MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE SERVEI PÚBLIC D'OCUPACIÓ ESTATAL
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES
Generalitat de Catalunya
SOC Servei d'Ocupació de Catalunya
IRON HACK SPAIN

Gestión de incidentes de seguridad informática

IFCT0109 – Seguridad informática

MF0488_3 (90 horas)

Implantación y puesta en producción de sistemas IDS/IPS

- Introducción
- Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio
- Definición de políticas de corte de intentos de intrusión en los IDS/IPS
- Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
- Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
- Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/ IPS
- Resumen

Introducción

Cuando una organización decide implementar un sistema de detección y prevención de intrusos (IDS/IPS), es esencial realizar análisis y comprobaciones previas para garantizar una implementación eficaz.

En este contexto, se abordan diferentes aspectos cruciales, como la ubicación del sistema, los equipos involucrados, los protocolos y servicios utilizados diariamente para la transferencia y utilización de datos.

Una vez determinada la ubicación y las características de estos sistemas, se exploran diversas políticas de seguridad que pueden emplearse cuando se detecta actividad sospechosa.

Es importante reconocer que no todas las intrusiones detectadas son reales, y algunas pueden pasar desapercibidas. Por lo tanto, se ofrecen recomendaciones para configurar los sistemas IDS/IPS y minimizar tanto las intrusiones no detectadas como las falsas alarmas.

Además, se detallan las informaciones que deben proporcionar estos sistemas al detectar una intrusión, facilitando así una adecuada monitorización de los eventos y la verificación del funcionamiento correcto del equipo y sus dispositivos.

Finalmente, se presentan recomendaciones para definir niveles óptimos de monitorización, actualización y pruebas antes y después de la implementación del sistema de detección y prevención de intrusos.

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

Introducción

Los sistemas de detección y prevención de intrusiones (IDS/IPS) son esenciales en la protección de la infraestructura de red empresarial, especialmente ante el aumento constante de intentos de intrusión y manipulación de datos. Sin embargo, su implementación requiere más que simplemente desplegarlos.

Las organizaciones deben complementar estos sistemas con medidas de seguridad adicionales y asegurarse de que los responsables de la infraestructura comprendan su funcionamiento. Antes de la implementación, es crucial realizar un análisis exhaustivo de la infraestructura, servicios, equipos, zonas y protocolos utilizados. Esto garantiza una implementación efectiva de los sistemas IDS/IPS y otras medidas de seguridad.

El proceso de implementación requiere una planificación meticulosa, preparación, pruebas y capacitación especializada para los administradores. Esto asegura que, una vez implementados, los sistemas funcionen a pleno rendimiento y brinden un nivel de seguridad adecuado.

La implementación de los sistemas IDS/IPS debe adaptarse a los recursos y políticas de la organización, realizándose de manera escalonada para permitir que los administradores adquieran experiencia a lo largo del proceso.

Es fundamental recordar que los IDS detectan accesos no autorizados, mientras que los IPS tienen como objetivo evitarlos. Se describirán las opciones de ubicación de los sistemas IPS/IDS, junto con sus características, ventajas e inconvenientes, para ayudar a las organizaciones a tomar decisiones informadas sobre su implementación.

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

Sistemas de detección y prevención de intrusiones en red o NIDPS

Los NIDPS son sistemas que monitorizan el tráfico de red en busca de actividades maliciosas o anómalas. Su objetivo es detectar intrusiones y prevenir ataques, así como proporcionar información sobre las amenazas y los eventos de seguridad.

Los NIDPS se pueden colocar en diferentes puntos de la red, cada uno con sus ventajas e inconvenientes:

Delante del cortafuegos:

Ventajas:

- Detecta ataques externos, incluyendo aquellos dirigidos al cortafuegos.
- Ofrece una visión general de la actividad de la red.

Desventajas:

- No detecta ataques con información encriptada.
- Puede saturarse con el tráfico de red.
- Genera una gran cantidad de información que puede dificultar la identificación de las amenazas reales.
- Es vulnerable a ataques directos.

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

Sistemas de detección y prevención de intrusiones en red o NIDPS

Detrás del cortafuegos:

Ventajas:

- Detecta intrusiones que han logrado superar el cortafuegos.
- Monitoriza el tráfico interno y externo.
- Ofrece información más precisa y relevante sobre las amenazas.
- Reduce la cantidad de logs que se generan.

