UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

TEMA

ESTUDIO DEL ARTE DE LOS SISTEMAS DE IDENTIFICACIÓN DE INTRUSOS

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA

AUTORES:

Wilson Antonio Carrión Samaniego

DIRECTOR:

Msc. María Paula Espinosa Vélez

LOJA – ECUADOR
2009

Tema

Estudio del arte de los IDS - Sistemas de Identificación de Intrusos

Autoría

Los conocimientos, conceptos y criterios vertidos en el presente trabajo de Investigación, son de absoluta responsabilidad del autor.

Wilson Carrión .....

Agradecimiento

Quiero dejar constancia de mi profundo agradecimiento primeramente a Dios por ser un Padre excelente a su Hijo amado por dar su vida por salvar la mía y al Espíritu Santo por tratar con mi vida y formarme día a día como a un vaso de barro que necesita ser perfeccionado.

De manera especial, quiero agradecer a la Msc. María P. Espinoza directora de la tesis por la colaboración brindada, por la orientación durante el desarrollo de esta tesis.

Gracias de igual manera a Carlos Mex Perera y Tomas Heredia por sus valiosos consejos y asesoramientos con respecto a la tesis.

Finalmente a mis padres por el apoyo económico al esforzarse en entregarme una educación técnica profesional, incluso sacrificando su economía con el anhelo de ver en su hijo un gran profesional.

Atentamente:

Wilson Carrión

Dedicatoria:

El presente trabajo lo dedico de manera muy especial a la directora del proyecto investigativo, a la comunidad de desarrollo Open-Source en el cual todas las herramientas utilizadas para la elaboración de esta tesis son de GNU.

Y de manera especial a mis padres que con sacrificio y esfuerzo apoyaron para la culminación de esta carrera, gracias a todas esas personas que me han animado a seguir, bendiciones.

Wilson A. Carrión S.

Universidad Técnica Particular de Loja

IDS- Sistemas de Identificación de Intrusos

María P. Espinoza(Directora) mpespinoza@utpl.edu.ec, Julia Pineda(Codirectora), Wilson Carrión(Investigador) wacarrion@utpl.edu.ec, 2009

Universidad Técnica Particular de Loja

1 Resumen

El presente trabajo se ubica en el área de seguridad para redes y tiene como objetivo la investigación de la tecnología conocida como IDS o conocida también como Sistemas de Identificación de Intrusos, la cual ayudara a determinar un ataque sobre la red y los recursos que se encuentren en ella, logrando así aumentar el nivel de seguridad en la red, reconocer las posibles falencias de la actual red de la UTPL.

Index Terms-- IDS, IP, seguridad

2 Introducción

En el ámbito de la seguridad el problema de la intrusion ha ido creciendo cada día más, en GARCÍA[01] se puede ver a diario salen nuevos programas que buscan afectar a un equipo, ya sea para daños locales o para llegar a perjudicar toda una red informática.

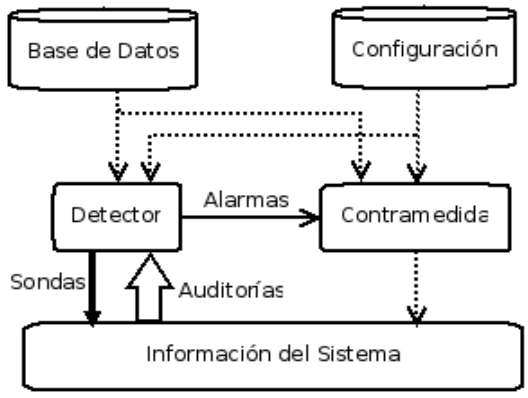
Es necesario entender que es un ataque informático. Se puede decir que un ataque informático es un intento organizado por parte de una persona o conjunto de personas cuyo objetivo es causar daños o problemas dentro de un Sistema Informático o red.

3 IDS

Es un conjunto de métodos y técnicas que se encargan de revelar una actividad sospechosa, incorrecta o inapropiada sobre un recurso o un grupo de recursos computacionales ya puedan ser estos firewalls, estaciones de trabajo, dispositivos de red, servidores, etc.

3.1 Descripción de un IDS

Un IDS puede ser descrito como un detector que procesa la información proveniente del sistema monitoreado como se ilustra en la Figura 1:



Nota: El calibre de la flecha representa la cantidad de información que fluye desde un componente hasta el otro.

Figura 1: Un sistema de detección de intrusos Simplificado [02].

El IDS se vale de tres tipos de información para detectar un tipo de intrusión, estos son: la información recolectada de ataque previos, la configuración actual del sistema y la descripción del estado actual referente a comunicaciones y procesos.

3.2 Características que proporciona un IDS:

Permite tener una alerta anticipada ante una actividad sospechosa, aunque también estos buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre la red o host. Otra característica importante de estos, es que están diseñados para detener el ataque, se puede generar algún tipo de alerta.

3.3 Estructura de un IDS

Por el tiempo han llegado a existir dos grandes tendencias en la estandarización de los IDS, IDEF(Intrusion Detection Exchange Format) y CIDF(Common Instrusion Detection Framework) y otras menos populares como son el Autopost de AusCERT(Computer Emergency Response Team), IDWG(Intrusion Detection Exchange Format) y CVE(Common Vulnerabilities and Exposures).

3.3.1 IDEF (Intrusion Detection Exchange Format)

Esta fue desarrollado por “Intrusion Detection working Group del IETF” el cual a su vez estaba formado por empresas que se dedicaban a las intrusiones, básicamente este se dio por el rechazo con la CIDF, estos definen protocolos, en las comunicaciones contamos con IDXP (intrusion Detection Exchange Protocol) y en los datos IDMEF (Intrusion Detection Message Exchange Format).

3.3.2 CIDF(Common Intrusion Detection Framework)

Esta fue promovida por DARPA(Defense Advance Research Proyects Agency), su principal meta es la orientación a la investigación de detección de Intrusos, aunque entre en el sector comercial tuvo poca aceptación sus conceptos se han abierto camino hasta la actualidad

definiendo lenguajes propios, uno para la comunicación entre los elementos del Framework, y otro para definir los datos, CISL(Common Intrusion Specification Languaje). Una de las características principales se da en el equipo de repuesta al poder interactuar con otras cajas y poder responder a los eventos como se muestra en la figura 2 a continuación.

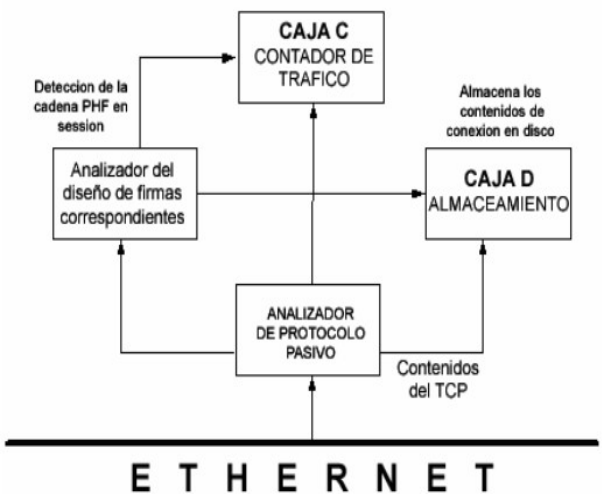


Figura 2. Descripción de un modelo CERT (Computer Emergency Response Team)[03].

3.3.3 Autopost de AusCert (Australia CERT)

Esta diseñado sobre un sistema en el cual se puede trabajar de una manera más fácil que el CIDF/CISL, además de que tiene una alta interoperabilidad y es muy sencillo de construir y analizar, también permite que se analice y se agregue un informe en una base de datos tan solo usando unas cuantas líneas del lenguaje Perl. La manera de trabajo de esta frente a un incidente es como la del informe que se presenta a continuación en la tabla 1.

IP Origen	Puertos	Tipos de incidente	Redistribución	Tiempo de Zona	Repetición
172.16.x.x	TCP 111	Escáner de Red	Si	GTM+1200	No

Tabla 1. Resultados obtenidos del modelo CERT [03].

Los problemas que se presenta en este modelo es que no contiene una gran fidelidad en la recopilación de datos, ya que en ciertos casos como un análisis forense el gran nivel de detalle en el evento que estos solicitan se pierde.

3.3.4 IDWG (Intrusion Detection Working Group)

IETF creó un grupo de trabajo llamado IDWG que contrarreste al complejo CISL, este tiene como objetivo "definir formatos y procedimientos de intercambio de información entre los diversos subsistemas del IDS", cuyos resultados se presentan a continuación:

• Elaboración de documentos que detalle los requerimientos funcionales de alto nivel en las comunicaciones que se dan en los sistemas de detección de intrusos y sus sistemas de gestión.

• Un mismo lenguaje de especificación que describa el formato de los datos.

• Un marco de trabajo en el cual se reconozca los mejores protocolos en los cuales se puede usar en la comunicación entre los IDS y que determine como se mapean en éstos los formatos de datos.

Como se puede ver en la figura 3. se muestra la arquitectura IDWG con sus correspondientes componentes.

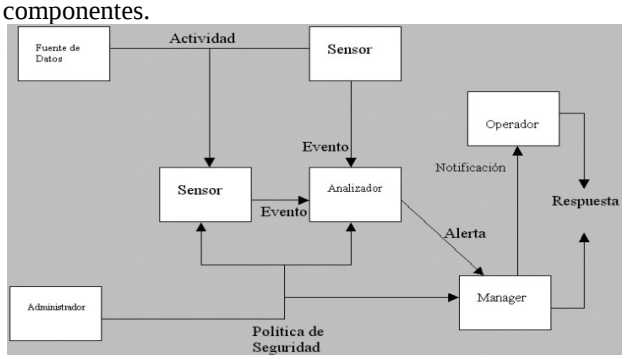


Figura 3. Arquitectura IDWG [04].

4 Tipos de IDS

En la figura 4 se presenta un enfoque por Dorothy Denning que se proporciona una clasificación de los IDS.

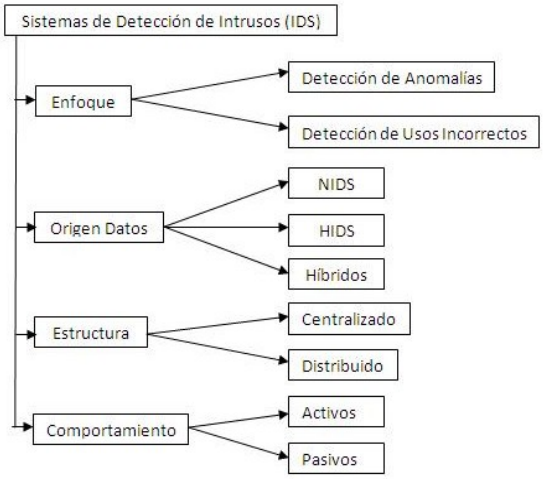


Figura 4. Clasificación de los IDS [05]

4.1 Por su enfoque tenemos

Como se puede ver en la figura 5, se tiene dos enfoques de los cuales se explicara a continuación:

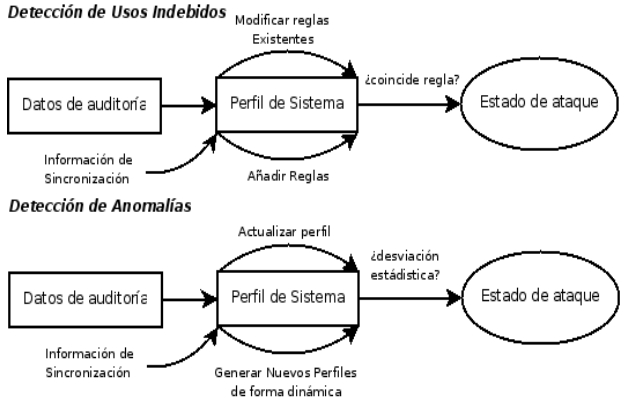


Figura 5. Modelo de Funcionamiento por su enfoque [06].

4.1.1 IDS de detección de usos incorrectos

O también conocido como modelo de Usos Indevidos, en este tipo de sistemas, el IDS está configurado para detectar patrones, estos utilizan sistemas basados en firmas que ayudan a identificar ataques previamente conocidos tales como: paquetes malformados, escaneo de puertos, etc.

Entre las ventajas se puede mencionar las siguientes:

• Son efectivos sin generar tantas falsas alarmas.

• Da un diagnostico rápido ante un ataque especifico.

Desventajas de la detección de Abusos o Firmas:

• Deben de ser actualizados constantemente.

• No pueden hacer frente a los denominados ataques del día cero o no conocidos además que toma tiempo actualizar los parches y actualizar la base de firmas.

• No pueden hacer frente a los ataques modificados de un patrón ya conocido (variación de comportamiento).

• Necesitan ser administrados y supervisados constantemente por personal especialmente preparado para esta tarea, además de un proceso arduo de "finetunning"[1].

• El problema de que arroja "Falso Positivo" y "Falso Negativo" de los cuales se estudiara más adelante.

4.1.2 Detección de Anomalías

O también conocido como modelo Heurístico, en este se propone la creación de perfiles del sistema por un tiempo específico, permitiendo hacer un análisis de dicho perfil y el ver el porqué de la desviación o anomalía del mismo.

Entre las ventajas se puede mencionar las siguientes:

• Puede detectar ataques de los cuales no tiene ningún conocimiento específico.

• La información que produce, puede ser utilizada para generar firmas en la detección de abusos.

Desventajas de la detección de anomalías:

• Genera un gran número de falsas alarmas.

• Requiere conjuntos de entrenamientos muy grandes.

• En las actividades de monitoreo, las medidas y técnicas incluyen los siguientes parámetros:

• Detección de una entrada sobre ciertos atributos del comportamiento de un usuario, de los cuales pueden ser el número de ficheros accedidos por el usuario sobre un tiempo especifico, el número de intentos fallidos para ingresar al sistema, el porcentaje de utilización del CPU por un proceso.

• Otras técnicas que se llegan a usar en los IDS actuales son las Redes neuronales y algoritmos genéticos como son SOM (Self Organized Maps) y LVQ (Learning Vector Quantization).

4.2 Por origen de Datos

4.2.1 Host IDS (HIDS)

Los primeros en su clase, funcionan de manera local al controlar el tráfico en la máquina mediante la utilización de los recursos de su anfitrión y nos permite analizar las acciones que tienen que ver contra nuestro servidores, PC o host, al analizar los procesos y usuarios que se involucran, para esto guardan información como logs, ficheros del sistema, entre otros.

Entre las ventajas se puede citar las siguientes:

• Detectan ataques que no pueden ser vistos por un NIDS los cuales se verán más adelante.

• Pueden operar en entornos con tráfico encriptado.

• Son potentes, registran comandos, ficheros abiertos, modificaciones importantes.

• Capacidad para operar en ambientes cifrados.

Entre las desventajas podemos mencionar las siguientes:

• Más difíciles de administrar que un NIDS.

• Puede ser deshabilitado si el ataque logra tener éxito

1 Proceso para mejorar el rendimiento. Un control de calidad

(Penetración o DoS).

• Disminuyen el rendimiento del sistema monitorizado.

• Análisis limitado de tráfico, ya que solo analiza el segmento al que pertenece.

4.2.2 Network IDS (NIDS)

Más conocidos como sniffers de tráfico de red, cuyo funcionamiento se da de una manera autónoma, estos capturan paquetes de la red, para luego analizarlos en busca de patrones que supongan algún tipo de ataque. Estos reciben los datos de la red local, en donde están instalados y permiten la detección de ataques a un mayor nivel de abstracción al tener la información de múltiples host, no obstante solo analiza la información que pasa por la red siendo inútil ante los ataques entre host de un mismo segmento de red.

Entre las ventajas podemos mencionar las siguientes:

• No dan un impacto grande en la red.

• Pueden no solo funcionar a nivel de TCP/IP si no también a nivel de aplicación.

• No necesitan software adicional en los servidores.

Entre las desventajas podemos mencionar las siguientes:

• Presenta problemas en redes con tráfico elevado por características de Hadware.

• No hace un análisis de información Encriptada.

• No sabe a la final si el ataque tuvo éxito o no.

• Tiene problemas con los paquetes fragmentados.

• En el caso de los NIDS por firmas se da una limitante por la dependencia de la red, al proporcionar al usuario reglas definidas para poder detectar el código malicioso.

• En los NIDS heurísticos se da una limitación cuando el patrón de comportamiento de las intrusiones son similares a los patrones de comportamiento de un programa normal. Una limitación de los NIDS heurísticos se da cuando un usuario se sale del comportamiento normal sin ánimo malicioso, obligando una readaptación de los perfiles de usuario para el nuevo comportamiento y así evitar los falsos positivos, descubriendo la verdadera debilidad de los NIDS heurísticos que se llegarían a limitar por la información analizada en el momento.

4.2.3 Hybrid IDS

Es la unión de los dos anteriores constituido por sensores en cada host que permite una detección local de los sistemas y un sensor en cada segmento de red. Para mayor información visitar http://www.prelude-ids.org

4.3 Por su Infraestructura

4.3.1 Distribuidos (DIDS)

Son aquellos donde se implementan varios IDS que se comunican entre sí o con un servidor central que permite centralizar y correlacionar todos los datos generados. Tener varios agentes por toda la red permite tener una amplia información para la detección en caso de un incidente en el sistema.

4.3.2 Centralizados

Estos IDS contienen sensores que trasmiten información a un servidor central del cual se maneja todo.

4.4 En función de su comportamiento

Se puede apreciar los pasivos que se muestra en la figura 6a y los activos figura 16b de los cuales se explicara a continuación:

4.4.1 Pasiva

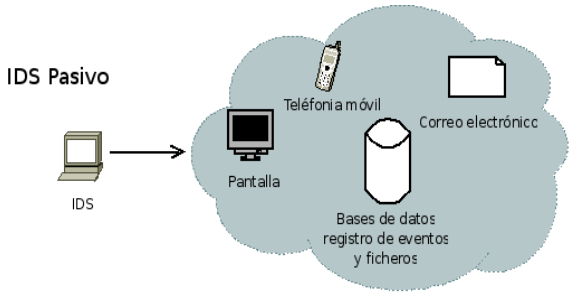


Figura 6a. Modelo por su comportamiento (pasivo) [06]

En este caso el IDS avisa al administrador del sistema atacado usando alguna vía que se ha configurado como puede ser: alertas, correo electrónico, notificaciones SNMP (Simple Network Management Protocol)[2] , mensajes en pantalla u otros.

2Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

4.4.2 Activa

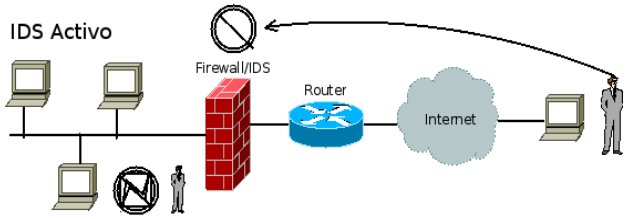


Figura 6b. Modelo por su comportamiento (Activo) [06]

Cuando se detecta un ataque este de forma automática toma una o algunas acciones modificando las Access Control Lists (ACLs)[3] del firewall corporativo.

5 Funcionamiento de un IDS.

5.1 Ubicación de un IDS en la red.

Hay que tener en cuenta en donde se deberá colocar el IDS. En la figura 7, se da una pauta de los posibles lugares en el cual debería ubicarse según URBINA[03] y WALC[07].

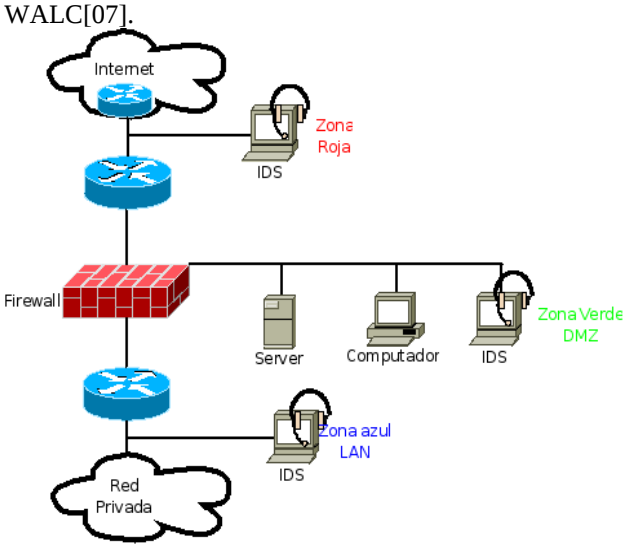


Figura 7. Localización de un IDS dentro de una organización [07].

A continuación se verá los criterios que debemos tomar en cuenta para la configuración de los IDS en las diferentes áreas de la red la cual se a representado en 3 colores.

• Zona roja: La sensibilidad del IDS debe ser baja por la cantidad de falsos positivos por la razón de que este verá todo el tráfico que entre o salga de la red.

• Zona verde: Debe ser un poco más sensible a la roja, ya que es esta zona los firewall deberán de estar en la capacidad de filtrar cualquier intrusión, en esta zona se da una tasa baja de falsas alarmas con respecto a la zona roja, debido que solo se debe permitir acceso a los servidores.

• Zona azul: Es la zona donde los IDS tendrán una sensibilidad más alta a todas las otras zonas, denominada también zona de confianza, aquí cualquier irregularidad se la tiene que tomar como una acción hostil, también se tiene que dar el más bajo número de falsas alarmas, de las cuales se tiene que estudiar inmediatamente. Hay que tener en cuenta que la zona azul no es parte de la red interna, "Todo lo que llegue al IDS de la zona azul ira hacia el firewall (por ejemplo, si utilizamos un Proxy-cache[4] . Para nuestros usuarios de web) o hacia el exterior. El IDS no escuchará ningún tipo de tráfico interno dentro de nuestra red. "En el caso de tener un IDS escuchando tráfico interno (por ejemplo, colocando entre una VLAN y su router), las falsas alarmas vendrán provocadas en su mayor parte por máquinas internas al acceder a los servidores de la red, por servidores nuestros (DNS sobre todo) y escaneadores de red, por lo que habrá que configurar el IDS para que no sea muy sensible." URBINA[03-pag18]

5.2 Criterios de Evaluación de un IDS

Según CÓRDOBA[02] hay tres criterios para evaluar este tipo de sistema, cuyos conceptos se verá a continuación.

• Precisión: Efectividad de la detección y ausencia de falsas alarmas.

• Rendimiento: Taza de eventos procesados por unidad de tiempo.

• Completitud: Capacidad del IDS para detectar la mayor cantidad de ataques posibles.

Aparte de estos tres criterios se dan unos indicadores estadísticos, que permita cuantificar la bondad del IDS tal como se puede ver en la figura 8.

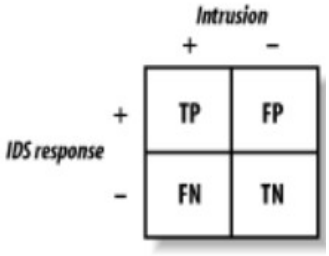


Figura 8. Cuantificación Estadística de los IDS

3 Es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

4Es un servidor especializado en guardar todos los objetos que se solicita desde internet, para luego hacer referencia a este en una nueva petición, logrando reducir así el ancho de banda.

[02].
A continuación se revisara brevemente los conceptos que tienen que ver con estos valores cuantitativos.

• Verdaderos positivos (TP): Cuando la intrusión se realiza y es correctamente detectada.

• Falsos positivos (FP): Cuando la intrusión no se realiza y aparece como correctamente detectada.

• Falsos negativos (FN): Cuando la intrusión se realiza y no es detectada.

• Verdaderos negativos (TN): Cuando la intrusión no se realiza y no es detectada.

Ya una vez conocidos los anteriores conceptos podemos definir los indicadores que se muestran a continuación.

• Sensibilidad: Mide la efectividad de las detecciones cuando existe alguna intrusión. S=(#TP/(#TP+#FN)).

• Especificidad: Mide la efectividad de las detecciones cuando no existe intrusión. E=(#TN/(#TN+#FP)).

• Precisión: Mide la efectividad de las detecciones cuando existe o no existe intrusión. P=(#TP+#TN)/ (#TP+#TN+#FP+#FN).

Con estos criterios ya se puede contar con una medida que ayude a determinar el estado del IDS dentro de la organización y así poder establecer metas que ayuden al mejoramiento de la calidad del servicio.

6 CORRELACIÓN DE EVENTOS

Se entiende por correlación de eventos a la capacidad de agrupar eventos provenientes de varias fuentes, con el objetivo de facilitar el análisis, especificando lo más detalladamente posible los mismos. La correlación de datos según NING[08] surge de la necesidad de identificar las acciones anómalas, al darse una monitorización sobre los canales de comunicación. Este proceso se puede apreciar en la figura 9. que se encuentra a continuación.

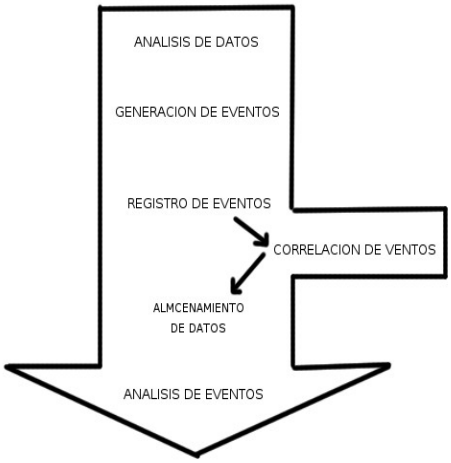


Figura 9. Proceso de Monitorización de eventos de seguridad. [08]

El proceso se da en el momento del registro de eventos de datos en los sistemas de IDS. Entre el evento generado y su almacenamiento, se compara el evento con los datos que el sistema conoce y pueda llegar a ser relacionado.

6.1 Ejemplo.

El siguiente ejemplo está basado en la figura 10 que esta propuesto en NING[08]. La ilustración consta de una red con un servidor, un HIDS, un NIDS y un equipo de análisis de vulnerabilidades del servidor de los cuales todos reportan a una base de datos centralizada que se encarga de almacenar los eventos de seguridad.

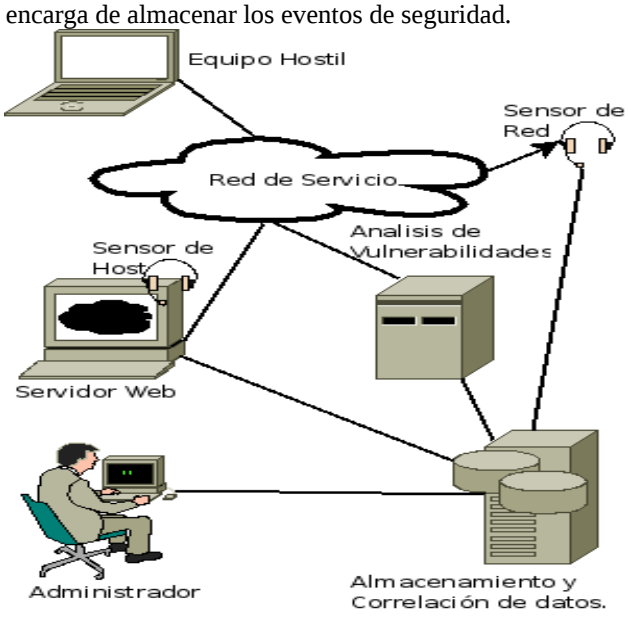


Figura 10. Arquitectura ejemplo.[08]

El atacante está en la misma red, el cuál lanza un ataque de escaneo de puertos sobre el servidor web. El ataque es

detectado tanto por el HIDS como por el NIDS dando lugar a la correlación de datos que se detallarán a continuación.

• Correlación entre varios puntos de la arquitectura: Se da para prever que los eventos aparezcan por duplicado, siendo identificados como el mismo evento generado por los diferentes IDS en la base de datos.

• Correlación con otros eventos relacionados: Se da para evitar identificar todos los eventos de conexión a cada puerto como eventos aislados, se agrupan todos los intentos de conexión dentro de un mismo evento. Correlación con otros datos conocidos: Cualquier intento de conexión a otro servicio que no sea Web se lo marcará con un nivel de cuidado inferior ya que el servidor no proporciona dicho servicio.

7 Ataques en IDS.

La información que pasa por un NIDS es lo único que se llega a conocer por estos, no se sabe de la topología de la red, ni las máquinas que lo conforman ni de los sistemas que poseen, también carece de memoria para recordar datos anómalos que hayan sucedido anteriormente, haciendo que carezcan de la habilidad de detectar ataques como son los slow scans. También se cuenta con unos ataques que afecta propiamente a los IDS.

7.1 Evasión.

Este ataque es cuando el IDS rechaza un paquete que el sistema final si acepta, perdiendo el contenido del paquete (figura 11). Este problema puede ser usado por el intruso para evadir al IDS, dado que al ser más estricto que los sistemas finales, rechazará información que si es procesada por los sistemas finales como se puede ver en la figura 11.

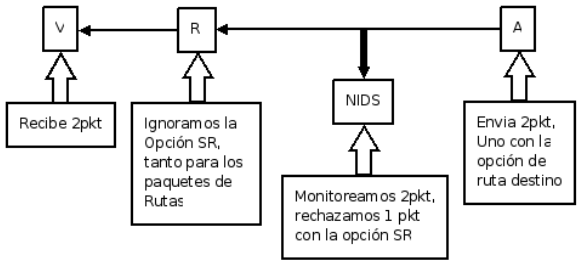


Figura 11, Funcionamiento de Evasión PORWAL[11].

Figura 11. Diferencias entre IPv4 e IPv6.

7.1.1 Soluciones ante las Técnicas de Evasión.

• Activar solo las firmas para la detección de patrones de que es de interés de la organización. Para esto, el administrador deberá decidir cuales serán activadas o cuales no, de acuerdo a las políticas que se lleguen a establecer para la red.

• Usar correlación de eventos, el cual se profundiza más adelante.

• Usar un esquema distribuido de IDS, que se detalla en la sección de recomendaciones.

7.1.2 Inserción de información.

Esta funciona cuando a un protocolo de comunicación o de seguridad se le inserta los mensajes adecuados para que llegue a experimentar múltiples implicaciones (ver figura 12); aunque llegue a ser complicado la inserción de información ya sea por los mecanismos que nos permite detectar o prevenir, es una alternativa más para esquivar al IDS. Ejemplo de esto es la inserción de paquetes de información de encaminamiento, con la finalidad de desviar tráfico de manera favorable para un intruso; cuando introducimos mensajes de gestión para la configuración de equipos.

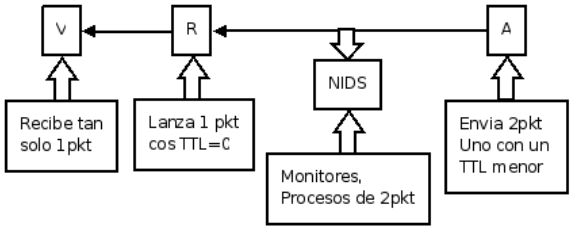


Figura 12. Funcionamiento de Inserción PORWAL[11].

7.1.3 Soluciones ante las Técnicas de Inserción.

La solución ante un ataque de inserción es el ajustar de una manera más rigurosa la selección de tramas. Claro que esto trae una mayor vulnerabilidad para que se realice un ataque por evasión que ya se vio anteriormente.

8 Recomendaciones.

• Hay algunas arquitecturas que se podrían implementar para una red, en el caso específico de la red de la UTPL, se daría mejor la implantación de la arquitectura DIDS (Distributed Intrusion Detection System) el cual combina monitoreo distribuido y reducción de datos (por medio de monitores individuales en hosts y LANs) con un análisis centralizado de datos (por medio del DIDS director) el cual ya se mencionó en esta tesis, como se ha podido ver esta arquitectura podría emplearse en la actual red de la UTPL, considerando el tamaño de la red, el tamaño del equipo capacitado en el tema de los IDS y los factores económicos que significan el mantenimiento de una infraestructura IDS.

• Una de las razones más importantes para implementar esta arquitectura se da por el tamaño de la empresa, por el

personal que se necesita para implementar o mantener un sistema IDS, si se opta por ampliar el sistema de Detección de Intrusos se debe tener IDS con sus propias bases lo que significa tener más personal capacitado para manejar estas bases de datos y por consiguiente, se necesitaría de mayores recursos económicos. Al implementar un DIDS se centraliza los datos que en general es donde se debe tener un mayor análisis y se invierte un mayor esfuerzo que en realidad solo la puede llevar a cabo una persona especializada en el tema de los IDS, logrando así una reducción en los costos de mantenimiento.

• Como se muestra en la figura 13, se puede ver la actual red de la UTPL, en un caso inicial sería recomendable ubicar el IDS entre el ASA y la red que quieran monitorear, si bien tendrá muchos falsos positivos inicialmente, el enlace al router de borde es un buen lugar para comenzar. ¿Porqué es recomendable ubicar el IDS entre el ASA y una red?. Ya que el ASA es un equipo dedicado principalmente a la seguridad, además de la conectividad, porque posee capacidades de IDS y finalmente porque tiene una muy buena visibilidad del tráfico entre las diferentes redes, cabe destacar que esto ya se encuentra implementado en la actual red de la UTPL, futuramente se puede colocar 5 IDS para monitorear las demás redes.

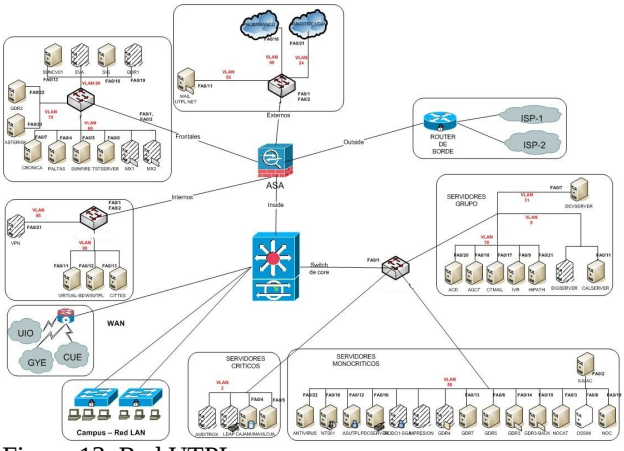


Figura 13. Red UTPL.

• Realizar un testeo de seguridad a los IDS que se tienen implementados en la red de la universidad con las herramientas ya sugeridas a lo largo de esta tesis.

• A pesar de los esfuerzos por el desarrollo de esta tecnología se presenta la limitación general ante el desarrollo de cualquier tecnología, que es la integración con otros sistemas, por tanto la interoperabilidad es un criterio que se debe mantener al insertar un IDS en la red de la UTPL.

• Para un futuro desarrollo de este tema, se debe seguir profundizando en el estudio de los IDS, sobre todo, orientado esta investigación en temas primordiales como son, la correlación de datos, la investigación acerca de nuevas herramientas que ayuden a dar una mayor seguridad a la red, como también al fortalecimiento de los IDS y su administración, garantizando así, un mejor desarrollo y funcionamiento de los mismo, claro sin olvidar el trabajo de estos juntamente con otras tecnologías como son los honeynet, los cuales son un punto clave en el fortalecimiento de la seguridad, que juntamente a los IDS, han logrado ser un gran complemento en el robustecimiento en las arquitecturas de seguridad.

9 Conclusión

• En vista de que los sistemas actuales como son los firewalls o los VPN[5] ya no son suficientes para enfrentar los actuales problemas de seguridad, se necesita incorporar un elemento más al conjunto de sistemas destinados al fortalecimiento de la seguridad de la red, como son los IDS, los cuales completarán el proceso de aseguramiento al permitir la detección o la presencia de intrusos que hoy en día debe de estar en la infraestructura.

