CAPITULO 1. INTRUSIONES

- **Concepto de Intruso**

Un intruso es cualquiera que intente irrumpir o hacer mal uso de un sistema, se asume que para cada caso la palabra intruso tiene diferentes niveles de importancia.

1.2 Tipos de Intrusos

Los intrusos se clasifican principalmente de acuerdo al lugar al que pertenecen en:

Intrusos de Fuera.

La mayoría de las personas piensan que el mundo exterior es la amenaza más grande a su seguridad; debido a que ha sido difundido por los medios de comunicación un miedo hacia los hackers que entran a través de Internet. La realidad, es que los hackers representan una pequeña parte de las amenazas reales a las que se enfrenta una compañía.

Intrusos de Adentro.

Estudios realizados por el FBI han revelado que el 80% de las intrusiones y de los ataques provienen de dentro de las organizaciones. Es muy lógico si se piensa que una persona de adentro conoce el esquema del sistema, donde se encuentran la información valiosa y la localización de puntos y sistemas de seguridad.

Por lo anterior hay que desechar la idea de que la mayoría de las medidas de seguridad deben estar puestas para proteger al interior de un malévolo exterior, ya que realmente gran parte de las intrusiones ocurren desde adentro de las organizaciones. Es necesario un mecanismo que detecte *ambos* tipos de Intrusos, los externos y los internos. Un sistema detector de intrusos efectivo detecta ambos tipos de ataques en un alto grado.

1.3 Políticas de seguridad para evitar intrusiones

Una Política de Seguridad define lo que se permite y lo que se niega en un sistema. Hay dos filosofías básicas detrás de cualquier política de seguridad:

- **Prohibitiva**.− En esta política todo aquello que no esta expresamente permitido es negado
- **Permisible**.− En esta política todo lo que no esta negado expresamente es permitido

Generalmente, un lugar que es más paranoico sobre seguridad toma la primera opción. Se usara una política que detalla exactamente los funcionamientos u operaciones que se permite en un sistema. Cualquier otra operación que no este detalla en éste documento de la política será considerada como ilegal dentro del sistema. Es claro que este tipo de políticas se prestan bien para un ambiente militar, y estos tipos de políticas son raros en establecimientos civiles.

La segunda filosofía está más ligada al espíritu de la informática. Los usuarios de computadoras siempre han intentado usar el potencial de las computadoras al máximo, aun cuando esto signifique violar las reglas. Esto era aceptable con tal de que el trabajo se realizara bien y completo en el tiempo necesario, y nadie resultaba afectado.

Desgraciadamente, esta filosofía no funciona bien en los ámbitos de trabajo actuales. El espíritu competitivo tiende a nublar la ética profesional cuando un usuario se entromete con los archivos de otro usuario. De hecho,

el sabotaje puede ser una norma de conducta en algunos ambientes laborales donde la supervivencia se logra con una competencia extrema.

La mayoría de los usuarios se comportará según un conjunto de reglas "sociales". Estas reglas los animan a respetar la privacidad y el trabajo de los demás. Semejante población de usuarios tiene una alianza de funcionamiento basada en la confianza, y la confianza es fácil subvertir. Una población de usuarios confiables es contaminada fácilmente por un usuario malévolo, que intente emplear mal los sistemas.

1.4 Detección de Intrusiones

Antes de hablar sobre la detección de intrusiones es necesario definir que es una intrusión.

Intrusión.− Es un conjunto de acciones que intenten comprometer la integridad, confidencialidad o disponibilidad de algún recurso. Todas las intrusiones se definen o clasifican a partir de una política de seguridad.

Las intrusiones se clasifican de la siguiente manera:

- **Intrusiones para mal uso**.− son ataques en puntos débiles conocidos de un sistema. Pueden ser detectados observando y buscando ciertas acciones que se realizan a ciertos objetos.
- **Intrusiones anómalas**.− se basa en la observación de desviaciones de los patrones de uso normales del sistema. Pueden ser descubiertos construyendo un perfil del sistema que se desea supervisar, y detectando desviaciones significantes del perfil creado.

Mientras las intrusiones de mal uso sigan patrones bien definidos pueden ser detectadas haciendo un análisis y chequeo en la información de auditoria y reportes del sistema. Por ejemplo, un intento de crear un archivo invalido puede ser descubierto examinando los mensajes en los Logs que son resultado de las llamadas al sistema.

Las intrusiones anómalas son descubiertas observando desviaciones significantes del comportamiento normal del sistema. El modelo clásico para el descubrimiento de la anomalía fue propuesto por Denning. En el se propone la construcción de un modelo que contiene métricas que se derivan del funcionamiento del sistema.

Una métrica se define como: una variable aleatoria x que representa una medida cuantitativa acumulada durante un periodo.

Estas métricas se calculan de los parámetros del sistema disponibles como promedio de carga del CPU, número de conexiones de la red por minuto, número de procesos por usuario y cualquier otro tipo de medida disponible que describa un cierto consumo de recursos en un periodo definido.

Una anomalía puede ser un síntoma de una posible intrusión. Dado un conjunto de métrica que definen el uso normal del sistema, podemos asumir que la explotación de las vulnerabilidades de un sistema involucra el uso anormal del sistema, por consiguiente, ser pueden descubrir violaciones al sistema a partir de patrones anormales del uso del sistema.

El descubrimiento de anomalías también se realiza por medio de otros mecanismos, como redes neuronales, técnicas de clasificación de maquinas que aprenden (machine learning), e incluso sistemas que imitan la inmunidad biológica.

Las intrusiones anómalas son más difíciles de detectar. No hay patrones fijos que puedan ser monitoreados. Idealmente nos gustarían un sistema que combine la capacidad de las personas de localizar patrones y la vigilancia que brinde un programa de computadora. Así siempre se estaría supervisando el sistema para

detectar las intrusiones potenciales, pero podría ignorar las intrusiones falsas, si ellas resultaran ser acciones legítimas de usuarios.

Muchos sistemas de detección intrusiones basan sus operaciones en el análisis de los rastros de accesos al Sistema Operativo. Estos datos forman una huella del uso del sistema en un cierto tiempo. Es una fuente conveniente de datos y es fácilmente disponible en la mayoría de los sistemas. De estas observaciones, los Sistemas de Detección de Intrusiones calcularán métrica sobre el estado total del sistema, y decidirán si está ocurriendo una intrusión.

Un sistema de detección de intrusiones deberá también realizar su propio monitoreo del sistema. Puede ir incrementando las estadísticas que dan el perfil de uso del sistema. Esta estadística se puede derivar de una variedad de fuentes tales como uso de la CPU, entradas y salidas del disco, uso de la memoria, actividades por usuario, número de conexiones hechas, etc. Las estadísticas se debe actualizar continuamente para reflejar el estado actual del sistema. Además se debe correlacionar con un modelo interno que permita que el sistema detector de intrusiones determinen si una serie de acciones constituyen una intrusión potencial.

CAPITULO 2. SISTEMA DE DETECCIÓN DE INTRUSIONES

2.1 Concepto

Los sistemas informáticos se apoyan en los Sistemas de Detección de Intrusiones (IDS −de sus siglas en inglés) para prepararse y ocuparse del mal manejo y del uso indebido de la información de una organización. Logran esta meta, recopilando la información de una gran variedad de fuentes del sistema y de la red y analizando la información que contribuye a los síntomas de los problemas de seguridad de la misma, y permiten que el usuario especifique las respuestas en tiempo real a las violaciones.

Los productos de detección de intrusos son aplicaciones que monitorean activamente los sistemas operativos y el tráfico de red, con el objeto de detectar ataques y violaciones a la seguridad.

Es decir, los IDS son herramientas de seguridad en red que recopilan información de una variedad de fuentes del sistema, analizan la información de los parámetros que reflejan el uso erróneo o la actividad inusual, responden automáticamente a la actividad detectada, y finalmente informan el resultado del proceso de la detección.

- **Objetivos**

Para el buen funcionamiento de los Sistemas de Detección de Intrusiones, es necesario que cumplan con los objetivos que tienen asignados, estos consisten en el cumplimiento de los siguientes puntos:

- Vigilar y analizar la actividad de los usuarios y del sistema.
- Revisar las configuraciones del sistema y de las vulnerabilidades.
- Evaluar la integridad de los archivos críticos del sistema y de los datos.
- Reconocimiento de los modelos de la actividad que reflejan ataques conocidos.
- Análisis estadístico para los modelos anormales de la actividad.
- Gerencia del rastro de intervención del sistema operativo, con el reconocimiento de las violaciones de la actividad del usuario respecto a la política establecida.
- Vigilar el cumplimiento de políticas y procedimientos establecidos dentro de la organización.

La combinación de estas características hace que sea más fácil para los encargados del sistema, vigilar la intervención y la evaluación de sus sistemas y redes. Esta actividad en curso de la intervención y de la evaluación, es una práctica necesaria de una sana gerencia de seguridad.

- **Tipos**

Es importante mencionar antes de describir el funcionamiento de un IDS, los tipos más comunes de estos sistemas en el mercado actual.

La meta de un IDS es proporcionar una indicación de un potencial o de un ataque verdadero. Un ataque o una intrusión es un acontecimiento transitorio, mientras que una vulnerabilidad representa una exposición, que lleva el potencial para un ataque o una intrusión. La diferencia entre un ataque y una vulnerabilidad, entonces, es que un ataque existe en un momento determinado, mientras que una vulnerabilidad existe independientemente de la época de la observación. Otra manera de pensar en esto es que un ataque es una tentativa de explotar una vulnerabilidad (o en algunos casos, una vulnerabilidad percibida). Esto nos conduce a categorizar varios tipos de IDS.

Hay cinco diversas categorías de las identificaciones. No todas estas categorías representan la "detección clásica de la intrusión" pero desempeñan un papel en la meta total de intrusiones de detección o de prevención en una red corporativa. Las categorías son:

- IDS Network−based
- IDS Host−based
- IDS Híbridos
- Inspector de la Integridad del Archivo
- Explorador de la vulnerabilidad de la Red
- Explorador de la vulnerabilidad del Host

Los tres primeros puntos son tipos de IDS y los tres puntos restantes son herramientas de detección de vulnerabilidad.

Una intrusión, explota una vulnerabilidad específica y debe ser detectada cuanto antes, después de que comience. Por esta razón, las herramientas de la detección de la intrusión deben de ejecutarse con más frecuencia que los exploradores de vulnerabilidad. Los sistemas de la detección de la intrusión (IDS) examinan el sistema o la actividad de la red para encontrar intrusiones o ataques posibles.

Como mencionamos anteriormente, hay dos tipos básicos de sensores de IDS: *network−based* y *host−based.* Los sensores network−based se encargan de monitorear las conexiones de red, observar el tráfico de paquetes TCP, y así poder determinar cuando se está realizando un ataque. Los sensores host−based se ejecutan en los sistemas −servidores, workstations o en las máquinas de usuarios − y localizan alguna actividad sospechosa en el nivel del sistema. Buscan las cosas que pueden indicar actividad sospechosa, tal como tentativas de conexión fallidas. Los encargados de los IDS actúan como un centro centralizado de vigilancia, recibiendo datos de los sensores y accionando alarmas.