Desventajas:

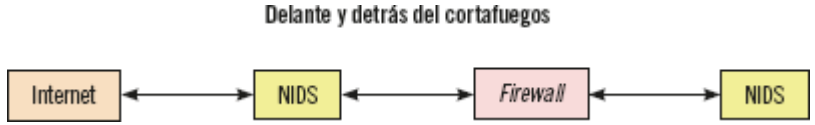
- No detecta ataques en la zona desmilitarizada (DMZ).
- No puede identificar ataques con información encriptada.
- Requiere medidas de seguridad adicionales para proteger el NIDPS.

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

Sistemas de detección y prevención de intrusiones en red o NIDPS

Tanto antes como detrás del cortafuegos:

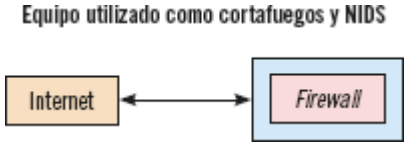
Esta combinación reúne las ventajas de las dos ubicaciones y además, proporciona otras adicionales:



- Mayor control de las posibles intrusiones en la red.
- Mejora de 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.

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

Sistemas de detección y prevención de intrusiones en red o NIDPS

Ubicación en las redes principales de la organización

Independientemente de si se ubica el IDS/IPS antes o después del cortafuegos, es necesario 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:

- No se detectan ataques con información encriptada.
- Los sistemas situados en las redes generales pueden hacerlas más vulnerables ante ataques internos.

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

Sistemas de detección y prevención de intrusiones en red o NIDPS

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.

Recomendaciones:

La ubicación ideal del NIDPS depende de las necesidades específicas de cada organización.

Se recomienda combinar la ubicación del NIDPS con otras medidas de seguridad como firewalls, sistemas de detección de intrusiones basados en host (HIDS) y análisis de seguridad de la red (NSA).

Es importante mantener el NIDPS actualizado con las últimas definiciones de amenazas y configurar correctamente las reglas de detección.

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

Sistemas de detección y prevención de intrusiones en hosts o HIDPS

Los sistemas de detección y prevención de intrusiones basados en hosts (HIDS) son aquellos que se instalan en el mismo equipo que monitorizan y se encargan de protegerlo de intrusiones. A diferencia de los NIDS/NIDPS, no monitorizan todo el tráfico de la red de una organización.

Ventajas: Consumen menos recursos que los NIDS/NIDPS y no impiden un buen rendimiento del sistema.

Desventajas:

- Combaten las intrusiones una vez que el equipo ya está en peligro, lo que aumenta el riesgo.
- Requieren medidas de seguridad adicionales en el equipo para combatir los ataques.
- No detectan ataques con información encriptada.

Los HIDS monitorizan con más profundidad los datos del equipo que los NIDS/NIDPS, incluyendo:

- Tráfico inalámbrico
- Tráfico de red
- Accesos a los archivos
- Cambios de configuración en el equipo o en alguna aplicación

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

IDS / IPS en ambientes virtuales

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

- Ahorro de energía: Se necesita una infraestructura menor en la organización para almacenar datos.
- Coste reducido de mantenimiento: Permite que los equipos tengan mayor capacidad de almacenamiento y reduce el espacio físico, lo que implica menos gastos de electricidad, alquiler de local, etc.

Definición de 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.

Seguridad:

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.

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

IDS / IPS en ambientes virtuales

Ventajas de usar IDS/IPS en ambientes virtuales:

- Mayor visibilidad: Los IDS/IPS pueden monitorizar todo el tráfico de red, incluso el tráfico entre máquinas virtuales.
- Detección más precisa: Los IDS/IPS pueden utilizar técnicas de análisis de comportamiento para detectar ataques que no se basan en firmas conocidas.
- Respuesta más rápida: Los IDS/IPS pueden automatizar la respuesta a las intrusiones, lo que puede ayudar a minimizar el daño causado por un ataque.

Desventajas de usar IDS/IPS en ambientes virtuales:

- Mayor complejidad: La configuración y gestión de IDS/IPS en ambientes virtuales puede ser más compleja que en entornos físicos.
- Impacto en el rendimiento: Los IDS/IPS pueden consumir recursos adicionales, lo que puede afectar al rendimiento de las máquinas virtuales.

