Sistema de detección de intrusos en redes corporativas

Intrusion Detection System in Corporate Networks

Carlos Alberto Ocampo, Yanci Viviana Castro Bermúdez, Guillermo Roberto Solarte Martínez
Ingeniería de sistemas, Universidad Tecnológica de Pereira, Pereira, Risaralda
Correo-e: caos@utp.edu.co, yvcastro@utp.edu.co,roberto@utp.edu.co

***Resumen*—En la actualidad existen muchas herramientas que permiten proteger los computadores y las redes informáticas corporativas de posibles ataques, estos aplicativos permiten detectar intrusos y aunque las maquinas posean varios software con controles de seguridad, siempre existe un margen de error que puede ocasionar que dicho software falle.**

Los sistemas operativos cuentan hoy con herramientas que apoyan la seguridad, ejemplo de ello son los firewall, estos ayudan a proteger las máquinas de los ataques de un cracker, pero eso no significa que estos sean completamente seguros, pues el cracker puede generar una gran cantidad de registros, haciendo virtualmente inutilizable la información generando con ello un acceso no autorizado, comprometiendo la integridad, confidencialidad o disponibilidad de los datos del sistema, es entonces cuando se hace necesaria la creación de un Sistema de Detección de Intrusiones (IDS), que pueda proteger tanto las máquinas como la red así como avisar al administrador de la misma por varios medios, como por ejemplo el correo electrónico.

Palabras claves— IDS, HIDS, NIDS, intrusiones, seguridad, crackers, Escaneo de Puertos.

Abstract—Today there are many tools to protect computers and corporate computer networks from attacks, these applications can detect intruders and although the machines possess several software security controls, there is always a margin of error that can cause the software to fail.

Operating systems now have tools that support the safety, example is the firewall, these help protect machines from attacks by a cracker, but that does not mean that they are completely safe, as the cracker can generate a lot of records, making it virtually unusable thereby generating information from unauthorized access, compromising the integrity, confidentiality or availability of system data, It then becomes necessary Intrusion Detection System (IDS), that can protect both the machines and the network and alert the network administrator by various means, such as email.

Key Word— IDS, HIDS, NIDS, intrusion, security, crackers, Portscan.

I. INTRODUCCIÓN

Se han observado a través de los diferentes medios de comunicación (televisión, radio, etc...), noticias importantes sobre ataques informáticos a entidades como Yahoo, Microsoft entre otras entidades, pero eso significa que ¿Solo las Grandes Empresas son las que están propensas a recibir dichos ataques?, pues lastimosamente no es así, cualquier persona que posea un computador está en riesgo de sufrir un ataque por un hacker, aunque la información que se obtenga de este computador puede no tener mucho significado para el hacker, este puede hacer uso de su computador para realizar ataques a terceras personas, quedando así incognito, de tal forma que puede desaparecer fácilmente sin que su verdadera identidad se dé a conocer.

Existen algunas herramientas que son capaces de coordinar ataques de DoS entre múltiples maquinas afectadas, de forma que el hacker solo debe infectar unos cuantos ordenadores de usuarios finales (débilmente defendidos) y lanzar el ataque desde ahí. Ni siquiera tiene que estar conectado a Internet cuando el ataque se realiza. Citado de [3].

Lo cierto es que cada día que pasa más Empresas y Corporativos, se adaptan a los nuevos cambios y necesidades de la sociedad, por tal motivo se encuentran sistematizando la información mediante uso de tecnologías de computación y muy especialmente la implementación de redes informáticas que a cada instante se encuentran en la mira de los hacker, cuyo objetivo principal es la violación de los Sistemas de Seguridad con el fin de hacer intrusión en las organizaciones con miras a sustraer, modificar, desintegrar o simplemente acceder a la toda la información disponible y sensible de vulnerar, lo que indica que son personas expertas en sistemas de cómputo. *Se debe entonces contrarrestar este fenómeno exponiendo los conceptos de Sistemas de Detección de Intrusos (IDS), Sistema de Detección de Intrusos en un Host (HIDS)[1], Sistema de Detección de Intrusos en una Red (NIDS)[1], las técnicas y herramientas de detección, con el fin de crear esquemas seguros en las redes corporativas.*

Fecha de Recepción: 30 de enero de 2015
Fecha de Aceptación: 18 de marzo de 2017

Cada vez se hace necesario que las redes de computadores sean más seguras y capaces de detectar intruso a tiempo, ya que de esto depende el bienestar de la empresa (éxito o fracaso).

La gran mayoría de los sistemas de seguridad de una organización se centran en la detección de intrusos, para eso se utiliza su propio proceso de manejo de claves uno de ellos es la clasificación de claves por usuarios para permitir el acceso los diferentes partes del sistemas dependiendo de clave de acceso, debido a débil seguridad de claves la información termina en terceros , cada vez que se instala nuevos programas en los computadores brindar nuevos servicios de acceso de información pero estos servicios tiene muchas vulnerabilidades de seguridad.

En muchas ocasiones hasta los sistemas más seguros pueden ser infligidos por los mismos usuarios autorizados, por lo tanto mantener un sistema de seguridad no es nada fácil y peor aún diseñar estos tipos de programas a prueba de todo tipo de error es un proceso difícil de llevar acabo, se debe tener en cuenta otro tipos de controles adicióneles y externos de la máquina.