• En cuanto a la arquitectura se debe poner un especial énfasis al motor de análisis, ya que este componente es el encargado de detectar todo el posible tráfico malicioso y para ello se tendrá que disponer para este componente de un equipo con altas prestaciones.

• Un componente medular es la correlación de datos, proceso en el cual la mayor ganancia se da por las aportaciones externas de las empresas que se dediquen a investigar sobre esta área. Hay que tener en cuenta que un punto principal es el análisis de tráfico cifrado que hoy en día no es posible.

• Un punto importante a tener en cuenta, es que se tendrá que orientar la investigación acerca de los ataques no solo a los diferentes recursos en la red, sino también al propio IDS ya que el atacante crece en habilidades, además puede utilizar mecanismos para obligar al IDS a funcionar de una manera incorrecta. Aunque los IDS son mecanismos de seguridad a lo largo de los estudios realizados en esta investigación se ve que estos pueden llegar a ser blanco de ataques, logrando así que estos no funcionen de una manera adecuada.

• Un riesgo para los NIDS, es el aparecimiento de la Ipv6 que incluye la codificación, puede significar un gran golpe mortal a estos sistemas, ya que el NIDS se ve limitado en el análisis de los paquetes encriptados y por lo tanto no es capaz de analizar si un paquete es malicioso o no y con ello tomar una acción de defensa.

• En conclusión, he aprendido que el tema de la seguridad es un campo el cual nunca se puede llegar a garantizar, que un intruso no logré burlar los sistemas empleados

5 Red Privada Virtual (Virtual Private Network), es una tecnología de red que permite extender la red local sobre una red pública.

para proteger una red. Propiamente en los IDS se ve, que como todo sistema tiene sus ventajas como sus falencias, el cual puede llegar a significar una gran ganancia en el fortalecimiento de la seguridad, al permitir no solo responder ante un ataque, si no también entregar una apreciación del estado actual de la seguridad de una red.

[01] GARCÍA, M. (2008, septiembre): La aparición de nuevo malware se ralentiza, pero se especializa cada vez más. (en línea). Formato html, Disponible http://www.gdata.es/unternehmen/ES/articleview/4240/1/229/

[02] CÓRDOBA, J., RICARDO, L., ORTIZ, D. Y PUENTES D. (2005): Los IDS y los IPS: Una comparación práctica. Formato doc. Disponible http://www.criptored.upm.es/guiateoria/gt_m142w.htm

[03] URBINA: Descripción general de los sistemas de detección de intrusos. Formato pdf. Disponible catarina.udlap.mx/u_dl_a/tales/documentos/lem/urbina_p_j/capitulo2.pdf

[04] LÓPEZ, O., PRIETO PARRA, M. Y ACOSTA, B. (2001): Arquitectura y comunicaciones en un sistema de detección de intrusos. Formato pdf. Disponible http://www.govannom.org/modules.php?name=Seguridad&d_op=getit&lid=84

[05] GARCÍA OREA, A. (2000): Presente y futuro de los IDS. Formato pdf. Disponible http://www.neurosecurity.com/whitepapers.php

[06] MUKHERJEE, B., HEBERLEIN, T. Y LEVITT, K. (1997): Network intrusion detection. Formato pdf. Disponible http://seclab.cs.ucdavis.edu/papers/mhl94.pdf

[07] WALC (2004): Sistemas de detección de intrusos. Formato pdf.

[08] NING,P. Y XU,D. Adapting query optimization techniques for efficient intrusion alert correlation. Formato pdf. Disponible http://www.germinus.com/sala_prensa/articulos/Correlacion%20Eventos%20Seguridad.pdf

[09] TRIULZI, A. (2003): Intrusion detection systems and IPv6. Formato pdf, Disponible http://www.alchemistowl.org/arrigo/Papers/SPI2003-IDS-and-IPv6.pdf

[10] JOHO, D. (2004, diciembre): Active honeypots. Formato pdf. Disponible http://www.cybertesis.cl/n-mundo.html

[11] PORWAL, P. (2005, abril): Evading/Attackin NIDS. Formato pdf.

Universidad Técnica Particular de Loja

Cesión de derechos:

Yo, Wilson Antonio Carrión Samaniego declaro ser autor del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que su parte pertinente textualmente dice: "Forman parte del parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o instucional (operativo) de la universidad".

F.....
Wilson A. Carrión S.

Estudio del Arte de los IDS- Sistemas de Identificación de Intrusos

wacarrion@utpl.edu.ec

October 13, 2009

Contents

1 Introducción. **4**
- 1.1 Malwares o Virus. . . . 6
- 1.2 Ataques. . . . 7
- 1.3 Atacantes. . . . 9

2 Seguridad Informática. **11**
- 2.1 Principios de la Seguridad Informática. . . . 11
- 2.2 Servicios de la seguridad Informática. . . . 12
- 2.3 Tecnologías de Seguridad Informática. . . . 12
  - 2.3.1 Antivirus. . . . 13
  - 2.3.2 Monitores de red y sistemas. . . . 13
  - 2.3.3 Detectores de vulnerabilidades. . . . 13
  - 2.3.4 Analizadores de Logs. . . . 14
  - 2.3.5 Proxies. . . . 14
  - 2.3.6 Cortafuegos. . . . 14
  - 2.3.7 IDS (Intruder Detection Systems). . . . 14
  - 2.3.8 Sistemas Verificadores de Integridad (SIV). . . . 14
  - 2.3.9 Monitores de Ficheros de Auditoria (LFM). . . . 15
  - 2.3.10 Sistemas Víctimas (potes de miel). . . . 15

3 IDS. **17**
- 3.1 Descripción de un IDS. . . . 17
- 3.2 Características que proporciona un IDS. . . . 18
- 3.3 Estructura de un IDS 18
  - 3.3.1 IDEF (Intrusion Detection Exchange Format). . . . 18
  - 3.3.2 CIDF(Common Intrusion Detection Framework). . . . 21
  - 3.3.3 Autopost de AusCert (Australia CERT). . . . 22
  - 3.3.4 IDWG (Intrusion Detection Working Group). . . . 22
- 3.4 Tipos de IDS. . . . 23
  - 3.4.1 Por su enfoque tenemos. . . . 24
  - 3.4.2 Por origen de Datos. . . . 26

3.4.3 Por su Infraestructura. 30
3.4.4 En función de su comportamiento. 31

4 Common Intrusion Detection Framework (CIDF). 34
4.1 Generadores de Eventos (E-boxes). 35
4.2 Motor de Análisis (A-boxes). 35
4.2.1 Redes Neuronales Artificiales. 35
4.2.2 Métodos Estadísticos. 36
4.3 Unidades de Almacenaje (D-boxes). 36
4.4 Unidades de Repuesta (R-boxes). 36
4.5 Capas y Servicios. 36
4.5.1 Capa de GIDOs (Generalized Intrusion Detection Objects). 37
4.5.2 Capa de Mensajes. 39
4.5.3 Capa de Transporte. 39
4.6 CISL(Common Intrusion Specification Language). 40
4.6.1 Requerimientos del leguaje. 41

5 Funcionamiento de un IDS. 44
5.1 Ubicación de un IDS en la red. 44
5.2 Requisitos de un IDS. 45
5.3 Ciclo de Vida de un IDS. 46
5.4 Criterios de Evaluación de un IDS. 47
5.5 Análisis entre diferentes tecnologías de seguridad. 48
5.5.1 Sistemas de Prevención de Intrusiones. 48
5.5.2 Firewall vs IPS. 49
5.5.3 IDS vs IPS. 49
5.5.4 Respuestas Activas vs IPS. 49
5.6 Análisis de la rentabilidad de un IDS. 50

6 Correlación de eventos. 51
6.1 Ejemplo 1. 52
6.2 Ejemplo 2. 54
6.3 Definición de una correlación de alerta. 56
6.3.1 Definición 1: Correlación Directa (Caso simple). 56
6.3.2 Definición 2: Correlación Directa (Caso General). 57
6.4 Definición 3: Correlación Indirecta. 58
6.5 Generación de reglas de correlación. 58
6.6 Herramientas de Correlación de Datos. 62
6.7 Métodos de replicación de datos. 63
6.7.1 Conectividad con medios compartidos. 63
6.7.2 Puertos Espejos. 63
6.7.3 Test Access Point (TAP). 63
6.8 IP factor determinante en los IDS. 66
6.8.1 IPv4 vs IPv6. 66
6.8.2 No hay información de fragmentación en la cabecera. . . . 68
6.8.3 Comparación. 68

7 Ataques en IDS. 69
7.1 Evasión. 69
7.1.1 Soluciones ante las Técnicas de Evasión. 70
7.2 Inserción de información. 71
7.2.1 Soluciones ante las Técnicas de Inserción. 73
7.3 Resource exhaustion o agotamiento de recursos. 73
7.3.1 Técnicas DOS. 73
7.4 Otros Ataques. 74
7.4.1 Verificación de la lista de protocolos. 74
7.4.2 Verificación de los protocolos de la capa de aplicación. . . 74
7.5 Criterio de evaluación ante el ataque. 74
7.5.1 Algoritmo de activación. 75

8 Discusión. 76

9 Recomendaciones. 82

10 Conclusiones. 84

11 Anexo 1.1 89

12 Anexo 2.1 94

13 Anexo 3.1 98

14 Anexo 4.1 105

15 Anexo 5.1 110

1 Introducción.

En el ámbito de la seguridad el problema de la intrusion ha ido creciendo cada día más, en GARCÍA[01] se puede ver como en este ámbito día a día salen nuevos programas que buscan afectar a un equipo, ya sea para daños locales o para llegar a perjudicar toda una red informática. En un informe publicado con fecha 11 de Septiembre del 2008 por parte de la empresa alemana G DATA Software [1], se registró una cantidad de 100.000 nuevos programas de malware [2]. A continuación se puede ver en la tabla 1 el crecimiento del mes de agosto con respecto al mes de Julio del malware.

Tabla 1: Porcentajes de Ataques por Malware del mes de Agosto con relación al mes de Julio. GARCÍA[01]

Malware	Porcentaje
Troyanos	26.9%
Puertas Traseras	20.5%
Spyware	19.6%
Trojan downloaders	15.7%
Adware	6.0%
Otros	11.3%

Donde el principal objetivo de los cybercriminales fue el robo de los datos de los usuarios y la integración de los PCs [3] infectados en botnets [4]. En esta misma publicación el director de los laboratorios de seguridad de G data Ralf Benzmüller ha pronosticado que para el año 2009 el número de malware que se tendrá fácilmente superará el millón, lo cual llega a representar un incremento del 778% frente al año pasado. Hay que tener en cuenta que estos datos están orientados al Sistema Operativo Windows, en el caso de sistemas operativos que no sean Win 32[5] la aparición de un virus llega a ser muy baja como se muestra en una estadística entregada en la figura 1 que se encuentra a continuación.

[1] G DATA SOFTWARE, es una empresa de software innovadora y en proceso de rápida expansión enfocada en las soluciones de seguridad informática. Como especialistas en seguridad en Internet y pionera en el sector de la protección antivirus, esta empresa fundada en 1985 desarrolló el primer programa antivirus hace ya más de 20 años. Desde hace cinco años G DATA ha ganado más distinciones y ha salido triunfador de más certámenes nacionales e internacionales que ningún otro fabricante europeo de software de seguridad.

[2] Software malicioso.

[3] Término genérico utilizado a veces para referirse a todas las microcomputadoras.

[4] PCs que se pueden controlar remotamente.

[5] Versión del API de Windows de 32 bits. Está compuesta por funciones en C almacenadas en librerías de enlace dinámico DLL.

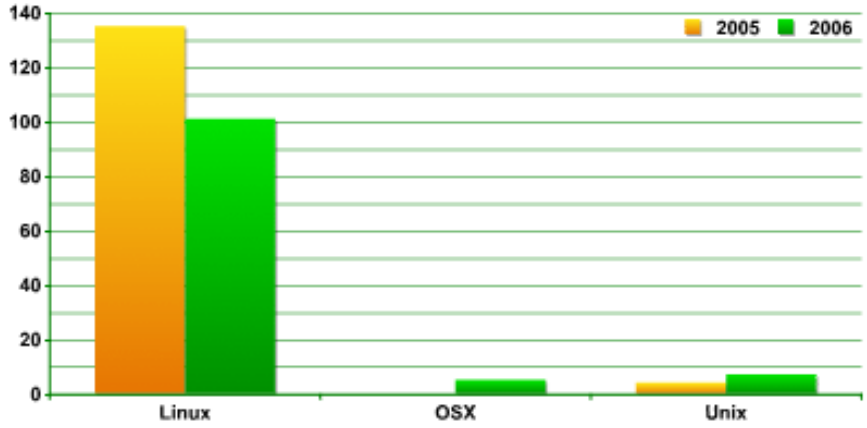


Figura 1: Número de programas malintencionados para sistemas operativos similares a Unix KONSTANTIN[02].

Al ver las estadísticas de la figura uno, se llega a entender el porqué a un malware en plataformas diferentes a Win32 llega a denominarse un virus de colección como en KONSTANTIN[03] se menciona que la causa de esto es porque en la actualidad estos sistemas no gozan de la popularidad como un Win32, pero en el futuro se podría tener una apreciación diferente de acuerdo al Sistema Operativo que llegue a ser común en los ordenadores. Otro dato que hay que destacar que existen periodos donde estos ataques se intensifican y esto depende de las oportunidades que se llegan a presentar. Un ejemplo de esto es, en determinadas fechas en donde se dan eventos de interés mundial como los pasados juegos olímpicos de Pekín, donde los cybercriminales aprovechan estos eventos para capturar datos importantes como por ejemplo, números de cuentas de crédito y lucran con estos datos en el mercado negro. Como se puede apreciar, el problema de seguridad cada día toma nuevos retos, al tratar de darle solución a los ataques que cada vez son más creativos por parte de los cybercriminales.

Otro factor importante que hay que considerar dentro del entorno de la Universidad Técnica Particular de Loja (UTPL) es la necesidad del fortalecimiento de la seguridad. El esquema de seguridad de la universidad ha tenido un desarrollo importante, en el se han incoporado nuevos componentes con la finalidad de dar mayores beneficios, sin embargo; no se cuenta con un estudio detallados de los mismos, dejando a los administradores con una falta de conocimiento sobre el funcionamiento de estos sistemas que permita optimizar su uso y rendimiento. Además no se tiene claridad sobre los problemas de seguridad que tiene los IDS[6] al ser equipos perimetrales de seguridad o a que ataques están sometido ni que problemas de seguridad pueden presentar.

Por otro lado existe algunos IDS y hay que determinar cuál es el sistema adecuado a utilizar dentro de la universidad y los pasos siguientes a mejorar la determinación de los IDS.

[6]Sistemas de Identificación de Intrusos

Finalmente qué viene después de los IDS's cuáles serían las tendencias y su papel con respecto al protocolo IPv6 es uno de los temas a abordar en la proyección de esta tesis.

1.1 Malwares o Virus.

En primer lugar hay que entender que un virus informático no es un virus que va a infectar al cuerpo humano, si no que es un programa diseñado para ejecutarse en la PC el cual realizará una acción en nuestro ordenador, según la empresa de antivirus Panda Security [7], los virus pueden ser clasificados de muchas maneras. En la tabla 2 se muestra una de las clasificaciones de estos.

Tabla 2: Clasificación de virus. PANDA SECURITY[04]

Clasificación de clases de Virus
Por su origen
Por las técnicas que utilizan para infectar
Por los tipos de ficheros que infectan
Por los lugares donde se esconden
Por los daños que causan
Por el sistema operativo o la plataforma que atacan

Incluso algunos al inicio no se llegan a clasificar ya que pueden traer un comportamiento novedoso o totalmente nuevo, o algunos pueden llegar a pertenecer a varias clasificaciones. El anexo "1.1" presenta mayor detalle de esta sección. Pero no todos son simples programas, también hay los denominados Códigos de Explotación. En la tabla 3 y 4 se da una breve descripción de como actúan.

Tabla 3: Diferentes tipos de Código de Explotación. ARCE[05]

Código de Explotación	
Exploit	Código de explotación. Algoritmo, programa o herramienta desarrollada para explotar una vulnerabilidad y lograr un objetivo específico.
PoC	Prueba de concepto del código de explotación. Código de explotación cuyo único objetivo es demostrar la existencia de una vulnerabilidad.
0-day vulnerability	Vulnerabilidad para la que el conocimiento de su existencia no es de acceso público.
0-Day exploit	Código de explotación para una vulnerabilidad de día cero.

[7] Panda Security es el cuarto mayor vendedor de antivirus en todo el mundo. Fundada en 1990 en la ciudad de Bilbao, España.

Tabla 4: Funcionamiento de "código de Explotación" ARCE[05].

Código de explotación	
Código de explotación separado en componentes	- Shellcode monolítico (1989-1994-2000). - Aislación funcional: Vector de ataque, adquisición del control de flujo, Código-objetivo.
Componentes re-usables	- Técnicas de explotación. - Método de conexión. - Funcionalidad Final. - Stagers.
Implementación de técnicas de explotación	- Sobre-escritura de pila (stack), heap, exception handler. - Signal handlers, GOT, PLT, vpointers, protección de la pila, DEP.
Técnicas anto-detección y prevención	- Polimorfismo, metamorfismo, encoding, fragmentación (red). - Syscall proxying, agentes multi-propósito, volatibilidad, rootkits (host)

1.2 Ataques.

En esta sección se tratará de los tipos de ataque, antes es necesario entender que es un ataque informático. Se puede decir que un ataque informático es un intento organizado por parte de una persona o conjunto de personas cuyo objetivo es causar daños o problemas dentro de un Sistema Informático o red. El anexo "2.1" presenta mayor detalle de los tipos de ataque. En la tabla 5 se puede ver unos conceptos básicos que hay que tener en cuenta para entender de una manera más exacta que es un ataque.

Tabla 5: Ataques terminología. ARCE[05]

Terminología	
Explotar	Utilizar en provecho propio, por lo general de un modo abusivo, las cualidades o sentimientos de una persona, de un suceso o de una circunstancia cualquiera.
Falla	Defecto material de una cosa que merma su resistencia.
Vulnerabilidad	Falla en un sistema que, de ser explotada, causan un efecto negativo en la seguridad de dicho sistema (Bug).

Una vez entendidos estos conceptos básicos en la figura 2 se puede ver un cuadro de la realidad de los atacantes y su desarrollo a lo largo de la historia. Como se observa, el conocimiento de estos atacantes ha bajado con el tiempo pero la diversidad de herramientas y los tipos de ataques se han incrementado.

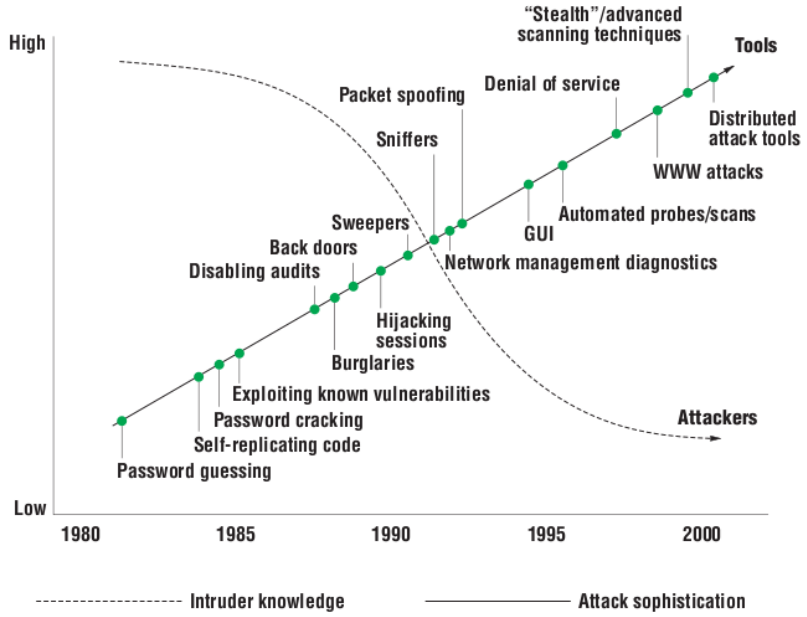


Figura 2. Sofisticación de los ataques vs Técnicas de Intrusión MCHUGH[07].

Esto dá una pauta de lo fácil que se está volviendo realizar un ataque, donde ya el conocimiento técnico no es tan fundamental como antes, simplemente el atacante tiene que saber qué es lo que quiere hacer y conseguir una herramienta que le ayude en su objetivo. Hasta este momento se ha podido apreciar que es un ataque y como estos se están adaptando. Pero es necesario analizar la orientación en la cual se está dando los ataques, en tabla 6 se da un listado del porque algunos atacantes se enfocan en atacar una estación de trabajo.

Tabla 6: Razones por las cuales se da un ataque a una estación de trabajo. ARCE[05]

Ataques a la estación de trabajo	
Client-side exploits	Cúmulo de aplicaciones vulnerables. Web browser, lector de email, Media players, instant Messaging. Aplicaciones de negocios, administrativas y de oficina, file viewers, utilitarios, agentes de resguardo (backup) y seguridad (PF, av, IDS). Componentes re-usables y de terceros.
Difícil control de Inventarios y Cambios	Que estaciones hay en la red, direcciones IP, software instalado, usuarios.
Difícil control instalación de contra-medidas	Patches, políticas de acceso, etc.
Operada por Usuarios despreocupados y/o novatos	Usuarios que dejan entradas para posibles ataques, mala utilización de recursos, etc.
Cuestión de escala y probabilidad de éxito	Son menos monitoreados y tiene una alta probabilidad de tomar el control de la máquina.

Lo que refleja la tabla 6 es lo que se conoce como la ley del menor esfuerzo, ya que es más fácil atacar un equipo de trabajo, el cual puede tener un montón de puntos débiles, que atacar un servidor que está muy bien protegido.

Para poder entender el progreso de los ataques, hay que ver las nuevas fuentes que pueden aprovechar los atacantes. En la tabla 7 se da una breve referencia de los posibles medios que el atacante seguramente aprovechará para realizar su ataque.

Tabla 7: Tabla que muestra los futuros medios y destinos de ataque. ARCE[05]

Nuevos vectores de Ataque	
Redes Inalámbricas	- 802.11 - bluetooth
Nuevas interfaces para periféricos	- Firewire. - ISB. SCSI, PCMCIA, etc.
Nuevos dispositivos "Conectados"	- PDA, teléfono celular, cámara de fotos, consolas de juegos. - Electrodomésticos. - Automóviles.

El área que se tiene para realizar un ataque, es bastante amplia y a lo largo de esta lucha se ha tratado de dar muchas soluciones frente a este problema.

1.3 Atacantes.

Como se ha podido ver no solo ha cambiado la complejidad de las herramientas utilizadas para efectuar ataques, sino también su variedad y sencillez. Hoy por hoy estas herramientas dan la capacidad de realizar una mayor variedad de ataques. Según ARROYAVE[10] ya no solo se puede hablar de una distinción

entre herramientas o clases de ataques, tenemos también una distinción entre los atacantes, de los cuales se nombrarán a continuación.

- Hacker: Según ARROYAVE[10] Se dice de un hacker a una persona que posee un gran conocimiento en las distintas áreas de la computación, cuya área fuerte es lo relacionado con las tecnologías de información, redes y sistemas operativos, este denominado hacker se especializa en entrar en un sistema del cual no tiene ningún permiso. En la actualidad estos denominados hackers han despertado la atención de varias empresas, razón por la cual han sufrido un cambio en su nombre y se han llegado a dividir en 2 grupos como podemos mencionar los White hats o "hacker buenos" y los Black hats o "crackers".

- Script kiddies: Según ARROYAVE[10] Se dice de un script kiddies a una persona que posee pocos conocimientos sobre informática y cuyo fin es el tratar de violar la seguridad de un sistema ajeno, lo particular de este denominado script kiddies es que se vale de exploits [8] y programas creados por terceros. Este script kiddies puede llegar a ser tomado como una amenaza dentro de una red pequeña, entre cibernautas desprevenidos o de personas que posee herramientas de seguridad poco desarrolladas.

- Personal descontento o desprevenido: Una de las mayores amenazas que puede llegar a tener una empresa o institución en lo referente a la seguridad es un empleado descontento, ya que estos llegan a tener un mayor conocimiento de la red en la que trabaja y las manera de realizar los procesos dentro de ella, según ARROYAVE[10] "Ya sea por error o por descontento en su trabajo, un empleado puede causar grandes perjuicios a un sistema informático. Desde perder un password o dárselo a la persona equivocada de manera desprevenida hasta atentar contra la infraestructura de la red misma." Esta clase de atacante pone a prueba las políticas de seguridad de nuestra red no solo desde afuera si no desde a dentro.

[8] Un 'exploit' es un programa o técnica que aprovecha una vulnerabilidad. Los exploits dependen de los sistemas operativos y sus configuraciones, de las configuraciones de los programas que se están ejecutando en un ordenador y de la LAN donde están.

2 Seguridad Informática.

A lo largo de la historia este tema ha crecido grandemente, siendo sometido a varias formas de desarrollo y también a muchos cambios, dando problemas no sólo de carácter tecnológico si no cultural, por estos motivos se ha establecido ciertas características que se estudiarán a continuación.

2.1 Principios de la Seguridad Informática.

En los anteriores puntos se ha visto los ataques y sus formas de empleo, pero en realidad un ataque solo está dirigido a la penetración de un sistema. No solo se debería ver este punto, la mayoría de los ataques tienen un objetivo primordial y el cual en la actualidad viene a constituir el bien más importante y costoso de una empresa que es la información, como se puede ver en SÁNCHEZ[12] se da mención de 4 maneras de atacar este activo los cuales son: Corrupción, acceso indebido e incluso hurto y eliminación, en cierta manera la seguridad informática se basa en la preservación de 3 principios básicos que se cita en SÁNCHEZ[12] son los siguiente:

- Confidencialidad: El principal objetivo de este principio es el de garantizar que solo la persona o personas autorizadas tengan acceso a cierta información, tomando en cuenta que la información está destinada para cierto grupo de personas y en muchas ocasiones a una sola persona. "La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, es decir en los sistemas y dispositivos en los que reside dentro de la red, como durante su procesamiento y tránsito, hasta llegar a su destino final".

- Integridad: En este principio se tiene que garantizar que la información no sea modificada o alterada en su contenido por personas que no tienen autorización o de forma indebida y por parte del sistema garantizando la exactitud y confiabilidad de los mismos, este principio se ha definido en dos partes: "La integridad de los datos, se refiere a que la información y los programas solo deben ser modificados de manera autorizada por las personas indicadas para ello. Estas alteraciones pueden darse por inserciones, sustituciones o eliminaciones de contenido de la información. Por su parte, la integridad de los sistemas, hace referencia a que todo sistema debe poder cumplir su función a cabalidad, sin ninguna violación o modificación del mismo, en su estructura física o lógica, sin perder necesariamente su disponibilidad" SÁNCHEZ[12].

- Disponibilidad: Su función es la de asegurar que la información y los sistemas que la soportan, estén siempre disponibles para el que los necesita, al referirse a los sistemas que soportan la información, se trata de

toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento de la información. Una segunda cualidad que se menciona acerca de la disponibilidades es "la capacidad que deben tener los sistemas de recuperarse ante interrupciones del servicio, de una manera segura que garantice el continuo desarrollo de la productividad de la organización sin mayores inconvenientes" SÁNCHEZ[12].

2.2 Servicios de la seguridad Informática.

Para lograr llevar a cabo los principios básicos de la seguridad informática que se habla en el paso anterior se tiene que implementar cuatro servicios principales definidos por el mismo autor de los cuales se verá a continuación.

- Autenticación: Su función es la de garantizar la validez de una identificación que se entrega para acceder a cierta información, previendo medios para verificar la identidad de un sujeto, básicamente de tres formas: "por algo que el sujeto es, por algo que el sujeto tiene o por algo que el sujeto conoce".
- Autorización: Este por su parte permite la especificación y continua administración de las acciones permitidas por ciertos sujetos, para el acceso, modificación o inserción de información de un sistema, principalmente, mediante permisos de acceso sobre los mismos.
- No repudio: Este debe garantizar quién o quiénes son los remitentes y destinatarios de cualquier información, de lo cual su función principal es dar los mecanismos para identificar quien ha llevado una o varias acciones en un sistema.
- Auditabilidad: Este tiene la función de entregar mecanismos que nos permita la detección y recuperación ante posibles fallas o incidentes de seguridad, mediante el registro de una bitácora que almacenará todos los eventos y acciones hechas sobre un sistema. En la actualidad contamos con algunas tecnologías que podrían ayudar al cumplimiento de estos principios, los cuales se estudiara a continuación.

2.3 Tecnologías de Seguridad Informática.

La seguridad se ha convertido en un elemento clave y totalmente necesario en el entorno de un sistema, ya que al colocar información o recursos en la red, resulta necesario proteger estos recursos en cualquiera de sus acciones, ya sea su almacenamiento, procesamiento o intercambio. Razón por la cual se tiene que pensar en la implementación de algunas herramientas de las cuales se puede nombrar las siguientes:

- Antivirus.
- Monitores de red y sistemas.

- Detectores de vulnerabilidades.
- Analizadores de Logs.
- Proxies.
- Cortafuegos.
- IDS (Intruder Detection Systems).
- Sistemas Verificadores de Integridad (SIV).
- Monitores de Ficheros de Auditoria (LFM).
- Sistemas víctimas (potes de Miel).

A continuación se verá una breve introducción a cada una de estas herramientas o programas tanto comerciales como no comerciales que han llegado sin duda a tener una gran aceptación en el área de la seguridad informática.

2.3.1 Antivirus.

Muchas empresas como Norton Antivirus, Panda Antivirus, Vantivirus entre otros coinciden en una cosa, que un antivirus es un programa que se encarga de detectar y eliminar otros programas maliciosos denominados "Malware", en la actualidad el antivirus es una herramienta que tiene una gran popularidad y está en la mayoría de los computadores.

Herramientas de Antivirus:

- Antivir (http://www.avira.com/es/pages/index.php).
- Panda Antivirus (http://www.pandaantivirus.com.ar/index.php).

2.3.2 Monitores de red y sistemas.

Como su nombre lo revela, es un programa que esta monitoreando la red o el sistema, este generalmente funciona en modo promiscuo [9] y es muy usado tanto por los intrusos como por los desarrolladores.

2.3.3 Detectores de vulnerabilidades.

Los detectores de vulnerabilidades son herramientas que ayudan hacer un análisis de los equipos que se encuentran en una red, su trabajo se especializa en analizar los puertos que puede tener abiertos un equipo o conjunto de equipos, para esto es necesario definir el rango que se desea analizar y finalmente dar un informe de que puertos estan abiertos. Esta clase de herramientas pueden ser utilizadas tanto por atacantes como administradores de redes.

[9] Que se infiltra de una manera silenciosa o que los usuarios no conocen que está operando en su red o sistema.

2.3.4 Analizadores de Logs.

Estas herramientas tienen muchas utilidades pero en general permiten tener o contar con una plataforma que facilite el manejo de los Logs. Más adelante se puede apreciar una derivación de un analizador de logs en los denominados LFM [10].

2.3.5 Proxies.

Un servidor proxy es muy famoso dentro de la red de una empresa o institución, es muy común que una computadora quiere salir a Internet y esta pase por un servidor proxy, aunque se lo use principalmente para la web su concepto da una explicación más amplia "proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro". En otras palabras es un intermediario.

2.3.6 Cortafuegos.

Según RIVERA[13] proporciona el siguiente concepto "Programa o equipo que separa a un equipo, una red local (LAN) o una red global (WAN) en dos o más partes, con propósitos de seguridad, limitando o supervisando los accesos a sus recursos."

2.3.7 IDS (Intruder Detection Systems).

Según ARROYAVE[10] un sistema de detección de intrusos es un programa que funciona en una red determinada y su función es la de detectar intrusiones, además que se puede considerar como el guardián de nuestra red y la alarma que nos avisa de los posibles ataques de los cuales somos víctimas. "Sus aplicaciones como herramienta de seguridad son varias y el implementarlas y mantenerlas como bastión para la seguridad de nuestra información constituyen buenas prácticas en las redes telemáticas." De esta herramienta se profundizará más adelante.

2.3.8 Sistemas Verificadores de Integridad (SIV).

La función de esta herramienta es la de comprobar la integridad de los ficheros del sistema donde se ubican, esto se lleva a cabo al realizar sumas de verificación que son ejecutadas en un determinado intervalo de tiempo y sobre los ficheros seleccionados por el administrador del sistema. Según GARCÍA[14] "Dichos programas suelen verificar los permisos en ficheros y directorios, las cuentas de usuarios, sentencias en el registro de Windows y en el cron de Unix". A diferencia de los IDS que emiten alarmas, estos no hacen emisiones de alarmas, más bien generan registros (Logs) con los resultados que proporcionan, hay que destacar que gracias a la cantidad inmensa que arrojan de información el análisis de estos registros se vuelve complejo.

[10] Log file monitor (Monitores de fichero de Auditoria).

Herramientas SIV

- Tripwire (www.tripwire.com)[11].

2.3.9 Monitores de Ficheros de Auditoria (LFM).

Esta herramienta proporciona un análisis para la búsqueda de patrones de ataques que son reflejados en los registros que nos proporcionan los programas del sistema al revisar los ficheros logs de cualquier sistema con la condicionante que estos ficheros deben estar en un texto claro. Según GARCÍA[14] "La labor de revisión de los ficheros se apoyan en marcas (offset) para garantizar la reanudación del trabajo de forma eficiente. Las bases de datos utilizadas son modificables o actualizables. Esto permite el "afinamiento" de la herramienta de acuerdo a las características del sistema que se pretende proteger. De manera general envían mensajes de correo para notificar el resultado de sus trabajo." Hay que tener en cuenta, que la frecuencia que estos programas tienen, para entrar en funcionamiento depende de la velocidad que poseen para reaccionar ante los ataques. Es claro que entre mayor sea la velocidad de revisión de los logs, mayor será la repuesta ante un ataque. Un punto clave que hay que tener en cuenta, es en la emisión de notificaciones, éstas deben ser cortas, no deben ser muy frecuentes para que no le quite importancia a las notificaciones y principalmente no tienen que ser muy retardadas para que se pueda reaccionar de una manera rápida ante una intrusión detectada.

Herramientas de LFM

- SALDI (http://cujae.edu.cu/telematica/).
- Logcheck (http://sourceforge.net/projects/logcheck/).
- GFI LANguard Security Event Log Monitor (http://www.gfi.com/lanselm/).

2.3.10 Sistemas Víctimas (potes de miel).

En términos más sencillos, es una computadora fácil de atacar, donde sus servicios y sistema operativo está desactualizado y sus vulnerabilidades son conocidas y cuyo fin es el de desviar la atención de los atacantes a estos sistemas no tan seguros. En GARCÍA[14] nos dice que "la implementación de estas herramientas puede ser compleja e incluso la comprensión de su necesidad difícil para muchas entidades." Para lograr este fin se puede usar herramientas que simulan varios sistemas operativos y los servicios que los mismos ofrecen. La ventaja que le podemos obtener a estos sistemas carnadas, es el de estudiar como un intruso pretende atacar el sistema, el momento de inicio, el origen (si no se emplean técnicas de spoofing) y la estrategia que emplea el atacante. Generalmente estos sistemas generan logs detallados y lanzan alertas ante un ataque detectado,

[11] El SIV más conocido es sin duda Tripwire, comentado en este mismo trabajo; la importancia de estos mecanismos es tal que en la actualidad algunos sistemas Unix integran 'de serie' verificadores de integridad, como Solaris y su ASET (Automated Security Enhancement Tools).

para luego ser estudiando tanto por usuarios como por investigadores, tal es el caso de proyecto Honeynet [15] cuyo fin ante esta investigación es la de "elevar la atención en la comunidad de usuarios de las amenazas existentes en la red, informar y enseñar sobre los procedimientos mencionados y realizar investigaciones sobre el tema de la seguridad."

