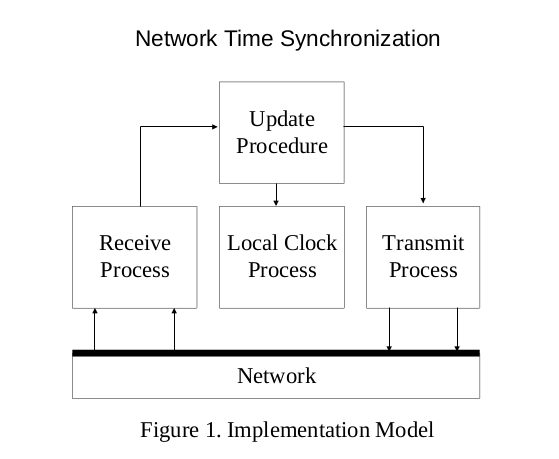
Sistema de gestión de eventos e información de seguridad

* ¿Qué es un NTP?

El Protocolo de tiempo de red (NTP) se utiliza para construir y mantener un conjunto de servidores de tiempo y rutas de transmisión como una subred de sincronización. NTP se basa en el Protocolo de Internet (IP) [DAR81b] y el Datagrama de usuario

Protocolo (UDP) [POS80], que proporciona un mecanismo de transporte sin conexión; sin embargo lo és fácilmente adaptable a otros conjuntos de protocolos. Se desarrolló a partir del Protocolo de tiempo [POS83b] y el Mensaje de marca de tiempo ICMP [DAR81a], pero está específicamente diseñado para mantener la precisión y confiabilidad, incluso cuando se utiliza sobre rutas de Internet típicas que involucran múltiples puertas de enlace y poco confiables redes.



La Figura 1 muestra un modelo de implementación para un host de servidor de tiempo que incluye tres procesos compartidos una base de datos particionada, con una partición dedicada a cada par e interconectada por un sistema mensaje.

* ¿Qué es un SEIM?

Es una forma de software que de forma indirecta integra un sistema de detección y prevención de intrusión IDPS, tiene como objetivo otorgar información útil sobre potenciales amenaza. Esto es posible mediante un análisis de datos, obtenidos desde múltiples sistemas y soluciones de prevención de intrusiones para detectar comportamientos anormales o sospechosos que pueden traducirse en vulnerabilidades.

El software SIEM trabaja con inteligencia procesable para que se pueda gestionar de forma proactiva las potenciales vulnerabilidades, protegiendo a su sistema de devastadoras filtraciones de datos. Empieza por disponer de visibilidad de toda la actividad que se produce en los sistemas permitiendo priorizar, investigar y responder rápidamente.

* ¿Por qué es importante tener un SIEM?

No es un secreto que las amenazas de seguridad aumentan continuamente, y que puede provenir tanto de fuente internas como externas. Una preocupación que crece es la posibilidad de que accidentalmente, se configure erróneamente los ajustes de seguridad, dejando los datos vulnerables a un ataque.

Las desventajas de estos sistemas de protección es que generan tanta información para monitorizar, que los equipos de it se enfrentan al problema de tener que interpretarla en su totalidad para poder reconocer los problemas reales. de hecho, el volumen de datos de seguridad que fluyen a los equipos de seguridad it con poco personal, es más que inútil, a menos que pueda ser rápidamente analizado y filtrado en alertas procesables. Teniendo en cuenta la cantidad de datos que se puede llegar a tener, para las organizaciones ya no es posible hacer este análisis en forma manual. es aquí donde aparece el software SIEM.

Con un SIEM, los profesionales de IT cuentan con un método efectivo para automatizar sus procesos y centralizar la gestión de seguridad de una forma que ayude a simplificar la difícil tarea de proteger información sensible, Un SIEM proporciona a los expertos una venta para comprender la diferencia entre una amenaza de bajo riesgo y una que pueda ser determinante para un negocio.

Todos los informes d e análisis ponen de manifiesto una tendencia clara: las amenazas de seguridad aumentan continuamente, y todas las empresas, independientemente de su tamaño y naturaleza, pueden ser víctimas de estos ataques, que puede provenir tanto de fuentes internas como externas.

Las tecnologías SIEM va a facilitar detectar las amenazas externas, así como aquellas más difíciles de detectar: los ataques internos. Su finalidad es detectar y prevenir amenazas, sean del tipo que sean, y lo hacen gracias a la información que se recopila y unifica en el sistema central.