Uno de los medios que puede ayudar a este fin son los logs de auditoría[1] tanto al interior de cada una de las máquinas como en el tráfico de la red. Para la generación de estos registros en las máquinas, los distintos sistemas operativos tienen sus propios medios para obtenerlos; para inspeccionar el tráfico de la red, se puede utilizar firewalls de los que puede conocerse un poco más a fondo consultando en [2], los cuales con base en un conjunto predefinido de reglas permite o niega el paso de tráfico de información o paquetes al interior ó al exterior de la respectiva red corporativa.

Por lo mencionado anteriormente se debe llevar un control adicional para los logs de auditoria del tráfico de la red y cada uno de los eventos que pasen en servidor, de esta manera podemos afirmar que este control nos informara antes que el servidor destinado, así se puede evitar que los ataques lleguen al servidor, además de la utilización de un conjunto de dispositivos de seguridad y /o la intervención del administrador de la red, se puede reducir los ataque rápidamente.

II. SISTEMA DE DETECCIÓN DE INTRUSIONES

La detección de intrusos se explica claramente en el libro Díaz Vizcaíno [3], además especifica como seleccionar IDS, en qué lugar se debe ubicar dentro de la estructura de la red, también toca otros aspectos como su clasificación, requisitos, anomalías y su utilización indebida se puede consultar en [4] y [5].

conocer más de los sistemas de detección de intrusos se deben tener concepto claro sobre la historia de estos sistemas, la seguridad empieza desde nuestras viviendas como por ejemplo una buena seguridad de nuestra casa debe tener puertas, ventanas, cerraduras y cerras, además de contar con un sistema de alamar instalado, existe otro sistemas un poco más sostificados como cámaras de vigilancia que utiliza diferentes tipos dispositivos como sensores , infrarrojos y sensores de o temperatura para la detección de un intruso , otras forma de seguridad es la contratación de empresas de seguridad
Existe una analogía entre los sistemas de seguridad "**Domótica**" y la red de los sistemas de seguridad. Hoy en día vemos que el tema de seguridad de redes con la **Domótica** viene creciendo a un nivel exponencial ya que cada vez las personas se vienen concientizando sobre la importancia de la seguridad informática. Una técnica son lo (IDS) los Sistemas de detección de intrusos, estos sistemas ayudan a mantener un sistemas defensa permanente alertando cualquier intento o actividad sospechosa que ocurra en el sistema, además de tomar medidas clásicas de protección perimetral, existen IDS reactivos que interactúan con el sistemas de protección en el caso de encontrar una anomalía bloque dicho tráfico o cierre de algún dispositivo de la red , sin embargo este tipo de seguridad a veces puede provocar bloque o denegación del servicio de nuestro propio sistema

Hoy en día se puede contar con diversos tipos de sistemas de detección de intrusos que son adaptable a diferentes tipos de entornos, como por ejemplo están Sistemas de Detección diseñados para monitorizar redes completas mientras otros se implementan a nivel de host. Una de las estrategias más utilizadas en control de espacio perimetral son los cortafuegos [6], los cortafuegos actúan como las rejas con puntas afiladas y las puertas con una docena de cerraduras. Sirven para mantener fuera a los bandidos, es decir, sirven al propósito de prevenir ataques o intrusiones en la red interna por ellos protegida, pero todo esto no garantiza que algún intruso puede acceder por otro lado o través de tipos de dispositivo, sin embargo, el cortafuego garantiza una poderosa línea de defensa frente amenazas externas, pero en algunos casos puede generar falsa sensación de seguridad.

Generalmente si no se cumplen procesos adecuados de seguridad o una mala configuración del sistema tanto en SW como HW, puede llevar a que se tenga punto vulnerable en la red y en este caso la ventaja de utilizar cortafuegos se inútil.

Debido a estos tipos de inconveniente se hace importante la utilización (IDS), esta herramienta sirve como vigilante permanente ante cualquier anomalía del sistema.

Los IDS se utilizan para diferentes campos y aplicaciones no solo en la computadora o redes, pero para poder ser utilizados

[1]Logs son información vital para la seguridad de un sistema de cómputo, pero pueden llegar a ser voluminosos, por lo cual muchas veces son información inservible, pues no se tienen los medios para procesarlos y convertirlos en información que sirve para mejorar el sistema de seguridad de una empresa.

con éxito deben ser exactos en el sentido que no pueden dar información errónea (no considerar como ataque uno que en realidad sí lo era o, al contrario).

Si queremos medir la eficiencia del sistema IDS lo podemos hace a través del tiempo de respuesta del mismo sistema, ya que nos permite tener una ventaja para poder ejecutar acciones ante cualquier ataque, esta característica es la que debe tener todo sistema IDS par que se considerado como útil en la detección de intrusos en un sistema.

_____

Los sistemas de detección de intrusos (IDS)
Ayudan a los cortos fuegos a la detección de ataques, ya que en algunos casos existen anomalías que no pueden se detectadas por los, además de informar antes y después del ataque.

El resultado de la aplicación del Procesamiento Electrónico de Datos (EDP) a las auditorías de seguridad, utilizando mecanismos de identificación de patrones y métodos estadísticos que son indispensables en las tecnologías actuales de seguridad de redes, un meto que va de la mano con la detección de intrusos es la Auditoria de seguridad esta es la encargada de recolectar y revisar sucesos de un sistema en cada cierto periodo de tiempo con el objetivo de llevar historia y la detención de fallas o debilidades en la forma como se ejecutan los procesos.

