# IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED LOCAL DE LA GERENCIA DEPARTAMENTAL COLEGIADA DEL CAQUETÁ DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

ALVEIRO MEJIA LARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA
2017

# IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED LOCAL DE LA GERENCIA DEPARTAMENTAL COLEGIADA DEL CAQUETÁ DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

ALVEIRO MEJIA LARA

Trabajo de grado para optar al título de especialista en seguridad informática

ANIVAR CHAVES TORRES
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA
2017

Nota de Aceptación

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Florencia, 26-abr-2017

Se dedica este trabajo a todas las personas que directa o indirectamente me apoyaron para lograr esta meta.

# AGRADECIMIENTOS

A mi madre, que desde niño me inculcó el amor al estudio

A Bercy Montes, mi compañera de toda la vida, que siempre me apoyó y alentó para cumplir mis sueños, aunque eso significara muchos sacrificios para ella.

A Christian y Greisy, mis hijos, que desde muy niños debieron soportar mis largas horas sentado frente a un computador.

A la UNAD, que con su modalidad virtual y a distancia, me permitieron lograr este objetivo anhelado por tantos años.

A la Contraloría General de la República, por permitirme realizar la práctica.

CONTENIDO

pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

## GLOSARIO

ALIENVAULT: Gestión de Seguridad Digital Integrada (USM, por sus siglas en inglés), es una plataforma unificada diseñada para proporcionar y garantizar una defensa completa contra las amenazas de seguridad más recientes a un precio razonable, y enfocada especialmente a Pequeñas y Medianas Empresas.

ATAQUES POR FUERZA BRUTA: Se usa para acceder de forma ilícita a un sistema, ensayando una gran cantidad de composiciones posibles del teclado o contraseñas.

BACKBONE: Son conexiones troncales de Internet. Se ajusta de un número de routers gubernamentales y comerciales. Transportan datos mediante fibra óptica a través de los países y continentes.

BASE: (*Basic Analysis and Security Engine*): Esta aplicación suministra un *front-end* web para examinar y analizar las alertas originarias del sistema IDS Snort, por lo que marcha como un complemento a Snort.

BOTS: Programa informático que copia el comportamiento de un ser humano. Pueden elaborar cualquier orden, optimizando las técnicas de infección actualizando las vulnerabilidades que usan para propagarse.

CERT: (Equipo de Respuesta ante Emergencias Informáticas) Grupo de expertos que responden en el desarrollo de las medidas preventivas y de las correctivas ante fallos de seguridad en los sistemas de información.

CIBERNÉTICA: Ciencia que estudia las nociones interdisciplinarias de la estructura de los sistemas reguladores. Está relacionada con la teoría de sistemas y la teoría de control.

CIBERSEGURIDAD: Es parte de la seguridad que enlaza los delitos realizados en el ciberespacio y la prevención en la materialización de estos.

CÓDIGO MALICIOSO: Código informático que estimula a infracciones de seguridad para romper un sistema.

DNS: Es una nomenclatura jerárquica de nombres para computadoras, o cualquier recurso que se encuentre conectado a Internet o a una red privada.

EASYIDS: Es un sistema de detección de intrusos, muy fácil de instalar basado en Snort.

FIREWALLS: Sistema que acredita la información que sale de internet o red y bloquea o limita el paso al sistema de acuerdo a su disposición.

FTP: (Protocolo de Transferencia de Archivos) se fundamenta en la arquitectura cliente servidor y es un protocolo que se utiliza para la transferencia de archivos entre sistemas interconectados por una red.

HTTP: (Protocolo de transferencia de hipertexto) es un procedimiento de intercambio de información en la red, por el que es posible, entre otras cosas, trasladar las páginas web a una computadora.

H-IDS (Sistema de detección de intrusiones en el *host*). Es un IDS que revisa el computador en el que está instalado.

ICMP: (Protocolo de Mensajes de Control de Internet) Es usado para enviar mensajes de error, revelando que un servicio determinado no está accesible o que un router o host no puede ser hallado.

IDS (*Intrusion Detection System*) Sistema de Detección de Intrusos: es una herramienta de seguridad que se encarga de monitorear los sucesos que ocurren en un sistema informático en busca de ensayos de intrusión.

IPS (*Intrusion Prevention System*) sistema de prevención de intrusiones: Es un dispositivo o es un software que se utiliza para impedir que los intrusos accedan a sistemas mediante actividad dudosa o maliciosa. Esto se confronta a un sistema de detección de intrusiones (IDS), que únicamente efectúa detecciones y las notifica, pero no las evita.

LIDS: (*Linux Intrusion Detection System*, LIDS) Es el sistema de detección de intrusos Linux construido como un parche del *kernel* y una herramienta de revisión.

LOGS: Es un registro de las actividades de un sistema, que se almacena en un fichero de texto, al que se le van ampliando líneas a medida que se efectúan acciones sobre el sistema.

NETBIOS: Es la interfaz para el acceso a los servicios de la red, enlaza un Sistema Operativo de red con un hardware o dispositivo en particular.

NFS: (Sistema de archivos de red), en el Modelo OSI es un protocolo de nivel de aplicación. Es usado en sistemas de archivos distribuido en ambientes de red de área local.

N-IDS (Sistema de Detección de Intrusiones de red), Es un IDS que revisa la red sobre la cual está instalado.

NTOP: muestra el uso de la red en tiempo real. Se despliega una lista de hosts que actualmente usan la información de red y los muestran en relación con la IP (Protocolo de Internet) y *Fibre Channel* (FC) del tráfico generado por cada host. El tráfico es clasificado según host y protocolo.

