UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CIENCIAS

SISTEMAS DE DETECCIÓN DE INTRUSOS
UN PREÁMBULO AL MONITOREO DE SEGURIDAD DE REDES.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO EN CIENCIAS DE LA COMPUTACIÓN

P R E S E N T A :

SAMUEL MARCELO REYNA SILVA

TUTOR

M. EN C. LEOBARDO HERNÁNDEZ AUDELO

2010

AGRADECIMIENTOS.

Antes de comenzar quiero agradecer al principal sustento en mi vida, que es mi madre Delia, ya que nunca perdió las esperanzas en mí, para ver terminado este trabajo. También a mis hermanos Carolina, Cecilia, Raúl y Deborah que siempre han estado conmigo para ayudarme y darme un consejo. Ellos son mí familia que amo tanto.

Doy las gracias de una manera muy especial al M. en C. Leobardo Hernández Audelo, quien como amigo me enseñó a superar mis miedos y como profesor a corregir mis errores, sin él nunca hubiera culminado este trabajo.

Al Dr. Enrique Daltabuit Godas agradezco de una manera muy afectuosa, por haberme encaminado hacia el mundo del arte de la intrusión el cual no habría comprendido sin sus consejos.

Finalmente, gracias al Dr. José de Jesús Vázquez Gómez. por su paciencia y por sus valiosos comentarios que ayudaron a enriquecer este trabajo.

Hoja de Datos del Jurado

1. Datos del alumno
Reyna
Silva
Samuel Marcelo
57950641
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
092376209

2. Datos del tutor
M en C
Leobardo
Hernández
Audelo

3. Datos del sinodal 1
Dr
Sergio
Rajsbaum
Gorodezky

4. Datos del sinodal 2
Dra
Hanna
Jadwiga
Oktaba

5. Datos del sinodal 3
Dr
Enrique
Daltabuit
Godas

6. Datos del sinodal 4
Dr
José de Jesús
Vázquez
Gómez

7. Datos del trabajo escrito
Sistemas de Detección de Intrusos Un preámbulo al Monitoreo de Seguridad en Redes
105 p
2010

INDICE

CAPÍTULO 3.

Monitoreo de la Seguridad en Redes y Detección de Intrusiones.

CAPÍTULO 4.

Modelo de un Sistema Detector de Intrusiones.

PRÓLOGO.

El crecimiento de las TIC sigue subestimando las expectativas que se tienen acerca de la Internet, donde existe un mundo virtual que ya es necesario para la investigación, economía, comunicaciones etc. Es ahora tan común tener la necesidad de conectarse a Internet, que es un tanto difícil darse cuenta de los problemas que ha desencadenado su crecimiento.

Una guerra en la Internet se ejecuta en este momento, a cada instante y es llamada infoguerra, la cual va en conjunto con el ciberterrorismo, donde gente sin nombre “hackers” aplica estrategias de guerra y hace intrusiones en las redes para generar conflictos sociales, económicos y políticos a nivel mundial.

Como ejemplo se tiene que a principios de los años 80´s la National Security Agency (NSA) interceptaba mensajes encriptados de Libia, Irán y decenas de países, gracias a sus tratos con la empresa Suiza Crypto AG, que vendía programas de criptología con puertas traseras sólo conocidas por la agencia norteamericana y que a su vez pone en marcha la red Echelon, destinada a espiar las comunicaciones telefónicas, por satélite e Internet en Europa. Descubierta su existencia oficialmente en 1998, su principal misión parece ser el espionaje económico.

Cada vez es más complejo evitar que la información no sea susceptible de algún ataque, atacante o que las redes no sufran alguna vulnerabilidad por causas de malas administraciones. A esto se refieren dos problemas de la seguridad de la información.

Primero es la manera de establecer mecanismos para que la información no sea legible, esto se logra con Criptografía [11], ya que si alguien logra tener acceso a ella, obviamente hará mal uso de ella. Se sabe que no es totalmente la culpa de los administradores de los sistemas, algunos de ellos ya concientes de los problemas que le atañen, implementan políticas o reglas para tener un mejor control de la información y los dispositivos de red. Segundo se tiene el problema de los protocolos de la suite TCP/IP que por construcción no son seguros, ya que cuando se comenzaron a concebir, no se percataron de su demanda masiva y de su susceptibilidad para ser atacados.

Ya que se mencionan las políticas o reglas de administración, el control de acceso se implementa como política, que será la primera frontera a vencer por el enemigo, pero esto no es suficiente. El concepto por sí mismo es sencillo, pero en ocasiones llega a ser difícil de implementar, ya que el factor humano es decisivo para poder tener éxito.

Existen herramientas y técnicas que ayudan a controlar problemas hechos por causas humanas tales como los detectores de intrusos, estas son herramientas que ayudan a monitorear eventos que ocurren en nuestro sistema de red, y analizan las señales que son lanzadas por problemas en la seguridad.

Se puede pensar análogamente en sistemas de monitoreo de otras áreas como, sistemas bancarios donde suena una alarma cuando alguien no autorizado ingresa o intenta introducirse. También los hay a gran escala en la defensa militar donde las alarmas son lanzadas según la categoría que se tenga. Esos sistemas están compuestos de funciones centinelas, alarmando y alertando a los responsables, cuando las actividades de interés ocurren.

La detección de intrusiones es una tecnología relativamente joven, como una rama no criptológica de la seguridad en general. La mayor parte de la investigación y el desarrollo de la detección de intrusos se ha hecho desde 1980. Sin embargo, este desarrollo ha producido gran rango de soluciones y estrategias como solución para obtener una verdadera ganancia en la detección de intrusiones.

Aun existe una brecha teórica y práctica entre los aspectos de la detección de intrusiones. Esta situación crea todo tipo de tentaciones para los investigadores y desarrolladores.

Este trabajo de tésis se desarrolla en 6 capítulos en los que se dará una descripción de la detección de intrusiones, comenzando con la ideología del Arte de la Intrusión y finalizando con un modelo basado en entropía para la detección de anomalías que es una de las técnicas para la detección de intrusiones. Modelo que hoy en día se encuentra en desarrollo en la DARPA.

En el primer capítulo, se describirá como la infoguerra que actualmente se encuentra en la Internet está ya acompañada de una ideología más seria y más profunda basada en las máximas del estratega de guerra Sun Tzu.

En el segundo capítulo, se estudiará la detección de intrusos desde su inicio como la auditoría de seguridad en redes, donde los administradores de red hacían un gran esfuerzo por leer bitácoras para juntar grandes volúmenes de información para así poder etiquetar y evaluar situaciones de riesgo. También se llegará a una definición formal de la detección de intrusiones y se estudiará su madurez como una técnica del monitoreo de seguridad en redes.

En los capítulos posteriores se estudiarán varios modelos de detección de intrusiones enfocados hacia las anomalías, que es una de las partes de más estudio de estos modelos.

La construcción del *capítulo 2*, que es el tema principal de este trabajo de tésis, es motivado por algunas preguntas: ¿Cómo se puede saber si un sujeto o usuario está haciendo mal uso de los recursos de la red y de programas?, ¿Cómo se

puede saber si alguien está en contacto con información que no le corresponde? ¿Cómo se puede detectar a los intrusos?; ¿Se podrá saber en tiempo real?.

Afortunadamente todas esas preguntas tienen respuesta, y los encargados de responder, son las personas que se dedican al Monitoreo de Seguridad de Redes. Los expertos la definen como: la recolección, análisis y notificación de indicaciones y advertencias, con objeto de detectar entradas y responder a ellas [1].

El tercer capítulo tiene como finalidad describir las técnicas del Monitoreo de Seguridad de Redes. La cual es una área muy grande. Aquí se describen: procesos de seguridad, detección de intrusiones y respuestas a las mismas y también se describen las zonas de monitoreo. Esto es importante ya que cuando se instala cualquier programa para monitoreo, nunca se revisa si se ha instalado en el lugar correcto y si está configurado. Aún más drástico es si los administradores de redes o el personal que se dedica a monitoreo no mantiene al día las herramientas dedicadas a la seguridad de la red [3], y esto porque estas mismas pueden ser susceptibles de vulnerabilidades y hasta dar una terminal con privilegios de súper usuario.

Existen un sinnúmero de herramientas de software libre para monitoreo de: Datos de Contenido Completo, Análisis Adicionales de Datos, Datos de Sección, Datos Estadísticos, Datos de Alertas, sin embargo, por cuestiones de tiempo y alcance de este trabajo, sólo se mencionan 3 de manera breve: Tcpdump [3], Snort [15] y Ethereal [13], cuya finalidad es ver distintas formas para la captura de tráfico. Estas herramientas son muy populares en el “underground”, donde su buen manejo traerá muchas satisfacciones a los administradores de red.

El Monitoreo de Seguridad de Redes recomienda algunas prácticas dentro de sus procesos que son: *La estimación*, que está basada en políticas de seguridad definidas, donde se implementan muros como *protección*, es aquí donde entra el control de acceso, y entonces se espera *detectar* quién quiere penetrar el muro y por lo tanto se tendrá una *respuesta,* si llegaran a franquear dicho muro [1].

Todas estas recomendaciones hacen que un profesional de la seguridad deba de ser experto en cinco disciplinas: Armas y tácticas, Telecomunicaciones, Administración de Sistemas, Scripts y programación, Gestión de reglamentos. Aquí se hace la recomendación de agregar una sexta disciplina más: La criptografía*,* ya que ésta dará una visión mucho más general de cómo trabajan los protocolos que implementan las herramientas de monitoreo.

Ya que se ha hablado y se han desarrollado las técnicas del monitoreo de seguridad en redes, es necesario hablar de la detección de intrusos. Para ello en el capítulo cinco se describe con detalle uno de los modelos para la detección de intrusos, que dio una gran disputa a un gran número de productos, modelos y fue el propuesto por Dorothy Denning [5], de esté se hace una descripción a detalle.

El Sistema Experto para la Detección de Intrusiones es un sistema en tiempo real para la detección de intrusiones que está motivado por los siguientes 4 factores:

i) Los fallos de seguridad que existen en los sistemas y que los hacen susceptibles frente a intrusiones, penetraciones y otras formas de abuso. Por lo tanto buscar y corregir todas estas deficiencias no resulta una buena idea por razones técnicas y económicas.

ii) Los sistemas existentes, que tienen fallos conocidos, no son fáciles de reemplazar por sistemas más seguros, sobre todo porque estos sistemas poseen características atractivas que faltan en los sistemas más seguros, o bien no se pueden reemplazar por cuestiones económicas.

iii) El desarrollo de sistemas que sean absolutamente seguros es extremadamente difícil, si no es que imposible.

iv) Incluso los sistemas más seguros son vulnerables frente a abusos cometidos por personal interno que hace un uso inadecuado de sus privilegios.

De aquí se describe un mecanismo que es capaz de detectar intrusiones mientras ésta se está produciendo, y este sistema no es dependiente de la vulnerabilidad.

Estos cuatro argumentos son excepcionales y relevantes para el entorno de la seguridad, así que Denning y Neumann diseñan el IDES (Intrusión Detection System Expert) para monitorear la actividad de sistemas mientras que ésta se registra en el bloque de Registros de Auditoría. En el proceso se examinarán los registros a medida que estos se generan, se actualizarán los perfiles que caracterizan el comportamiento de los sujetos (usuarios, proceso, el sistema mismo) con respecto a los objetos (archivos, órdenes, etc.) y determinará si la actividad actual es anormal con respecto a los perfiles. Cuando IDES detecte una anomalía determinará si debe alertarse de inmediato al personal que está monitoreando.

Como una parte más actual y siguiendo el desarrollo para el *capítulo 6,* se describe el modelo basado en entropía, de los autores Yu Gu, Andrew McCallum, Doc Towsley [19]. Aquí se explota la idea de la detección de anomalías basadas en el comportamiento, usando técnicas de entropía, donde se verá que es capaz de detectar anomalías con el cambio abrupto del tráfico.

Para el sexto capítulo se desarrolla un capítulo previo donde se describen algunos conceptos matemáticos de la Teoría de la Información, para entender de una manera más cómoda lo que es la entropía en la información.

El acercamiento de la entropía máxima descrita en el trabajo exhibe muchas ventajas: Primero, este provee a los administradores una vista multidimensional del tráfico de red por la clasificación de paquetes de acuerdo al conjunto de atributos que estos traen. Segundo, este detecta anomalías que causan un

abrupto cambio en el tráfico de red, como un incremento en el tráfico lento. Tercero, provee información del tipo de anomalía detectada.

Pero la gran riqueza está en que el método requiere sólo una cantidad constante de memoria y consiste solamente en contar los paquetes en el tráfico y lo hace de la siguiente manera: el desarrollo está dividido en dos fases. La fase número uno es para tomar una distribución de lo que se tomará como una base de aprendizaje y la fase dos es para detectar anomalías en el tráfico observado. En la primera fase, se dividen paquetes en clases de paquetes multidimensionales de acuerdo al protocolo y número de puerto destino. Esas clases de paquetes, sirven como el espacio del dominio de probabilidades. Entonces la distribución de lo que se tomó base de los paquetes es determinada por el aprendizaje un modelo de densidad del tren de datos usado para estimar la entropía máxima.

Durante la segunda fase, se da una traza de tráfico de red observado como entrada. Se calcula la entropía relativa de las clases de los paquetes en las trazas de tráfico observado con respecto a la distribución. Las clases de los paquetes contribuyen significativamente a la entropía relativa para ser grabados. Si ciertamente las clases de los paquetes continúan contribuyendo significativamente a la entropía relativa, se generan anomalías y advertencias y se reportan las clases de correspondientes. Esto corresponde a la información de las clases de paquetes que revela el protocolo y el número de puerto destino relacionado a la anomalía.

Hay muchas personas que dicen hacer monitoreo de seguridad en redes y pasan bastante tiempo tras el monitor viendo el tráfico de red y revisando herramientas para probar cual les funciona mejor, sin embargo nunca revisan la teoría, para así tener una idea más general de lo que pueden hacer o qué medidas se deben de tomar en caso de hallar alguna anomalía.

La recomendación es desde luego revisar la teoría del monitoreo de seguridad en redes para saber qué medidas tomar en caso de hallar alguna anomalía o intrusión y claro está, la revisión de modelos abstractos de Detectores de Intrusiones y Anomalías sin dejar pasar por alto la evaluación de herramientas que se utilizan para monitorear el tráfico de red. De esta manera se podrán evaluar las violaciones a las políticas de seguridad de una manera más precisa.

S. Reyna S.

Capítulo 1
La Infoguerra en la Internet.

Resumen.

Hoy en día, los *hackers* juegan entre ellos a estar siempre un paso adelante del otro, compiten todo el tiempo para saber quién hace la mejor intrusión *concepto que se definirá con toda propiedad en los capítulos siguientes*, esto indica que, cada vez son más hábiles, ya que ahora aplican diferentes mecanismos de ataque y estrategias sofisticadas de guerra. Tal es el caso de las máximas citadas en el famoso libro "*El Arte de la guerra" del general chino Sun Tzu, creado hace ya 2500 años*, éste no es únicamente un libro de práctica militar, sino un tratado que enseña la estrategia suprema de aplicar con sabiduría el conocimiento de la naturaleza humana en los momentos de confrontación, que renace hoy con los principios estratégicos aplicados a la "*infoguerra"* que está ejecutándose todo el tiempo en el ciberespacio de la Internet.

1.1 El Arte de la Infoguerra.

El arte de la guerra menciona: "*Un líder hábil es el que logra derrotar las tropas del enemigo sin luchar*", así también "*el que captura ciudades sin sitiarla*s".

Es decir "*Todo el arte de la guerra se basa en el engaño*" no se podría dejar de pensar en la "*ingeniería social*" establecida ahora como el arte derivado de las máximas de Sun Tzu.

La filosofía del arte de la guerra ha ido más allá de los límites estrictamente militares, aplicándose a los negocios, los deportes, la diplomacia, el comportamiento personal e incluso en la infoguerra de la Internet.

Desde los traviesos hackers hasta los misteriosos magos informáticos al servicio de alguna potencia agresora, se va configurando la nómina de enemigos reales y potenciales en la infoguerra, en la que también se generan mecanismos de defensa y contraataque.

La expresión básica de la infoguerra viene a ser la invasión o intrusión en una red de computadoras por parte de un enemigo, llámese hacker, lammer, cracker, etc. Que está implicado en destruir un sistema de información, sustraerle sus datos o alterarlos con propósitos que generaran escenarios de conflicto.

En la infoguerra no se lanzan bombas ni se disparan balas sino que se intervienen correos electrónicos, se controla el contenido de las comunicaciones, se lanzan falsos rumores o se distribuyen falsos mensajes se influye sobre el estado de ánimo del adversario, etc. Es la guerra de la información que tanta influencia y

poder ha demostrado tener en muchos conflictos a lo largo de la historia y que ahora tiene su máximo exponente y expresión en la Internet.

En Estados Unidos, el Instituto para Estudios Avanzados de Guerra de Información [35] define a la Infoguerra como: *"el uso defensivo y ofensivo de la información y de sistemas de información para explotar, corromper o destruir la información"* y los sistemas de información de un adversario, protegiendo los propios y agrega que "*este tipo de acciones apuntan a lograr ventajas sobre contrincantes militares o de negocios*".

El punto de partida de esta guerra podría situarse en 1980, cuando se establece la alianza entre las telecomunicaciones y la informática, que permite crear vastos sistemas de información hasta llegar a la Internet.

Desde entonces, en el espacio virtual abundan historias de intrusión que responden a las definiciones de esta guerra, aunque no debe perderse de vista que se trata de un terreno también propicio para la paranoia. En otras palabras, se corre el riesgo de atribuir a terceros todo virus que infecte a una red de organismos de defensa, sistemas financieros o gobiernos y magnificar supuestas vulnerabilidades, lo cual llevará a la respuesta no deseable de extremar controles y censuras, llamadas políticas de seguridad.

1.2 Los Niveles de la Infoguerra.

Se dice que existen tres niveles de *infoguerra*, siendo el más elemental el de los hackers, que es también el de más compleja delimitación, pues allí es fácil confundir una simple jugarreta con una agresión.

El segundo nivel es el de la *ciberguerra*, con acciones que no difieren mayormente de las de los hackers, en cuanto a invadir sistemas para inutilizarlos *"Intrusión"* o corromperlos con la introducción de virus o datos errados, o simplemente robar información. Pero en la "*ciberguerra"*, los ataques no son actos aislados como los de los hackers y se realizan con un objetivo preciso: "*interferir o destruir los sistemas de información de un enemigo, que puede ser un país o una corporación*".

El tercer y definitivo nivel, de "*netwar"* o guerra de redes, tendría como propósito atacar a toda una nación, no sólo afectando los sistemas de información, sino también a la población que habita en ese territorio. Se usaría la "*Intrusión*" para la interrupción de servicios y la diseminación de mensajes destinados a confundir a la opinión pública, canalizando toneladas de propaganda.

En esté nivel de *netwar* se puede pensar que alguien intenta confundirnos utilizando alguna estrategia de guerra como la siguiente:

Si las tropas enemigas se hallan bien preparadas tras una reorganización, intenta desordenarlas. Si están unidas, siembra la deserción entre sus filas. Ataca al enemigo cuando no está preparado, y aparece cuando no te espera. Estas son las claves de la victoria para el estratega de guerra, o *infoguerra.*

Con situaciones como esta, Internet ha tornado realidad el sueño del guerrero: vencer sin combatir, controlar al enemigo sin exponerse uno mismo. La innovación imparable en tecnologías de la información y las comunicaciones (TIC), especialmente las basadas en ordenadores e Internet, ha creado el potencial de una nueva forma de hacer la guerra en la era de la información, claramente "*infoguerra".*

En los últimos años, la "*infoguerra"* está invadiendo la red de redes. La dependencia creciente de las TIC hacia la que camina sin retorno nuestra sociedad la convierte precisamente en blanco vulnerable de ataques a través de redes: virus de ordenador que paralicen sistemas financieros, ataques a sistemas de distribución de energía eléctrica, denegación de servicio en centros de comunicaciones móviles, incomunicación de torres de control aéreo.

En Medio Oriente, Europa del Este y Asia se están sintiendo los primeros embates de la infoguerra. Aunque mal entendida por el mito y la ciencia ficción, los conflictos bélicos que tienen lugar en estas regiones del planeta pronto encuentran su eco en Internet: ataques de crackers coordinados o no coordinados en India, Pakistán, Israel, China...

Tradicionalmente, los objetivos militares han sido las centrales de energía y las infraestructuras de transportes y comunicaciones.

Bastaría con atacar o realizar una pequeña intrusión en los mercados financieros internacionales, como por ejemplo el Nasdaq, para desestabilizar sectores enteros de la economía mundial. Socavar sistemas de democracia electrónica, para sentar en el poder a partidos de ideología afín. Alterar el funcionamiento de centros de control del suministro energético.

Las posibilidades de éxito y autofinanciación de la infoguerra son alarmantes; su efectividad, devastadora, y su costo, mínimo. A medida que nuestra sociedad se informatizan y sus sistemas se vuelven más complejos, crece su vulnerabilidad ante ese tipo de ataques. Y la situación empeorará con el tiempo, a menos que las inversiones en defensa contra la infoguerra crezcan paralelas a la digitalización de la sociedad.

El valiente puede luchar, él cuidadoso puede hacer de centinela, y el inteligente puede estudiar, analizar y comunicar.

Los hacker atacan y se introducen en las redes haciendo que los adversarios se agoten, para eso se borran las huellas "*bitácoras y registros*" de esta manera dificultan la auditoría. Interrumpen sus provisiones de vida "*Ancho de banda*"

cortan sus vías de aprovisionamiento "*manipulan los firewalls*". Aparecen en lugares críticos "*dejan mensajes o documentos de texto burlándose y amenazando*". Atacan en donde menos se lo esperan "*Máquinas secretariales, gerenciales, etc.*" Si se llega a detectar la intrusión, hay que acudir al rescate.

La Infoguerra en sus tres vertientes tiene una conducta en la cual está implícita la "*Intrusión",* concepto y materia de estudio que se abordará desde lo más elemental hasta los trabajos científicos desarrollados en los últimos años, en este trabajo de tesis.

En el capítulo siguiente se comenzara a estudiar los conceptos previos de la detección de intrusiones, como son las auditorias y la revisión de registros en los sistemas operativos. Esta necesidad nace en los ambientes militares, donde es de alta prioridad vigilar y monitorear a usuarios. Aunque propiamente una auditoría no es una detección de intrusiones, es de mucha ayuda para visualizar lo que está pasando en un sistema.

Capítulo 2
Antecedentes y Formalización de la Detección de Intrusiones.

Resumen.

En este capítulo se describen algunos conceptos de la detección de intrusiones y también su desarrollo desde sus inicios como consecuencia de las auditorias en donde era necesario revisar un gran número de registros para poder clasificar elementos de mal comportamiento, y en consecuencia el poder tomar decisiones. Por esta razón y algunas otras se han creando productos que automatizan procesos para revisar elementos que son importantes en la toma de decisiones.

Estos elementos son llamados Detectores de Intrusos y en este capítulo se describe su comportamiento, así como su esencia, y también cuál es el objetivo de tener un Detector de Intrusiones instalado en un sistema de red.

2.1 Auditoría el Comienzo de la Era para la Detección de Intrusiones.

Antes de comenzar a describir qué es la detección de intrusiones es necesario hablar de la auditoría. La auditoría define un proceso para generar registros y una revisión cronológica a los eventos del sistema.

La gente audita sistemas para completar sus metas, esas metas incluyen lo siguiente:

a) El personal que está asignado para dar mantenimiento a las actividades del sistema.
b) La reconstrucción de eventos.
c) La evaluación del daño.
d) Monitorear áreas problemáticas del sistema.
e) Recobrar daños eficientemente.
f) Determinar el uso impropio del sistema.
g) Comprobar la efectividad del sistema y su desempeño.

Una premisa que subraya todos los procesos de auditoría es que el conjunto de reglas gobierna a la auditoría. La forma exacta y substancia de este conjunto de reglas varía, dependiendo en el contexto del proceso de auditoría.

En el caso especial de la auditoría de seguridad en computo, el conjunto de reglas es usualmente articulado en una política de seguridad, para desarrollar un completo y competente análisis de los datos auditados.

Ahora se describe en la figura 2.1 el sistema básico de auditoría, éste cuenta con un analizador de bitácoras que está formado por archivos de auditorías, éste a su vez es el resultado de un proceso generador de auditoría, que es alimentado por todos los eventos del sistema, usuarios y procesos que interactúan al mismo tiempo, todo esto será afectado y controlado conforme a las políticas de seguridad que estén vigentes. La finalidad de éste es poder llegar a un sistema de reportes que es el que tendrá lo más relevante del sistema, haciendo un intento de bajar la complejidad al revisar millones y millones de registros de auditora, y en seguida se da un ejemplo de una auditoría militar.

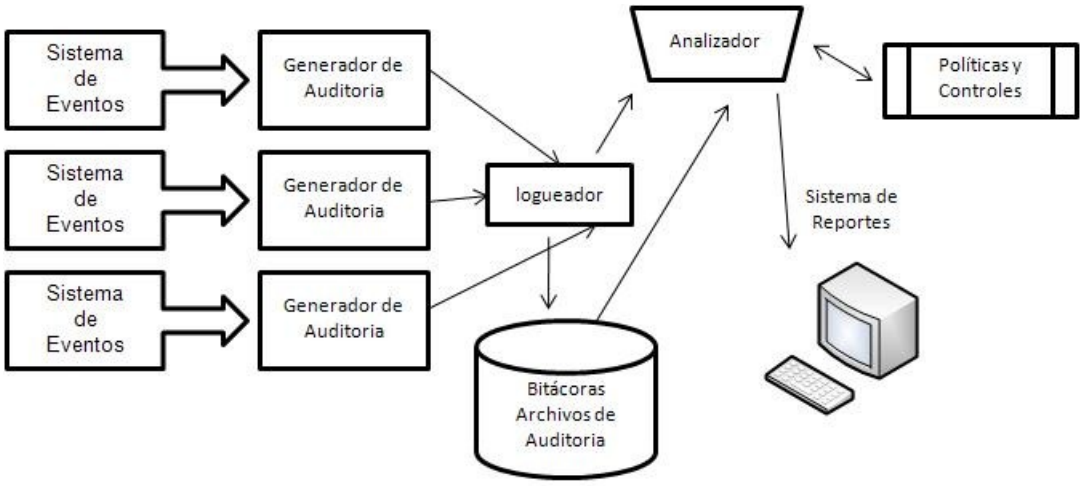

Figura 2.1 Sistema básico de Auditoría

2.1.1 Auditoría y los Modelos Militares de Seguridad en Cómputo.

El Departamento de Defensa de los Estados Unidos (DOD) hizo un extensivo desarrollo durante los años 70`s donde estudiaron las políticas de seguridad, líneas para guiarse y controles de operación, como los sistemas confiables culminando en la iniciativa de seguridad del DOD del año 1977. Dichos sistemas fueron definidos como “sistemas que emplean suficiente hardware y software para garantizar medidas que permitan el uso de procesos simultáneos de un rango o sensitivos a información clasificada”.