Herramientas de Sistemas Victima.

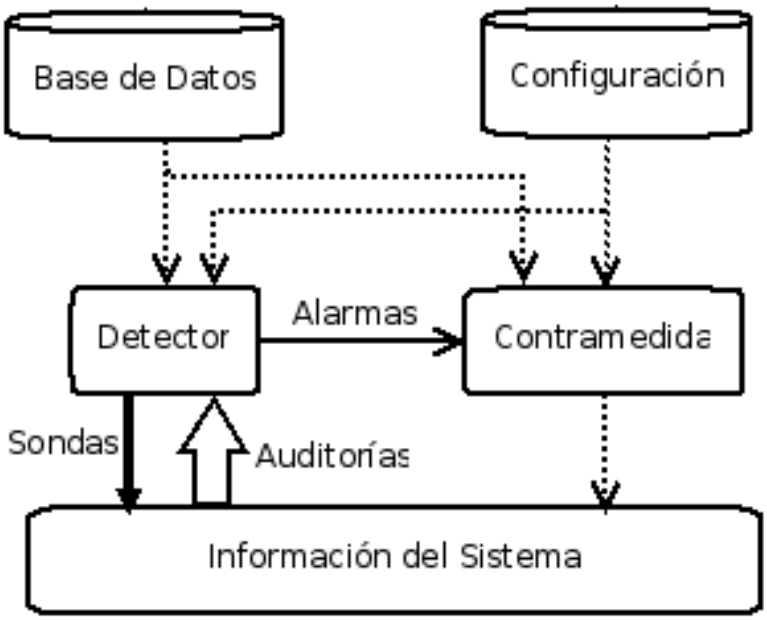
- Specter (http://www.specter.com).
- Honey Net Project (http://honeynet.org).

3 IDS.

El estudio de este capitulo se centran en los sistemas de Detección de Intrusos que es un conjunto de métodos y técnicas que se encargan de revelar una actividad sospechosa, incorrecta o inapropiada sobre un recurso o un grupo de recursos computacionales ya puedan ser estos firewalls, estaciones de trabajo, dispositivos de red, servidores, etc. Hay que entender que un IDS se puede dar tanto en software como en Hadware o puede ser una combinación de ambos cuyo objetivo será el de detectar la actividad de un intruso. A continuación se entrará más a detalle de lo que es un IDS.

3.1 Descripción de un IDS.

Un IDS puede ser descrito como un detector que procesa la información proveniente del sistema monitoreado. El cual es considerado como una herramienta de apoyo en procesos de auditoría, entendida como el control del funcionamiento de un sistema a través del análisis de su comportamiento interno como se ilustra en la Figura 3:



Nota: El calibre de la flecha representa la cantidad de información que fluye desde un componente hasta el otro.

Figura 3: Un sistema de detección de intrusos Simplificado CÓRDOBA[19].

El IDS se vale de tres tipos de información para detectar un tipo de intrusión, estos son: la información recolectada de ataque previos, la configuración actual del sistema y la descripción del estado actual referente a comunicaciones y procesos.

3.2 Características que proporciona un IDS.

Primeramente es una herramienta que intenta detectar o monitorear los eventos que se dan lugar en un sistema informático o red. Permite tener una alerta anticipada ante una actividad sospechosa, aunque también estos buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre la red o host. Otra característica importante de estos, es que están diseñados para detener el ataque, se puede generar algún tipo de alerta ante estos como puede ser, el envió de un email, al administrador encargado. También los IDS permiten ir documentando los riesgos de la organización.

3.3 Estructura de un IDS .

Por el tiempo han llegado a existir dos grandes tendencias en la estandarización de los IDS, IDEF(Intrusion Detection Exchange Format) y CIDF(Common Instrusion Detection Framework) y otras menos populares como son el Autopost de AusCERT(Computer Emergency Response Team), IDWG(Intrusion Detection Working Group) y CVE(Common Vulnerabilities and Exposures).

3.3.1 IDEF (Intrusion Detection Exchange Format).

Esta fue desarrollado por "Intrusion Detection working Group del IETF" el cual a su vez estaba formado por empresas que se dedicaban a las intrusiones, básicamente este se dio por el rechazo con la CIDF de la cual se hablara más adelante, estos definen protocolos, en las comunicaciones contamos con IDXP (intrusion Detection Exchange Protocol) y en los datos IDMEF (Intrusion Detection Message Exchange Format) que se mencionará más adelante.

IDXP: Intrusion Detection eXchange Protocols. Está basado en el protocolo BEEP (Blocks Extensible Exchange Protocol, RFC 3080), el que se encarga de establecer sesiones para permitir el intercambio de mensajes entre emisor y receptor, codificados en XML[12]. A continuación se verá algunos puntos que se refieren a IDXP:

Mecanismos:

[12]XML, siglas en inglés de Extensible Markup Language («lenguaje de marcas), es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). Es una simplificación y adaptación del SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML). Por lo tanto XML no es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades.

- Establecimiento de sesión BEEP.
- Negociación de un perfil de seguridad aceptable.
- Transmisión de datos IDXP.

Garantías:

Se garantiza los requisitos exigidos para el transporte de datos IDMEF como son:

- Transmisión fiable de mensajes.
- Interacción con cortafuegos.
- Autenticación.
- Confidencialidad.
- Integridad.
- Autenticación unívoca de emisores.
- Resistencia ante ataques DoS.
- Resistencia ante mensajes duplicados.

IDMEF: Intrusion Detection Message Exchange Format. Se encarga de definir un formato de datos estándar con el cual se plantea el manejo de alertas entre los diferentes elementos dentro del esquema en el cual se trabaja. Este está basado en XML para el establecimiento de un DTD (Document Type Definition) en el cual se define la sintaxis adecuada para representar la información relativa a intrusiones.

Alertas de IDMEF. La clase alert esta es prácticamente el corazón de IDMEF, donde cada alerta tiene un identificador de tipo STRING y una serie de clases agregadas que se muestras en la figura 4 a continuación.

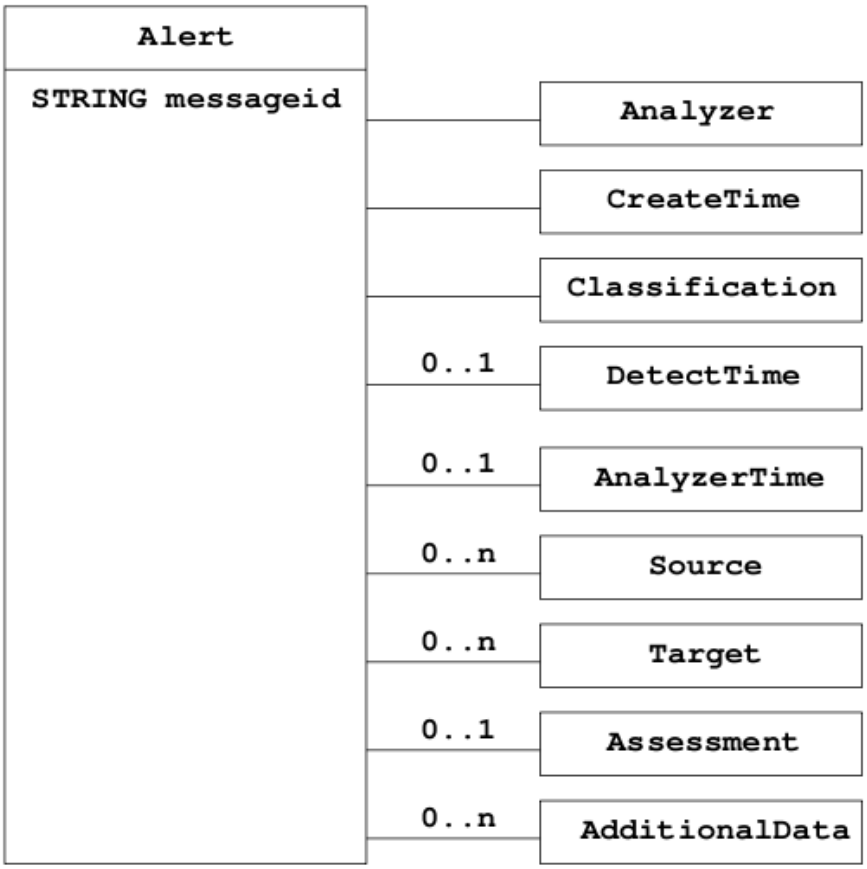


Figura 4. Diagrama de clase agregadas de la clase alert de IDMEF VILLALÓN[22].

Como se puede ver la clase alert está conformada de 11 clases agregadas de las cuales se verá su función a continuación:

- Analyzer: Identificador del analizador que dispara la alerta.
- CreateTime: Es la fecha y hora de la creación de la alerta.
- DetectTime: Es la fecha y la hora en donde se detecta un evento que origina la alerta.
- AnalyzerTime: Fecha y hora del analizador cuando origina la alerta.
- Classification: Nombre de la alerta.
- Assessment: Información relativa al impacto del evento, acciones de repuesta emprendidas y confianza de la detección.

- AdditionalData: Información adicional de la alerta.
- Source: Fuente del evento que disparo la alerta.
- Target: Objetivo del evento que disparo la alerta.

IDMEF Ejemplo:
<idmef: IDMEF-Message version="1.0" xmlns: idmef="http://iana.org/idmef">
<idmef:Alert messageid="abc123456789">
<idmef:Analyzer analyzerid="bc-sensor01">
</idmef:Analizer>
<idmef: CreateTime ntpstamp="0xbc71e980.0x00000000"> 2000-03-09T08:12:32-01:00
</idmef:CreateTime>...
Para mayor información visitar http://www.ietf.org/html.charters/idwg-charter.html

3.3.2 CIDF(Common Intrusion Detection Framework).

Esta fue promovida por DARPA(Defense Advance Research Proyects Agency), su principal meta es la orientación a la investigación de detección de Intrusos, aunque entre en el sector comercial tuvo poca aceptación sus conceptos se han abierto camino hasta la actualidad definiendo lenguajes propios, uno para la comunicación entre los elementos del Framework, y otro para definir los datos, CISL(Common Intrusion Specification Languaje). Una de las características principales se da en el equipo de repuesta al poder interactuar con otras cajas y poder responder a los eventos como se muestra en la figura 5 a continuación.

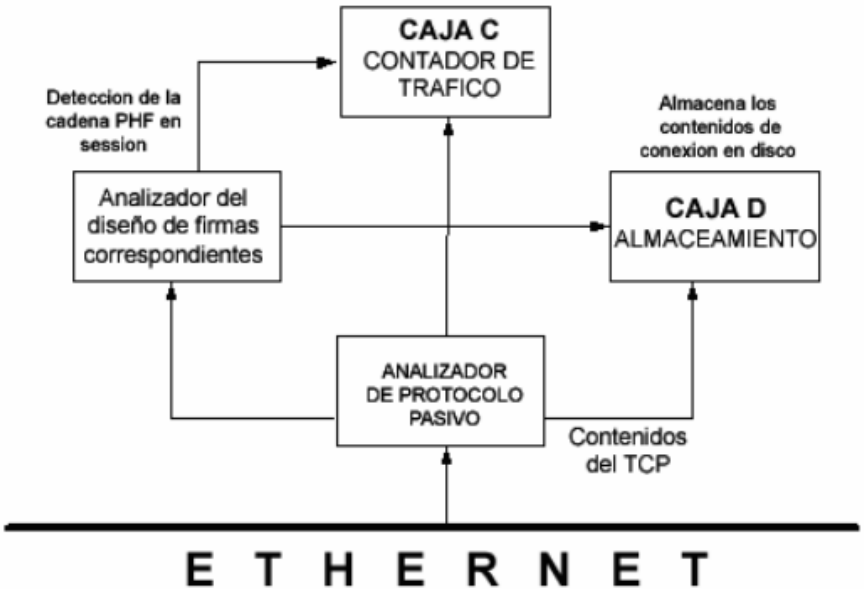


Figura 5. Descripción de un modelo CERT (Computer Emergency Response Team) URBINA[20].

3.3.3 Autopost de AusCert (Australia CERT).

Esta diseñado sobre un sistema en el cual se puede trabajar de una manera más fácil que el CIDF/CISL, además de que tiene una alta interoperabilidad y es muy sencillo de construir y analizar, también contamos con que este permite que se analice y se agregue un informe en una base de datos tan solo usando unas cuantas líneas del lenguaje Perl. La manera de trabajo de esta frente a un incidente es como la del informe que se presenta a continuación en la tabla 8.

Tabla 8. Resultados obtenidos del modelo CERT URBINA[20].

IP Origen	Puertos	Tipo de Incidente	Redistribución	Tiempo de Zona	Repetición
172.16.X.X	TCP 111	Escáner de Red	Si	GTM+ 1200	NO

Los problemas que se presenta en este modelo es que no contiene una gran fidelidad en la recopilación de datos, ya que en ciertos casos como un análisis forense el gran nivel de detalle en el evento que estos solicitan se pierde.

3.3.4 IDWG (Intrusion Detection Working Group).

IETF creó un grupo de trabajo llamado IDWG que contrarreste al complejo CISL, este tiene como objetivo "definir formatos y procedimientos de intercambio de información entre los diversos subsistemas del IDS", cuyos resultados se presentan a continuación:

- Elaboración de documentos que detalle los requerimientos funcionales de alto nivel en las comunicaciones que se dan en los sistemas de detección de intrusos y sus sistemas de gestión.
- Un mismo lenguaje de especificación que describa el formato de los datos.
- Un marco de trabajo en el cual se reconozca los mejores protocolos en los cuales se puede usar en la comunicación entre los IDS y que determine como se mapean en éstos los formatos de datos.

Arquitectura El principal interés de IDWG no es definir una arquitectura, si no definir un esquema de comunicación y mensajería. Igual que CIDF se distinguen 4 módulos no necesariamente separados de los cuales se verá a continuación.

- Analizador: Es el componente que se encarga de analizar los datos que ha recolectado el sensor.
- Sensor: Es el componente que se encarga de recolectar los datos para luego enviarlos al analizador.

- Fuente de datos: Es de donde se toma la información para detectar las actividades consideradas como sospechosas, en este componente se incluye varias herramientas de red como son logs de auditoría del S.O., logs de aplicaciones.
- Manager: Es el componente encargado de la administración de los demás componentes entre sus funciones se encuentran: Configuración de los sensores y los analizadores, administrar la notificación de eventos, consolidar los datos y generación de reportes.

Como se puede ver en la figura 6. se muestra la arquitectura IDWG con sus correspondientes componentes.

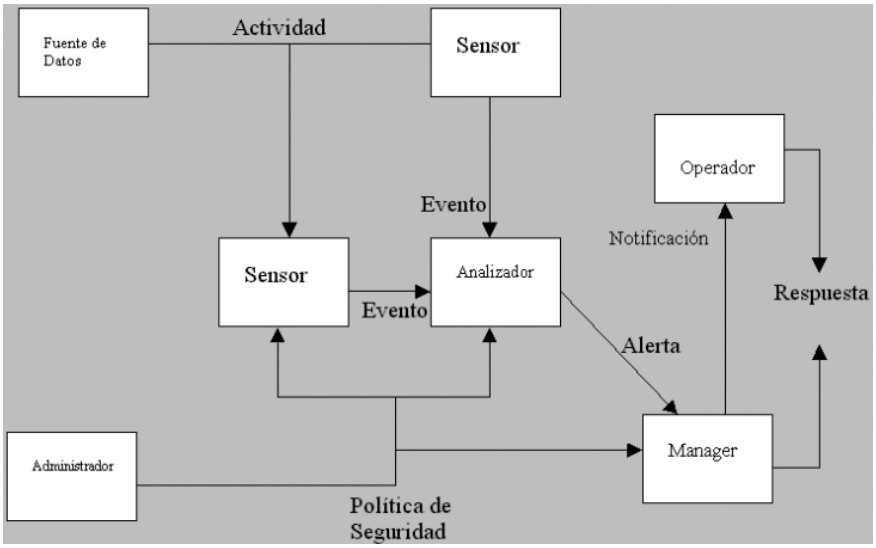


Figura 6. Arquitectura IDWG LÓPEZ[23].

3.4 Tipos de IDS.

El enfoque que se verá a continuación en la figura 7 fue presentado por Dorothy Denning en el articulo cuyo nombre es "An intrusion detection model" en el cual se proporciona una clasificación de los IDS.

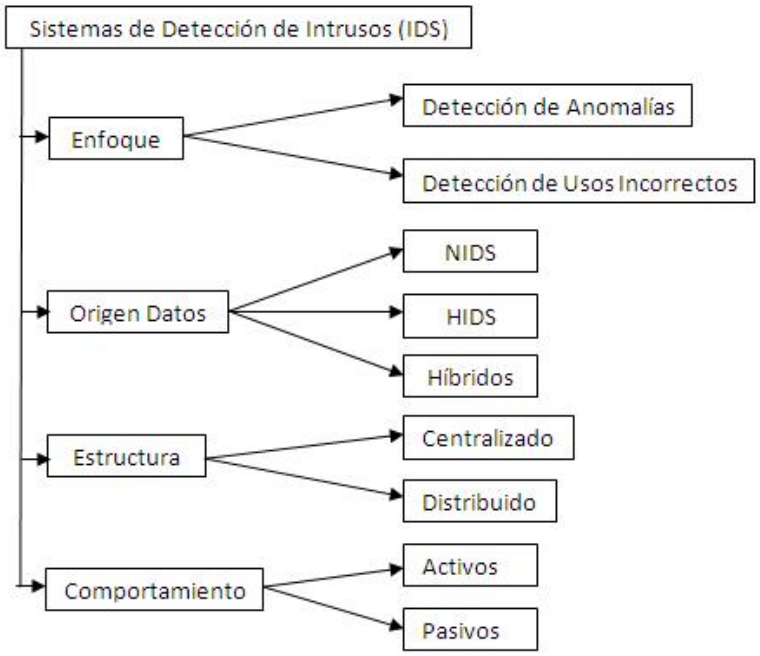


Figura 7. Clasificación de los IDS GARCÍA[25].

3.4.1 Por su enfoque tenemos.

Como se puede ver en la figura 8, se tiene dos enfoques de los cuales se explicara a continuación:

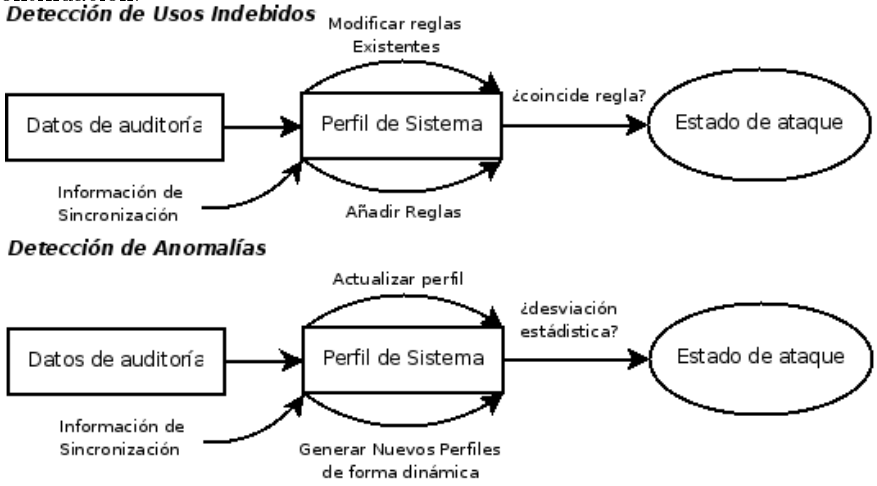


Figura 8. Modelo de Funcionamiento por su enfoque MUKHERJEE[26].

IDS de detección de usos incorrectos. O también conocido como modelo de Usos indedidos, en este tipo de sistemas, el IDS está configurado para detectar patrones, estos utilizan sistemas basados en firmas que ayudan a identificar ataques previamente conocidos tales como: paquetes malformados, escaneo de puertos, etc. Según Pfleeger y Pfleeper en GARUBA[28] describen a los IDS basados en firmas como un sistema que detecta una amenaza basada en una firma de un ataque que se ha dado a conocer por un patrón. Para entender de una manera precisa el funcionamiento de este, se explicara que es una firma, según CAMERON[17] se puede entender como firma a un modelo que se busca dentro de un paquete de datos, esta se emplea para la detección de uno o varios tipos de ataques. Las firmas pueden estar presentes en diferentes partes de un paquete de datos en función de la naturaleza del ataque, un ejemplo de esto se puede dar en la identificación de la firma de encabezado IP, en la cabecera de la capa de transporte (TCP o UDP) o en la cabecera de la capa de aplicación. Estas firmas pueden ser creadas cuando el tipo de ataque sea descubierto. Ya entendido que es una firma continuemos con las ventajas que se verán a continuación.

Entre las ventajas se puede mencionar las siguientes:

- Son efectivos sin generar tantas falsas alarmas.
- Da un diagnostico rápido ante un ataque especifico.

Desventajas de la detección de Abusos o Firmas:

- Deben de ser actualizados constantemente.
- No pueden hacer frente a los denominados ataques del día cero o no conocidos además que toma tiempo actualizar los parches y actualizar la base de firmas.
- No pueden hacer frente a los ataques modificados de un patrón ya conocido (variación de comportamiento).
- Necesitan ser administrados y supervisados constantemente por personal especialmente preparado para esta tarea, además de un proceso arduo de "finetunning" [13].
- El problema de que arroja "Falso Positivo" y "Falso Negativo" de los cuales se estudiara más adelante.

Detección de Anomalías. O también conocido como modelo Heurístico, en este se propone la creación de perfiles del sistema por un tiempo específico, permitiendo hacer un análisis de dicho perfil y el ver el porqué de la desviación o anomalía del mismo. Un tipo de desviación que se puede producir seria una

[13] Proceso para mejorar el rendimiento. Un control de calidad

enorme cantidad de conexiones TCP que se encuentren abiertas, paquetes ICMP que no sean validos tanto como el código fuente o las direcciones de destino. Para poder establecer un correcto funcionamiento del IDS por anomalías, este se debe someter a un proceso de entrenamiento, donde adquirirá conocimiento del normal desenvolvimiento del tráfico donde opera. Hay que tener en cuenta que durante esta etapa de entrenamiento toda la información sobre el flujo de datos se transformaran en metadatos, entre estos datos se encuentran las direcciones de red, los puertos que se utilizan, las banderas, los tamaños de los paquetes y los tiempos y como último paso a definir son los umbrales o limites de los valores recogidos en este proceso, claro cualquier cambio en el flujo de la red o adquirir un nuevo servicio provocaría una enorme cantidad de falsas alarmas.

Entre las ventajas se puede mencionar las siguientes:

- Puede detectar ataques de los cuales no tiene ningún conocimiento específico.
- La información que produce, puede ser utilizada para generar firmas en la detección de abusos.

Desventajas de la detección de anomalías:

- Genera un gran número de falsas alarmas.
- Requiere conjuntos de entrenamientos muy grandes.
- En las actividades de monitoreo, las medidas y técnicas incluyen los siguientes parámetros:
- Detección de una entrada sobre ciertos atributos del comportamiento de un usuario, de los cuales pueden ser el número de ficheros accedidos por el usuario sobre un tiempo especifico, el número de intentos fallidos para ingresar al sistema, el porcentaje de utilización del CPU por un proceso.
- Otras técnicas que se llegan a usar en los IDS actuales son las Redes neuronales y algoritmos genéticos como son SOM (Self Organized Maps) y LVQ (Learning Vector Quantization).

3.4.2 Por origen de Datos.

Host IDS (HIDS). Los primeros en su clase, funcionan de manera local al controlar el tráfico en la máquina mediante la utilización de los recursos de su anfitrión y nos permite analizar las acciones que tienen que ver contra nuestro servidores, PC o host, al analizar los procesos y usuarios que se involucran, para esto guardan información como logs, ficheros del sistema, entre otros. Como se puede ver, se basa en el proceso de análisis sobre un archivo y es perfectamente entendible que una vez compilado un archivo ya no necesite ser modificado si se

llega a ver un cambio en las característica del archivo como puede ser tamaño, fecha de creación y control de integridad se llega a determinar si ha ocurrido alguna acción irregular. Gracias al diseño del HIDS y las características que se han podido ver este permite monitorizar, detectar y responder a los datos generados por un usuario o un sistema en un host, una de las características propias de un HIDS es que estos son reactivos lo que quieres decir que sólo informa cuando algo ha sucedido. Entre estos Host IDS podemos ver algunos tipos que se enumerarán a continuación.

Filesystem monitoring:

- Aide (http://www.cs.tut.fi/~rammer/aide.html)
- Mtree.

Analizador de Logfile:

- Swatch (http://swatch.sourceforge.net/)
- Sec (http://www.linux-sec.net/Logger/)

Analizador de Conexión:

- Scanlogd (http://www.openwall.com/scanlogd/)
- PortSentry (http://sourceforge.net/projects/sentrytools/)

Kernel-based IDS (process monitoring etc.):

- IDSpbr
- LIDS (http://www.lids.org/)

Entre las ventajas se puede citar las siguientes:

- Detectan ataques que no pueden ser vistos por un NIDS los cuales se verán más adelante.
- Pueden operar en entornos con tráfico encriptado.
- Son potentes, registran comandos, ficheros abiertos, modificaciones importantes.
- Capacidad para operar en ambientes cifrados.

Entre las desventajas podemos mencionar las siguientes:

- Más difíciles de administrar que un NIDS.
- Puede ser deshabilitado si el ataque logra tener éxito (Penetración o DoS).
- Disminuyen el rendimiento del sistema monitorizado.
- Análisis limitado de tráfico, ya que solo analiza el segmento al que pertenece.

Herramientas de Host IDS

- Snort.- Disponible en Unix y Windows.www.snort.org
- Real Secure http://www.iss.net
- Serie Cisco 4200: (http://www.cisco.com/support/LA/public/nav/series_277026257.shtml).

Network IDS (NIDS). Más conocidos como sniffers de tráfico de red, cuyo funcionamiento se da de una manera autónoma, estos capturan paquetes de la red, para luego analizarlos en busca de patrones que supongan algún tipo de ataque. Estos reciben los datos de la red local, en donde están instalados y permiten la detección de ataques a un mayor nivel de abstracción al tener la información de múltiples host, no obstante solo analiza la información que pasa por la red siendo inútil ante los ataques entre host de un mismo segmento de red.

Cobertura de un NIDS. Está cobertura es pertinente a la capacidad para aplicar la seguridad a todas las facetas de la red. La cobertura de la red implica la protección y el seguimiento en contra de la amenazas ya sean internas como externas. En el caso de los NIDS basados en firmas, cuya característica es la identificación de los ataques que se encuentran en la base de datos, tiene una limitación en su capacidad de cubrir todos los ataques que salen de su cobertura. La razón de esto es porque la construcción de las firmas se orienta a los ataques externos como son virus o códigos maliciosos, en el caso de los ataques internos los usuarios que atacan a la red no generan ninguna firma detectable. Para poder combatir el problema de los ataques internos lo más aconsejable seria implementar un NIDS por anomalías o también llamada NID heurístico el cual tiene la capacidad de cubrir todos los aspectos de la red así como las amenazas ya sean estas externas como internas, esto es posible ya que su análisis se da en base de sus patrones de comportamiento anormal. Estableciendo así un perfil de usuario en el cual se espera que el mismo se mantenga dentro de estos lineamientos o actividades en un futuro, cualquier desviación de este perfil generaría una alerta para su detección. Claro que esta tarea puede ser un poco molestosa ya que se requiere tener una gran precisión en la creación del perfil de usuario, de lo cual tenemos que tener en cuenta todas las actividades que generan los programas que utiliza y actividades que llegaría a realizar el usuario para así lograr una correcta cobertura.

Entre las ventajas podemos mencionar las siguientes:

- No dan un impacto grande en la red.
- Pueden no solo funcionar a nivel de TCP/IP si no también a nivel de aplicación.
- No necesitan software adicional en los servidores.

Entre las desventajas podemos mencionar las siguientes:

- Presenta problemas en redes con tráfico elevado por características de Hadware.
- No hace un análisis de información Encriptada.
- No sabe a la final si el ataque tuvo éxito o no.
- Tiene problemas con los paquetes fragmentados.
- En el caso de los NIDS por firmas se da una limitante por la dependencia de la red, al proporcionar al usuario reglas definidas para poder detectar el código malicioso.
- En los NIDS heurísticos se da una limitación cuando el patrón de comportamiento de las intrusiones son similares a los patrones de comportamiento de un programa normal. Una limitación de los NIDS heurísticos se da cuando un usuario se sale del comportamiento normal sin ánimo malicioso, obligando una readaptación de los perfiles de usuario para el nuevo comportamiento y así evitar los falsos positivos, descubriendo la verdadera debilidad de los NIDS heurísticos que se llegarían a limitar por la información analizada en el momento.

Herramientas de NIDS.

- Firestorm.- Potente NIDS que incluye soporte para análisis, reportes y una consola para configuración remota disponible en http://sourceforge.net/projects/firestorm-ids/.

Hybrid IDS. Es la unión de los dos anteriores constituido por sensores en cada host que permite una detección local de los sistemas y un sensor en cada segmento de red. Para mayor información visitar http://www.prelude-ids.org

Red de Nodo Base IDS (NNIDS). Aunque este no consta dentro de la clasificación se lo verá como parte de ella. A diferencia de los basados en red, este se adjunta a la red de cables, es un nodo de red basado en sistema de detección de intrusos instalados en el sistema objetivo en sí, este no sólo analiza el tráfico de la red si no también el sistema operativo de cualquier acción realizada sobre este, estos denominados NNIDS son capaces de bloquear los paquetes de la red si llegarán a detectar un ataque. Entre sus ventajas tenemos que a diferencia de los NIDS que sólo pueden observar todo el segmento de red en el cual esta, los NNIDS pueden llegar a ver toda la red, siendo capaces de recoger información adicional. Entre sus desventajas según JOHO[18] estos tienen que ser instalados en un sistema de producción, cuyo impacto sobre el equipo llegaría a golpear sobre los recursos del mismo y por otro lado la mayoría de los usuarios preferirían no tocar estos equipos implementadoles un servicio adicional al que ya ofrecen.

3.4.3 Por su Infraestructura.

En esta área no se profundizara mucho ya que en las recomendaciones que se hace más adelante se detalla su funcionamiento.

Distribuidos (DIDS). Son aquellos donde se implementan varios IDS que se comunican entre sí o con un servidor central que permite centralizar y correlacionar todos los datos generados. Tener varios agentes por toda la red permite tener una amplia información para la detección en caso de un incidente en el sistema.

En general la arquitectura DIDS combina monitoreo y reducción de datos distribuidos con análisis centralizado de datos. Posteriormente se verá que un esquema totalmente centralizado ya no es aplicable en la actualidad por el creciente ancho de banda, obligando a usar un esquema distribuido con la consecuencia del aumento de los costes, pero la ventaja de los DIDS es que combina ambos esquemas logrando así una reducción en los costes en el esfuerzo por el mantenimiento de las políticas o asignaturas que utiliza el IDS para determinar un ataque. La implementación de la arquitectura DIDS se da por un sólo HIDS por cada host y un NIDS por cada segmento LAN en la red monitoreada, estos se encargan de recolectar evidencia sobre actividades sospechosas o no autorizadas, mientras que el DIDS director es el principal responsable de su evaluación. Los informes dados por los monitores son enviados de una manera independiente y asíncrona a través de la infraestructura de comunicaciones, estas comunicaciones es bidireccional, ya que el director puede pedir al monitor un informe más detallado. La arquitectura DIDS se muestra en la figura 9.

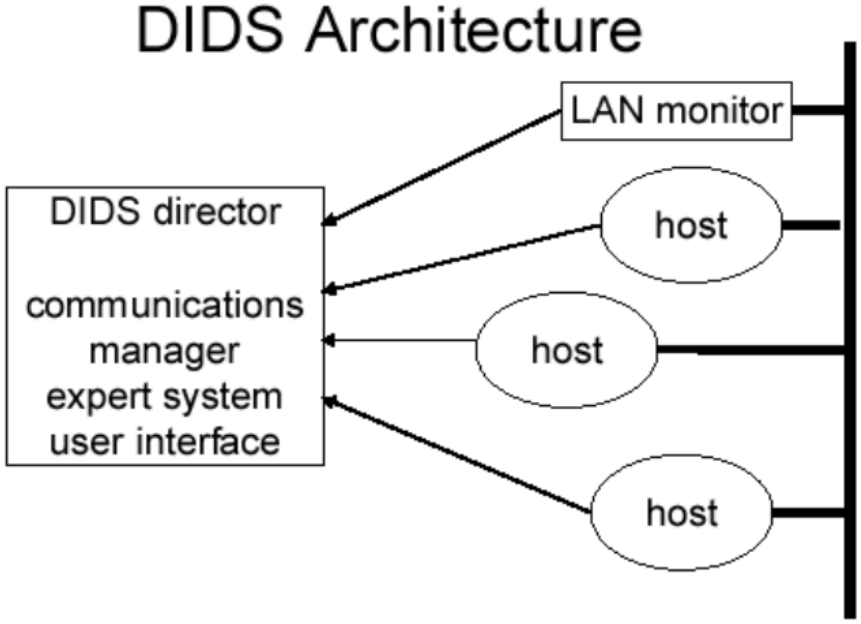


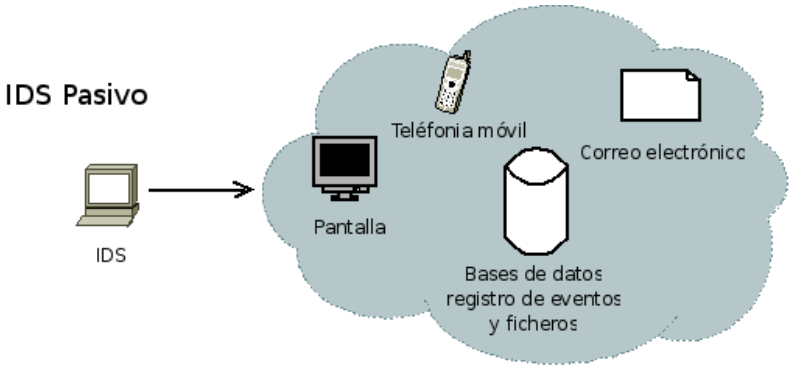
Figura 9. Arquitectura de DIDS LÓPEZ[23].

En la comunicación entre los monitores y el director se da mediante la norma ISO CMIP (Protocolo Común de Información de Gestión) permitiendo así la futura utilización de herramientas de gestión CMIP que sean útiles para el manejo del DIDS en varias áreas como el manejo de los incidentes, la gestión, detección y respuesta activa.

Centralizados. Estos IDS contienen sensores que trasmiten información a un servidor central del cual se maneja todo, como se menciono anteriormente estos en la actualidad ya no se usan, razón por la cuál no se profundizará en ellos.