IDS basados en Red

Los sistemas network−based actúan como estupendos detectores, es decir, ellos observan el tráfico en las capas del TCP/IP y buscan modelos conocidos de ataque, como los que generalmente realizan los hakers o los ataques al web server. Tales sistemas hacen frente a desafíos significativos, especialmente en los ambientes cambiantes donde los detectores no ven todo el tráfico en la red. Además, la mayoría de los sistemas network−based pueden buscar solamente los modelos de abuso que se asemejan al estilo de los ataques de los hackers, y esos perfiles están cambiando constantemente. Los sistemas network−based son también propensos a los positivos falsos. Por ejemplo, si el web server tiene sobrecarga de trabajo y no puede manejar todas las peticiones de conexión, los IDS quizá pueden detectar que el sistema está bajo un ataque, aunque en realidad, no lo sea. Típicamente, un sistema basado en red no va a buscar la otra actividad sospechosa, tal como que alguien de su entorno de trabajo, intente tener acceso a los datos financieros de su compañía. Por supuesto, los

detectores de la red se pueden adaptar para buscar apenas sobre cualquier tipo de ataque, pero es un proceso laborioso. Los sistemas network−based son los más comunes, y examinan el paso del tráfico de la red para las muestras de la intrusión.

Los sistemas basados en red son un poco diferentes: se diseñan empleando una arquitectura de consola−sensor y suelen ser totalmente pasivos. Este tipo de detección integrada a la red "husmea" el cable y compara los patrones de tráfico, en vivo, con listas internas de "rúbricas" de ataque.

IDS basados en Host

Los sistemas host−based emplean un diverso procedimiento para buscar a los malos individuos. No característico de los detectores, los sistemas host−based dependen generalmente de los registros del sistema operativo para detectar acontecimientos, y no pueden considerar ataques a la capa de red mientras que ocurren. En comparación con los IDS basados en red, estos sistemas obligan a definir lo que se considera como actividades ilícitas, y a traducir la política de la seguridad a reglas del IDS. Los IDS host−based se pueden también configurar para buscar tipos específicos de ataques mientras que no hace caso de otros. Pero otra vez, el proceso de templar un sensor puede ser desperdiciador de tiempo. Es decir, los sistemas host−based observan al usuario y la actividad del proceso en la máquina local para las muestras de la intrusión.

Los sistemas relacionados al host se despliegan de la misma forma que los escáners antivirus o las soluciones de administración de red: se instala algún tipo de agente en todos los servidores y se usa una consola de gestión para generar informes.

Ambas formas de detección pueden reaccionar cuando identifican un ataque. Los dos enfoques tienen puntos fuertes y débiles. Los sistemas basados en red casi no se hacen notar y son independientes de la plataforma; se pueden desplegar con poco o ningún impacto sobre las redes de producción. Sin embargo, estos sistemas tienen que superar varios obstáculos importantes. Por ejemplo, la tecnología se basa en la capacidad del sensor para ver todo el tráfico de red. En un entorno conmutado, esta situación complica demasiado la vida, ya que es preciso utilizar espejos de puertos. Pocos sistemas basados en red pueden manejar una línea de 100 Mbps saturada, y ya no hablemos de velocidades de gigabits.

Los sistemas basados en host no tienen problemas de ancho de banda; no obstante sólo pueden reconocer ataques contra máquinas que están ejecutando sus agentes. Si la compañía tiene servidores que usan un sistema operativo no reconocido, el administrador no habrá ganado nada. Sin embargo, las soluciones que operan en host ofrecen algunos servicios adicionales, más allá de los que ofrecen los sistemas basados en red, como verificación de integridad binaria, análisis sintáctico de logs y terminación de procesos no válidos.

IDSs Híbridos

Los vendedores han observando las limitaciones que presentan los IDS network−based y los IDS host−based, y han concluido en combinar ambos sistemas para mejorar su capacidades. Estos sistemas híbridos combinan las mejores características de ambos en una configuración del sensor del IDS. RealSecure de Internet Security Systems (ISS), CyberCop de Network Associates (NAI) y CMDS de ODS son ejemplos de soluciones que han adoptado este acercamiento híbrido de IDS.

RealSecure, por ejemplo, originalmente se basaba en un sensor network−based, pero ahora tiene detección host−based de la intrusión también. CyberCop ofrece actualmente solamente las IDS host−based, pero se está moviendo hacia una nueva configuración de la " fusión " que incorpore detectores de red IDS host−based. Y CMDS trabaja con la red y la información de IDS host−based para buscar ataques.

- **Características**

Las características de un buen IDS deben tratar las siguientes cuestiones, sin importar en que mecanismo se basen:

- Debe ejecutarse continuamente sin la supervisión humana. El sistema debe ser bastante confiable y permitir que se ejecute en el fondo del sistema que es observado. Sin embargo, no debe ser un "rectángulo negro". Es decir, sus funcionamientos internos deben ser observables desde el exterior.
- Debe ser tolerante a fallos, en el sentido de que debe mantenerse ante un fallo del sistema, además no debe de poder reiniciar el sistema.
- Debe resistir el cambio. El sistema puede vigilarse para asegurarse de que no ha sido alterado.
- Debe imponer los gastos mínimos para el sistema.
- Debe observar desviaciones del comportamiento normal.
- Debe ser adaptado fácilmente al sistema en cuestión. Cada sistema tiene un diverso modelo de uso, y el mecanismo de la defensa debe adaptarse fácilmente a estos modelos.
- Debe hacer frente a comportamiento del sistema que cambia en un cierto periodo de tiempo, mientras que se están agregando las nuevas aplicaciones. El perfil del sistema cambiará en un cierto plazo, y el IDS debe poder adaptarse.
- Finalmente, debe ser difícil engañar.

Algunos sistemas proporcionan ciertas características adicionales, incluyendo:

- La instalación automática de correcciones lógicas al software.
- Instalación y operación de los servidores que registran la información de intrusos.

Los tipos de errores que probablemente puedan ocurrir en el sistema, se pueden categorizar cuidadosamente como:

- Positivo falso
- Negativa falsa,
- Errores de cambio.

Un positivo falso ocurre cuando el sistema clasifica una acción como anómala (una intrusión posible) cuando es una acción legítima. Una negativa falsa ocurre cuando ha ocurrido una acción intrusa real pero el sistema permite que pase como no intruso. Un error de cambio, ocurre cuando un intruso modifica la operación del detector de la intrusión para forzar a que ocurran negativas falsas. Los errores positivos falsos conducirán a los usuario del IDS a no hacer caso de su salida, pues clasificará acciones legítimas como intrusiones. Las ocurrencias de este tipo de error se deben reducir al mínimo (puede no ser posible eliminarlas totalmente), para proporcionar la información útil a los operadores. Si muchos positivos falsos se generan también, los operadores vendrán no hacer caso de la salida del sistema en un cierto plazo, que puede conducir a una intrusión real que es detectada pero no hecha caso por los usuarios.

Un error negativo falso ocurre cuando procede una acción aunque es una intrusión. Los errores negativos falsos son más serios que errores positivos falsos porque dan un sentido engañoso de la seguridad. Permitiendo que todas las acciones procedan, una acción sospechosa no será traída a la atención del operador. El IDS ahora es un defecto, pues la seguridad del sistema es menor que la que era antes de que el IDS fuera instalado. Los errores de cambio son más complejos Un intruso podría utilizar conocimientos sobre los mecanismos internos de un IDS para alterar su operación, permitiendo posiblemente que el comportamiento anómalo proceda. El intruso podría entonces violar los apremios operacionales de la seguridad del sistema. Esto se puede descubrir por un operador humano que examina los registros del detector de la intrusión, pero parecería que el IDS todavía trabaja correctamente.

El uso del término "detección de intrusos" está proliferando en todos lados. Los medios de comunicación y la gente de mercadotecnia utilizan la frase a diestra y siniestra. A cualquier tipo de herramienta se le describe

como sistema de detección de intrusos, desde analizadores de logs de web hasta productos de administración de activos.

Los sistemas de detección de intrusos pueden ayudar a los administradores a mantener vigilados los sistemas y las redes, estos productos pueden, en tiempo real, percatarse de cuándo está ocurriendo un ataque. Esto ofrece al administrador la oportunidad de reaccionar ante las agresiones o incluso marcarles el alto −lo cual es mucho mejor que recibir a las cuatro de la mañana una llamada telefónica de alguien que dice que el sitio web se ve un poco diferente−−. En muchos casos, el costo de un sistema de detección de intrusos se puede justificar tan sólo por su valor "forense". Si un sistema fue violado y sus logs están contaminadas, este tipo de sistemas pueden ahorrar a los administradores los días que llevaría averiguar qué pasó exactamente.

Los sistemas de detección de intrusos son excelentes adiciones al arsenal de seguridad; sin embargo, no son el factor que permitirá ganar la guerra. Si una compañía posee redes de alta disponibilidad o muy expuestas, la tecnología podría resultar muy valiosa. No obstante, si la empresa todavía está batallando con políticas, procedimientos y bloqueos de hosts, será necesario dejar para después la detección de intrusos y ocuparse primero de lo básico.

- **Ventajas y Desventajas**

Cada nuevo mercado sufre de la exageración y de la idea falsa, algunas de las demandas hechas en materia de comercialización son razonables y otras son engañosas. Los Sistemas de Detección de Intrusiones, tienen sus ciertas ventajas y desventajas, mismas que se analizan en los siguientes párrafos.

Ventajas

- Pueden prestar un mayor grado de integridad al resto de su infraestructura de seguridad. Los IDS proporcionan capas adicionales de protección a un sistema asegurado. La estrategia de un atacante del sistema incluirá a menudo los dispositivos de seguridad que atacan, que anulan o que protegen. Los IDS la intrusión pueden reconocer estos primeros sellos de ataque, y potencialmente responden a ellos, atenuando daños Además, cuando estos dispositivos fallan, debido a la configuración, al ataque, o al error del usuario, los IDS puede reconocer el problema y notificar a la gente adecuada.
- Los encargados del sistema, pueden tener fuentes de información a menudo obtusas del sistema, diciéndole lo qué realmente está sucediendo en sus sistemas. Los rastros de intervención del sistema operativo y otros registros de sistemas son información clave sobre lo que se está intentando realizar sobre sus sistemas. Son también a menudo incomprensibles. Los IDS permiten que los administradores y los encargados templen, que ordenen, y que comprendan lo que les dicen estas fuentes de información, a menudo revelando problemas antes de que ocurra la pérdida
- Pueden rastrear la actividad del usuario de la punta de entrada a la punta de salida o del impacto. En el acontecimiento inverosímil que un intruso consigue más allá de un dispositivo de la defensa del perímetro, tal como un firewall, las identificaciones proporcionan una manera de coger sus acciones. Además, las identificaciones pueden detectar las acciones de un "mal individuo " ya dentro, un ataque ya iniciado o un camino previamente desconocido de la entrada a la red.
- Pueden reconocer y señalar alteraciones a los archivos críticos del sistema y de datos. Las herramientas de integridad del archivo utilizan sumas de comprobación criptográficas fuertes por bloques, y en el caso de un problema, comprobar rápidamente el fragmento del daño.
- Pueden manchar los errores de su configuración de sistema que tienen implicaciones de la seguridad, corrigiéndolas a veces si el usuario desea. Los productos de revisión de vulnerabilidad permiten la revisión y la diagnosis constantes de las configuraciones del sistema que pudieron causar problemas de la seguridad.
- Pueden reconocer cuando su sistema parece ser vulnerable a los ataques determinados. Los productos de detección de vulnerabilidad también permiten que el administrador de un sistema se determine rápidamente lo que deben ser los ataques de preocupación.