Así los sistemas seguros fueron diseñados permitiendo a los militares y organizaciones de inteligencia tener lugares para información con diferentes niveles de sensibilidad en la misma computadora.

Inicialmente los sistemas confiables proporcionaron un lugar en el cual los expertos de seguridad en cómputo fueron ciertamente los exploradores de las características y necesidades para que funcionaran los sistemas confiables.

Durante las exploraciones iníciales, desarrolladores realizaron debates donde los mecanismos de auditoría de seguridad contribuyeron a garantizar los niveles de sistemas confiables. Como última instancia los mecanismos de auditoría fueron ciertamente incluidos como parte de los "*Trusted Computer System Evaluation Criteria*" (Libro Naranja) requerimiento para la evaluación de sistemas confiables de nivel C2 y por encima de estos.

La serie de documentos que perfilan el DOD´s Trusted Systems Initiative son frecuentemente referidos como "*La serie Arcoíris*" [36].

Un documento, que direcciona al tema de Auditoría en Sistemas Seguros. Está incluido en las Series Arcoíris, este es el Libro Marrón. Titulado "*Una guía para entender la auditoría en sistemas confiables*".

El libro marrón subraya cinco metas de los mecanismos de seguridad:

a) Cómo permitir la revisión de patrones de acceso y el uso de mecanismos de protección del sistema.
b) Cómo permitir el descubrimiento de personal con acceso y personal sin acceso que merodean los mecanismos de protección.
b) Cómo permitir el descubrimiento de una transición de un usuario menos interesante que gana un nivel privilegiado.
d) Cómo servir como algún elemento distractor de usuario intenta romper los mecanismos de protección.
e) La forma de garantizar que un usuario al intentar romper los mecanismos de seguridad será grabado y descubierto.

A través del Libro Marrón se puede ver un rango centralizado del marco principal del cómputo, estos son los servicios que aún se aplican en la auditoría de seguridad.

2.2 Conceptos y Definiciones en la Detección de Intrusiones.

La detección de intrusiones es el proceso de monitorear redes de computadoras y violaciones en los sistemas de sus políticas de seguridad. Y en simples términos se puede decir que todo sistema detector de intrusos consiste en tres componentes fundamentales:

a) Una fuente de información, que provee un flujo de registros de eventos.
b) Un motor de análisis, que encuentra señales de intrusiones.
c) Un componente de respuesta, que genera relaciones basadas en la llegada de los componentes del motor de análisis.

La detección de intrusiones es una encarnación de la práctica tradicional de la Auditoría en Sistemas. Y la auditoría está definida como "*El exámen oficial y sistemático de cuentas para acertar su precisión*".

Sin embargo, la detección de intrusiones ha evolucionado en los pasados 20 años, incluyendo estrategias que asocian inteligencia y problemas de monitoreo en los sistemas.

Cuando la auditoría fue propuesta como una protección para sistemas sensibles, fue para auditar información que tenía que ser confiable, que debía de ser almacenada y procesada en ambientes separados del sistema de procedencia. Sus requerimientos fueron inherentes por la detección de intrusiones, separando la información auditada de los sistemas que los auditores protegieron, esto fue necesario por tres razones:

α) Para poder mantener a un intruso lejos, ya que pudo haber desactivado un detector de intrusiones mediante el borrado de registros de auditoría.
β) Para mantener a un intruso fuera del ambiente de modificación de los resultados de un detector de intrusiones que pudo haber estado escondiendo la presencia de una intrusión.
χ) Para disminuir el desarrollo asociado con los detectores de intrusiones que se toma en un sistema operativo.

2.2.1 Definición Formal de Seguridad en Cómputo.

Desde una perspectiva práctica, un sistema seguro es "*aquél con el que se cuenta que actúe de manera esperada*". Este punto de vista tiene explícitas implicaciones de confianza. Pero el problema es que la confianza no se puede medir. No podemos confiar en que un sistema se comporte como debe. Es decir, nadie nos puede asegurar que un sistema se comporte como realmente tiene que hacerlo.

Un enfoque formal y preciso de seguridad se tiene a través de la Triada de Confidencialidad, Integridad y Disponibilidad, que son requerimientos que se deberían de cumplir a un cien por ciento, pero eso nunca pasa.

Confidencialidad: es el requerimiento al acceso de la información restringida que solamente usuarios restringidos pueden tener acceso. Mucho del trabajo hecho por el gobierno en seguridad en cómputo se enfoca en la confidencialidad.

Integridad: Es el requerimiento que la información debe de tener para ser protegida para así estar sin alteraciones. La integridad es especialmente crítica en sistemas que manejan datos de registros médicos y cuentas financieras.

Disponibilidad: Es el requerimiento que la información y los recursos del sistema siguen para trabajar y para que los usuarios autorizados sean capaces de acceder a los recursos, cuando se necesiten éstos.

Ahora que se definió seguridad es necesario hablar de lo siguientes conceptos: confianza, amenaza y vulnerabilidad. En general se verá que cuando un sistema está amenazado, un intruso intentará explotar alguna vulnerabilidad en él.

2.2.1.1 Confianza.

Otro aspecto muy importante en la seguridad de sistemas es la confianza, "*la confianza es la esperanza que se tiene de que un sistema se comporte como realmente debería*". Establecer relaciones de confianza sin garantías conlleva a la aparición de vulnerabilidades, que se convierten en potenciales amenazas.

2.2.1.2 Amenaza.

Amenaza determina el concepto de política de seguridad. Y está definida como cualquier situación o evento que tiene como potencial perjudicar a un sistema. Este daño puede ser de forma abierta, destructiva, para modificar los datos, y también para hacer una denegación de servicio. En otras categorías de Amenaza están incluidos los hackers, virus, el fuego, el flujo de datos y así la lista sigue.

Aquí se tiene una pregunta muy interesante, "*¿Cómo se estructuran las amenazas en el mundo de la seguridad en cómputo?",* Hay varios caminos para clasificar las amenazas y algunas amenazas involucran la fuente de la amenaza. En el siguiente modelo básico se clasifican las amenazas en tres categorías:

a) Penetraciones externas: Usuarios no autorizados del sistema.
b) Penetraciones internas: Usuarios autorizados del sistema quien se hacen pasar por legítimos usuarios para tener acceso, estas a su vez están divididas de la manera siguiente:
   i) Enmascarados: Son quienes se apropian de la identificación y credenciales de otros usuarios.
   ii) Usuarios Clandestinos: Son quienes exitosamente evaden la auditoría y monitorean las medidas de seguridad.
c) Usuarios legítimos: que exceden de sus privilegios.

2.2.1.3 Vulnerabilidad.

Los problemas de seguridad en sistemas de cómputo resultan de las Vulnerabilidades. Las vulnerabilidades están en los sistemas que pueden ser explotados en varias maneras para violar las políticas de seguridad.

Por ejemplo:

a) Vulnerabilidades en el diseño e implementación de sistemas en software y hardware.
b) Vulnerabilidades técnicas.
c) Vulnerabilidades en las políticas de seguridad “procedimientos, controles, configuración y otras áreas de mantenimiento”.
d) Vulnerabilidades de Administración.

Sin embargo las vulnerabilidades y las amenazas están intrínsecamente relacionadas, pero no son lo mismo. Amenaza es el resultado de explotar una o más vulnerabilidades. “*La Detección de Intrusiones está diseñada para identificar y responder a ambos conceptos”***.**

2.2.1.4 Política de Seguridad.

Las políticas de seguridad son requeridas en orden para mapear algunas veces conceptos de seguridad del mundo real. En una definición inicial de seguridad, está basada en la noción de que constituye expectativas de comportamiento de un sistema.

Hay algunos otros elementos que forman la infraestructura de los sistemas de seguridad y claro está, que es muy importante mencionarlos, como una solución al léxico de la Detección de Intrusiones:

a) Control de Acceso.
b) Identificación y Autenticación
c) Cifrado
d) Firewall

2.2.2 Estrategias de Monitoreo.

El primer requerimiento de la detección de intrusiones son los datos como recurso, los elementos pueden también ser considerados un generador de eventos. Los datos pueden ser categorizados en una gran variedad de maneras. En el propósito de la Detección de Intrusiones primeramente se le clasifican por su localización. Esta clasificación de esquemas divide las vistas del sistema de monitoreo en cuatro categorías: Host, Red, Aplicación y un Sistema como Blanco, u objetivo. Se usará el termino monitoreo para describir la acción de recolectar datos de un recurso de datos y pasarlos en un motor de análisis:

a) **Monitoreo basado en Host:** recolecta datos de un recurso interno en una computadora, usualmente a nivel de sistema operativo. Esos recursos pueden incluir un tren de datos del sistema operativo y logs.
b) **Monitoreo basado en Red:** En este esquema, son recolectados paquetes del flujo de red. Usualmente se usa un dispositivo NIC en modo promiscuo que captura todo el tráfico de red que es accesible.
c) **Monitoreo basado en Aplicación:** Recolecta datos de las aplicaciones que están corriendo. Estos incluyen las bitácoras, dispositivos de almacenamiento y demás aplicaciones.
d) **Monitoreo basado en un Sistema como Blanco:** Aquí se utilizan técnicas criptográficas, como funciones hash, para detectar alteraciones en los objetos de los sistemas y entonces comparar esas alteraciones con la política de seguridad establecida.

2.2.3 Tipo de Análisis.

En el proceso de la detección de intrusiones, después de que el flujo de información es definido y la localización está establecida, se requiere un motor de análisis. Este componente del sistema toma información del flujo de datos y examina los síntomas de los datos para un ataque u otra violación de política de seguridad.

En la detección de intrusiones, el enfoque del análisis implica, la detección del uso indebido y detección de anomalías o alguna mezcla de los dos.

a) **Detección del uso indebido:** Los motores buscan algo como “malo”, para hacer esto el filtro de flujo, busca patrones de actividad para encontrar ataques conocidos u otras violaciones a las políticas de seguridad. La detección del uso indebido busca técnicas de patrones conocidos y actividad que indique algún problema. Actualmente la detección de intrusos comercial usa técnicas de detección basadas en el uso indebido.

b) **Detección de Anomalías:** El motor busca algo raro o inusual, es analizado un flujo de eventos, usando técnicas estadísticas para encontrar patrones de actividad que aparecen a ser etiquetados como anormales. Este acercamiento refleja la visión del desarrollo de la detección de intrusiones y las intrusiones son un subconjunto de la actividad anómala.

Las ventajas significantes son asociadas con la combinación de estos dos esquemas, en la *f*igura 2.2.3.1 se denota un sistema detector de intrusiones genérico*.* El motor del esquema basado en anomalías mantiene al sistema para detectar nuevos ataques que no son conocidos u otros tipos de escenarios concernientes. El motor de perfiles ayuda a la detección del mal uso y protege la integridad de la detección de anomalías para garantizar que el adversario no puede cambiar el comportamiento del detector de anomalías y aceptar el comportamiento del ataque como algo normal, basado en las políticas de seguridad.

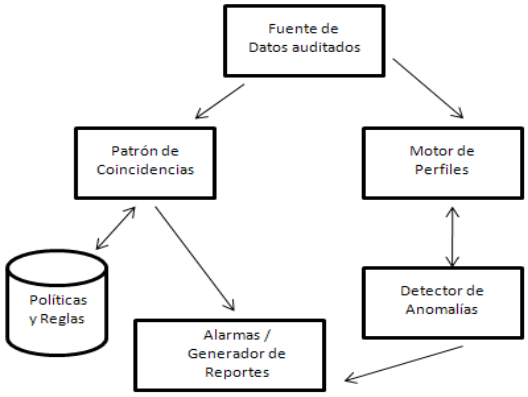

Figura 2.2.3.1 Sistema detector de intrusiones genérico.

En el crecimiento de la Internet y su subsecuente empuje va más allá de información crítica y redes conectadas. Los sistemas crean escenarios en los cuales la seguridad es de importancia crítica.

Así, el monitorear eventos y el reconocimiento de ataques son capacidades de los Sistemas de Detección de Intrusiones, Ahora se verán las diferentes fuentes de información:

2.3 Fuente de la Información.

El primer requerimiento de la detección de intrusiones que necesita son los datos este será el primer conjunto de entrada para evaluar qué serán los datos. Estos pueden llegar de una diversa variedad de entradas, como son los datos derivados de recursos internos o de sistemas individuales, datos asociados con recursos de la red y también otro tipo de datos relacionados con switches telefónicos o sistemas de seguridad física.

Una de las preguntas que se necesitan tener en mente es: ¿Cuál de esos recursos es el mejor para la detección de intrusiones? Así mismo la respuesta correcta sería que depende de lo que yo quiera detectar. Para detectar un ataque, el Sistema de Detección de Intrusiones debe de ser capaz de ver la evidencia del ataque.

2.3.1 Recursos de Información Basados en Host.

Los productos de detección de intrusiones comúnmente se dividen en varias ramas. Algunos definen la detección de intrusiones como estrictamente basados en redes.

Otros definen sistemas de detección de intrusos estrictamente como los basados en host o como sistemas específicamente basados en aplicaciones.

Finalmente muchos integran ambas técnicas para tener un mejor desarrollo de ellos.

Ese aprovechamiento es basado en técnicas de monitoreo del sistema que es un punto en el cual se recolecta información.

Los recursos de información basados en host consisten en auditar el sistema operativo, que es grabar registros de los eventos del sistema que son generados, y especialmente del sistema operativo, también bitácoras del sistema y eventos de aplicaciones, los cuales son usualmente archivos de texto que son escritos en línea en el tiempo preciso que se ejecutan las aplicaciones del sistema.

2.3.1.1 Auditoría del Sistema Operativo.

El primer recurso de información basado que es considerado como un recurso significativo de seguridad es el auditar el sistema operativo.

El sistema operativo genera archivos que son generados especialmente por un subsistema de auditoría incluido como parte del software del sistema operativo. Esos archivos tienen información que es recolectada por las actividades del sistema, cada archivo de auditoría es puesto en orden cronológico y es organizado en uno o más archivos de auditoría.

Muchos sistemas de auditoría fueron originalmente diseñados y desarrollados con los requerimientos del "*Trusted Product Evaluation Program*". Esta fue una iniciativa del gobierno de los E.U. puesto en el conocido "*Libro Naranja*" que implementa características a los sistemas operativos comerciales y aplicaciones que contienen procesos de información clasificada.

2.3.1.2 Pros y Contras de Auditar el Sistema Operativo.

Los expertos de la Detección de Intrusiones consideran que la auditoría del sistema operativo es preferible a otros recursos de información comúnmente basados en host, para los propósitos de la detección de intrusiones. La primera razón es que el sistema operativo está estructurado y provee una protección sustantiva para los subsistemas de auditoría.

Otra motivación es el precio que tiene el sistema operativo para auditar trenes de información como los recursos de detección que son eventos que finalmente tienen que tener mucho detalle. Esta información mantiene al sistema. El recolectar datos a cierto nivel de detalle presenta problemas, en particular se tienen que diferenciar actividades de usuario invocadas por programas u otros usuarios.

Otra de las ventajas de monitorear las actividades con un gran nivel de detalle es que esto nos lleva a la luz de ver patrones anormales en los procesos de ejecución. Este nivel de monitoreo es capaz de reconocer la ejecución de "caballos de troya y otro código malicioso".

2.3.1.3 Reduciendo la Auditoría.

El reducir la Auditoría es el proceso de filtrar las bitácoras. Identificando y removiendo información que es redundante e irrelevante. Este proceso representa el problema clásico que ha tenido impedimentos significantes para diseñar e implementar reducción de datos en operación. La clave para reducir el proceso es la capacidad de introducir un determinismo para hacer no inherente el proceso que no se puede determinar.

En otras palabras, dar la capacidad de dar un estado como un evento X, que siempre lanzará eventos Y, Z y K bajo las condiciones A y B que pueden reducir el flujo de eventos consistente de (X, bajo las condiciones A y B, seguido por Y, Z, K) el evento X.

El problema con este acercamiento es que (especialmente en sistemas multiproceso y multitárea) este nivel de acercamiento simplemente no está presente.

Además, la complejidad de los sistemas operativos modernos permite a los escenarios lanzar comandos a un nivel alto para generar cientos de registros de auditoría. Peor aún, el orden en el cual los registros son grabados en las bitácoras de auditoría no es consistente. Por ejemplo en un sistema operativo Sun Os de Unix el comando "ls" puede generar más de 1500 registros de auditoría.

2.3.1.4 Importancia de las Bitácoras

Las bitácoras son archivos que reflejan varios eventos del sistema, cambios y ajustes. El sistema operativo Unix provee un sistema de bitácoras basado en el servicio *SYSLOG.* Este genera y actualiza los eventos de las bitácoras vía un demonio llamado "syslogd".

Las bitácoras son de suma importancia ya que nos dan un historial de todo aquello que ha sucedido en el sistema como:

a) Software instalado.
b) Dispositivos conectados.
c) Conexiones remotas.
d) Entrada de usuarios.
e) Etc.

Las bitácoras tienen un resumen de evento en específico, así como fecha de creación de la bitácora, tiempo en que duró el evento, usuario que efectuó dicho evento. Desgraciadamente estos archivos crecen de una manera sorprendente inundando los sistemas de información que a veces se piensa que no tienen importancia. Es por ello que se tiene que configurar de manera rigurosa, para evitar éste problema existe software GNU como "*logwatch y logdog*" entre otros, para el manejo, filtrado de las bitácoras y así como eventos importantes.

Los usuarios mal intencionados son los encargados de borrar y/o alterar estos archivos, ya que los administradores carecen de conocimientos acerca de criptografía para poder protegerlas y esconder su contenido.

La revisión de las bitácoras puede ser clasificado como un acercamiento a la detección de intrusos, este procedimiento se ha ido perdiendo ya que hoy en día los administradores ya no revisan estos archivos, dado que son muy grandes y tediosos. Basta imaginar un esquema descentralizado de bitácoras donde llegan millones de archivos donde estos a su vez tienen millones de registros (pensando en un sistema de bitácoras bancario o el sistema de bitácoras de la red telefónica).

Para la captura de información de eventos, los sistemas cuentan con librerías de captura "*pcap*".

El **pcap** es un interfaz de una aplicación de programación para captura de paquetes. La implementación del pcap para sistemas basados en Unix se conoce como libpcap; el correspondiente en sistemas windows del libpcap recibe el nombre de winpcap.

El libpcap y winpcap pueden ser utilizados por un programa para capturar los paquetes que viajan por toda la red y, en las versiones más recientes, para transmitir los paquetes en la capa de enlace de una red así como para conseguir una lista de los interfaces de red que se pueden utilizar con el libpcap o winpcap.

El libpcap y winpcap son la captura del paquete y los motores de filtración de muchas herramientas de código abierto y comerciales de la red, incluyendo analizadores de protocolo, monitores de la red, sistemas de detección de intrusos en la red, programas de captura de las tramas de red (packet sniffers), generadores de tráfico y puesta a punto de la red. Algunas de estas herramientas, tales como tcpdump, wireshark (antes ethereal), nmap, cain y abel, y snort son conocidos y utilizados a través de la red y de una comunidad de seguridad internacional.

Ahora con esta sección se tiene una visión de lo que se necesita y se tiene para la detección de intrusos. Así se pueden considerar varios puntos de vista, diferentes puntos de detalle y en esencia, la pregunta de qué es lo que nuestros sistemas deberían de analizar.

2.4 Análisis de Esquemas.

Dada la gran variedad de recursos de información acerca de las actividades de los sistemas, esta cambia mientras esta monitoreando. Así la siguiente parada para la detección de intrusiones es el análisis, con el análisis ahora se tendrá que enfrentarse a nuevas preguntas como: ¿Qué es lo que está pasando aquí?, ¿Qué es lo que me debe de interesar?.

2.4.1 ¿Qué es el Análisis?

En el contexto de la detección de intrusiones el análisis es la organización, caracterización de las actividades de usuarios y sistemas para identificar actividades de interés. Esta actividad puede ser aislada, esto pasa después del hecho. Esto depende del tipo de análisis, una nueva evaluación se puede realizar para ajustar o mejorar el resultado del análisis posterior.

2.4.2 Metas del Análisis.

Uno de los beneficios que los administradores de seguridad buscan es determinar el problema del factor para disuadir el comportamiento. El conocimiento de que el análisis desarrolla y las amenazas creíbles que se descubren deben servir para disuadir a los intrusos.

Los problemas que son descubiertos en el curso del análisis pueden indicar flujo en el diseño y administración de los sistemas de seguridad. El administrador de seguridad, notificará que puede corregir el problema antes de que los adversarios puedan dañar o robar información.

La información útil acerca de las intrusiones, debe ser muy relevante y detallada y digna de confianza ya que esto puede ser un recurso para apoyar de manera penal o civil.

El análisis de la detección de Intrusiones soporta dos ideas básicas:

α) La rendición de cuentas.
β) La detección en tiempo real y respuesta.

Estos requerimientos incluyen la capacidad de organizar rápidamente las cadenas asociadas con el ataque y también la capacidad de bloquearlo, (por ejemplo

poniendo fin a la conexión de un atacante desconectándolo) o poniendo un sistema que funcione como escudo para frenar el impacto del atacante.

2.4.3 Técnicas.

Retomando la definición de análisis se puede observar que está dividida en dos partes: la detección del uso indebido, que se refiere a la búsqueda de eventos de datos para predefinir patrones de uso y la detección de anomalías, la cual caracteriza datos en términos matemáticos y se dedica a buscar eventos de patrones anómalos.

2.5 Respuesta.

Después de que el análisis está hecho y el sistema ha identificado problemas, es momento de que alguien se entere del problema y se encargue de el, y en algunos casos de que se tome una decisión de qué acción se debe de tomar. En el proceso del modelo de la Detección de Intrusiones éste esta detenido por un proceso de respuesta. En esta parte del sistema sirve a todos los miembros del equipo de administradores de seguridad para intentar dar una respuesta cada uno de ellos.

Las técnicas de detección de intrusiones pueden dar resultados en varios caminos, con respecto al análisis y subrayar algunas opciones para responder a problemas, estas opciones incluyen respuestas activas, en el cual los sistemas automáticamente informan al usuario. Tomar acciones en orden de bloques que afectan el proceso de ataque. En la sub sección siguiente se mostrará la manera de tomar resultados en el sitio del proceso de la seguridad.

2.5.1 Requerimientos para la Respuesta.

Muchas consideraciones vienen inmersas en el diseño de la respuesta de un sistema detector de intrusiones. Algunas respuestas pueden ser diseñadas para reflejar estándares actuales de la administración de seguridad o la respuesta a incidentes, otros pueden reflejar administración local y políticas. Cuando se diseña una respuesta de productos comerciales. Los vendedores deberían proveer a los usuarios finales mecanismos de respuesta para un ambiente particular.

En algunos días del desarrollo y diseño de los detectores de intrusos, más diseñadores se enfocaron en el monitoreo y análisis del sistema, dejando el componente “*respuesta” al usuario. Sin embargo ese fue un gran tema de discusión*“ ¿Qué es lo que realmente un usuario buscaba como componente de respuesta? Ninguno tenía una idea clara del ambiente operacional en el cual los sistemas detectores de intrusiones fueran sembrados.

2.5.1.1 Ambiente de Operación.

Cuando se diseña un mecanismo de respuesta, y obviamente se considera que es su naturaleza la del ambiente operacional en el cual el sistema detector de intrusiones está operando, la alarma y los requerimientos de notificación de un sistema detector de intrusiones que tiene un numero de consolas para atender alarmas en el centro de operaciones.

La información proveniente de sistemas detectores de intrusiones es parte de la notificación también depende del ambiente. El centro de operaciones de la red y medios administradores prefieren usar productos que proveen detalles de tráfico a nivel bajo.

Un administrador de seguridad considera más allá una alarma con un mensaje para ponerse en contacto con la persona en problemas.

Las alarmas audibles son ideales en las instalaciones en las cuales una persona es responsable de monitorear los resultados de múltiples sistemas detectores de intrusiones. Cada alarma puede ser un pista, de un mapeo de múltiples operaciones de una red que es muy compleja y que se muestra en una simple consola.

Las alarmas visuales y gráficas de actividad pueden ser de valor para las instalaciones que tienen operaciones todo el tiempo, para quienes se sientan enfrente de una consola. Así son especialmente de ayuda cuando los componentes de otra infraestructura de seguridad no pueden ser visualizados por los administradores de seguridad.

2.5.1.2 EL Propósito del Sistema y las Prioridades.

Otro factor que conduce a una respuesta, es el sistema de monitoreo. El necesita proveer respuestas activas, como sistemas que proveen datos críticos y servicios a otros usuarios. Un ejemplo de este tipo de sistema es un servidor de registros médicos en un cuarto de emergencia, otro es un servidor web de alto tráfico, y también un servidor de comercio electrónico.

En esos casos, el impacto de un ataque de denegación de servicio exitoso puede ser devastador. El valor de preservar la disponibilidad de los sistemas se compensa con creces generales asociados con la provisión de activos en las respuestas a intrusiones detectadas.

Con esto se cubre la tercera parte del proceso que compone a un detector de intrusiones. En el componente de la respuesta es claro que es manejado por el análisis que genera respuestas activas o pasivas de las intrusiones que son detectadas.

También se exponen definiciones y requerimientos de esos componentes fundamentales, y se definen unas clasificaciones de esquemas, que dan como resultado el proceso de la detección para el proceso de administración de la seguridad.