III. CLASIFICACION DE LOS IDS

Existen dos campos de clasificación están los sistemas de detección de intrusos:

Sistemas de vigilancia
Como se hace esa vigilancia

A. Los IDS basados en red.

Un IDS basado en red monitorea los paquetes que circulan por la red en busca de elementos que indiquen un ataque contra alguno de los sistemas ubicados en ella; el IDS puede situarse en cualquiera de las terminales o en un elemento que analice todo el tráfico (como un HUB o un enrutador). Esté donde esté, monitoreará diferentes máquinas y no una sola: esta es la principal diferencia con los sistemas de detección de intrusos basados en host.

Estos sistemas utilizan diferentes puntos estratégicos de la red ya que poseen una o varias interfaces de redes conectada a estos puntos, que sirven para monitorear el tráfico en búsqueda de tráfico malicioso, esto dispositivo se encuentra en estado inactivos, pero se adhieren a los NIDS (Sistema de Detección de Intrusos en una Red) cortafuegos y enrutadores, de manera que el propio sistema puede forzar el cierre de conexiones y modificar reglas de filtrado de una manera más directa ,se puede monitorear el intercambio interno y externo de la red mediante la utilización de un solo dispositivo en conclusión esto sistemas no controla toda la red si no punto estratégicos de la red.

Para que los IDS ayuden a evitar posibles ataques en la red es necesario mantener actualizado el Software del equipo, ya que como no depende del tipo de Sistema Operativo es muy fácil de instalar y actualizar, pero a la vez no se puede descuidar el cortafuego.

B. IDS basados en máquina

Estos IDS protegen una máquina, es decir un único sistema, su función es la de manejar distancias, de tal forma que trabaja bajo un proceso denominado background, que analiza la maquina periódicamente de tal forma que pueda encontrar factores importantes que indiquen que el sistema se encuentra amenazado por un hacker, alertando y tomando las medidas necesarias para proteger el sistema.

Al Igual que los NIDS se instalan en ciertos puntos de la red, los HIDS(Sistema de Detección de Intrusos en un Host) suelen instalarse en las maquinas que componen la red, estamos hablando entonces de las estaciones de trabajo y sus servidores, que a través de los sensores instalados en la maquina se puede obtener información importante del nivel semántico[2] como por ejemplo llamadas al sistema, eventos complejos dentro de aplicaciones de alto nivel, etc.
Por otra parte, la tendencia actual al uso de conexiones encriptadas, de incuestionable interés para mejorar la seguridad de los sistemas, hace que un sistema que solo escuche la red disponga de muy poca información para distinguir el tráfico malicioso del aceptable.

Se ha encontrado que algunos Autores bibliográficos dividen el sistema de detección de intrusos basados en máquina, en varias categorías:

C. Periódicos o de tiempo real

Una de las diferencias entre los primeros HIDS y los NIDS es que el primero busca cada cierto periodo de tiempo elementos que le permitan identificar que existen indicios de intrusión, mientras el segundo se encarga de dar una respuesta de la intrusión en tiempo real. Pero con el tiempo se fue reduciendo el intervalo entre la ocurrencia del evento y su análisis en los HIDS, hasta que se logró gestionar los eventos en el instante de su registro.

Los sistemas de red implementados como parte de la pila de red de las máquinas protegidas ofrecen las mismas ayudas de respuesta inmediata con posibilidad de cancelar una conexión de los NIDS[8].

[2]Parte de la Lingüística que estudia el significado de los signos y de sus combinaciones, desde un punto de vista sincrónico.

D. Verificadores de integridad del sistema (SIV)

Un verificador de integridad es él encargado de buscar en el sistema las modificaciones que se realizaron de forma No autorizada, monitoreando este tipo de actividades a través de puertas traseras o (backdoors), que son huellas dejadas por el intruso a después de haber realizado los cambios, se pueden identificar claramente hechos como por ejemplo una entrada adicional en el fichero de contraseñas o un /bin/login que permite el acceso ante cierto nombre de usuario no registrado.

Uno de los problemas más grabes en los primero IDS era que detectaban el ataque, pero el administrador no era informado de manera inmediata, sino que este era informado a través de un mensaje horas después de la intrusión, motivo por el cual no se pudo hacer nada para frustrar el ataque. Esto sucedía porque los IDS eran pasivos, pero con el tiempo y notando las deficiencias que tenía el IDS lograron realizar las modificaciones necesarias para que éste se convirtiera en un IDS activo que les permitiera tomar acciones correctivas orientadas a detener ataques en el mismo instante en que se producían.

E. Monitores de registros (LFM).

Estos sistemas monitorean los archivos log generados por los programas llamados demonios de red de una máquina en busca de patrones que puedan indicar un ataque o una intrusión. Un ejemplo de monitor puede ser swatch (Vigilante simple), pero más habituales que él son los pequeños shellscripts (Sencillas órdenes de código), la mayoría de los administradores buscan entradas sospechosas como, por ejemplo, conexiones rechazadas en varios puertos provenientes de un determinado host, intentos de entrada remota como administrador entre otras, para esto comprueban periódicamente sus archivos de log.
Es posible que el sistema no sea capaz de detectar una determinada pretensión de ataque conocido al ser incapaz de encontrar la coincidencia con el patrón de búsqueda, si el atacante se las arregla para introducir pequeñas variaciones en su interacción con la máquina precisamente con el objetivo de evitar el IDS.