OINKCODE: es una clave única inscrita a las cuentas de los usufructuarios que se registran en la página de Snort. Esta clave permite la descarga de los paquetes de reglas actualizadas.

OSSEC: (*Open Source SECurity* ) :Es un sistema de detección de intrusos basado en host de código abierto que ejecuta análisis de registro.

PATRIOT NG es una sencilla aplicación encargada de monitorear los sistemas Windows.

PHISHING: (Suplantación de identidad) es un delito informático el cual se comete usando una clase de ingeniería social en la cual se adquiere información sensible de manera fraudulenta, engañando a las personas.

PROXY: Es un servidor que se usa para intermediar entre las solicitudes de recursos que se efectúan de un cliente a otro servidor.

RCP: (*Remote Procedure Call*) este protocolo admite que un programa de computador realice un código en otra máquina remota, sin preocuparse por las comunicaciones entre los dos.

REGLAS: Las reglas o firmas son los patrones de caracteres que se buscan dentro de los paquetes que son estudiados por Snort, si encuentra una coincidencia crea una alerta, ya que la presencia de estos patrones puede indicar un potencial ataque.

RPM COMO UN IDS: El Manejador de paquetes RPM es uno de los varios programas que puede ser empleado como un IDS basado en host.

ROUTERS: Facilita conectividad a nivel de red, la función principal es remitir paquetes o interconectar subredes

SAMHAIN: es un sistema de detección de intrusos basado en host (HIDS) suministra la comprobación de integridad de ficheros y registro de monitoreo.

SMOOTH-SEC: (Distribución de Linux IDS/IPS): es una distribución de Linux Debian 7 que contiene un IDS/IPS ligero y listo para usar.

SMTP: (Protocolo para la transferencia simple de correo electrónico), es un protocolo de red que se emplea para intercambiar mensajes de correo electrónico. Su funcionamiento es en línea y opera con los servicios de correo electrónico.

SNMP: (Protocolo Simple de Administración de Red) Es un protocolo que permite el intercambio de información de una forma expedita entre varios dispositivos de red.

SNORT: es un sistema de prevención y detección de intrusos de redes (IDS / IPS) de software abierto desarrollado por Sourcefire.

STACK TCP/IP: Conjunto de protocolos de red, basado en Internet y permite la transmisión de datos entre redes de ordenadores.

SURICATA: Es un IDS/IPS de alto rendimiento y motor de monitoreo de la seguridad de una red.

SWATCH: Es usado ampliamente como un IDS basado en host. Registra cualquier evento que el usuario desee añadir en el archivo de configuración.

TELNET: Es un protocolo de red que permite conectarse a otra máquina manejándola remotamente.

TRIPWIRE: es el IDS basado en host más popular para Linux

# RESUMEN

En la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, es posible que se presenten ataques informáticos por parte de terceros interesados en obtener información sobre las auditorías y los procesos de responsabilidad fiscal que allí se adelantan. Los *hackers* tienen las herramientas y conocimientos suficientes para introducirse a una red de computadores y acceder a información confidencial sin que los sistemas de seguridad tradicionales los detecten. Por ello se plantea el objetivo de Implementar un sistema de detección de intrusos - IDS que establezca si en la actualidad se presentan ataques a la red, y disminuya a futuro la posibilidad de ataques de terceros interesados en la información que se maneja al interior en la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República. Por ser un proyecto académico se usa software libre que permite realizar todas las tareas de detección y arroja los informes requeridos para tomar decisiones acertadas, tendientes a aumentar la seguridad de la información en la Institución. Se revisó documentación técnica de varios sistemas de detección de intrusos, luego se hizo una selección preliminar de cuatro de estos programas y al final se determinó probar dos: el EasyIDS y el SmoothSet. Luego de su instalación y pruebas de funcionamiento, se estableció que SmoothSet resultó ser el más versátil y por ende es el que se usó en el proyecto. Con él se monitoreó la red local por espacio de tres meses al cabo de los cuales se estableció que no existen evidencias de ataques de terceros. Se deja operativo para que alerte al departamento de sistemas de la Entidad en caso que a futuro se presente una actividad sospechosa. Como es de software libre, no hay inconvenientes con respecto al licenciamiento. Con los resultados obtenidos se realizan recomendaciones a la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República.



Palabras Clave: IDS, Sistema de Detección de Intrusos, Ataques Informáticos, Seguridad Informática, Gerencia Departamental Colegiada del Caquetá.

# INTRODUCCIÓN

Los ingenieros de sistemas son profesionales cuya misión es crear soluciones adecuadas a las necesidades que le formulen los clientes, usando para ello las tecnologías de la información y la comunicación. Una creciente necesidad que plantean los usuarios finales es tener redes seguras que le brinden cierto nivel de confianza en que su información estará protegida.

No bastan los antivirus, firewall, antimalware y todo el arsenal que existe en el mercado para que alguien pueda decir con total convencimiento que su red es segura. Solo basta leer las noticias para ver como grandes empresas tanto comerciales como de software han sido atacadas con éxito por *hackers*, que les han robado información muy valiosa.

Es por ello que la detección de intrusos en redes, es una actividad necesaria para establecer si en determinada red se presentan hechos anormales o fuera de lo común que puedan inducir a pensar que un tercero no autorizado está navegando entre los recursos de la red.

En la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República donde a pesar de tener antivirus, firewall, software de control de acceso y otras medidas de seguridad, esporádicamente se ha detectado algún tipo de malware almacenado en los discos duros lo que hace presumir que existen fallas en esos mecanismos de control, y que la red pueda estar bajo ataque, por lo tanto es necesario implementar un IDS que permita conocer con mayor certeza la presencia de intrusos en la red local.