Como proceso de la administración de seguridad hoy por hoy se hace más a menudo mención del concepto de "*monitoreo*" así mismo "*monitoreo de seguridad en redes*" , este es un campo de estudio un poco mayor, ya que abarca la detección de intrusiones como parte de el.

El monitoreo de seguridad en redes, consta de 4 partes básicas: estimación, protección, detección y respuesta. Donde la detección de intrusiones obviamente está inmersa en la segunda, se dará en el capítulo posterior a la descripción del Monitoreo de Seguridad en Redes, donde se describirán las zonas de monitoreo y algunas herramientas para la ayuda del mismo.

Capítulo 3
Monitoreo de Seguridad en Redes y Detección de Intrusiones.

Resumen.

Ahora que están puestas las bases de la Seguridad de la información y se ha alcanzado cierta madurez, en este capítulo se hablará del concepto de Monitoreo de Seguridad de Redes

El Monitoreo de Seguridad de Redes, en esencia es la recolección, análisis y notificación de indicaciones y advertencias con objeto de detectar entradas y respuestas a ellas.

Así también en este capítulo se verán algunas de las herramientas mas populares del software libre para la monitoreo de redes, como tcpdump [3], snort [15], ethereal [19] y se introducirán los conceptos previos acerca de la Detección de Intrusiones sin descuidar su taxonomía para tener una idea global de los Sistemas Detectores de Intrusos.

3.1 ¿Qué es el Monitoreo de Seguridad de Redes?

Por "*indicaciones* y *advertencias se entiende"* que es un proceso de monitoreo estratégico que analiza los indicadores y produce advertencias. También se definen como se hace en el ejército y se dice que los *indicadores* y *advertencias* dan monitoreo estratégico del tráfico de red destinada a apoyar la detección y verificación de intrusiones.

Por lo tanto el Monitoreo de Seguridad de Redes y los productos Detectores de Intrusiones se centran en amenazas. Se hace notar que los indicadores que generan los IDS suelen denominarse "alertas".

Por ejemplo:

a) Todos los indicadores tienen valor, pero algunos tienen más valor. Una alerta que indica que un servidor de correos ha iniciado una sesión FTP saliente hacia Rusia es un indicador.

b) Un pico en la cantidad de tráfico ICMP a las 2 de la mañana es otro indicador

En general, el primer indicador tiene más valor que el segundo, salvo que la organización nunca haya utilizado anteriormente ICMP.

Las *advertencias* son los resultados de la interpretación de los indicadores por parte de los analistas. Los analistas escrutan los indicadores generados por sus

productos y pasan advertencias a quienes toman las decisiones (Así debería de Ser). Si los indicadores son similares a la información, las advertencias son similares a los informes finales de inteligencia.

Las evidencias de reconocimiento, explotación, refuerzo, consolidación y pillaje son indicadores.

El informe al Coordinador del Centro que indica "*Es probable que nuestro servidor WEB este comprometido*" es una advertencia, entonces, él obviamente optará por la reconstrucción del Sistema.

Quienes practican el Monitoreo de Seguridad de Redes usan los indicadores y advertencias para detectar y verificar intrusiones, también formulan conclusiones basándose en el tráfico que pasa a través de las redes.

Ambas comunidades hacen estimaciones ponderadas, porque un perfecto conocimiento del dominio público resulta casi imposible.

Según la definición de Monitoreo de Seguridad de Redes, los indicadores se recolectan y se analizan, y las advertencias pasan a instancias superiores.

Los productos son los encargados de realizar la recolección, por producto entendemos a un software o artefacto cuyo propósito es analizar paquetes de la red.

En la sección siguiente se analizan las bondades de algunos productos de software libre para el Monitoreo de la Red.

Las personas se encargan del análisis, aunque los productos pueden llegar a conclusiones respecto al tráfico que ven, por lo tanto se necesitan personas para proporcionarles un contexto adecuado. Conseguir un contexto requiere de poner en una correcta perspectiva el resultado del producto, dada la naturaleza del entorno en que opera el producto.

3.1.1 Detección de Intrusiones y Respuestas a las Mismas.

Suponiendo que fracasara la prevención, las organizaciones tienen que mantener la capacidad de determinar rápidamente cómo ha podido un intruso comprometer a una víctima y qué ha hecho el intruso tras conseguir un acceso sin autorización.

Este proceso se denomina valoración del incidente "*Compromiso*" no siempre significa que obtuvo acceso a "*root*".

Un intruso que aprovecha las prevenciones que le otorga una base de datos defectuosa es tan mortífero como un atacante que obtiene acceso de administrador en una máquina con sistema operativo Windows.

Por eso se deben de formular típicamente las siguientes preguntas:

a) ¿Qué ha hecho el intruso?
b) ¿Cuándo lo hizo?
c) ¿Sigue teniendo acceso el intruso?
d) ¿Qué gravedad puede tener el compromiso?
e) ¿Cómo lo evito?

Las respuestas a estas preguntas servirán de guía a los administradores de sistemas.

Por lo general nadie pregunta: ¿Ha detectado esto el sistema de detección de intrusos? ¿Lo ha detectado el sistema de estadísticas de monitoreo? Los analistas de Monitoreo de Seguridad de Redes aprovechan esto en su propia ventaja, empleando todo el rango de fuentes de información disponibles para detectar intrusiones.

Se hace notar que las intrusiones son violaciones de políticas tanto de extraños como del personal interno. Cualquiera puede ser responsable de estas transgresiones.

Aunque los datos aportados por el Monitoreo en la red pueden servir de ayuda para identificar configuraciones de red incorrectas, para determinar la utilización de recursos y para llevar a la cuenta de los hábitos de navegación por la WEB de los empleados, su foco legitimo es identificar intrusiones.

Algunas veces el Monitoreo de Seguridad de Redes, "*es confundido con la administración de dispositivos"*, esto debido a que hay proveedores de servicios de administración de seguridad que ofrecen la posibilidad de monitorear y administrar firewalls, routers e IDS´s, la mayoría de estos fabricantes no practica el Monitoreo de la Red tal como está definida en este trabajo de tesis.

Estos fabricantes se preocupan más por mantener el funcionamiento de los sistemas que administran que de los indicadores que proporcionan estos dispositivos. Hay otros fabricantes que agregan información precedente de distintos dispositivos de la red en una única consola, esta capacidad puede ser una condición necesaria pero insuficiente para hacer Monitoreo de Seguridad de Redes, aunque ciertamente sirve de ayuda, disponer de información resumida al analista.

A comienzos del año 2002, la expresión sistema de prevención de intrusiones (IPS) pasó a ocupar un lugar importante en las mentes de los administradores de seguridad. En algunos lugares en las redes, los comerciales más avispados

decidieron que sería positivo cambiar de la D de IDS a P de prevención. Después de todo, se deben de haber preguntado, si podemos detectarlo, ¿Por qué no podemos evitarlo? De este modo comenzó el último debate tecnológico que ha llegado a la comunidad de la seguridad. Un sistema para la prevención de intrusiones es un dispositivo de control de acceso, como un firewall. Un sistema de detección de intrusiones es un dispositivo de detección, destinado a efectuar una auditoría de la actividad y a comunicar los fallos observados en la prevención.

Los operadores del Monitoreo de la Seguridad de Redes creen que es preciso separar los roles de prevención y de detección. Si estas dos tareas tienen lugar en una misma plataforma ¿qué agente externo está disponible para verificar su efectividad?

Los productos de prevención de intrusiones acabarán por migrar hacia los firewalls comerciales. Aunque los firewalls tradicionales tomaban decisiones de control de acceso en la capa 3 del modelo OSI, (dirección IP) y en la capa 4 (puerto), los cortafuegos modernos permitirán o denegarán el paso del tráfico después de inspeccionar la capa 7 (datos de aplicación). Los fabricantes de firewalls se ven forzados a dar estos pasos como consecuencia de unas opciones tecnológicas equivocadas. A medida que los fabricantes de aplicaciones hacen funcionar cada vez más servicios sobre el http, puerto 80 TCP van degradando el modelo que permitía funcionar a los cortafuegos de la capa 4.

Los problemas seguirán persiguiendo el puerto 80 y otros tantos hasta que los fabricantes de control de acceso compensen las malas decisiones del fabricante de aplicaciones y también encuentren una buena administración de la seguridad en sus servidores.

3.2 Zonas de Monitoreo.

Antes de vigilar el tráfico de red, el personal a cargo de la seguridad tiene que decidir que objetivos debe monitorear y quién tiene más posibilidades de atacar esos objetivos. Los atacantes se pueden agrupar en cuatro clases:

a) Atacantes externos que lanzan intrusiones desde Internet (clase 1).

b) Atacantes externos que lanzan intrusiones desde segmentos inalámbricos (clase 2).

c) Atacantes internos que lanzan intrusiones desde redes locales cableadas (clase 3).

d) Atacantes internos que lanzan intrusiones desde segmentos inalámbricos (clase 4).

La capacidad de visualizar a las víctimas de cada tipo de ataque procede del despliegue de plataformas de monitoreo, que también se conocen con el nombre

de sensores. Un sensor es un dispositivo que recolecta y analiza tráfico de red con el propósito de identificar sucesos sospechosos.
En general cualquier red consta de cuatro zonas básicas de monitoreo *figura 3.2.1*. Las cuales son ubicaciones donde los usuarios de red comparten ciertos privilegios, basados en el nivel de confianza que les otorga un oficial de seguridad.

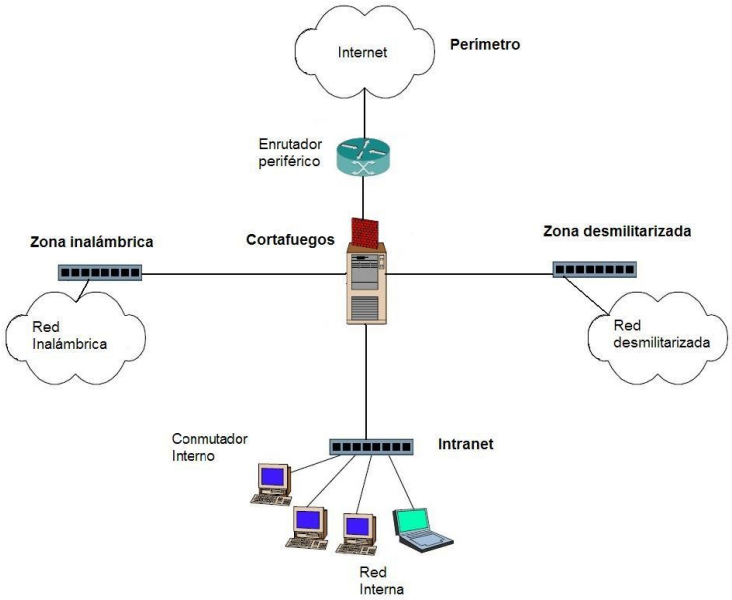

Figura 3.2.1 Esquema de las 4 zonas de monitoreo de seguridad de redes.

Estas características están determinadas mediante un dispositivo de control de acceso, que segmenta el tráfico de las distintas zonas. Aquí el dispositivo de control de acceso es un único firewall.

1.- El perímetro se extiende desde la interfaz externa del firewall, a través del router periférico, hacia Internet.

2.- La zona desmilitarizada (DMZ) se extiende desde la interfaz DMZ del firewall é incluye todas las computadoras que están conectadas al conmutador DMZ.

3.- La zona inalámbrica incluye todas las máquinas que tienen conectividad inalámbrica.

4.- La intranet se extiende desde la interfaz interna del firewall e incluye todas las computadoras conectadas al conmutador interno.

Cada una de estas zonas contiene sistemas que están sometidos a ataques de personal interno y externo. Un firewall bien configurado limita el grado hasta el cual se pueden alcanzar entre sí los sistemas de distintas zonas. Las reglas tradicionales del firewall limitaban el grado hasta el que el perímetro podría acceder a la DMZ o a la intranet, implementando un control de acceso. Estas

configuraciones limitan el daño que pueden causar las intrusiones, pero no limitan su acceso una vez que comprometen a una computadora de cualquier zona. Las configuraciones de los cortafuegos modernos limitan el tráfico saliente así como el entrante. Estos firewall ofrecen un control de salida.

La condición de salida suele ser la última línea de defensa de la organización una vez que se ha producido el compromiso, porque esta técnica limita la capacidad de los intrusos para ejecutar sus planes.

A continuación se examinan cada una de las cuatro zonas, para decidir cómo sirve de asistencia para el personal se seguridad el monitoreo de cada una de ellas.

3.2.1 El Perímetro.

El *perímetro* es una zona clásica donde se desplegaban sensores, porque ofrece una única ubicación con la mejor visibilidad posible contra amenazas externas de Internet (atacantes de clase 1). Se considera que el perímetro es la zona “de menos confianza” entre todas, porque la empresa tiene escaso control sobre las computadoras que inicien un contacto desde ellas. Hay excepciones claro, Que son las sesiones que solicitan empleados estudiantes importantes situados en ubicaciones remotas.

Las prácticas más recomendables indican que no deben ubicarse computadoras de la empresa en la periferia. Esto es, que ninguna computadora debería situarse más allá del control de acceso de un firewall. Aunque un router con filtro ofrece un cierto grado de protección, su papel principal es el de permitir el paso del tráfico.

El monitoreo del perímetro es un asunto ruidoso. Salvo el posible filtraje realizado por el router de frontera, los sensores de perímetro van a detectar todo el tráfico procedente de ataques de clase 1. Este tráfico incluye todo lo que el firewall está programado para rechazar. Las organizaciones que despliegan sensores en el perímetro se preocupan por recoger datos de inteligencia relativos a las amenazas. Consideran que los intentos de reconocimiento e intrusión que no llegan a atravesar el firewall son indicadores de futuros ataques. Sin embargo, unos sensores configurados para recolectar grandes cantidades de tráfico van a crear una cantidad de trabajo proporcional para los analistas.

3.2.2 Zona Desmilitarizada.

El monitoreo de la *DMZ* suele realizarse para mantener vigiladas aquellas computadoras que tengan más probabilidades de verse comprometidas por atacantes externos procedentes de Internet (clase 1). Sabemos que entre los sistemas de la zona DMZ se cuentan los servidores de correo electrónico, web, dns, servidor ftp, y otros más. Suponiendo que el cortafuegos limite la cantidad de

tráfico que llega a la DMZ, los sensores de la DMZ registrarán mucha menos actividad que los que se encuentren en el perímetro. Las computadoras de la DMZ comparten a veces una o más direcciones públicas que se le asignan al firewall a través de NAT. Cuando se emplea esta estrategia, es más fácil para los analistas detectar actividades sospechosas en la DMZ cuando los sensores tienen una visibilidad directa de la misma.

Los sensores de la DMZ son especialmente adecuados para observar ataques contra computadoras de la DMZ y desde otras zonas. Los productos de detección basados en red son especialmente efectivos para observar computadoras de la DMZ, debido al menor nivel de ruido de tráfico y a la relativa sencillez de las reglas de seguridad que gobiernan la actividad de la DMZ.

La DMZ es una red de confianza media porque las computadoras están bajo control directo de la empresa o institución. Desafortunadamente, dado que están expuestas a usuarios que no son de confianza y que se conectan desde Internet, también tienen más probabilidades de verse comprometidos. Los administradores de red más expertos limitan la conectividad de las computadoras de la DMZ hacia otros segmentos, y especialmente hacia el perímetro.

3.2.3 Zona Inalámbrica.

Las computadoras de la *zona inalámbrica* no se consideran de confianza, del mismo modo que las computadoras que se conectan desde Internet no se consideran de confianza. Los usuarios basados en Internet, tales como los empleados que se conectaban desde su hogar y socios del negocio que se conectan desde sus lugares de trabajo, deberían encapsular su tráfico en una red privada virtual (VPN) e identificarse empleando una autenticación de dos factores como cualquiera que esté dentro del alcance del punto de acceso inalámbrico se puede conectar al segmento inalámbrico, así la zona debería tratarse como una red de confianza media.

Los intrusos externos que lanzan ataques desde segmentos inalámbricos (los atacantes de clase 2) pertenecen a dos subcategorías. Una mayoría muy amplia son pasajeros sin billete que se cuelan en segmentos inalámbricos mal configurados. Una pequeña minoría son espías corporativos que están intentando sustraer propiedades intelectuales. Es preciso tener en cuenta a ambos en la ecuación de despliegue de sensores.

La detección de la zona inalámbrica es una ciencia inmadura. Las estrategias actuales se centran en detectar los ataques de clientes inalámbricos contra la intranet. Hay muchas organizaciones que abandonan a su suerte a los clientes inalámbricos. En lo concerniente a amenazas externas procedentes de Internet, las computadoras de la zona inalámbrica suelen tener el mismo aspecto que computadoras de Internet.

3.2.4 La Intranet.

La cuarta parte es la que llamamos *Intranet* definida como una red de uso privado que emplea los mismos estándares y herramientas de Internet, está formada por los elementos de mayor confianza de la organización. No se debe permitir que los usuarios basados en Internet tengan acceso directo a estos sistemas salvo que antes entren en contacto con un servidor de autenticación a través de una VPN.

Las intrusiones contra computadoras de intranet tienen más posibilidades de ser lanzadas por intrusos de clase 3, los que tienen el status de personal interno. El personal interno no hace barridos en busca de sistemas vulnerables. No lanzan explotaciones contra sus victimas, no copian propiedades intelectuales a través de la red, enviándolas a computadoras externas. El personal interno inteligente hace uso de los privilegios que le concede su organización para obtener un acceso autenticado pero inadmisible a información privilegiada en unidades de disco USB o en DVD y salen por la puerta. Los atacantes de clase 4, o personal interno que lanzan intrusiones desde segmentos inalámbricos emplean las mismas técnicas.

Los métodos de detección basados en red se centran típicamente en los atacantes de clase 1, o intrusos externos que lanzan asaltos desde Internet. Estos atacantes tienen que efectuar un reconocimiento para descubrir computadoras vulnerables. No tienen que elevar sus privilegios para acceder a información privilegiada. Los atacantes de clase 1 que no necesitan dar ninguno de estos pasos son probablemente ex empleados que se vengan de este modo de sus antiguos jefes.

Otra dificultad para los sensores de intranet es la complejidad de la red de confianza y el elevado tráfico que soporta. Los sensores suelen colocarse en el perímetro y en la DMZ porque estas áreas suponen cuellos de botella naturales a través de los cuales tiene que pasar el tráfico. A diferencia de las redes a las que se puede acceder externamente, las redes internas suelen ser una maraña de conmutadores y routers que hacen muy difícil resultar invisible.

Aunque seria deseable vigilarlo todo, esto suele no ser posible. Es recomendable poner sensores en zonas próximas a las ubicaciones que se piensa que tienen un mayor riesgo y claro esta lo que queremos proteger.

3.3 Productos para el Monitoreo de Seguridad de Redes.

No se puede dejar de mencionar, algunas de las innumerables herramientas de software libre que existen en el mercado para el monitoreo de seguridad de redes, también existen herramientas para la búsqueda de vulnerabilidades de redes, sin embargo este trabajo de tesis se centra en las primeras, las cuales se tienen clasificadas en cuatro vertientes.

a) Datos de Contenido Completo.
b) Análisis Adicional de Datos.
c) Datos de sesión.
d) Datos estadísticos.

De esta clasificación se hace gran énfasis en las herramientas para el análisis de datos de contenido completo, donde sólo se mencionan 3 herramientas de software libre de gran popularidad en el ámbito de la seguridad de redes y que no se deben de olvidar, las otras tantas no son menos importantes, simplemente se perdería mucho el contexto del trabajo.

La captura de paquetes en sistemas UNIX empieza y termina con la biblioteca de captura de paquetes libpcap. Desarrollada originalmente por Van Jacobson, Craig Leres y Steven McCanne en el Lawrence Berkeley National Laboratory, libpcap está siendo mantenida activamente en la actualidad por The Tcpdump Group, [3].

Casi todos los sistemas UNIX adjuntan libpcap en su instalación básica, por lo tanto no encontraremos problemas al buscarla en cualquier sistema UNIX o algún sabor de LINUX.

Tcpdump, es una utilidad de captura de paquetes que se despliega con libpcap y es mantenida por los desarrolladores de libpcap donde tiene múltiples Autores. Tanto libpcap como tcpdump tienen un desarrollo muy activo, según muestran las frecuentes comunicaciones efectuadas en las listas de correo de tcpdump.

Por omisión tcpdump pone la interfaz que escucha en modo promiscuo, lo cual significa que se observará todo lo que pase en el puerto al que está conectado el dispositivo.

También se puede también utilizar *snort* [15] como registrador de paquetes, su propósito es de una utilidad de captura y de análisis de paquetes. Snort es especialmente famoso por ser un sistema de detección de intrusiones basado en red, y mucha otra gente dirá que está basado en reglas pero también se puede emplear para capturar y visualizar paquetes. Cuenta una leyenda que Marty Roesch escribió Snort porque deseaba un detector que mostrase el contenido de los paquetes de manera más uniforme que la de otros programas disponibles en 1998. Por omisión los resultados de Snort son básicamente distintos a los de Tcpdump.

Snort puede registrar en dos modos: ASCII y binario. El uso de registrar paquetes en modo ASCII es lento, ¿Qué tanto puede ser lento?

Snort tiene una diferencia notable respecto al resultado de tcpdump y ethereal y es la tendencia que tiene para visualizar ciertos valores en formato hexa-decimal y al finalizar imprimirá estadísticas del tráfico que ha observado.

Ya que se menciona ethereal [19], es imperante recalcar que está dotado de una utilidad gráfica para la captura y análisis de paquetes, ethereal es una de las mejores herramientas de software libre para el tratamiento de redes y análisis de protocolos.

Ethereal puede leer ficheros de captura mediante una invocación efectuada a través de la línea de comandos, según se muestra aquí.

#ethereal –n –r emo.lpc
Sin embargo existe un libro dedicado a ethereal: “Ethereal Packet Sniffing”, donde se expresan las bondades y libertades que se tiene al estar capturando paquetes de contenido completo con este potente sniffer.

Más allá de las herramientas de software libre que se mencionarón, ciertos fabricantes ofrecen productos comerciales para la captura de paquetes. Entre estos se cuentan productos de Network Associates, Sandstorm Enterprises y Niksun. Estos productos ofrecen enormes discos duros y NIC, diseñadas para soportar elevados volúmenes de tráfico.

Otra opción implica el despliegue de sensores que admitan RMON MIB (Remote Monitoring Management Information Base, Base de Gestión de Información para Monitoreo Remoto). RMON emplea SNMP para transmitir estadísticas, alarmas e incluso capturas de paquetes, razón por la cual se menciona RMON, el cual es un estándar de Internet Engineering Task Force (IETF), soportado por varias RFC, y sigue estando en desarrollo activo.

Ya que se han mencionado las herramientas básicas para la captura y análisis de datos de contenido completo. La biblioteca libpcap es la que se utiliza con más frecuencia en herramientas de software libre. Tcpdump es la herramienta de captura de paquetes más popular, con unas capacidades de captura y visualización que se utilizan con múltiples fines y en muchos lugares. Tethereal ofrece más características y una gama más extensa de paquetes decodificados. Snort se puede emplear también como registrador de paquetes, y también como NIDS. Ethereal es el Cadilac de los analizadores de protocolos de software libre, con características que superan a las de sus competidores comerciales.

3.4 Procesos de Seguridad para el Monitoreo de Seguridad de Redes.

Dentro del Monitoreo de Seguridad de Redes se presenta una gama de prácticas recomendadas, como son: La Estimación, Protección, Detección y Respuesta, en la figura 3.4.1 se esclarece el esquema de este proceso de seguridad, sin embargo lo que típicamente se practica son los análisis de seguridad en la red,

para tener en cuenta los valores propios que se tienen que asegurar y así para ser monitoreados.

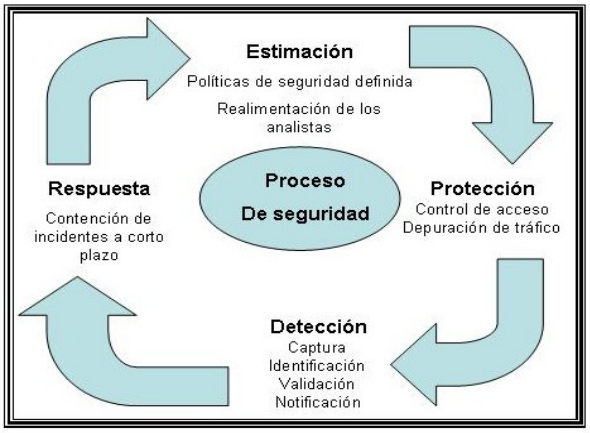

Figura 3.4.1 Proceso de Seguridad para el Monitoreo de Seguridad de Redes.

3.4.1 Estimación.

Una Estimación consiste en realizar acciones destinadas a asegurar la probabilidad de defender con éxito la empresa, o en dado caso lo que se quiera proteger. En el proceso del Monitoreo de Seguridad de Redes, la Estimación significa implementar productos, personas y procesos que sean especialmente adecuados para identificar de forma precisa las intrusiones y mitigar sus efectos.

Para que la estimación lleve a cabo su efecto es imperante implementar una política de seguridad bien definida para los sitios que se estén monitorizando. "*Bien definida*" en el contexto de, describir los tipos de tráfico permitidos y prohibidos en la frontera de la organización.

En el contexto de esta política de seguridad, cualquier cosa que no sean los protocolos especificados es sospechosa de inmediato. De hecho, si se ha impuesto rigurosamente la política, la aparición de cualquier otro protocolo constituye un incidente.

Sin una política de seguridad definida, los analistas y las personas involucradas tienen que preguntarse si los protocolos que se observan estarán autorizados. Los analistas tienen que despejar sus dudas poniéndose en contacto con los administradores del sitio. Una vez que un responsable valida el uso del protocolo, los analistas pueden pasar al siguiente evento. Los analistas que trabajan sin políticas de seguridad bien definidas suelen definir sus propios "perfiles de sitio" en los cuales enumeran los protocolos observados en el pasado y que se consideran aceptables. La creación y mantenimiento de estas listas supone un gasto de tiempo y de cerebro que seria preferible dedicar a la detección de intrusiones.