F. Sistemas de decepción.

Existen herramientas que incentivan al pirata a ingresar al sistema de manera no autorizada y atacar dicho equipo, lo que este no sabe es que todas sus actividades pueden quedar registradas en el sistema, este tipo de registros se logran por medio de mecanismos que simulan servicios con problemas de seguridad como por ejemplo Deception Toolkit (DTK) ó (honeypots).

Como se mencionó anteriormente se puede rastrear la conexión del atacante, esto se logra si se entretiene lo suficiente al hacker, pero ¿Existe algún riesgo con estas herramientas?, lamentablemente debemos afirmar que esta práctica es arriesgada, pues si el sistema decepción del atacante cuenta con un bug(error) que se desconoce, fácilmente el hacker podría aprovechar esto para acceder a la máquina.

Estos detectores de anomalías, generalmente son programados por expertos en el tema, o son programas que se han modificado a través del tiempo, pues pasaron por una fase de aprendizaje y finalmente una de modificación o perfeccionamiento. Mediante métodos estadísticos se intentará posteriormente comparar la información recibida en cada instante con el modelo de actividad permitida, y aquello que no esté conforme será clasificado como intrusión. Esta comparación se puede realizar por técnicas estadísticas, por sistemas expertos basados en reglas, con minería de datos [9], con redes neuronales [10], o con algún otro tipo de reconocimiento de patrones que pueda emitir con una certeza razonable si una determinada secuencia de eventos en un sistema forma parte del funcionamiento ordinario del mismo.

G. Requisitos de un IDS

Los sistemas de detección de intrusos deben cumplir ciertos requisitos para que su trabajo sea confiable y puedan desarrollar su labor de manera efectiva:
Una de las principales características es que un IDS debe mantenerse en constante funcionamiento, es decir este se debe ejecutar continuamente sin ayuda y sin supervisión de ninguna persona, si el IDS detectara un problema o intrusión en el sistema se debe informar a un operador o se debe enviar una respuesta automática, pero su funcionamiento habitual debe ser independiente por tal motivo no es necesaria la interacción con personas.
Además, es inevitable afirmar que las empresas dispuestas a contratar personas que desarrollen esta labor son muy escasas, pues el analizar logs o controlar los patrones del tráfico de una red generaría costos adicionales para la empresa por el personal innecesario que se necesitaría.

Sin embargo a la hora de utilizar los IDS es necesario preguntarnos ¿puede un algoritmo determinar perfectamente si un uso del sistema está correctamente autorizado? , pero también se genera el siguiente interrogante ¿sería capaz una persona de analizar en tiempo real todo el tráfico que llega a un servidor web mediano?, hay que tener presente que los sistemas de detección son mecanismos automatizados que se instalan y configuran de forma que su trabajo habitual sea transparente a los operadores del entorno informático.
Otra propiedad, y también como una característica a tener siempre en cuenta, es el grado de aceptación del IDS, al igual que sucedía con cualquier modelo de autenticación, los IDS han de ser aceptables para las personas que trabajan habitualmente en el entorno. Por ejemplo, no se puede introducir una sobrecarga considerable en el sistema donde un IDS vuelve más lenta una máquina, simplemente no se utilizará, ni generar una cantidad elevada de falsos positivos o

de logs, ya que entonces llegará un momento en que nadie se preocupe de comprobar las alertas emitidas por el detector. Por supuesto y esto puede parecer una necesidad, pero es algo que se hace más seguido de lo que se pueda imaginar, si para evitar problemas con las intrusiones simplemente se apaga el equipo o se desconecta de la red, se tendrá un sistema bastante seguro pero inaceptable.
Una tercera característica que debe tener en cuenta un IDS es que este debe adaptarse fácilmente a los cambios que surjan en su entorno, pues como bien se sabe todo ambiente laboral está sujeto a cambios día tras día y es necesario adaptarse a ellos y a los nuevos ataques que se puedan generar. Como ya es sabido, ningún sistema informático puede considerarse estático desde la aplicación más pequeña hasta el propio kernel de Unix. Si los IDS no son capaces de adaptarse rápidamente a esos cambios, están condenados al fracaso.
Al Igual que muchos sistemas los IDS deben presentar cierta tolerancia a fallos o capacidad de respuesta ante situaciones inesperadas, ya que se pueden producir cambios bruscos, de tal forma que un IDS debe encontrarse en la capacidad de responder siempre adecuadamente ante los mismos. Se Puede contemplar, por ejemplo, un reinicio inesperado de varias máquinas o un intento de engaño hacia el IDS. Hay que reflexionar que, si un atacante obtiene cambiar el comportamiento del sistema de detección y el sistema no se da cuenta, la intrusión nunca será notificada, con los dos graves problemas que eso implica: aparte de la intrusión en sí, la falsa sensación de seguridad que produce un IDS que no genera ninguna alarma.

Para que los IDS ayuden a evitar posibles ataques en la red es necesario mantener actualizado el Software del equipo, ya que como no depende del tipo de Sistema Operativo es muy fácil de instalar y actualizar, pero a la vez no se puede descuidar el cortafuego.