El presente documento presenta aspectos relevantes sobre los sistemas de detección de intrusos - IDS, referencias a la normatividad sobre seguridad informática, una comparación entre IDS donde se estudiaron algunas de las soluciones de software libre que existen, se seleccionó e instaló Smooth-sec, se analizaron las alertas detectadas y finalmente se hicieron recomendaciones.

El resultado principal consiste en que no se detectó actividad sospechosa como transferencias fuera del horario laboral, que se encendieran equipos remotamente, que se enviaran archivos hacia el exterior de la red, que se detectaran escaneos ni dentro de la red ni de origen externo, es decir, no se obtuvo evidencia de ataques actuales a la red local durante el periodo de observación.

# 1 EL PROBLEMA DE INVESTIGACIÓN

## 1.1 DESCRIPCIÓN DEL PROBLEMA

En la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, es posible que se presenten ataques de terceros interesados en obtener información sobre las auditorías y los procesos de responsabilidad fiscal que allí se adelantan.

En la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, se adelantan auditorias y procesos de responsabilidad fiscal que involucra a personalidades de la vida política departamental, además que las cuantías de los procesos pueden ser de varios miles de millones de pesos. Esto hace que la información reservada que se maneja sea apetecible por ciertas personas que pretendan sabotear o sacar algún provecho.

El hecho que terceras personas tengan acceso al nombre, cuantía, presuntos hechos y demás datos reservados en uno de estos procesos, puede desencadenar en una gran cantidad de situaciones delictivas como: chantajes, calumnias, estafas, entre otros.

Pese a que se cuenta con los sistemas de protección estándar como antivirus, firewall, software de seguridad del PC, filtrado WEB, esporádicamente se ha detectado malware almacenado en algunos de los computadores de la gerencia, lo que hace presumir que existen fallas en esos mecanismos de control y que además la red pueda estar bajo ataque.

Algunas de las situaciones que podrían indicar la posibilidad de que algo fuera de lo común esté ocurriendo son:
Hace algún tiempo uno de los computadores amanecía encendido, aunque en la noche anterior se apagaba normalmente.
Pese a que se cuenta con un antivirus que se actualiza permanentemente, en uno de los computadores se detectaron varios archivos asociados a malware.
Al correo de una de las funcionarias llegó un mensaje, donde aplicaban técnicas de *phishing* tratando de obtener claves y datos confidenciales.

Aunque esto no necesariamente indica la presencia de un intruso sí evidencia la necesidad de que se debe implementar un sistema de detección de intrusos, que brinde claridad sobre si actualmente hay ataques informáticos a la red o por el contrario no se detecta ninguna actividad sospechosa, con lo cual habría un parte de tranquilidad al respecto.

En el evento que actualmente se esté perpetrando un ataque informático y éste no sea detectado y detenido mediante la implementación de un sistema de detección de intrusos, podría caer en manos de personas inescrupulosas información reservada perteneciente a las auditorias o a los procesos de responsabilidad fiscal que se adelantan en dicho ente de control.

Adicionalmente el atacante podría realizar toda una gran cantidad de eventos dañinos en contra de los sistemas informáticos de esta entidad, que podrían ir desde borrado de información hasta bloquear los servicios provocando que los funcionarios no pudieran adelantar sus labores.

Decir que alguien pueda atacar a la red de la Contraloría no es ficción ya que solo basta echar una mirada a los portales de noticias para ver que son frecuentes los ataques a entidades estatales. Por ejemplo, la Revista Semana[1] informó que el miércoles 3 de agosto de 2011 fue atacada la página de gobiernoenlínea.gov.co, el Diario el Espectador[2] publicó que el 10 de diciembre de 2013 hackearon la página de la procuraduría y la Revista ENTER[3] informó que el 28 de abril de 2014 hackers atacaron las páginas del Ejército Nacional.

## 1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo detectar la presencia de intrusos actuales y disminuir la posibilidad de ataques futuros a la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, mediante la implementación de un sistema de detección de intrusos?

[1] REVISTA SEMANA. Otro ataque informático a una página del Estado colombiano. [En línea] Bogotá 03-ago-2011.

[2] DIARIO EL ESPECTADOR. Hackearon la página de la Procuraduría por decisión contra Petro. [En línea] Bogotá 03-ago-2011

[3] REVISTA ENTER. Hackers atacan páginas del ejército nacional. [En línea] Bogotá 28-abr-2014.

## 1.3 OBJETIVOS

### 1.3.1 Objetivo general

Implementar un sistema de detección de intrusos que detecte la presencia de intrusos actuales y disminuya la posibilidad de ataques futuros a la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República.

### 1.3.2 Objetivos Específicos

Estudiar algunos de los diferentes Sistemas de detección de intrusos de software libre y determinar cuál es el más apropiado para la situación particular de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República.

Instalar y configurar el sistema de detección de intrusos seleccionado para monitorear la red local.

Establecer la existencia o no de intrusos en la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República.

Presentar recomendaciones al representante legal de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República con base en los resultados del monitoreo a la red local.

## 1.4 JUSTIFICACIÓN

Este proyecto es conveniente porque con la implementación de un sistema de detección de intrusos, se podrá monitorear el comportamiento del tráfico de red al interior de la Gerencia e identificar anomalías así como detectar los intentos de intrusión desde el exterior, que podrían significar intentos de accesos no autorizados a la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República. A partir del análisis de las alarmas se podrán realizar

acciones de mejora que logren corregir las fallas en la seguridad y con esto aumentar la seguridad de la información al interior de la organización.