3.4.4 En función de su comportamiento.

Se puede apreciar los pasivos que se muestra en la figura 10a y los activos figura 10b de los cuales se explicara a continuación:

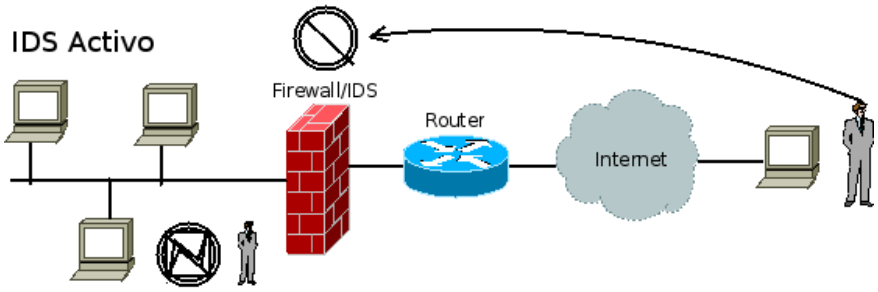


Pasiva.

Figura 10a. Modelo por su comportamiento (pasivo) MUKHERJEE[26].

En este caso el IDS avisa al administrador del sistema atacado usando alguna vía que se ha configurado como puede ser: alertas, correo electrónico, notificaciones SNMP (Simple Network Management Protocol) [14], mensajes en pantalla u otros. Estos solamente procesan la información en busca de algún intruso para que en caso de encontrar un intruso pasar el accionar al administrador dando por sentado que no hay unidades de repuesta (R-Boxes).

[14] Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.



Activa.

Figura 10b. Modelo por su comportamiento (Activo) MUKHERJEE[26].

Cuando se detecta un ataque este de forma automática toma una o algunas acciones modificando las Access Control Lists (ACLs) [15] del firewall corporativo. Aunque parezca interesante estos IDS su funcionamiento es muy simplista y en absoluto inteligente. Las repuestas que se pueden generar sobre el sistema atacante pueden ser las siguientes:

- Respaldo de paquetes como evidencia.
- Incremento de la monitorización de un evento.
- Corrección de vulnerabilidades.
- Ejecución de programas.
- Cierre de la conexión de usuarios.
- Configuración de los cortafuegos.

Acciones a tomar Dentro de este tipo de respuesta podemos distinguir 2 grupos:

- Recopilación de información adicional: Es la acción de incrementar la sensibilidad de sensor para obtener más pistas de los posibles ataques, un ejemplo de esto: Es en la captura de paquetes desde la fuente que se origino el ataque con un tiempo límite y un número máximo de paquetes.
- Reestructuración del entorno: Como otra opción dentro de las repuestas activas se puede anular o cerrar el ataque en una conexión TCP al insertar segmentos TCP RST[16] Tanto al atacante como a la unidad atacada o filtrar la dirección IP del atacante o el puerto atacado en el router de acceso o al firewall.

[15] Es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

[16] Es un bit que se encuentra en el campo del código en el protocolo TCP, y se utiliza para reiniciar la conexión. Un ejemplo práctico de utilización es el que realiza un servidor cuando le llega un paquete a un puerto no válido: este responde con el RST activado.

Desventajas Pueden ser peligrosos porque pueden bloquear el ingreso a recursos de los sistemas informáticos por falsos positivos o análisis erróneo de los datos de entrada.

Tiempo de Detección

- In-Line: Son aquellos sistemas que pueden llegar a detectar una intrusión en un tiempo muy corto casi inmediato, incluso dando la noción o apreciación de que se da la alerta en el mismo momento del ataque.
- Off-Line: En este tipo de detección las alertas se dan luego que el ataque se ha realizado, incluso no se llega a emitir una alerta al administrador, si no simplemente se guarda el ataque en un historial para que el administrador pueda revisar el ataque realizado.

4 Common Intrusion Detection Framework (CIDF).

Una de las arquitecturas más usadas y mejor desarrolladas en el proceso de construcción de un IDS es la arquitectura CIDF, por su diseño tan escalable como se muestra en la figura 11 a continuación.

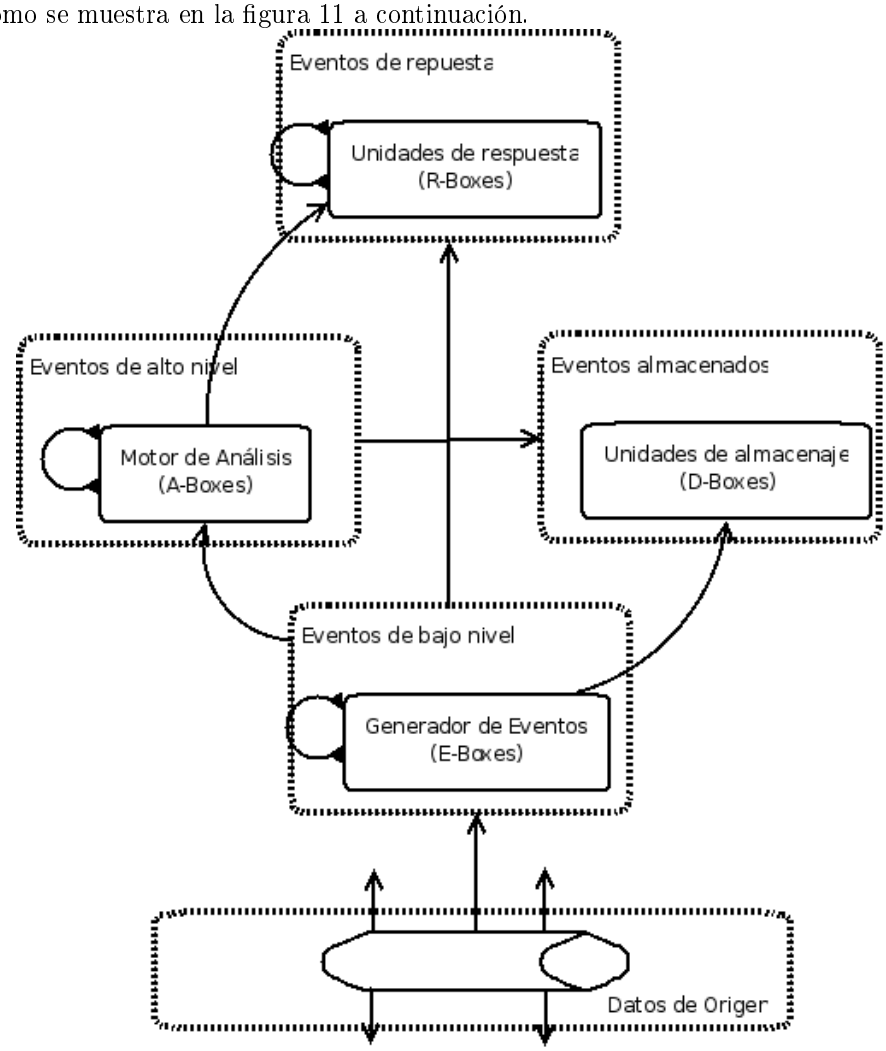


Figura 11. Diagrama de la arquitectura CIDF GARCÍA[25].

CIDF consiste en una serie de componentes (unidades lógicas) discretos que se comunican mediante el paso de mensajes, los cuales se pueden identificar en 4 grupos básicos.

- Generador de Eventos (E-Boxes).
- Motor de Datos o análisis (A-Boxes).
- Unidad de Almacenaje (D-Boxes).
- Unidad de Respuesta (R-Boxes).

Estos componentes pueden producir o consumir mensajes generados por otros componentes y ser implementados como un solo proceso o thread o como un conjunto de procesos distribuidos en varias máquinas o procesadores (Snornet o Didra).

4.1 Generadores de Eventos (E-boxes).

Su objetivo es la obtención de datos del exterior al IDS y sus entradas son los datos en bruto que recolectan y cuyas salidas serán ya los datos representados de una manera comprensible para el resto de componentes prácticamente en tiempo real, ej. Sniffer, Monitores o el algoritmo publico pcap conocido en Unix como libpcap disponible en http://www.tcpdump.org.

4.2 Motor de Análisis (A-boxes).

Es el núcleo del IDS que gracias a este y algunos conocimientos será capaz de discernir la importancia de ciertos eventos recibidos de los E-Boxes y genera nuevos elementos como salida. Entre estos podemos contar con ciertos tipos como pueden ser sistemas estadísticos de profiling, reconocedores de patrones, sistemas de correlación de eventos, etc. De los cuales se dará una breve descripción a continuación.

4.2.1 Redes Neuronales Artificiales.

Una de las características fundamentales de estos tipos de sistemas es que permite una gran cantidad de almacenamiento de patrones, las redes neuronales son sistemas distribuidos de computación con una alta tolerancia a fallos. Su funcionamiento está reflejado en el estudio del cortex humano, el cual es capas de diferenciar la desviación de un patrón aprendido. A pesar de ser un modelo muy plástico y potente, su mayor desventaja está reflejado en su elevando consumo computacional y el no poder determinar el por qué un IDS clasifica una acción como un ataque, provocando que no se pueda tener una acusación formal contra el atacante. Dentro de los modelos más utilizados en la actualidad según GARCÍA[25] son los llamados Spiking Neural Networks, que emplean parámetros biológicos como son la dimensión temporal y la predicción. Entre los Spiking Neural Networks están los Mapas Autosociados o perceptrón multicapa con backpropagation que trabajan con datos normalizados. Claro hasta el momento todo modelo de red neuronal tiene dos fases, ya sea su fase de aprendizaje que se realiza en modo "off-line" en otras palabras, tiene que dejar de funcionar para dedicarse solamente a aprender el nuevo patrón y la fase clasificativa en

modo "on-line" en donde hace uso del conocimiento aprendido para clasificar los patrones desconocidos.

4.2.2 Métodos Estadísticos.

El funcionamiento base de este modelo según VILLALÓN[22] se da cuando se establece un "perfil de normalidad" de acuerdo a las actividad que realiza el actor. Para luego almacenar las actividades actuales del actor en un nuevo perfil que se conoce como "current profile" con el cual se hace una comparación en busca de una desviación. A este proceso se lo conoce como "Pattern Matching".

4.3 Unidades de Almacenaje (D-boxes).

Es el encargado de almacenar la inferencia del motor de análisis, de él se extraerán los datos al momento de datamining y correlación de datos como fuentes de información forense, ej. loggers En el caso de datamining o también conocida como minería de datos se puede dar un tratamiento de la información permitiendo filtrar, transformar y organizar grandes volúmenes de información. Además de que permite reconocer nuevos patrones de ataque o ataques entre sí. Por su capacidad de reducir el análisis que se tiene que realizar en la consola facilita mucho el trabajo incluso puede llegar a detectar intrusiones que los IDS no pueden llegar a detectar como se llega a mencionar en GARCÍA[14].

4.4 Unidades de Repuesta (R-boxes).

Es el encargado de realizar una acción por todo el sistema, en caso de una intrusión, desplegar unidades que ejecuten contramedidas permitiendo al sistema que reaccione de una forma activa. Su accionar es prevenir ataques de fuentes maliciosas ya previamente identificadas o detener un ataque en proceso, si logra hacer esto el sistema pasa a denominarse Sistema de Prevención de Intrusos (IPS), ej. Alarmas, firewalls.

4.5 Capas y Servicios.

Los cuatro componentes vistos anteriormente (E-boxes, A-boxes, D-boex, R-boxes) se comunican mediante 3 capas como se muestra en la figura 12. que se verá a continuación.

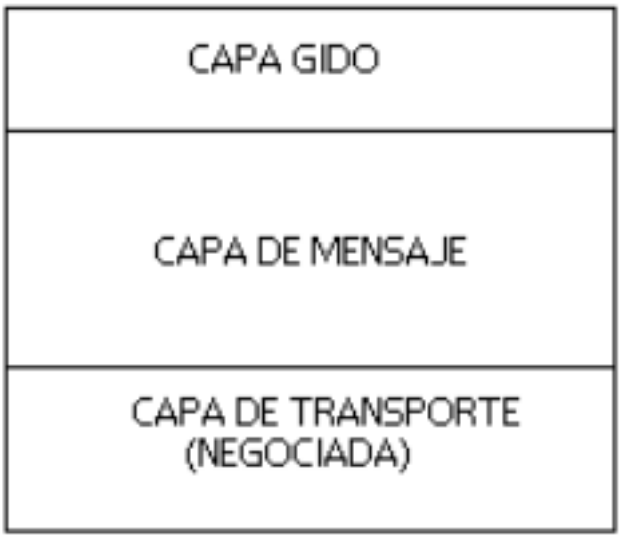


Figura 12. Capas de comunicación en CIDF LÓPEZ[23].

4.5.1 Capa de GIDOs (Generalized Intrusion Detection Objects).

Sin importar el protocolo de red o lenguaje de programación o cualquier otra variante, CIDF define formatos de datos comunes para la detección de intrusos, estos paquetes son los llamados GIDOs. Todo lo que se necesite desde la organización de datos, la semántica para un componente, la codificación en bytes, todo esto está en este nivel. Además éste permite separar los datos de acuerdo a su organización y lo que estos significan. Esta capa permite que los IDS operen de una manera significativa al poderse entender entre si la semántica que poseen los datos.

GIDO Addendum: Es usado por un componente CIDF para agregar información a un GIDO existente sin llegar a alterarlo, permitiendo así la autenticación de origen. "Cuando se aplica el GIDO addendum a un GIDO, se crea un nuevo GIDO reflejando los cambios especificados en el addendum. Si hay múltiples addendums, entonces el primer addendum es aplicado al GIDO para crear un GIDO modificado. El segundo es entonces aplicado al GIDO resultante para crear un nuevo GIDO modificado, y así sucesivamente."LÓPEZ[23] En la figura 13. se muestra los rasgos del encabezado de un GIDO formado con los lineamientos que propone CIDF.

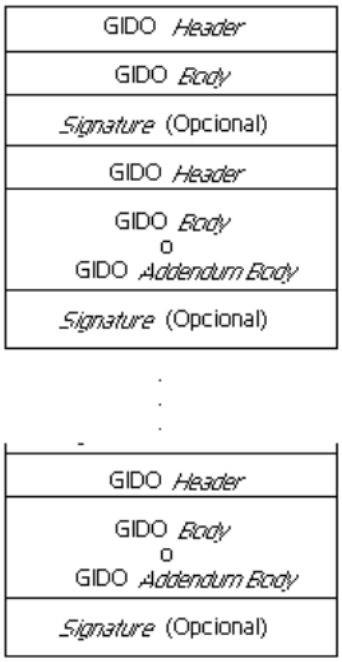


Figura 13. Estructura de un GIDO con sus correspondientes GIDO addendums LÓPEZ[23].

Entre los campos que se ubican en el encabezado de un Guido se tienen los siguientes:

- Versión ID (2 octetos).
- Class ID (2 octetos).
- Lenght (4 octetos, big-endian).
- Timestamp (4 octetos, big-endian).
- Thread ID (4 octetos).
- Originatos ID (16 octetos).
- Flags (1 octet).

El contenido del GIDO, plano o comprimido esta inmediatamente al encabezado. Si el valor del bit de signature es 1, significa que tiene una firma digital. Esta estructura tiene los siguientes campos:

- Algoritmos de la firma (2 octetos).
- Longitud de la firma (2 octetos).

- Longitud específica del algoritmo de firma (2 octetos).
- Parámetros específicos del algoritmo.
- Datos de la firma.

Claro que el tema es amplio y el objetivo de esta sección es dar una breve descripción del mismo, pero se puede profundizar sobre el tema en http://www.gidos.org

4.5.2 Capa de Mensajes.

Se dio porque las múltiples opciones de transporte presentaban deficiencias en este tipo de aplicaciones y esta capa proporciona la estabilidad deseada y además permite el envió de mensajes de encriptación, a través de un firewall o cualquier otro dispositivo. Esta se encarga de llevar un mensaje desde una fuente a su destino sin preocuparse de la semántica de dicho mensaje.

4.5.3 Capa de Transporte.

Esta capa existe debajo de la capa de mensajes ya que necesitamos que los componentes entiendan los mensajes, esto es independiente de la manera en que son transmitidos. Todos los componentes por defecto pueden soportar unos mecanismos de protocolo, haciendo de UDP [17] un protocolo confiable. "Esto es necesario solamente si los participantes en una comunicación no han acordado previamente un mecanismo de transporte usando medios externos (por Ej., configuraciones locales o mediante el servicio de directorio de CIDF)."LÓPEZ[23]. A continuación en la figura 14 se puede ver un esquema de la interoperación entre componentes.

[17] User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

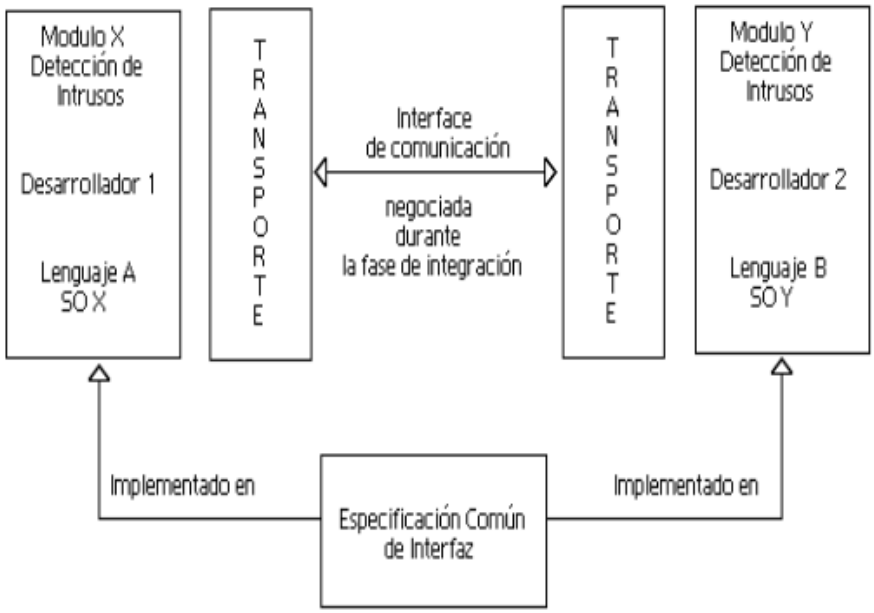


Figura 14. Interoperación entre componentes LÓPEZ[23].

4.6 CISL(Common Intrusion Specification Language).

El lenguaje de Especificación de Intrusiones Común es utilizado para unir los cuatro tipos de componentes de CIDF, su leguaje es bastante complicado parecido al del LISP [18] Razón por la cual no llegó a participar en la comunidad de seguridad, se encarga básicamente de transmitir el siguiente tipo de información.

- Información de eventos en bruto: Permite que se comuniquen el generador de eventos con el motor de datos y se la clasifica como Auditoria de registros y tráfico.
- Resultados de los análisis: Permite que se comuniquen el motor de datos con la unidad de almacenaje y este con las descripciones de las anomalías y ataques del sistema.
- Prescripciones de repuestas: Permite que se comunique el motor de datos con la unidad de repuesta y esta se encarga de detener ciertas actividades o "modificar parámetros de seguridad de componentes"URBINA[20]

[18](LISt Processing) Procesamiento de listas. Lenguaje de programación de alto nivel utilizado en programación no numérica. Desarrollado en 1960 por John McCarthy, su sintaxis y estructura es muy diferente de los lenguajes de programación tradicionales. Por ejemplo, en LISP no hay diferencia sintáctica entre datos e instrucciones.

4.6.1 Requerimientos del leguaje.

Impacto en la arquitectura CIDF (Generalized Intrusion Detection Objects). Ya que los componentes manejan entradas y salidas, estas entradas y salidas pueden llegar a servir a otro componente, en donde la variada información que está siendo intercambiada, puede servir de proceso para expresar todos estos tipos de información. Hay que tener en cuenta que los registros de eventos solo representan eventos hechos por un componente sobre un sistema lo cual puede involucrar una carga de computación ordinaria o de rutinas de mantenimiento de los cuales pueden ser producidos en gran volumen.

Lista de Metas del Lenguaje. Hay que contar con características propias para el intercambio de información de los ataques como son:

- Expresivo: Donde los componentes deben estar en la capacidad de expresar un amplio rango de intrusiones y malos usos, fenómenos relacionados y prescripciones. Razón por la cual el lenguaje debe tener un amplio vocabulario y perfeccionada sintaxis a tal nivel que pueda cubrir un amplio rango de expresiones.

- Único en Expresión: Que las mismas sentencias no se pueda expresar de varias maneras. Aunque no hay lenguaje expresivo donde se admita una formulación por cada sentencia, el lenguaje debe permitir que un emisor con un receptor puedan ponerse de acuerdo sobre los objetos de interés, pero no sobre la forma que ellos expresan información acerca de estos objetos.

- Preciso: Que la expresión en un leguaje debe estar bien definido, en otras palabras dos receptores del mismo mensaje no pueden contener conclusiones contrarias.

- Por Capas: Aquí se debería poner en un sentido general los mismos casos específicos, así que los diferentes receptores con diferentes requerimientos puedan juzgar tanto como ellos necesiten de un mensaje. Para esto el lenguaje debería estar en la capacidad de tener mecanismos en los cuales los conceptos específicos son definidos en términos de lo más general. Es decir que lo que el lenguaje expresa lo hace mediante la forma más general.

- Autodefinido: Los usuarios que reciben un reporte deberían de estar en la capacidad de interpretar los mensajes en el nivel que se lleguen a necesitar, sin recurrir a una negociación externa.

- Eficiente: Los mensajes deberían consumir la menor cantidad de recursos posibles.

- Extensible: Si un grupo de usuarios o productores llegan a decidir sobre información adicional, deberían ser capaces de expresarla. Donde se tendría que contar con un mecanismo donde el productor pueda usar su

propio vocabulario, y notificar este hecho a los receptores, de tal manera que estos puedan recuperar el significado del nuevo vocabulario, o decidir cómo entender el resto del mensaje donde se dio lugar.

- Simple: Los productores deberían de estar en la capacidad de codificar la información de una manera rápida y los consumidores deberían de estar en la capacidad de extraer la información de una manera rápida sin procesos excesivos. Estos componentes deberían estar en la capacidad de enviar y recibir mensajes simples, sin la necesidad de entender al lenguaje como un todo, simplemente llenando los espacios vacíos o extrayendo de ellos la información solicitada.

- Portable: El lenguaje debería ser multiplataforma con gran soporte en mecanismos de transporte y soportar significados que no deberían limitarse a la información que se intercambia. En el lenguaje la codificación de este no tiene que depender del orden del host sobre el cual el mensaje este codificado, o sobre los detalles de su red.

- Fácil de implementar: Que el lenguaje sea lo más sencillo posible para su implementación. Aunque el establecimiento de este requerimiento es el más difícil de establecer, esta se llega a asegurar en la etapa de pruebas.

S-Expresiones. S-expresiones son grupos recursivos de marcadores (tags) y datos, que da la ventaja de proveer una asociación explicita entre términos sin la desventaja de limitar lo que expresan esos términos y sus grupos. "Para llevar a cabo la auto-definición, se añade a la S-expresión un tag inicial, que proporciona alguna clave semántica a la interpretación del resto de la S-expresión. Por esta razón, estos tags serán llamados identificadores semánticos (SIDs)" LÓPEZ[23].

Ejemplo de SIDs y la S-Expresiones.
(And
(OpenapplicationSession
(When
(Time 14:57:36 24 Feb 1998)
)
(Initiator
(HostName ´isis.edu.co´)
)
(Account
(UserName ´jonny´)
(RealName ´Jonny Dumb´)
(HostName ´tetris.com´)
(ReferAs 0x12345678)
)
(Receiver
(StandardTCPPort 223)
)

)
(Delete
(World Unix)
(When
(Time 14:58:12 24 Feb 1998)
)
(Initiator
(ReferTo 0x12345678)
)
(FileSource
(HostName ´tetris.com´)
(FullFileName ´/etc/passwd´)
)
)
)

Lo que dice este mensaje, es que se ha iniciado una sesión por parte de un usuario cuyo nombre real es Jonny Dumb usando un alias Jonny en el host tetris.com desde un host isis. Después de 1 minutos se ve dentro del tráfico de red una cadena sospechosa como lo es "/etc/passwd" y se indica que se está borrando un archivo. Lo que demuestra este ejemplo es que mediante un SID se puede tener datos simples como argumentos y que en otros SIDs se puede tener una s-exp como argumento.

5 Funcionamiento de un IDS.

5.1 Ubicación de un IDS en la red.

Hay que tener en cuenta en donde se deberá colocar el IDS. En la figura 15, se da una pauta de los posibles lugares en el cual debería ubicarse según URBINA[20] y WALC[27].

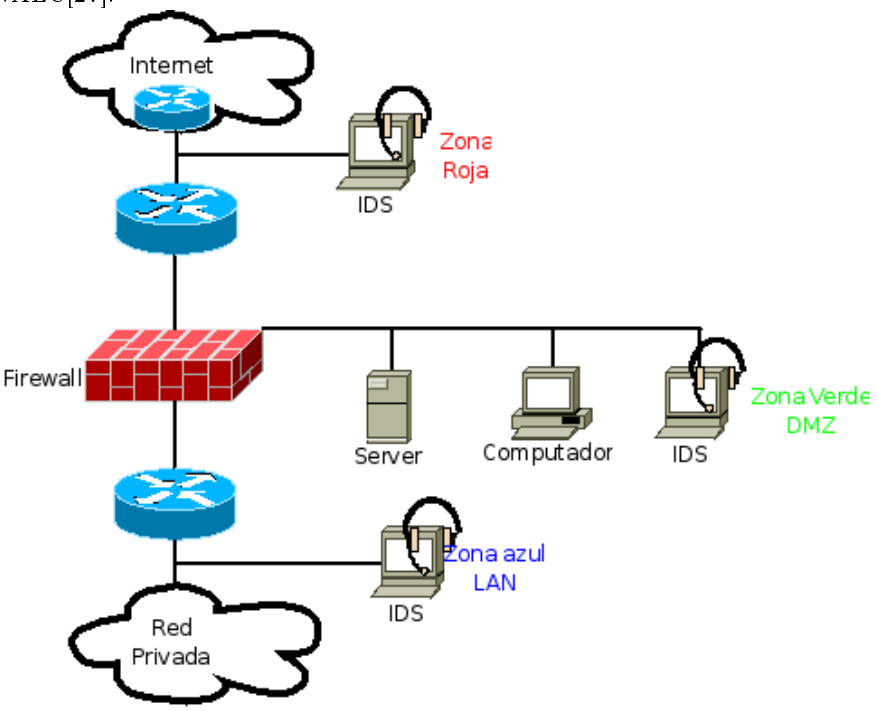


Figura 15. Localización de un IDS dentro de una organización WALC[27].

A continuación se verá los criterios que debemos tomar en cuenta para la configuración de los IDS en las diferentes áreas de la red la cual se a representado en 3 colores.

- Zona roja: La sensibilidad del IDS debe ser baja por la cantidad de falsos positivos por la razón de que este verá todo el tráfico que entre o salga de la red.
- Zona verde: Debe ser un poco más sensible a la roja, ya que es esta zona los firewall deberán de estar en la capacidad de filtrar cualquier intrusión,

en esta zona se da una tasa baja de falsas alarmas con respecto a la zona roja, debido que solo se debe permitir acceso a los servidores.

- Zona azul: Es la zona donde los IDS tendrán una sensibilidad más alta a todas las otras zonas, denominada también zona de confianza, aquí cualquier irregularidad se la tiene que tomar como una acción hostil, también se tiene que dar el más bajo número de falsas alarmas, de las cuales se tiene que estudiar inmediatamente. Hay que tener en cuenta que la zona azul no es parte de la red interna, "Todo lo que llegue al IDS de la zona azul ira hacia el firewall (por ejemplo, si utilizamos un Proxy-cache [19]. Para nuestros usuarios de web) o hacia el exterior. El IDS no escuchará ningún tipo de tráfico interno dentro de nuestra red. "En el caso de tener un IDS escuchando tráfico interno (por ejemplo, colocando entre una VLAN y su router), las falsas alarmas vendrán provocadas en su mayor parte por máquinas internas al acceder a los servidores de la red, por servidores nuestros (DNS sobre todo) y escaneadores de red, por lo que habrá que configurar el IDS para que no sea muy sensible." URBINA[20]

Como menciona GARCÍA[14] se da unas pautas del porque debería ubicarse los NIDS en estas secciones de la red. Como se puede apreciar, la ubicación está orientada al diseño de la red y no a la capacidad de tráfico de la red, ya que este puede llegar a ser un factor no estable, ya sea por el desarrollo tecnológico del hadware o por la infraestructura física de la red.

- Computadoras conectadas a la red: Es el conjunto de computadoras que se encuentran en la red ya sean de la misma organización o computadoras personales.
- Zona desmilitarizada: Son los equipos que se encuentran en las redes externas, la configuración de los NIDS debe ser mucho más detallada y ampliamente estudiada.
- Servidores: Esta es una variante que permite proteger cada servidor individualmente.

Ante el problema de la ubicación de los NIDS en la red se puede aplicar los denominados métodos de replicación de datos que servirán para proteger determinadas zonas de las redes conmutadas y se revisara más adelante.

5.2 Requisitos de un IDS.

Para que un IDS sea considerado una herramienta de seguridad aceptable tiene que cumplir con algunos requisitos que se verán a continuación:

[19] Es un servidor especializado en guardar todos los objetos que se solicita desde interner, para luego hacer referencia a este en una nueva petición, logrando reducir así el ancho de banda.

- Ejecución autónoma continua: El IDS debe de estar en la capacidad de ejecutarse continuamente sin la necesidad de que alguien esté obligado de supervisarlo, esto implica que el funcionamiento habitual no tiene que tener ninguna interacción humana, excluyendo la que el administrador tendría con el IDS al darse una alerta ante un ataque.

- No introducir cambios en el comportamiento habitual del sistema que protege: Este punto está comprometido con el grado de aceptación del IDS, en el cual se trata que los mecanismos de detección sean aceptables para los usuarios que se encuentran dentro del entorno a proteger, hay que tener en cuenta que estos mecanismos no deben de introducir una sobrecarga en el sistema, ni generar una gran cantidad de falsos positivos o de logs.

- Adaptación a cambios en el entorno de trabajo: Su adaptación se debe a los cambios en el entorno de trabajo, ya que no hay sistema informático que se pueda mantener de una manera estática, todo cambia con una periodicidad más o menos elevada, si estos mecanismos no son capaces de adaptarse rápidamente a esos cambios, lo más seguro es que no lleguen a permanecer.

- Tolerancia a fallos: Todo sistema debe de tener cierto grado de tolerancia ante los fallos dados por las situaciones inesperadas. Estos cambios que se presentan dentro del entorno informático no son graduales, si no instantáneos, razón por la cual los IDS deben de ser capaz de responder siempre adecuadamente ante los mismos.

5.3 Ciclo de Vida de un IDS.

Como se puede ver en ICSALABS[31] se tiene un gran vacío en el momento de adquirir un equipo de IDS ya que se desconoce las marcas, los resultados entre otros datos que pueden llegar a ser importantes en el momento de decidirse por una u otro solución. En el caso de la certificación que proporciona la empresa ICSA[20] esta nos da una pauta a ciertas medidas como puede ser:

- Vulnerability-focused attack testing,

- Evasion testing.

- Denial-of-service testing.

- Network performance/latency testing.

- Administrative function testing.

[20] ICSA Labs, antes conocida como la International Computer Security Association, gestiona y patrocina los consorcios de seguridad que proporcionan un foro para el intercambio de inteligencia entre los principales vendedores de productos de seguridad. Además, ICSA Labs publica encuestas, estudios de seguridad de la industria y los compradores de guías para los productos de seguridad. www.icsalabs.com

En los cuales ya tiene casos desarrollados frente a los cuales se realiza pruebas, además que se da una certificación no solamente a los IDS si no a un conjunto de tecnologías que están relacionados a la seguridad como podemos mencionar antivirus, firewall, IPsec, VPN y SSL-VPN. Para mayor información consultar www.icsalabs.com

5.4 Criterios de Evaluación de un IDS.

Según CÓRDOBA[19] hay tres criterios para evaluar este tipo de sistema, cuyos conceptos se verá a continuación.

- Precisión: Efectividad de la detección y ausencia de falsas alarmas.
- Rendimiento: Taza de eventos procesados por unidad de tiempo.
- Completitud: Capacidad del IDS para detectar la mayor cantidad de ataques posibles.

Aparte de estos tres criterios se dan unos indicadores estadísticos, que permita cuantificar la bondad del IDS tal como se puede ver en la figura 16.

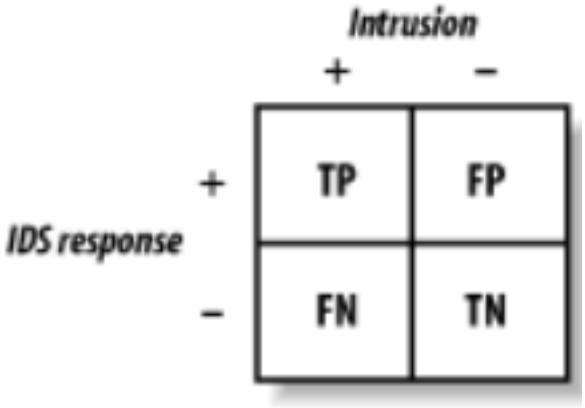


Figura 16. Cuantificación Estadística de los IDS CÓRDOBA[19].

A continuación se revisara brevemente los conceptos que tienen que ver con estos valores cuantitativos.

- Verdaderos positivos (TP): Cuando la intrusión se realiza y es correctamente detectada.
- Falsos positivos (FP): Cuando la intrusión no se realiza y aparece como correctamente detectada.
- Falsos negativos (FN): Cuando la intrusión se realiza y no es detectada.

- Verdaderos negativos (TN): Cuando la intrusión no se realiza y no es detectada.

Ya una vez conocidos los anteriores conceptos podemos definir los indicadores que se muestran a continuación.

- Sensibilidad: Mide la efectividad de las detecciones cuando existe alguna intrusión. S=(#TP/(#TP+#FN)).
- Especificidad: Mide la efectividad de las detecciones cuando no existe intrusión. E=(#TN/(#TN+#FP)).
- Precisión: Mide la efectividad de las detecciones cuando existe o no existe intrusión. P=(#TP+#TN)/(#TP+#TN+#FP+#FN).

Con estos criterios ya se puede contar con una medida que ayude a determinar el estado del IDS dentro de la organización y así poder establecer metas que ayuden al mejoramiento de la calidad del servicio.

5.5 Análisis entre diferentes tecnologías de seguridad.

5.5.1 Sistemas de Prevención de Intrusiones.

Como se puede ver los IPS o Intrusion Prevention Systems son sistemas que servirán para el control de acceso a los recursos del sistema, según GARCÍA[25] estos están catalogados dentro de los IDS activos, por la capacidad que tienen de reaccionar ante un ataque de manera inmediata, rechazando los paquetes de la red. Al tener esta ventaja de que el sistema llegue a reacciona de manera automática, obliga al administrador a que sea mucho más estricto en las configuraciones de un sistema de este tipo, si las configuraciones no llegaran a estar correctas, se tendría el riesgo de que llegaría a rechazar paquetes válidos y a bloquear usuarios normales que en realidad no han ejecutado ninguna acción delictiva contra el sistema o los recursos que contiene. Entre los IPS se puede mencionar dos tipos del mismo que han llegado hasta la actualidad de los cuales se verá a continuación.