H. IDS basados en máquina

Estos IDS protegen una máquina, es decir un único sistema, su función es la de manejar distancias, de tal forma que trabaja bajo un proceso denominado background, que analiza la maquina periódicamente de tal forma que pueda encontrar factores importantes que indiquen que el sistema se encuentra amenazado por un hacker, alertando y tomando las medidas necesarias para proteger el sistema.

Al Igual que los NIDS se instalan en ciertos puntos de la red, los HIDS(Sistema de Detección de Intrusos en un Host) suelen instalarse en las maquinas que componen la red, estamos hablando entonces de las estaciones de trabajo y sus servidores, que a través de los sensores instalados en la maquina se puede obtener información importante del nivel semántico[3] como por ejemplo llamadas al sistema, eventos complejos dentro de aplicaciones de alto nivel, etc.

[3]Parte de la Lingüística que estudia el significado de los signos y de sus combinaciones, desde un punto de vista sincrónico.

Por otra parte, la tendencia actual al uso de conexiones encriptadas, de incuestionable interés para mejorar la seguridad de los sistemas, hace que un sistema que solo escuche la red disponga de muy poca información para distinguir el tráfico malicioso del aceptable.

Se ha encontrado que algunos Autores bibliográficos dividen el sistema de detección de intrusos basados en máquina, en varias categorías:

I. Periódicos o de tiempo real

Una de las diferencias entre los primeros HIDS y los NIDS es que el primero busca cada cierto periodo de tiempo elementos que le permitan identificar que existen indicios de intrusión, mientras el segundo se encarga de dar una respuesta de la intrusión en tiempo real. Pero con el tiempo se fue reduciendo el intervalo entre la ocurrencia del evento y su análisis en los HIDS, hasta que se logró gestionar los eventos en el instante de su registro.

Los sistemas de red implementados como parte de la pila de red de las máquinas protegidas ofrecen las mismas ayudas de respuesta inmediata con posibilidad de cancelar una conexión de los NIDS[8].

J. Verificadores de integridad del sistema (SIV)

Un verificador de integridad es él encargado de buscar en el sistema las modificaciones que se realizaron de forma No autorizada, monitoreando este tipo de actividades a través de puertas traseras o (backdoors), que son huellas dejadas por el intruso a después de haber realizado los cambios, se pueden identificar claramente hechos como por ejemplo una entrada adicional en el fichero de contraseñas o un /bin/login que permite el acceso ante cierto nombre de usuario no registrado.

Uno de los problemas más grabes en los primero IDS era que detectaban el ataque, pero el administrador no era informado de manera inmediata, sino que este era informado a través de un mensaje horas después de la intrusión, motivo por el cual no se pudo hacer nada para frustrar el ataque. Esto sucedía porque los IDS eran pasivos, pero con el tiempo y notando las deficiencias que tenía el IDS lograron realizar las modificaciones necesarias para que éste se convirtiera en un IDS activo que les permitiera tomar acciones correctivas orientadas a detener ataques en el mismo instante en que se producían.

K. Monitores de registros (LFM).

Estos sistemas monitorean los archivos log generados por los programas llamados demonios de red de una máquina en busca de patrones que puedan indicar un ataque o una

intrusión. Un ejemplo de monitor puede ser swatch (Vigilante simple), pero más habituales que él son los pequeños shellscripts (Sencillas órdenes de código), la mayoría de los administradores buscan entradas sospechosas como por ejemplo, conexiones rechazadas en varios puertos provenientes de un determinado host, intentos de entrada remota como administrador entre otras, para esto comprueban periódicamente sus archivos de log .
Es posible que el sistema no sea capaz de detectar una determinada pretensión de ataque conocido al ser incapaz de encontrar la coincidencia con el patrón de búsqueda, si el atacante se las arregla para introducir pequeñas variaciones en su interacción con la máquina precisamente con el objetivo de evitar el IDS.

L. Sistemas de decepción.

Existen herramientas que incentivan al pirata a ingresar al sistema de manera no autorizada y atacar dicho equipo, lo que este no sabe es que todas sus actividades pueden quedar registradas en el sistema, este tipo de registros se logran por medio de mecanismos que simulan servicios con problemas de seguridad como por ejemplo Deception Toolkit (DTK) ó (honeypots).

Como se mencionó anteriormente se puede rastrear la conexión del atacante, esto se logra si se entretiene lo suficiente al hacker, pero ¿Existe algún riesgo con estas herramientas?, lamentablemente debemos afirmar que esta práctica es arriesgada, pues si el sistema decepción del atacante cuenta con un bug(error) que se desconoce, fácilmente el hacker podría aprovechar esto para acceder a la máquina.

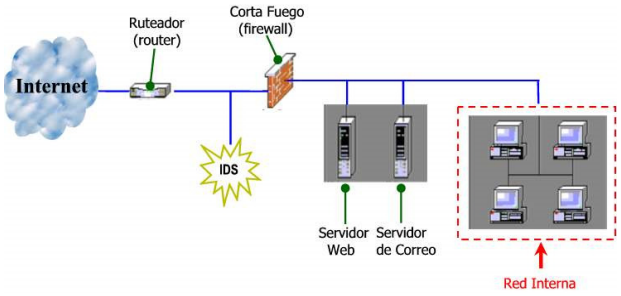
Estos detectores de anomalías, generalmente son programados por expertos en el tema, o son programas que se han modificado a través del tiempo, pues pasaron por una fase de aprendizaje y finalmente una de modificación o perfeccionamiento. Mediante métodos estadísticos se intentará posteriormente comparar la información recibida en cada instante con el modelo de actividad permitida, y aquello que no esté conforme será clasificado como intrusión. Esta comparación se puede realizar por técnicas estadísticas, por sistemas expertos basados en reglas, con minería de datos [9], con redes neuronales [10], o con algún otro tipo de reconocimiento de patrones que pueda emitir con una certeza razonable si una determinada secuencia de eventos en un sistema forma parte del funcionamiento ordinario del mismo.