La gran ventaja de utilizar productos de detección de intrusos es que proporcionan a los administradores una visión en tiempo real de lo que realmente está ocurriendo en la red. Sin monitoreo activo, muchos sitios están volando a ciegas. Pocas personas revisan sus logs de sistema y quienes lo hacen casi nunca las examinan en tiempo real. Peor aún, muy pocas organizaciones han instalado mecanismos de loggins seguros; si un host es violado en el nivel de raíz o de administrador, está a merced de las técnicas de borrado de logs. La consecuencia es una serie de posibles pesadillas, sin tener idea de cómo entraron los intrusos, qué hicieron ni qué tan lejos llegaron.

Desventajas

- La seguridad es un área compleja con posibilidades y dificultades innumerables. No hay soluciones mágicas a los problemas de la seguridad de la red, y los productos de la detección de la intrusión no son ninguna anomalía a esta regla. Sin embargo, como parte de una gerencia comprensiva de la seguridad saben desempeñar un papel vital en la protección de sus sistemas.
- No pueden compensar para los mecanismos débiles de la identificación y de la autentificación. Una infraestructura de la seguridad que incluye la detección fuerte de I&A y de la intrusión es más fuerte de una que contiene solamente uno o la otra.
- No pueden conducir investigaciones de ataques sin la intervención humana. Uno debe realizar la dirección del incidente. Uno debe investigar los ataques, determinarse, en lo posible, el partido responsable, después diagnosticar y corregir la vulnerabilidad que permitió que ocurriera el problema, señalando el ataque y los detalles a las autoridades donde se requiera.
- No pueden intuir el contenido de la política organizacional de la seguridad. Los sistemas expertos de la detección de la intrusión aumentan de valor cuando se permiten funcionar como alarmas de hacker.
- No pueden compensar para los problemas en la calidad o integridad de la información que el sistema proporciona. Es decir la " basura es basura " todavía se aplica.
- No pueden analizar todo el tráfico en una red ocupada. La detección network−based de la intrusión es capaz de vigilar tráfico de una red, pero solamente a una punta.
- No pueden ocuparse siempre de los problemas que implican ataques del nivel de paquete. Hay debilidades en sistemas la detección de la intrusión de la red. El corazón de las vulnerabilidades implica la diferencia entre la interpretación de IDS's del resultado de una transacción de la red (basada en su reconstrucción de la sesión de la red) y del nodo de destinación para la dirección real de esa sesión de la red de la transacción. Por lo tanto, un adversario bien informado puede enviar la serie de paquetes hechos fragmentos y de otra manera cuidados que eludan la detección, pero lanza ataques contra el nodo de destinación. Peor todavía, un adversario puede utilizar esta clase de manipulación del paquete para lograr una negación del ataque del servicio contra las identificaciones sí mismo por la memoria que desborda afectada un aparato para las coletas entrantes del paquete.

2.6 IDS y Firewalls

Una idea errónea pero generalizada acerca de los firewalls, es que garantizan la protección de una red. Aunque es indudable que esta tecnología es necesaria, por sí sola no determina que la red sea segura. Un firewall no posee poderes místicos; deja entrar algunos paquetes y bloquea el paso de otros. Lo que hay que recordar es que tan pronto como se dejan entrar algunos paquetes, aunque éstos hayan atravesado un firewall, la red de la empresa está en riesgo. Por tal motivo, es crucial contar con expertos que entiendan qué paquetes hay que dejar entrar y cómo minimizar los riesgos que implica el permitirles el acceso. Dado que el firewall está situado en un punto muy estratégico de la red, no es sorprendente que los fabricantes añadan otros servicios. Varios firewalls incluyen funciones de autenticación, capacidades VPN, filtrado de URL, escaneo de virus e incluso integración con sistemas de detección de intrusos.

Axent Technologies, Check Point y Cisco se cuentan entre los fabricantes que han integrado software para detección de intrusos en los firewalls, el cual activa automáticamente filtros si el software cree haber detectado un ente extraño.

La funcionalidad básica del firewall, que se concentra en filtrar paquetes con base en aplicaciones y direcciones IP; casi todos los productos cumplen su promesa. El problema radica en decidir qué servicios se deben ejecutar en el hardware de firewall, además del filtrado básico de paquetes. La tentación de añadir soluciones debe moderarse, en la inteligencia de que la ejecución de más programas podría hacer lento o desestabilizar al firewall.

Por último, tenga presente que un firewall no se puede descartar que los paquetes que el firewall deja entrar en la red formen parte de un ataque.

Una pregunta común es cómo la detección de la intrusión complementa firewalls. Una forma de caracterizar la diferencia es proporcionada clasificando la violación de la seguridad por fuente −− si vienen fuera de la red de la organización o de dentro. Acto de los firewalls re como barrera entre las redes (internas) corporativas y el mundo exterior (Internet), y tráfico entrante del filtro según una política de la seguridad.

Esto es una función valiosa y sería suficiente protección era él no para estos hechos:

- No todo el acceso de Internet ocurre a través del firewall

Los usuarios por diversas circunstancias instalaron en ocasiones conexiones desautorizadas del módem entre sus sistemas conectados con la red interna y los abastecedores de acceso de Internet del exterior u otras proveedoras de Internet. El firewall no puede atenuar el riesgo asociado a las conexiones que nunca considera.

- No toda la amenaza se origina fuera del firewall.

Hay ocasiones que se ha detectado que los problemas se originan dentro de la organización Una vez más el firewall ve solamente tráfico en los límites entre la red interna y el Internet. Si la seguridad de reflejo del tráfico nunca práctica una abertura flujos más allá del firewall, no puede considerar los problemas.

Actualmente más organizaciones utilizan la encripción para proteger sus archivos y las conexiones públicas de la red, el punto importante será proteger aquella información que no este protegida dentro de la red interna. Es aquí donde la detección de intrusiones toma parte ya que solo se ocupa del tráfico en la red interna.

Por lo tanto, llegarán a ser aún más importantes como las infraestructuras de la seguridad se desarrollan.

- Los firewalls están conforme a ataque ellos mismos

Una estrategia común del ataque es utilizar un túnel para desviar protecciones del firewall. El hacer un túnel es la práctica de encapsular un mensaje en un interior del protocolo (que se pudo bloquear por los filtros del firewall) un segundo mensaje.

CAPITULO 3. VULNERABILIDAD

3.1 Concepto de Vulnerabilidad

Los paquetes de vulnerabilidad (también conocidos como escáners de seguridad) adoptan un enfoque proactivo respecto a la seguridad de redes y procuran identificar de forma eficiente, exhaustiva y automatizada huecos en la seguridad, tanto en el nivel de host como en las redes. Muchos de los puntos de vulnerabilidad son específicos en el Sistema Operativo.

Además de que realizan rigurosas tareas de sistemas en orden, para determinar el lado débil que a fuerzas permite la violación de la seguridad, estos productos usan estrategias para realizar tareas:

El primero: ***pasivo***; es un mecanismo basado en el host; el cual inspecciona la configuración del archivo del sistema para la instalación discreta de la clave del sistema de archivo y para uso del mismo, y otro sistema de objetos para la violación de la política de la seguridad. Estas señales son seguidas en más casos ***por activos***; es la evaluación basada en la red, la cual reactúa en la instrusión común del texto, anotando la respuesta del texto para el sistema.

Los resultados de evaluación de vulnerabilidad de las herramientas representan una seguridad instantánea del sistema para un punto a tiempo. Aunque estos sistemas no pueden detectar confiablemente un ataque en progreso, sólo pueden determinar que ataque es el que ha ocurrido.

3.2 Objetivos

Los productos para la evaluación de la vulnerabilidad (conocidos como escáners) son herramientas de administración de seguridad que:

- Comprueban la conducta exhaustiva de un sistema que procura localizar las tareas para la seguridad de la vulnerabilidad.
- Reporta el número, natural y la rigidez de esas tareas.
- Permite al sistema administrador determinar el estatus de seguridad de un sistema para un tiempo particular.
- Permite a los auditores de seguridad determinar la eficacia de un sistema de organización en la seguridad de la administración.
- En algunos casos, algunas veces suceden incidentes y permite a los investigadores determinar la ruta de entrada para un atacante o intruso.

3.3 Ventajas y Desventajas

Ventajas

- Las herramientas de vulnerabilidad pueden ser utilizadas para probar la red y nos permite hallar la debilidad de la red, incluso los agujeros que aparecen constantemente en las redes.
- Tiene la capacidad de identificar una gran variedad de agujeros en la seguridad y configuraciones erróneas.
- Son parecidos a los escáners antivirus en cuanto a que utilizan bases de datos internos, que incluyen un listado de defectos conocidos (para determinar sí un sistema es vulnerable o no a un tipo de ataque específico).
- Si los fabricantes de tecnología de seguridad tienen conocimientos nuevos del agujero, se codifican verificaciones, se integran a la siguiente versión y ésta es distribuida.
- La persona que hace uso de la evaluación de la herramienta, podrá obtener el uso adecuado de ella, así mismo como poder tomar decisiones en cuanto a la compra (claro que hay que considerarse que tipo de licencias es con las que cuenta la empresa).

Desventajas

- Se debe evitar anunciar los Sistemas Operativos de sus servidores; ejemplos como: las extensiones de archivos.asp, uso de .htm en lugar de html y página principales llamadas default.htm, las cuales ayudan a atacante a identificar el servidor, además de que el atacante al determinar el Sistema Operativo sólo necesita de la dirección IP del servidor.
- No puede realizar una prueba de vulnerabilidad una sola vez, ya que es necesario utilizar una herramienta frecuentemente con una base de datos actualizada de los puntos vulnerables del Sistema Operativo.
- En NT la debilidad aparece todo el tiempo.
- Los atacantes pueden usar las herramientas para probar donde existen debilidades en la red.
- No es una tarea sencilla el estar dedicándole tanto tiempo a investigar agujeros en la seguridad, sino se

cuentan a la mano con versiones actualizadas de las herramientas de escáneo.
- Si el atacante esta al tanto de las actualizaciones de los sistemas, tienen mayor probabilidad de tener éxito si usa los métodos más recientes.
- Si los administadores no se mantienen al día de los parches o hotfix pueden convertirse en víctimas seguras y aún más, si no tiene conocimiento del agujero.