3.4.2 Protección.

El Monitoreo de Seguridad de Redes no incluye la Protección como aspecto tradicional, ya que esta no es un componente activo de una estrategia de control de acceso, la teoría abarca la prevención de intrusiones o los sistemas de protección contra intrusiones (IPS). Un IPS es un dispositivo de control de acceso, como un firewall, Un sensor de IDS o de Monitoreo de Seguridad de Redes es un sistema para efectuar auditorías o inspecciones del tráfico. El hecho de que un dispositivo de control de acceso tome decisiones en la capa 7 del modelo OSI en lugar de emplear la capa 3 o la capa 4 no justifica cambiar su nombre de firewall a IPS. Cualquier dispositivo que impida o de otro modo bloquee el tráfico es un dispositivo de control de acceso, independiente de la forma en que tome su decisión.

Aunque el Monitoreo de Seguridad de Redes no es, en sí, una estrategia de prevención, la prevención hace ciertamente que el Monitoreo se más efectivo. Hay tres pasos de protección que resultan especialmente útiles: *control de acceso, (que implementa la política) depuración del tráfico y uso de proxies.*

3.4.3. Detección.

La Detección es el proceso consistente en capturar, identificar, validar y notificar eventos sospechosos. Tradicionalmente, ha sido el núcleo del razonamiento que subyace el despliegue de un IDS. Se han dedicado demasiados recursos al problema de la identificación, y demasiados pocos al problema de la validación y notificación. Esta sección es una revisión independiente de fabricantes de la detección de intrusiones empleando los principios del Monitoreo.

Según se ha indicado, la detección requiere cuatro fases:

1.- Captura. El proceso comienza con todo el tráfico. Una vez que el sensor efectúa la captura, envía al analista el tráfico observado. Con respecto a la captura de datos de contenido completo, estos datos son un subconjunto de todo el tráfico que observa el sensor.

2.- Identificación. El analista lleva a cabo una identificación del tráfico que ha observado, y juzga si es *normal, sospechoso o malicioso.* Este proceso envía eventos a la fase siguiente.

3.- Validación. El analista clasifica los eventos, ubicándolos en una de entre varías categorías de incidentes, como lo muestra la tabla 3.4.3.

La validación produce indicaciones y advertencias [31].

Categoría I	Acceso Root/ admin. No autorizado
Categoría II	Acceso de usuario no autorizado
Categoría III	Intento de acceso no autorizado
Categoría IV	Ataque de denegación de servicios con éxito
Categoría V	Prácticas de seguridad incorrectas o Violación de política
Categoría VI	Reconocimiento/sondeos/barridos
Categoría VII	Infecciones de virus.

Tabla 3.4.3. Clasificación de categorías de incidentes

4.- Notificación. El analista reenvía los incidentes a quienes toman las decisiones. Los incidentes contienen datos fehacientes de que se ha detectado algo malicioso.

La notificación también se hace para eventos serios, como los incidentes de las Categorías I, II, IV y VII. Las reglas que gobiernan la notificación deberían de estar en acuerdo entre la operación y sus clientes. Esto es aplicable tanto a tratos internos como a cualquier plan de respuestas contra incidentes, así que es muy conveniente tener unas líneas maestras claras, que identifiquen a quién hay que llamar cuando se produce una intrusión.

3.4.4 Respuesta.

Típicamente el Monitoreo de Seguridad de Redes desempeña dos roles en el proceso de Respuesta a incidentes: contención de incidentes a corto plazo y monitoreo de urgencia.

La contención de incidentes a corto plazo es el paso que se da inmediatamente en cuanto se confirma que se ha producido una intrusión. Cuando un sistema está comprometido, los equipos de respuesta a incidentes reaccionan de una o más maneras siguientes:

- Se apaga el puerto del conmutador a través del cual se conecta a la red el blanco.
- Se quita el cable que une físicamente el blanco a la red.
- Se instala una nueva regla de control de acceso en un router con depuración o en un firewall, para impedir el tráfico entrante y saliente del blanco.

Cualquiera de estos pasos es una respuesta a corto plazo adecuada para el descubrimiento de una intrusión.

La iniciación de Incidentes a corto plazo da al equipo de respuesta a incidentes un tiempo y un espacio muy necesarios para formular una respuesta a medio plazo. Esto puede implicar poner el equipo en una “pecera” para vigilar la actividad

adicional del intruso o parchar y reconstruir a la víctima y volver a ponerla en servicio.

Para un Monitoreo de Seguridad de Redes de urgencia debería de vigilar en busca de signos adicionales del intruso e implementar una monitoreo mejorado. En aquellos casos en los que no se despliegue una captura de datos de contenido completo de veinticuatro horas y en todo el espectro, deberá ponerse en marcha algún tipo de captura limitada de datos de contenido completo que afecte a la víctima y/o al origen de la intrusión.

El Monitoreo de Seguridad de Redes de urgencia no es necesario si el sitio afectado ya se basa en una robusta operación de Monitoreo.

En esta sección se menciona el papel técnico de los administradores sobre un Monitoreo de Seguridad de Redes en las fases de Estimación, Protección, Detección y Respuesta aunque el monitoreo suele asociarse a la detección, el monitoreo desempeña un papel en la mejora de las defensas de la organización a lo largo de todo el ciclo de seguridad. Con este conocimiento de base, los administradores pueden sentirse preparados para ver la forma en que se ponen en acción estas ideas en estudios de caso.

3.5 Historia de los Sistemas Detectores de Intrusos

Con el gran crecimiento de las redes de computadoras, también se ha incrementado las personas que intentan introducirse a ellas sin permiso alguno, y que intentan hacer cosas ilegales adentro de los sistemas, es por eso que es tarea de los Administradores de Redes monitorear, para poder detectar ese tipo de intrusiones no autorizadas.

Así que se tiene la necesidad de definir a un IDS (Intrusión Detection System) como producto que intenta detectar atentados y penetraciones en el sistema

En 1980 James Anderson primero propone auditar los eventos y usar un monitor de pistas, así mismo no se entiende muy bien la idea ya que todos los programas están enfocados a la Denegación de Acceso y Servicio.

Siete años después en 1987 Dorothy Denning presentó un modelo abstracto de un IDS, este modelo fue la primera propuesta del concepto de Detección de Intrusos como una solución al problema de proveer un significado de seguridad en los sistemas computacionales [5].

En 1988 el GUSANO DE INTERNET bien conocido como Morris Word causó en el Internet una indisponibilidad por cerca de 5 días, el incidente trajo en el acto la necesidad de la seguridad computacional, así que en el mismo año Teresa Luna y colaboradores reorganizaron el modelo de Intrusion Detection propuesto por

Denning y crearon IDES (Intrusión Detection Expert System), este sistema fue diseñado para detectar los atentados de Intrusión en un sencillo host. En 1995 una nueva versión de este fue desarrollada, el famoso NIDES (Next Generation Intrusion Detection Expert).

Al finales de 1988 el sistema Haystack fue desarrollado para asistir a los Oficiales de Seguridad de la Fuerza Aérea, para detectar malversaciones, malos usos de los mainframes usados en las bases de la Fuerza Aérea y MIDAS (Multics Intrution Detection and Alerting System) fue creado por las mismas razones, pero para la National Computer Security Center´s Multics mainframe.

En 1989 se tenía, Wisdorm and Sense de Los Alamos National Laboratory e Information Security Officer´s Assistant (ISOA) for Planning Research Corporation.

En 1990. Un nuevo concepto fue introducido con NSM (Network Security Monitor), ahora llamado *Network Intrusion Detection* o NID este se instala y audita los rastros de computadoras así como comportamientos sospechosos que fueron detectados por monitoreo pasivo de una red LAN.

Dadas las circunstancias en 1991 una nueva idea fue introducida con el NADIR (Network Anomaly Detection and Intrusion Reporter) y DIDS (Distributed Intrution Detection Systems), los datos se auditan de múltiples hosts donde se recolectan y agregan en orden para detectar direcciones de ataques de un conjunto de hosts.

Para 1994 las cosas cambian donde Mark Crosbie y Gene Spafford sugieren el uso de agentes autómatas para ordenar y mejorar la escalabilidad en el mantenimiento, la eficiencia y la alta tolerancia de un Intrusión Detection System.

En 1996 se diseñan y se implementan los GrIDS, este sistema facilita la detección a larga escala de ataques coordenados.

Finalmente en 1998 Ross Anderson y Abida Khattak ofrecen un desarrollo innovador para la detección de intrusos por la incorporación, (Informational retrieval), dentro de las herramientas de la detección de intrusiones así como la investigación en el campo continua vemos que esto es una respuesta a los requerimientos de seguridad y otras áreas como las redes móviles.

En la *figura 3.5.1* se puede apreciar la línea del tiempo de los IDS´s desde 1980 con James Anderson hasta el año 1999.

El estudio y el proceso de desarrollo de los Detectores de Intrusos no termina ahí, se han adoptado nuevas técnicas de detección de intrusos más eficaces y drásticas ya que la necesidad ha ido cambiando con el pasar de los años, en el penúltimo capítulo se describirá el sistema detección de intrusiones basado en entropía, en cual está encargado de evaluar el tráfico de red.

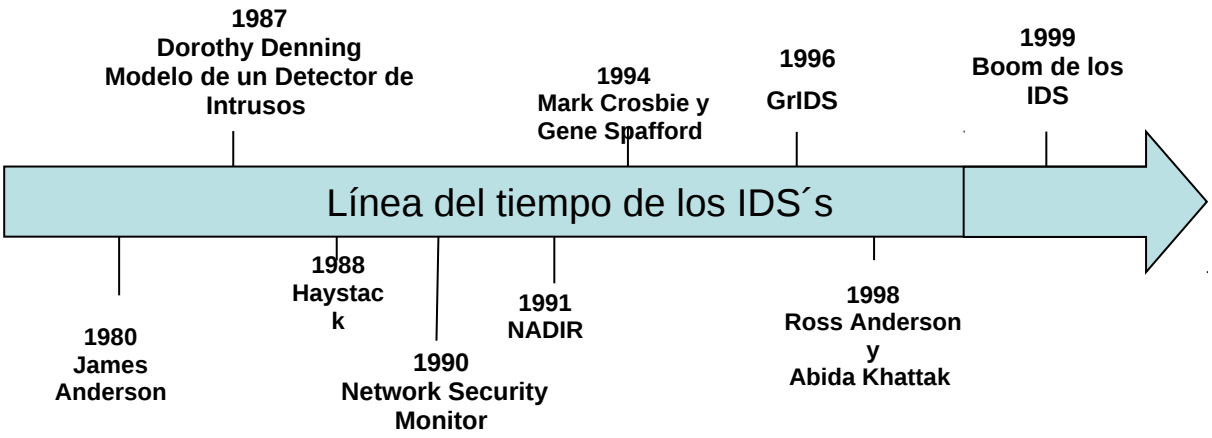

Figura 3.5.1. Línea del tiempo del desarrollo de los Detectores de Intrusos.

Como *intrusión se* debe de entender que es la realización de un acto no autorizado, como puede ser:

a) Acceso al sistema
b) Ejecución de programas sin autorización.
c) Ataque a una red informática

De aquí se dice que una Intrusión también es nombrada como Ataque Dirigido, aunque existe una controversia sobre el ataque, ya que no cuenta en la definición la recolección de información.

Los IDS tienen la característica de que previenen ataques y también los detectan en un tiempo muy reducido, así diríamos que detectan ataques en caliente, también fortalecen el trabajo de la Seguridad de la Información siguiendo dos métodos de trabajo fundamentales: La Prevención y la Reacción.

Entonces se entiende por un IDS como un sistema de seguridad que analiza información de varias áreas de una computadora o de una red para identificar posibles brechas de seguridad. Sus funciones incluyen:

- *Monitoreo de los usuarios y actividades del sistema.*
- *Analizar las configuraciones del sistema.*
- *Aseguramiento del sistema y la integridad de los archivos.*
- *La habilidad de reconocer típicos patrones de ataque.*
- *Analizar patrones de actividad anormal.*
- *Violaciones hacia las Políticas de Seguridad.*

Estas funciones son las diferentes funciones que dan idea y motivación al desarrollo de los Sistemas Detectores de Intrusos, y esto se logra introduciendo una prevención para después reaccionar.

- La Prevención.

Esto es referible a las actividades de los intrusos, esto se logra escuchando el tráfico, es decir se realiza “En caliente para detectar al sospechoso”.

- La Reacción.

Aquí analizamos las bitácoras en sistemas protegidos y las trazas de los servicios de la red, se tratan de detectar patrones que evidencian actividades de intrusión realizadas por elementos malignos.

Las tecnologías de los IDS implementan en sus herramientas tres componentes fundamentales, como se muestra en la figura 3.5.2.

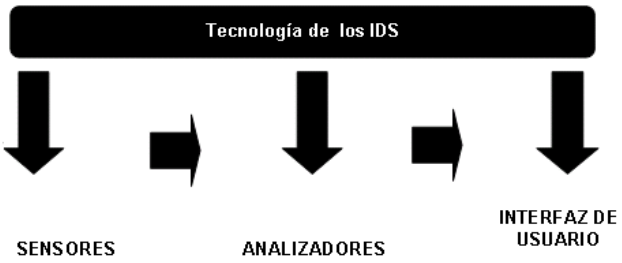

Figura. 3.5.2. Esquema de los componentes básicos de los Detectores de Intrusos.

Primeramente, los *sensores* tienen la responsabilidad de coleccionar datos de interés y enviar esta información a la parte de los *analizadores*. La información puede ser obtenida de cualquier parte del sistema que contenga evidencia de intrusiones. Esto es, paquetes provenientes del análisis de tráfico, secciones de las bitácoras y otros. Los componentes denominados analizadores atienden la información que reciben de los sensores o de otro analizador. Su responsabilidad fundamental es determinar si ha ocurrido una intrusión y presentar pruebas de esta afirmación. Como resultado de su trabajo debe indicar la intrusión detectada de forma clara y, en muchos casos, referenciar o ejecutar un grupo de medidas que permitan contrarrestar los efectos de la intrusión.

La interfaz de usuario tiene un uso trivial pues permite al usuario, probablemente el administrador de la seguridad, observar las salidas del sistema y controlar su comportamiento y así generar una respuesta [15].

3.6 Clasificación de los Sistemas Detectores de Intrusos:

Existen varios criterios para clasificar a los IDS´s, la siguiente figura 3.5.3 muestra gráficamente los criterios de clasificación de los IDS´s

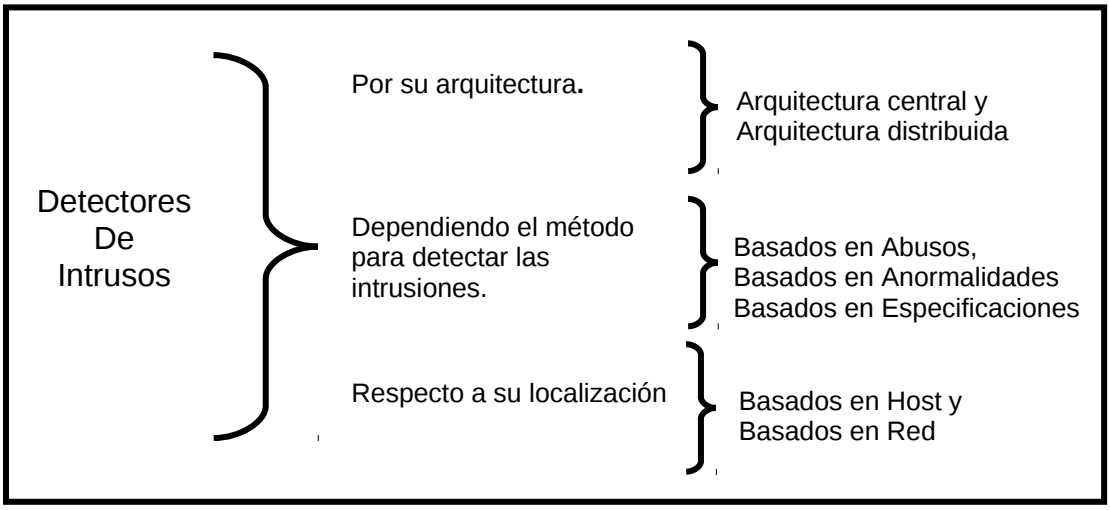

Figura 3.5.3 Clasificaciones de los IDS.

3.6.1 IDS Basados en su Arquitectura

Con respecto a su Arquitectura pueden ser clasificados en dos partes: porque su Arquitectura Central y por tener una Arquitectura Distribuida.

- *En una arquitectura central,* todos los datos recolectados del análisis de varios hosts son procesados por un simple servidor de detección de intrusiones. Esto trabaja muy bien para pequeñas redes de computadoras pero definitivamente es inadecuado para redes muy grandes ya que decrementa el rendimiento de los IDS´s.

- *La arquitectura distribuida o descentralizada*, presenta un análisis distribuido de los datos auditados. Varios servidores de IDS son diseminados a través de las redes y entonces analizan los datos recolectados en un lugar específico.

3.6.2 IDS Basados en Intrusiones.

En la literatura se encontrarán muchísimas clasificaciones para los Sistemas Detectores de Intrusos pero al terminar de revisar todas, se darán cuenta que todos caen dentro de las siguientes categorías.

- *Detección por abusos* esta detección es identificada por un ataque conocido, que son identificados por una biblioteca de patrones de ataque. En general cada biblioteca requiere un conocimiento experto de la construcción y esta necesita ser actualizada regularmente para identificar

nuevos ataques. Su contenido puede ser basado en experiencias con ataques del pasado y es por eso que se tienen ataques futuros.

La representación más común, son las secuencias de bytes las cuales se conocen como ráfagas de ataque, (Todos los NIDS usan esa técnica) las llamamos señales de patrones a nivel byte, su principal ventaja es la precisión, obviamente si el patrón de byte es definido podemos claramente identificar el ataque.

Uno de los productos Open Source existentes en el mercado que integra esta técnica es el Snort, donde este NIDS aparte de detectar abusos, escanea puertos y reporta las violaciones que se encuentran en ellos. (Véase http://www.snort.org)

- *Detección por anomalías,* esta parte es referida hacia una desviación del comportamiento esperado. Es decir, cada usuario tiene un perfil de actividades y al observar que la actividad se desvía significativamente una alerta es lanzada previniendo el desorden.

Un modelo clásico en la detección de intrusiones basado en anomalías es el NIDS de Dorothy Denning que se verá con gran detalle hasta estar dentro del alma misma del modelo. También se podrá apreciar que usa una combinación de métricas estadísticas y modelos de umbrales para configurar los intervalos de tiempo y poder etiquetar algunas de las anomalías. El acento principal de la detección de anomalías está basado en la hipótesis de que el comportamiento legítimo de los usuarios son completamente predecibles, lo cual en lo particular se duda mucho (quien no se ha parado a las 2:00 a contestar el correo electrónico o a leer), consecuentemente los problemas de los NIDS basados en anomalías es definitivamente su alto índice de falsos positivos. Sin embargo los estudios recientes sugieren que los detectores basados en anomalías trabajan bien para un dominio pequeño de aplicaciones bien definido.

- Detección por especificación. Los sistemas basados en especificación caracterizan un explícita especificación del comportamiento permitido, Si se observa actividad que no es cubierta por la especificación esta es abanderada como maliciosa. Esta categoría cae muy bien en los IDS basados en host.

  La detección basada en especificación es la inversa de la detección que esta basada en abusos y en principio ambos son potencialmente poderosos, evidentemente si se saben caracterizar y aplicar.

3.6.3 IDS Basados en su Localización.

A continuación se da la clasificación típica de los IDS´s.

- IDS Basados en Host*:* Los IDS basados en host (HIDS) son los IDS´s más viejos, ellos recolectan información de cada una de las computadoras que monitorean. En esa información ellos reflejan la actividad que ocurre en el sistema en particular, toman información de cada sistema operativo y auditan los rastros las bitácoras a nivel kernel, o los logs del sistema, logs a nivel usuario.

Una desventaja de los HIDS es el hecho de que generan algunos falsos positivos como los IDS basados en Red (NIDS).

Los HIDS pueden reconocer ataques que los NIDS no reconocen en el mismo sitio como una conexión encriptada y programas maliciosos (Caballos de Troya), sin embargo la desventaja es que son algo difíciles de manejar y cada host para ser monitoreado debe de ser configurado individualmente.

- IDS Basados en Red (NIDS). Este IDS detecta ataques por la captura de paquetes que son analizados en la red, así se puede monitorear pasivamente el tráfico de red entre múltiples interconexiones de hosts, escuchando en un segmento de la red o el switch.

Los NIDS requieren de avance administrativo y de recursos financieros como los HIDS, sin embargo ellos pueden tener dificultad al procesar todos los paquetes y grandes problemas al operar por detrás de los switches de las redes, como el dividir la red en otras pequeñas, dedicar segmentos de red, y no pueden analizar información cifrada.

Todos los IDS usan técnicas basadas en detección de conductas de intrusión o en el conocimiento basado en detectar las intrusiones para identificar ataques.

Para finalizar este capítulo es bueno aclarar que la Detección de Intrusiones es una parte integral de la seguridad en cómputo. Donde ellos nos ayudarán a que prevalezca la Confidencialidad, Integridad y Disponibilidad de nuestros datos.

Ahora se puede cambiar un poco la definición de sistemas detectores de intrusiones, viendo el mundo tan vasto que existe en ellos como el proceso de monitorear redes de computadoras y sistemas por violaciones de políticas de seguridad donde no se debería olvidar algunas cosas vitales:

- La Información de los registros de eventos es esencial para poder evaluar
- Los análisis que encuentran señales de intrusión son vitales para poder actuar

- Un comportamiento que genera reacciones puede ser el principio de una Denegación de Servicio.

A principios de siglo la Detección de Intrusiones era una tecnología relativamente joven como una rama de la seguridad no criptológica, sin embargo no dejan de sorprender los artículos de USENIX.

Ahora que se tiene una visión mucho mas general del objetivo que persigue la detección de intrusos y el monitoreo de seguridad en redes, es necesario revisar el siguiente modelo: ”*Sistema Experto Detector de Intrusos*”, el cual es de suma importancia en el estudio de la detección de intrusos ya que fue el marco de referencia para lo que hoy en día aun se conocen como Detectores de Intrusos, su única desventaja es que fueron hechos para mainframes y no contemplaban intrusiones por dispositivos externos.

Capítulo 4
Modelo de un Sistema Detector de Intrusos.

En la década de los 80´s a medida que el número de sistemas crecía, también crecía el número de eventos para su análisis. Esta tarea era tan engorrosa que se volvía humanamente imposible. Las autoridades militares norteamericanas se dieron cuenta que el uso masivo de computadoras requería un sistema que automatizara las auditorias.

James P. Anderson fue la primera persona capaz de documentar la necesidad de tener un mecanismo que automatizara la revisión de eventos de seguridad y en 1980 redactó un informe que sería el primero de los futuros trabajos de la detección de intrusiones. Uno de los objetivos de este informe era la eliminación de información redundante o irrelevante en los registros de sucesos.

Anderson propuso un sistema de clasificación que distinguía entre ataques internos y externos basado en que si los usuarios tenían permisos de acceso o no.

Ideó un sistema para dar solución al problema de los intrusos que se habían apoderado de cuentas legítimas. El cual debía de distinguir entre el comportamiento normal o inusual de las cuentas basándose en patrones de uso basándose a partir del análisis de estadísticas del comportamiento del usuario.

El siguiente modelo de Detección de Intrusos desarrollaría esta idea y sería el marco de referencia para los siguientes sistemas detectores de intrusos, es por eso que es de gran valor analizar este modelo en su totalidad.

Resumen.

Así este modelo que se describirá a continuación intenta captar las penetraciones y otras formas de abuso en las computadoras, basándose en las hipótesis de que las violaciones de seguridad, pueden ser detectadas por monitoreos y sistemas que auditan los registros anormales del sistema.

El modelo incluye perfiles que representan el comportamiento de sujetos con respecto a objetos en términos de métricas y modelos estadísticos, las reglas de conocimiento acerca del comportamiento de auditar los registros y detectar anomalías de comportamiento y a su vez es independiente de cualquier sistema en particular, aplicaciones de ambiente, vulnerabilidades de sistema o algún tipo de intrusión en cualquier lugar dando un marco para un propósito general de un sistema experto de detección de intrusos.

4.1 El Modelo de Dorothy Denning.

Es muy importante analizar y desmenuzar a fondo el desarrollo de este modelo, para algunos el mejor *("sistema hibrido")* que se haya presentado, este ha sufrido muchas criticas por su arquitectura (no se puede esperar que salve de todo) y claro sus bondades, sin olvidar que es de las principales motivaciones para que se hayan creado otras nuevas direcciones en la Detección de Intrusiones.

El desarrollo y la conceptualización de un Sistema Experto Detector de Intrusos en tiempo real, es motivado por 4 razones primordiales:

1.- Desde que los sistemas existen tienen defectos de seguridad y estos claro está son susceptibles a intrusiones, penetraciones y otras formas de abuso. En encontrar y fijar todas esas deficiencias no es factible por razones técnicas y económicas.

2.- Existen sistemas con un comportamiento conocido que no son fáciles de reemplazar, por sistemas que son principalmente más seguros porque los sistemas tienen atractivas características que son olvidadas en los sistemas más seguros, o no se pueden reemplazar nuevamente por razones económicas.

3.- Desarrollar sistemas que son absolutamente seguros es extremadamente difícil y generalmente imposible.

4.- Incluso los sistemas más seguros son vulnerables por abuso de gente que está adentro de ellas quienes maliciosamente obtienen privilegios para después hacer daño.

Con el pasar de los años se ha notado que esta motivación se ha ido incrementando ya que con el desarrollo de los Sistemas Operativos los sistemas comienzan a hacerse más complicados en su administración,

Por lo tanto es valido el mencionar un quinto motivo de hoy en día:

5.- Por la falta de administración.

El modelo está basado en la hipótesis de la explotación de las vulnerabilidades de un sistema que involucra un uso anormal como pueden ser violaciones de seguridad que son detectadas por patrones anómalos del sistema.

A continuación se mencionan algunos ejemplos Ilustrativos que motivaron al desarrollo del Sistema Experto Detector de Intrusos**:**

Intentando forzar la entrada, (Break-in). Alguien que intentó entrar forzadamente en un sistema pudo generar un alto índice anormal de fallo de la contraseña con respecto a una sola cuenta o al sistema en su totalidad.