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

IDS/IPS inalámbricos o wireless IDS/IPS

Los IDS/IPS inalámbricos analizan los protocolos inalámbricos para detectar actividades sospechosas. Funcionan de manera similar a los IDPS basados en red, con servidor, consola y base de datos, y permiten monitorizar el tráfico de red que circula por la red inalámbrica de la organización.

Desventaja:

Los análisis se limitan a un solo canal. Si la organización utiliza varios canales inalámbricos, no podrán realizarse análisis de todos los canales simultáneamente

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

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

Análisis previo a la implementación:

- Procesos de negocio e información valiosa: Identificar la información crítica en cada proceso.
- Protocolos de red: Analizar los protocolos utilizados para la transferencia de datos.
- Políticas de la organización: Asegurar la coherencia con la política de seguridad y costes.
- Zonas de la organización: Evaluar la ubicación de equipos y servidores para determinar la ubicación más conveniente del IDS/IPS.
- Servicios: Identificar los servicios que requieren un nivel de seguridad especial.

Planificación e implementación:

- Los sistemas IDS/IPS no deben ser los únicos sistemas de seguridad.
- Se deben implementar otras medidas como antivirus, firewalls, etc.

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

Introducción

Las políticas de corte de intentos de intrusión en los IDS/IPS definen la respuesta del sistema ante un ataque o intento de intrusión.

Tipos de análisis en IDS/IPS:

- Detección de usos indebidos (misuse): Comparación de las firmas de la base de datos con la información recogida.
- Detección de anomalías: Empleo de técnicas estadísticas para definir patrones de comportamiento normal.

Modos de análisis:

- Análisis por lotes (batch mode): Detección de intrusiones cada cierto intervalo de tiempo.
- Análisis en tiempo real: Examen de los datos a medida que se van recibiendo.

Tipos de políticas de seguridad:

- Política prohibitiva: Prohíbe todo lo que no se ha definido como permitido.
- Política permisiva: Define todo lo que se va a prohibir y permite el resto.

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

Introducción

Definición de políticas de actuación:

- Política de corte: Define qué acciones se tomarán ante un ataque.
- Nivel de severidad: Define la gravedad de un ataque para determinar la acción a tomar.

Opciones de acción:

- Generar una alerta: Informar al administrador del sistema sobre el ataque.
- Bloquear el tráfico: Detener el tráfico malicioso.
- Deshabilitar la cuenta: Desactivar la cuenta del usuario atacante.
- Reiniciar el dispositivo: Reiniciar el dispositivo afectado.

Consideraciones:

- Minimizar los falsos positivos: Evitar que el sistema bloquee tráfico legítimo.
- Equilibrar la seguridad y la usabilidad: No restringir demasiado el acceso al sistema.
- Mantener las políticas actualizadas: Adaptar las políticas a las nuevas amenazas.

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

Políticas de corte de intrusiones en sistemas IDS/IPS

Las políticas de corte de intentos de intrusiones en los IDS/IPS son esenciales para proteger los sistemas informáticos de ataques. Estas políticas definen la respuesta del sistema ante un ataque o intento de intrusión, y deben ser cuidadosamente configuradas para minimizar los falsos positivos y mantener un equilibrio entre la seguridad y la usabilidad.

Tipos:

- Respuesta pasiva
- Respuesta activa

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

Políticas de corte de intrusiones en sistemas IDS/IPS

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.

Ejemplos de políticas de respuesta pasiva:

- Envío de un correo electrónico: Se envía un correo electrónico a uno o varios usuarios informando de la intrusión.
- Registro del ataque: Se almacenan los detalles de la alerta en una base de datos.
- Almacenamiento de paquetes sospechosos: Se almacenan todos los paquetes de datos que originaron la alerta.
- Apertura de una aplicación: Se abre una aplicación que realiza una acción específica, como el envío de mensajes de texto o la emisión de un sonido.
- Notificación visual: 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.

- Las políticas de respuesta pasiva pueden integrarse con herramientas de SOAR (Security Orchestration, Automation and Response) para automatizar la respuesta a incidentes.
- Se puede utilizar inteligencia artificial para analizar los datos de las alertas y determinar si se trata de un ataque real o un falso positivo.
- Se pueden definir diferentes niveles de respuesta en función de la gravedad del ataque.