3.4 Evaluaciones para el Host

Este tipo de aplicación usa pasivo; ejecuta el estudio de la clave como parte del análisis de la evaluación de la clave, la cual consiste en correr el password contra el password del archivo, utilizando un buen conocimiento de ataque en orden para rápidamente localizar el franco no existente o de otra manera la subida del password.

Ventajas

- Rendimiento exacto ,del host específico del agujero de seguridad.
- Contiene agujeros de seguridad que no son expuestos durante la evaluación de la red.

Desventajas

- La estimación de métodos son plataformas específicas y así se requiere de la configuración precisa para cada tipo de host usado por la organización.
- Desplegar y poner al día muchas veces si se requiere, mucho más esfuerzo que en la evaluación de la red.

3.5 Evaluaciones para la red

La vulnerabilidad de la evaluación de la red, usa activo; las cuales son técnicas para determinar si se ha dado un sistema vulnerable para un determinado ataque. En red la valuación se basa, como variedad de escenarios de ataques que son conectados contra la tarjeta del sistema, y sus resultados son analizados en orden para determinar la vulnerabilidad del sistema para ataque. En algunos casos la evaluación de la red, es usada para explorar los problemas de la red en específico.

Ventajas

- Hallar agujeros de seguridad sobre una variedad de plataformas y sistemas
- Porque no es una plataforma independiente como el host, ya que este último es fácil de desplegar rápidamente.
- Que no asume el nivel de acceso del host, este es fácil para desplegar un punto político de vista.

Desventajas

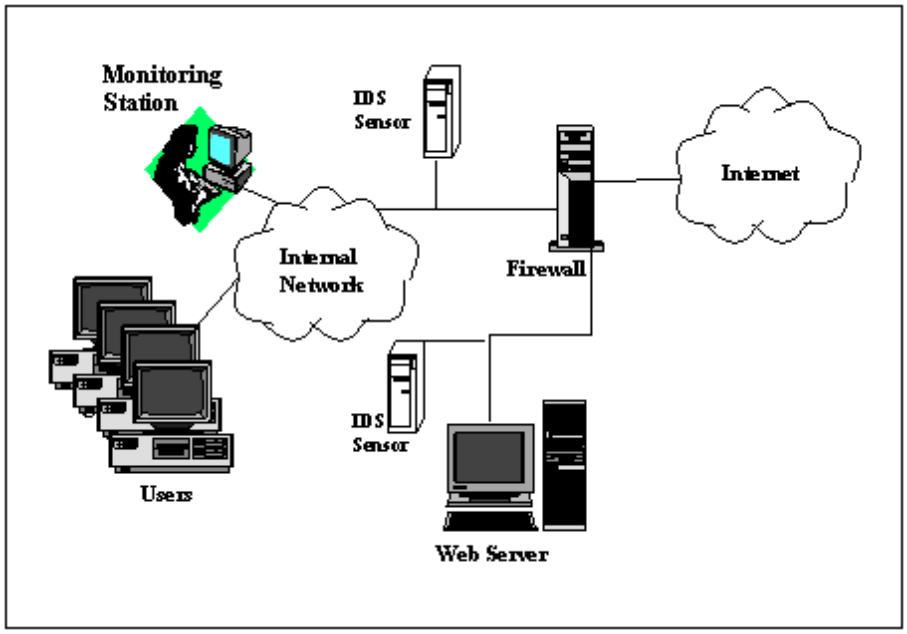
- Que no considera la plataforma específica de vulnerabilidad, este a menudo es menos exacto que la evaluación del host.
- Puede afectar las operaciones y ejecución de la red.

CAPITULO 4. FUNCIONAMIENTO DE IDS

4.1 Red IDS

Usualmente una red IDS tiene dos componentes lógicos: el sensor y la estación administradora. El sensor radica en un segmento de red, y los monitores para detectar tráfico sospechoso. La estación administradora recibe alarmas de los sensores y las muestra al operador.

Los sensores usualmente son sistemas dedicados que existen solo para monitorear la red. Estos tienen una interfase de red que recibe todo el tráfico no solo aquel destinado para su dirección IP, además capturan y analizan todo el tráfico que fluye en la red. Si detectan algo que parezca inusual lo envían a una estación de análisis.



La estación de análisis puede mostrar las alarmas o hacer un análisis adicional. Algunas de las alarmas que se muestran son simplemente una interfase a una herramienta administradora de la red, como HP OpenView, pero algunas son GUI's (interfaces gráficas de usuario) diseñadas para ayudar al operador a analizar el problema.

Este diagrama muestra esquema de una red tradicional basada en IDS con dos sensores sobre segmentos de redes separados que comunican con una estación que monitorean la red interna.

Ventajas

El IDS puede detectar algunos de los ataques a la red. Es buena para detectar accesos sin autoridad o algunos tipos de accesos con exceso de autoridad.

Un IDS basado en red no requiere modificación o un servidor de producción. Esta es una ventaja porque frecuentemente los servidores de producción de servicios tienen tolerancia a las operaciones cercanas al CPU, I/O, y capacidad de disco, instalando software adicional podría exceder la capacidad del sistema.

El IDS no es una trayectoria critica para ninguna producción de servicios o procesos porque una red basada en IDS no actúa como una ruta o un dispositivo critico. Sistemas fracasados no tienen un significativo impactante en los negocios. El lado benéfico de esto es que será probable que usted encuentre menos resistencia de otras personas dentro de su organización el riesgo que existe con procesos críticos es bajo con un sistema de red que con un servidor.

Las redes basadas en sistemas IDS tienden a ser más auto contenidas que un sistema basado en servidor. Ellas corren sobre un sistema dedicado que es sencillo de instalar; hace algunas configuraciones, y conecta esta dentro de su red en una locación que permite monitorear sensitivamente él trafico.

Desventajas

Por otra parte en una red IDS el sensor solo examina el tráfico del segmento al que esta conectado directamente, pero no puede detectar en ataque que viaje a través de un diferente segmento de red.

Este problema es particularmente endémico en un ambiente ethernet switchado. El problema puede requerir que una organización compre muchos sensores para llegar a todos los puntos de la red que desee cubrir. Dado que los sensores cuestan dinero, la amplia cobertura de una red IDS con sensores, puede resultar extremadamente caro.

Los sistemas de detección de intrusiones de una red tienden a usar análisis de firmas para conocer los requerimientos de desempeño. Esto detectará ataques programados comunes provenientes de fuentes externas, pero es inadecuado para detectar amenazas con información más complejas. Esto requiere una habilidad más robusta para examinar el entorno.

Un sistema de detección de intrusiones de una red puede tener la necesidad de comunicar largos volúmenes de datos de regreso al sistema central de análisis. A veces esto significa que cualquier paquete monitoreado genera una gran cantidad de tráfico de análisis. Muchos de estos sistemas usan procesos agresivos de reducción de datos, para reducir la cantidad de tráfico de comunicación. Ellos también hacen mucho uso de los procesos de toma de decisiones, afuera en el sensor mismo y usan la estación central para desplegar las condiciones, en lugar de usarlo para el análisis actual. La desventaja de esto es que provee muy poca coordinación entre los sensores. Cualquier sensor dado, ignora que otro ha detectado un ataque. Tales sistemas no pueden detectar normalmente ataques sinérgicos o complejos.

Una red basada en IDS puede enfrentar tiempos difíciles manejando ataques dentro de sesiones de encriptado. Afortunadamente, hay muy pocos ataques que toman lugar dentro de sesiones de tráfico encriptadas, que atacan en contra de servidores web débiles.

4.2 Servidor IDS

Los IDS basados en el servidor, buscan señales de intrusión en el sistema local del servidor. Estos frecuentemente usan los sistemas de intervención del servidor y sus mecanismos de acceso como fuente de información para el análisis.

Ellos buscan actividad inusual limitada al servidor local, tal como accesos, acceso incorrecto a archivos, escalación de privilegios del sistema. Esta arquitectura de IDS generalmente usa motores basados en reglas para el análisis d las actividades; un ejemplo de tales reglas podría ser, privilegio de super usuario sólo puede ser conseguido a través del comando su. Por lo tanto los intentos sucesivos de acceso a la cuenta raíz serán considerados un ataque.

Ventajas

Un IDS basado en el servidor puede ser una herramienta extremadamente poderosa para analizar un posible ataque. Por ejemplo, a veces puede decir exactamente que hizo el atacante, qué comandos ejecutó, que archivos abrió, y que sistemas que llamó fueron ejecutados, en lugar de solo una vaga acusación de que el atacante intentó ejecutar un comando peligroso. Un IDS basado en el servidor usualmente provee mucha más detallada y relevante información que los IDS basados en la red.

Los sistemas basados en el servidor tienden a registrar índices más bajos de falsas alarmas que los sistemas basados en red. Esto pasa porque el rango de comandos ejecutados en un servidor especifico es mucho más específicos que los tipos de tráfico. Fluyendo a través de la red. Esta propiedad puede reducir la complejidad de los motores de análisis basados en el servidor.

Los sistemas basados en el servidor pueden ser usados en entornos donde una amplia detección de intrusiones

no es necesaria, o donde el ancho de banda no esta disponible para comunicaciones sensor−análisis. Los sistemas basados en el servidor pueden estar completamente auto contenidos. Esto también permite correr a los sistemas basados en el servidor en algunos casos, desde medios de solo lectura; esto previene los ataques para deshabilitar al IDS.

Finalmente, un sistema basado en el servidor, puede ser menos riesgoso configurado con respuesta activa, tal como terminación de un servicio o desconectar a un usuario ofensivo. Un sistema basado en el servidor es más difícil de engañar restringiendo el acceso desde fuentes legitimas.

Desventajas

Los sistemas basados en el servidor requieren instalación en los dispositivos particulares que se desee proteger. Si, por ejemplo, se tiene un servidor de recursos humanos, y se quiere protegerlo, se tendrá que instalar el IDS en ese servidor. Como se mencionó antes esto puede ocasionar problemas de capacidad. En algunos casos, esto puede hasta representar problemas de seguridad, dado que el personal de seguridad puede no tener ordinariamente acceso al servidor en cuestión.

Otro problema asociado con los sistemas basados en el servidor es que tienden a detenerse sobre los accesos innatos y las capacidades de monitoreo del servidor. Si el servidor no esta configurado para dar accesos adecuados y monitorear, se tiene que cambiar posiblemente la configuración de una máquina de producción, lo cual representa un tremendo problema de cambios administrativos.