Los beneficiarios directos del proyecto son los treinta y nueve funcionarios de la Gerencia Departamental Colegiada del Caquetá que verán protegida la información de sus procesos asignados y por ende se alejan de la posibilidad de un escándalo e investigaciones disciplinarias por fuga de información, ya que por ejemplo, si aparecen en los medios de comunicación datos reservados del proceso de un funcionario en particular, lo primero que se viene a la mente de todos es que el funcionario lo hizo a propósito y se empezaría a especular sobre todo tipo de motivaciones, pasando por corrupción o negligencia, que en últimas dañan la imagen del funcionario y de la Entidad en general.

De manera indirecta se beneficia la ciudadanía en general ya que si se previene el ataque informático por parte de terceros, los procesos misionales internos se realizarían de acuerdo a los procedimientos establecidos y la ciudadanía recibiría el servicio de control fiscal, sin ningún tipo de alteración. Esto aumenta la credibilidad de la ciudadanía al saber que sus instituciones están blindadas ante los ataques informáticos que podrían ser ordenados por las personas que se apropian de los dineros públicos y con estos actos buscarían quedar impunes.

De otra parte, la principal ventaja es que tener instalado un sistema de detección de intrusos permite saber si hay intentos de ataques externos con lo que se podrán implementar mejoras a la seguridad informática en los aspectos que se requieran. El no tener este sistema mantendría al personal de sistemas de la Organización ignorantes de si un ataque ha sido exitoso, hasta que fuera demasiado tarde.

# 2 MARCO DE REFERENCIA

## 2.1 ANTECEDENTES

El uso de sistemas de detección de intrusos no es una actividad nueva, desde la misma aparición de las redes de computadores y de personas con la suficiente preparación para penetrarlas, se hizo evidente que se necesitaba algún tipo de sistema de detección y de prevención de este tipo de actividades no autorizadas. Esto cobra cada día mayor vigencia con la aparición de miles de herramientas para vulnerar los sistemas de protección informática que implementan las organizaciones. A continuación se enuncian algunos antecedentes de los cuales se aprende sobre los Sistemas de detección de intrusos, su clasificación, sus características y, sobre todo su pertinencia para afrontar el presente problema de investigación.

Garzón Gilberzon[4] en la implementación de un sistema de detección de intrusos (IDS) en la Dirección General Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC -PIDSINPEC en Bogotá, planteó como objetivo el buscar violaciones a la política de seguridad y entre los resultados relevantes obtuvo que dicha red está a la merced de ataques e intrusiones que pueden llevar a pérdida de información. Este estudio es un antecedente importante para la presente investigación por cuanto aborda el mismo tema de estudio y puede ser tomado como referente desde lo conceptual y metodológico, ya que brinda un estudio de las características, clasificación y arquitectura de un IDS.

Cotarelo Genmota[5] realiza un estudio, en Méjico, sobre las intrusiones a sistemas informáticos, donde muestra los tipos de intrusos, describe los tipos de sistemas de detección de intrusos, habla sobre las ventajas y desventajas de los mismos. Se resalta el apartado sobre los puntos a considerar en la selección de un IDS, que explica una serie de cuestiones que orientan la selección de un IDS, lo cual lo hace muy pertinente para el presente proyecto.

[4] GARZON, Gilberzon. Propuesta para la implementación de un sistema de detección de intrusos (IDS) en la Dirección General Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC “PIDSINPEC” UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD. Tunja. 2015.

[5] COTARELO, Genmota. Sistema de detección de intrusos. [En línea]. Resumos e Trabalhos México. 2011

Cyrille Larrieu[6] de Francia, en su introducción a los sistemas de detección de intrusiones (IDS), habla sobre los sistema de detección de intrusiones de red NIDS y sobre los sistemas de detección de intrusiones en el host HIDS, además de explicar las técnicas de detección como son la verificación de la lista de protocolos, verificación de los protocolos de la capa de aplicación y reconocimiento de ataques de "comparación de patrones", toda esta información es totalmente aplicable al proyecto actual.

Mira Emilio[7] implementa un sistema de detección de intrusos en la Universidad de Valencia España, para aumentar la seguridad ya que reciben una media de seis ataques diarios tipo *exploit* considerados como los más peligrosos. De este trabajo se consideran muy relevantes todos los apartes que tratan sobre los procesos de instalación del IDS Snort, que es uno de los analizados en el presente trabajo.

De otra parte, Amaya y Quiroga[8] realizan una prueba piloto de la Herramienta de Monitoreo Alienvault en la Plataforma Tecnológica de Telefónica TELECOM en Bogotá, cuyo objetivo principal es implementar la herramienta AlienVault y realizar pruebas para poder determinar su eficiencia técnica, económica y funcional. De este trabajo se destacan los temas: Los riesgos informáticos, Riesgo informáticos más significativos y su impacto en la empresa, La gestión de los riesgos y Ataques a la red, que brinda un punto de partida en el conocimiento de los ataques que pueden sufrir las redes de datos. Esto es fundamental para el desarrollo del presente trabajo por cuanto se incrementa el conocimiento sobre los posibles ataques que puede sufrir una red local y cómo el sistema de detección de intrusos seleccionado los detectará.

Britos José[9] presenta un estudio sobre la detección de Intrusiones en redes de datos con captura distribuida y procesamiento estadístico, que tiene como objetivo el análisis y desarrollo de tecnologías basadas en la investigación estadística, las

6 LARRIEU, Cyrille. Sistema de detección de intrusiones (IDS). Introducción a los sistemas de detección de intrusiones. [En línea] CCM Benchmark Group. 2003.