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

Políticas de corte de intrusiones en sistemas IDS/IPS

Respuesta activa

Los sistemas de detección y prevención de intrusos (IDS/IPS) no solo detectan actividades sospechosas, sino que también pueden tomar acciones para detenerlas o mitigarlas. Estas acciones se conocen como respuestas activas.

Algunos ejemplos de respuestas activas en sistemas IDS/IPS incluyen:

- El sistema IDS/IPS puede bloquear la dirección IP del atacante para evitar que acceda a la red.
- Cerrar las sesiones activas del atacante para evitar que acceda a los recursos de la red.
- Forzar el cambio de contraseñas de las cuentas comprometidas.
- Cuarentena de dispositivos: aislar los dispositivos infectados para evitar que propaguen la infección a otros dispositivos de la red.
- Alertas automáticas: enviar alertas automáticas a los administradores de seguridad para que investiguen el incidente.

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

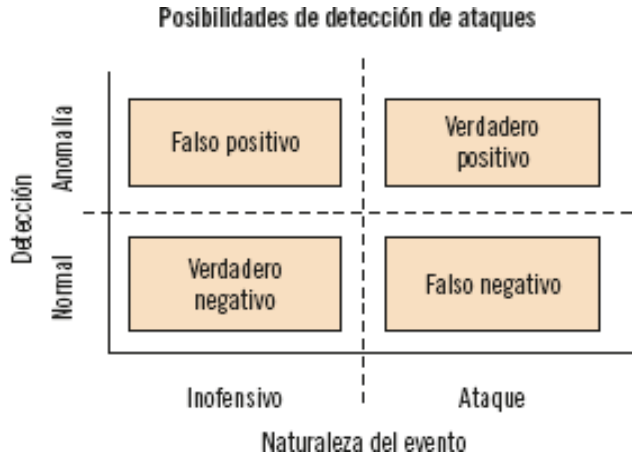
Imprecisiones en la detección de eventos por IDS/IPS

Limitaciones:

- Bases de datos desactualizadas: Las firmas de ataque pueden no estar al día con las últimas amenazas, generando falsos negativos
- Imperfecciones en la detección de anomalías: Los métodos estadísticos pueden generar falsos positivos al no distinguir entre comportamientos normales e inusuales

Posibilidades en la toma de decisiones:

- Falso positivo: El sistema identifica tráfico inofensivo como un ataque
- Falso negativo: Un ataque no es detectado por el sistema
- Verdadero positivo: Un ataque es correctamente detectado.
- Verdadero negativo: El sistema identifica correctamente tráfico inofensivo.



Mejora del análisis:

- Actualización constante de las bases de datos de firmas.
- Afinación de los métodos de detección de anomalías para minimizar los falsos positivos.
- Implementación de técnicas de aprendizaje automático para mejorar la precisión.

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

Imprecisiones en la detección de eventos por IDS/IPS

El objetivo de un IDS/IPS es minimizar los errores (falsos positivos y falsos negativos) y maximizar los aciertos (verdaderos positivos y verdaderos negativos).

Razones:

- Efectividad: Un alto número de errores reduce la eficacia del sistema.
- Recursos: Los falsos positivos consumen tiempo y recursos innecesarios.
- Seguridad: Los falsos negativos pueden tener graves consecuencias para la información de la organización.

Para reducir los errores, se debe ajustar la configuración del sistema, optimizándola, según las características de la red y sus necesidades.

Es necesario realizar pruebas, que nos sirvan de referencia, con diferentes configuraciones y comparar los resultados para detectar y eliminar la causa de los errores.

Las alarmas generadas por el sistema pueden indicar un ataque real, un falso positivo o un falso negativo. El objetivo final es encontrar un equilibrio entre los falsos positivos y los falsos negativos.

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

Imprecisiones en la detección de eventos por IDS/IPS

El gráfico presentado ilustra el comportamiento de la tasa de error en un sistema de detección y prevención de intrusiones (IDS/IPS) al modificar dos variables clave: la sensibilidad del sistema y la cantidad de paquetes inspeccionados.

Relación entre sensibilidad y errores:

Mayor sensibilidad:

- Aumenta la probabilidad de detectar falsos positivos (alertas por actividad inofensiva).
- Disminuye la probabilidad de falsos negativos (ataques no detectados).

Menor sensibilidad:

- Disminuye la probabilidad de falsos positivos.
- Aumenta la probabilidad de falsos negativos.