Los sistemas basados en el servidor son relativamente caros. Muchas organizaciones no tienen los recursos financieros para proteger todos los segmentos de red usando sistemas basados en el servidor. Estas organizaciones deben elegir muy cuidadosamente el sistema para protegerse. Esto puede dejar amplias brechas en la cobertura ID, porque, por ejemplo, un atacante en un sistema vecino no protegido puede rastrear información auténtica u otro material sensible para nuestra red.

Finalmente, los sistemas basados en el servidor padecen en gran grado, de restricciones en su visión local. Ellos ignoran casi en su totalidad el entorno de la red. Así, el tiempo de análisis requerido para evaluar dalos de una intrusión potencial aumente linealmente con el número de servidores protegidos.

4.3 Verificador de Integridad de Archivos

Un verificador de integridad de archivos examina los archivos en una computadora para determinar cuál de ellos ha sido alterado desde la última vez que se le verificó. Los verificadores de integridad guardan una base de datos de valores aleatorios para cada archivo. Cada vez que se corre el verificador, recalcula los valores y los compara con los guardados en la base de datos. Si los valores son diferentes, quieres decir que el archivo ha cambiado.

Una función de aleatorización, es un proceso matemático para reducir la secuencia de bytes en un archivo, a un número de longitud fijado. El mismo archivo siempre producirá el mismo valor aleatorio y cualquier cambio en el archivo produce un valor diferente. A diferencia de la encripción una aleatorización es una función con un solo camino; no se puede producir el archivo original a partir del valor aleatorio.

Algunas aleatorizaciones son más seguras que otras. Muchas aleatorizaciones seguras, que siguen requerimientos matemáticos especiales, son llamados aleatorizaciones seguras criptográficamente. Uno de los requerimientos para aleatorizaciones seguras criptográficamente es que resulta muy difícil calcular una colisión, es decir, dos entradas que se aleatorizan al mismo número. Esto significa que aún si un atacante cambia un archivo, no podrá cambiar el archivo de forma que burle al verificador de integridad.

Ventajas

No es computacionalmente factible vencer a las matemáticas en un verificador de integridad. Esto los hace una muy pero muy buena herramienta para detectar cambios en los archivos de una computadora. Es muy fuerte, de hecho esta es una de las herramientas más importantes que se usan para detectar un mal trato a los sistemas computacionales.

Los verificadores de integridad observan todo en un sistema, o solo archivos importantes. Son extremadamente flexibles.

Una vez que los atacantes comprometen al sistema, les gusta hacer dos cosas. Primero les gusta cubrir sus ataques, lo que significa que alterarán sistemas binarios, librerías, o archivos de registró de acceso para esconder el hecho de que ellos están o han estado en el sistema. Segundo, ellos harán cambios para asegurar que seguirán accesando al sistema. Un verificador de integridad de archivos correctamente configurado detectará ambas actividades.

Desventajas

Los verificadores de integridad cuentan con datos almacenados en las computadoras locales. Como archivos de acceso, estos datos son vulnerables a modificaciones en el sistema. Dicen a un atacante como obtener privilegios de super usuario en el sistema el atacante puede encontrar el verificador de integridad, hacer algún cambio hostil en el sistema y volver a correr el verificador de integridad para crear nuevamente los valores aleatorios de la base de datos, y cuando el administrador del sistema corra el verificador, no encontrará ningún cambio en el sistema. Una forma de rodear este problema es mantener la base de datos en modo de solo lectura tales como CD escribible.

El verificador de integridad debe estar configurado para cada sistema. Usualmente esto es una tarea que consume mucho tiempo y es complicado. Si el sistema operativo no es bueno al cumplir con la integridad del sistema, la instalación se convierte en algo más complejo.

Una vez que el verificador es configurado, debe correrse frecuentemente. Dependiendo del sistema operativo, simples cambios u operaciones normales pueden reportar desde decenas hasta miles de cambios. Por ejemplo, un verificador de integridad corre justo después de actualizar MS−Outlook en un sistema Windows NT, entonces justo antes de la instalación se reportan mas de 1800 cambios.

Finalmente, el verificador de integridad consume un considerable número de recursos del sistema. Estos pueden masticar al CPU, memoria, y espacio de disco. Muchos administradores no querrán correr frecuentemente el verificador de integridad. Esto limita su funcionalidad, porque un verificador que corre una vez al mes, reportará tantos cambios que un ataque real tiene una buena oportunidad de pasar desapercibido.

4.4 Explorador de Vulnerabilidad

Un explorador de vulnerabilidad puede buscar vulnerabilidad en un NFS conocido, examinando los servicios disponibles y la configuración de un sistema remoto. Un IDS, manejando la misma vulnerabilidad, podría reportar solo la existencia de la vulnerabilidad cuando un atacante intente explotando.

Los exploradores de vulnerabilidad, sean de red o de servidor, dan la oportunidad de que la organización arregle problemas antes de que lleguen, en vez de reaccionar a una intrusión o un mal uso que ya esté en progreso. Un IDS detecta intrusiones en progreso, mientras que un explorador en primer lugar, una intrusión. Los exploradores de vulnerabilidad pueden ser de mucha ayuda en organizaciones sin una buena capacidad de respuesta a los incidentes.

Un explorador de vulnerabilidad de red opera remotamente, examinando la interfase de red en un sistema remoto. Este buscará servicios vulnerables, corriendo en una máquina remota, y reportando una posible

vulnerabilidad. Por ejemplo, es bien sabido que rexd es un servicio débil; un explorador de vulnerabilidad de red intentará conectarse al servicio de rexd. Si la conexión tiene éxito el explorador reportará vulnerabilidad en el servicio rexd.

Después de que el explorador de vulnerabilidad de red pueda ser corrido desde una sola máquina en la red, este puede ser instalado sin impactar la configuración de otras máquinas. Frecuentemente estos exploradores son usados por auditores y grupos de seguridad porque pueden proveer una vista externa de los hoyos de seguridad en una computadora o una red.

Ventajas

Los exploradores de vulnerabilidad de red pueden reportar una gran variedad de objetivos en la arquitectura. Algunos trabajan con ruteadores, otros son sistemas Unís y algunos otros con NT u otra plataforma Windows.

Los exploradores de vulnerabilidad de red son, en general, muy fáciles de instalar y de comenzar a usarlos. A diferencia de los sistemas basados en el servidor, los cuales usualmente requieren instalación o reconfiguración del software, un sistema basado en la red puede ser depositado en un lugar en la red. Simplemente conectando la interfase dentro del switch y encendiendo la máquina.

La GUI (interfase gráfica de usuario) con un sistema de red, tiende a ser completamente intuitiva, lo cual significa que el personal junior puede monitorear el sistema y llamar a más analistas señor si algo inusual ocurre.

Desventajas

Los exploradores de vulnerabilidad de red son casi exclusivamente sistemas basados en firmas. Como un IDS basado en firmas, un explorador de vulnerabilidad basado en firmas, puede detectar sólo aquellas vulnerabilidades que este programado para reconocer. Si una nueva vulnerabilidad surge, como frecuentemente ocurre, hay una gran oportunidad para el atacante antes de que el vendedor actualice las firmas. Si la vulnerabilidad continua, los sistemas pueden permanecer vulnerables a ataques durante un periodo de tiempo.

Si los clientes son tan inteligentes con sus exploradores la vulnerabilidad de firmas como lo muestra la historia, entonces muchas organizaciones serán vulnerables a los ataques aún si corren sus exploradores de vulnerabilidad regularmente. Un análisis reciente muestra que el 90% de los servidores de red corriendo IIS aún son vulnerables a una bien documentada y muy seria vulnerabilidad de seguridad, para lo cuál el vendedor ha producido avisos de seguridad. Un explorador de vulnerabilidad sólo puede enfatizar posibles problemas que la organización debe resolver.

Otro problema potencial con los exploradores de vulnerabilidad de red es que las salidas siempre requieren de hábiles interpretaciones. Cada ambiente tiene diferentes requerimientos de operación y diferentes vulnerabilidades en seguridad. De hecho, el concepto de vulnerabilidad engloba otros conceptos vagamente definidos, tales como riesgo, aceptabilidad y las habilidades esperadas del atacante. Como cada uno de estos conceptos varía con cada organización, el grado en que una configuración particular represente vulnerabilidad, también varían con cada organización.

Cuando el explorador de vulnerabilidad reporta una vulnerabilidad particular, la red de la organización o el personal de operación deben evaluar ese reporte dentro del contexto del ambiente operativo de la organización. La vulnerabilidad puede no representar un riesgo inaceptable en ese ambiente de la organización, o el riesgo puede ser forzado sobre la organización por los requerimientos de negocios. Esto puede parecer tonto en el contexto de discusiones de seguridad, pero en el mundo real de la seguridad, las preocupaciones frecuentemente caen en víctimas de justificaciones de negocios.

Los exploradores de vulnerabilidad han sido conocidos por disminuir a la máquina objetivo. Algunas implementaciones IP no son suficientemente robustas para manejar conexiones simultaneas, o paquetes IP con combinaciones de banderas inusuales. El tráfico generado por una agresiva búsqueda en un puerto, por ejemplo, puede hacer que a veces la máquina se carga.

Finalmente, los exploradores de vulnerabilidad de red tienden a contener una enorme cantidad de datos de vulnerabilidad. Si alguien alguna vez irrumpe en el sistema del explorador, compromete a las demás máquinas de la red puede convertirse en un juego de niños. Es necesario proteger el explorador para prevenir el uso no autorizado de la exploración de datos.

4.5 Exploradores de Vulnerabilidad del Servidor

Un explorador de vulnerabilidad del servidor difiere de un explorador de vulnerabilidad de red en que éste está completamente confinado al sistema operativo local. Un explorador de vulnerabilidad de red requiere que la máquina objetivo sea accesible desde la red para poder operar; en un explorador de vulnerabilidad del servidor no es así.

Los exploradores de vulnerabilidad del servidor son software instalado en sistemas operativos particulares. Una vez que el software es instalado puede ser configurado para corres a cualquier hora del día o la noche.

Ventajas

Los exploradores de vulnerabilidad del servidor tienden a estar mucho más sintonizado y preciso en cualquier sistema operativo. Ellos pueden decirle frecuentemente al usuario que parches deberán aplicar para arreglar una vulnerabilidad identificada, mientras los exploradores de red, algunas veces solo proveen información general.

Cuando considere que producto comprar observe una muestra del reporte para su sistema operativo especifico, para determinar cuanta información está contenida en los reportes. La amplitud y precisión del reporte podría ser un criterio de selección.

Los exploradores de vulnerabilidad del servidor no consumen ancho de banda de la red cuando corren, todo el procesamiento está restringido al sistema del servidor local. Los exploradores de vulnerabilidad del servidor no son similares a los exploradores de red. Algunos sistemas operativos tienen débiles o pobres implementaciones de pilas asociadas con sus interfaces de red, enviar un gran volumen de tráfico o banderas TCP inusuales puede causar que la interfase se trabe, lo cual necesitará que se reinicie.

