limitar su rendimiento a lo que permita la capacidad de procesamiento del equipo.

  De este modo las organizaciones deberán buscar un equilibrio entre la cantidad de tráfico de red a analizar y la cantidad de recursos que quieren o pueden utilizar para este análisis.
- **Completitud:** la completitud de un sistema IDS/IPS se consigue cuando detecta todos los tipos de ataques sucedidos en el equipo. Lo habitual es que estos sistemas no puedan detectar todos los tipos de ataques y sea necesario el establecimiento de otras soluciones que completen esta carencia. Las organizaciones deben conseguir un equilibrio entre la completitud de un sistema y su precisión para que así se detecte el mayor número posible de ataques sin que haya un exceso de falsos positivos o falsas alarmas.

La fórmula de la plenitud de un sistema se define a continuación:

$$\text{Completitud} = \frac{\text{Ataques reales detectados}}{\text{Ataques reales detectados} + \text{Falsos negativos}}$$

En este caso también es recomendable que la ratio obtenida de la fórmula sea lo más próxima a 1 posible, ya que esto indicará que todos los ataques han sido detectados y que los falsos negativos se han reducido al mínimo.

- **Tolerancia a fallos:** la tolerancia a fallos de un IDS/IPS es su capacidad para resistir a los ataques y a los fallos del sistema (cortes de electricidad, etc.). Un IDS debe ser sólido y seguro para que un ataque no pueda inutilizarlo y dejar el sistema expuesto a todo tipo de riesgos.
  Además, un IDS/IPS también debe ser capaz de recuperar la configuración establecida, los patrones para detectar intrusiones y los registros y alarma generados anteriormente.
- **Tiempo de respuesta:** el tiempo de respuesta de un IDS/IPS consiste en el período de tiempo que tarda en reaccionar cuando se produce un ataque. Esta reacción puede ser tanto la generación de alarmas como el establecimiento de medidas de corte del ataque.
  Está claro que las organizaciones deben configurar estos sistemas para que el tiempo de respuesta sea lo más reducido posible, pues así se conseguirá una mayor efectividad.

Actividades

9. Busque más indicadores que considere fundamentales para conocer la eficacia de la implantación de un sistema IDS/IPS en una organización.
10. Explique qué diferencia hay entre la precisión y la completitud de un IDS/IPS. ¿Por qué se recomienda encontrar un equilibrio de los dos indicadores? Justifique su respuesta.

Aplicación práctica

Usted, como responsable de seguridad y administrador del sistema de red de su empresa, quiere determinar si el IDS/IPS tiene un nivel de precisión apropiado. Teniendo en cuenta que la cantidad de ataques reales detectados han sido 53 y que los falsos positivos han sido 2, determine la precisión del sistema y evalúe si el nivel es apropiado.

SOLUCIÓN

Teniendo en cuenta que los ataques reales detectados han sido 53 y los falsos positivos han sido solo 2, se establece que el nivel de precisión es 0,96 (53 / (53 + 2)). Este nivel es bastante aproximado a 1, lo que indica que la precisión del sistema es adecuada al ser prácticamente todos los ataques detectados correctos.

7. Resumen

Los sistemas de detección y prevención de intrusiones son una potente herramienta para evitar posibles ataques que pueden producirse en la infraestructura de red de la organización. Son sistemas complejos y muy especializados, por lo que es vital que las organizaciones realicen un análisis previo de sus infraestructuras, servicios, equipos, zonas y protocolos utilizados para determinar el sistema a implantar, sus características y configuraciones y su localización dentro de sus instalaciones o a través de entornos virtuales.

Una vez ya tomada la decisión sobre el sistema de detección y prevención de intrusiones que se va a implantar en una organización deben decidirse qué políticas de corte de ataques se van a aplicar cuando se detecte alguna intrusión distinguiendo entre políticas de respuesta pasiva (cuando el sistema se limita a informar de los detalles de la intrusión) y políticas de respuesta activa (cuando el sistema además de informar toma medidas que frenen el ataque).

La siguiente fase en la detección y prevención de intrusiones consiste en analizar los eventos que ha registrado el IDS/IPS y que ha calificado como ataques. Estos sistemas no son perfectos y puede ser que haya falsos positivos

y falsos negativos. Por ello, las organizaciones deben configurar sus sistemas para que el número de errores sea el mínimo posible consiguiendo un equilibrio entre la sensibilidad del sistema y la cantidad de datos a inspeccionar según sus requerimientos y necesidades.

Los registros de auditoría en un IDS/IPS son aquellos en los que se registran eventos realizados por los usuarios en un sistema y facilitan información tanto de los usuarios como de los demás detalles del evento realizado.

Una vez definidas las políticas de actuación y analizados los registros de auditoría, los administradores de la organización ya tienen suficiente información para comprobar la eficacia del sistema de detección y prevención de intrusiones. Aun así, siempre será necesario el establecimiento de pruebas y actualizaciones periódicas del sistema implantado que garanticen que no hay ninguna merma de eficacia mediante la comprobación de una serie de indicadores como el rendimiento, la completitud, la precisión, la tolerancia a fallos y el tiempo de respuesta del sistema.

Ejercicios de repaso y autoevaluación

1. **Indique cuál de las siguientes ventajas no está ofrecida por el IDS/IPS situado detrás del cortafuegos.**

    a. El riesgo de ataques exitosos disminuye considerablemente.
    b. Al poder identificar los ataques más comunes permite una configuración más efectiva del cortafuegos principal.
    c. Permite una correlación entre los ataques detectados antes y después del cortafuegos.
    d. La cantidad de logs es inferior, pero la información facilitada por estos sistemas está mejor seleccionada y es más relevante.

2. **¿Qué son los IDS/IPS inalámbricos o Wireles IDS/IPS? ¿Cómo funcionan?**

    _____
    _____
    _____
    _____

3. **¿Cuál de los siguientes aspectos no se incluye en el análisis previo para implantar un sistema IDS/IPS en una organización?**

    a. Análisis de los protocolos de red utilizados.
    b. Análisis de las zonas externas de la organización.
    c. Análisis de los servicios que ofrece la organización.
    d. Análisis de los procesos de negocio e identificación de la información valiosa en cada uno de los procesos.

4. Rellene la siguiente tabla indicando los distintos tipos de análisis existentes atendiendo a las clasificaciones indicadas:

Análisis de los datos obtenidos por los IDS/IPS	
Clasificación del análisis	**Tipo de análisis**
Según el procedimiento de análisis de los datos	
Según el tiempo del análisis	

5. Indique a qué tipo de política de respuesta (activa o pasiva) a la detección de un ataque pertenecen las siguientes acciones.

a. Envío de un correo electrónico para notificar la detección del ataque.
b. Almacenaje de los detalles de la alerta en una base de datos.
c. Envío de un ResetKill.
d. Almacenamiento de los paquetes sospechosos.

6. Complete los espacios libres de la siguiente oración:

Una política de seguridad _____ se basa en prohibir todo lo que no se ha definido como permitido expresamente. Sin embargo, las políticas de seguridad _____ son todo lo contrario, definen todo lo que se va a prohibir y todo lo demás se considera como permitido.