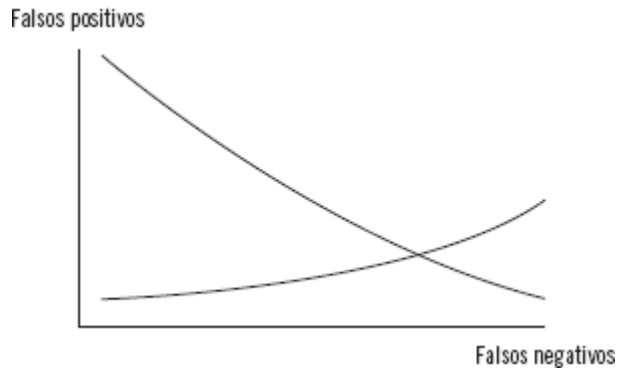
Relación entre cantidad de paquetes y errores:

Mayor cantidad de paquetes:

- Aumenta la probabilidad de detectar falsos positivos.
- Disminuye la probabilidad de falsos negativos.

Menor cantidad de paquetes:

- Disminuye la probabilidad de falsos positivos.
- Aumenta la probabilidad de falsos negativos.



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

Encontrar el equilibrio

El objetivo al configurar un IDS/IPS es encontrar un equilibrio entre la sensibilidad y la cantidad de paquetes a inspeccionar, considerando las necesidades de cada organización.

Recomendaciones para minimizar falsos positivos:

- Eliminar alertas de sistemas de supervisión de red: Los sistemas de supervisión de red monitorean el tráfico de la red para detectar problemas de rendimiento o disponibilidad. El IDS/IPS puede interpretar la actividad legítima de estos sistemas como intentos de intrusión, generando falsos positivos. La solución es configurar el IDS/IPS para que excluya las direcciones IP o subredes utilizadas por los sistemas de supervisión de red.
- Desactivar el IDS/IPS durante pruebas de vulnerabilidad: Evitar que las pruebas sean detectadas como ataques.
- Configurar alertas de comportamiento de usuario: El IDS/IPS puede monitorizar el comportamiento de los usuarios en la red y generar alertas ante actividades sospechosas. Sin embargo, algunas actividades legítimas, como compartir archivos o utilizar mensajería instantánea, pueden activar estas alertas.
- No desactivar alertas de troyanos/gusanos: Mantener estas alertas activas para detectar ataques reales.
- Ajustar alertas de cadenas de registro web: Configurar las alertas para evitar que se activen por cadenas no maliciosas. Las cadenas de registro web son líneas de texto que contienen información sobre un recurso web específico, como una página web o una imagen
- Desactivar alertas de actividad de autenticación de base de datos: Si la organización tiene un alto nivel de actividad legítima, desactivar estas alertas para reducir falsos negativos.

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

Encontrar el equilibrio

Metodologías para evaluar la configuración:

- OSSTM (Open Source Security Testing Methodology): Ofrece una metodología para evaluar sistemas de seguridad, especialmente firewalls e IDS/IPS.
- OSSEC (Open Security Evaluation Criteria): Similar a OSSTM, pero enfocado en estandarizar productos de seguridad para NIDS y firewalls.

Herramientas para generar falsos ataques:

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 específicas o aleatorias.
- Sneeze: Generador de falsos positivos diseñado para Snort.
- Stick: Evalúa la capacidad del sistema para detectar intrusiones y probar las reglas del IDS y del firewall.

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

Introducción

Los registros de auditoría del IDS/IPS son vitales para la seguridad de la red, ya que permiten:

Monitorizar y supervisar el correcto funcionamiento del sistema:

- Detectar fallos o anomalías en el funcionamiento del IDS/IPS.
- Verificar que las reglas de detección están funcionando correctamente.
- Identificar posibles vulnerabilidades en el sistema.

Detectar eventos de intentos de intrusión:

- Identificar los tipos de ataques que se están intentando realizar.
- Conocer la fuente de los ataques.
- Evaluar el impacto potencial de los ataques.

Los tipos de registros de auditoría que se pueden generar en un IDS/IPS son:

- Eventos
- Alertas
- Mantenimiento

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

Introducción

Registros de eventos:

- Inicio de sesión y cierre de sesión.
- Acceso a archivos y carpetas.
- Ejecución de aplicaciones.
- Cambios en la configuración del sistema.
- Tráfico de red.