7 MIRA, Emilio. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. [En línea] Universidad de Valencia. España. 2012.

8 AMAYA, Eduardo y QUIROGA, Laura. Evaluación del Piloto de la Herramienta de Monitoreo Alienvault en la Plataforma Tecnológica de TELECOM. [En línea] Universidad de San Buenaventura. Bogotá. 2012

9 BRITOS, José. Detección de intrusiones en redes de datos con captura distribuida y procesamiento estadístico. Tesis de Maestría en Redes de Datos [En línea] Universidad Nacional de La Plata, Argentina. 2010.

redes neuronales y los sistemas autónomos aplicados a los problemas de detección de intrusiones en redes de datos. Este trabajo en su capítulo 2 presenta los ataques y vulnerabilidades más comunes encontradas en las redes. En el capítulo 3 se realiza una introducción al estudio de los aspectos más relevantes de los IDS, ambos temas necesarios para el desarrollo del presente trabajo.

González Antony[10] realiza la instalación de un Sistema de Detención de Intrusos (IDS) en la Red Wifi del Laboratorio G de la Universidad Simón Bolívar, Venezuela, con el objetivo de monitorear el tráfico de páginas web visitadas por los usuarios durante el día. El marco teórico de este trabajo abarca temas como el IDS EasyIDS, DHCP, SSH y describe algunas herramientas de seguridad de redes, todos temas congruentes con el objetivo del presente trabajo.

Robayo Eduard[11] planteó un sistema de detección de intrusos basado en detección de patrones de tráfico usando Modelos Ocultos de Markov.
El modelo tuvo una capacidad de detección de ataques e intrusiones superior al 95%, lo que lo hace una muy buena alternativa como producto de investigación. En su trabajo se abordan los IDS, sus características, las arquitecturas y los mecanismos de detección más comunes, así como ataques de red que pueden servir para soportar teóricamente el presente trabajo.

## 2.2 MARCO TEÓRICO CONCEPTUAL

Los ataques informáticos son algo real, cualquier persona o entidad puede ser atacada en cualquier momento, nadie está exento de ser víctima de los delincuentes informáticos. Se hace primordial implementar todas las medidas posibles para aumentar la seguridad y los sistemas de detección de intrusos no deben faltar. A continuación se puntualizan algunos aspectos claves sobre los IDS, se enumeran algunos cuantos hechos de ataques informáticos ocurridos durante el año 2015 en el mundo y en Colombia. Posteriormente se enuncian algunos marcos de trabajo o estándares que ayudan a aumentar la seguridad de la información.

[10] GONZÁLEZ, Anthony. Informe Final de Pasantías. Implementar un Sistema de Detención de Intruso (IDS) en la Red Wifi del Laboratorio G de la Universidad Simón Bolívar sede litoral. [En línea] Universidad Simón Bolívar, Venezuela. Abril 2011.

[11] ROBAYO, Eduard. Detección de intrusos en redes de telecomunicaciones IP usando modelos ocultos de Markov. [En línea] Tesis de Maestría presentada para optar al título de Magíster en Ingeniería de Telecomunicaciones. Universidad Nacional de Colombia. Bogotá, 2009.

### 2.2.1 Sistemas de detección de intrusos.

El concepto de Sistemas de Detección de Intrusos fue introducido en el año 1980 por Anderson[12] en su reporte *computer security threat monitoring and surveillance* cuyo objetivo era mejorar la capacidad de auditoría y vigilancia de la seguridad informática de los sistemas de los clientes. Este documento es el punto de partida para el desarrollo de los sistemas de detección de intrusos y es fundamental para el conocimiento de los mismos.

Un sistema de detección de intrusos o IDS (*Intrusion Detection System*) es una herramienta de seguridad, implementada como hardware o software, que se encarga de monitorear los eventos que ocurren en un sistema informático, computador o red, tratando de detectar intentos de intrusión por terceros no autorizados.

Un intento de intrusión, lo define Mira[13] como cualquier tentativa de comprometer la confidencialidad, integridad, disponibilidad o evadir los mecanismos de seguridad de una red o computadora. Las intrusiones se materializan de varias formas: agresores que acceden a los sistemas a través de Internet, usuarios autorizados del sistema que quieren ganar privilegios adicionales de los que tienen y usuarios permitidos que hacen mal uso de los privilegios que se les han establecido.

### 2.2.2 Implementación de un sistema de detección de intrusos

La detección de intrusiones a tiempo permite a las organizaciones proteger sus sistemas de las amenazas que se incrementan con la conectividad en red y la total dependencia que se tiene con respecto a los sistemas de información. En palabras de Amaya y Quiroga esta interconexión “hace que las empresas sean más vulnerables y estén expuestas a diferentes amenazas (denegación de servicio, intrusión en la red, suplantación de identidad, entre otros) que pone en riesgo sus activos informáticos”[14]

[12] ANDERSON, James. Computer security threat monitoring and surveillance. [En Línea] Fort Washington, Pa. February 26, 1980. p. 6.

[13] MIRA, Emilio. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. [En línea] Universidad de Valencia. España. 2012. p. 13

[14] AMAYA y QUIROGA, Op. cit., p. 31.

Un sistema de detección de intrusos es la respuesta lógica a esta situación y viene a ser una pieza primordial en la infraestructura de seguridad de cualquier organización, ya que tienen la capacidad de descubrir ataques y otras transgresiones que no son advertidas por otros sistemas de protección. Con ello se previene inconvenientes al disuadir a posibles atacantes, ya que al temer que los puedan descubrir y sancionar, cambiarán su comportamiento y muchos ataques no llegarán a materializarse.