Enmascarado o entrada forzada exitosa, (Masquerading or sucessful break-in). Alguien que se logró un login en un sistema con una cuenta y contraseña no-autorizadas pudo tener un diferente tiempo de conexión, localización o tipo de conexión que el de la cuenta legítima del usuario. Además, el comportamiento de los penetradores puede diferenciar considerablemente de él, del legítimo usuario. Particularmente, él pudo pasar la mayor parte de su tiempo curioseando a través de directorios y ejecutando comandos del estado de sistema, mientras que el usuario legítimo pudo concentrarse en corregir o compilando y conectándose a programas. Muchas de las entradas forzadas han sido descubiertas por los oficiales de seguridad u otros usuarios en el sistema quienes han notado al supuesto usuario con un comportamiento extraño.

Penetración del usuario legítimo, (Penetration by legitimate user). Un usuario que intentaba penetrar los mecanismos de seguridad en el sistema operativo pudo ejecutar diferentes programas o accionar más violaciones de protección de intentos de acceso a archivos no-autorizados o a programas. Si su intento tiene éxito, tendrá el acceso a los comandos y archivos no permitidos.

Filtración por parte del usuario legítimo, (Leakage by legitimate user). Un usuario que intentaba filtrarse a documentos sensibles pudo registrarse en el sistema en horas inusuales o encaminar datos a las impresoras lejanas o que no son usadas normalmente.

Inferencia del usuario legítimo, (Inference by legitimate user). Un usuario intenta obtener datos no-autorizados de una base de datos a través de agregación e inferencia, así pudo recuperar más expedientes que lo usual.

Trojan Horse, (Caballo de Troya). El comportamiento de un caballo de Troya es un substituto de programa que puede ser diferente que el legítimo en términos de CPU y actividad.

Virus, (Virus). Un virus en el sistema puede causar un incremento en la frecuencia de los archivos ejecutables, reescribir, almacenar, así el programa comienza ejecutándose como un virus que se propaga.

Denegación del Servicio, (Denial-of-Service). Un intruso puede monopolizar un recurso o red, así la red puede tener una alta actividad anormal con respecto a los recursos, mientras la actividad de los otros usuarios es normalmente baja.

Por supuesto, las formas antes mencionadas de uso *aberrante* se pueden también vincular con acciones sin relación a la seguridad. Podían ser una señal de los cambios de trabajo del usuario, adquiriendo nuevas habilidades o haciendo errores de mecanografía; actualizaciones del software o cambiando la carga laboral en el sistema. Un objetivo importante de nuestra investigación actual es

determinar qué actividades y medidas estadísticas proporcionan el mejor poder de discriminación, es decir, tener un alto índice de la detección y un índice bajo de falsas alarmas.

El modelo es independiente de cualquier sistema, aplicación, vulnerabilidad del sistema o tipo de intrusión, de tal modo se proporciona un marco para un sistema experto de intrusión-detección de uso general que es concebido como IDES.

4.1.1 Componentes Principales del Modelo.

El modelo puede ser considerado como un sistema de patrones basado en reglas. Cuando un registro de auditoría es generado, este es relacionado nuevamente con un nuevo perfil. El tipo de información en los perfiles comparados determina qué reglas aplicar para actualizar las características, comprobación para comportamiento anormal y reporte de anomalías detectadas. El oficial de seguridad asiste estableciendo las plantillas del perfil para supervisar las actividades, pero las reglas y las estructuras del perfil son en gran parte independientes del sistema.

La idea básica es supervisar las operaciones estándares en un sistema objetivo: conexiones, comandos y programas en ejecución, archivos y dispositivos de acceso, etc., buscando solamente las desviaciones en uso. "*El modelo no contiene ninguna característica especial para el manejo con acciones complejas que explotan un conocimiento o un flujo de seguridad sospechoso en un sistema"*; de hecho, no tiene ningún conocimiento de los mecanismos o deficiencias de la seguridad del sistema objetivo. Aunque un mecanismo de detección basado en flujo puede tener algún valor, esto debería ser considerablemente más complejo y podría ser inútil para contener las intrusiones que explotan las deficiencias que no se sospechan o con vulnerabilidades en relaciones personales. Detectando la intrusión, sin embargo, el oficial de seguridad puede localizar mejor las vulnerabilidades.

4.1.2 Sujetos y Objetos.

"Los sujetos" son los iniciadores de acciones en el sistema objetivo. Un sujeto es típicamente usuario en una terminal, pero podría también ser un proceso en acción a nombre de usuarios o de grupos de usuarios, o podría ser el sistema en sí mismo. Toda la actividad surge a causa de comandos iniciados por sujetos. Los sujetos pueden ser agrupados en diferentes clases con el propósito de controlar el acceso a los objetos en el sistema. Los grupos de usuario pueden coincidir.

"Los objetos" son los receptores de acciones y típicamente incluyen las entidades tales como archivos, programas, mensajes, registros, terminales, impresoras, y las estructuras del usuario o programas creados. Cuando los sujetos pueden ser recipientes de las acciones (por ejemplo, correo electrónico), entonces esos sujetos son considerados a ser objetos en el modelo.

Los objetos son agrupados en clases por tipo (programa, archivo de texto, etc.). La estructura adicional también puede ser impuesta, por ejemplo: los registros pueden ser agrupados en archivos o relaciones de base de datos; los archivos pueden ser agrupados en directorios. Diferentes ambientes pueden requerir diferentes objetos, por ejemplo: para algunas aplicaciones de bases de datos, el nivel de registro puede ser deseado, mientras que para más aplicaciones, un archivo o nivel del directorio puede ser suficiente.

4.1.3 Registros de Auditoría.

Los registros de auditoría son 6-túplas que representan las acciones realizadas por sujetos en objetos:

<Subject, Action, Object, Exception-Condition, Resorce-Usage, Time-Stamp>

Donde:

- **Action:**
  Operación realizada por el sujeto en ó con el objeto por ejemplo: login, logout, read, execute.

- **Exception-Condition:**
  Denota cual, si cualquier condición de excepción es aumentada de regreso. Esta debería ser la actual condición de excepción actual real lanzada por el sistema, no solamente la aparente condición de excepción regresará al sujeto.

- **Resource-Usage:**
  Lista los elementos cuantitativos, donde cada elemento da la cantidad usada de algún recurso, por ejemplo: El número de líneas o páginas impresas, el número de registros leídos o escritos, tiempo de CPU o unidades 1/0 usadas, tiempo usado en sesión.

- **Time-stamp:**
  Únicos Tiempo/fecha de stamp que identifica cuando ocurrió la acción.

Se asume que cada campo se identifica así mismo, cualquiera implícitamente o explícitamente, por ejemplo: el campo de acción también implica el tipo de campo previsto del objeto o bien el campo del objeto en si mismo especifica su tipo. Si los registros auditados se recogen para múltiples sistemas, entonces un campo adicional es necesario para un identificador del sistema.

Desde que los registros de auditoría especifican un sujeto y objeto, estos son conceptualmente asociados con alguna célula en una "matriz de auditoría", cuyas filas corresponden a los sujetos y las columnas a los objetos.

La matriz de auditoría es análoga al modelo de protección de *"matriz de acceso",* que especifica los derechos del sujeto de acceder objetos; es decir, las acciones de cada sujeto están autorizadas a realizarse en cada objeto.

Este modelo de la detección de intrusiones difiere del modelo de matriz de acceso substituyendo el concepto de la "acción realizada" (como evidencia de los registros auditados asociado a una célula en la matriz) para la "acción autorizada" (según lo especificado por un registro auditado asociado con la célula en la matriz). De hecho, desde que la actividad es observada sin considerar la autorización, se asume implícitamente que los controles de acceso en el sistema permitieron que la acción ocurriese.

La tarea de la detección de intrusión es determinar si la actividad es suficientemente inusual para sospechar una intrusión. Cada medida estadística usada para este propósito es calculada (computada) para los registros de auditoría asociados con una o más células en la matriz.

Más operaciones en un sistema involucran múltiples objetos. Por ejemplo copiar un archivo involucra el programa para copiar, el archivo original y la copia. Compilar involucra el compilador, el archivo fuente y un objeto, el archivo de programa y posiblemente archivos intermedios y además archivos fuentes referidos a través de sentencias "Include", mandar un mensaje electrónico por mail, involucra el programa mail, posiblemente múltiples destinatarios en el "PARA" y "CC" con copia y posiblemente los archivos "Include".

El modelo descompone toda actividad en acciones de objetos sencillos y cada registro de auditoría en un objeto.

Copiar un archivo por ejemplo: es descompuesto en una operación ejecutable en el comando *copy* y leer la operación de el archivo fuente y una operación escribir en el archivo destino.

Lo siguiente ilustra: Registros Auditados, generados en respuesta al comando.

COPY GAME.EXE to <Library> GAME.EXE

Emitido por el usuario Smith para copiar un archivo ejecutable GAME.EXE en el directorio <Library>; se aborta la copia porque Smith no tiene permisos para escribir en <Library>.

(Smith, execute, <Library> COPY.EXE, 0, CPU=00002, 11058521678)
(Smith, read, <Smith> GAME.EXE, 0, RECORDS=0, 11058521679)
(Smith, write, <Library> GAME.EXE, write-viol, RECORDS=0, 11058521680)

La descomposición de acciones complejas tiene tres ventajas:

1.- Desde que los objetos son las entidades protectoras de un sistema, la descomposición es consistente con los mecanismos de protección del sistema. Así, IDES puede descubrir potencialmente ambos intentos de subversión de los controles de acceso (observando una anormalidad en el número de las condiciones de excepción de retroceso) y la subversión acertada (observando una anormalidad en el sistema de objetos accesibles al sujeto).

2.-Los objetos simples de registros de auditoría simplifican avances del modelo y su uso.

3.-Los registros auditados producidos por sistemas generalmente contienen un solo objeto, aunque algunos sistemas proporcionan una manera de conectar a través de los registros de auditoría asociados con un paso de trabajo, “job step” (por ejemplo copia o compilación) eso es que todos los archivos accesados durante la ejecución de un programa pueda ser identificado.

El host es responsable de revisar y de estar transmitiendo registros de auditoría para el Sistema de Detección de Intrusiones para su análisis (puede también guardar un rastro auditado independiente).

El tiempo en el cual los registros de auditoría son generados, determinan qué tipo de datos es disponible. Si el registro de auditoría para alguna acción es generado al mismo tiempo que una acción se requiere, esto es posible en la medida, que ambos exitosamente o no exitosamente intenten el desarrollo de la actividad, aunque la acción podría abortar, por ejemplo: porque es de una violación de protección o causa un fallo en el sistema. Si este es generado cuando la acción se completa, es posible medir los recursos consumidos por la acción y las condiciones de excepción que pueden causar la acción para terminar

anormalmente (por ejemplo: debido al desbordamiento del recurso). Así, la revisión de una actividad después de que se completa, tiene la ventaja de proporcionar más información, pero la desventaja de no permitir la detección inmediata de anormalidades, especialmente ésas relacionadas con *break-ins* y fallos del sistema.

Así, las actividades tales como conexión, ejecución de comandos de alto riesgo (por ejemplo: adquirir privilegios especiales del *"súper usuario o root"*), o acceso a los datos sensibles que deben ser revisadas cuando son intentos de penetración pueden ser detectados inmediatamente.

Si los datos del recurso usado también son deseados, la revisión adicional también puede ser realizada por completo y calificada como buena.

Por ejemplo, el acceso a una base de datos que contiene datos altamente sensibles puede ser monitoreado cuando el acceso es intentado nuevamente, cuando es completado para reportar el número de registros recuperados o actualizados.

La mayoría de los sistemas de monitoreo de actividad de sesión de auditoría existentes se inicializan al mismo tiempo (login), cuando el tiempo y la localización de una conexión es registrada la terminación (el logout), cuando los recursos consumidos durante la sesión son registrados. Sin embargo, no monitorean el comienzo y el final del comando y ejecución del programa o acceso al archivo. IBM's System Management Facilities (SMF), por ejemplo, revisan solamente la terminación de estas actividades.

Aunque los mecanismos de revisión de sistemas existentes se aproximan al modelo, son típicamente deficientes en términos de monitorear actividades y grabar estructuras generadas.

Por ejemplo: UNIX usa comandos para monitorear pero no tiene acceso al archivo o violaciones de protección del archivo. Algunos sistemas no graban todas las fallas de los login´s. *Programas*, incluyendo programas del sistema, invocados por debajo del nivel de comando no son explícitamente monitoreados (su actividad es incluida en un programa principal). El nivel en el cual la revisión debe ocurrir, sin embargo, es confuso, es desde que demasiadas intervenciones podrían degradar seriamente el funcionamiento en el host o sobrecargar el sistema de la detección de intrusiones.

Las deficiencias en las estructuras de registro también están presentes. La mayoría de los registros de auditoría SMF, por ejemplo, no contienen un campo sujeto; el sujeto debe ser reconstruido por el ligado de los registros asociados con un trabajo dado.

Las violaciones de protección algunas veces se proporcionan con formatos de registro separados en vez de una condición de excepción en un registro común, las fallas de las passwords de la VM como la conexión, por ejemplo, se manejan de esta manera (hay registros separados de conexiones exitosos y fallas en las contraseñas).

Otro problema con los registros de auditoría existentes es que contienen poca o nada de información descriptiva para identificar los valores contenidos en ellos.

Cada tipo de registro tiene su propia estructura, y el formato exacto de cada tipo de registro se debe saber para interpretar los valores. Un formato de registro uniforme con datos de identificación propia sería preferible de modo que el software de detección de intrusiones pueda ser un sistema independiente. *Esto podría ser logrado modificando el software que produce los registros de auditoría del host, o escribiendo un filtro que traduzca los registros en un formato estándar.*

4.1.4 Perfiles.

Un perfil de actividad caracteriza el comportamiento de un sujeto dado (o un conjunto de sujetos) con respecto a un objeto dado (o conjunto de ellos), de tal modo sirviendo como una firma o descripción de la actividad normal para su respectivo sujeto(s) y objeto(s).

El comportamiento observado es caracterizado en términos de métrica estadística y modelo. Una métrica es una variable aleatoria ***x*** que representa una medida cuantitativa acumulada en un período. El período puede ser un intervalo fijo de tiempo (minuto, hora, día, semana, etc.) o el tiempo entre dos eventos intervención-relacionados (es decir, entre una conexión y desconexión, iniciación del programa y terminación del programa, archivo abierto y archivo cerrado, etc.). Las observaciones (muestran puntos) $\mathbf{x_i}$ de ***x*** obtenidas de los registros de auditoría son usados junto con un Modelo Estadístico para determinar si una nueva observación es anormal. El Modelo Estadístico no asume sobre la distribución subyacente de ***x;*** todo el conocimiento de ***x*** es obtenido de observaciones.

Antes de describir la estructura, la generación y el uso del perfil, primero se discuten las métricas estadísticas y sus modelos.

4.1.4.1 Métricas.

Definimos 3 tipos de métricas:

- Contador de Evento:

x es un número de registros de auditoría que satisface algunas propiedades que ocurren durante un periodo (cada registro de auditoría corresponde a un evento) Ejemplo: El número de conexiones durante una hora, el número de veces que un comando es ejecutado durante una sección de conexión y el número de passwords fallidos durante un minuto.

- Contador de Intervalos:

x es la longitud del tiempo entre dos eventos relacionados es decir, la diferencia entre los *time-stamps* en los respectivos registros de auditoría. Un ejemplo es la longitud del tiempo entre las sucesivas conexiones en una cuenta.

- Medida del Recurso:

x es la cantidad de recursos consumidos por una cierta acción durante un período según lo especificado en el campo del Recurso-Uso de los expedientes de la intervención. Los ejemplos son el número total de páginas impresas por un usuario por día y cantidad total de tiempo consumido del CPU por algún programa durante una sola ejecución. Obsérvese que una medida del recurso en el modelo de la detección de intrusiones está puesta en ejecución como un contador de acontecimientos o contador de intervalos en la tarjeta del sistema. Por ejemplo, el número de páginas impresas durante una sesión de conexión se pone en ejecución en la tarjeta del sistema como contador de acontecimientos que cuenta el número de los acontecimientos de la impresión entre la conexión y la desconexión, el tiempo del CPU consumido por un programa como contador de intervalos que funciona entre la iniciación del programa y la terminación. Así, mientras que los contadores de acontecimientos y los contadores de intervalos miden los acontecimientos en el nivel de registros de auditoría, las medidas del recurso adquieren datos de los acontecimientos en la tarjeta del sistema que ocurren en un nivel debajo de los registros de auditoría. De tal modo el campo del uso del recurso de los registros de auditoría proporciona medios para reducción de datos de modo que pocos eventos necesiten ser registrados explícitamente en los registros de auditoría.

4.1.4.2 Modelo Estadístico.

Dada una métrica de variable aleatoria *x* y *n* observaciones $X_{1,\ldots},X_n$ el propósito del modelo estadístico de ***x*** es que determine si una nueva observación X_{n+1} es anormal respecto a las observaciones previas.

- Modelo Operacional*:*

Este modelo está basado en el supuesto conocimiento operacional que anormalmente puede ser decidida por la comparación de una nueva observación de ***x*** contra límites fijos. Aunque los previos observaciones de la muestra de ***x*** no son usados, probablemente los límites son determinados de observaciones anteriores del mismo tipo de variables. El Modelo Operacional es más aplicable a las métricas donde la experiencia ha mostrado que ciertos valores son frecuentemente ligados con intrusiones. Un ejemplo es un contador de eventos para el número de contraseñas, "passwords" que fallan durante un breve periodo, donde más de 10 decimos que se hizo un intento de Break-in.

- Modelo de Desviación Estándar y Medio:

Este modelo se basa en el conocimiento que se tiene sobre $X_{1,\ldots},X_n$ que son la desviación estándar y media según lo determinado a partir de estos dos momentos:

$$sum = x_1 + \ldots + x_n$$

$$sumsquares = x_1^2 + \ldots + x_n^2$$

Obviamente la $$media = sum/n$$

$$stdev = sqrt\ (sumsquares / (n+1) - media^2\ )$$

Una nueva observación x_{n-1} está definida para ser anormal si cae fuera del intervalo de confidencialidad esto puede ser una desviación estándar de la media de un parámetro d:

$$media+d*stdev$$

Por la desigualdad de Chebyshev, la probabilidad de que un valor caiga fuera del intervalo es al menos $1/(d^2)$ para $d=4$, por ejemplo, esto es a lo mas 0.0625 Nótese que las ocurrencias 0 o (null) deben ser incluidas para no posponer datos.

Este modelo es aplicable al conteo de eventos, contadores de intervalos y medidas del recurso acumulados sobre un intervalo de tiempo fijo o entre dos eventos relacionados. Esto tiene dos ventajas sobre un modelo operacional. Primero esto no requiere ningún conocimiento previo acerca de la actividad normal para fijar limites, en su lugar aprende y constituye una actividad normal para estas observaciones, y los intervalos de confidencialidad automáticamente reflejan este conocimiento creciente. Segundo, porque los intervalos de confidencialidad dependen en los datos observados, que es considerado normal, para un usuario puede ser considerablemente diferente que otro.

Una variación leve en el Modelo de Desviación Estándar y medio es para computadoras grandes con un gran peso y valores recientes.

- Modelo Multivariable*:*

Este modelo es similar al Modelo de Desviación Estándar y medio, excepto que este está basado en correlaciones entre dos o más métricas. Este modelo sería útil si los datos experimentales han mostrado el poder discriminatorio que puede ser obtenido de combinaciones de medidas relacionadas más bien individuales, por ejemplo el tiempo del CPU y 1/0 unidades usadas por un programa, conexiones frecuentes, y tiempo transcurrido en la sesión (el cual puede ser relacionado inversamente).

- Modelo de Proceso de Harkov:

Este modelo, el cual aplica solamente contador de eventos, considera cada tipo distinto de evento (registro de auditoría) como estado variable y usa una matriz de transición de estado que caracteriza las frecuencias de transiciones entre estados (más bien solo las frecuencias y los estados individuales, es decir toman registros de auditoría separadamente). Una nueva observación es definida como anormal si su probabilidad quedó determinada por el estado anterior y la matriz de transición es muy baja.

Este modelo pudo ser útil para la búsqueda de transiciones entre los comandos certeros donde la secuencia de comandos eran importantes.

- Modelo de Series de Tiempo*:*

Este modelo, el cual utiliza un contador de intervalos junto con un contador de eventos o medida de recursos, considera en la cuenta el orden y el intervalo de tiempos de las observaciones $X_{1,\ldots,}X_n$ así como sus valores. Una nueva observación es anormal si su probabilidad de ocurrencia en aquel momento es demasiado baja.

Una serie de tiempo tiene la ventaja de medir tendencias de comportamiento en un cierto plazo sobre el tiempo y detecta gradualmente cambios significantes en el comportamiento, pero la desventaja sigue siendo tan costosa como la desviación estándar media.

Otros modelos estadísticos pueden ser considerados, por ejemplo, modelos que utilizan más que los primeros dos momentos pero menos que el conjunto de valores completos.

4.1.4.3 Estructura del Perfil.

Un perfil de actividad contiene información que identifica el modelo estadístico y la métrica de una variable aleatoria. Tan buena como el conjunto de medida de

eventos auditados por la variable. La estructura de un perfil contiene 10 componentes, los primeros 7 son independientes específicamente de los sujetos y la medida de los objetos.

<Variable-Name, Action-Pattern, Exception-Pattern, Resource-Usage-Pattern, Period,Variable-Type, Threshold, Subject-Pattern, Object-Pattern, Value>

Componentes Independientes Sujeto y Objeto.

- **Variable-Name:** Nombre de la Variable.

- **Action-Pattern:** Patrón que compara cero o más acciones en el registro de auditoría, por ejemplo: “login”, “read”, “execute”.

- **Exception-Pattern:** Patrón que compara el campo Exception-Condition de un registro de auditoría.

- **Resourse-Usage-Pattern:** Patrón que compara en el campo Resource-Use un registro de auditoría.

- **Period:** Intervalo de tiempo para la medida, por ejemplo: día, horas, minutos (expresado en unidades de décimas de tiempo). Este componente es nulo si este no es un intervalo de tiempo fijo, el periodo es la duración de la actividad.

- **Variable-Type:** Nombre del tipo de dato abstracto que define un tipo particular de métrica y modelo estadístico, por ejemplo: contador de eventos con el modelo de desviación estándar y medio.

- **Threshold (Umbral):** Parámetros que definen los Límites usados en la prueba estadística para determinar la anormalidad. Este campo y esta interpretación es determinada por el modelo estadístico (Variable-Type), para el modelo Operacional es superior (y posiblemente mas bajo) limitado en el valor de una observación para el modelo de desviación estándar y medio, este es el número de desviaciones estándar de la media.

Componentes Dependientes-Sujeto y Objeto.

- **Subject-Pattern:** Patrón que compara el campo Sujeto de los registros de auditoría.

- **Object-Pattern:** Patrón que compara en el campo Objeto de los registros de auditoría.

- **Value:** Valor actual (el más reciente) observaciones y parámetros usados por el modelo estadístico que representa la distribución de los valores previos. Para el modelo de desviación y medio, esos parámetros son cuenta, suma, y suma-de-cuadrados (los primeros dos momentos). El modelo operacional no requiere parámetros.

Un perfil es identificado únicamente por Variable-Name, Subject-Pattern, y Object-Pattern. Todos los componentes de un perfil son invariantes excepto por el valor.

Aunque el modelo deja sin especificar el formato exacto de los patrones, hemos identificado el siguiente: SNOBOL- mientras que las construcciones comienzan a ser útiles, como lo muestra la tabla 4.1.4.3.

'string'	Cadena de caracteres
*	Comodín que equivale a cualquier cadena
#	Compara cualquier cadena numérica.
IN(list)	Compara cualquier cadena en list.
p -> name	La cadena comparada con p es asociada con nombre
pi p2	Compara patrón p1 seguido por p2
pi | p2	Compara patrón p1 o p2
pi, p2	Compara patrón p1 y p2
Not p	Compara todo menos patrón p.

Tabla 4.1.4.3 Formato de Snobol del IDES.

Ejemplos de patrones:

'Smith'
* -> User - - Compara cualquier cadena y asigna un Usuario
'<Library>*' – –Compara archivos en el directorio <Library>
IN(Special-Files) – –Compara archivos en Archivos-Especiales
'CPU=' # -> Cantidad – compara cadena 'CPU=' seguida por número entero; asigna el número entero a la cantidad

La siguiente tabla 4.1.4.4. muestra un ejemplo de perfil para medir la cantidad de salida a la terminal del usuario Smith sobre una sesión básica. El tipo variable ResourceByActivity denota una medida del recurso usando el Modelo de Desviación Estándar y Medio.

Variable-Name:	SessionOutput
Action-Pattern:	'logout'
Exception-Pattern:	0
Resource-Usage-Pattern:	'SessionOutput=' # -> Amount
Period:	
Variable-Type:	ResourceByActivity

Threshold:	4
Subject-Pattern:	'Smith'
Object-Pattern:	*
Value:	record of ::

Tabla 4.1.4.4. Perfil del usuario Smith.

Siempre que el Sistema de Detección de Intrusiones recibe un registro de auditoría que compara patrones de una variable, éste actualiza la distribución de la variable y comprueba si hay anormalidad. La distribución de los valores para una variable es así derivada, es decir, aprende que los registros de auditoría comparan los patrones del perfil que son procesados.

3.1.4.4 Perfiles por Clases.

Los perfiles se pueden definir por pares individuales sujeto-objeto (es decir, donde los patrones del Sujeto y Objeto comparan nombres específicos, por ejemplo, Sujeto “Smith” y Objeto “Foo”) o para agregados de sujetos y objetos (es decir, donde los patrones del Sujeto y Objeto comparan conjuntos de nombres). Por ejemplo, los perfiles del archivo de actividad se podían crear por pares de usuarios y de archivos individuales, por grupos de usuarios con respecto a archivos específicos, por usuarios individuales con respecto a clases de archivos o por grupos de usuarios con respecto a clases de archivo. Los nodos en el enrejado se interpretan como sigue:

- Sujeto-Objeto: Las acciones se realizaron por sujeto individual sobre objeto individual, por ejemplo, usuario Smith-archivo Foo.