Registros de alertas:

- Alertas generadas por el IDS/IPS.
- Información sobre la alerta: fecha, hora, tipo de alerta, origen y destino del ataque, etc.

Registros de mantenimiento:

- Tareas de mantenimiento realizadas en el IDS/IPS.
- Información sobre las tareas de mantenimiento: fecha, hora, tipo de tarea, usuario que la realizó, etc.

Es importante tener en cuenta que la lista de registros de auditoría no es exhaustiva y puede variar en función del tipo de IDS/IPS y de las necesidades específicas de la organización.

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

Introducción

Recomendaciones para la configuración de la auditoría:

- Determinar los equipos y dispositivos en los que se va a configurar la auditoría.
- Determinar los eventos que se quieren auditar.
- 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.

La auditoría de los registros del IDS/IPS es una herramienta fundamental para la seguridad de la red. Una configuración adecuada de la auditoría puede ayudar a detectar y prevenir intrusiones en la red, así como a identificar posibles vulnerabilidades en el sistema.

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

Introducción

Posibles categorías de registros

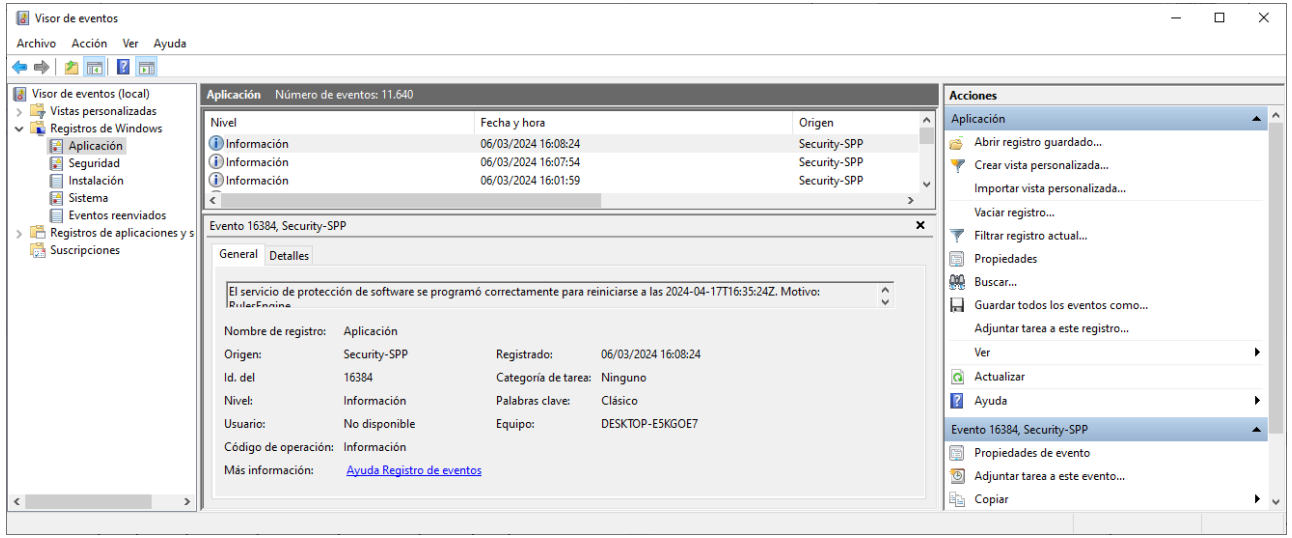
Categoría del registro	Descripción
Error	Para eventos de seguridad importantes.
Advertencia	Para eventos que no son importantes pero que pueden causar algún problema en un futuro.
Información	Para operaciones realizadas con éxito.
Auditoría correcta	En eventos ocurridos cuando la auditoría se ha realizado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

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

Introducción

Un evento en el registro de auditoría contiene información sobre:

- La acción realizada: qué acción se ha realizado en el sistema. Por ejemplo, un inicio de sesión, un cambio de configuración o la creación de un archivo
- El usuario que ha realizado la acción: quién ha realizado la acción en el sistema. Se puede identificar por el nombre de usuario, la dirección IP o la identificación del usuario.
- El éxito o fracaso del evento: si la acción se ha realizado correctamente o si ha fallado.
- Cuándo se ha producido el evento: la fecha y hora en que se ha producido la acción.
- Información adicional: detalles adicionales sobre la acción, como el tipo de objeto que se ha modificado, la aplicación que se ha utilizado o la dirección IP desde la que se ha realizado la acción.