Los atacantes, aplicando procedimientos muy especializados, pueden conseguir accesos no autorizados, especialmente a redes públicas. Esto acontece muchas veces porque las vulnerabilidades conocidas en el medio no son corregidas, esto sucede en casos como los siguientes:

Algunos sistemas operativos obsoletos no son parcheados o renovados.
Los administradores, algunas veces, no dedican el tiempo y recursos para instalar las últimas actualizaciones. Esto es una dificultad común en ambientes que incluyen un gran número de máquinas con sistemas operativos y hardware diverso.
Errores al configurar los sistemas.

En este escenario un sistema de detección de intrusos logra ser una excelente herramienta de apoyo en la seguridad de los sistemas computacionales. Como lo indica Larrieu “se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil” [15]

Se debe tener en cuenta que cuando un sujeto ataca un sistema, primeramente hace pruebas e inspecciona el sistema o red en busca de puntos de penetración. En organizaciones que no disponen de un sistema de detección de intrusos el atacante puede examinar el sistema casi sin riesgo de ser detectado. En cambio, un sistema o red con un sistema de detección de intrusos monitoreando sus operaciones, le presenta mayores dificultades a un atacante, aunque el agresor pueda intentar escanear la red el sistema de detección de intrusos observará estas actividades, las identificará como sospechosas, podrá activamente bloquear el acceso y avisar al administrador. Incluso si el sistema de detección de intrusos no es capaz de bloquear los ataques, puede almacenar información importante sobre éstos, que puede ser usada como prueba ante tribunales. También se puede usar

[15] LARRIEU, Op. cit., p. 3.

esta información para corregir fallos en la configuración de seguridad o en la política de seguridad de la entidad.
Con esto en mente, cuando se crea un plan para la gestión de seguridad de la información o se desea escribir la política de seguridad de la organización, es obligatorio conocer el riesgo de la organización a potenciales amenazas, la posibilidad de ser atacada o si ya está siendo agredida.

### 2.2.3 Clasificación de los sistemas de detección de intrusos.

Existen varias clasificaciones de los sistemas de detección de intrusos, Mira[16] presenta una que se muestra en el cuadro 1:

Cuadro 1. Clasificación de los Sistemas de detección de intrusos

| Criterio de clasificación | Tipos |
|---|---|
| Fuentes de información | IDSs basados en red (NIDS) |
| | IDSs basados en host (HIDS) |
| Tipo de análisis | Detección de abusos o firmas |
| | Detección de anomalías |
| Respuesta | Respuestas pasivas |
| | Respuestas activas |

Fuente: http://www.rediris.es/cert/doc/pdf/ids-uv.pdf

De acuerdo al problema planteado y al alcance del presente proyecto, se estima que el IDS a emplear debe ser seleccionado de acuerdo a la fuente de información que analiza, por ello, a continuación se amplía un poco esta clasificación.

Algunos IDS examinan paquetes de red tomados de la troncal de la red o de segmentos de ella, mientras que otros IDS examinan sucesos creados por los sistemas operativos o los aplicativos en busca de señales de intromisión. Es decir, hay IDS que toman los eventos de la red llamados NIDS (Network IDS) o directamente de los equipos llamados HIDS (Host IDS).

Respecto la herramienta IDS basada en Host, Britos establece que “está diseñada para responder a ataques sobre un determinado servidor. Se basan en la supervisión de las acciones de los usuarios y de los archivos del servidor”[17]. Operan con la información acumulada desde dentro de un computador, como pueden ser

16 MIRA, Op. cit., p. 18.
17 BRITOS, Op. cit., p. 36.

los archivos de auditoría del sistema operativo. Esto ocasiona que el IDS examine las actividades con una gran precisión, estableciendo exactamente qué procesos y usuarios están implicados en un ataque específico dentro del sistema operativo.

A diferencia de los NIDS, los HIDS pueden ver el resultado de un intento de agresión, es decir, si el ataque tuvo éxito o no, al igual que pueden acceder directamente y monitorear los archivos de datos y procesos del sistema atacado.

Ventajas:

Los IDSs basados en host, al tener la capacidad de monitorear sucesos locales, pueden descubrir ataques que no pueden ser descubiertos por un NIDS.
Pueden operar en un entorno donde el tráfico de red corre cifrado, ya que la fuente es examinada antes de que los datos sean cifrados en el host origen y posteriormente de que los datos sean descifrados en el destino.

Desventajas:

Los HIDS consumen más tiempo de administración, ya que deben ser gestionados y configurados en cada host monitoreado.
Mientras que con los NIDS se tiene un IDS que monitorea muchos host, con los HIDS se tiene un IDS por cada sistema monitoreado.
El IDS puede ser cerrado o deshabilitado si una agresión logra tener éxito y accede al control sobre el computador.
No pueden detectar ataques a toda una red porque solo analiza los paquetes de red remitidos a él.
Afectan el rendimiento del sistema monitorizado, al consumir recursos.

En cuanto a los IDS basados en red, que son una gran parte de los sistemas de detección de intrusos, descubren ataques captando y examinando paquetes de la red. Un NIDS puede monitorear el tráfico que afecta a todos los hosts que están conectados a ese segmento de red.

Con respecto a los IDS basados en red, Larrieu[18] indica que “forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal” Adicionalmente agrupan varios sensores localizados en diferentes puntos de la red.

[18] LARRIEU, Op. cit., p. 2.