Los exploradores de vulnerabilidad del servidor, son menos susceptibles a ser usados contra la organización por algún intruso. Un pirata que entre en el sistema y encuentre un explorador de vulnerabilidad de red haga una exploración desde él puede utilizar la herramienta para atacar otros sistemas dentro de la organización. Una herramienta basada en el servidor provee mucho menos información útil para hacer más grande un ataque.

Desventajas

Los exploradores de vulnerabilidad del servidor son, basados en firmas. Ellos buscan conocidas configuraciones peligrosas y las reportan en una especie de libro de cocina para eliminar esas amenazas. Los procedimientos del sistema local y sus requerimientos de operación pueden requerir flexibilidad para encontrar y aplicar soluciones a una vulnerabilidad dada.

Instalar una explorador de vulnerabilidad del servidor requiere la cooperación de los administradores del sistema como el software corre usualmente con privilegios, el administrador de cada máquina debe aprobar el

propósito y la configuración de la herramienta. En muchas organizaciones, esto puede representar un severo problema de coordinación.

Tal como cualquier sistema basado en el servidor, los atacantes pueden modificar el explorador de vulnerabilidad sin que se reporte que ha sido modificado.

CAPITULO 5. PUNTOS A CONSIDERAR EN LA SELECCIÓN DE UN IDS

5.1 Pautas para Seleccionar Productos

Las capacidades técnicas son ciertamente una parte importante de la decisión de compra, pero ellos no son la única parte. Hay varias consideraciones orgánicas y medioambientales cuando se trata de un IDS. ¿Muchos de estos problemas contestan la pregunta "Debemos nosotros situar un sistema de detección de intrusión?" ¿Qué debe preguntarse y razonablemente debe contestarse antes de la pregunta, "Qué IDS debemos nosotros situar?"

Esta sección proporciona tres arboles de decisión separados para ayudarnos con los procesos que realizan decisiones. Se piensa que estos árboles proporcionan guías básicas en la decisión que hacen los procesos para una compra de IDS. Empiece examinando algunos de los puntos de decisión en el árbol de la Administración. Entonces proceda al árbol Técnico para examinar algunos de los problemas relacionados para usar un IDS en una red interior. Finalmente, si usted tiene una misión el servidor de web crítico que nosotros recomendamos evaluar, Sitio Web se considera en el Paso 3. Usted puede encontrar que requiere más de un tipo de producto de IDS. En ese caso, esta sección puede ayudarle a decidir qué tipos de IDS cubren la mayoría de sus necesidades de seguridad de información.

Problemas de Administración

El primer paso para evaluar un proyecto de detección de intrusos es determinar el alcance del apoyo a la organización para este proyecto. Recuerde que el propósito de un proyecto de detección de intrusos es no solo detectar posibles intrusiones, pero a de "hacer algo" sobre ellos. Por consiguiente, la detección de intrusos debe ser considerada como parte de un proceso de contestación más grande a incidentes. La administración debe decidir qué tipo de contestación es apropiada y cómo resolverse cualquier incidente identificado.

Además, la contestación de un incidente responde a una intrusión que puede involucrar un número significativo de asuntos legales, públicos, conexión de una red, y personal de administración de sistemas, así como la productividad perdida y tiempo fuera de servicio del sistema. La organización debe entender estos problemas totalmente antes de iniciar un proyecto de detección de intrusos. La magnitud de apoyo orgánico tendrá un efecto en la selección del producto final; sistemas que son duros de llevarse a cabo y aquellos en los que el campo requerirá más paciencia de administración que sistemas que están esencialmente enviados en cajas. El último, sin embargo, requerirá mejores esfuerzos del análisis humano para interpretar y detectar falsas alarmas.

Los procesos administrativos relativamente fuertes configurados dentro de la organización afectarán la selección y eficacia de cualquier sistema servidor−basado directamente y, a un menos grado, cualquier sistema red−basado. En algunas organizaciones, cualquier usuario en el sistema puede alterar la configuración del sistema. Ellos pueden, por ejemplo, alterar los archivos que podrían parecer ser un acto hostil. Una vez que el cambio es nombrado, debe investigarse antes de que la organización pueda continuar realmente en el sistema. Sin embargo algunas Organizaciones con procesos de CM fuertes, pueden sentirse cómodas ante cualquier cambio completamente sospechoso no reconocido.

Problemas técnicos

Los problemas técnicos abundan al instalar un sistema de detección de intrusos. Típicamente, el problema técnico más serio está tratándose del tráfico de la red adicional que puede ser generado por un IDS. Otro problema es crear un proceso para interpretar resultados del IDS. Las organizaciones deben decidir cómo manejar los resultados interpretados y cómo integrar esos resultados en un plan para la contestación y corrección.

El primer paso en sistemas planeados es identificar los recursos críticos de información, ambos para el almacenamiento y comunicaciones. En otras palabras, haga una lista de lo que usted está intentando proteger. En algunos casos, este poderío es un servidor de web en su perímetro DMZ. En otros casos, podría ser la configuración del firewall que le permite tráfico al DMZ. En otros casos, podría ser los mainframe o sistemas de base de datos back end que guardan información del cliente en extremo crítica. Incluso podría ser, a alguna magnitud, la imagen de su compañía (sí usted está angustiado sobre los sitios Web borrados). Cuando usted construye la lista de recursos críticos, haga el diagrama de los sistemas y redes para proporcionar una representación visual del ambiente y colocación de herramientas de IDS. Este diagrama debe compararse con mapas de red de oficial para asegurar consistencia con la arquitectura de la red global.

Una vez que se han identificado recursos de información críticos, evalúe su habilidad de mantener la seguridad de esos recursos. ¿Si usted no tiene ningún medio de dirección de la configuración en el sitio Web, tiene usted realmente la capacidad para mantener la integridad del servidor? ¿Si no hay prioridad en la organización para reparar vulnerabilidades conocidas en los sistemas críticos, será el software de detección en esos sistemas valiosos?

Acceder a las máquinas también es un factor crítico. El Servidor basado en sistemas de detección de datos requiere más atención que una red basada en detección de intrusos. Desde que un Servidor basado en IDS requiere acceso privilegiado a la rutina del OS de la máquina afectada, un Servidor basado en IDS requiere el apoyo significante del grupo que mantiene esas máquinas. Este solo factor es la consideración más importante al instalar a un Host basado en IDS.

Problemas de Sitio Web

Instalando un IDS para un servidor web o DMZ presenta consideraciones especiales. Puesto que los servidores de web son más susceptibles a la manipulación, a ellos se les deben dar consideraciones especiales por el equipo de IDS. Los servidores web de transacciones son más vulnerables que los servidores de web estrictamente informativos, puesto que el rango de interacción es más grande. Considere usando más de un tipo de IDS en estos ambientes, porque ellos son más sensibles y la dirección de la configuración para los servidores de web es normalmente más firme que la Administración de la Configuración para los sistemas interiores.

Productos de Arboles de Decisión

Problemas de la Integración Práctica

Instalando o integrando un IDS con otras herramientas en el arsenal de seguridad requieren alguna planificación extra. Debe conocerse acerca de los problemas para configuración del firewall y las consideraciones para topologías de seguridad de redes.

Es importante que dentro de la Administración se realicen políticas de contestación de intrusión interior y el personal experimentado necesario para supervisar el IDS. Asumiendo que usted tiene un firewall. Así mismo se asume que su topografía de sistema de perímetro sigue los principios de seguridad prudentes.

Colocación del Sensor para una Red IDS

Si usted está desplegando una red IDS, usted debe decidir dónde poner los sensores supervisándolo de antemano. Esto dependerá significativamente de qué tipo de intrusión o del esfuerzo de intrusión que usted intentará descubrir.

Empiece creando un diagrama de la red detallado, si es que no lo tuviese. Un diagrama de la red puede ser inestimable a la planificación de IDS. Al mirar el diagrama, evalúe puntos de ahogo de red importantes o colecciones de sistemas que son sensibles a los funcionamientos comerciales. Un diagrama bien preparado puede mantener pistas intrínsecas a la situación correcta los sensores de IDS.

Si el IDS va a supervisar un servidor de web para penetraciones, entonces la posición más útil para el sensor estará en el segmento de DMZ con el servidor de web. Esto asume, por supuesto, que su servidor de web está en un segmento de DMZ, en lugar de fuera de o dentro del firewall (ninguna de las cuales es una idea particularmente buena). Si los atacantes componen el servidor, el IDS tiene la mejor oportunidad de descubrir la penetración original o la actividad resultante que origina del organizador compuesto.

Si el IDS va supervisar a los intrusos detectados en servidores internos, como servidores de DNS o servidores del correo, el mejor lugar para un sensor simplemente es el interior del firewall en el segmento que conecta el firewall a la red interior. La lógica detrás de esto es que el firewall prevendrá la inmensa mayoría de ataques apuntada a la organización, y ese monitoreo regular de los firewall anotará aquello que sean identificados. El IDS en el segmento interior descubrirá algunos de esos ataques que se realizan para estar dentro de los firewalls. Esto se llama "la defensa a fondo."

Algunas organizaciones querrán usar el IDS para supervisar recursos interiores como una colección sensible de máquinas o una sección específica o situación física. En ese caso, el lugar más lógico para el sensor de IDS estará en el punto de ahogo entre esos sistemas y el resto de la red interior.

¿Qué pasa fuera de un Firewall?

Es importante mencionar que por el momento no se ha discutido el poner un sensor fuera del firewall. Algunas fuentes recomiendan o defienden un sensor de IDS fuera del firewall con el fin de supervisar ataques del Internet. Miremos esa idea en un ambiente operacional ver lo que significa.

El propio firewall debe anotar cualquier ataque que detiene (asumiéndolo tienen un firewall anotando y leyendo los registros) ¿Qué agregó valor que proporcionan los IDS en este guión? ¿Si usted no está mirando los logs del firewall, por qué le prestaría usted la atención al IDS? Si lo hace, verá los ataques detenidos a ese punto. El IDS es redundante. Probablemente no es un uso productivo de dinero orgánico y tiempo para instalar y supervisar un IDS fuera del firewall.

Eso que se dice, si usted todavía quiere contar o evaluar ataques que se detienen al firewall, un IDS puede simplificar el proceso de rastrear y clasificar ataques. Los datos todavía deben estar en los logs del firewall, pero el IDS puede mejorar la legibilidad o claridad de la información.

Servidor de Integración para un Servidor IDS

Si usted planea usar un sistema Servidor−basado, usted debe tener una comprobación adecuada y fase de familiarización. Esto permite a los operadores y a analistas conocer el funcionamiento de esa parte en particular del software. El IDS debe instalarse bien de antemano en un sistema de desarrollo de instalación planeada en un sistema de la producción. Incluso en un sistema inmóvil, algunos archivos cambiarán regularmente (por ejemplo, el archivo de auditoría), así que el IDS informará algunos cambios. Algunos sistemas Servidordor−basado, como un ejemplo adicional, informarán cuando un proceso del usuario altera el archivo de contraseña de sistema. Esto pasaría si un intruso agregó una cuenta. También pasa, sin embargo, cuando un usuario cambia su o sus contraseñas. El analista de IDS necesita tiempo para familiarizarse con el

funcionamiento correcto de cada sistema, para que él o ella puedan diagnosticar desviaciones propiamente de "normal" las alarmas.