- IPS de primera generación: Este tiene la capacidad que al detectar un ataque que proviene de una dirección IP especifica, el IPS procedía a descartar todos los paquetes que precedían de esta dirección IP, aunque el resto de paquetes tengan que ver o no con el ataque.
- IPS de segunda generación: En esta generación se dio una mejor adaptación sobre la toma de decisión frente al ataque, en este caso el IPS solo bloquea los paquetes que considera que son parte de un ataque sin bloquear el resto de paquetes que proceden de la dirección IP de la cual se origino el ataque.

5.5.2 Firewall vs IPS.

Como se puede ver el comportamiento de los IPS es semejante a un firewall pero la diferencia radica en que le firewall toma su decisión en base a los encabezados del paquete entrante solamente en especial de las capas de red y transporte. Pero el IPS no solo se basa en el encabezado del paquete entrante si no también en el contenido de los datos del paquete "payload" lo cual lo convierte en una herramienta aun más efectiva que un firewall.

5.5.3 IDS vs IPS.

Uno de las diferencias más importantes radica en la respuesta que cada uno tiene frente a un ataque. El comportamiento que tiene el IDS frente a una amenaza se limita a detectar y notificar la intrusión al personal que está encargado de recibir y responder ante estas alertas generadas por el IDS. Mientras que el IPS al momento de detectar una intrusión su manera de reaccionar ante esta no es la generación de una alarma, aunque se lo podría configurar para que realice esa acción, si no que el busca la manera de contrarrestar el ataque. Como una segunda característica podemos ver que el tiempo de respuesta es también diferente, en el caso del IDS este responde de una manera mucho más rápido que un IPS, claro hay que tomar en cuenta que esto se debe a que el IDS se limita a generar una alerta, mientras que el IPS busca la manera de detener el ataque, razón por la cual su tiempo de repuesta es más alto con relación a un IDS. Por otra parte hay que tener en cuenta que el IPS tiene una gran desventaja frente a un falso positivo, este puede llegar a la negación de los servicios de los clientes hasta el total aislamiento de la máquina.

5.5.4 Respuestas Activas vs IPS.

Los IPS (Instrusion Prevention System) han llegado a popularizarse como una necesidad para robustecer las herramientas de seguridad, el objetivo de este dispositivo es anular los ataques que se realizan contra los elementos que protege. Su función se da más en los dispositivos inline como puede ser los swith o los router por la razón que estos dispositivos tienen la capacidad de descartar o modificar los paquetes individuales en el momentos que atraviesan las interfaces. Como anteriormente se vio la respuesta activa se aplica a cualquier función que altera o bloquea el tráfico de una red como resultado de la ocurrencia de la detección de una intrusión que a diferencia de los IPS no necesitan ser implementado por un dispositivo inline. Al entender que la diferencia entre las respuestas activas y los IPS radica en los dispositivos inline, se puede decir que las repuestas activas tienen la ventaja para reaccionar ante un ataque con mecanismos de repuesta que no están en línea antes de que dicho ataque alcance su objetivo y por el contrario en el caso de los IPS si el flujo de ataque no está en línea con algún dispositivo de este, no podrá detenerlo. El IDS al poder responder con métodos que no están basados en dispositivos inline crearán una carrera entre el tráfico del atacante y la respuesta el cual puede llegar a tener éxito dependiendo de la cantidad de paquetes necesarios para realizar el ataque.

5.6 Análisis de la rentabilidad de un IDS.

El primer paso para establecer que tan conveniente es incorporar un IDS, es el de analizar los ataques y los riesgos donde se lo implementará, determinando así el ahorro financiero que se tendrá. Hay que tener en cuenta que la implementación de un IDS en la organización exigirá personal calificado, además de unos equipos adecuados que puedan soportar esta clase de trabajo. Los directivos se tendrán que preguntar qué tan grande es la organización para saber si en realidad la implementación de un IDS en la organización podría ser justificable, como lo señala CHUVAKIN[32], en un artículo han llegado a opinar que en la implementación de un IDS en una empresa pequeña sería una adquisición Costosa. En CAPPELLI[33] Iheagwara, Blyth y Singhal opinan que la rentabilidad de un IDS es determinante sobre cualquier pérdida estimada que se pueda dar por causa de las intrusiones. Aunque se ha estado tratando de la adquisición de un IDS este en realidad es difícil determinar cuánto llegaría a costar, sin embargo McHugh, J. en un publicado MCHUGH[30] ha llegado a determinar una estimación del coste de este: en el costo inicial se determina un costo de $10000; por costo de mantenimiento está incluido en el 15% del costo inicial por año, y costo de personal se define por la organización basada en el nivel de seguimiento que se requiere, ya sea esta continua o periódica, claro el costo puede variar de acuerdo de cuanto se le quiera pagar al personal, este valor sería sólo una aproximación de acuerdo a lo que ha determinado McHugh, J. Ya con esta estimación se puede llegar a determinar si en realidad es conveniente la implementación del IDS en la organización al enfrentar con los costes que pueden causar los posibles riesgos, entre ellos ataques externos (Virus y otros códigos maliciosos) o ataques internos, como es el robo de información clasificada la cual llegaría ser la más costosa de acuerdo a su naturaleza y así poder determinar si hay un verdadero ahorro para la organización.

6 Correlación de eventos.

Se entiende por correlación de eventos a la capacidad de agrupar eventos provenientes de varias fuentes, con el objetivo de facilitar el análisis, especificando lo más detalladamente posible los mismos. La correlación de datos según NING[38] surge de la necesidad de identificar las acciones anómalas, al darse una monitorización sobre los canales de comunicación. Este proceso se puede apreciar en la figura 17. que se encuentra a continuación.

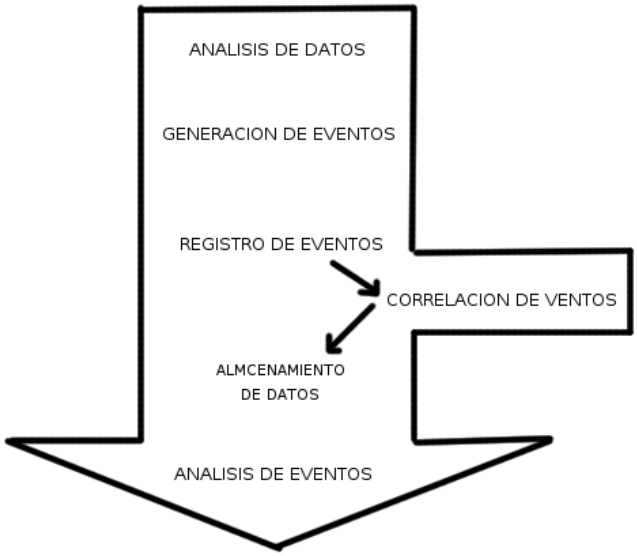


Figura 17. Proceso de Monitorización de eventos de seguridad NING[38].

El proceso se da en el momento del registro de eventos de datos en los sistemas de IDS. Entre el evento generado y su almacenamiento, se compara el evento con los datos que el sistema conoce y pueda llegar a ser relacionado.

De acuerdo a los tipos de datos se distinguen varios tipos de correlación, los cuales se verá más adelante. Para lograr el objetivo de agrupar eventos con el fin de reducir la cantidad de falsas alarmas se han dado dos corrientes, el cual según GALVÁN[37] en la primera corriente el objetivo ya no es el de proteger un servidor que pueda ser atacado, si no impedir que un servidor que ha sido atacado no sea utilizado para realizar otros ataques a esta corriente se la ha denominado como "Outbound Intrusion Detection" y cuya ventaja ha resultado en ser un modelo más colaborativo de seguridad. En la segunda corriente se da

un estudio de los ID[21] a nivel de host el cual está orientado a funcionar como un multiclasificador con el objetivo de reducir la cantidad de las falsas alarmas. La función del clasificador es la de extraer el modelo del comportamiento de los usuarios y así poder determinar los comportamientos normales y anormales, según GALVÁN[37] para los clasificadores se ha usado la fusión "Oracle" para obtener una decisión única sobre la actividad en llamadas al sistema, entre sus ventajas se encuentran el bajo nivel de utilización de los recursos del CPU, memoria, etc. En relación con el tipo de datos que se utilice para el análisis del evento se pueden mencionar los siguientes que se presentán en NING[38]:

- Correlación entre varios puntos de la infraestructura.- En este tipo se permite hacer un seguimiento de los puntos exactos en los que se ha detectado el comportamiento anómalo que genera el evento, evitando así la duplicación de eventos.
- Correlación con otros eventos relacionados.- Son eventos que por sí solos no tienen un significado importante, pero junto a otros eventos llegan a ser un ataque especifico.
- Correlación con otros datos conocidos del sistema objetivo.- El evento que se desarrolla se compara con información de vulnerabilidades registradas por el sistema o sistemas objetivos, ajustándose el nivel crítico del mismo de acuerdo a si el ataque llega a tener éxito o no.

Para un mayor entendimiento de como funciona una correlación de eventos referirse al anexo 4.1

6.1 Ejemplo 1.

El siguiente ejemplo está basado en la figura 18 que esta propuesto en NING[38]. La ilustración consta de una red con un servidor, un HIDS, un NIDS y un equipo de análisis de vulnerabilidades del servidor de los cuales todos reportan a una base de datos centralizada que se encarga de almacenar los eventos de seguridad.

[21] Detección de intrusos (Intrusion Detection)

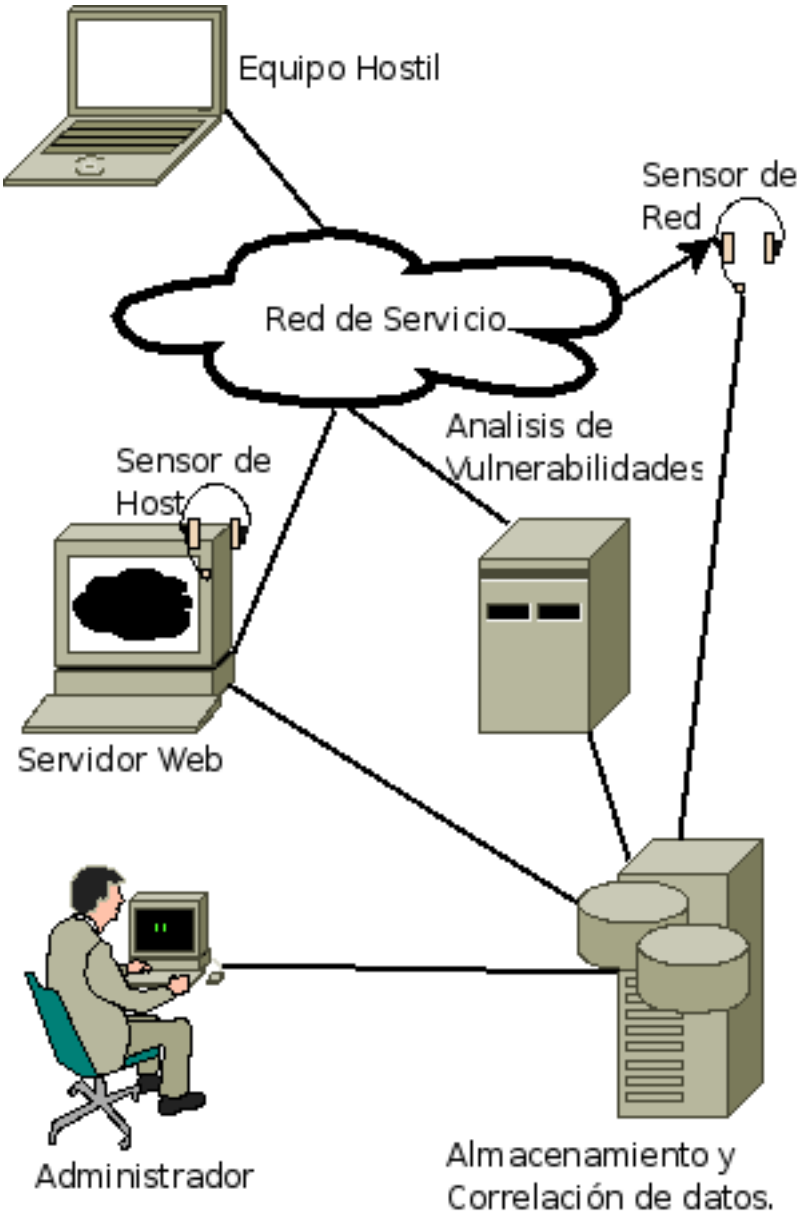


Figura 18. Arquitectura ejemplo NING[38].

El atacante está en la misma red, el cuál lanza un ataque de escaneo de puertos sobre el servidor web. El ataque es detectado tanto por el HIDS como por el NIDS dando lugar a la correlación de datos que se detallarán a continuación.

- Correlación entre varios puntos de la arquitectura: Se da para prever que

los eventos aparezcan por duplicado, siendo identificados como el mismo evento generado por los diferentes IDS en la base de datos.

- Correlación con otros eventos relacionados: Se da para evitar identificar todos los eventos de conexión a cada puerto como eventos aislados, se agrupan todos los intentos de conexión dentro de un mismo evento. Correlación con otros datos conocidos: Cualquier intento de conexión a otro servicio que no sea Web se lo marcará con un nivel de cuidado inferior ya que el servidor no proporciona dicho servicio.

6.2 Ejemplo 2.

El siguiente ejemplo esta propuesto por CUPPENS[40] como se puede ver, el lenguaje usado para representar los ataques está basado en LAMBDA que es un lenguaje no estandar, pero que ayudará entender la manera en que funciona una correlación de datos, del cual se revisara a mayor detalle en el anexo 4.1 en el cual consta de 4 ejemplos de ataques en LAMBDA: NFS mount, Modificación del archivo .rhost, TCPScan y Winnuke como se puede ver en la figura 19, para determinar una regla de correlación como se muestra en la figura 20.

```
<?xml version="1.0" encoding="UTF-8"?>
<attack attackid="MIR-0163">
<name>mount partition</name>
<pre>access_level(Source_user,Target_address,remote),
        mounted_partition(Target_address,Partition),
</pre>
<post>can_access(Source_user,Partition)
</post>
<scenario>Action</scenario>
<cond_scenario>
 script(Action,'mount -t nfs $Partition:$Target_address $Partition')
</cond_scenario>
<detection>Alert</detection>
<cond_detection>alert(Alert),
                source(Alert,Source),
                source_user(Source,Source_user),
                target(Alert,Target),
                target_node(Target,Target_node),
                address(Node,Target_address),
                classification(Alert,"MIR-0163")
</cond_detection>
</attack>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<attack attackid="MIR-0164">
<name>modification du .rhost</name>
<pre>access_level(Source_user,Target_address,remote),
      can_access(Source_user,Partition),
      owner(Partition,Target_User),
      userid(Target_user,Target_address,Userid),
</pre>
<post> access_level(Source_user,Target_address,user)
</post>
<scenario>Action</scenario>
<cond_scenario>script(Action,'cat "++" > .rhost')</cond_scenario>
<detection>Alert</detection>
<cond_detection>alert(Alert),
                source(Alert,Source),
                source_user(Source,Source_user),
                target(Alert,Target),
                target_node(Target,Target_node),
                address(Target_node,Target_address),
                classification(Alert,"MIR-0164")
</cond_detection>
</attack>
```

Lambda attack MIR-0163-NFSMount y Lambda attack MIR-0163-Modification of -rhost Lambda attack MIR-0036-Winnuke y Lambda attack MIR-0074-TCPScan

```
<?xml version="1.0" encoding="UTF-8"?>
<attack attackid="MIR-0036">
<name>winnuke sur la cible</name>
<pre>use_os(Target_address,windows),
        state(Target_address,available),
        dns_server(Target_address)
</pre>
<post>deny_of_service(Target_address)
</post>
<scenario>Action</scenario>
<cond_scenario>
   script(Action,'winnuke $Target_address')
</cond_scenario>
<detection>Alert</detection>
<cond_detection>alert(Alert),
                source(Alert,Source),
                source_node(Source,Source_node),
                address(Source_node,Source_address),
                target(Alert,Target),
              target_node(Target,Target_node),
              address(Target_node,Target_address),
              classification(Alert,"MIR-0036")
</cond_detection>
</attack>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<attack attackid="MIR-0074">
<name>tcpscan sur la cible</name>
<pre>use_soft(Source_address,tcpscan),
      use_service(Target_address,Target_service),
     service_type(Target_service,tcp)
</pre>
<post>
  knows(Source_user,use_service(Target_address,Target_service))
</post>
<scenario>Action</scenario>
<cond_scenario>script(Action,'tcpscan $Target_address')
</cond_scenario>
<detection>Alert</detection>
<cond_detection>alert(Alert),
                source(Alert,Source),
                source_node(Source,Source_node),
                address(Source_node,Source_address),
                source_user(Source,Source_user),
                target(Alert,Target),
                target_node(Target,Target_node),
                target_service(Target,Target_service),
                classification(Alert,"MIR-0074")
</cond_detection>
</attack>
```

Figura 19. Especificaciones del ataque en Lambda CUPPENS[40].

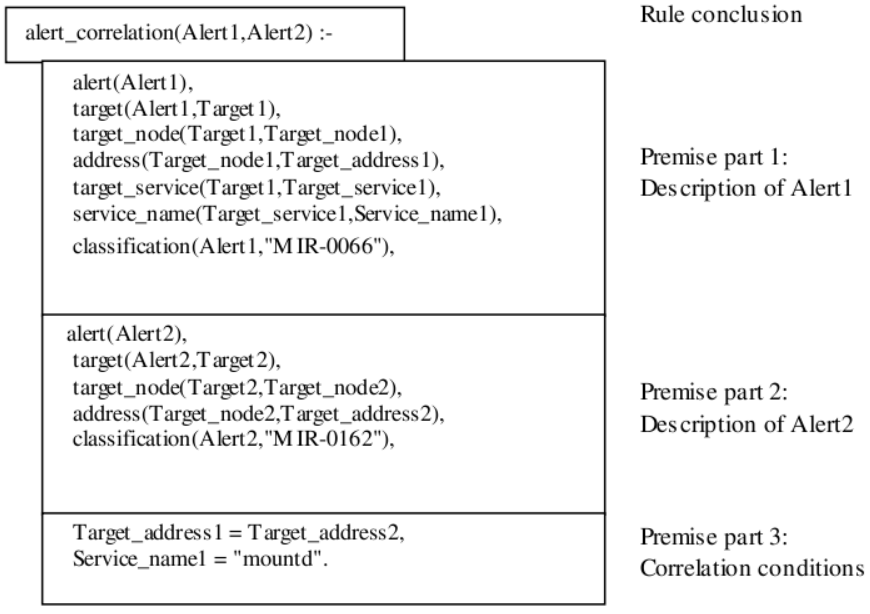


Figura 20: Ejemplo de regla de correlación entre las alertas correspondientes a los ataques. "MIR-0066"(rcpinfo) y "MIR-162"(showmount) CUPPENS[40].

6.3 Definición de una correlación de alerta.

Se entenderá que se tiene dos ataques el ataque A y el ataque B y post(A) y pre(B) respectivamente como una post condición del ataque A y una pre condición para el ataque B, entendiendo que post(A) y pre(B) tienen la siguiente forma:

Post(A)=exprA1,exprA2,...,exprAm.
Pre(B)=exprB1,exprB2,...,exprBn.
en donde cada uno de las expresiones expri debe tener la siguientes formas:
expri=pred.
expri=not(pred).
expri=knows(User,pred)
expri=knows(User,not(pred))
en donde pred es un predicado.

6.3.1 Definición 1: Correlación Directa (Caso simple).

Se puede decir que el ataque A y el ataque B están directamente correlacionadas si cumple con las siguientes condiciones:

- Debe existir un i en [l,m] y un j en [l,n] talque exprAi y exprBj es unificable a través de un unificador mas general (mgu)ϑ.

Ejm. En el ataque "MIR-0163" (NFS Mount) y "MIR-0164" (Modificación de .rhost) están directamente correlacionados. Esto es porque post("MIR-0163") es igual a can_access(Source_user,Partition) y este predicado también aparece en pre("MIR-0164"). Después de cambiar las variables de can_access(Source_user,Partition) que respectivamente aparecen en post("MIR-0163") y en pre("MIR-0164") en can_access(Source_user1,Partition1) y can_access(Source_user2,Partition2) concluyéndose que estas expresiones son unificables a través de mgu ϑ tal que Source_user1=Source_user2 y Partition1=Partition2. Como se puede ver "MIR-0163" esta directamente correlacionado con "MIR-0164" pero "MIR-0164" no está directamente correlacionado con "MIR-163". Esto es porque post("MIR-0164") es igual a access_level(Source_user,Target_address,user). El predicado acces_level(Source_user,Target_address,remote) aparece en pre("MIR-0163") pero las constantes "user" y "remote" no son unificables, la correlación de "MIR-0164" con "MIR-0163" ha fallado. En un segundo caso, se tratará de correlacionar el ataque "MIR-0162" (Showmount) con el ataque "MIR-0163" (Mount partition). Una posible post condición de "MIR-0162" es

knows(Source_user,mounted_partition(Target_address,Partition)), donde el intruso Source_user conoce que particiones son montadas en un objetivo cuya dirección IP es Target_address. Por otro lado, mounted_partition(Target_address,Partition) aparece en pre("MIR-0163"). Sin embargo, debido a la modalidad "knows", está última expresión no es directamente unificable con post("MIR-0162"). Esta intuición no es satisfactoria ya que permite ejecutar Showmount, habilitado el intruso puede montar una partición observada en Showmount. Por lo tanto, hay

que modificar ligeramente la definición 1 de modo que el ataque "MIR-0162" pueda estar relacionada con "MIR-0163", llevando a la siguiente definición.

6.3.2 Definición 2: Correlación Directa (Caso General).

Se puede decir que un ataque A y el Ataque B son directamente correlacionados si una de las siguientes condiciones se satisfacen:

Existe un i en [l,m] y un j en [l,n] tal que exprAi y exprBj son unificables a través de mgu ϑ. ó

Existe un i en [l,m] y un j en [l,n] tal que exprAi y knows(User.exprBj) son unificables a través de mgu ϑ.

Como se puede apreciar hasta el momento se ha podido ver ejemplos de lo que es correlación directa, a continuación se presentara ejemplos de correlación indirecta. Se considerará los ataques "MIR-0073" (TCPScan) y "MIR-0036" (Winnuke). Estos dos ataques no son correlacionados usando la definición 2. Sin embargo, para que el ataque Winnuke tenga éxito se requiere que el sistema objetivo sea Windows. El intruso puede llegar a verificar el sistema mediante la realización de un TCPScan y por la observación del puerto 139 está abierto (Puerto característico de netbios que se haya en el sistema Windows). Lo más lógico es correlacionar los ataques "TCPScan" y "Winnuke" en el caso que se dé un escaneo con la finalidad de comprobar que el puerto 139 este abierto. Pará llegar a una solución factible de este tipo de casos, lo más conveniente es la especificación de normas ontológicas en donde se representaría las posibles relaciones entre los predicados y representadas también por medio de una pre y post condición. En la figura 21 se muestra un ejemplo de tal regla. Esta regla ontológica dice que si un sistema cuya dirección IP es System_address usando por el servicio NetBios, entonces el sistema operativo usado es un sistema Windows.

```
<?xml version="1.0" encoding="UTF-8">
<rule ruleid="RULE-0001">
   <pre>
      use_service(System_address,'NetBios')
   </pre>
   <post>
      use_os(System_address,windows)
   </post>
</rule>
```

Figura 21. Ejemplo de regla ontológica CUPPENS[40].

Desde un punto de vista sintáctico, se supone que las restricciones que se aplican a la representación de una pre y post condición en una regla ontológica son similares a la de la pre y post condición de un ataque, el siguiente paso es la de generalizar la definición 2 cuando la regla ontológica[22] es usada para dar

[22]a) Una ontología es una especificación explícita de una conceptualización, es decir proporciona una estructura y contenidos de forma explícita que codifica las reglas implícitas de una parte de la realidad, independientemente del fin y del dominio de la aplicación en el que

una correlación. Está generalización se da en dos pasos. Primeramente generalizamos la definición 2 a modo que se pueda correlacionar dos reglas ontológicas o un ataque con una regla ontológica o una regla ontológica con un ataque, esta generalización es sencilla ya que se entiende que es igual que la forma sintáctica de una pre y post condición de un ataque, a continuación se da la notación de definición de la correlación indirecta.

6.4 Definición 3: Correlación Indirecta.

Se dice que un ataque A y un ataque B están indirectamente correlacionadas a través de las reglas ontológicas R1, ..., Rn si cumple las siguientes condiciones.

- El ataque A está directamente correlacionado con la regla R1, a través de un unificador más general $\vartheta 0$,
- Para cad j en [l,n-1], la regla Rj es directamente correlacionada con la regla Rj+1 a través de un unificador mas general ϑj, Regla Rn es directamente correlacionada con el ataque B a través de un unificador más general ϑn, Usando la definición 3, Se puede concluir que el ataque "MIR-0073" (TCP-Scan) es indirectamente correlacionado con el ataque "MIR-0036" (Winnuke). Esto se debe a que la post-condición del ataque "MIR-0073" es igual a knows(Source_user,use_service(Target_address,Target_service)). Entonces, ya que la pre-condición de "RULE-0001" es igual a use_service(System_address, 'NetBios'), "MIR-0073" está directamente correlacionado a "RULE-0001" a través de mgu:
- Target_address = System_address, Target_service = "netBios". Del mismo modo, la post-condición de "RULE-0001" es igual a use_os(System_address, windows). Dado que este predicado también aparece en la precondición de "MIR-0036", "RULE-0001" es correlacionada con "MIR-0036" cuando System_address = Target_address.

Así que se puede decir que el ataque "MIR-0073" esta indirectamente correlacionado con "MIR-0036". Hasta este momento se ha podido apreciar la correlación de datos tanto directa como indirecta, a continuación se profundizará en la generación de reglas para la correlación.

6.5 Generación de reglas de correlación.

La idea es la generación automática de las reglas de correlación, para lograr este objetivo se procederá de la siguiente manera. Se tiene dos ataques Attack1 y Attack2 cuya descripción se correlaciona según la definición 2 a través de un mgu ϑ. Después se cambia el nombre a las variables que se encuentran en

---

se usarán o reutilizarán sus definiciones.

b) Una ontología define el vocabulario de un área mediante un conjunto de términos básicos y relaciones entre dichos términos, así como las reglas que combinan términos y relaciones que amplían las definiciones dadas en el vocabulario.

la descripción del Attack1 y el Attack2 de modo que no hay ninguna variable común en estas descripciones, la generación de la regla de correlación tendrá la siguiente forma:

correlation_rule(Alert1, Alert2):-
cond_detection(Attack1),
cond_detection(Attack2),
ϑ.

Donde Alert1 y Aler2 son respectivamente las variables que aparecen en la detección de los campos de Attack1 y Attack2. Por ejemplo en la figura 22a, se presenta la regla de correlación correspondiente a los ataques "MIR-0163" (NFS Mount) y "MIR-0164" (Modificación de .rhost). Esta regla es correcta pero no está totalmente optimizada. En particular, la descripción objetivo de las dos alertas podría ser suprimida ya que no está relacionada con la condición de la correlación. Este proceso también genera condiciones como Partition1 = Partition2. Esto es correcto para este escenario, donde el intruso necesita modificar el archivo .rhost de una partición previamente montada con un ataque de tipo NFS Mount. Pero, ya que Partition1 y Partition2 siguen siendo variables libres, esta condición siempre será evaluada como verdadera. Esto se da por que se asume que la información acerca de las particiones montadas no es proporcionadas por las alertas que corresponden a NFS Mount y la Modificación de .rhost. En el caso de los dos ataques "Attack1" y "Attack2" son indirectamente correlacionadas usando reglas ontológicas esto es ligeramente más complicado. Si el Attack1 y Attack2 son indirectamente correlacionados usando las reglas ontológicas R1,..., Rn a través de un conjunto de mgu ϑo, ..., ϑn, Para la generación de estas reglas de correlación se tiene que seguir la siguiente forma: correlation_rule(Alert1,Alet2):-

cond_detection(Attack1),
cond_detection(Attack2),
ϑ0, ..., ϑn.

Por ejemplo, la figura 22b se presenta la regla de correlación que corresponde a los ataques "MIR-0073" (TCPScan) y "MIR-0036" (Winnuke). Observe que todas las reglas de correlación son generadas automáticamente por el analizador de descripciones en LAMBDA de un conjunto de ataques. Este proceso es realizado fuera de línea y por lo tanto, no es mucho tiempo consumido para la detección de intrusiones en línea.

```
alert_correlation(Alert1,Alert2) :-

  alert(Alert1),
  source(Alert1,Source1),
  source_user(Source1,Source_user1),
  target(Alert1,Target1),
  target_node(Target1,Target_node1),
  address(Target_node1,Target_address1),
  classification(Alert1,"MIR-0163"),

  alert(Alert2),
  source(Alert2,Source2),
  source_user(Source2,Source_user2),
  target(Alert2,Target2),
  target_node(Target2,Target_node2),
  address(Target_node2,Target_address2),
  target_user(Target2,Target_user2),
  classification(Alert2,"MIR-0164"),

  Source_user1 = Source_user2,
  Partition1 = Partition2.
```

Figura 22a. Regla de Correlación para "MIR-0163" (NFSMount) y "MIR-0164" (Modificación de .rhost) CUPPENS[40].

```
alert_correlation(Alert1,Alert2) :-

  alert(Alert1),
  source(Alert1,Source1),
  source_node(Source1,Source_node1),
  address(Source_node1,Source_address1),
  source_user(Source1,Source_user1),
  target(Alert1,Target1),
  target_node(Target1,Target_node1),
  address(Target_node1,Target_address1),
  target_service(Target1,Target_service1),
  classification(Alert1,"MIR-0073"),

  alert(Alert2),
  source(Alert2,Source2),
  source_node(Source2,Source_node2),
  address(Source_node2,Source_address2),
  target(Alert2,Target2),
  target_node(Target2,Target_node2),
  address(Target_node2,Target_address2),
  classification(Alert2,"MIR-0036"),

  Target_address1 = System_address3,
  Target_service1 = 'NetBios',

  System_address3 = Target_address2.
```

Figura 22b. Regla de Correlación para "MIR-0073" (TCPScan) y "MIR-0036" (Winnuke) CUPPENS[40].

Ya una vez generada la regla de correlación hay que aplicarla, de lo cual se tratará a continuación.

Después de que se ha generado toda la regla de correlación fuera de línea, el proceso de correlación en línea puede comenzar. Cuando este proceso recibe una nueva alerta "Alert1" se procede de la siguiente manera. Se hará que Attack1 sea asociado con la clasificación de Alert1. Primeramente se comprobará si existen otras alertas ya almacenadas en la base de datos y cuya clasificación es Attack2 de tal manera que el hecho attack_correltion(Attack1,Attack2) o attack_correlation(Attack2,Attack1) es almacenado en la base de correlación. Observe que este primer paso es sólo para la optimización desde la regla de correlación que puede ser aplicado directamente. Sin embargo es más eficiente para el primer filtro en el predicado attack_correlation para comprobar si existen alertas que son potencialmente correlacionados con Alert1. Sin embargo se puede observar el hecho attack_correlation(Attack1,Attack2) y at-

tack_correlation(Attack2,Attack1) porque no se asume que las alertas no son recibidas en el mismo orden que en el orden que ocurren. Si estas alertas "Alert2" son potencialmente correlacionadas con Alert1, entonces las correspondientes reglas de correlación se aplican para comprobar si las condiciones de correlación son satisfechas. El resultado es un conjunto de pares de alertas que están correlacionadas, un miembro de este par de alertas contiene Alert1. Para cada par en esta serie, se aplicara un algoritmo para comprobar si este par puede ser agregada a un escenario existente. Si no, un nuevo escenario a partir de este par de alertas es generado. Por ejemplo, se asumirá que ya existe un escenario con tres alertas (alert1, alert2, alert3). En la cual se asume que alert4 es recibida y el proceso de correlación en línea genera un par (alert3, alert4). En este caso, un escenario "largo" (alert1, alert2,alert3, alert4) es generado. Observe que un escenario complejo con varias ramas es descompuesto dentro de varios escenarios secuenciales correspondientes a cada rama. Por ejemplo, en el escenario que se presenta en la figura 23. Es representado por dos escenarios (alert1, alert2, alert3, alert4) y (alert2, alert5, alert6, alert4). Esta será el papel de la interfaz grafica para "agregar" estos dos escenarios secuenciales. Para cada escenario secuencial, el proceso de correlación en línea generara una alerta especial que se llama "scenario alert". Ésta alerta es totalmente compatible con el formato IDMEF. El campo "Correlation alert" de la alerta corresponde a la lista de alertas de correlación (El orden de esta lista es importante). Los otros campos de esta alerta son generados por la función de fusión para unir los datos contenidos en las alertas de correlación.

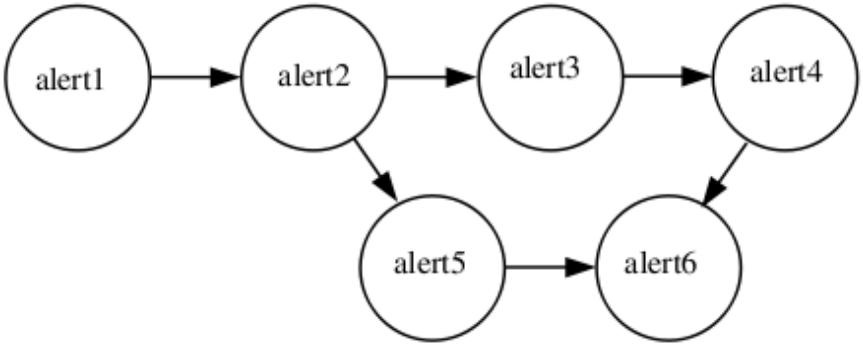


figura 23. Ejemplo de un escenario de ataque CUPPENS[40].

Y es de esta manera como se puede aplicar las reglas de correlación a los diferentes datos, claro estas reglas están susceptibles de errores y no siempre puede llegar a detectar el ataque, pero sin duda proporcionan una gran ayuda.

6.6 Herramientas de Correlación de Datos.

- HP OpenView Event Correlation Solutions (ECS) disponible en:http://www.hp.com/
- ISS Security Fusion Module disponible en:

http://www.iss.net/products_services/enterprise_protection/rssite_protector/sec_fusion_module.php

- NetlQ Security Manager disponible en:http:www.netiq.com/products/sm/default.asp

6.7 Métodos de replicación de datos.

Hay dos maneras de encargarse de llevar los datos al IDS, el primero aunque no muy recomendado es mediante la conectividad con medios compartidos, hub o con la técnica de spanning de puertos en los switches de comunicaciones.

6.7.1 Conectividad con medios compartidos.

La mayor desventaja de estos es el nivel de tráfico que llega a generar un medio de red compartido y a las vulnerabilidades que se introduce en la red por estos medios.

6.7.2 Puertos Espejos.

Según GARCÍA[14] es un puerto del conmutador en el que se da la operación de replicar los paquetes de otros puertos definidos, esta operación le permite monitorizar todo el tráfico que pasa por ellos como si fuera un sensor, lamentablemente los conmutadores no tienen la capacidad de que todo el trafico pase por este puerto, perdiendo paquetes que llegaría a ser clave para la identificación de un ataque.