Estos sensores monitorean el tráfico ejecutando análisis e informando de los posibles ataques. Dado que los sensores están programados solo para ejecutar el software de detección, consiguen estar más blindados frente a ataques que pretendan deshabilitarlos, además corren en modo oculto y es más difícil para un atacante establecer su presencia y localización.

Ventajas:

Un IDS bien localizado y en un equipo potente logra monitorear una red grande.
Los NIDS tienen un impacto mínimo en la red, normalmente no interfieren en las operaciones.
Se pueden configurar para que sean muy seguros frente a los ataques, haciéndolos invisibles al resto de la red.

Desventajas:

Pueden tener dificultades procesando todos los paquetes en una red grande o con alto tráfico y pueden fracasar en reconocer ataques lanzados durante los picos de tráfico.
No examinan la información cifrada. Este inconveniente se incrementa cuando se usa cifrado en el propio nivel de red (IPSec) entre hosts.
No especifican si el ataque tuvo o no éxito, lo único que reportan es que la agresión fue lanzada. Esto significa que posteriormente los administradores deben manualmente indagar al interior de la red y determinar si la tentativa tuvo éxito o no.

Tienen dificultades al detectar ataques basados en red que corren en paquetes fragmentados. Estos paquetes fragmentados hacen que el IDS no detecte dicho ataque o que sea inconsistente su detección.

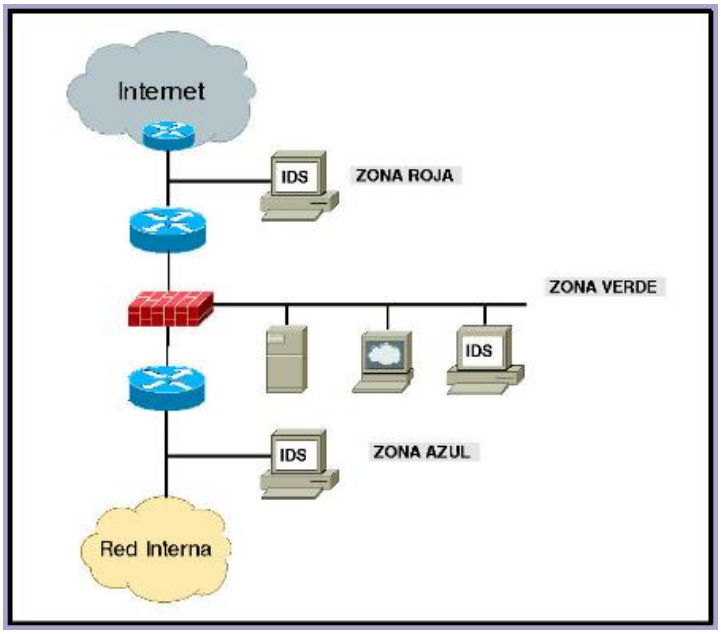
Quizá el mayor inconveniente, es que su ejecución de la pila de protocolos de red puede variar de la pila de los sistemas a los que protege. Muchos servidores y equipos de escritorio no cumplen en ciertos aspectos los patrones TCP/IP, pudiendo rechazar paquetes que el NIDS ha capturado.

### 2.2.4 Ubicación de un IDS

Como lo establece Mira[19] la decisión de dónde colocar el IDS es la decisión inicial que se debe tomar y estará basada en las características técnicas del equipo que se use, como del propio software IDS o el tamaño de la base de datos que guardará la información.

Existen tres zonas en las que se podría colocar un sensor: Ver figura 1.

Figura 1. Localización de un IDS dentro de una organización




Fuente: http://www.rediris.es/cert/doc/pdf/ids-uv.pdf

Las características que presenta cada una de estas zonas, son las siguientes:

Zona roja: Esta es una zona de alta peligrosidad. En esta zona el IDS debe ser configurado para ser poco sensible, puesto que vera todo el tráfico que ingrese o salga de la red y habrá muchas más posibilidades que se generen falsas alarmas.

Zona verde: Al IDS correspondería ser configurado para tener una sensibilidad un poco más alta que en la zona roja, puesto que ahora, el firewall deberá filtrar y bloquear algunos accesos definidos previamente a través la política de la

[19] MIRA, Op. cit., p. 23.

organización. En esta zona aparece un número pequeño de falsas alarmas debido a que en este punto solo deberían estar autorizados accesos hacia los servidores.

Zona azul: Esta es la zona de confianza. Cualquier tráfico desconocido que llegue hasta aquí debe ser estimado como peligroso o dañino. En este segmento de la red se causará el menor número de falsas alarmas, por consiguiente, cualquier alarma del IDS debe ser inmediatamente estudiada y solucionada.

Es importante destacar que la zona azul no es una porción de la red interna. Todo lo que alcance al IDS de la zona azul ira hacia el firewall (ejemplo, si se usa un proxy-caché para los usuarios de web) o hacia el exterior. El IDS no atenderá ningún tipo de tráfico interno dentro de la red.

En la eventualidad que se tenga configurado un IDS para atender tráfico interno, las falsas alarmas aparecerán provocadas mayoritariamente por equipos internos al enviar solicitudes a los servidores de la red, también por servidores propios (Servidores de Nombre de Dominio principalmente) y olfateadores de red que se tengan instalado, por lo que habrá que configurar el IDS para que algunas de sus reglas no sean tan sensibles.