Tenga presente, al usar un sistema servidor−basado que frecuentemente debe supervisarse. Esto significa un día dos veces, por lo menos. Si un atacador tiene superuser podra o tendrá la capacidad de acceder al sistema, él o ella puede alterar el IDS o el banco de datos de IDS a las alarmas del supress. Si el IDS escribe a un archivo, el atacante puede revisar el archivo del rendimiento simplemente. En otras palabras, siempre es sospechoso que algo puede haber alterado la configuración del IDS.

Configuración de Alarmas

IDSs vienen con niveles configurables de alarma. Algunos se integrarán con dirección de las estaciones de la red, algunos permiten compaginar, algunos envíar e−mail, y algunos pueden interoperar con firewalls para cerrar todo el tráfico de la red que originó el ataque.

Sea muy cauto sobre usar estos rasgos. De hecho, para el primer mes o segundos apague todas las alarmas. Sólo mire el rendimiento del sistema ver lo que está descubriendo. Todos los IDSs tienen, como discutió anteriormente, algún nivel de positivo falsos; ese nivel puede ser tan alto como 80 o 90 por ciento de alarmas informadas. Usted necesita estar familiarizado con su sistema particular antes de que usted empiece encendiendo alarmas.

Alarm misconfiguration, o over−aggresive responde a las alarmas, puede llevar a una decisión orgánica para apagar el IDS. Los locos de las computadoras saben que las instalaciones de IDS son supervisadas por humanos, y que los humanos tienen fracasos humanos. Ellos saben que si ellos activan alarma después de la alarma, las personas que supervisan el sistema dejarán de prestar atención.

Igualmente, si el IDS se configura para instruir el firewall para negar todo el tráfico "atacando" las redes, los locos de las computadoras pueden aprovecharse de esto fácilmente. Alguien motivó suficientemente o malévolo podría usar esto contra la organización por spoofing ataca a los compañeros del negocio de la organización o los sitios muy conocidos (Bestia, AltaVista, Amazona, CNN, Microsoft, el etc.) para que el firewall negara tráfico entrante de esos sitios, incluso el e−mail y tráfico de sitio web. Recuerde, el IDS no es la seguridad está ahorrando gracia, es sólo una herramienta (y uno bastante poco inteligente a eso).

Horario de la Integración

Instale un sensor en un momento. No se apresure la instalación para rodar fuera la capacidad de IDS en un palmo de tiempo corto. Toma una cierta cantidad de tiempo para los administradores y analistas ganar familiaridad con las peculiaridades de un sistema dado o punto de la red, y las peculiaridades no pueden ser el mismo del punto para apuntar. Un sensor en un DMZ puede ver un juego dado de conductas, mientras un sensor en la red interior puede ver otro juego de conductas, con una intersección muy pequeña.

Es crucialmente importante que el personal asignado para supervisar el IDS esté adecuadamente familiarizado con cada dispositivo en la configuración.

CAPITULO 6. EJEMPLOS

6.1 Elección de un IDS

La compañía la llamaremos X.com Inc.. El Internet ha permitido que la compañía establezca una variedad amplia de mercados, tales como educación en línea, de servicios Internet y de un surtido de programas de la difusión que permiten la comunicación de dos vías entre abastecedores, estudiantes y clientes. Cuando decidíamos desplegar las IDS, la meta fundamental era lograr una equilibrio razonable entre controlado,

asegura el acceso y la alta disponibilidad. Otra meta era elegir un producto que no requeriría muchos de administración y de entrenamiento, en vista de la tamaño de nuestro departamento de IT., que es pequeño.

Consideraciones

Después de una filosofía de seguridad de varias capas, no deseamos una solución para nuestro sistema de la detección de intrusiones, sino algo varias capas de protección, comenzando con los riesgos asociados a servicios y a dispositivos de red. Deseamos la protección en el nivel de sistema y una herramienta para vigilar en tiempo real. Y finalmente, necesitamos poder atarlo todo junto con una solución robusta que podría obrar recíprocamente con los dispositivos existentes de la red, tales como nuestros firewalls y ruteador.

Después de que identificáramos algunos de los productos populares de las IDS, creamos una matriz que enumeraba cada nombre del producto, requisitos de la plataforma, la metodología de la detección (estadística o en tiempo real), la información del contacto y el coste. Además, creamos una lista de preguntas que deseamos contestar sobre cada producto:

- ¿Qué equipo especializado se requiere?
- Es un producto de red o es basado en host?
- Qué cantidad de ataques puede el producto detectar?
- Cómo y cada cuánto se hacen las actualizaciones?
- ¿es capaz de responder automáticamente a los ataques?
- Cuál es el precio?
- Qué tipo de infraestructura se debe crear para implementar y manejar el producto?

El paso de progresión siguiente era construir un diagrama de la red existente de X.com's para entender qué con que equipo se contaba: hosts, subnets, lruteadores, gateways y otros dispositivos de la red fueron situados en nuestra infraestructura. Esto nos dio una comprensión más clara de nuestra exposición y con tal que una buena referencia para el desarrollo de política. Con esta información a disposición, también podíamos estimar los costes que licenciaban de varias opciones de las IDS −− no una tarea fácil, puesto que algunas configuraciones se licencian según la segmentación de la red, otros por el número total de hosts.

Con estas preguntas preliminares en mente, seleccionamos cuatro productos para poner a través los pasos: RealSecure de los sistemas Internet de la seguridad (ISS) (www.iss.net), de NetRanger de la aplicación de la detección del Cisco Systems (www.cisco.com/netranger), de la intrusión de NFR del registrador de vuelo de la red (www.nfr.net) y de SessionWall−3 de AbirNet (www.sessionwall.com). Para cada uno de estos productos, el primer paso de progresión era leer a través de cualesquiera white papers y literatura del producto Entonces, solicitamos versiones del demo para ver el producto en la acción antes de hacer una consolidación financiera. A continuación se realizaron las pruebas pertinentes sobre los servidores, donde se detectaron los posibles problemas que se tenía. Una vez que se han probado todas las opciones se debe elegir por aquella que más se acople a nuestras necesidades en cuanto a la interfaz y la forma como detecta los intrusos.

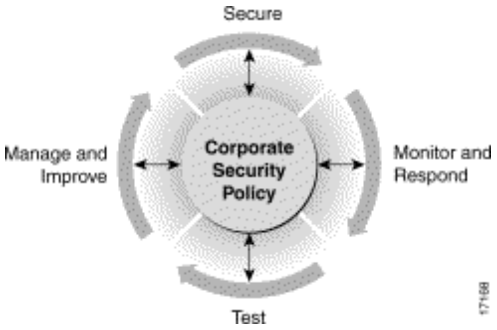
6.2 Cisco Secure Intrusion Detection System (NetRanger)

A continuación presentamos un producto IDS. NetRanger, es u sistema de detección de intrusiones con las características de que es empresa−escala, tiempo real, diseñado para detectar, para señalar, y para terminar actividad no autorizada a través de una red. Es el primer sistema de la detección de intrusiones de la industria, el Cisco Secure Intrusion Detection System es el componente dinámico de seguridad de la línea de productos de Cisco.

El entorno de seguridad

El entorno en el que se desenvuelve el NetRanger se basa en una perspectiva operacional más bien que en

productos independientes o políticas. Esta filosofía de la seguridad se refleja en la imagen de la rueda de la seguridad que se muestra a continuación. La premisa de esta filosofía es como la administración de la red, la administración de la seguridad es un proceso dinámico, los procesos cambian constantemente.



El entorno de la seguridad es cíclico para asegurar su buen funcionamiento y mejora la seguridad. El paradigma incorpora los cinco pasos de progresión siguientes:

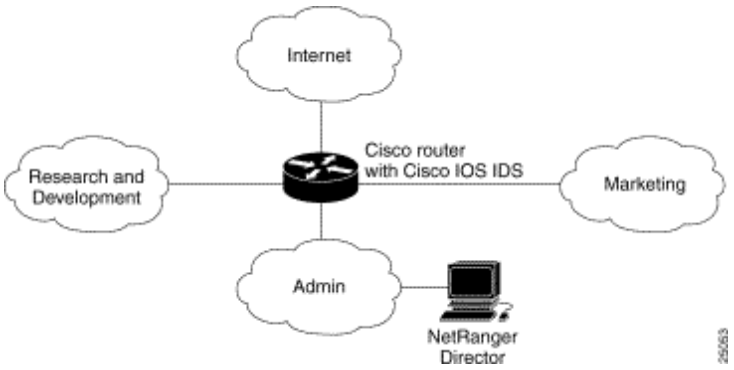
- Desarrolla una política fuerte de seguridad
- Plantea una red segura
- Monitoreo de la red y responde a ataques
- Pruebas existentes para mantener la seguridad
- Maneja y mejora la seguridad corporativa

Los resultados o los datos obtenidos en los pasos de progresión 2 al 5 necesitan siempre ser comparados a la política de la seguridad desarrollada en el paso de progresión 1 para asegurarse de que se están resolviendo los objetivos de alto nivel de la seguridad.

El IDS de Cisco como Perímetro de la Defensa de la Detección de Intrsuiones

El sistema de entrada y salida (IOS) de un IDS y el de un Firewall, crean una estructura muy sólida, lo que se llama el perímetro de defensa de la detección de intrusiones. Porque Cisco IOS IDS contienen solamente un subconjunto de firmas encontradas en el sensor del NetRanger, no detectará todos los ataques, sino que combinado del control de acceso listas fuertes y un firewall, debe proporcionar a un servicio de seguridad bastante robusto.

Con esta información, usted debe ahora considerar la red que usted desea proteger. Determínese qué segmentos deben ser vigilados. Tenga presente que el componente del Cisco IOS IDS mantiene una política de seguridad configurada para el segmento que está vigilando. Éstos pueden ser estándares a través de la organización o únicos para cada dispositivo del sensor del IDS. Se puede considerar cambiar la topología de la red para forzar el tráfico a través de esta y vigilar un segmento dado de la red. Hay siempre compensaciones operacionales al pasar por este proceso. El resultado final debe ser una idea aproximada del número de los sensores del IDS requeridos para proteger la red deseada.