6.7.3 Test Access Point (TAP).

Su función se basa en la duplicación del tráfico entre dos puertos a un tercero, de forma unidireccional (el puerto de copia no puede enviar no recibir tráfico, solo recibir copias). Como desventaja se tiene que este tipo de técnica puede determinar un problema en la configuración y rendimiento en la electrónica de la red, pero sus ventajas nos ofrecen una mayor estabilidad de red entre prestaciones, seguridades y funcionalidad. Estas arquitecturas basadas en IDS se han visto en la necesidad de dar nuevas soluciones frente a los problemas dados por la cantidad de tráfico que llega a ver, volviéndose criticas, frente a esto se ha dado los denominados TEST ACCESS POINT (TAP). La función de estos dispositivos TAP es, mediante conexiones hadware replican el tráfico de ambos sentidos de una comunicación, estos dispositivos en caso de un fallo de energía no llegan a perjudicar el trafico de red, simplemente la replicación del trafico a los puertos del TAP dejarían de funcionar. En la figura 24 se puede apreciar el funcionamiento de un TAP, como podemos ver el TAP extrae la señal de trasmisión como de recepción que se da entre los 2 equipos de una manera unidireccional, al ser unidireccional la comunicación del IDS no se da con los equipos.

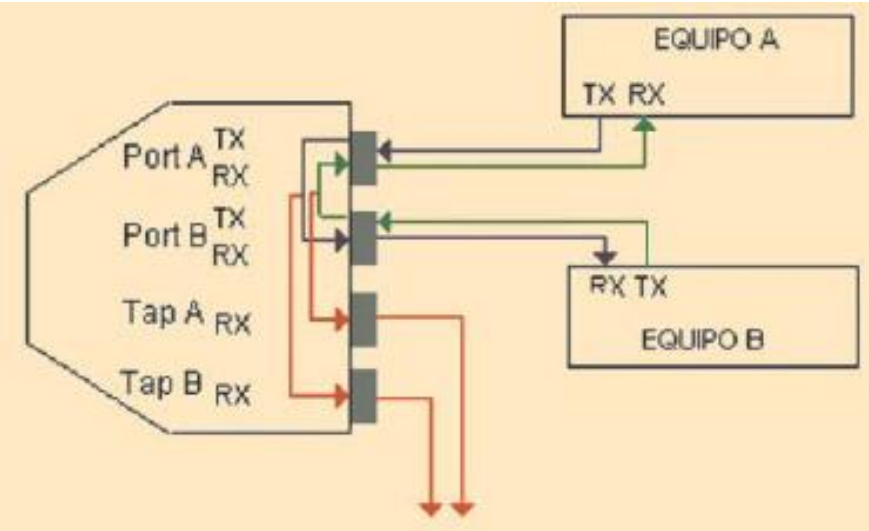


Figura 24. Esquema de funcionamiento de un tap FRANCO[41].

Se puede ver los TAP nos proporcionan 2 puertos de salida, como no podemos agregar ambos tráficos en una misma instancia de nuestro IDS por las limitantes de software hay que habilitar un mecanismo adicional entre el TAP y nuestro NIDS para agregar el trafico, podemos hacer esto mediante un medio compartido o un balanceador de IDS como se puede ver en la figura 25.

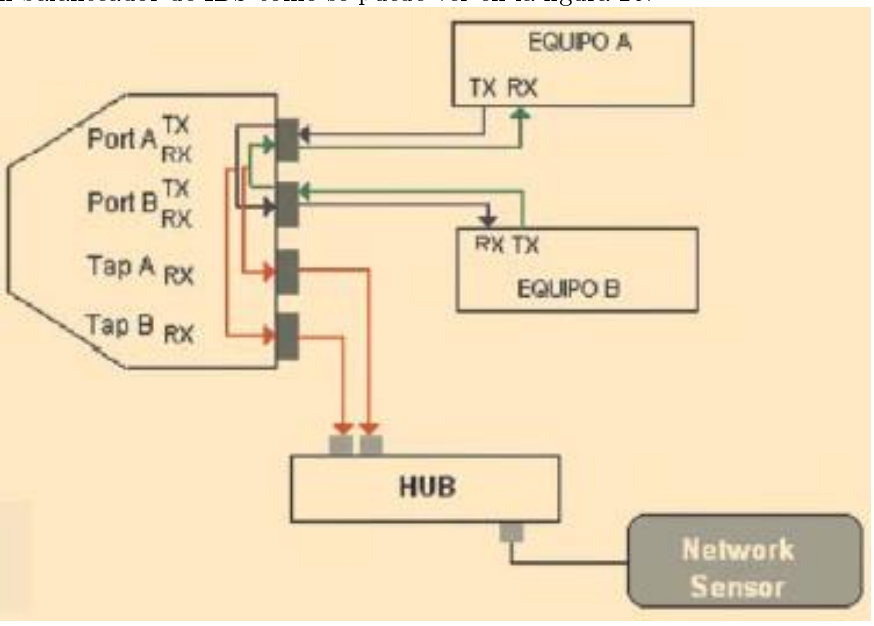


Figura 25. Esquema de conexión de un TAP a un NIDS FRANCO[41].

En la figura 26 se puede apreciar una arquitectura de un TAP mono puerto ubicado en la DMZ, dándonos la ventaja que el NIDS detectaría cualquier ataque originado en la red externa con destino a cualquiera de los servidores instalados en dicha red, sin ninguna configuración especial en el swich (port spanning) haciendo que no se perjudique el rendimiento de la electrónica en la red.

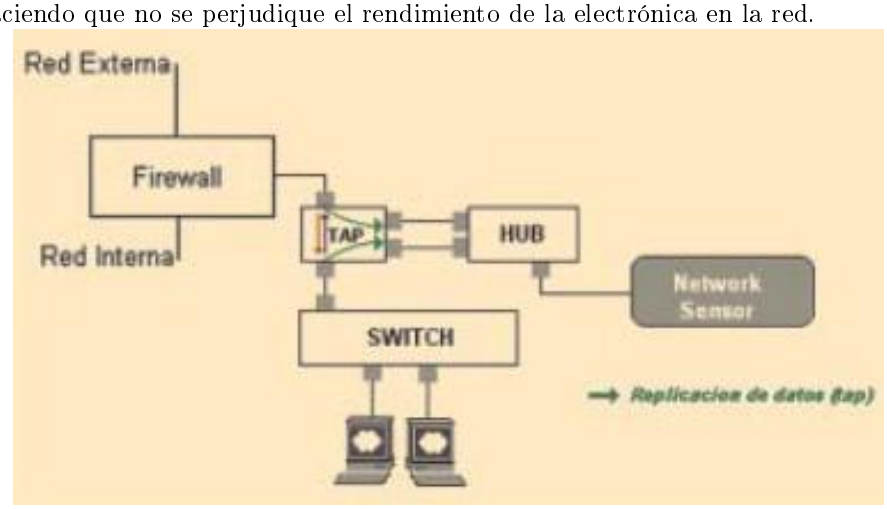


Figura 26. Arquitectura con tap monopuerto FRANCO[41].

Al implementar esta arquitectura se puede ver que no se tiene defensa ante los ataques de los equipos de la misma red, si el atacante obtiene acceso a un equipo ubicado en la DMZ, desde ahí puede introducirse a los demás equipos sin ser detectado por el IDS. Para solucionar el problema se debería sustituir el tap mono puerto por un TAP multipuerto como se muestra en la figura 27.

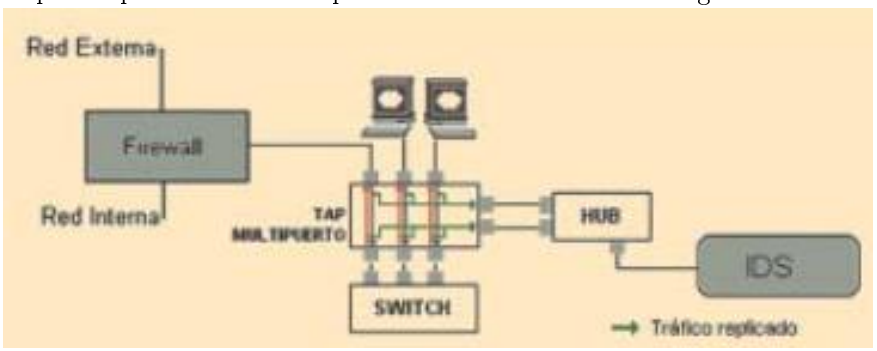


Figura 27. Arquitectura ejemplo con taps multipuerto FRANCO[41].

Así logramos que el trafico también atraviese por el TAP entre los diferentes equipos, con el único problema que por el trafico se pueda tener una posible saturación de puertos de salida del tap. Un segundo panorama es cuando el tráfico de red supero la capacidad de análisis de un NIDS, este problema se puede solucionar al incorporar a la arquitectura un balanceador de IDS. Un

balanceador de IDS, es un dispositivo encargado de repartir el tráfico entre varios NIDS, con la finalidad de poder analizar todo el tráfico de red como podemos apreciar en la figura 28.

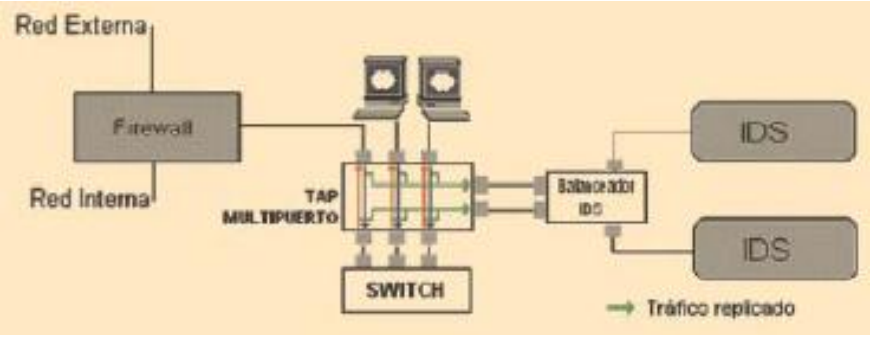


Figura 28. solución con taps y balanceadores de IDS FRANCO[41].

Al incorporar este panorama en el cual los intervienen los TAPs y los balanceadores de IDS, podemos instalar los IDS en cualquier parte de la arquitectura de red sin afectar el rendimiento de los sistemas en la red.

6.8 IP factor determinante en los IDS.

6.8.1 IPv4 vs IPv6.

El aparecimiento de las IPv6 que se dio en el año de 1995 bajo el nombre de IPng (IP de nueva generación) ha traído nuevos retos para los IDS de los cuales es conveniente entender los cambios frente a las IPv4 que se verá a continuación como mensiona TRIULZI[43] y como se puede apreciar en la figura 29:

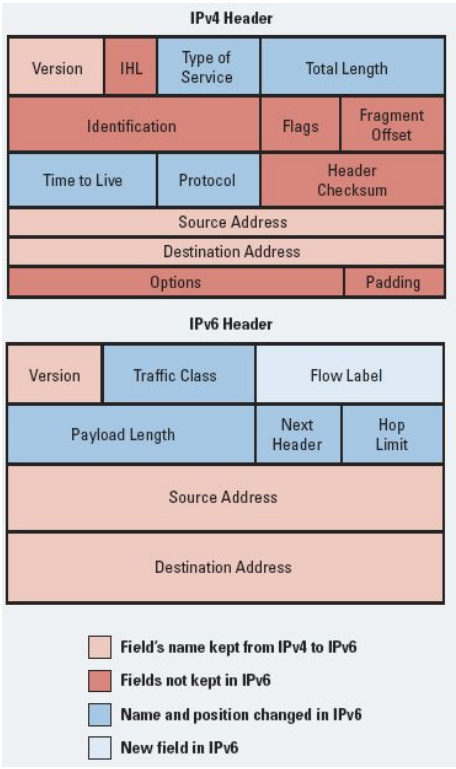


Figura 29. Diferencias entre IPv4 e IPv6 LUIS[46].

Simplificado de cabecera. La cabecera IPv6 es más limpia y con menos campos frente a una IPv4, estos cambios en la cabecera de los paquetes se da, por la experiencia que se ha tenido con estos campos que en realidad no han llegado a ser de mucha utilidad. Desde la perspectiva de un IDS es excelente ya que las CPUs moderna con una cabecera IPv4 no son muy eficientes por el problema de la alineación de los campos de datos pero en una cabecera IPv6 la descomposición de los distintos campos de la cabecera es mucho más eficiente, representado una ganancia en la velocidad de procesamiento por cada paquete.

Un mayor espacio de direcciones. Uno de los mayores problemas que se está enfrentando en la actualidad es el agotamiento de las direcciones IPv4, con IPv6 se tiene un espacio de 2^{128} direcciones disponibles. Creando una tendencia a conectar todo a internet, como algunas empresas ya están trabajando en las llamadas casas inteligentes, permitiendo que cada aparato sea conectado directamente al internet. Ahora hay que entender que cada uno de estos aparatos tendrá que ejecutar un Sistema Operativo con una interfaz de tipo TCP/IP y con el poder de ejecutar un servidor WEB para la configuración y la interacción del usuario, si el atacante llegara a encontrar un defecto de seguridad y llega a tomar el control del aparato para posteriormente llegar a utilizarlo en

una Denegación de Servicios, el atacante tendría a su favor una innumerable cantidad de sistemas.

Autenticación y cifrado de paquetes. La autenticación y cifrado están disponibles en IPv4 a través del uso de IPSec principalmente usado en los denominados túneles VPN. Para un IDS la implementación de los canales protegidos por Ssl o TLS se convierte en un problema, ya que el NIDS puede ver sin problema un ataque realizado por una fuente de tipo HTTP, pero al momento de usar HTTPS este ataque se vuelve invisible frente al NIDS, una solución que se intento aplicar es usar ssldump para decodificar SSL pero el inconveniente que se tiene es que se necesita el control de los parámetros para obtener las claves de sesión. Esto es respecto a las IPv4, en un entorno como es IPv6 esto no mejora, antes empeora, ya que IPv6 tiene una cabecera de extensión por defecto llamada "IPv6 Authentication Header" (AH) que no es otra cosa que el mismo mecanismo de IPsec de IPv4 pero en IPv6, con la diferencia de que IPsec no es ampliamente usado por su dificultad de configuración pero en IPv6 llegaría se ser totalmente usado.

6.8.2 No hay información de fragmentación en la cabecera.

Una consecuencia positiva de esta carencia de la información es un mayor rendimiento en el procesamiento, claro esto llega a significar que la base de la cabecera no necesita ser decodificado por la fragmentación de información y se puede dar para un datagrama una incorrecta reensamblaje.

6.8.3 Comparación.

Se puede decir que el papel que desempeña IPv6 en la actualidad es necesario, prontamente se tiene que dar una migración mundial de IPv4 a este protocolo, dando un nuevo panorama a los diseñadores de seguridad frente a los nuevos retos que de seguro se darán por el manejo de paquetes más concretamente el cifrado o encriptación de los datos.

7 Ataques en IDS.

La información que pasa por un NIDS es lo único que se llega a conocer por estos, no se sabe de la topología de la red, ni las máquinas que lo conforman ni de los sistemas que poseen, también carece de memoria para recordar datos anómalos que hayan sucedido anteriormente, haciendo que carezcan de la habilidad de detectar ataques como son los slow scans[23]. También se cuenta con unos ataques que afecta propiamente a los IDS de los cuales se observará en está sección:

7.1 Evasión.

Este ataque es cuando el IDS rechaza un paquete que el sistema final si acepta, perdiendo el contenido del paquete (figura 30). Este problema puede ser usado por el intruso para evadir al IDS, dado que al ser más estricto que los sistemas finales, rechazará información que si es procesada por los sistemas finales como se puede ver en la figura 30.

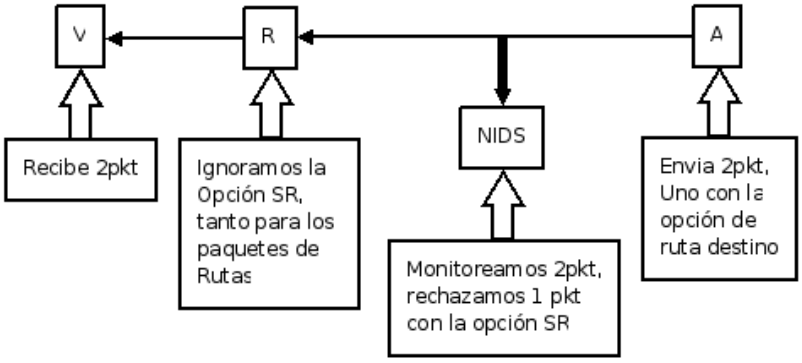


Figura 30, Funcionamiento de Evasión PORWAL[34].

En la figura 31 se puede apreciar un ataque por evasión de una manera más clara. Como se puede ver el atacante envía una cadena de datos, el NIDS no acepta el flujo en la cual consta un dato duplicado, al no aceptar el cuarto duplicado interpreta la cadena como "ATXACK". El sistema final recibe el dato duplicado remplazandolo y así recibe la cadena de la siguiente manera "ATTACK".

[23] Escaneos que se realizan con un tiempo bien alto de separación entre cada uno

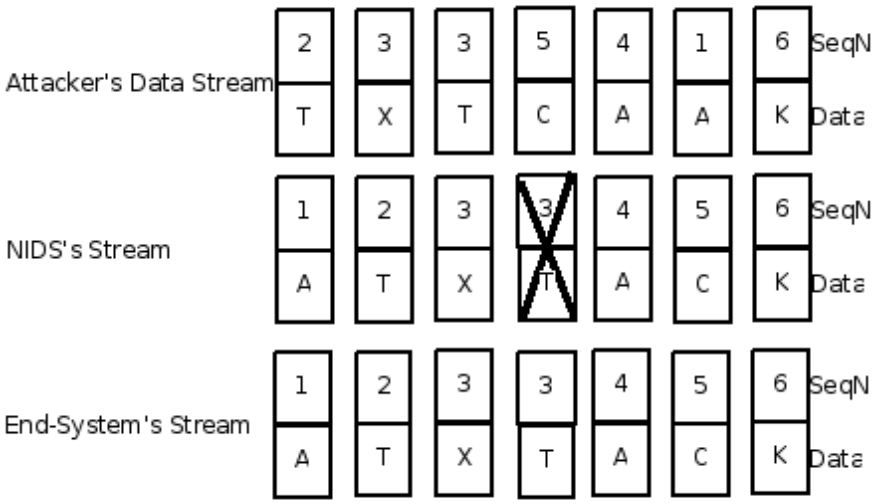


Figura 31, Ejemplo de Evasión PORWAL[34].

Según HANDLEY[35] la evasión se puede clasificar en tres tipos:

- Análisis Incompleto de un NIDS: Se aprovecha que el NIDS no tiene la habilidad de reensamblar un paquete IP que ha sido Fragmentado, en tal caso no se podría analizar el paquete en sí, sino solo una sección del paquete.
- Incapacidad para predecir el comportamiento del sistema final: Un problema que afronta el NIDS es que tiene que trabajar con diferentes entradas debido a que esta interactuando con diferentes Sistemas Operativos, por la fragmentación que se emplea y los diálogos de autenticación que se usa.
- Conocimiento incompleto de la topología de la red: Al no tener un conocimiento de la topología interna de la red, el NIDS puede suponer acerca de los comportamientos de los protocolos que son incorrectos.

7.1.1 Soluciones ante las Técnicas de Evasión.

- Activar solo las firmas para la detección de patrones de que es de interés de la organización. Para esto, el administrador deberá decidir cuales serán activadas o cuales no, de acuerdo a las políticas que se lleguen a establecer para la red.
- Usar correlación de eventos, el cual se profundiza más adelante.
- Usar un esquema distribuido de IDS, que se detalla en la sección de recomendaciones.

7.2 Inserción de información.

Esta funciona cuando a un protocolo de comunicación o de seguridad se le inserta los mensajes adecuados para que llegue a experimentar múltiples implicaciones (ver figura 32); aunque llegue a ser complicado la inserción de información ya sea por los mecanismos que nos permite detectar o prevenir, es una alternativa más para esquivar al IDS. Ejemplo de esto es la inserción de paquetes de información de encaminamiento, con la finalidad de desviar tráfico de manera favorable para un intruso; cuando introducimos mensajes de gestión para la configuración de equipos. Otro ejemplo de inserción que se puede mencionar es el caso en que el IDS se encuentra entre el Router de la Organización y el Router del Internet Service Provider(ISP), el atacante envié un paquete al IDS con un Time to Live(TTL) igual a uno como se puede apreciar un ejemplo en la figura 34, este es aceptado por el IDS pero no por el router de entrada a la organización, otra manera es usando el bit de no fragmentación de IP(DF) y la Maximum Transmitting Unit(MTU) de la red atacada, donde el segmento del IDS la MTU es suficiente para guardar el paquete el IDS lo aceptará pero si es pequeño lo descartará.

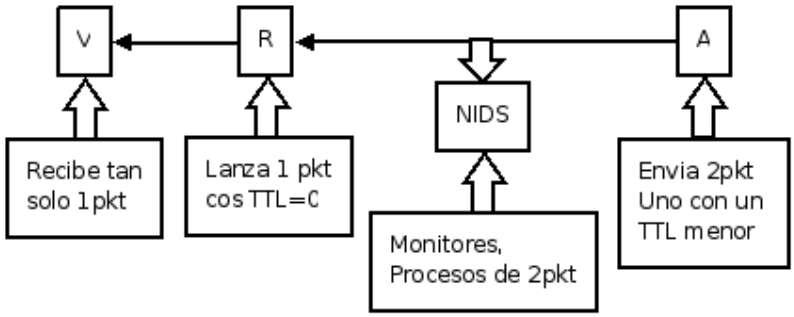


Figura 32. Funcionamiento de Inserción PORWAL[34].

En la figura 33 se puede apreciar un ataque por inserción de una manera más clara. Como se puede ver el atacante envía una cadena de datos, el NIDS acepta el flujo en la cual consta un dato duplicado, acepta esta cadena porque sobrescribe el tercer dato con el dato que le continúa dentro del análisis interpretando la cadena como "ATXACK". El sistema final no recibe el dato duplicado recibiendo la cadena de la siguiente manera "ATTACK".

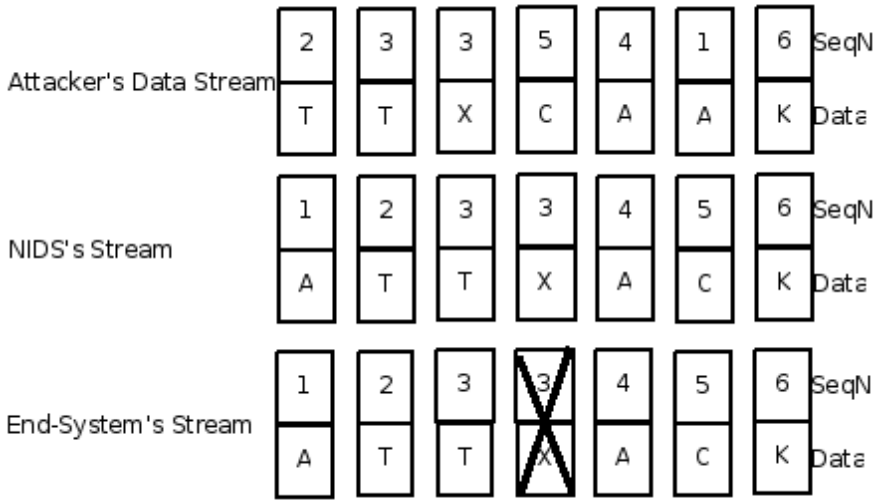


Figura 33. Ejemplo de Inserción PORWAL[34].

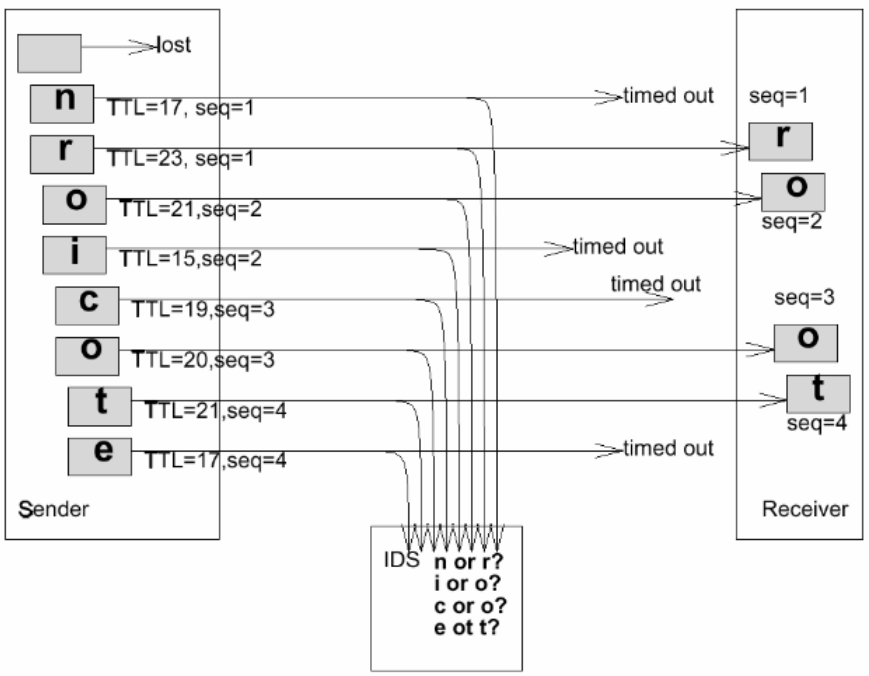


Figura 34: La predicción y topología de la red HANDLEY[35].

En la figura 34 se puede ver como el atacante en realidad envía una cadena "root" ocultada en la cadena "nroicote", cuando el IDS verifica esta cadena pasa sin

generar ninguna clase de alerta pero el sistema final al ser más estricto rechaza los paquetes cuyo TTL (Tiempo de vida) es inferior a 20 conformándose la cadena que el atacante quería introducir a través de los Sistemas de seguridad.

7.2.1 Soluciones ante las Técnicas de Inserción.

La solución ante un ataque de inserción es el ajustar de una manera más rigurosa la selección de tramas. Claro que esto trae una mayor vulnerabilidad para que se realice un ataque por evasión que ya se vio anteriormente.

7.3 Resource exhaustion o agotamiento de recursos.

Este tipo de ataque también conocido como Denial of Service (DOS), está dirigido directamente al IDS por la razón de que un IDS pueden ser deshabilitados ya que son sistemas fail-open[24] y al pasar esto el atacante puede atacar al resto de la red que se estaba protegiendo, en contrarresto de esta vulnerabilidad podemos hablar de sistemas fail-safe[25] (firewalls) en el caso de ser deshabilitados cierran todas las conexiones de red que protegen.

7.3.1 Técnicas DOS.

- Generación de alarmas: En esta técnica se busca generar un gran número de alarmas con el fin de ocultar el verdadero ataque entre un gran número de falsos ataques esto se conoce también como “DOS al administrador”.
- Evitar que el IDS vea el ataque: El objetivo es que el IDS no sea capaz de analizar la información correctamente para que este sea incapaz de ver la acción maliciosa.

A continuación se verá algunos de los problemas que enfrenta un IDS y que son aprovechados por los DOS.

- Como los IDS solo pueden analizar los datos que circulan a través de ellos, los switch que cada vez son más usados, vienen a ser un serio problema, ya que hay que poner más sensores en la red para analizar los datos de toda la red.
- Muchos NIDS no tienen la capacidad de analizar todo los paquetes que pueden pasar en una red Ethernet de 100Mbps haciéndolos propensos a perder paquetes con información relevante.
- Los IDS deben mantener los estados de cada una de las conexiones de TCP que tiene abiertas que se conoce como “stateful”[26], lo cual consume memoria de manera muy altas cuando la carga de la red es elevada.

[24] Una vez deshabilitados queda la red abierta a cualquier ataque
[25] Una vez deshabilitados queda la red cerrada a cualquier ataque
[26] El Stateful Application permite abrir "Puertas" a cierto tipo de tráfico basado en una conexión y volver a cerrar la puerta cuando la conexión termina.

- Los sensores pueden llegar a cegarse debido a una saturación del enlace donde residen, siendo deshabilitados y volviéndolos inútiles en la detección de intrusos.
- Los componentes que almacena un IDS pueden llegar a ocupar un gran espacio físico, sobrepasando la capacidad del servidor, haciendo que este deje de funcionar o que comience a perder registros significativos.

7.4 Otros Ataques.

7.4.1 Verificación de la lista de protocolos.

Algunas formas de intrusión, como "Ping de la muerte" y "escaneo silencioso TCP" utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos e indicar esta táctica comúnmente utilizada. Uno de los ataques más utilizados es el denominado TCP RESET el cual es un tipo de ataque cuyo objetivo es bloquear los recursos o servicios del cual tenía acceso una máquina. Como se puede ver, este tipo de ataque se vale del protocolo TCP, donde el atacante quiere terminar prematuramente con la sesión TCP activa de la víctima. Para lograr este tipo de ataque se tiene que predecir de forma aproximada los números de secuencia generados durante las sesiones, para poder lograr construir un paquete que sea aceptable para la terminación de la conexión. Una vez descubierto el número de secuencia se necesita construir un paquete falso cuya dirección IP y MAC de origen sean las mismas del equipo emisor y con el número de secuencia correcto, en el paquete se tiene que activar la bandera RESET del encabezado del protocolo TCP, esta bandera RESET es un bit de control, el cual indica al receptor que tiene que eliminar la conexión sin ningún otro tipo de interacción como reconocimiento o banderas FIN. Estos tipos de ataques se benefician del gran ancho de banda que poseen las actuales redes.

7.4.2 Verificación de los protocolos de la capa de aplicación.

Algunas formas de intrusión emplean comportamientos de protocolos no válidos, como "WinNuke", que utiliza datos NetBIOS no válidos (al agregar datos fuera de la banda). Para detectar eficazmente estas intrusiones, un NIDS debe haber implementado una amplia variedad de protocolos de la capa de aplicación, como NetBIOS, TCP/IP, etc. Esta técnica es rápida (el NIDS no necesita examinar la base de datos de firmas en su totalidad para secuencias de bytes particulares) y es también más eficiente, ya que elimina algunas falsas alarmas. Por ejemplo, al analizar protocolos, NIDS puede diferenciar un "Back Orifice PING" (bajo peligro) de un "Back Orifice COMPROMISE" (alto peligro).

7.5 Criterio de evaluación ante el ataque.

A continuación se verá el algoritmo empleado por parte de lo que se conoce como respuesta automática o activa, el cuál representa el proceso general que

seguirá el IDS ante la detección de una amenaza, sin preocuparse del método que se este empleando ya sea para detectarlo o responder ante la intrusión.

7.5.1 Algoritmo de activación.

Algoritmo de activación
ESTADO: {Detección ataque}
SI umbral de respuestas superado: REGISTRAR && FIN
SI NO
Comprobación actor atacante
Si es actor protegido: REGISTRAR && FIN
SI NO
Ponderación histórica de gravedad
SI umbral de gravedad superado ACTUAR
SI NO
REGISTRAR
FSI
FSI
FSI
Para revisión de otros ejemplos revisar el Anexo 3.1

8 Discusión.

Como se ha mostrado en el mundo de internet y Sistemas informáticos se tiene una amplia gama de programas o herramientas con las cuales un atacante se podría valer para lograr su objetivo, ya sea el simple hecho de ingresar al Sistema o causar daños dentro del mismo. La realidad actual de este malware es frustrante, ya que las empresas que desarrolla software para contrarrestarlos ya no pueden darse abasto para controlar el 100% de estos programas maliciosos que salen a infectar un sistema, a tal punto que tener un antivirus ya no es garantía total de que éste llegue a proteger, antes es una carga más para el equipo en el que está trabajando, ya que ocupa recursos del sistema sin llegar a proteger el sistema. Razón por la cual ya no sólo es suficiente estudiar el malware y tratarlo de eliminar, si no estudiar su comportamiento y tratar de establecer la manera en que ataca, para lograr desarrollar mejores mecanismos contra estos.

Al inicio el desarrollo de virus fue lenta y gracias a esto se pudieron desarrollar aplicaciones para contrarrestarlos, dando lugar a los antivirus en manera de utilidades, los cuales eran programas diseñados propiamente para detectar y eliminar virus individuales específicos o a medida dando paso a mejoras que se conoce actualmente como antivirus. Los investigadores comenzaron a introducirse a la detección de virus de una manera proactiva, ya no basándose en una signatura específica si no dando paso al campo del análisis heurístico, dentro de lo cual los investigadores adquirieron experiencia al analizar los patrones de estos códigos maliciosos y separar estas características. El siguiente paso para hacer frente a estos ataques fue el análisis de comportamiento, el cual recurre a un programa en el que se decide si el comportamiento analizado es malicioso o no y dependiendo de este análisis el programa procede a ser bloqueado o no. Claro la ventaja de éste radica que el usuario ya tenía una prevención de los nuevos programas que aún no se conocía, pero la desventaja de este es que dejaba una cierta incertidumbre entre las acciones claramente maliciosas y las que realmente son legítimas, ya que en realidad un programa puede hacer acciones que pueden ser consideradas como maliciosas tal como la eliminación de archivos del computador, que pudieron ser ejecutadas por el usuario o el sistema. Anteriormente los atacantes eran personas expertas con altos conocimientos, una gran experiencia y desarrollados métodos para romper en los sistemas, ahora en la actualidad este perfil ha cambiado, un atacante se puede ayudar de herramientas automatizadas y scripts [27], los cuales ya están adaptados para las amplias y conocidas vulnerabilidades, poniendo en riesgo los servicios que se ofrecen como

[27] Un script es un guión o conjunto de instrucciones. Permiten la automatización de tareas creando pequeñas utilidades. Es muy utilizado para la administración de sistemas UNIX. Son ejecutados por un intérprete de línea de órdenes y usualmente son archivos de texto. También un script puede considerarse una alteración o acción a una determinada plataforma.

los e-commerce[28], la bolsa en línea y sitios de venta de algunas empresas, aquí es cuando un IDS llega a tener mejores resultados ya que pueden llegar a detectar estos ataques

En los tiempos actuales, se ha podido ver que cada vez el número de ataques son más frecuentes ya sean por personas especializadas y que saben lo que hacen como los denominados hacker que llegan a ser una gran amenaza, ya que estas personas se tomarán el trabajo de burlar un sistema de seguridad y llegar a cumplir su objetivo sin importar los avanzados y muy bien implementados sistemas de seguridad y por último los denominados script kiddies que a simple vista parecería que solo llegan a ser una gran amenaza en las redes pequeñas, pero lamentablemente el número de script kiddies son cada día más numerosos gracias a que no necesitan tener un gran conocimiento en el área de la informática y en la misma red pueden llegar a encontrar un gran número de herramientas. Estos pueden llegar a amenazar la infraestructura de una red grande y muy bien protegida al coincidir que el ataque de varios de estos script kiddies puedan llegar a sobrepasar el nivel de procesamiento de los equipos que protegen esta red, logrando de esta manera descubrir una vulnerabilidad que lamentablemente pudo quedar olvidada o que en realidad no se conocía o dejar al sistema inoperante.