Sysmon

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

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

Para garantizar un control efectivo de intrusiones, es esencial auditar una serie de eventos clave en los IDS/IPS. Estos registros proporcionan información crucial para detectar y prevenir actividades no autorizadas. A continuación, se detallan los elementos esenciales que deben ser objeto de auditoría:

Sucesos de inicio de sesión de cuenta:

- Se deben auditar los intentos de inicio de sesión de cuenta, tanto exitosos como no exitosos.
- Las auditorías de inicios de sesión exitosos permiten identificar quién accedió, cómo lo hizo y en qué equipo, crucial para investigaciones de seguridad.
- Las auditorías de inicios de sesión sin éxito son útiles para detectar intentos de intrusiones y prevenir futuros ataques.

Administración de cuentas:

- Registra eventos como la creación, modificación o eliminación de cuentas de usuario, cambios de contraseña y activación/desactivación de cuentas.
- Es fundamental auditar tanto los eventos exitosos como los no exitosos para mantener un seguimiento adecuado de los cambios en las cuentas y los usuarios responsables.

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

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

Sucesos de inicio de sesión:

- Proporcionan información sobre cada inicio o cierre de sesión de usuario, así como conexiones de red al equipo.
- Registrar los inicios de sesión exitosos permite identificar quién accede a cada equipo, mientras que los inicios de sesión sin éxito ayudan a detectar intentos de acceso no autorizado.

Es vital diferenciar entre los sucesos de inicio de sesión de cuenta y los sucesos de inicio de sesión, ya que estos últimos se refieren a los intentos de acceso desde el mismo equipo local.

Auditoría de Acceso a Objetos

- Este proceso implica registrar y monitorear las interacciones de los usuarios con los diversos elementos del sistema, como archivos, carpetas y dispositivos.
- Por ejemplo, cuando un empleado intenta acceder a un archivo confidencial o modificar una carpeta protegida, la auditoría de acceso a objetos registra estos intentos y proporciona información detallada sobre quién intentó acceder, cuándo y si la acción tuvo éxito o no. Este tipo de auditoría es esencial para garantizar la integridad y la confidencialidad de los datos en una organización.

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

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

Uso de Privilegios

- Se centra en monitorear las acciones realizadas por los usuarios que poseen ciertos privilegios dentro del sistema.
- Por ejemplo, cuando un administrador realiza una tarea crítica como la creación de cuentas de usuario o la instalación de software, la auditoría de privilegios registra estos eventos.
- Del mismo modo, si un usuario intenta realizar una acción para la que no tiene los privilegios necesarios, como eliminar archivos importantes, se genera un registro de error.
- Estos registros son vitales para detectar actividades inapropiadas o maliciosas dentro de un entorno informático.

Seguimiento de Procesos

- El seguimiento de procesos implica registrar y analizar los eventos relacionados con la ejecución de programas y aplicaciones en un sistema informático.
- Por ejemplo, cuando se inicia una aplicación crítica para el funcionamiento del negocio o cuando se accede a un proceso importante del sistema, se generan registros de seguimiento de procesos.
- Aunque esta auditoría puede proporcionar información valiosa sobre el rendimiento y la estabilidad del sistema, su activación puede generar una gran cantidad de datos, lo que dificulta la identificación de eventos significativos en entornos de alta actividad.

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

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

Sucesos del Sistema

- Los sucesos del sistema comprenden eventos importantes que afectan el funcionamiento y la seguridad del sistema en su conjunto. Esto incluye acciones como reinicios o apagados inesperados, así como eventos críticos que pueden indicar vulnerabilidades o ataques en curso.
- Por ejemplo, si un sistema experimenta un reinicio no programado o un cierre repentino, la auditoría de sucesos del sistema registra este evento y proporciona detalles sobre su causa y momento. Activar esta auditoría es esencial para identificar y mitigar posibles riesgos para la seguridad y el rendimiento del sistema.

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

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

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	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.