- Clase Sujeto-Objeto: Las acciones se realizaron por sujeto individual agregado sobre todos los objetos en la clase. La clase de objetos se pudo representar como un patrón comparado en un subcampo del campo del Objeto que especifica el tipo del objeto (clase), como un patrón comparado directamente o 'n nombres de objetos (por ejemplo, el patrón “*. EXE” para todos los archivos ejecutables), o como patrón comparado que prueba si el objeto está en alguna lista (por ejemplo, “IN (hit-list)”).

Sujeto Clase-Objeto: Acciones realizadas sobre objeto individual agregado sobre todos los sujetos en la clase, por ejemplo: archivos privilegiados directorio-de-usuarios <Library>, archivos no-privilegiados directorio-de-usuarios <Library>.

Sujeto Clase, Clase-Objeto: Acciones agregadas sobre todos los sujetos en la clase y objetos en los archivos clase-privilegiada, sistema-de-usuarios, archivos no privilegiados y sistema de usuarios.

Sujetos: Acciones realizadas por un usuario sobre todos los objetos, es decir la actividad de una sección.

Objeto: Acciones realizadas por un objeto agregadas sobre todos los usuarios es decir la actividad del archivo passwords.

Sujeto Clase: Acciones agregadas sobre todos los sujetos en la clase, es decir actividad del usuario privilegiado, actividad del usuario no privilegiado.

Objeto Clase: Acciones agregadas sobre todos los objetos el la clase, es decir actividad de los archivos ejecutables.

System: Acciones agregadas sobre todos los sujetos y objetos.

La variable aleatoria representada por el perfil de una clase puede agregar actividad para la clase de dos maneras:

- **Clase-como-una-actividad completa:** El conjunto de todos los sujetos u objetos en la clase se trata como entidad individual, y cada observación de la variable aleatoria representa actividad agregada para la entidad. Un ejemplo, es un perfil para la clase de todos los usuarios que representan el promedio de conexiones en el sistema por día, donde todos los usuarios son tratados como una identidad individual.

- **Actividad individual agregada:** Los sujetos o los objetos en la clase son tratados como entidades distintas, y cada observación de la variable aleatoria representa actividad para algún miembro de la clase. Un ejemplo es un perfil para la clase de todos los usuarios que caracterizan el número medio de conexiones por cualquier usuario por día. Así, el perfil representa un miembro “típico” de la clase.

Mientras que la actividad de la Clase-como-una-actividad-completa puede ser definida por un contador de eventos, contador de intervalos, o una medida del recurso para la clase, la actividad individual agregada requiere la métrica separada para cada miembro de la clase. Así, se define en términos de perfiles de bajo nivel (en sentido del enrejado) para los miembros individuales de la clase. Por ejemplo, la frecuencia media de las conexiones por día se define como el promedio de las frecuencias diarias totales en los perfiles individuales de conexiones de un usuario. Una medida para una *Clase-como-una-actividad* se podría definir en términos de perfiles de bajo nivel, pero no es necesario.

Los dos métodos de agregación responden a propósitos diferentes con respecto a la detección de la intrusión. La Clase-como-una-actividad completa revela si un cierto patrón general del comportamiento normal con respecto a una clase.

Una variable que da la frecuencia con la cual la clase de los archivos de programa ejecutable se actualiza en el sistema por día, por ejemplo, pudo ser útil para detectar la inyección de un virus en el sistema (que causa archivos ejecutables para ser reescritos como las extensiones del virus). Una distribución de frecuencia de conexiones remotas en la clase de líneas de marcado pueden ser útiles para detectar intentos de *break-ins.*

La actividad individual agregada revela si el comportamiento de un usuario dado (o del objeto) es consistente con el de otros usuarios (o de objetos). Esto puede ser útil para detectar intrusiones por nuevos usuarios que tienen comportamiento irregular desde el comienzo.

4.1.4.5 Plantillas del Perfil.

Cuando una cuenta de usuario y objetos se crean dinámicamente, un mecanismo necesita generar los perfiles de la actividad para los nuevos sujetos y objetos. Tres acercamientos son posibles:

1) Manual creado: El oficial de seguridad crea explícitamente todos los perfiles.

2) Creación Automático Explicita: Todos los perfiles para un nuevo usuario u objeto se generan en respuesta a "*crear*" el registro en el trayecto de la auditoría.

3) Primer uso: Un perfil se genera automáticamente cuando un sujeto (nuevo o viejo) utiliza primero un objeto (nuevo o viejo).

El primer acercamiento tiene la desventaja obvia de requerir la intervención manual de parte del oficial de seguridad. El segundo acercamiento supera esta desventaja, pero introduce otras dos. Lo primero es que este automáticamente no versa sobre condiciones fundadas, donde habrá muchos sujetos y objetos existentes. Lo segundo es que requiere un perfil del sujeto-objeto para ser generado por cualquier par que sea un candidato para monitorear, aunque el sujeto nunca utiliza el objeto particular. Esto podía causar más perfiles de lo necesario para ser generado. Por ejemplo, supóngase que los archivos de acceso archivo son monitoreados a nivel de usuario y archivos individuales. Considérese un sistema con 1,000 usuarios, donde cada usuario tiene un promedio de 200 archivos, dando un total de 200.000 archivos y 200.000.000 combinaciones posibles de los pares de archivo de usuario. Si cada usuario accesa a lo más 300 de esos archivos, sólo 300,000 perfiles son necesarios

El modelo IDES sigue el tercer acercamiento, que supera las desventajas de los otros generando perfiles cuando son necesarios desde las plantillas. Una plantilla del perfil tiene la misma estructura que el perfil que generó, salvo que ambos patrones del sujeto y objeto definen un patrón que compara (en los registros de auditoría) y un patrón de reemplazo (para colocar en el perfil generado). El formato para los campos Patrón-Sujeto y Patrón-Objeto es así:

comparar-patrón < - reemplazo-patrón

Donde los patrones se definen dinámicamente durante la comparación del patrón. El componente del valor de una plantilla del perfil contiene los valores iniciales para la variable, según lo especificado por su tipo.

Cuando un nuevo registro de auditoría es recibido, un proceso compara el registro contra ambos perfiles de actividad y perfiles de plantillas, obteniendo perfiles existentes y nuevos perfiles generados de las plantillas comparadas. Los patrones del sujeto y objeto en un perfil generado contienen los patrones de reemplazo definidos durante la comparación; todos los otros campos se copian exactamente de la plantilla. Si un nuevo perfil tiene los mismos patrones (para todos los componentes) como un perfil de actividad existente, este es desechado; si no, se agrega al conjunto de perfil es de actividad. El proceso entonces regresa los perfiles activos comparando los registros auditables.

Es necesario separar la comparación y el reemplazo de patrones de modo que una plantilla pueda comparar un amplio rango de sujetos y objetos, de momento se genera un perfile para sujetos, objetos, y clases específicos. Por ejemplo, considérese los siguientes patrones:

Subject-Pattern: * -> user <- user

Object-Pattern: IN(Special-Files) -> file **<-** file

El patrón del sujeto comparará cualquier nombre de usuario y generará un patrón de reemplazo con ese nombre. Semejantemente, el patrón del objeto comparará cualquier archivo en la lista de Archivos-Especiales y generará un patrón de reemplazo con ese nombre. Ahora, suponga que la lista de Archivos-Especiales contiene los nombres de archivo llamado PASSWORD y las cuentas. La siguiente tabla 4.1.4.5 muestra una sucesión de registros de auditoría y los perfiles que una plantilla con estas comparaciones y patrones de reemplazo generarán:

Registros de Auditoria		Perfiles Generados	
Subject	Object	Subject-Pattern	Object-Pattem
'Smith'	'Password'	'Smith'	'Password'

'Jones'	'Accounts'	'Jones'	'Accounts'
‘Smith'	'Foo'	no match,	so no profile

Tabla 4.1.4.5 Registros de auditoría y perfiles generados.

Los patrones de sujeto y objeto para una plantilla pueden ser mutuamente dependientes como en los patrones siguientes:

Subject-Pattern: * -> user <- user
Object-Pattern: '<' user '> *' <- '<' user '> *'

Aquí, el objeto patrón comparará cualquier archivo en el directorio del usuario y generará un perfil para el directorio del usuario (si no existe uno todavía). La siguiente tabla 4.1.4.6 muestra una secuencia de registros de auditoría y los perfiles que podrían generar desde un plantilla conteniendo estos patrones.

Audit Records		**Generated Profiles**	
Subject	**Object**	**Subject-Pattern**	**Object-Pattern**
‘Smith’	‘<Smith>Game’	‘Smith’	‘<Smith>*’
‘Smith’	‘<Smith>Let’	no new profiles generated	
‘Jones’	‘<Jones>Foo’	‘Jones’	‘<Jones>*’
‘Jones’	‘<Jones>Foo’	no new profiles generated	
Nuevos Usuarios y Objetos			

Tabla 4.1.4.6 Muestra una secuencia de registros de auditoría.

Introduciendo nuevos usuarios (y objetos) en el sistema objetivo aumenta potencialmente dos problemas:

El primero, es causado por la escasez de información del perfil sobre el comportamiento del usuario y el segundo por la propia inexperiencia del usuario con el sistema. Esta genera un número excesivo de registros anómalos. Este problema se podía solucionar ignorando las anomalías para los nuevos usuarios que no fue esto para el segundo problema: fallando en detectar una intrusión por el nuevo usuario.

Aquí se desearía una solución que minimice falsas alarmas sin pasar por alto intrusiones actuales.

Las falsas alarmas se pueden controlar por una opción apropiada del Modelo Estadístico para las actividades que causan las alarmas y por una opción apropiada de los perfiles.

Con el modelo de la Desviación Estándar, por ejemplo, los intervalos confidenciales son inicialmente grandes para tolerar más diversidad, mientras que los datos se están recogiendo sobre el comportamiento de un usuario; entonces los intervalos se contraen mientras que el número de observaciones aumenta. Esto reduce falsas alarmas causadas por un perfil de usuario individual, pero no protege el sistema contra nuevos usuarios (o usuarios infrecuentes) cuyo comportamiento es desviado o contra usuarios quienes establecen comportamiento inusual desde el principio, como un refugio. Para ocuparse de este problema, la actividad actual puede ser comparada con esa en agregar perfiles individuales o con un conjunto de perfiles para todos los usuarios o todos los usuarios en algún grupo.

Aunque el modelo operacional no se adapta automáticamente a un usuario individual (porque utiliza umbrales fijos para determinar anormalidades), el problema puede ser solucionado usando límites más indulgentes con los nuevos usuarios y ajustando los límites mientras que el usuario gana experiencia.

4.1.4.6 Perfiles Posibles.

Ahora describiremos los perfiles candidatos para medir las conexiones y la actividad de la sesión, comando y uso del programa, y acceso del archivo. Para cada perfil, sugerimos un modelo métrico y estadístico para medir la actividad:

1.- Conexión y actividad de la sesión: La conexión y actividad de la sesión se representa en expedientes de la intervención donde el sujeto, usuario i, el objeto están localizados bajo conexión del usuario (terminal, sitio de trabajo, red, host alejado, puerto, etc., o una cierta combinación), y la acción es “conexión” o la “desconexión”. Las localizaciones se pueden agrupar en clases por propiedades tales como tipo de conexión: hard-wired, marcado manual, red, etc. o tipo de localización: terminal muda, sitio de trabajo inteligente, red host, etc. Lo siguiente es una lista de perfiles posibles:

- **Frecuencia de conexión:** Contador de eventos que mide frecuencia de la *conexión* por día y tiempo usando el Modelo de Desviación Estándar y medio. Desde que la conducta de la conexión del usuario varía considerablemente durante una semana de trabajo, las incidencias de la

conexión se pueden representar por un arreglo de eventos opuestos parametrizados por día de la semana (día específico o día laborable contra fin de semana) y hora del día (hora o cambio) (otra interrupción posible es: día laborable, tarde, fin de semana, noche) Perfiles para las frecuencias de conexión pueden ser especialmente útiles para detectar enmascarados, que son probables de registrar en una cuenta no autorizada durante las horas-apagado cuando el legitimo usuario no se espera que use una cuenta. Los perfiles de la Conexión se pueden definir para un simple usuario (y grupos de usuarios) con la excepción de clases de locations- either todas las localizaciones tomadas juntas o agregadas por tipo de localización o conexión.

Capítulo 4. Modelo de un Sistema Detector de Intrusos

Frecuencia de localización: Contador de eventos que mide la frecuencia de la conexión en diferentes *localizaciones* usando El Modelo de la Desviación Estándar. Esta medida podría ser interrumpida por día o semana y hora del día puesto que un usuario puede conectarse a partir de una localización durante horas de trabajo normales y otras durante horas no trabajadas. Porque la variable se relaciona con objetos específicos, debería ser definida para localizaciones individuales o tipos de localización esto puede ser útil para detectar enmascaramientos.

Por ejemplo, si alguien se conecta con una cuenta en un lugar que el legítimo usuario nunca usa, o intenta penetrar por legítimo usuario. Por ejemplo, si alguien que trabaja normalmente desde una terminal local no privilegiada se conecta desde una terminal altamente privilegiada.

- **Última Conexión:** Intervalo de tiempo medible desde la última conexión usando el modelo operacional. Este tipo de perfil podría ser definido para los usuarios individuales con clases de localización, puesto que la localización exacta parece menos relevante que el lapso del tiempo. Sería particularmente útil para detectar un break-in en una cuenta “muerta”.

- **Tiempo Transcurrido de la Sesión:** Medida del recurso del tiempo transcurrido por sesión usando El Modelo de la Desviación estándar. Este tipo de perfil se podría definir para usuarios individuales o grupos, con excepción de las clases de objeto. Las desviaciones podrían significar enmascaramientos.

- **Salida de la Conexión:** Medida del recurso de la cantidad de salida a la terminal por sesión usando El modelo de la desviación estándar (la salida se pudo medir también sobre una base diaria. Definir este tipo de perfil para las localizaciones individuales o clases de eso puede ser útil para detectar cantidades masivas de datos que son transmitidos a las localizaciones remotas, las cuales podrían significar la salida de datos sensibles.

- **Sesión CPU, Sesión IO, Sesión Pages, etc.:** Las medidas del recurso acumuladas en una base diaria (o base de sesión) usando el modelo de la desviación estándar. Estos perfiles pueden ser útiles para detectar mascaradas.

- **Falla de Contraseña:** Contador de eventos que mide fallas de contraseña en la conexión usando el modelo operacional. Este tipo de perfil es extremadamente útil para detectar intentos de break-ins, y se deben definir para usuarios individuales y todos los usuarios juntos. Un ataque que implica muchos intentos de passwords en una cuenta particular se demostraría como un número anormalmente alto de fallas de contraseña con respecto a un perfil para todos los usuarios. Fallas en las contraseña se pudieron registrar sobre un período de tiempo bastante corto, bastan al menos algunos minutos, puesto que los break-ins son usualmente intentos en una ráfaga de actividad.

- **Fallas de localización:** Contador de eventos que miden fallas de conexión de terminales específicas basadas en el modelo operacional. Este tipo de perfil se podría definir para usuarios individuales, con excepción de localizaciones totales puesto que la localización exacta es menos significativa que esa que era no autorizada. Puede ser utilizado para detectar intentos de break-ins o intentos de conexión en terminales privilegiadas.

2.- Comando o Ejecución de programa*:* La actividad del comando o la ejecución del programa es representada en registros de auditoría donde el sujeto es un usuario, el objeto es el nombre de un programa (por simplicidad, se asume que todos los comandos son programas y no distingue entre los dos) y la acción es “execute”. Los programas se pueden ser clasificados y sumados por tanto si son privilegiados, ejecutable solamente por los usuarios privilegiados o en modo privilegiado o sin privilegios, tanto si son programas del sistema o programas del usuario, o por alguna otra propiedad.

- **Frecuencia de Ejecución:** Contador de eventos que mide el número de veces que un programa se ejecuta durante un cierto período usando el Modelo de la Desviación Estándar. Este tipo de perfil se puede definir para usuarios individuales y programas o clases de eso. Un perfil para los usuarios individuales y comandos puede ser útil para detectar enmascarados, los cuales son probables de usar diversos comandos de los usuarios legítimos; o para detectar una penetración exitosa por un usuario legítimo, que entonces tendrá acceso a comandos privilegiados que fueron rechazadas previamente. Un perfil para los programas individuales con excepción de todos los usuarios puede ser útil para detectar la substitución de un *Caballo de Troya* en una biblioteca experimental que es buscada antes de la biblioteca estándar, puesto que él caería apagado en la frecuencia de ejecución el programa original.

- **Programa CPU, Programa IO, etc.:** Recurso medido por la ejecución de un programa usando el Modelo de la Desviación Estándar. Este tipo de perfil se puede definir para los usuarios individuales y los programas o las clases. Un valor anormal para una de estas medidas se aplicó al conjunto de todos los usuarios se sugirió la inyección de un Caballo de Troya o virus en el programa original, que realiza los efectos secundarios que aumentan su 1/0 o uso del CPU.

- **Ejecución Denegada:** Contador de eventos per número de intentos para ejecutar un programa no autorizado durante un día firma el modelo operacional. Definir este tipo de perfil para usuarios individuales puede ser útil para detectar un intento de penetración de algún usuario particular. Este tipo de perfil se puede definir también para los programas individuales que son altamente sensibles, en este caso un umbral de 1 puede ser apropiado.

- **Agotamiento del Recurso del Programa:** Contador de eventos para el número de veces que un programa termina anormalmente durante un día debido a recursos inadecuados usando el Modelo Operacional. Este tipo de perfil se puede definir para programas individuales o clases de programas para detectar un programa que aborta constantemente (por ejemplo, porque se están escapando datos al usuario a través de un canal secreto basado en uso del recurso).

3) **Actividad del Archivo de Acceso*:*** La actividad del archivo-acceso es representada en los registros de auditoría donde el sujeto es un usuario, el objeto es el nombre de un archivo, y acción es "read," "write," "create," "delete" o "append". Los archivos se pueden clasificar por tipo: texto, programa ejecutable, directorio, etc.; por si son archivos de sistema o archivos del usuario; o por alguna otra propiedad. Puesto que un programa es un archivo, puede ser monitoreado tanto con respecto a su actividad de ejecución y su actividad del archivo-acceso.

Las medidas siguientes son candidatos a perfiles:

- Frecuencia Leída, Frecuencia Escrita, Frecuencia Creada, Frecuencia de borrado: Contadores de eventos que miden el número de accesos de sus respectivos tipos durante un día (o algún otro período) usando el Modelo de la Desviación Estándar y media. Leer y escribir la frecuencia de accesos de perfiles puede ser definido para los usuarios individuales y archivos o clases. Crear y borrar perfiles de acceso, sin embargo, sólo tiene sentido para agregar archivos de actividad puesto que cualquier archivo individual es creado y borrado a lo más una vez. Las anormalidades para leer y escribir las frecuencias de acceso para los usuarios individuales pueden significar enmascaramientos o curioseadas. Pueden también indicar una penetración exitosa, puesto que el usuario entonces tendría acceso a los archivos que fueron rechazados previamente.

- Registros Leídos, Registros Escritos: Recurso, medidas para el número de registros leídos o escritos por el acceso (las medidas se podrían también hacer en una base diaria) usando el Modelo de la Desviación Estándar. Este tipo de perfil se puede definir para los usuarios individuales y archivos o clases. Una anormalidad podría significar un intento de obtener datos sensibles por inferencia y agregación (por ejemplo, obteniendo cantidades extensas de datos relacionados).

- Falla Leída, Falla Escrita, Falla Borrada, Falla Creada: Contadores de eventos que miden el número de violaciones de acceso por día usando el modelo operacional. Este tipo de perfil se puede definir para los usuarios individuales y archivos o clases de eso. Los perfiles para los usuarios individuales y la clase de todos los archivos podrían ser útiles para detectar a los usuarios quienes persistentemente intentan tener acceso a archivos no autorizados. Los perfiles para los archivos individuales y la clase de todos los usuarios podrían ser útiles para detectar cualquier acceso no autorizado a los archivos altamente sensibles (el umbral se puede fijar a 1 en ese caso).

- Agotamiento del Recurso del Archivo: El contador de eventos que mide el número de fallas causadas por el sobreflujo de la cuota disponible usando el modelo operacional. Este tipo de perfil se puede definir para los usuarios individuales agregados sobre todos los archivos. Una anormalidad pudo significar un canal cubierto, donde el proceso señalado consume todo el espacio de disco disponible para señalar un “1” bit.

4.1.5 Registros Anómalos.

A través de sus reglas de actividad (sección siguiente), IDES actualiza perfiles de actividad y comprueba para saber si hay comportamiento irregular siempre que se genere un registro de auditoría o un período termina. Si se detecta comportamiento anormal, se genera un registro anormal teniendo tres componentes:

<Event, Time-stamp, Profile>

Donde:

- **Event:** Indica el evento que da lugar a la anormalidad y es además “auditado”, significa que los datos en los registros de auditoría se encontraron anormales o “periodo,” significa que los datos acumulados sobre el intervalo actual se encontraron anormales.

- **Time-stamp:** Cualquier time-stamp en el registro de auditoría o intervalo de tiempo detenido (puesto que se asume que los registros de auditoría tienen time-stamps únicos, esto proporciona medios de atar una anomalía de nuevo a un registro de auditoría).

- **Profile:** El perfil activo con respecto al cual la anormalidad fue detectada (más bien que incluyendo el perfil completo, IDES pudo incluir un campo "key", el cual identifica el perfil en la base de datos, y el estado actual del campo valor).

4.1.6 Reglas de Actividad.

Una regla de actividad especifica una acción que se tomará cuando se genera un registro de auditoría o registro anómalo es generado, o un período termina. Consiste en dos partes: una condición que, cuando es satisfecha, causa la regla de ser "fired" y un cuerpo. Utilizaremos el término "body" más bien que "action" para evitar la confusión con las acciones monitoreadas por IDES. La condición se especifica como patrón de comparación en un evento. Hay cuatro tipos de reglas:

- *Regla de registro de auditoría*, accionada por una comparación entre un nuevo registro de auditoría y un perfil de actividad, actualiza el perfil y checa los comportamientos anómalos.

- *Regla de actividad de actualización periódica*, accionada por el final de un intervalo de comparación el componente del período de un perfil de actividad, actualiza el perfil y comprueba si hay comportamiento anómalo.

- *Reglas de Anomalía-registro,* accionadas por la generación de un registro anómalo, trae la anomalía a la atención inmediata del oficial de seguridad.

- *Regla de análisis de anomalía periódica*, accionada por el fin de un intervalo, genera los resúmenes de informes de las anomalías durante el período actual.

A) Reglas de Registros de Auditoría.

Un registro de auditoría es accionado siempre que un nuevo registro de auditoría compara los patrones en un perfil de actividad. Este actualiza el perfil para reflejar la actividad reportada en el registro y comprueba si hay un comportamiento irregular. Si se detecta una anormalidad éste genera un registro anómalo. Puesto que el algoritmo para actualizar el perfil y comprobar la anormalidad depende solamente de la variable de tipo t, (métrica y modelo estadístico) representado por el perfil, pero no en otros componentes del perfil (por ejemplo, sujeto, objeto, acción, etc.), puede ser codificado en un procedimiento AuditProcess. Así, todas

las reglas de los registros de auditoría, como lo muestra la tabla 4.6.1, son representadas por la regla genérica siguiente:

REGLA DEL REGISTRO DE AUDITORÍA	
Condition:	*new Audit.Record* *Audit.Record matches Profile* *Profile.Variable-Type = t*
Body:	*AuditProcess(Audit-Record, Profile);*
END	

Tabla 4.6.1 Tabla que muestra una regla genérica para los registros de auditoría.

B) Reglas de Actividad de Actualización Periódica.

Este tipo de regla, que también es parametrizada por el tipo “t” de la medida estadística, se acciona siempre que el reloj implique un período de la longitud “p” completa, el componente del período de un perfil es p, y el componente Variable-Tipo es t. La regla actualiza el perfil de comparación, comprueba para saber si hay comportamiento anormal, y genera un registro de anomalía si una anormalidad es detectada. Puede también producir un resumen de informe de actividad, como se muestra en la tabla 4.6.2 siguiente:

REGLA DE ACTIVIDAD DE ACTUALIZACIÓN PERIÓDICA**.**	
Condition:	*Clock mod p = 0* *Profile.Period = p* *Profile.Variable-Type = t*
Body:	*PeriodProcesst(Clock, Profile)*
END	

Tabla 4.6.2 Tabla que muestra una regla genérica para los registros de auditoría.

C) Reglas de Registros Anómalos.

Cada regla de registro anómalo se acciona siempre que un nuevo registro anómalo compara los patrones dados en la regla para sus componentes “Evento y Perfil”. Así, una regla se puede condicionar en una variable particular, un sujeto u objeto particular, en la acción de la auditoría que se encontró para ser anómala, y así sucesivamente. Para esos componentes de un Perfil que son también patrones (por ejemplo, los componentes del sujeto y objeto), los patrones dados en una regla anómala deben ser idénticos para que una comparación ocurra; es decir, un patrón compara otro solamente si los patrones son idénticos. El registro comparado es traído a la atención inmediata del oficial de seguridad, con una indicación del tipo sospechado de intrusión. La forma general de tal regla es como lo muestra la tabla 4.6.1 que se presenta a continuación.

REGLA REGISTRO ANÓMALO	
Condition:	new Anomaly-Record Anomaly-Record.Profile matches profile-pattern Anomaly-Record.Event matches event-pattern
Body:	PrintAlert('Suspect intrusion of type ...', Anomaly-record);
END	

Tabla 4.6.1 Tabla que muestra una regla genérica para los registros de auditoría.

Desafortunadamente se tiene muy poco conocimiento sobre la relación exacta entre ciertos tipos de anormalidades e intrusiones. En esos casos donde tenemos experiencia, podemos escribir las reglas que incorporan nuestro conocimiento. Un ejemplo está en las fallas de la contraseña, donde el oficial de seguridad debe ser notificado inmediatamente de un BREAK-IN posible si el número de las fallas de la contraseña en el sistema durante un cierto intervalo de tiempo es anormal. Otras anormalidades que son candidatos a la notificación inmediata incluyen un lapso anormal desde la última conexión o un tiempo o lugar de conexión anormal. Por ejemplo, el usuario nunca ha entrado previamente tan tarde en la noche lo cual podría indicar enmascaramiento.