Por los motivos anteriormente mencionados se debe establecer los principios de la Seguridad informática, más que un conjunto de técnicas o procedimientos a seguir es propiamente dicho "principios" que al darse en sus tres formas básicas "Confidencialidad, Integridad y disponibilidad", se garantiza que la información es correcta, además de permitir que se llegue a identificar los problemas y la solución adecuada o soluciones adecuadas a estos problemas mediante una correcta administración de la seguridad, motivo por la cual hay que tenerlas presentes y en toda medida tratar de dar al sistema el cumplimiento de esta medidas mediante herramientas que ayuden al cumplimientos de estos principios como las implementadas por la universidad, ya sean la implementación de servidores de antivirus, firewall, etc. Referente a los servicios de la Seguridad Informática, en estos se proporciona una idea de la manera en la que se puede dar cumplimiento a los principios de la Seguridad Informática, ayudando en dichos puntos a pensar en las posibles herramientas, técnicas o tecnologías que se podrían llegar a usar para que esto principios de la Seguridad Informática se lleguen a cumplir. Para lo referente a las tecnologías de seguridad informática se puede decir que en los momentos actuales los avances tecnológicos en el área de la seguridad han sido una necesidad que no se puede dejar ya de lado, por todos los factores que afectan a la red, sistemas o información. Una empresa o institución tiene que pensar muy seriamente en todos los medios que tiene que implementar en sus sistemas e infraestructura para tratar de alguna manera de volverle al atacante una tarea un poco más complicada al tratar de burlar dichos sistemas de seguridad. Razón por la cual es necesario implementar políticas en las cuales se llegue a la necesidad de estar capacitando al personal encargado de la seguridad

[28] El e-commerce (del anglicismo Electronic Commerce) consiste en comprar y vender productos o servicios a través de sistemas electrónicos como Internet y otras redes computacionales.

de nuestra red para que estos lleguen a utilizar de una forma cada vez más eficientes cada una de las herramientas que se han visto en esta sección y a pensar en nuevas soluciones que nos ayuden a la prevención de ataques, razón por la cual los denominados IDS van a ayudar bastante a entender la posición defensiva que se encuentra la universidad, aunque estos ataques no lleguen a tener éxito, el IDS emitirá alarmas que adviertan de los ataques y poder tomarlos en cuenta para reestructurar una nueva postura defensiva, además que el IDS permite darse cuenta de que tan buenas son las configuraciones de otros dispositivos de seguridad ya sean firewall. Al entender que un IDS es un aspecto más en la postura defensiva de una red que más comienza con un establecimiento de políticas de seguridad que sean efectivas y adecuadas, donde los administradores y usuarios deben estar debidamente capacitados para tomar las correctas acciones y cuya políticas van a ayudar en mucho a las configuraciones de los firewall y los IDS. Con respecto a su estructura se puede decir que es necesario comprender cuales existen en la actualidad para poder determinar cual implementar dentro de la universidad. Por su misma naturaleza no comercial y en vista que sus conceptos han llegado hasta la actualidad teniendo una gran aceptación y permite tener sistemas de detección de Intrusos Interoperables y con el máximo de información compartida, además de los componentes de detección de intrusión son fácilmente reutilizables en contextos para los que no fueron diseñados, razones para las cuales nos enfocaremos en la arquitectura definida por Common Intrusion Detection Framework (CIDF).

Esta CIDF se encuentra entre las arquitecturas más usadas y mejor desarrolladas, pero con el inconveniente de que su lenguaje es un poco complejo de usar lo cual no le ha dado mucha aceptación, fomentando la creación de otras arquitecturas, sin embargo su estructura dividida en cuatro partes (Generador de Eventos "E-Boxes", Motor de datos "A-Boxes", Unidad de Almacenaje "D-Boxes" y la Unidad de Respuesta "R-Boxes") ha permitido estructurar de una mejor manera el trabajo que realiza en forma global, a pesar de tener grandes cualidades, como cualquier otra arquitectura, CIDF no está totalmente desarrollado para hacer frente a todos los posibles requerimientos que se puedan presentar.

Referente a los tipos de IDS, la implementación de estos depende mucho de los fines que la universidad persiga. Los Host IDS permitirán saber las amenazas que se pueden dar sólo en el equipo, entre otros tipos de IDS como son los NIDS que se vio anteriormente, los IDS pueden llegar analizar un ataque que llega al equipo ya sea que la información que se ha enviado sea encriptada o no, se use otras tecnologías como son fragmentación[29] de paquetes, esto se da, ya que al momento de llegar el paquete al host, éste ya llega completo y descifrado lo cual ya no da mucho inconveniente para analizar. Los NIDS se han convertido en una de las primeras líneas de defensa, aunque sean prometedores en la vigilancia de tráfico que atraviesa la red, esta tarea de vigilar se está compli-

[29] Cada paquete de red se ha basado en una MTU (Maximum Transmission Unit) de tamaño. La MTU es el tamaño de la mayor red de paquetes que pueden transmitir, donde los paquetes más grandes que las permitidas MTU debe ser dividido en varios paquetes más pequeños o los fragmentos, a fin de que puedan recorrer la red.

cando día a día. Esto se da por razones ajenas al sistema como es que aparecen nuevas amenazas y vulnerabilidades cada año, como la creciente incorporación de sitios que contienen códigos maliciosos y la facilidad en que estos pueden llegar expandirse. Hay que tener muy en cuenta que estos NIDS tienen un serio problema en lo que es su mantenimiento y para este mantenimiento se requiere de personal realmente calificado, ya que se necesitara hacer un análisis de todo la información que maneja y de cómo los usuarios interactúan con ella, ya sea por manejo directo o por medio de programas que lleguen a realizar actividades que puedan determinar un comportamiento dentro del sistema. Razón por la cual se debe tener muy en cuenta la adquisición del personal que deberá realizar un mantenimiento y estudio de los perfiles de usuario y el análisis de los falsos positivos. O en el caso de los NIDS por firmas el establecimiento de un personal riguroso se deberá contratar para la creación de las firmas que deberán ser alojadas en la base de datos y que se tenga un especial cuidado al momento de la instalación de las actualizaciones o parches que se lleguen a aplicar a los servidores, ya que en este proceso pueden dar nuevas vulnerabilidades y este personal este en constante análisis de las nuevas firmas ya que si se da un ataque que no consta en la base de firmas, lamentablemente el ataque no será detectado y tampoco detenido. Desde el punto de la infraestructura, los tiempos van exigiendo nuevos métodos en los cuales se apunta al ahorro de recursos, anteriormente era muy bueno usar un modelo centralizado ya que no existía un gran flujo de datos y los equipos no necesitaban un gran procesamiento, pero en la actualidad las redes han alcanzado una gran velocidad, lo que implica que es necesario contar con equipos de gran rendimiento para analizar los datos y se ha llegado a la necesidad de dividir el trabajo de procesamiento para lograr analizar toda esta gran cantidad de datos.

Para el análisis de esta información se puede llegar a implementar los TAPS, hay que tener en cuenta que para la eficacia de la seguridad hay que desplegar o ubicar los sensores de tal manera que se llegue a proteger los activos más críticos, donde la configuración del IDS es el reflejo de las políticas de seguridad, la instalación de las firmas apropiadas y otras condiciones iniciales que permitan tener un adecuado desempeño y un correcto procedimiento forense ayudara de gran manera en el descubrimiento de pruebas para posibles procedimientos. Algo muy importante es que se debe establecer un procedimiento para el manejo de alertas de IDS y examinar la manera de correlacionar alertas con otra información, como puede ser sistemas o aplicación de logs, en el caso de la universidad se recomendaria implementarlo en el ASA por la visibilidad.

Un punto a tocar referente a estos sistemas es que hay problemas de seguridad que afrontan los IDS, como pueden ser los ataques de evasión o inserción, como se puede ver, no hay sistema que este excepto de errores, los atacantes están constantemente buscando nuevas técnicas para evadir los sistemas de seguridad que se puede llegar a tener implementado en una organización, existe una gran diversidad para lograr estos objetivos, ya sean aprovechándose de la manera en que trabajan los IDS o de los errores que puedan ver en lo que es el mismo software. Lo que sí es seguro, que siempre se tendrá que buscar métodos cada vez más eficientes para tratar de contrarrestar los ataques como los

honeynet que ya se esta investigando en la universidad y llega a ser un gran complemento con los IDS para fortalecer la seguridad.

El IDS aparte de ser una herramienta en el control de Intrusiones permitirá saber el estado real de la seguridad y de las políticas implementadas, de lo cual lo recomendable es la elaboración de un procedimiento en el que se detalle cómo manejar las alertas producidas por un IDS y la manera de correlacionar estas alertas con otra información. La tecnología por sí sola no es suficiente para mantener la seguridad de una red, la organización debe atraer, retener y formar el personal técnico cualificado para operar y mantener estas tecnologías de Identificación de Intrusos.

En cuanto a la rentabilidad, la adquisición de un IDS, la realidad es que las empresas que desarrollan IDS al sacar su producto estos pasan por una agresiva competencia por adquirir una cuota del mercado, donde la evaluación de estos equipos o productos no es nada sencillos y donde la información de estas evaluaciones en realidad no es tan accesible, completa o creíble y mucho más se viene a dificultar con el personal, ya que conseguir y retener el personal calificado que sea capaz de administrar la seguridad en un plano general y la detección de Intrusos se ha convertido en una tarea muy competitiva y por último el inconveniente que presenta la tecnología en la actualidad que es el rápido desarrollo de estas, lo cual representa para la empresa un impacto grande ya que se torna más difícil que pueda aplicar de una manera eficaz a largo plazo las estrategias de seguridad con las que cuenta. Obviamente si una empresa quieres adquirir un IDS lo primero que tiene que ver son los recursos con los que cuenta para la implantación y funcionamiento de éste y ahí ver uno que se ajuste a las necesidades que tenga la empresa para dentro de sus limitaciones escoger el que más le convenga, claro el proceso de selección es complicado ya que dentro de esta industria no hay estándares bien definidos contra los cuales se pueda comparar varios IDS, por la razón de que todos los fabricantes de IDS no siempre va a presentar sus productos en comparación con los estándares de otra empresa, ya sea por motivos de competencia o márquetin. Se aconseja usar guías de actualización por terceros en un período por lo menos mensual ya que hacerlo de una forma personal sería algo prohibitivamente costoso. Con respecto a las implementaciones de un IDS, éste sería segura su ubicación como complemento a las herramientas de seguridad, sobre todo del tipo de NIDS ya que en la actualidad se tiene como necesidad el proteger la información con el mayor número de herramientas y técnicas que se tenga a disposición. Al ver que se cuenta con una gran variedad de IDS, se debe que tener en cuenta que sea cual sea la estructura, el funcionamiento o la marca de éste, hay que llevar a cabo un control de lo que es la comprobación del sistema y responder a las descripciones que tenemos en los informes. A consecuencia de esto se debe llegar a tener un establecimiento de funciones y responsabilidades para analizar y actuar sobre las alertas que lleguen a ser generados por el IDS, una vez realizado se debe hacer un seguimiento de los resultados ya sean manuales o automáticos con la respectiva auditoria del propio IDS, ya que como sistema también puede llegar ser atacado por parte de un intruso y aprovecharse de las posibles falencias que pueda tener esta clase de sistemas, las cuales no son

reveladas por el proveedor de dicho IDS, hay que tener en cuenta que se debe ser una revisión de la integridad de los archivos contenidos en el IDS. Como punto final hay que tener en cuenta el mantenimiento del IDS, en el cual se incluye la instalación de las firmas conforme estas estén disponibles, la instalaciones periódicas que necesita el mismo IDS.

Hablando genralmente ya sobre la investigación en si, se puede decir que éste tema de tesis no solo es importante, si no también que es indispensable, ya que la seguridad es un tema que hoy por hoy ya no se puede dejar de lado, razón por la cual el estudio de nuevas técnicas o herramientas que permitan tener una barrera ante los posibles ataques, contra cualquiera de los sistemas que hay en la universidad, debe ser un prioridad, por esta razón es necesario tener un mejor entendimiento de que es un IDS y como este podría ayudar a dar una mayor seguridad a los sistemas que se encuentran actualmente implementados en la red de la universidad.

Referente al material que se puede hallar con respecto a los IDS, se cuenta con una gran variedad de información general, en donde se puede ver que hay un mayor aporte de materiales comprendido entre el año 2003 al 2006, por la sencilla razón del aparecimiento de nuevas tecnologías como son los honeynet, desviando la mira en la investigación sobre los IDs, pero no por esto deja de ser importante, ya que se ha llegado a ver que estas dos tecnologías se complementan muy bien en su fin que es dar una mejor estructura para la defensa de una red, con respecto a encontrar información más detallada en lo que se refiere a configuración o la parte técnica, se ha visto un poco de complicaciones, no por el hecho de que no exista información sobre esto o no se cuente con un aporte investigativo sobre el tema, si no más bien, por el lado en que las personas conocedoras del tema se han visto un poco reservadas a brindar o liberar la información, posiblemente por la competencia en esta área, garantizando así su estabilidad laboral. Como se menciona anteriormente, la adquisición de personal calificado en esta área se ha vuelto muy competitiva y dificil de retener.

En cuentión a la bibliografía, en un inició no fue sencilla, ya que obtener material realmente bueno, a nivel de un estado del arte, fué una tarea de mucha paciencia, pero una vez identificados los sitios y establecidos algunos contactos que ayudaron sobre el tema, sin interes alguno, se logro contar con el material adecuado para el desarrollo de esta investigación.

9 Recomendaciones.

- Hay algunas arquitecturas que se podrían implementar para una red, en el caso específico de la red de la UTPL, se daría mejor la implantación de la arquitectura DIDS (Distributed Intrusion Detection System) el cual combina monitoreo distribuido y reducción de datos (por medio de monitores individuales en hosts y LANs) con un análisis centralizado de datos (por medio del DIDS director) el cual ya se mencionó en esta tesis, como se ha podido ver esta arquitectura podría emplearse en la actual red de la UTPL, considerando el tamaño de la red, el tamaño del equipo capacitado en el tema de los IDS y los factores económicos que significan el mantenimiento de una infraestructura IDS.

- Una de las razones más importantes para implementar esta arquitectura se da por el tamaño de la empresa, por el personal que se necesita para implementar o mantener un sistema IDS, si se opta por ampliar el sistema de Detección de Intrusos se debe tener IDS con sus propias bases lo que significa tener más personal capacitado para manejar estas bases de datos y por consiguiente, se necesitaría de mayores recursos económicos. Al implementar un DIDS se centraliza los datos que en general es donde se debe tener un mayor análisis y se invierte un mayor esfuerzo que en realidad solo la puede llevar a cabo una persona especializada en el tema de los IDS, logrando así una reducción en los costos de mantenimiento.

- Como se muestra en la figura del anexo 5.1, se puede ver la actual red de la UTPL, en un caso inicial sería recomendable ubicar el IDS entre el ASA y la red que quieran monitorear, si bien tendrá muchos falsos positivos inicialmente, el enlace al router de borde es un buen lugar para comenzar. ¿Porqué es recomendable ubicar el IDS entre el ASA y una red?. Ya que el ASA es un equipo dedicado principalmente a la seguridad, además de la conectividad, porque posee capacidades de IDS y finalmente porque tiene una muy buena visibilidad del tráfico entre las diferentes redes, cabe destacar que esto ya se encuentra implementado en la actual red de la UTPL, futuramente se puede colocar 5 IDS para monitorear las demás redes.

- Realizar un testeo de seguridad a los IDS que se tienen implementados en la red de la universidad con las herramientas ya sugeridas a lo largo de esta tesis.

- A pesar de los esfuerzos por el desarrollo de esta tecnología se presenta la limitación general ante el desarrollo de cualquier tecnología, que es la

integración con otros sistemas, por tanto la interoperabilidad es un criterio que se debe mantener al insertar un IDS en la red de la UTPL.

- Para un futuro desarrollo de este tema, se debe seguir profundizando en el estudio de los IDS, sobre todo, orientado esta investigación en temas primordiales como son, la correlación de datos, la investigación acerca de nuevas herramientas que ayuden a dar una mayor seguridad a la red, como también al fortalecimiento de los IDS y su administración, garantizando así, un mejor desarrollo y funcionamiento de los mismo, claro sin olvidar el trabajo de estos juntamente con otras técnologias como son los honeynet, los cuales son un punto clave en el fortalecimiento de la seguridad, que juntamente a los IDS, han logrado ser un gran complemento en el robustecimiento en las arquitecturas de seguridad.

10 Conclusiones.

- En vista de que los sistemas actuales como son los firewalls o los VPN[30] ya no son suficientes para enfrentar los actuales problemas de seguridad, se necesita incorporar un elemento más al conjunto de sistemas destinados al fortalecimiento de la seguridad de la red, como son los IDS, los cuales completarán el proceso de aseguramiento al permitir la detección o la presencia de intrusos que hoy en día debe de estar en la infraestructura.
- En cuanto a la arquitectura se debe poner un especial énfasis al motor de análisis, ya que este componente es el encargado de detectar todo el posible tráfico malicioso y para ello se tendrá que disponer para este componente de un equipo con altas prestaciones.
- Un componente medular es la correlación de datos, proceso en el cual la mayor ganáncia se da por las aportaciones externas de las empresas que se dediquen a investigar sobre esta área. Hay que tener en cuenta que un punto principal es el análisis de tráfico cifrado que hoy en día no es posible.
- Un punto importante a tener en cuenta, es que se tendrá que orientar la investigación acerca de los ataques no solo a los diferentes recursos en la red, sino también al propio IDS ya que el atacante crece en habilidades, además puede utilizar mecanismos para obligar al IDS a funcionar de una manera incorrecta. Aunque los IDS son mecanismos de seguridad a lo largo de los estudios realizados en esta investigación se ve que estos pueden llegar a ser blanco de ataques, logrando así que estos no funcionen de una manera adecuada.
- Un riesgo para los NIDS, es el aparecimiento de la Ipv6 que incluye la codificación, puede significar un gran golpe mortal a estos sistemas, ya que el NIDS se ve limitado en el análisis de los paquetes encriptados y por lo tanto no es capaz de analizar si un paquete es malicioso o no y con ello tomar una acción de defensa.
- En conclusión, he aprendido que el tema de la seguridad es un campo el cual núnca se puede llegar a garantizar, que un intruso no logré burlar los sistemas empleados para proteger una red. Propiamente en los IDS se ve, que como todo sistema tiene sus ventajas como sus falencias, el cual puede llegar a significar una gran ganancia en el fortalecimiento de la seguridad, al permitir no solo responder ante un ataque, si no también entregar una apresiación del estado actual de la seguridad de una red.

[30] Red Privada Virtual (Virtual Private Network), es una tecnología de red que permite extender la red local sobre una red pública

References

[1] GARCÍA, M. (2008, septiembre): La aparición de nuevo malware se ralentiza, pero se especializa cada vez más. (en línea). Formato html, Disponible http://www.gdata.es/unternehmen/ES/articleview/4240/1/229/

[2] KONSTANTIN, S. (2006, septiembre): Boletín de seguridad Karpersky. Enero-junio de 2006. Programas maliciosos para plataformas diferentes a Win32. (en línea). Formato html, Disponible http://www.viruslist.com/sp/analysis?pubid=197329957

[3] KONSTANTIN, S (2005): Evolución de los programas maliciosos para Unix, Linux y similares. Formato pdf y html, Disponible http://blog.seguinfo.com.ar/2006/08/2005-evolucin-de-los-programas.html

[4] PANDA SECURITY (2009): Tipos de virus. Formato html. Disponible http://www.pandasecurity.com/spain/homeusers/security-info/about-malware/technical-data/date-3.htm

[5] ARCE, I. (2005, octubre): Tendencias en ataques informáticos. Formato pdf. Disponible http://www.coresecurity.com/files/attachments/Arce_2005-PDF.pdf

[6] ISECOM (2004): Malware. Formato pdf, Disponible http://www.hackerhighschool.org/lessons/HHS_es6_Malware.pdf

[7] MCHUGH, J., CHRISTIE, A. y ALLEN, J. (2000, octubre): The role of intrusion detection systems, formato pdf,

[8] EMM, D. (2008, abril): Ante amenazas cambiantes, soluciones cambiantes: una historia de los virus y los antivirus, (en línea). Formato html. Disponible http://www.viruslist.com/sp/analysis?pubid=207270980

[9] ALLEN, J., CHRISTIE, A., FITHEN, W., MCHUGH, J., PICKEL, J., STONER, E., ELLIS, J., HAYES, E., MARELLA, J. Y WILKE, B. (2000, enero): State of the practice of intrusion detection technologies. Formato pdf. Disponible http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf

[10] ARROYAVE, J., HERRERA, J. Y VÁSQUEZ, E. (2007): Propuesta de modelo para un sistema inteligente de detección de intrusos en redes informáticas(SIDIRI). Formato pdf.

[11] HERNÁNDEZ, C. (2001): Hackers los piratas del chip y de internet. Formato pdf. Disponible http://proton.ucting.udg.mx/tutorial/hackers/hacking.pdf

[12] SÁNCHEZ ACEVEDO, N. Y CASTAÑEDA SEGURA, J. (2006, junio): Una guía metodológica para el cálculo del retorno a la inversión en seguridad informática. Formato pdf. Disponible http://www.criptored.upm.es/descarga/TesisRetornoInversionSI.zip

[13] Asesoriainformatica. RIVERA, E. (2009). Formato html. Disponible http://www.asesoriainformatica.com/definiciones_f.htm

[14] GARCÍA BALUJA, W. (2004): Los sistemas detectores de intrusos. Formato pdf. Disponible http://www.criptored.upm.es/guiateoria/gt_m189d.htm

[15] The Honeynet Project (2008). Formato html. Disponible http://project.honeynet.org/

[16] MENGUAL GALÁN, L. (1998): Implementación de protocolos de seguridad. formato pdf. Disponible http://oa.upm.es/979/

[17] CAMERON, J., HERTEL, C., MASSA, A. , PAUL, C. Y REHMAN, R. (2003): Intrusion detection systems with snort advaced IDS techniques using snort, apache, mysql, php and acid. Formato pdf. Disponible http://www.informit.com/content/downloads/perens/0131407333.pdf

[18] JOHO, D. (2004, diciembre): Active honeypots. Formato pdf. Disponible http://www.cybertesis.cl/n-mundo.html

[19] CÓRDOBA, J., RICARDO, L., ORTIZ, D. Y PUENTES D. (2005): Los IDS y los IPS: Una comparación práctica. Formato doc. Disponible http://www.criptored.upm.es/guiateoria/gt_m142w.htm

[20] URBINA: Descripción general de los sistemas de detección de intrusos. Formato pdf. Disponible catarina.udlap.mx/u_dl_a/tales/documentos/lem/urbina_p_j/capitulo2.pdf

[21] CAMPO GIRALTE, L. (2001): Diseño de sistemas distribuidos de detección de anomalías de red. Formato pdf. Disponible is.ls.fi.upm.es/doctorado/Trabajos20052006/Campo.pdf

[22] VILLALÓN HUERTA, A. (2005, mayo): Sistemas de detección de intrusos. Formato pdf. Disponible http://www.criptored.upm.es/guiateoria/gt_m209g.htm

[23] LÓPEZ, O., PRIETO PARRA, M. Y ACOSTA, B. (2001): Arquitectura y comunicaciones en un sistema de detección de intrusos. Formato pdf. Disponible http://www.govannom.org/modules.php?name=Seguridad&d_op=getit&lid=84

[24] MARICHAL ALCANTARA, L., ZARAGOZI JIMENO, J. Y BALUJA GARCÍA, W. (2007): Solución de cortafuegos basada en la integración de herramientas de software libre: Snort e Iptables. Formato pdf. Disponible http://www.criptored.upm.es/guiateoria/gt_m189g.htm

[25] GARCÍA OREA, A. (2000): Presente y futuro de los IDS. Formato pdf. Disponible http://www.neurosecurity.com/whitepapers.php

[26] MUKHERJEE, B., HEBERLEIN, T. Y LEVITT, K. (1997): Network intrusion detection. Formato pdf. Disponible http://seclab.cs.ucdavis.edu/papers/mhl94.pdf

[27] WALC (2004): Sistemas de detección de intrusos. Formato pdf.

[28] GARUBA, M., LIU, C. Y FRAITES, D. (2008): Intrusion Techniques: Comparative study of network intrusion detection systems. Formato pdf.

[29] BOER, P. Y PELS, M. (2005, febrero): Host-based intrusion detection systems (HIDS). Formato pdf. Disponible http://staff.science.uva.nl/~delaat/snb-2004-2005/p19/presentation.pdf

[30] MCHUGH, J. (2006, octubre) "Intrusion and intrusion detection". Business Source Premiere Database.1,14-36

[31] ICSALABS (2008, agosto): Network intrusion prevention systems certification testing report. Formato pdf. Disponible http://www.icsalabs.com/icsa/docs/html/communities/nips/certifiedproducts/FortiGate_NIPS_report_

[32] CHUVAKIN, A. (2006) "Monitoring IDS". Business Source Premiere Database. 6,12-16

[33] CAPPELLI, D., DESAI, A., MOORE, A., SHIMEALL, T., WEAVER, E. Y WILLKE, B. (2006, noviembre): Management and education of the risk of insider threat (MERIT): System dynamics modeling of computer system sabotage. Formato pdf. Disponible http://www.cert.org/archive/pdf/merit.pdf

[34] PORWAL, P. (2005, abril): Evading/Attackin NIDS. Formato pdf.

[35] HANDLEY, M., PAXSON, V. Y KREIBICH, C. (2002): Network intrusion detection evasion, traffic normalization and end-to-end protocol semantics. Formato pdf,

[36] ARBOLEDA, A., BEDÓN, C. PÉREZ, F. Y VIVAS, L.(2006): El IDS ante un ataque de TCP RESET. Formato doc. Disponible http://www.criptored.upm.es/guiateoria/gt_m124e.htm

[37] GALVÁN RODRIGUEZ, A., PARRA, M. Y MEX, C. (2005): Detección y tolerancia a intrusos en un sistema distribuido. Formato pdf. Disponible http://speech.mty.itesm.mx/cybersecurity/res_proj_01.html

[38] NING,P. Y XU,D. Adapting query optimization techniques for efficient intrusion alert correlation. Formato pdf. Disponible http://www.germinus.com/sala_prensa/articulos/Correlacion%20Eventos%20Seguridad.pdf

[39] CORLETTI, A. Y BRAVO VICENTE, J. Generación de ataques/Detección con NIDS. Formato doc. Disponible http://www.criptored.upm.es/guiateoria/gt_m292c.htm

[40] CUPPENS, F. Y MIEGE, A. (2002): Alert correlation in a cooperative intrusion detection framework. Formato pdf.

[41] FRANCO, A. (2003, abril): Arquitectura avanzadas para los sistemas de detección de intrusos. Formato pdf.

[42] DESAI, N. (2003, febrero): Intrusion Prevention Systems: The next step in the evolution of IDS. Formato pdf. Disponible http://www.securityfocus.com/printable/infocus/1670/

[43] TRIULZI, A. (2003): Intrusion detection systems and IPv6. Formato pdf, Disponible http://www.alchemistowl.org/arrigo/Papers/SPI2003-IDS-and-IPv6.pdf

[44] MUKHERJEE, B., HEBERLEIN, L. Y LEVITT, K. (1994, junio): Network intrusion detection. Formato pdf. disponible http://seclab.cs.ucdavis.edu/papers/mhl94.pdf

[45] GRAMAJO, A. (2005, septiembre): Introducción a conceptos de IDS y técnicas avanzadas con snort. Formato pdf. Disponible http://www.baicom.com/eventos/010905.pdf.

[46] LUIS, R. (2009, FEBRERO): Encabezado IPv6. Formato html. Disponible http://ipref.wordpress.com/2009/02/20/ipv6-header/

[47] JULIA, R. (2007, SEPTIEMBRE): Optimización a lo ancho . Formato pdf. Disponible http://www.revistaitnow.com/pdfs/Telefonia_OpenSource_ITNOW27.pdf

Anexo 1.1

8 de septiembre de 2009

De la amplia gama de virus que hay se puede ver que en PANDA SECURITY[04] se tiene las siguientes clasificaciones:

1. Virus residentes

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, etc. Estos virus sólo atacan cuando se cumplen ciertas condiciones definidas previamente por su creador (por ejemplo, una fecha y hora determinada). Mientras tanto, permanecen ocultos en una zona de la memoria principal, ocupando un espacio de la misma, hasta que son detectados y eliminados. Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

2. Virus de acción directa

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos. Además, también realizan sus acciones en los directorios especificados dentro de la línea PATH (camino o ruta de directorios), dentro del fichero AUTOEXEC.BAT (fichero que siempre se encuentra en el directorio raíz del disco duro). Los virus de acción directa presentan la ventaja de que los ficheros afectados por ellos pueden ser desinfectados y restaurados completamente.

3. Virus de sobreescritura

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles. También se difer-

encian porque los ficheros infectados no aumentan de tamaño, a no ser que el virus ocupe más espacio que el propio fichero (esto se debe a que se colocan encima del fichero infectado, en vez de ocultarse dentro del mismo). La única forma de limpiar un fichero infectado por un virus de sobreescritura es borrarlo, perdiéndose su contenido. Algunos ejemplos de este tipo de virus son: Way, Trj.Reboot, Trivial.88.D.

4. Virus de boot o de arranque

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador. Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los disquetes. Cuando un ordenador se pone en marcha con un disquete infectado, el virus de boot infectará a su vez el disco duro. Los virus de boot no pueden afectar al ordenador mientras no se intente poner en marcha a éste último con un disco infectado. Por tanto, el mejor modo de defenderse contra ellos es proteger los disquetes contra escritura y no arrancar nunca el ordenador con un disquete desconocido en la disquetera. Algunos ejemplos de este tipo de virus son: Polyboot.B, AntiEXE.

5. Virus de macro

El objetivo de estos virus es la infección de los ficheros creados usando determinadas aplicaciones que contengan macros:documentos de Word (ficheros con extensión DOC), hojas de cálculo de Excel (ficheros con extensión XLS), bases de datos de Access (ficheros con extensión MDB), presentaciones de PowerPoint (ficheros con extensión PPS), ficheros de Corel Draw, etc. Las macros son micro-programas asociados a un fichero, que sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas. Cuando se abre un fichero que contenga un virus de este tipo, las macros se cargarán de forma automática, produciéndose la infección. La mayoría de las aplicaciones que utilizan macros cuentan con una protección antivirus y de seguridad específica, pero muchos virus de macro sortean fácilmente dicha protección. Existe un tipo diferente de virus de macro según la herramienta usada: de Word, de Excel, de Access, de PowerPoint, multiprograma o de archivos RTF. Sin embargo, no todos los programas o herramientas con macros pueden ser afectadas por estos virus. Estos son algunos ejemplos: Relax, Melissa.A, Bablas, O97M/Y2K.

6. Virus de enlace o directorio

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos. Los virus de enlace o directorio alteran las direcciones que indican donde se almacenan los ficheros. De este modo, al intentar ejecutar un programa (fichero con extensión EXE o COM) infectado por un virus de enlace, lo que se hace en realidad es ejecutar el virus, ya que éste habrá modificado la dirección donde se encontraba originalmente el programa, colocándose en su lugar. Una vez producida la infección, resulta imposible localizar y trabajar con los ficheros originales.

7. Virus encriptados

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran o encriptan a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar. Estos son algunos ejemplos de este tipo de virus: Elvira, Trile.

8. Virus polimórficos

Son virus que en cada infección que realizan se cifran o encriptan de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas por lo que suelen ser los virus más costosos de detectar. Algunos ejemplos de este tipo de virus son: Elkern, Marburg, Satan Bug, Tuareg.

9. Virus multipartites

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc. Se consideran muy peligrosos por su capacidad de combinar muchas técnicas de infección y por los dañinos efectos de sus acciones. Algunos ejemplos de estos virus son: Ywinz.

10. Virus de fichero

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos. La mayoría de los virus existentes son de este tipo.

11. Virus de compañía

Son virus de fichero que al mismo tiempo pueden ser residentes o de acción directa. Su nombre deriva de que "acompañan" a otros ficheros existentes en el sistema antes de su llegada, sin modificarlos como hacen los virus de sobreescritura o los residentes. Para efectuar las infecciones, los virus de compañía pueden esperar ocultos en la memoria hasta que se lleve a cabo la ejecución de algún programa, o actuar directamente haciendo copias de sí mismos. Algunos ejemplos de este tipo de virus son: Stator, Asimov.1539, Terrax.1069.

12. Virus de FAT

La Tabla de Asignación de Ficheros o FAT es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador. Los daños causados a la FAT se traducirán en pérdidas de la información contenida en ficheros individuales y en directorios completos.

13. Gusanos (Worms)

De un modo estricto, los gusanos no se consideran virus porque no necesitan infectar otros ficheros para reproducirse. A efectos prácticos, son tratados como virus y son detectados y eliminados por los antivirus. Básicamente, los gusanos se limitan a realizar copias de sí mismos a la máxima velocidad posible, sin tocar ni dañar ningún otro fichero. Sin embargo, se reproducen a tal velocidad que pueden colapsar por saturación las redes en las que se infiltran. Las infecciones producidas por estos virus casi siempre se realizan a través del correo electrónico, las redes informáticas y los canales de Chat (tipo IRC o ICQ) de Internet. También pueden propagarse dentro de la memoria del ordenador. Estos son algunos ejemplos de gusanos: PSWBugbear.B, Lovgate.F, Trile.C, Sobig.D, Mapson.

14. Troyanos o caballos de Troya

Técnicamente, los Troyanos tampoco se consideran virus, ya que no se reproducen infectando otros ficheros. Tampoco se propagan haciendo copias de sí mismo como hacen los gusanos. A efectos prácticos, son tratados como virus y son detectados y eliminados por los antivirus. El objetivo básico de estos virus es la introducción e instalación de otros programas en el ordenador, para permitir su control remoto desde otros equipos. Su nombre deriva del parecido en su forma de actuar de los astutos griegos de la mitología: llegan al ordenador

como un programa aparentemente inofensivo. Sin embargo, al ejecutarlo instalará en nuestro ordenador un segundo programa, el troyano. Los efectos de los Troyanos pueden ser muy peligrosos. Al igual que los virus, tienen la capacidad de eliminar ficheros o destruir la información del disco duro. Pero además pueden capturar y reenviar datos confidenciales a una dirección externa o abrir puertos de comunicaciones, permitiendo que un posible intruso controle nuestro ordenador de forma remota. Estos son algunos ejemplos de Troyanos: IRC.Sx2, Trifor.

15. Bombas lógicas

Tampoco se consideran estrictamente virus, ya que no se reproducen. Ni siquiera son programas independientes, sino un segmento camuflado dentro de otro programa. Tienen por objetivo destruir los datos de un ordenador o causar otros daños de consideración en él cuando se cumplen ciertas condiciones. Mientras este hecho no ocurre, nadie se percata de la presencia de la bomba lógica. Su acción puede llegar a ser tremendamente destructiva.

16. Virus falsos

Al margen de las divisiones anteriores, existen ciertos tipos de mensajes o programas que en ciertos casos son confundidos con virus, pero que no son virus en ningún sentido. El principal componente de este grupo son los hoaxes o bulos. Los hoaxes no son virus, sino mensajes de correo electrónico engañosos, que se difunden masivamente por Internet sembrando la alarma sobre supuestas infecciones víricas y amenazas contra los usuarios. Los hoaxes tratan de ganarse la confianza de los usuarios aportando datos que parecen ciertos y proponiendo una serie de acciones a realizar para librarse de la supuesta infección. Si se recibe un hoax, no hay que hacer caso de sus advertencias e instrucciones: lo más aconsejable es borrarlo sin prestarle la más mínima atención y no reenviarlo a otras personas. Como se muestra hay una gran variedad de ataques que han surgido y seguirán surgiendo de acuerdo al avance tecnológico y mejoramiento de técnicas por parte de estos cybercriminales, queda claro que los virus son programas que atacan al computador o a la red a la que pertenecen, pero no todos los ataques se dan con un virus el cual se realiza de forma automática, también existen ataques dirigidos o guiados por usuarios, de los cuales veremos todos estos tipos de ataques a continuación para entenderlos mucho mejor.