M. Requisitos de un IDS

Los sistemas de detección de intrusos deben cumplir ciertos requisitos para que su trabajo sea confiable y puedan desarrollar su labor de manera efectiva:
Una de las principales características es que un IDS debe mantenerse en constante funcionamiento, es decir este se debe ejecutar continuamente sin ayuda y sin supervisión de ninguna persona, si el IDS detectara un problema o intrusión en el sistema se debe informar a un operador o se debe enviar una respuesta automática, pero su funcionamiento habitual debe ser independiente por tal motivo no es necesaria la interacción con personas.
Además, es inevitable afirmar que las empresas dispuestas a contratar personas que desarrollen esta labor son muy escasas, pues el analizar logs o controlar los patrones del tráfico de una red generaría costos adicionales para la empresa por el personal innecesario que se necesitaría.

Sin embargo a la hora de utilizar los IDS es necesario preguntarnos ¿puede un algoritmo determinar perfectamente si un uso del sistema está correctamente autorizado? , pero también se genera el siguiente interrogante ¿sería capaz una persona de analizar en tiempo real todo el tráfico que llega a un servidor web mediano?, hay que tener presente que los sistemas de detección son mecanismos automatizados que se instalan y configuran de forma que su trabajo habitual sea transparente a los operadores del entorno informático.
Otra propiedad, y también como una característica a tener siempre en cuenta, es el grado de aceptación del IDS, al igual que sucedía con cualquier modelo de autenticación, los IDS han de ser aceptables para las personas que trabajan habitualmente en el entorno. Por ejemplo, no se puede introducir una sobrecarga considerable en el sistema donde un IDS vuelve más lenta una máquina, simplemente no se utilizará, ni generar una cantidad elevada de falsos positivos o de logs, ya que entonces llegará un momento en que nadie se preocupe de comprobar las alertas emitidas por el detector. Por supuesto y esto puede parecer una necesidad, pero es algo que se hace más seguido de lo que se pueda imaginar, si para evitar problemas con las intrusiones simplemente se apaga el equipo o se desconecta de la red, se tendrá un sistema bastante seguro pero inaceptable.
Una tercera característica que debe tener en cuenta un IDS es que este debe adaptarse fácilmente a los cambios que surjan en su entorno, pues como bien se sabe todo ambiente laboral está sujeto a cambios día tras día y es necesario adaptarse a ellos y a los nuevos ataques que se puedan generar. Como ya es sabido, ningún sistema informático puede considerarse estático desde la aplicación más pequeña hasta el propio kernel de Unix. Si los IDS no son capaces de adaptarse rápidamente a esos cambios, están condenados al fracaso.
Al Igual que muchos sistemas los IDS deben presentar cierta tolerancia a fallos o capacidad de respuesta ante situaciones inesperadas, ya que se pueden producir cambios bruscos, de tal forma que un IDS debe encontrarse en la capacidad de responder siempre adecuadamente ante los mismos. Se Puede contemplar, por ejemplo, un reinicio inesperado de varias máquinas o un intento de engaño hacia el IDS. Hay que reflexionar que si un atacante obtiene cambiar el comportamiento del sistema de detección y el sistema no se da cuenta, la intrusión nunca será notificada, con los dos graves problemas que eso implica: aparte de la intrusión en sí, la falsa sensación de seguridad que produce un IDS que no

genera ninguna alarma. Es claro que los IDS tienen diferentes posiciones dentro de la red y aportan un sinnúmero de características desiguales. Por lo tanto se puede observar diferentes posibilidades en una misma red, por ejemplo se puede tener una red donde un cortafuego fracciona la Internet de la zona desmilitarizada (DMZ– Demilitarized Zone), y otro que divide la DMZ de la intranet de la organización como se muestra en el dibujo 1. Por zona desmilitarizada se entiende la zona que se debe mostrar al exterior, la zona desde la cual se muestra los servicios o productos [16]:

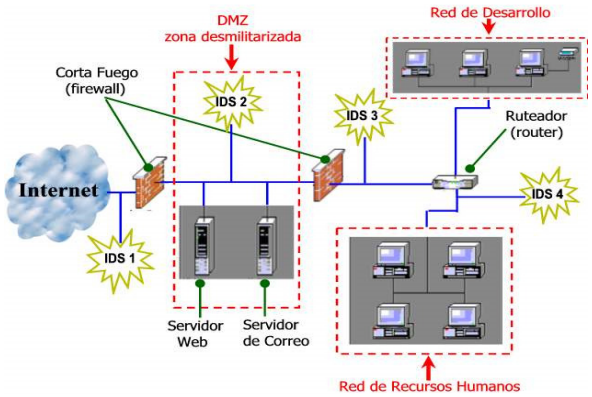


Dibujo 1: Red con IDS simple
Fuente: Carlos Jojoa[3]

Para descubrir el inicio de una acción hacking se debe instalar un IDS antes del cortafuego exterior, este procedimiento ayudara a descubrir y rastrear los puertos de reconocimiento que señala el comienzo de una anomalía en la red, aun que se tenga una ventaja con el aviso prematuro, se puede presentar una numerosa cantidad de alerta innecesarias con el peligro que no sean tomadas en cuenta.