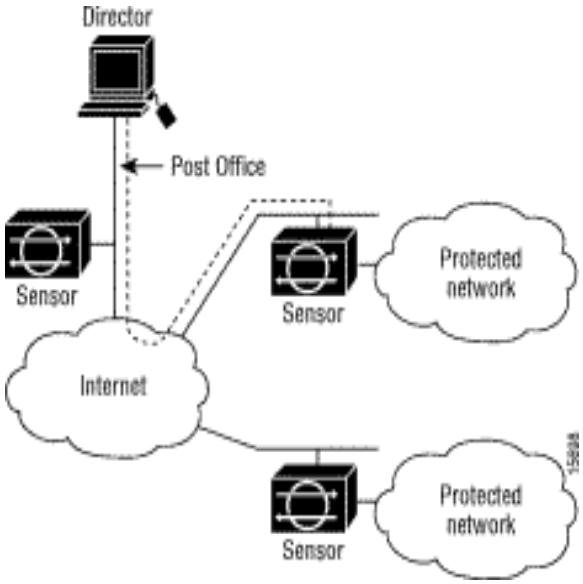
Componentes del Cisco Secure Intrusion Detection System

Los IDS seguras del Cisco son un sistema en tiempo real que incluye los sensores seguros de los IDS del Cisco, las aplicaciones cautelosas de la seguridad de la detección de la intrusión de la seguridad que actúan como los " succionadores" y el director de seguridad, una consola centralizada de administración. El director recoge datos entrantes del sensor, los traduce, y los presenta al personal de responsable de la seguridad en un interfaz. Los usuarios pueden tener acceso rápidamente a la información adicional sobre el tipo de ataque desde el Network Security Database (NSDB) del director. El director también permite que el personal de la seguridad maneje la configuración de sensores remotos. Y finalmente, el director puede manejar datos del sensor exportándola a las bases de datos emparentadas de tercera persona.

La información que se tiene en específico es:

- El sensor. El sensor en una red es una aplicación de la red que combina alta confiabilidad con simplicidad de la instalación y del mantenimiento. Cada segmento de la red monitoreado requiere un sensor dedicado, incluyendo Internet, los Intranets, y las Extranets. La aplicación del sensor se optimiza para rangos de datos específicos y las interfaces, tales como Ethernet (10BaseT), Ethernet rápida (100BaseT), el Token Ring (4 y 16 Mbps), y el Fiber Distributed Data Interface (FDDI) (modo solo o dual). Utiliza un motor experto basado en reglas del sistema para destilar volúmenes grandes de tráfico de la red del IP en acontecimientos significativos de la seguridad. Ofrece una característica llamada "three−tiered" para la detección del ataque para establecer claramente la actividad no autorizada, incluyendo: nombre los ataques, la categoría general de los ataques, y los ataques extraordinarios. El sensor puede también monitorear los syslogs de un ruteador para las violaciones de la política de seguridad, registra los datos de la seguridad, " mata " a las sesiones activas del TCP, y maneja dinámicamente las listas del control de acceso de una ruteador para evitar a intrusos
- El director. Proporciona una interfaz gráfica que proporciona a la administración local, centralizada o distribuida hasta centenares de sensores a través de una red distribuida. El director fue desarrollado para proporcionar a una operación amigable, interfaz point and click para la respuesta constante a los acontecimientos de la seguridad. Puede también realizar otras funciones importantes: manejo de datos a través de las herramientas de tercera persona, tenga acceso a una base de datos de la seguridad de la red, remotamente pueda monitorear y manejar los sensores, y envíe la información del acontecimiento a un sistema de perturbación, a una página o a un e−mail al personal de alerta de la seguridad cuando ocurren eventos sobre seguridad.
- Post Office. Es la configuración de las comunicaciones que proporciona robustas, confiables, y eficientes comunicaciones entre los Cisco Sensor y Director. Toda la comunicación es utilizada por un protocolo propietario, el protocolo es conectionless que pueda cambiar entre las rutas alternativas para mantener la comunicación punto a punto.

La relación que se da entre los componentes se ilustran a continuación

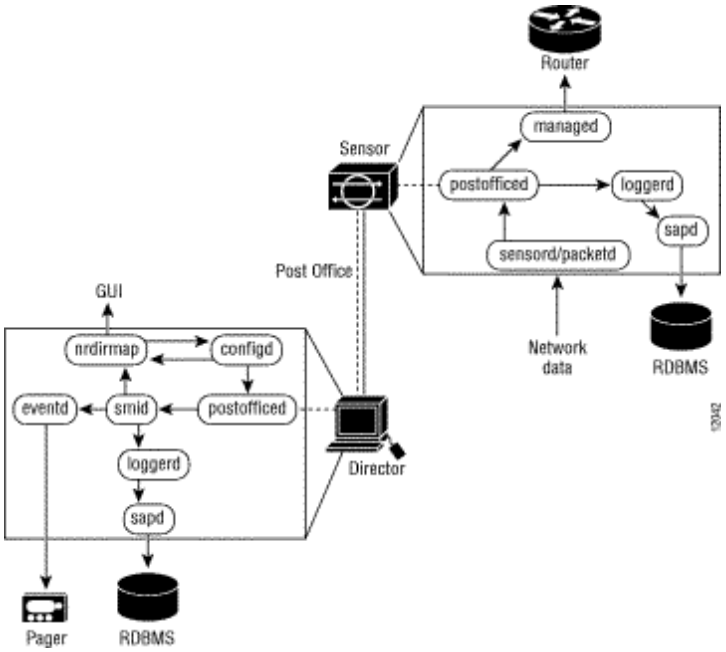


Arquitectura del Cisco Secure Intrusion Detection System

Los sensores, los directores, y el correos cada uno tienen componentes operacionales separados, llamados los demonios o servicios. Porque cada función es lograda por un servicio separado, los resultados son un sistema de seguridad que es rápido, durable, y escalable.

Los servicios que se muestran en la figura siguiente son:

- Sensor/packetd. Estos servicios proporcionan la detección de intrusiones. El sensord se utilizan cuando un sensor está cooperando con un dispositivo de la red que utilice las funciones de copy_to/log_to (que envía las copias de paquetes capturados al sensor); se utiliza el packetd cuando el sensor en sí mismo está capturando los paquetes directamente de la red.
- El servicio de Loggerd. Es el recurso de registro de las IDS. Es responsable de error de la escritura, de comando, y alarma de entradas a archivos log en el sensor.
- Sapd. Este servicio proporciona a datos y a la administración de archivos. Es responsable de mover archivos log a las áreas del respaldo de la base de datos, a los archivos off−line, y a otros procesos de la rutina para evitar que los sistemas de archivos no se puedan guardar adecuadamente.
- El servicio de Postofficed. Maneja la comunicación entre los servicios seguros de los IDS del Cisco y los nodos seguros de los IDS del Cisco. Según lo ilustrado en la figura, cuando el sensord detecta actividad desautorizada, señala postofficed; postofficed es entonces responsable de decir loggerd para comenzar a registrar, alertando el smid en el director, y ordenar la comunicación a un ruteador si el ataque va a ser evitado.
- El servicio de smid. Se ejecuta en el director solamente, y es responsable de traducir datos del sensor en la información significativa para el nrdirmap.
- El servicio de nrdirmap. Es responsable de visualizar los varios símbolos que representan las máquinas, las colecciones de máquinas, las aplicaciones, los alarmar, y los errores en el interfaz gráfico del director.
- El servicio de eventd. Es responsable de mantener procesos definidos por el usuario de la notificación del acontecimiento. Los utilizadores pueden definir qué clases de alarmas o de otros acontecimientos lanzan una acción, generalmente un e−mail o una notificación de página.
- El servicio de configd. Este proporciona un mecanismo a través del cual el nrdirmap pueda interconectar con otros servicios postofficed, sensord, y manejó. Es decir los comandos en el interfaz gráfico se pueden ejecutar vía el servicio subyacente del configd.



BIBLIOGRAFIA

- Revista Windows NT Magazine (Especial de Seguridad)

Año 2 volumen 11.

Direcciones de Internet:

http://www.infosecuritymag.com/newsletter/

http://www.infosecuritymag.com/newsletter/

http://www.guardiacivil.org/kio/seg/sld001.htm

http://www.idsdetection.com/

www.icsa.net

http://www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/index.shtml

Redes y Conectividad Sistema de Detección de Intrusiones

36

Las herramientas IDS

no le darán molestias. Ellas quizá incrementen su productividad

¿La administración organizacional constantemente mantiene el programa de seguridad de la información?

¿Esta la administración dispuesta a investigar las intrusiones computacionales?

¿Esta la administración dispuesta a investigar las intrusiones computacionales?

Es un escáner de vulnerabilidad una red en uso

¿La organización tiene una Configuración administrativa efectiva para los sistemas de procesos críticos?

Ir al paso 2

Comienza con redes con escáner de vulnerabilidad

Ir al paso 2

No

No

No

No

Yes

Yes

Yes

Yes

No

Yes

Examine el cambio entre una red con escáner de vulnerabilidad y redes IDS

Use una red con escáner de vulnerabilidad junto con un checador de integridad de archivos en sistemas críticos.

PASO 1: ADMINISTRADOR

Use redes con escáner de vulnerabilidad

¿Es más importante prevenir o detectar intrusiones?

(Si las dos son importante, siga ambos lados del árbol)

¿Ha usted escaneado sistemas internos para conocer la vulnerabilidad?

¿Esta usted dispuesto a instalar software adicional en servidores y estaciones de trabajo críticas?

Esta usted aptos para instalar software adicional en servidores & estaciones de trabajo criticas?

¿Esta el perímetro de tu red efectivamente protegida?

Prevenir

No

Yes

No

Detectar

Yes

No

Yes

Examine el cambio entre una red con escáner de vulnerabilidad y redes IDS

PASO 2:SISTEMAS DE REDES

Use redes con escáner de vulnerabilidad

¿Tiene usted una efectiva configuración de administración de procesos en lugar de software de sistema?

Use un Servidor con escáner de vulnerabilidad y un checador de integridad de archivos

Yes

Examiné cambios entre el escáner de vulnerabilidad de un Servidor y una red

No

Es más sensible el trafico basado en TCP/IP, o hay un significado en medio de la actividad non−IP

Tiene usted una configuración efectiva de administración de procesos en lugar de sistemas de software

¿Son sensibles los Servidores segregados dentro de las especificaciones de los segmentos de red?

¿El trafico de la red rutinariamente excede

50 MB/s en el backbone?

Use una Red IDS

Use un Servidor IDS y un checador de integridad de archivos

Examine el cambio entre un Servidor y una red IDS

Yes

Yes

IP

Yes

No

Considere una Red IDS como un firewall

No

Non−IP

No

Yes

Use una red basada en IDS

¿Esta el sitio web protegido por un firewall?

Utiliza una salida a una Red IDS para justificar la compra de un firewall.

¿Esta el servidor de web configurado bajo el administrador?

No

No

Yes

Yes

No

Yes

¿Es el Site el que provee acceso a otros que http y ftp?

Use un Servidor basado en IDS con Checador de Integridad de Archivos

PASO 3:SERVIDORES CRITICOS DE WEB

¿Él trafico de un site rutinariamente excede

30 MB/s?

Use igualmente Servidores o Redes basadas en IDS con checador de integridad de Archivos

No

Use un Servidor basado en IDS con un Checador de Integridad de Archivos.

Yes