Anexo 2.1

8 de septiembre de 2009

Como se puede ver a continuación los ataques se han clasificado de acuerdo a su manera de proceder o comportamiento de los cuales se pueden agrupar en dos grupos, los ataques pasivos y los ataques activos como se muestra en la figura 1.

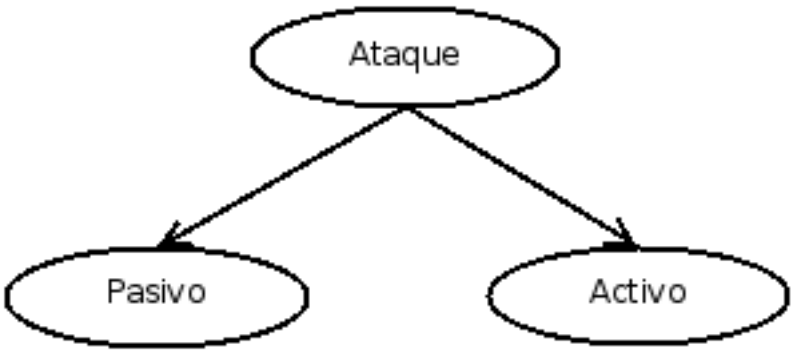


Figura 1 Tipo de ataques MENGUAL[16].

1. Los ataque pasivos

Tienen su lugar en la escucha o monitorización de una transmisión, también denominada revelación. Mediante está se llega a obtener la información contenida entre las unidades de datos que transmiten por la red y como un segundo objetivo el análisis de tráfico.

Dentro de este grupo tenemos (ver figura 2):

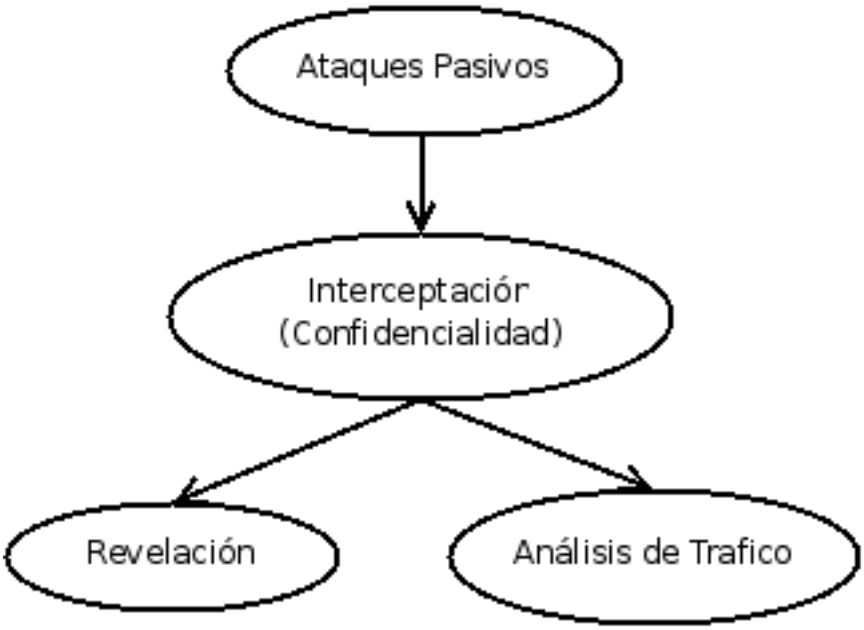


Figura 2: Ataques Pasivos MENGUAL[16].

1.1. Revelación

Afecta a los sistemas distribuidos convirtiéndolos en una amenaza frecuente, cuando se envía un email o un fichero se transporta por la red, la información susceptible o confidencial de este puede ser accedida por un intruso.

1.2. Análisis de Trafico

Aquí un tercero implementa una sonda en modo promiscuo entre las entidades, con la finalidad de descubrir información que luego pueda usar en contra de las entidades monitoreadas. En MENGUAL[16] dice que "El intruso podría determinar la localización y la identidad de las entidades que se comunican, podría observar la frecuencia y longitud de las unidades de datos intercambiadas, capturar palabras de paso, etc. Estas informaciones podrían ser útiles para analizar la naturaleza de la comunicación que está teniendo lugar.". Hay que tener en cuenta que ataques pasivos son muy difíciles de detectar por su naturaleza, ya que no hacen daño a las unidades de datos, razón por la cual no hay que enfocarse en la detección si no en la prevención de estas.

2. Los ataques activos

Tienen su lugar en la modificación de el flujo de unidades de datos, creación de unidades falsas o interrupción de la comunicación con la respectiva perdida

de la información que esta implica, Estos ataques activos llegan a afectar la disponibilidad de los recursos, la integridad y la autenticidad de las unidades de datos (ver figura 3).

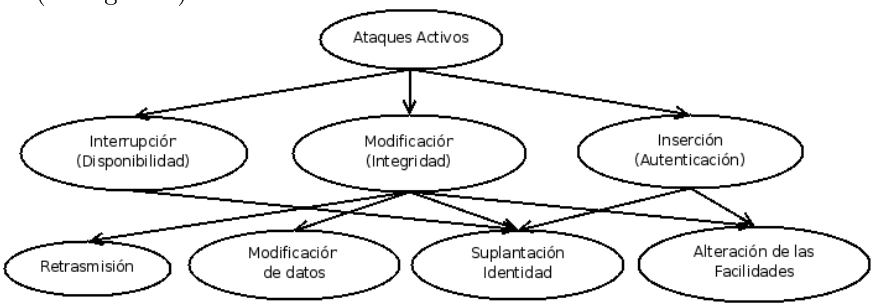


Figura 3: Ataques Pasivos MENGUAL[16].

Dentro de este grupo se tiene:

2.1. Interrupción

En este tipo de ataque el recurso ya no se encuentra disponible ya sea porque este es destruido o simplemente deja de estar disponible.

2.2. La suplantación de Identidad

Esta se da cuando una entidad pretende ser otra, al insertar o modificar información en un unidad de datos transmitida por la red. "Un intruso, por ejemplo, podría haber capturado en una comunicación orientada a conexiones las direcciones origen y destino, así como los números de secuencia de las unidades de datos intercambiadas. En un instante dado podría enviar una unidad de datos suplantado a una de las entidades que se comunican".MENGUAL[16]

2.3. La modificación de la información en tránsito

Esta funciona a la par entre la observación de la información que se esta transmitiendo y la inserción de datos que veremos a continuación. Inserción de datos: Este tipo de ataque puede llegar a ser complejo debido a los requisitos en tiempo real de ciertas aplicaciones. Ejemplo de esto es que un intruso llegue a alterar el funcionamiento normal de los dispositivos de red modificando la información en tránsito que tiene lugar a un protocolo de gestión, modificando los mensajes de un protocolo de relojes, podemos llegar a alterar la consideración de actualidad de dicho mensajes, o al cambiar el número de secuencia de los mensajes en las comunicaciones que están orientadas a la conexión.

2.4. Retrasmisión

Esta funciona en la captura pasiva de datos para su posterior retransmisión, produciendo un efecto no deseado y estos pueden afectar a la integridad del flujo

de información en una comunicación orientad a la conexión. Ejemplo de esto es la retrasmisión de transferencia de fondos cifrados causando múltiples sumas en las cantidades transferidas o la retrasmisión de la secuencia de comportamientos, este tipo de ataque es sencillo de ejecutar a acepción de algunos casos en los que se desea reproducir códigos de redundancia.

2.5. La Alteración de las facilidades o recursos de comunicaciones

Funciona de una manera especifica al deteriorar la comunicaciones entre las unidades de red, puede darse de dos maneras la primera al borrar todas las unidades de datos que se dirigen a un destino en particular o al introducir unidades de datos que van a entorpecer el trabajo que tiene la red al darles un trabajo extra. Como se puede ver en cuestión de ataques tenemos una amplia gama de ellos y entender estos nos permitirá entender la manera que se han desarrollado soluciones para hacerles frente a estos. ante los ataques también podemos hallar las respuestas activas que como se dicen se aplican a cualquier función que altera o bloquea el tráfico de red como resultado de la ocurrencia de la detección de una intrusión. De la cual obtenemos un concepto interesante que esta en relación con el tema IDS en el cual en MENGUAL[16] nos da la pauta que la diferencia fundamental entre la respuesta activa de los IDS y los IPS radica en que ningún mecanismo de repuesta que no esté en línea con un tráfico de ataque está en condiciones de detenerlo antes de alcanzar su objetivo. El IDS puede reaccionar de varias formas, pero algunos de sus métodos, Los cuales no están basados en dispositivos en línea, crearán una carrera entre el tráfico maligno y la respuesta, la cual puede llegar a ganar el primero dependiendo de la cantidad de paquetes necesarios para realizar el ataque.

Anexo 3.1

8 de septiembre de 2009

1. Ejemplos de configuración.

En CÓRDOBA[19] se da un analisis del funcionamiento de in IDS por software "Snort" el cual se verá a continuación.

Como IDS, se utilizó Snort 2.3.0 el cual fue brevemente comentado al final de la segunda sección del presente artículo.

Snort es un NIDS basado en detección de firmas relativamente liviano y altamente configurable. Su instalación no es compleja requiriendo únicamente la instalación previa de la librería de captura de paquetes Libpcap y la librería de expresiones regulares PCRE.

La configuración de Snort esta concentrada principalmente en el archivo snort.conf, ubicado usualmente en la carpeta etc del sistema o de la instalación. En este archivo se definen todas las variables correspondientes a la red sobre la que opera el IDS y se referencian todos los archivos de reglas para el motor de detección (uno de los componentes arquitectónicos de Snort para la detección de intrusiones).

En particular, en snort.conf, se definen las variables $EXTERNAL_NET (direcciones de las redes externas), $HOME_NET (dirección CIDR de la intranet), $HTTP_SERVERS (direcciones de los Servidores Web en la intranet), entre otras.

Por su lado, como IPS se utilizó Snort_inline 2.3.0 RC1, un IPS inline cuya instalación fue más complicada que la del IDS.

Es preciso tener en cuenta que en su principio Snort_inline fue un desarrollo independiente de Snort, que se basó en este último para procesar el tráfico de red.

Desde su versión 2.3.0 Snort incorporó la funcionalidad inline como parte integral del proyecto. Para activar el modo IPS basta usar el modificador –enable-inline a la hora de configurar el script de instalación antes de compilar el código fuente de la aplicación.

Adicionalmente, Snort_inline -a diferencia de Snort- debe operar en modo bridge, lo que requiere activar esta funcionalidad antes de poder ejecutar el IPS.

Por otro lado, Snort_inline no toma los paquetes directamente de la NIC (Network Interface Card) por medio de Libpcap como lo hace Snort, sino de la cola de salida del firewall de Linux (IPTables). Por esto es necesario configurar

IPTables de tal manera que enfile los paquetes entrantes en la susodicha cola para que puedan ser procesados por Snort_inline.

Finalmente, el kernel de Linux no permite ejecutar simultáneamente IPTables y Bridge, por lo que es necesario parcharlo con Ebtables que es una herramienta de filtrado para firewalls en modo bridge.

2. El experimento: DoS (Negación del servicio) sobre Apache 2.0.52.

El ataque consistió en una negación de servicio sobre el servidor Apache 2.0.52 a partir del envío de mensajes HTTP con peticiones (request) mal formadas de la siguiente manera:

GET / HTTP/1.0\n
[espacio] x 8000\n
[espacio] x 8000\n
[espacio] x 8000\n

El ataque se obtuvo está escrito en C y utiliza varios hilos para aumentar la cantidad de tráfico enviado a la víctima.

3. Detección del ataque con el IDS.

A partir de la descripción del ataque presentada anteriormente, se compuso la siguiente regla con el fin de detectarlo en el IDS:

alert tcp $EXTERNAL_NET any ->$HTTP_SERVERS $HTTP_PORTS (pcre:"/\x20{6000}/";msg:"6000 espacios contiguos detectados";)

Ésta regla tiene como función alertar sobre cualquier datagrama IP, que provenga de cualquier dirección IP, hacia cualquiera de los servidores HTTP (en el caso del experimento la dirección IP de V: 192.168.0.105), sobre los puertos HTTP definidos en la variable $HTTP_PORTS en snort.conf (80 y 443). El payload de datos debe contener 6000 espacios seguidos para que se cumpla la regla y se alerte sobre la posible intrusión.

Una vez se escribió la regla y se ejecutó el IDS en B, se inició el ataque desde A, monitoreando desde M el estado de V, en particular, su uso de memoria RAM.

Entre 03/16-00:51:02.609266 y 03/16-01:02:53.836897 se ejecutó el ataque con los siguientes resultados:

El IDS se ejecutó de tal manera que almacenó un registro detallado de los paquetes capturados, encontrándose que la víctima recibió 101463 peticiones HTTP mal formadas en el lapso de tiempo en el que se ejecutó el ataque. La captura de una petición se muestra a continuación:

=+
03/16-00:51:02.611854 192.168.0.125:32771 ->192.168.0.105:80
TCP TTL:64 TOS:0x0 ID:58731 IpLen:20 DgmLen:67 DF
AP Seq: 0x916637C2 Ack: 0xC0BCFFCC Win: 0x5B4 TcpLen: 32

TCP Options (3) =>NOP NOP TS: 512761 1220540
47 45 54 20 2F 20 48 54 54 50 2F 31 2E 30 0A GET / HTTP/1.0.
=+
03/16-00:51:02.613799 192.168.0.125:32771 ->192.168.0.105:80
TCP TTL:64 TOS:0x0 ID:58733 IpLen:20 DgmLen:1500 DF
A* Seq: 0x916637D1 Ack: 0xC0BCFFCC Win: 0x5B4 TcpLen: 32
TCP Options (3) =>NOP NOP TS: 512763 1220540
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
. . . (Siguen 87 líneas con 16 espacios (0x20))
=+

En la anterior captura se ve claramente la petición HTTP (GET / HTTP/1.0), seguida por una cantidad elevada de espacios (0x20).

Por su parte, el motor de detección del IDS detectó y clasificó los datagramas involucrados con las peticiones mal formadas, generando una entrada por cada uno de ellos en el log de alertas (ubicado usualmente en /var/log/snort/alert). Una de tales alertas se muestra a continuación:

[**] [1:0:0] 6000 espacios contiguos detectados [**]
[Priority: 0]
03/16-00:53:14.044895 192.168.0.125:32771 ->192.168.0.105:80
TCP TTL:64 TOS:0x0 ID:60225 IpLen:20 DgmLen:1500 DF
A* Seq: 0x9AB88C02 Ack: 0xc0EEF748 Win: 0x5B4 TcpLen: 32
TCP Options (3) =>NOP NOP TS: 177101 526711

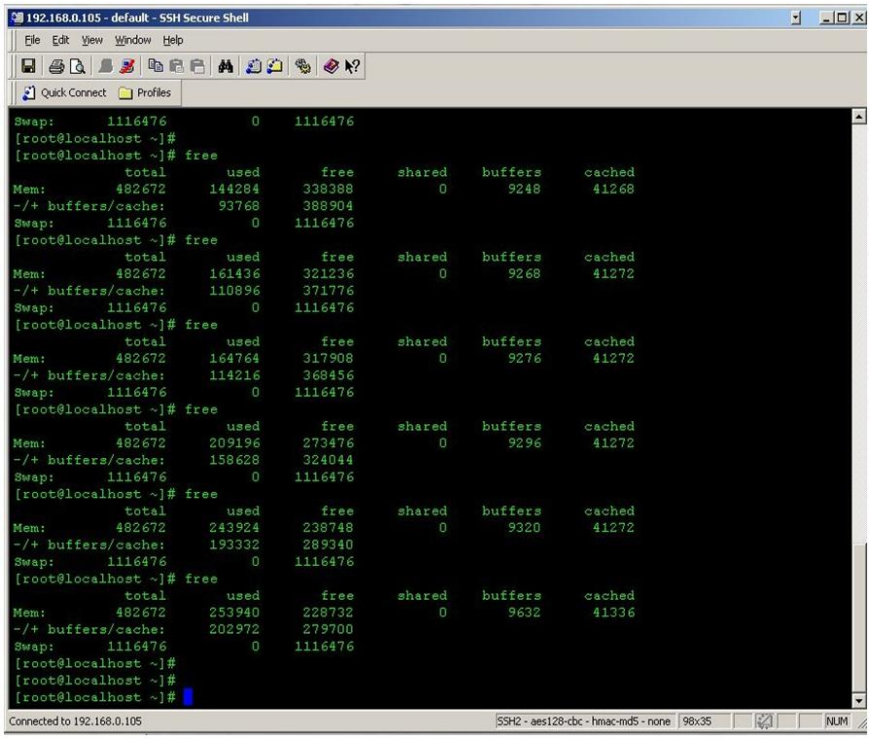


Figura 1. Estado de memoria de V CÓRDOBA[19].

Al ejecutarse el ataque, el consumo de memoria RAM aumento considerablemente en V como se muestra en la Figura 1.

Luego de varios minutos de ejecución del ataque desde A (Figura 2), no fue posible acceder al servidor Web, como se ve en la Figura 3, ni seguir verificando el estado de uso de la memoria de V vía SSH.

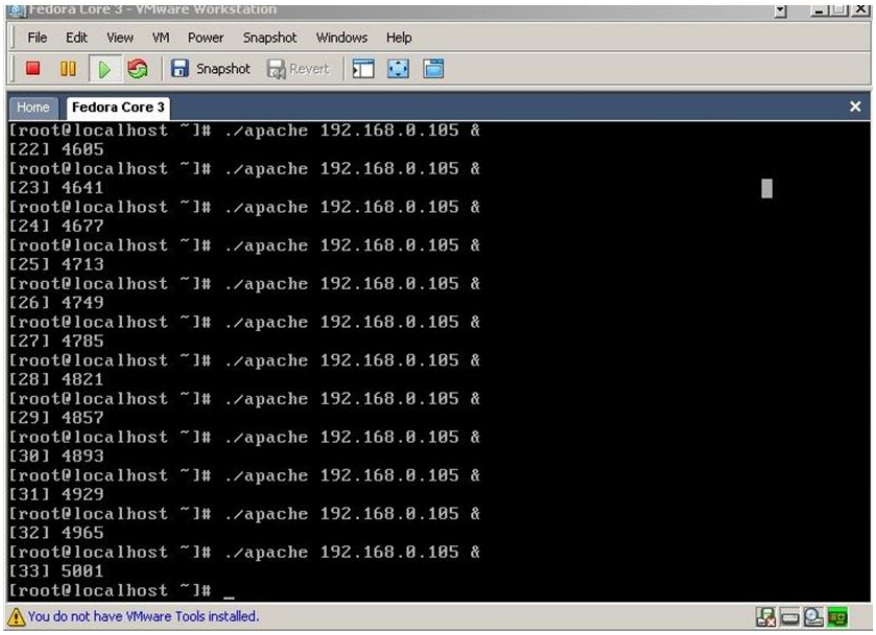


Figura 2. Ejercicio del ataque desde A CÓRDOBA[19].

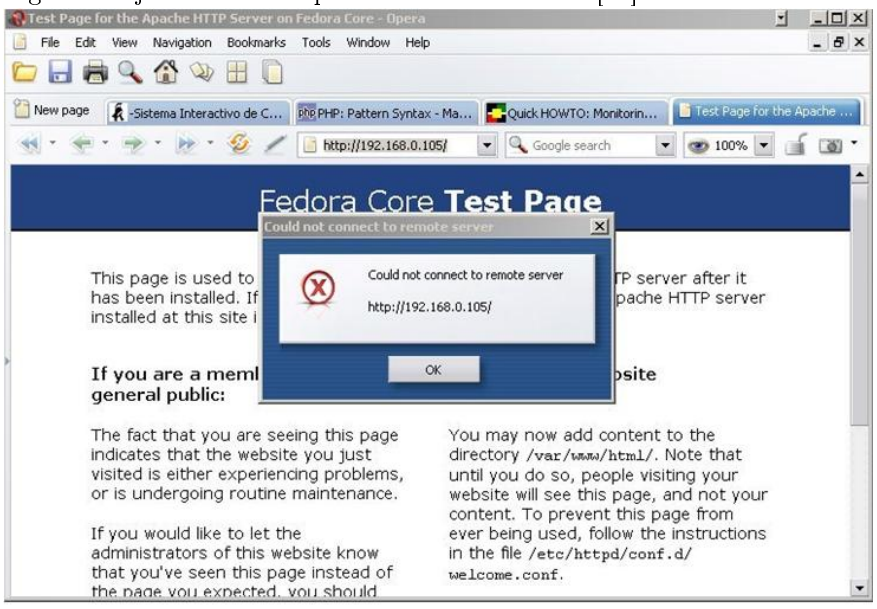


Figura 3. Error en el acceso al servidor Web CÓRDOBA[19].

En GRAMAJO[45] se da otros ejemplos que se verá a continuación. Se desea generar una alerta cuando se intenta loguear un usuario "root" al ftp

alert tcp any any ->any any 21 \

(content: "user root";)

Con esta regla se tiene el problema que el protocolo acepta variantes como se muestra en la figura 37.

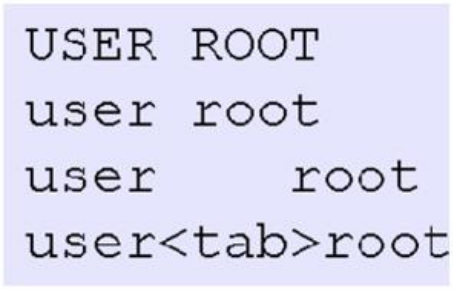


Figura 4. Otras maneras de logearse como usuario "root" GRAMAJO[45].

Para evitar el problema descrito anteriormente se puede usar una regla mejorada como se verá a continuación.

alert tcp any any ->any 21 \
(flow: to_server, established; \
content: "root"; \
pcre: "/user\s+root/i";)

En esta regla se usa Flow la cual se encarga de verificar que el tráfico este yendo hacie el server establecido y Pcre para expresiones regulares anteriormente nombrada.

4. Snort como un IPS.

Snort puede llegar a ser un examinador de logs mediante la herramienta SnortGuardian y puede llegar a armar reglas que bloqueen o rechacen las conexiones de acuerdo a los patrones utilizando FlexResp o Inline. Para el siguiente ejemplo aplicado a MySQL se modificara paquetes que pueden llegar a ser peligrosos por la naturaleza de algunos comandos que se verá a continuación.

UNION SELECT
LOAD_FILE ...
LOAD DATA INFILE ...
SELECT ... INTO OUTFILE ...
BENCHMAR ...
UFD
DROP DATABASE ...

Utilizando Inline, eliminamos el drop database como respuesta ante un posible ataque.

alert tcp any any <>any any \
(msg: "mysql replace"; \
content: "drop database"; \
replace: "select ´LAMER´";)

Obteniendo la respuesta que se muestra en la figura 5. a continuación.

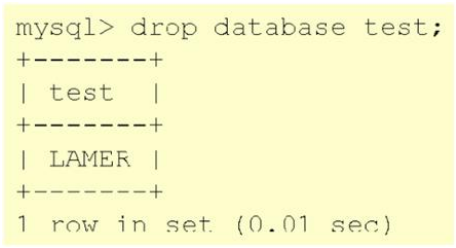


Figura 5. Resultado del comando drop database en msql GRAMAJO[45].
Para un mayor entendimiento de snort consultar CAMERON[17].

Anexo 4.1

September 8, 2009

1 Ejemplo 2

Especificación de ataques en LAMBDA.

Los principios básicos de este leguaje son cinco campos que se presentan a continuación.

- Pre-Condición del ataque: Es la condición lógica que especifica las condiciones que se tiene que cumplir para que el ataque tenga éxito.
- Post-Condición del ataque: Es la condición lógica que especifica el resultado del ataque cuando este tiene éxito.
- Escenario de ataque: Es la combinación de eventos que el atacante realiza para ejecutar el ataque.
- Detección de escenario: Es la combinación de eventos que son necesarias para la detección de un ataque.
- Verificación de escenario: Es una combinación de eventos que se lanzan para comprobar que el ataque allá tenido éxito.

A continuación se explicara el conjunto de predicados que se usaran para el ataque;

- Un predicado que especifica el nivel de acceso del intruso en el sistema destino : Ej. access_level (bad_guy, 192,168.12.3, local) Se refiere que alguien con el nombre bad_guy tiene acceso local al host 192.168.12.3 con posibles valores de acceso remoto a local, user, root and physical.
- Un conjunto de predicados para especificar los efectos de los ataques contra el sistema de destino. Ej. deny_of_service (192.168.12.3) el cual puede causar una negación en el servicio sobre el host 192.168.12.3.
- Predicados para especificar el estado de las condiciones de el origen o metas del sistema. Ejm. use_service(192.168.12.3, showmount) Especifica que el servicio showmount esta activo en el host 192.168.12.3.

Estos predicados son combinados usando un conectivo lógico denotado por coma "," y por negación "not". En la figura 1, se ofrece 4 ejemplos de ataques en LAMBDA: NFS mount, Modificación del archivo .rhost, TCPScan y Winnuke.

```
<?xml version="1.0" encoding="UTF-8"?>
<attack attackid="MIR-0163">
<name>mount partition</name>
<pre>access_level(Source_user,Target_address,remote),
      mounted_partition(Target_address,Partition),
</pre>
<post>can_access(Source_user,Partition)
</post>
<scenario>Action</scenario>
<cond_scenario>
 script(Action,'mount -t nfs $Partition:$Target_address $Partition')
</cond_scenario>
<detection>Alert</detection>
<cond_detection>alert(Alert),
                source(Alert,Source),
                source_user(Source,Source_user),
                target(Alert,Target),
                target_node(Target,Target_node),
                address(Node,Target_address),
                classification(Alert,"MIR-0163")
</cond_detection>
</attack>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<attack attackid="MIR-0164">
<name>modification du .rhost</name>
<pre>access_level(Source_user,Target_address,remote),
      can_access(Source_user,Partition),
      owner(Partition,Target_User),
      userid(Target_user,Target_address,Userid),
</pre>
<post> access_level(Source_user,Target_address,user)
</post>
<scenario>Action</scenario>
<cond_scenario>script(Action,'cat "++" > .rhost')</cond_scenario>
<detection>Alert</detection>
<cond_detection>alert(Alert),
                source(Alert,Source),
                source_user(Source,Source_user),
                target(Alert,Target),
                target_node(Target,Target_node),
                address(Target_node,Target_address),
                classification(Alert,"MIR-0164")
</cond_detection>
</attack>
```

Lambda attack MIR-0163-NFSMount y Lambda attack MIR-0163-Modification of -rhost Lambda attack MIR-0036-Winnuke y Lambda attack MIR-0074-TCPScan

```
<?xml version="1.0" encoding="UTF-8"?>
<attack attackid="MIR-0036">
<name>winnuke sur la cible</name>
<pre>use_os(Target_address,windows),
        state(Target_address,available),
        dns_server(Target_address)
</pre>
<post>deny_of_service(Target_address)
</post>
<scenario>Action</scenario>
<cond_scenario>
   script(Action,'winnuke $Target_address')
</cond_scenario>
<detection>Alert</detection>
<cond_detection>alert(Alert),
                source(Alert,Source),
                source_node(Source,Source_node),
                address(Source_node,Source_address),
                target(Alert,Target),
              target_node(Target,Target_node),
              address(Target_node,Target_address),
              classification(Alert,"MIR-0036")
</cond_detection>
</attack>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<attack attackid="MIR-0074">
<name>tcpscan sur la cible</name>
<pre>use_soft(Source_address,tcpscan),
      use_service(Target_address,Target_service),
     service_type(Target_service,tcp)
</pre>
<post>
  knows(Source_user,use_service(Target_address,Target_service))
</post>
<scenario>Action</scenario>
<cond_scenario>script(Action,'tcpscan $Target_address')
</cond_scenario>
<detection>Alert</detection>
<cond_detection>alert(Alert),
                source(Alert,Source),
                source_node(Source,Source_node),
                address(Source_node,Source_address),
                source_user(Source,Source_user),
                target(Alert,Target),
                target_node(Target,Target_node),
                target_service(Target,Target_service),
                classification(Alert,"MIR-0074")
</cond_detection>
</attack>
```

Figura 1. Especificaciones del ataque en Lambda CUPPENS[40].

Lo que se puede apreciar con una letra mayúscula corresponde a una variable y el resto a una constante. Por ejemplo en el ataque NFS se puede apreciar las siguientes instrucciones access_level(Source_user, Target_address, remote), mounted_partition(Target_address, Partition) que quiere decir que para llevar a cabo un ataque NFS, el intruso Source_user tiene que tener un acceso remoto a una meta cuya dirección IP es Target_address y Partition debe ser un mounted partition. La post condición de este ataque dice:

1.0.1 can_access(Source_user, Partition)

Donde el intruso Source_user obtiene un acceso en mounted partition. Hay que tener en cuenta que la razón de un ataque a veces es simplemente para la obtención de conocimiento sobre un sistema destino, como se verá a continuación en los ataques TCPScan que generalmente se los utiliza como un escenario a los ataques más globales, se explicara a continuación las sentencias de este. Ejm. Si bad_guy es el atacante en las sentencias (bad_guy, use_service (192.168.12.3, ´netbios´)) da a referir que bad_guy conoce que el servicio NetBios está activo en el sistema cuya dirección IP es 192.168.12.3. Para los otros campos de descripción de un ataque LAMBDA que corresponden a los escenarios de ataque, detección y verificación se representará por situaciones elementales como se ejemplefica a continuación:

- <scenario>Action</scenario>

  Para especificar que Action es el único evento que corresponde al escenario del ataque.

- <detection>Alert</detection>

  Para especificar que Alert es el único evento que corresponde al escenario del detección. Finalmente, las condiciones que aparecen en los campos cond_scenario y cond_detection son utilizadas para formular una descripción de los eventos especificados en el escenario y los campos de detección. El campo cand_scenario es generalmente especificado en el uso de script donde el intruso realiza un ataque. El campo cond_detection es utilizado para describir los principales atributos de la descripción que esperamos cuando se produce el ataque. Ahora para la representación de los modelos lógicos de alertas se tiene las siguientes expresiones: alert(Alert), classification(Alert,"MIR-0163"), source(Alert, Sorce), source_user(Source,Source_user) Especifica que la alerta es analert, cuya clasificación es "mIR-0163" y el origen debe coincidir con una variable de origen. El usuario asociado a esta variable de origen es otra variable de origen Source_user. Esta descripción permite formular las limitaciones de los distintos campos de un alerta y las variables utilizadas en la pre_condition y post_condition de la descripción de un ataque.

Ya establecida la descripción del ataque se procederá a la descripción de la correlación de datos que se logra mediante los siguientes predicados.

- attack_correlation (Attack1, Attack2): Aquí el Ataque 1 "Attack1" puede ser correlacionado con el Ataque2 "Attack2", es decir que el intruso inmediatamente del Ataque 1 puede realizar el Ataque 2. Ejm. Para attack_correlation ("MIR-0066","MIR-0162") este muestra que es posible correlacionar el ataque "MIR-0066" (que corresponde a "rpcinfo") con el ataque "MIR-0162" (que corresponde a "showmount"). Esto se debe a que el ataque "rpcinfo" permite al intruso saber si el servicio "showmount" está activo. Hay que tener en cuenta que la correlación de datos de attack_correlation ("MIR-0066","MIR-0162") es válida ya que entendemos ambos tipos de ataques son parte de un ataque más general, razón por la cual si esto no es así no tendría caso correlacionar estas alertas.

En vista del posible caso de fallo que se puede presentar en la correlación de datos se ha introducido el siguiente predicado.

- alert_correlation (Alert1, Alert2): Aquí la alerta 1 puede ser correlacionada con la alerta 2 ya que este predicado es usado específicamente para definir las reglas de la correlación. Es en alert_correlation (Alert1, Alert2) donde las premisas de las condiciones de Alert1 y Alert2 tienen que llegar a satisfacer, que ambas están relacionadas dentro de un escenario de ataque para ser correlacionadas.

Ejm. En la figura 2 se presenta las reglas de correlación para dos alertas, respectivamente "MIR-0066" y "MIR-0162", donde las reglas de correlación contienen 3 partes, las 2 primeras proveen una descripción de las 2 alertas que se han correlacionado y la tercera parte de la premisa expresa las condiciones que tienen que satisfacer para correlacionar las 2 alertas. En el ejemplo anterior hay 2 condiciones que se verán a continuación.

- Condición 1: Los objetivos de las direcciones que figuran en las alertas deben ser iguales, lo que significa que tanto el ataque rpcinfo y el ataque showmount tienen que ser dirigidos al mismo objetivo.

- Condición 2: El nombre de servicio que figura en la alerta 1 tiene que ser igual al servicio "mountd", lo que significa que uno de los servicios entregados por rpcinfo es igual a "mountd".

Hay que tener en cuenta que hay una condición implícita para correlacionar las 2 alertas. La condición es que la Alerta 1 tiene que suceder antes de la Alerta 2, como se puede ver la condición no está directamente expresada en las reglas de correlación, pero es sistemáticamente comprobado cuando las reglas de correlación son evaluadas.

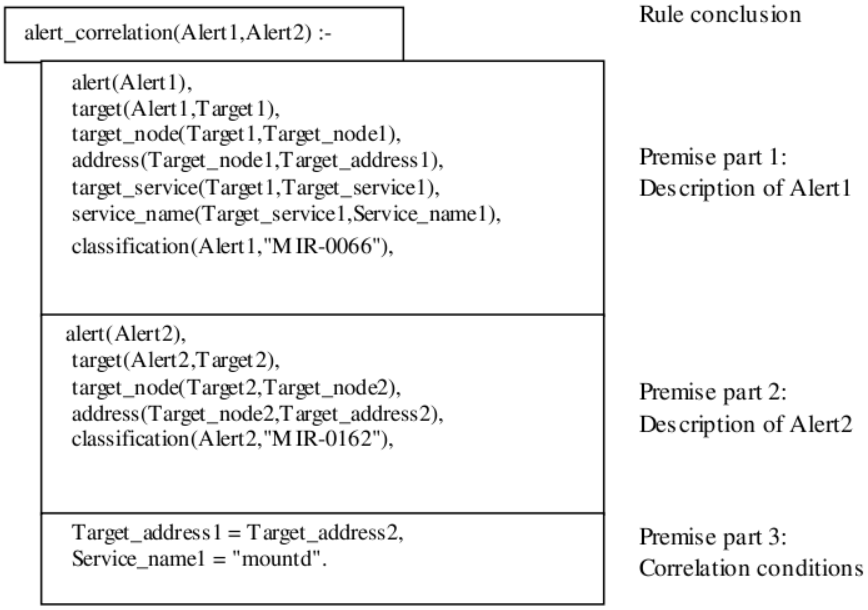


Figura 2: Ejemplo de regla de correlación entre las alertas correspondientes a los ataques. "MIR-0066"(rcpinfo) y "MIR-162"(showmount) CUPPENS[40].

Aunque la representación de un ataque es una parezca algo sencilla, puede resultar algo tediosa, para eso se puede propones la determinación de nuevas variables cuyo comportamiento pueda ser semi-explicito.

Anexo 5.1

September 8, 2009

Red de la Universitad Técnica Particular de Loja.