Una manera obtener una base de datos de los atacantes del NIDS, es instalar IDS en zona desmilitarizada DMZ (servidor web y servidor de correo) este nos permite controlar todos los ataques dirigidos a los sistemas del servidor web y el servidor de correo y con las posibilidades de utilizar cortafuegos para el bloqueo de tráfico.
Otra característica de un NIDS dentro de la red es que permite monitorear el tráfico por dentro y por fuera de esa red, por ejemplo recursos humanos podría hacer un seguimiento de lo que está pasando dentro de la red tanto interno como externo .
A continuación, se muestra una red completa de NIDS visualizar el segundo dibujo:

[3,4]http://share.pdfonline.com/969311b040e14ceea273c628772b84f9/Carlos%20Jojoa%20corregido2.htm



Dibujo 2: Red completa con IDS
Fuente: Carlos Jojoa[4]

Como se puede observar en el dibujo 2 el IDS1 se emplea para avisar del rastreo de puertos, si existe puertos envías un "aviso" en ambos sentidos eso lo podemos ver cuando se utiliza un ping a la dirección que se emite paquetes esto permite mantener un control de seguridad en la organización.

El IDS2, su función es de monitorear la zona desmilitarizada y analizar el tráfico que reciben tanto el servidor web como el servidor de correo.

Los función del IDS3 y el IDS4 controlar la red interna de la red, el que controla la seguridad de una parte de la red en este caso una sub red es el IDS4 , por ejemplo la parte de recurso humanos , además estos dos NIDS internos (el IDS3 y el IDS4) poseen sensores que capturan la información y se envía a un estante donde se analiza y se ejecuta cálculos [13]

N. Herramienta SNORT como alternativa para la Detección de Intrusos.

Esta herramienta sirve para prevenir intrusiones de la red abierta y el sistema de detección (IDS / IPS) desarrollado por Sourcefire.
La combinación de los beneficios de la firma, el protocolo y la inspección anomalía basado en Snort[5] es el mayor despliegue IDS / IPS de tecnología en todo el mundo. Con millones de descargas y cerca de 400.000 usuarios registrados, Snort ha convertido en el estándar de hecho para IPS. Para descarga y conocer la herramienta se debe referenciar a [14].
Short en una potente herramienta que sirve para análisis de paquetes y detector de intrusos basados en red (se monitorea todo un dominio de colisión), este tipo de software flexible ofrece una serie de

[5]http://www.snort.org
oportunidades como la capacidad de almacenamiento de sus bitácoras en archivo de texto, en base de datos como MySQL, además se puede ejecutar un motor de detección de ataques y barrido de puertos, además
permite realizar un registro de todas las alertar que se presente durante una anomalía, igualmente responde a cualquier suceso previamente definido.

Este software de IDS, es un lenguaje muy sencillo ya que contiene reglas flexibles y potentes, su instalación es muy simple ya que tiene una serie de filtros o reglas este programa puede desempeñarse
como analizador ya que permite monitorear lo que ocurre en la red desde la consola en tiempo real, esta información(registro de paquetes) se puede guardar en archivos logs para su posterior análisis

Snort está disponible con licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux.
Dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas. Una de las características más importantes es que posee un subsistema flexible de firmas de ataques, además de tener una base de datos de ataques que se actualiza constantemente la cual se puede modificar desde el internet. Cada vez que se presente un ataque los usuarios tienen la capacidad de crear firmas basadas en las características del ataque de la red, para sí poder tener informados a todos los usuarios, para que así todos los usuarios se puedan beneficiar.

La ética de comunidad y de compartir ha convertido a Snort en uno de los IDS de red más populares, actualizados y robustos. Tomado de [15].