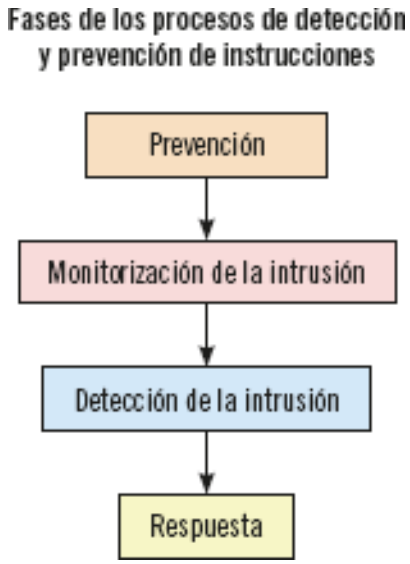
Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

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

El proceso de establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS es crucial para garantizar la efectividad de estos sistemas de detección y prevención de intrusiones.

Fases del Proceso:

- Prevención: Inicialmente, los IDS/IPS intentan prevenir ataques mediante mecanismos que dificultan el acceso de intrusos.
- Monitorización de la Intrusión: Si hay una intrusión o actividad sospechosa, los IDS/IPS detectan y monitorizan el tráfico de datos para análisis posterior.
- Detección de la Intrusión: Tras el análisis, si se confirma una intrusión, se genera una alarma para notificar al administrador.
- Respuesta: Frente a una intrusión confirmada, los IDS/IPS pueden tomar medidas para bloquear el acceso del atacante.



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

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

La inclusión de una base de datos de firmas es esencial para la monitorización y clasificación efectiva de eventos en IDS/IPS, asegurando la detección precisa de actividades sospechosas y intrusiones reales

Después de la implantación, es común enfrentar problemas como falsos positivos y intrusiones no detectadas. Realizar pruebas comparativas ayudará a definir la configuración óptima, adaptándose a las necesidades de seguridad.

A pesar de la verificación inicial del funcionamiento del IDS/IPS, es crucial realizar comprobaciones y actualizaciones periódicas para prevenir la obsolescencia de la base de datos de intrusiones y mantener la efectividad del sistema implantado.

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

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

Aunque la determinación de los niveles adecuados de monitorización, prueba y actualización de los sistemas IDS/IPS varía según las necesidades de cada organización, para evaluar su eficacia se deben considerar las siguientes características:

- Precisión: Es la capacidad del sistema para detectar y distinguir ataques del tráfico normal. Se calcula utilizando los porcentajes de falsos positivos y falsos negativos, buscando un equilibrio entre ambos para una detección precisa.
- Rendimiento: Indica la capacidad del sistema para analizar eventos. Se debe ajustar según la capacidad de procesamiento del equipo y los recursos disponibles, logrando un equilibrio entre el tráfico a analizar y los recursos utilizados.
- Completitud: Se refiere a la capacidad del sistema para detectar todos los tipos de ataques. Aunque es difícil alcanzar la detección total, se busca un equilibrio entre completitud y precisión para maximizar la detección de ataques sin generar falsos positivos.
- Tolerancia a fallos: Es la capacidad del sistema para resistir ataques y fallos del sistema. Un IDS/IPS debe ser sólido y capaz de recuperar la configuración y patrones de detección.
- Tiempo de respuesta: Indica el tiempo que tarda el sistema en reaccionar ante un ataque, generando alarmas o implementando medidas de mitigación. Se debe minimizar para una mayor efectividad.

Estas características son fundamentales para evaluar y optimizar la efectividad de los sistemas IDS/IPS en la protección de la red y los activos de una organización.

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

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

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

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.

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

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.

Resumen

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

Los sistemas de detección y prevención de intrusiones son esenciales para proteger la infraestructura de red de una organización contra posibles ataques.

Antes de su implementación, es crucial realizar un análisis exhaustivo de la infraestructura, servicios, equipos y protocolos utilizados. Además, se deben definir las políticas de respuesta ante intrusiones, distinguiendo entre respuestas pasivas e activas.

Posteriormente, es necesario analizar los eventos registrados por el IDS/IPS, teniendo en cuenta la posibilidad de falsos positivos y falsos negativos. Los registros de auditoría proporcionan información detallada sobre los eventos realizados por los usuarios.

Una vez establecidas las políticas y revisados los registros, los administradores deben realizar pruebas y actualizaciones periódicas para garantizar la eficacia del sistema, evaluando indicadores como rendimiento, completitud, precisión, tolerancia a fallos y tiempo de respuesta. Este enfoque integral asegura una protección continua y efectiva contra las amenazas cibernéticas.