D) Reglas del Análisis Anómalo Periódico.

Este tipo de regla se acciona por el fin de un intervalo. Analiza un cierto conjunto de registros anómalos para el período y genera un informe que resume las anomalías al oficial de seguridad. Su forma genérica es:

REGLA DEL ANÁLISIS ANÓMALO PERIÓDICO	
Condition:	Clock mod p = 0
Body:	Start = Clock - p; A = SELECT FROM Anomaly-Records WHERE Anomaly-Record.Time- stamp > Start; generate summary report of A;
END	

Tabla 4.6.1 Tabla que muestra el resumen para el oficial de seguridad.

La regla selecciona todos los registros anómalos que pertenecen al período del conjunto (relación) de todos los registros anómalos. Las reglas que procesan los registros anómalos pueden producir tablas de resumen de estadísticas interrumpidas por una o más categorías o gráficas de anormalidades. Puede ser que calculen funciones estadísticas sobre anomalías en orden para ligarlas a intrusiones posibles. Hasta el momento, no se tiene suficiente experiencia con la

detección de intrusión en línea para saber exactamente qué informes serán los más útiles.

Para facilitar el reporte de anomalías, el modelo se puede realizar para incluir perfiles de anomalía. Un perfil de anomalía sería similar a un perfil de actividad salvo que las actualizaciones serían accionadas por la generación de un registro anómalo dentro de IDES más bien que un expediente de registros de auditoría del host. Siempre que la estructura –A sería útil, sin embargo, es confuso.

4.2 Conclusión.

El artículo de Denning D. [5] es de suma importancia ya que sentó las bases de una gran cantidad de investigaciones posteriores especificando formalmente un modelo de Detección de Intrusiones, como se sabe al respecto de Sujetos y de Objetos al efectuar cualquier movimiento en el sistema, con la descomposición de sus partes en cadenas, lo cual fue una excelente idea y utilizar un lenguaje para la interpretación de las mismas. Ahora podríamos hacer la implementación en SNOBOL4 que es más rápido que PERL.

Se puede decir que es un modelo que ninguna persona que se está adentrando al estudio de la Monitoreo de Seguridad en Redes debe dejar pasar por alto. Sin ese conocimiento se podría estar ahogado en un desierto de simplemente manejar un Sistema Detector de Intrusiones sin realmente saber lo que esta pasando, no se sería capaz de mirar más haya del simple manejo, lo que se quiere decir: Que entre más conocimiento sobre Monitoreo se tenga en general, se puede ser participe de la solución en los problemas de diseño e implementación que atañen el estudio.

El siguiente modelo detector de intrusiones está basado en las técnicas de entropía máxima, donde el factor principal es el comportamiento del cambio abrupto en el tráfico de red, de esa manera se podrá clasificar las anomalías que van llegando por la red, este esquema rompe la necesidad de implementar métricas para la creación de perfiles sobre Sujetos (Usuarios), ya que lo que se analizará será la ignorancia que se tiene de un conjunto de distribuciones que viene siento el tráfico de red.

Una introducción previa a ese modelo será el capítulo siguiente donde se presentarán algunos conceptos matemáticos acerca de la teoría de la información, como el concepto de información y entropía que son la parte medular de dicho Sistema Detector de Intrusiones.

Capítulo 5
Introducción a la Entropía.

Introducción.

En este capítulo se tiene como objetivo dar una breve introducción matemática al concepto de información y máxima entropía, ya que son la parte medular del modelo: Detector de Anomalías Basado en Entropía Máxima. Dicho modelo se describirá en el capítulo 6, donde se describirá como ayuda a etiquetar con claridad ataques que vienen en la red.

El principio o método de Máxima Entropía es un procedimiento para generar distribuciones de probabilidad de forma sistemática y objetiva.

Se le puede describir de la siguiente manera: de entre todas aquellas distribuciones de probabilidad compatibles con cierta clase de información, escoger la que conlleve una mayor incertidumbre.

Como es aceptada que la incertidumbre de una distribución está representada por la función:

$$H:=\sum_{i=1} pi \ln pi$$

Llamada entropía, entonces la Máxima Entropía indica que se debe maximizar H, es decir:

Si se escoge una distribución con menos entropía que la máxima, esta reducción en la entropía pudo deberse a alguna información adicional que se haya utilizado, consiente o inconcientemente. No sería correcto utilizar esta información, puesto que no es parte de las restricciones. Por ello se debe utilizar únicamente la distribución con la máxima entropía.

Así mismo la teoría de la probabilidad tal y como es estudiada convencionalmente no es más que una rama de la teoría de la medida, al menos formalmente y que tiene sus fundamentos en la teoría de conjuntos.

Los cursos que tradicionalmente se imparten con el nombre de estadística generalmente incorporan el enfoque llamado frecuentista. Sin embargo hay distintos enfoques; entre los que se pueden mencionar el enfoque clásico, al enfoque frecuentista y al enfoque bayesiano.

La interpretación frecuentista o empírica construye la probabilidad directamente como una frecuencia relativa.

La probabilidad de una clase de eventos es una secuencia infinita de repeticiones se define como el limite de la frecuencia relativa de los eventos de esta clase dentro de la secuencia.

El principio de Máxima Entropía y el bayesianismo objetivo se encuentran relacionados, la entropía máxima se vuelve completamente natural una vez que se ha aceptado la idea central del bayesianismo objetivo, que es considerar a la probabilidad como una extensión de la lógica, que nos permite razonar en situaciones de información incompleta.

5.1 Información.

La palabra información tiene varios sentidos: se usará en el sentido de la reducción en la incertidumbre del receptor, después de haber conocido el resultado de un fenómeno aleatorio. Si S representa la incertidumbre respecto a alguna situación, e I la información, se tiene la relación:

$$I_{\text{obtenida}} = S_{\text{antes}} - S_{\textit{después}}$$

Por lo tanto, la primer tarea es definir una medida de incertidumbre.
Intuitivamente, incertidumbre significa falta de capacidad de predicción. En concreto significa falta de capacidad de predicción del resultado de un experimento aleatorio.

También significa poca seguridad en alguna afirmación, como en “el pasado incierto”. En cualquier caso es una noción que puede expresarse de forma natural en términos probabilísticas.

Considérese un experimento con n posibles resultados. Buscamos una medida de incertidumbre $S(n)$ asociada al experimento que tenga tres propiedades:

1. $S \geq 0$
2. $S(1) = 0$
3. $S(mn) = S(m)+S(n)$

La condición (1) se incluye por conveniencia. La condición (2) expresa la idea natural de que un experimento con un solo resultado posible (i.e. determinista) no nos causa ninguna incertidumbre. La condición (3) refleja el hecho de que si tenemos dos experimentos independientes, con m y n resultados, respectivamente, entonces la incertidumbre del experimento combinado debería ser la suma de las incertidumbres individuales.

Se puede probar que la única función que cumple estos tres puntos es el logaritmo $S(n) = k \log n$.

La constante *k* es un factor de escala, que se puede fijar como 1 definiendo un bit de información como la cantidad de información obtenida por la eliminación de la incertidumbre entre dos posibles resultados igualmente probables.

Es decir, requerimos que $S(2)=k \log_a 2=1$. Esto significa que $k=\log_2 a$, por lo que

$$S(n)=k\log_a n= \log_2 n= \log_2 1/(1/n).$$

Definición: Si un evento *A* ocurre con probabilidad *P(A),* se define la "información" *I(A)* obtenida al conocer que *A* há ocurrido como

$$I(A)= \log_2 1/P(A)=- \log_2 P(A)$$

La idea es que mientras más raro sea el evento, mas información obtenemos al saber que este ha ocurrido. También podría llamarse la "sorpresa" de *A.*

Si ocurre un evento con probabilidad alta, entonces no hemos obtenido mucha más información de la que ya disponíamos previamente (y por lo cual le habíamos asignado una probabilidad alta); al mismo tiempo, la incertidumbre se redujo un poco. El caso extremo de que la probabilidad sea uno significa que ya incorporamos toda la información relevante, y por lo tanto no obtenemos ninguna información nueva al realizar el experimento.

Si ocurre un evento con probabilidad baja, significa que teníamos muy poca información relevante. Este caso es interesante, pues indica que debemos revisar la información que nos condujo a asignar una probabilidad baja originalmente.

Ahora con el enfoque de probabilidad obtenido se tiene que un evento con probabilidad cero si puede ocurrir, simplemente sucedió algo que creíamos imposible. Después de reponernos de la impresión, lo natural es analizar e identificar en las hipótesis aquello que nos hizo creer que el evento era imposible.

Probabilidad	Información previa relevante	Información obtenida	sorpresa	Reducción de incertidumbre	Capacidad de predicción del evento
1	Toda	Ninguna	Ninguna	Ninguna	Completa
Alta	Mucha	Baja	Poca	Poca	Alta
Media	Media	Media	Neutra	Media	Media
Baja	Baja	Alta	Mucha	Alta	Baja
0	Ninguna	Muy alta	Milagro		Nula

Tabla 1. Relación de la probabilidad y la incertidumbre.

Esta tabla debe entenderse de la siguiente forma: si nuestra asignación inicial era una probabilidad muy baja para un evento A, y este evento ocurre, esto significa que la información.

Ahora con estas nociones de información será más sencillo el poder entender cómo es que está funcionando el modelo para la detección de anomalías basado en entropía máxima.

5.2 Entropía Máxima.

El concepto de Entropía que da Shannon, es un pilar central en la teoría de la Información, y refiere a la medida de la incertidumbre. La entropía de una variable aleatoria se define en términos de la distribución de la probabilidad y muestra una buena medida de la aleatoriedad de la incertidumbre, como se verá a continuación:

Sea X una variable aleatoria discreta, tomando un número posible de valores $x_1,\ldots,x_n$ con probabilidades $p_1,\ldots,p_n$ respectivamente tenemos que $pi \geq 0$, i=1,2,…,n $\sum p_{i=1,\ldots,n}$ procuramos llegar a un número que mida la cantidad de incertidumbre.

Sea h la función definida en el intervalo (0,1] y h(p) es interpretada como incertidumbre asociada al evento $X=x_i$, $i=1,2,\ldots,n$ o la información que conlleva a decir que X toma el valor xi en el desarrollo de un experimento.

Para cada n, definimos la función H_n de los n valores $p_1,\ldots,p_n$. La función $H_n (p_1,\ldots p_n)$ es interpretada como el promedio de incertidumbre asociado al evento $\{X= x_i\}$, i=1,2,…n dado por

$$H_n (p_1,\ldots, p_n)=\sum i=1,\ldots,n \quad p_i h(p_i)$$

Así $H_n(p_1 ,\ldots, p_n)=\sum i=1,\ldots,n \quad p_i h(p_i)$ es el promedio de la incertidumbre removido por la relevancia del valor X. Por simplicidad se denota:

$$\Delta_n =\{P=(p_1 ,\ldots,p_n): (p_i \geq 0 \sum p_i=1)$$

Y algunas caracterizaciones axiomáticas para la medida de incertidumbre $Hn(p_1 ,\ldots,p_n)$ para llegar a la expresión exacta. Sea X y Y dos experimentos independientes con n y m valores respectivamente. Sea $P=(p_1,\ldots,p_n) \in \Delta_n$ la distribución de probabilidad asociada a X y $Q=(q_1,\ldots,q_n) \in \Delta_m$ la distribución de probabilidad asociada a Y, entonces se escribe

$$H_{nm} (P*Q)=H_n(P)+ H_m(Q), \qquad (a)$$

Para todo $P=(p_1,\ldots,p_n) \in \Delta_n$, $Q=(q_1,\ldots,q_m) \in \Delta_m$ y $P*Q=(p_1q_1,\ldots, p_1q_m, p_2q_1,\ldots,p_2q_m,\ldots, p_nq_1,\ldots, p_nq_m) \in \Delta_{nm}$ sustituyendo $p_ih(p_i)$ por $f(p_i)$, para todo i=1,2,…,n, se tiene que:

$$H_n(p_1,\ldots,p_n)=\sum i=1,\ldots,n \quad f(p_i) \qquad (b)$$

Con esto se enuncia un primer teorema:

Sea $H_n:\Delta_n \rightarrow R$ $(n\geq 2)$ una función que satisface (a) y (b) donde f es la función continua de valores reales definida sobre [0,1]. Entonces H_n está dada por:

$$H_n(p_1,\ldots,p_n)=-C\sum p_i \log_b p_i$$

Donde C>0, b>1, y con $0 \log_b 0=0$. Entonces se caracteriza la medida.

Ahora veamos la aplicación en la Seguridad de la Información, más bien en el ámbito del monitoreo de seguridad en redes.

Capítulo 6
Modelo Basado en Entropía.

Introducción.

La técnica de la entropía máxima proporciona un flexible y rápido acercamiento para estimar una distribución de la línea de fondo, que también da al administrador de la red una vista multidimensional del tráfico de la red. Además, este método proporciona la información que revela el tipo de la anomalía detectada.

6.1 Modelo de un IDS basado en Entropía.

En este trabajo, desarrolla una técnica de detección de anomalías de la red, basada en técnicas de entropía máxima y entropía relativa. El enfoque explota la idea del comportamiento basado en detección de anomalías, donde primeramente se dividen paquetes en clases a lo largo de múltiples dimensiones.

La distribución de la lineabase de una entropía máxima de clases de paquete en el tráfico benigno es determinada por el aprendizaje de un modelo de densidad de un conjunto de datos pre-etiquetados. La distribución empírica de las clases de los paquetes en observación se compara entonces con la distribución de esta líneabase utilizando entropía relativa como métrica. Si las dos distribuciones difieren, se muestra que de los paquetes de clases, el principal responsable de la diferencia contiene paquetes relacionados a una anomalía.

6.1.1 Fases de Trabajo.

El enfoque está divido en dos fases donde:
La primera fase consiste en aprender la distribución de la lineabase y la segunda es detectar anomalías en el tráfico observado.

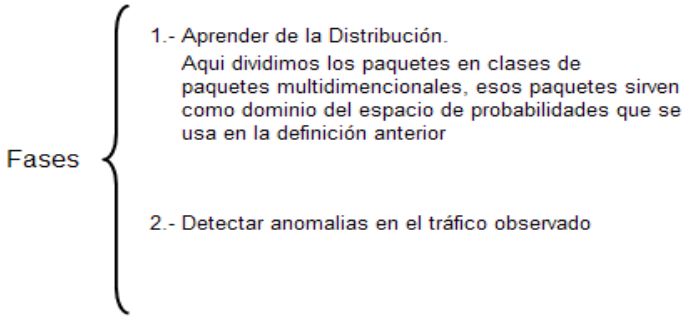

Figura 6.1 Cuadro sinóptico de Fases de trabajo para el modelo del IDS basado en Entropía.

En la primera fase, se dividen paquetes en clases de paquetes multidimensionales de acuerdo a la información de protocolo de los paquetes y el número de puerto de destino. En la figura 6.1 se muestra un cuadro sinóptico de las fases de trabajo.

Estas clases de paquetes sirven como el dominio del espacio de probabilidades. Luego, la distribución de la lineabase de las clases de paquete está determinada por el aprendizaje de un modelo de densidad desde los datos de instrucción usando la estimación de la entropía máxima. La instrucción de datos es un conjunto de datos pre-etiquetados con las anomalías etiquetadas por un humano y en la que paquetes etiquetados como anómalos son eliminados. Durante la segunda fase, una traza de tráfico de red observado se da como la energía o consumo. La entropía relativa de las clases de paquetes en la traza del tráfico de red observado con respecto a la distribución de la lineabase es calculada.

Las clases de paquete que contribuyen significativamente a la entropía relativa son entonces registradas. Si ciertas clases de paquetes continúan contribuyendo significativamente a la entropía relativa, se generan advertencias de anomalía y las clases de paquetes correspondientes se reportarán. Esta información correspondiente a la clase de paquete revela los protocolos y el destino de los números de puerto relacionados a la anomalía.

Existen paquetes que detectan anomalías como se ve en la *tabla 6.1.1* estos Open Source y se sabe que el costo es proporcional a la regla aplicada, también la complejidad de las reglas individuales afecta la estabilidad de estos acercamientos.

I. D. S.	DEFICIENCIA
SNORT	NO SON SENSIBLES A ANOMALIAS QUE NO SE HAYAN DEFINIDO ANTES
BRO	

Tabla 6.1.1 Deficiencia de los IDS de Software Libre más populares.

6.2 Clasificación de Paquetes.

El trabajo se enfoca en anomalías relativas a paquetes TCP y UDP. A fin de estudiar la distribución de estos paquetes, se dividen en un conjunto de dos clases dimensiónales de acuerdo con el protocolo de información y el destino de número de puerto en la cabecera del paquete. Este conjunto de clases de paquete es el dominio común del espacio de probabilidades.

En la primera dimensión los paquetes se dividen en cuatro clases de acuerdo con la información relacionada con el protocolo. Primero los paquetes son divididos en clases de paquetes TCP y UDP. Otras dos clases además se dividen desde la

clase de paquete TCP de acuerdo con la clase o no son los paquetes SYN y RST, figura 6.2.1 donde se muestra dicha partición.

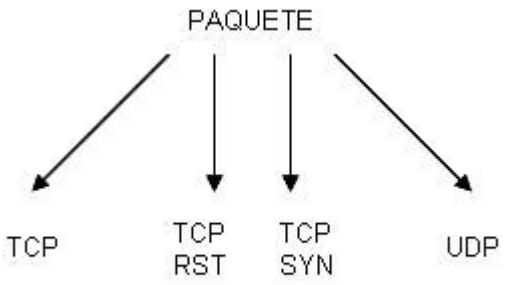

Figura 6.2.1 Partición de los protocolos TCP y UDP.

En la segunda dimensión, se dividen en paquetes de 587 clases de acuerdo a sus números de puerto de destino. Los números de puerto suelen determinar los servicios relacionados con el paquete de intercambio. Según IANA (Internet Assignet Number Autority) los números de puertos están divididos en tres categorías: Puertos bien conocidos (0-1024), Puertos de registro (1024-49151), y Puertos dinámicos o Puertos Privados (49152-65535), *figura 6.2.2.*

En este modelo los paquetes con puerto de destino en la primera categoría se dividen en clases de 10 números de puerto cada uno. Dado que los paquetes con el número de puerto 80 comprenden la mayoría del tráfico de red, están separados en una sola clase. Esto produce 104 clases de paquete. Los paquetes con puerto de destino en la segunda categoría se dividen en 482 clases adicionales, con cada clase que abarca 100 números de puerto con excepción de la clase que abarca los últimos 28 números de puerto de 49124 a 49151. Los paquetes con número de puerto de destino más grande que 49151 se agrupan en una sola clase. Por lo tanto, en esta dimensión, los paquetes se dividen en un total de 104+482+1=587 clases.

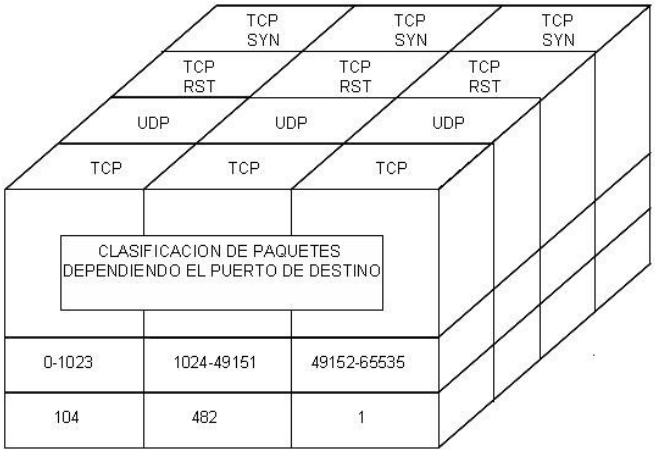

Figura 6.2.2 Espacio de probabilidad para el IDS.

En total, el conjunto de dos clases dimensiónales consiste en 4X587=2348 clases de paquetes, esto se puede visualizar gráficamente en la figura 6.2.2. Estas clases de paquetes comprenden el espacio de probabilidad. Se calcula la distribución de diferentes paquetes en el tráfico benigno según esta clasificación, y se usa éste como la distribución de la lineabase para detectar anomalías en el tráfico de red.

6.3 Estimación de la Entropía Máxima.

La estimación de la Entropía Máxima es un marco para obtener un modelo de distribución de probabilidades paramétricas de la instrucción de datos y un conjunto de limitaciones en el modelo. La estimación de la Entropía Máxima produce un modelo con la distribución más uniforme entre todas las distribuciones satisfaciendo las limitaciones dadas. Una métrica matemática de la uniformidad de una distribución P es ésta Entropía.

$$H(P) = -\sum_{\omega \in \Omega} P(\omega) \log P(\omega).$$

Donde Ω es el conjunto de clases definido previamente, y la secuencia de paquetes $S=\{x_1,\ldots,x_n\}$ como la instrucción de datos, la distribución empírica P sobre Ω en esta instrucción de datos es:

$$P(\omega) = \frac{\sum \mathbf{1}(x_i \in \omega)}{n},$$

Capítulo 6. Modelo Basado en Entropía

Donde ***1****(x)* es un indicador de la función que toma el valor ***1*** si *x* es verdad y 0 si es falso.

Supóngase que se da un conjunto de características F ={fi}, y sea fi el indicador de la función fi:Ω{0,1}. Usando la Estimación de la Entropía Máxima, buscamos un modelo de destino P que satisface que Ep(fi)=Ep(fi), para todo fi ∈ F y tiene Entropía Máxima.

En {11}, ha sido probado que en virtud de tales limitaciones, la estimación de la Entropía Máxima se garantiza de ser única y la misma que la Estimación de Máxima verosimilitud usando la distribución garantizada Gibbs, teniendo la siguiente forma (log-liner)

$$P(\omega) = \frac{1}{Z} \exp(\sum_i \lambda_i f_i(\omega)).$$

Por cada característica fi, un parámetro λi ∈ Λ determina el peso en el modelo, así Λ es el conjunto de parámetros de una función característica. Z es una normalización de constante que asegura la suma de las probabilidades sobre Ω es 1.

La diferencia entre dos distribuciones dadas P y Q es comúnmente determinada usando la divergencia de entropía relativa de Kullback-Leibler (K-L):

$$D(P||Q) = \sum_{\omega \in \Omega} P(\omega) \log \frac{P(\omega)}{Q(\omega)}.$$

Maximizando la probabilidad de la distribución con respecto a P es equivalente a minimizar la divergencia K-L de P con respecto de P.

$$P = \arg\min_P D(\tilde{P}\|P)$$

Como:

$$\prod_{\omega \in \Omega} P(\omega)^{\sum 1(x_i \in \omega)} \propto \exp(-D(\bar{P} \| P)).$$ odelo Basado en Entropía

Por motivos de eficiencia, la función característica es seleccionada a menudo para expresar la más importante cualidad de los datos de instrucción en el modelo log-linear y vuelta. El modelo log-linear expresa la distribución empírica con los menores parámetros y funciones de selección.

El procedimiento de la entropía máxima consiste en dos partes:

1. La selección de la característica.
2. La estimación de los parámetros.

La parte de la selección de la característica selecciona la más importante característica del modelo registro lineal y la parte de la estimación de los parámetros asigna un propio peso de cada una de las funciones características [11].

6.4 Selección de las Características y Estimación de los Parámetros.

El paso de función de selección es un algoritmo voraz el cual escoge la mejor función de selección que minimiza la diferencia entre la distribución del modelo y la distribución empírica de un conjunto de candidatos de funciones de selección.

Sabemos que Ω es el conjunto de todas las clases de paquetes P la distribución empírica del tren de datos de instrucciones sobre Ω y F un conjunto de candidatos a funciones de selección seleccionadas.

La distribución inicial del modelo sobre Ω es P0(ω)=1/z, Z=|ω|, la cual es una distribución uniforme sobre Ω.

Sea Pi un modelo con i funciones de selección seleccionadas.

$$P_i(\omega) = \frac{1}{Z} \exp(\sum_{j=1}^{i} \lambda_j f_j(\omega)).$$

Y queremos seleccionar la *i*+1st función característica y sea *g* la función característica en $F \backslash \{f_1,\ldots,f_n\}$ a ser la seleccionada en el modelo y λg será su peso, entonces dejemos.

$$P_{i,\lambda_g,g}(\omega) = \frac{1}{Z'} \exp(\sum_i \lambda_i f_i(\omega)) \exp(\lambda_g g),$$

También sea

$$\begin{aligned} G_{P_i}(\lambda_g, g) &= D(\tilde{P}||P_i) - D(\tilde{P}||P_{i,\lambda_g,g}) \\ &= \lambda_g E_{\tilde{P}}(g) - \log E_{P_i}(\exp(\lambda_g g)), \end{aligned}$$

donde Ep(g) es el valor esperado de g con la distribución de P.

$$G_{P_i}(\lambda_g, g)$$

Es una función cóncava con respecto a λg, y

$$G_{P_i}(g) = \sup_{\lambda_g} G_{P_i}(\lambda_g, g)$$

es la máxima disminución de la divergencia K-L que puede ser lograda añadiendo g en el modelo.

En [11] también se muestra que por indicador de candidato de función de selección, hay una forma cerrada de fórmulas relacionadas a la máxima de $G_{P_i}(\lambda_g, g)$ que la hace más fácil computacionalmente.

Después de que una nueva función de selección se añade al modelo log-liner a los pesos de todas las funciones de selección son actualizadas. Dando un conjunto de datos de instrucciones y un conjunto de funciones de selección elegidas {fi}, el conjunto de parámetros es entonces estimado. La estimación de la Entropía Máxima localiza un conjunto de parámetros Λ={λi} en

$$P(\omega) = \frac{1}{Z} \exp(\sum_i \lambda_i f_i(\omega)).$$

Para λi que minimiza la divergencia K-L de P con respecto de P:

$$\Lambda = \arg\min_{\Lambda} \sum_{\omega \in \Omega} \tilde{P}(\omega) \log \frac{\tilde{P}(\omega)}{P(\omega)}.$$

Hay un número de métodos numéricos que pueden ser explotados, y claro está se usará el algoritmo L-BFGS de Estimación de Entropía Máxima de Malouf.