IV. CONCLUSIONES

- Los Sistemas de Detección de Intrusos son una herramienta más que se puede utilizar para mejorar la seguridad de los sistemas de Información, además de ser una de las más utilizadas en la actualidad y robustas.
- Estos IDS no reemplazan a los cortafuegos, ni evitan nuestra responsabilidad de estar constantemente actualizando las máquinas y hacer todo lo necesario respecto a configuraciones, y medidas necesarias de prevención y de protección ante todo tipo de ataques.
- Los IDS, en especial si están encargados de extraer información que coincida o tenga propiedades entre sí, es necesario mantenerlos cuidadosamente actualizados.
- Las alertas que presenten deben ser meticulosamente examinadas para tomar las medidas apropiadas lo antes posible de ahí la importancia de que los sistemas tengan mínima tasa de los llamados falsos positivos [6].
- Ha habido críticas a los IDS debido a que en principio un IDS detecta intrusiones pero no toma medidas correctivas. Esto ha llevado a algunos expertos a afirmar que los IDS no resultan eficaces, sobre todo considerando los costos de implantación y mantenimiento, y que su futuro puede ser evolucionar hacia los IPS (Sistemas de Prevención de Intrusiones)[11], productos combinados con cortafuegos que sí son capaces de adoptar medidas correctivas inmediatas (cortar conexiones, cambiar reglas de filtrado, etc.).
- Los sistemas de detección de intrusos son los elementos que necesita un administrador para obtener una mayor visibilidad de lo que ocurre en su red mostrando lo que está circulando por ella.
- Antes de implementar un sistema de detección de intrusiones, se recomienda que nos aseguremos de tener una política de seguridad bien definida que cubra lo que está y lo que no está permitido en nuestros sistemas y nuestras redes.
- Finalmente deberíamos realizar auditorías regulares que confirmen que nuestras políticas están en vigencia y que nuestras defensas son las adecuadas para el nivel de riesgo al que estamos expuestos.
- Por ejemplo, la ejecución de rastreos comunes de red desde el exterior y desde dentro sobre los Firewalls de la organización para determinar cuáles son los puertos que están abiertos y cuanta información se le escapa a nuestros Firewalls y routers.
- Es necesario disponer de personal capacitado o soporte externo calificado para que pueda analizar las alertas conseguidas por las herramientas de seguridad y que estos recursos humanos son costosos pero de vital importancia si se desea contar con un sistema de detección de intrusos eficaz.[12].
- En el mercado existe una amplia gama de IDS desde el más costoso hasta lo más económicos, pero se debe tener en cuenta la capacidad del administrador (capacitación) para poder actualizar la base de datos del IDS además, de ser capaz de reconocer los diferentes tipos de ataques y sus variaciones. Otra cosa a tener en cuenta los costos cuando se incluye hardware especializado, además de los recursos humanos requeridos, la utilización de IDS en las organizaciones debería estar integrado en la política de seguridad de las mismas, en completa coordinación con los demás recursos como los cortafuegos [13].

[6] **Falso positivo.** En Informática es un error por el cual un software de antivirus informa que un archivo o área de sistema está infectada, cuando en realidad el objeto está limpio de virus.

REFERENCIAS

[1]. Rouse, M. (2008, Octubre). Hids/Nids sistema de detección de intrusiones en el host y los sistemas de detección de intrusiones de red. Sitio Web: http://searchsecurity.techtarget.com/definition/HIDS-NIDS

[2]. Tux. (2012, Febrero 06). Qué son y para qué sirven los Firewalls. Sitio Web: http://www.g3ekarmy.com/que-son-y-para-que-sirven-los-firewalls/

[3]. Díaz Vizcaíno, L.M. (2005). Sistemas de Detección de Intrusos. Tomado de. Universidad Carlos III de Madrid. Sitio Web: http://www.it.uc3m.es/~lmiguel/ids2.pdf

[4]. Villalón Huerta, A. (2005, Mayo). Sistemas de Detección de Intrusos. Seguridad en Unix y Redes v.

2. (Capítulo 18). Tomado de: http://shutdown.es/aptes-ids.pdf

[5]. Gonzalez Gómez, D. (2003, Julio). Sistema de Detección de Intrusiones. Sitio Web: http://www.dgonzalez.net/pub/ids/trans/IDStBN.pdf

[6]. Red, Iris. (2002). Sistema de Detección de Intrusos. Sitio Web: http://www.rediris.es/cert/doc/unixsec/node26.html

[7]. Ventura Ruiz, L. (1999). Artículos Invitados. Cortafuegos. Sitio Web: (http://www.iec.csic.es/criptonomicon/articulos/expertos35.html).

[8]. Bauer, M. (2001). swatch: Automated Log Monitoring for the Vigilant but Lazy. Sitio Web: http://www.linuxjournal.com/article/4776

[9]. Becerro Martínez, A. (2005). Introducción a Shell Script. Sitio Web: http://www.elviajero.org/antoniux/tutos/shell_intro.pdf

[10]. Arellano, G. (2005, Marzo). Seguridad Perimetral. Sitio Web: http://cisco.frcu.utn.edu.ar

[11]. Gerometta, O. (2012, Agosto). Dominio de colisión - Dominio de broadcast. Sitio Web: http://librosnetworking.blogspot.com/2012/08/dominio-de-colision-dominio-de-broadcast.html

[12]. Salinas, R. (2005). Revista del Instituto Tecnológico de Informática. Sitio Web: http://www.iti.es/media/about/docs/tic/06/2005-02-intrusos.pdf

[13]. Kroll – Quantil. (2012, Marzo). Introduccion a la Mineria de Datos. Sitio Web: http://www.quantil.com.co/qt/images/stories/presentaciones/intro%20MD.pdf

[14]. García Báez, P. (2011, Septiembre). Introducción a las redes neurales y su aplicación. Sitio web: http://www.iac.es/sieinvens/SINFIN/Sie_Courses_PDFs/NNets/confiac.pdf

[15]. Network Juniper. (2013, Enero). Sistema de prevención de intrusiones (IPS). Sitio web: http://www.juniper.net/es/es/products-services/software/router-services/ips/#features

[16]. Déjà Vu. (2003, Enero). IDS - Intrusion Detection System. Sitio web: http://www.nvram.com.ar/viewtopic.php?f=31&t=2179

[17]. Sin autor. Sistema de Detección de Intrusos. Sitio Web: ttp://www.uv.es/~montanan/redes/trabajos/IDSs.doc

[18]. Sourcefire, Inc. (2010). Snort. Sitio Web: http://www.snort.org

[19]. Wikipedia. (2013. Marzo). Sistemas Detectores de Intrusos y Snort. Sitio Web: http://es.wikipedia.org/wiki/Snort