En esencia, SIEM es un agregador de datos búsqueda y sistema de informes, capaz de recopilar inmensas cantidades de datos de todo el entorno de red, consolidar y hacer que esos datos sean accesibles. Con los datos al alcance de la mano, facilita la investigación de brechas de seguridad. Pero en escencia son una forma de integrar un sistema IDPS.

* ¿Qué es un IDPS?

Los sistemas de detección y prevención IDPS se centran principalmente en identificar posibles incidentes, registrar información sobre ellos, intentar detenerlos e informarlos a los administradores de seguridad. Además, las organizaciones usan IDPS para otros fines, como la identificación de problemas con las políticas de seguridad, los IDPS suelen registrar información relacionada con eventos observados, notificar a los administradores de seguridad de muchos IDPS también pueden responder a una amenaza detectada al intentar que las tecnologías se diferencian principalmente por los tipos de eventos que supervisan y las formas en que se implementan. Esta publicación analiza los siguientes cuatro tipos de tecnologías IDPS:

* Basada en la red, que monitorea el tráfico de red para segmentos o dispositivos de red particulares y analiza la actividad de la red y el protocolo de aplicación para identificar actividad sospechosa
* Inalámbrico, que monitorea el tráfico de red inalámbrica y lo analiza para identificar sospechosos actividad que involucra los propios protocolos de redes inalámbricas.
* Network Behavior Analysis (NBA), que examina el tráfico de red para identificar amenazas que generan flujos de tráfico inusuales, como ataques de denegación de servicio distribuido (DDoS), ciertas formas de malware y violaciones de políticas (por ejemplo, un sistema cliente que proporciona servicios de red a otros sistemas) basados ​​en
* host, que monitorea las características de un solo host y los eventos que ocurren dentro de ese host para detectar actividades sospechosas.

Asegurar los componentes IDPS es muy importante porque los IDPS a menudo son atacados por atacantes que desean administrar, restringiendo el acceso a la red a los componentes IDPS y asegurando la administración de IDPS.

Los cuatro tipos principales de basados en las tecnologías de red de desplazados internos, inalámbrico, basado en host de la NBA, y la integración IDPS directa con más frecuencia cuando una organización utiliza varios productos desplazados de una

por lo general se realiza con software de información de seguridad y gestión de eventos (SIEM), que está diseñado. Antes de evaluar los productos IDPS, las organizaciones deben definir los requisitos que los productos evaluadores necesitan para comprender las características del sistema de la organización y los entornos de red. Los evaluadores también deben definir conjuntos de requisitos especializados para lo siguiente:

* Capacidades de seguridad, incluida la recopilación, registro, detección y prevención de la información
* Rendimiento, que incluye la capacidad máxima y características de rendimiento
* Gestión, incluido el diseño y la implementación (por ejemplo, confiabilidad, interoperabilidad, escalabilidad, producto seguridad), operación y mantenimiento (incluidas actualizaciones de software) y capacitación, documentación y soporte técnico
* Costos del ciclo de vida, tanto iniciales como de mantenimiento.

Los principios de detección y prevención de intrusiones utilizándolos en busca de signos de posibles incidentes, que son violaciones o amenazas inminentes de violación de

Internet, y usuarios autorizados de sistemas que usan indebidamente sus privilegios o intentan obtener permisos adicional. Un sistema de detección de intrusiones (IDS) es un software que automatiza el proceso de detección de intrusos. El sistema de prevención de intrusiones (IPS) es un software que tiene todas las capacidades de un sistema de detección de intrusiones y también puede intentar detener posibles incidentes.

Esta sección proporciona una descripción general de IDS e IPS. Primero explica cómo IDS e IPS. A continuación, describe las funciones clave que realizan las tecnologías IDS e IPS y las tecnologías IPS. Las tecnologías IDS e IPS ofrecen muchas de las mismas capacidades, y los administradores generalmente pueden deshabilitar los sistemas de detección y prevención de intrusiones (IDPS). Los IDPS se centran principalmente en identificar posibles incidentes. Identificar el tráfico de red que viola las políticas de seguridad o uso aceptable de la organización.

incluyendo lo siguiente:

* Identificación de problemas de política de seguridad. Un IDPS puede proporcionar cierto grado de control de calidad para la implementación de la política de seguridad, como la duplicación de los conjuntos de reglas del firewall y las alertas cuando ve tráfico de red que debería haber sido bloqueado por el firewall pero no debido a un error de configuración del firewall.
* Documentar la amenaza existente para una organización. Los IDPS registran información sobre las amenazas que detectan. Comprender la frecuencia y las características de los ataques contra los recursos informáticos de una organización es útil para identificar las medidas de seguridad adecuadas para proteger los recursos. La información también se puede utilizar para educar a la administración sobre las amenazas que enfrenta la organización.
* Disuadir a las personas de violar las políticas de seguridad. Si las personas son conscientes de que sus acciones están siendo monitoreadas por tecnologías IDPS por violaciones a la política de seguridad, es menos probable que cometan tales violaciones debido al riesgo de detección. Metodologías de detección comunes Detección
* basada en firma. Una firma es un patrón que corresponde a una amenaza conocida. La detección basada en firmas es muy efectiva para detectar amenazas conocidas pero en gran medida ineficaz para detectar amenazas previamente desconocidas. Es el método de detección más simple porque solo compara la unidad de actividad actual, como un paquete o una entrada de registro, con una lista de firmas mediante operaciones de comparación de cadenas. Las tecnologías de detección basadas en firmas tienen poca comprensión de que esta limitación impide que los métodos de detección basados ​​en firmas detecten ataques que comprenden múltiples eventos si ninguno de los eventos contiene una indicación clara de un ataque.
* La detección basada en anomalías es el proceso de comparar definiciones de qué actividad se considera normal. Un IDPS que utiliza detección basada en anomalías tiene perfiles que representan el comportamiento normal de usuarios, hosts, conexiones de red o los perfiles se desarrollan mediante el monitoreo de las características. de actividad típica durante un período Por ejemplo, un perfil para una red podría mostrar que la actividad web comprende un promedio del 13% que detecta cuándo la actividad web comprende significativamente más ancho de banda de lo esperado y alerta un correo electrónico, inicia un gran número de conexiones de red y realizar otro comportamiento que sería Un perfil inicial se genera durante un período de tiempo (generalmente días, a veces semanas), a veces llamado Perfiles para la detección basada en anomalías, puede ser estático o dinámico. con el tiempo, las medidas correspondientes de comportamiento normal también cambian; un perfil estático eventualmente
* Los perfiles dinámicos no tienen este problema, la tasa de cambio es lo suficientemente lenta, el IDPS podría pensar que la actividad maliciosa es un comportamiento normal y la actividad maliciosa también podría ser observada por un IDPS mientras construye su actividad maliciosa inicial involuntariamente como parte de un perfil es un problema común con los productos IDPS basados ​​en anomalías basados ​​en anomalías que a menudo producen muchos falsos positivos debido a la actividad benigna que se desvía significativamente de los perfiles, especialmente en Otro problema notable con el uso delbasado en anomalías
* Análisis de protocolo de estadoes proceso de comparar perfiles predeterminados de definiciones generalmente aceptadas de actividad de protocolo benigna para cada estado de protocolo contra eventos observados para identificar 6 A diferencia de la detección basada en anomalías, que utiliza perfiles específicos de host o red, el análisis de protocolo con estado se basa en perfiles universales desarrollados por el proveedor que especifican cómo protocolos particulares El "con estado" en el protocolo con estado El análisis significa que el IDPS es capaz de comprender y rastrear el estado de la red, el transporte y los protocolos de aplicación que tienen una noción Los usuarios no autenticados solo deben ejecutar algunos comandos en este estado, tal estado es emparejar solicitudes con respuestas, por lo que cuando un FTP se produce un intento de autenticación, el IDPS puede autenticarse con éxito, la sesión se encuentra en el estado autenticado y se espera que los usuarios realicen la mayoría de estos comandos mientras que en el estado no autenticado se consideraría sospechoso, pero en el estado autenticado, la mayoría de ellos considerado El análisis de protocolo con estado puede identificar secuencias inesperadas de comandos, como emitir el mismo Otra característica de seguimiento de estado del análisis de protocolo con estado es que para los protocolos que realizan El "análisis de protocolo" realizado por métodos de análisis de protocolo con estado generalmente incluye razonabilidad. modelos, que generalmente se basan primari en el protocolo El principal inconveniente de los métodos de análisis de protocolo con estado es que requieren muchos recursos debido a la complejidad del análisis y la sobrecarga involucrada en la realización del seguimiento de estado para Otro problema grave es que los métodos de análisis de protocolo con estado no pueden