6.4.1 Algoritmo de Malouf L-BFGS.

El modelo está construido por la iteración de los dos pasos anteriores hasta que algún criterio interrumpido se cumple. Este criterio interrumpido pude ser o que la divergencia K-L de P es menor que algún valor del umbral, o que la ganancia de añadir una nueva función de selección es muy pequeña para mejorar el modelo.

Las funciones de selección son seleccionadas desde un conjunto de candidatos de funciones de selección. Ya que el dominio Ω en el trabajo consiste de clases de paquete diferente en los protocolos y el destino de los números de puerto, nuestro conjunto de candidatos de función de selección se compone de tres conjuntos de indicador de funciones. El primer conjunto de indicador de funciones checa la información del protocolo del paquete, el segundo conjunto de indicador de funciones clasifica:

- Datos iniciales

Un conjunto de datos de instrucción con distribución empírica P.
Un conjunto de candidatos de funciones de selección F.
Y un modelo de densidad inicial Po, Po(w)=1/z, Z= |Ω|

- Pasos iterados

(0) Sea n=0

(1) Selección de la Característica
Para cada función característica g ∈ F, g ¢{fi}, calcule nuevamente Gpn(g)
Sea fn+1 la función característica con el mayor aumento.

(2) Estimación del Parámetro
Actualice todos los parámetros y ponga Pn+1 a ser el modelo actualizado

(3) Revise el criterio de paro de la iteración
Si el criterio de paro de la iteración no es conocido, entones sea n=n+1, y vaya a (1), en otro caso regrese al modelo de aprendizaje Pn+1

El número de puerto destino del paquete, y el tercer conjunto checa ambos la información del protocolo del paquete y el destino del número de puerto.

La instrucción de datos usada es pre-etiquetada por humanos y los paquetes relacionados con las anomalías etiquetadas no se usan en calcular la distribución

empírica “p”. De esta forma, tratamos de definir la distribución de clases de paquete mediante el modelo log-linear en (3) desde la estimación de Máxima Entropía a la distribución de la lineabase, y ahora son capaces de calcular la Entropía Relativa de cualquier tráfico de red dado.

6.5 Detectando Anomalías en el Tráfico de Red.

La entropía relativa muestra la diferencia entre la distribución de clases de paquete en el tráfico de red actual y la distribución de líneabase. Si esta diferencia es muy grande, esto indica que una porción de algunas clases de paquete que raramente aparecen en la instrucción de datos se incrementa significativamente. En otras palabras, esto sirve como una indicación de la presencia de una anomalía en el tráfico de red. Este modelo solo considera anomalías donde la anomalía de tráfico aumenta.

Dividimos el tiempo en los huecos de longitud fija δ. Supóngase que el tráfico en intervalos de tiempo contiene la secuencia de paquetes $\{x_1,\ldots,x_n\}$, la distribución empírica P de las clases de los paquetes en un intervalo de tiempo es:

$$\tilde{P}(\omega) = \frac{\sum \mathbf{1}(x_i \in \omega)}{n},$$

Para cada clase de paquetes definimos.

$$D_{\tilde{P}\|P}(\omega) = \tilde{P}(\omega) \log \frac{\tilde{P}(\omega)}{P(\omega)},$$

Donde P es la líneabase de la distribución obtenida de la Estimación de la Entropía Máxima. Este produce un valor cuantitativo que describe la distorsión de la distribución para cada clase de paquetes ω de la distribución de la lineabase y este es usado como indicador de anomalías.

Entonces se usa una detección de enfoque “ventana deslizante”. En cada intervalo de tiempo se registran las clases de los paquetes que tienen divergencia más grande que un umbral d. Si para ciertas clases de paquetes ω, Dp||p(ω)> para más que h tiempos en una ventana de intervalos de tiempos de W, una alarma es lanzada con la información de las clases de los paquetes , la cual revela el protocolo correspondiente y el numero de puerto.

6.6 Resultados e Implementación.

El algoritmo de la Estimación de la Entropía Máxima es usado para generar la líneabase de distribución de las clases de los paquetes de un tren de datos. Se

selecciona el criterio de paro para la construcción del algoritmo a ser la diferencia K-L de P respecto a P, es menos que 0.01. Por este criterio, el algoritme finaliza con un conjunto de 362 funciones características.

Todas las anomalías detectadas por el algoritmo que corresponde a la misma anomalía etiquetada por el ser humano se tratan como solo positivo. Si no hay anomalía etiquetada por un humano que corresponde a la anomalía divulgada por el algoritmo, se llama *un falso positivo.*

Consecutivamente los falsos positivos son tratados como un simple falso positivo. Las anomalías etiquetadas por el ser humano pero no por el algoritmo se llaman *las negativas falsas.* En cada caso, el algoritmo detecta la mayoría de las anomalías situadas por el humano. Sin embargo, el algoritmo también divulga muchos "falsos positivos". Estos falsos positivos son fenómenos de cualquier ' "muchedumbre", del tráfico que se comunica con los números de acceso que raramente se han visto en el tren de datos.

	Funcionamiento del algoritmo						
Fecha	**Humano etiquetado**	**Positivo**	**Falso Negativo**	**Falso Positivo**	**Precisión**	**Memoria**	**F1**
Jul-16	10	10	0	1	0.91	1	0.95
Jul-17	11	10	1	0	1	0.91	0.95
Jul-18	14	14	0	0	1	1	1
Jul-19	16	14	2	0	1	0.88	0.93
Jul-21	15	15	0	0	1	1	1
Jul-22	9	8	1	0	1	0.89	0.94

Tabla 6.6.1 Alcance del algoritmo, respecto a precisión, memoria, etc.

A pesar de la situación ambigua referente a todas las anomalías generadas por el algoritmo, encontramos que los resultados experimentales con respecto a los paquetes de SYN dan buenos resultados.

La *tabla 6.6.1* resume el funcionamiento del algoritmo en los experimentos, también resume el funcionamiento del algoritmo en términos de la precisión, memoria y F1. Sea a el número de positivos, el número de positivos falsos, b el número de falsos positivos, y c el número de falsos negativos. La precisión está definida como a/(a+b), la memoria está definida como a/(a+c) y F1 es definida como $2^a/(2^a+b+c)$. También la tabla muestra que el método de la Entropía Máxima detecta muchas de las anomalías detectadas por un humano que las etiquetó con pocos falsos negativos y pocos falsos positivos y el número de falsos negativos. Se define la precisión como se define memoria mientras que se define F1. La tabla muestra con qué el método máximo de la entropía detecta la mayoría de las anomalías detectadas por el etiquetado humano y pocas falsos negativos y pocos falsos positivos.

Capítulo 7.
Conclusiones.

7.1 Conclusiones.

En un principio se elige trabajar sobre el tema de la detección de intrusos por ser un tema bastante ambicioso en el campo de la seguridad informática, ya que abarca un sin número de teoría y estrategias para su desarrollo.

Al comenzar a desarrollar la teoría se encontraron enfoques e ideologías diferentes, acerca del concepto de la detección de intrusiones, se tenían 2 caminos a seguir para este trabajo: el primer camino era desmenuzar una herramienta para detectar intrusos en su totalidad y el segundo camino era abarcar de una forma generalizada y amplia la teoría de la detección de intrusos comenzando desde sus inicios como ideología hasta analizar la evolución que han tenido, consecuencia del cambio abrupto de las necesidad de las redes. Sin dejar pasar el análisis del diseño de un IDS clásico, y también el de un modelo contemporáneo.

Obviamente se opto por el segundo, ya que en este camino se podría profundizar en el conocimiento y aprendizaje del Monitoreo de Seguridad en Redes, además se piensa que este trabajo es una excelente manera para que cualquier persona sin conocimientos en la detección de intrusos pueda ser su punto de partida y estudio.

Como se vío la detección de intrusos es un área aplicada de la seguridad informática y no criptológica. Encargada de informar sobre eventos que puedan tener lugar en un sistema informático y pueda ser considerado por una u otras razones como parte de un intento de intrusión u acto no autorizado.

El campo de la detección de intrusos ofrece numerosas ventajas, pues el detectar intrusos que intentan atacar el sistema nos ayuda a garantizar:

- El mantenimiento de la integridad de los datos en el sistema. Esto es fundamental ya que en ocasiones los datos almacenados en el sistema pueden poseer una gran relevancia.
- El correcto funcionamiento del sistema tanto a nivel software como del hardware.

- Disponibilidad de los recursos del sistema para todos los usuarios registrados en el mismo, puesto que se pueden detectar ataques que saturen los mismos (buffer overflow).

- Una mayor facilidad en el mantenimiento del sistema.
- Confidencialidad de los datos. Mediante la detección de intrusos se puede asegurar con un nivel bastante alto que determinados datos sólo serán accedidos por aquellos usuarios que pueden hacerlo.
- El seguimiento de las tareas realizadas por el intruso dentro del sistema lo cual nos permite llevar el sistema a un estado más seguro.
- Mediante el registro de los pasos seguidos en el sistema por el intruso se pueden descubrir posibles agujeros de seguridad posibilitando la incorporación de mayor robustez en el sistema.
- El descubrimiento del origen del ataque permitiéndose tomar las medidas que se consideren oportunas (denuncia, denegación de servicio, etc.).

Sin embargo, existen esfuerzos de estandarización que los fabricantes tendrán que asumir como suyo, conocido como CIDF (Common Intrusion Detection Framework) que ha tenido como resultado el Grupo de Trabajo Formato de Intercambio de Detección de Intrusos (idwg) de la IETF. Dicho grupo de trabajo ha publicado trabajos en los que define un modelo de formato de datos y mensajes relacionados con elementos de detección de intrusos.

Si los fabricantes introducen este estándar podrá ser posible, en un futuro, la integración de elementos de detección de intrusos a consolas de distintos fabricantes, así como dentro de consolas generales de gestión de seguridad.

A nivel operativo, los detectores de intrusos también tienen carencias importantes que hace que su despliegue sea dificultoso, a veces se experimentan alarmas de ataques aún cuando la red no esté sufriendo ninguno.

Cabe destacar el desarrollo del IDES que nace como un esfuerzo sobre problemas de seguridad en computadoras de tipo framework, en 1986, ahí se comienza a desarrollar como una herramienta formal de seguridad, 20 años después la necesidad ha cambiado se crean detectores de intrusos basados en entropía máxima, donde uno dé los principales funciones es detectar intrusiones que vienen en el flujo de red como lo son los DDOS. Aún este tipo de detectores de intrusos no es del todo preciso ya que cuentan todavía con un error del .06

El trabajo arduo tiene lugar sin dudas en el tráfico de red, dada la necesidad que se tiene al trabajar en redes de tráfico elevado (velocidades Gigabit) Sin embargo un intruso siempre verá la manera de evadir este tipo de herramientas con inyectores de tráfico e intentando suplantar la identidad.

Estas tecnologías comienzan ya a ser maduras, existen productos que incorporan este tipo de técnicas y análisis, sin embargo, la detección de intrusiones es parte fundamental del Monitoreo de Seguridad en Redes.

En este trabajo de tesis se han expuesto las limitaciones y los logros conocidos en la actualidad de las tecnologías utilizadas para la detección de intrusos. Las limitaciones incluyen la incapacidad de tratar aplicaciones a medida, la falta de interoperabilidad entre fabricantes la sobre carga de análisis que lleva a la posibilidad de ataques contra el propio detector de intrusos. Así como, finalmente, la necesidad de actualizaciones y ajustes continuos del firewall.

En la detección de intrusos no se puede hablar de una herramienta única que cubra todo el espectro y avise de todas las intrusiones, en el caso del análisis de bitácoras, no se puede esperar detectar determinados ataques de denegación de servicio que fuercen un comportamiento anómalo del servidor y que no queden registrados como los ataques de desbordamiento de buffer.

Es por eso que se echa la mano de la teoría del Monitoreo de Seguridad en Redes, donde se deben de cumplir sus 4 puntos al pie de la letra:

- Estimación.
- Protección
- Detección.
- Respuesta a Incidentes.

Sin embargo la detección de intrusos aún es una utopía ya que siempre se encontrarán fallos en los sistemas.

Un Detector de Intrusiones siempre tendrá alguna vulnerabilidad vieja o nueva, la gente del *underground* se las arreglará para evadir dichos productos. Esto pensando en herramientas que inyectan paquetes al tráfico de red para así confundir a los Monitores de Red.

No se deben olvidar los usuarios que intentan obtener información del sistema al conectar periféricos USB, o aquellas personas que tienen acceso físico a las unidades de respaldo. Más aún usuarios mal intencionados que editan el archivo .profile del root, en sistemas Unix o Linux para poder ejecutar comandos que antes no podíamos utilizar, es decir: Se olvidan de los ataques más sencillos.

Se piensa que ahora los administradores de seguridad tienen que ser un expertos en: armas y tácticas de ataque, redes, telecomunicaciones, administración de sistemas, guiones y programación, gestión de reglamentos y desde luego que agregando la criptografía. Todo esto para poder hacer una mejor Administración de la Monitoreo de Seguridad de Redes ya que a veces sólo se pone una pequeña barrera con un firewall, donde a veces es un simple cerco de prevención y omiten utilizar módulos de cifrado, analizadores de bitácoras, verificadores de integridad y desde luego Detectores de Intrusos.

Aún así se seguirá pensando que el intento es muy bueno, pero los "*pastores"* es la moda para el fin de la década. El conocimiento que tienen estos hackers sobre nuestros sistemas y redes, es muy grande, entonces se seguirán viendo páginas WEB desfiguradas o con imágenes de las modelos de moda así con la llegada de los nuevos gusanos polimórficos.

Con todo esto se pensaría que es suficiente si se tuviera el mejor Sistema Detector de Intrusiones y junto con el mejor firewall, Todo esto aún no es suficiente, si la comunicación viniera en un canal de comunicación cifrado, entonces ¿Qué tan transparente sería para estos productos? Desde luego que no basta con estar monitoreando la red en todo momento, o estar verificando que tan bruscamente cambia el tráfico. Es necesaria la implementación de políticas de Seguridad bien establecidas, como las basadas en estándares internacionales [20], la puesta en marcha de fronteras de seguridad perimetral, física y contar con los planes de *Prevención, Detección y Respuesta*. Recordando que todo proceso de detección y respuesta lleva a un proceso de seguridad y desde luego utilizando herramientas de Auditoría de Seguridad y de Monitoreo de Seguridad en Redes.

La Internet crece y cambia en todo momento por lo tanto la necesidad de estar en ella cambien se hace presente arrastrándonos hacia un camino que no tiene final, ahora se plantean nuevas preguntas: ¿Cuál es el arma que podremos usar en nuestro mundo virtual que construimos? donde no podemos tocar nada pero el cual tiene tanto valor, y queremos estar presentes en ella más tiempo. ¿Qué tantas herramientas se inventarán en un futuro? ¿Cuáles son las amenazas con las que lucharemos en un futuro no tan lejano?.

No se debe de olvidar que la tarea primordial de la detección de intrusiones es determinar si la actividad es lo suficientemente inusual para sospechar de alguna intrusión, para ello se tiene que monitorear la seguridad de la red.
Concluyendo este trabajo, se piensa que constituye una buena base para introducirse en el campo de la detección de intrusos, conocer en qué consiste, métodos de llevarla a cabo, sus ventajas e inconvenientes, como parte del monitoreo de seguridad en redes.

S. Reyna S.

Referencias Bibliográficas.

[1] Bejtlich R., *"The Tao Networking Security Monitoring, Beyond Intrusion Detection".*
2Da. Edición. 2005.
ISBN: 10-0321246772

[2] Bell David Elliot, *"Looking back at the Bell-La Padula Model".*
IEEE Computer Security Applications, 21 st Annual, 9 Dec. 2005.

[3] Collings T., Wall K., "*Red Had Linux Networking and System Administration".*
Tercera Edición, 2003.
ISBN: 0-7645-3632-X

[4] Daltabuit E., Hernández L., Mallén G., Vázquez J., *"La Seguridad de la Información".*
1era. Edición 2007.
ISBN: 9789681869359

[5] Denning D., *"An intrusion Detection Model".*
IEEE Transactions on Software Engineering, Vol. SE-13 No. 2, February 1987.

[6] Diffie W. and Hellman M., *"New Directions in Cryptography".*
IEEE Transactions on Informatión Theory, 1976.

[7] Gurley Bace Rebecca., "Intrusion Detection".
1era. Edición 2000., Macmillan Technical Publishing
ISBN:1-57870-185-6

[8] Kasner E., Newman J. *"Matemáticas é Imaginación".*
2da. Edición 2006.
ISBN: 978-970-35-1300-0.

[9] Khan D., *"Code Breakers, The Comprensive History of Secret Communication for Ancient Times to the Internet".*
3era Edición 1996.
ISBN: 1591143087

[10]Long J., Bayles A. W., Foster J. C, Hurley C., Petruzzi M., *"Penetration Tester's"*.
2da. Edición. 2006.
ISBN: 10-1597490210

[11] Lucena M. J., *"Criptografía y Seguridad en Computadores".*
2da. Edición Libro Electrónico 2004.
Licencia Creative Commons.

[12] Menezes A. J, Van Oorschot P.C., Vanstone S.A., *"Handbook of Applied Cryptography".*
Ed. CRC Press, 1997.
ISBN: 084938523-7

[13] Orebaugh A., Morris G, Ramirez G, *"Ethereal Packet Sniffing".*
2nd. Edition, Spring-Verlag 2004.
ISBN: 1932266828

[14] Orebaught A., *"Wireshark & Ethereal Networking Protocol Analyzer".*
3era. Edición, Syngress, 2007.
ISBN: 13-978-1-59749-073-3

[15] Pietra S. D., Pietra, V.D, and Lafferty, J.,*"Inducing features of random fields".*
IEEE Transactions on Pattern Analysis and Machine Intelligence, 1997.

[16] Rusell R., *"Snort Intrusion Detection"*
2da. Edición, Syngress, 2007.
ISBN: 1-931836-74-4

[17] Schneier B., *"Applied Cryptography".*
2da. Edición, New York, NY; John Wiley and Sons, Inc., 1996.

[18] Taneja I., J., Pardo L., Morales D., *"On Generalized Information Measures and Their Applications".*
Department of Mathematics of Federal University of Santa Catarina, 2001.

[19] Tanenbaum A. S., *" Sistemas Operativos Diseño e Implementación".*
2da. Edición 2006.
ISBN: 9701701658

[20] Yu Gu, McCallum A., Towley Don, "Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation".
Department of Computer Science, University of Massachusetts, Amherst, MA 0100.
Internet Measurement Conference' 05, 2005.

Referencias en Internet.

[21] http://www.biometrics.org/
El sitio está dedicado al desarrollo, investigación, evaluación y pruebas de identificaciones personales basadas en biometría de alta tecnología.

[22] http://www.criptored.upm.es
Red Telemática Iberoamericana de Criptografía y Seguridad de la Información.

[23] http://www.elhacker.net
El sitio está dedicado a información hacker, donde se exponen vulnerabilidades de los sistemas operativos así como manuales y exploits.

[24] http://www.ethereal.com
Ethereal es un analizador de protocolos que es utilizado en varios sistemas operativos. Tiene la característica de estar bajo la licencia Open Source.

[25] http://www.gocsi.com
Instituto de Seguridad en Cómputo, está dedicado a la comunidad que desarrolla aplicaciones de seguridad de la información.

[26] http://kriptopolis.org
Sitio web dedicado a la criptografía, privacidad y seguridad en internet.

[27] http://resnet.uci.edu/security/bestpractices.asp
Buenas prácticas en seguridad. Aquí se tienen sugerencias y consejos de seguridad para protegerse en contra de los virus, hackers, etc.

[28] http://www.sans.org
SANS es la más confiable fuente de información en la certificación de seguridad en el mundo.
Ofrece investigación mundial sobre seguridad informática, respuesta a incidentes, hacking y detección de intrusos.

[29] http://securitydistro.com
Dominio dedicado a exponer las distribuciones mas recientes de software en seguridad.

[30] http://www.seguridad-informacion.blogspot.com
Blog dedicado al estudio de la Seguridad de la Información – Seguridad Informática – Auditoría informática, tiene la recopilación de las principales noticias, eventos, políticas de seguridad, guías de buenas practicas, normas, estándares, herramientas, etc.

[31] http://www.snort.org
Esta es la web principal de Snort un IDS e IPS open source basado en reglas, siendo el más popular del mercado y un estándar de facto.

[32] http://www.tcpdump.org
Este es el sitio principal del sniffer tcpdump el cual contiene también las librerías de captura libcap y wincap el cual contiene manuales, bugs, etc.

[33] http://www.verisign.com
Verisign es una de las entidades certificadoras más confiables en Internet, la cual emite certificados digitales de todo tipo.

[34] http://www.websensesecuritylabs.com/alerts/alert.php
Websense es un órgano mundial el cual expone los últimos avisos de seguridad en Internet, incluyendo código malicioso, spyware, phising, spam, crimeware y tiene una lista de sitios web comprometidos.

[35] http://www.redtercermundo.org.uy/revista_del_sur/texto_completo.php?id=1237
Dominio dedicado a la publicación de revistas electrónicas.

[36] http://www.worldlingo.com/ma/enwiki/es/Rainbow_Series
Este sitio se encarga de alojar una gran cantidad de artículos y referencias, aquí se explica brevemente en que consiste la serie de libros arcoíris así como temas relacionados en ellos.

Lista de Abreviaturas.

ACL	Acces Control List
AES	Advanced Standar System
ARP	Protocol Resolution Address
ASCII	American Standard Code for Information Interchange
BRO	Open Source Unix Based NIDS
CPU	Central Unit Proces.
DDOS	Distributed Denial Of Service Attack) o Ataque de Denegación de Servicio.
DES	Data Encription Standar
DIDS	Distributed Intrusion Detection Systems.
DMZ	Zona Desmilitarizada
DNS	Domain Name Server.
DOS	Denial Of Service Attack.
DSS	Digital Signature Estándar
DVD	Digital Versatile Disc.
ETHEREAL	Analizador de Protocolos bajo la licencia GPL
FTP	File Transfer Protocol.
GOOGOL	10^{100} = Diez mil hexadecillones.
GOOGOLPLEX	10^{googo}
HIDS	Sistema de detección de intrusos en un Host.
IANA	Internet Assignet Number Authority.
IBM	Internacional Business Machines
ICMP	Internet Control Messaging Protocol.
IDES	Sistema Experto Detector de Intrusiones
IDS	Sistema Detector de Intrusiones
IETF	Internet Engineering Task Force.
INTERNET	Red mundial de Computadoras
INTRANET	Red de computadoras dentro de una red de área local
IP	Internet Protocol
IPS	Intrusión Prevention System
ISOA	Information Security Officers Assistan.
LINUX	Sistema operativo tipo-Unix, Cuyo código fuente está disponible
MD5	Message Digest algorithm version 5.
MIDAS	Multics Intrusion Detection and Alerting System.
MIT	Institute Technologic of Massachussets
MSR	Monitoreo de la Seguridad en Redes
NADIR	Network Anomaly Detection and Intrusion Reporter.
NAT	Network Address Translation.
NBS	Nacional Bureau of Standars
NIC	Centro de Información de la Red.

NIDES	Next Generation Intrusion Detection Expert.
NIDS	NIDS, *Sistema de detección de intrusos en una Red*.
NIST	National Institute for Standard and Technology
NSA	National Security Agency.
OSI	Open System Interconnection
PERL	Practical Extraction and Reporting Languaje.
RFC	Petición de comentarios. Es uno dentro de una serie de documentos informativos numerados de Internet y estándares que tanto el software comercial y el freeware en Internet y las comunidades Unix siguen ampliamente.
RMON-MIB	Remote Network Monitoring MIB
ROOT	Super User
RSA	Algoritmo de llave publica de Rivest, Shamir and Adleman.
SHA	Secure Hash Algoritm
SMF	System Management Facilities.
SNMP	Simple Network Management Protocol.
SNOBOL	A String Processing Programming Languaje
SNORT	Free Software NID and Packet logging in real time.
TCP	Transmision Central Protocol
TCPDUMP	Common computer network debuggin tool.
UDP	User Datagram Protocol
UNIX	Sistema Operativo. Portable**,** multitarea **y** multiusuario.
URL	Uniform Resource Locutor
USB	Universal Serial Bus
USENIX	The Advanced Computing Technical Association.
VM	Maquina Virtual
VPN	Virtual Private Networks.
WEB	World Wide Web
XOR	O exclusivo, Operador de bits binarios en matemáticas.

CONVENCIONES TIPOGRÁFICAS.

Las convenciones en este trabajo de tésis se describen en la siguiente tabla, mostrando del lado izquierdo una breve descripción de la convención tipográfica y del lado derecho se muestra un ejemplo del formato que se utilizó.

Descripción de la convención	Ejemplo del formato
La numeración de capítulos, se mostrará en negritas, con un tipo de letra Arial, tamaño de 16 puntos y alineados hacia el margen derecho.	**Capítulo 1**
El título del capítulo, estará escrito con un tipo de letra Arial, tamaño de 16 puntos y alineado hacia el margen derecho.	Seguridad de la Información.
El nombre de las secciones y su correspondiente subsección, se mostrará con el tipo de letra Arial, tamaño de 14 puntos, en estilo negritas con y alineación hacia la izquierda.	**Conceptos de información.**
El contenido del trabajo está escrito con tipo de letra Arial, tamaño de 12 puntos y una alineación justificada.	Para introducir este concepto basta comenzar con un ejemplo:
El número de las figuras y tablas se colocará con tipo de letra Arial, tamaño de 10 puntos y con un estilo en negrita. El texto referente a la figura o tabla estará escrito con tipo de letra Arial, tamaño de 10 puntos y una alineación centrada, junto con su numeración.	**Figura. 1.1** Cuadro sinóptico de la Clasificación de la Criptografía.
Para hacer resaltar una palabra o frase dentro de un texto que represente algo importante, se utilizará como tipo de letra Arial con tamaño correspondiente al texto del cual viene incrustado y con un estilo cursivo y también con comillas	*“Confidencialidad”* *“Integridad”* *“Autenticidad”* *“No repudio”* *“Control de Acceso”*
Para hacer resaltar alguna definición en los listados o al inicio de párrafos se utilizará un tipo de letra Arial con el tamaño correspondiente al texto y con un estilo cursivo y en negritas.	***Resaltado***

LISTA DE FIGURAS.

LISTA DE TABLAS.