### 2.2.5 Los ataques son hechos reales.

A continuación se enuncian algunos casos reales de ataques informáticos que se han dado a conocer por los medios de comunicación: En enero 12 de 2015 las páginas privadas del ejército estadounidense en Twitter y YouTube fueron hackeadas por piratas informáticos que alegaron haber actuado bajo las orientaciones del Estado Islámico. Los *hackers* accedieron a las cuentas del Mando Central Militar de EE. UU. y publicaron varios mensajes con información sensible. Los *hackers* cambiaron las imágenes del perfil de la cuenta @centcom, colocando la imagen de una persona con el rostro cubierto y la bandera empleada por el Estado Islámico con la frase "*I love you ISIS*", según lo publicado por Pereda[20].

El 21 de enero de 2015, Lemaître[21] publicó que el diario francés *Le Monde* sufrió un ataque informático en su cuenta de Twitter, que tiene casi tres millones de

[20] PEREDA, Cristina. Piratas informáticos atacan la red del Ejército de EE UU. En: Diario El País [En Línea]. Washington 13 ENE 2015 - 00:19 CET.

[21] LEMAÎTRE, Damien. La cuenta de Twitter de 'Le Monde', pirateada por activistas pro-El Asad. En: Diario El País Internacional . Washington 21 ENE 2015 - 04:19 CET.

seguidores, esto les obligó a desactivar su canal de información por un tiempo de más de una hora. Los piratas consiguieron capturar la contraseña, luego bloquearon todos los accesos impidiéndole al diario volver a cambiar la contraseña.

Las grandes compañías de productos tecnológicos tampoco se salvan de los ataques, por ejemplo, según el artículo de Abad[22] en 2015 los dispositivos de Apple sufrieron el mayor ciberataque de su historia, lo que evidencia la gran planificación y los recursos significativos que se emplearon.

Pero estos ataques no son exclusivos de países lejanos, en Colombia también se presentan estos ataques. Ejemplo, con el uso del código Remtasu a través de correos electrónicos y usando nombres de empresas reconocidas, roban información de los computadores por medio de la captura de datos generados en el teclado, que son enviados a un equipo remoto indicado por el atacante.

Un caso más puntual sucedió en Bucaramanga, donde un delincuente informático robó información con falso correo de la Fiscalía. A cientos de ciudadanos les llegó el mensaje a sus cuentas de correo electrónico con una falsa citación de la Fiscalía, cuando las víctimas proceden a descargar el archivo que señala el correo como los detalles del supuesto proceso penal, el virus roba información personal de usuarios comunes y datos encriptados que puedan tener los equipos.

Como se aprecia en estos ejemplos, que constituyen una pequeña muestra de los miles de casos que a diario suceden en Colombia y el mundo, es muy real la amenaza de ataques informáticos para robar información u otro tipo de acciones ilegales. Es un error creer que alguien está a salvo de los ataques de los delincuentes informáticos.

### 2.2.6 Algunos estándares para aumentar la seguridad

Para ayudar a las organizaciones de todo tipo en el proceso de fortalecimiento de sus sistemas de seguridad y reducir al mínimo la posibilidad de un ataque por parte de delincuentes informáticos, la comunidad internacional ha creado una serie de estándares que presentan reglas precisas para el mejoramiento de la seguridad informática.

[22] ABAD LIÑAN, José Manuel. Los dispositivos de Apple sufren el mayor ciberataque de su historia. Diario el País, Sección Tecnología. [En línea]. Madrid. 2015.

#### 2.2.6.1 RFC 2196

En un artículo publicaod por Dulaunoy[23] presenta las características del RFC 2196 que es un estándar empleado en la práctica de la seguridad de la información. Entre sus características se tiene:

Se pone en práctica siguiendo los procedimientos de administración de sistemas, promulgación de guías sobre el uso aceptable de los recursos informáticos o por medio de otros procesos, todos muy prácticos y fáciles de seguir.
Puede implantarse de forma muy sencilla
Obliga al uso de herramientas de seguridad
Define las áreas de responsabilidad de usuarios, administradores y la dirección, y recomienda un uso responsable para toda situación posible.

Este estándar aborda entre otros, los siguientes temas:

Políticas de Seguridad
Define y precisa la importancia de una Política de Seguridad
Define los puntos clave de una buena Política de Seguridad
Establece el umbral de flexibilidad de la política de seguridad

Arquitectura de Red y de Servicios
Sugiere como realizar la configuración de Red y los servicios asociados
Sugiere configuración de los firewalls, para mayor efectividad

Servicios y Procedimientos de Seguridad
Autenticación
Integridad
Confidencialidad
Autorización
Auditoria
Acceso

Gestión de Incidentes de Seguridad
Sugiere cómo hacer la notificación de un incidente y definir los puntos de contacto
Da las pautas para la identificación un incidente

[23] DULAUNOY, Alexandre. RFC 2196 (Site Security Handbook) with ISO 27001 and other annotations. [En línea]. s/f.

Orienta sobre cómo gestionar un Incidente
Plantea las posibles consecuencias de un incidente
Indica cómo definir responsabilidades

#### 2.2.6.2 Estándar ISO/IEC 27000:2016

La ISO publica el estándar internacional ISO/IEC 27000 titulado “Tecnología de la Información – Técnicas de Seguridad – Sistemas de Administración de la Seguridad de la Información – Visión general y Vocabulario” [24].

Provee un panorama general a la entrada de los estándares de la familia ISO/IEC 27000, iniciando con un diccionario de términos fundamentales, lo cual es muy importante porque la seguridad de la información, como varios otros temas técnicos, utiliza una enmarañada red de términos que no son dominados por la mayoría de las personas.

El ISO/ IEC 27000 es admitido internacionalmente para la administración de la seguridad de la información y es empleado por todo tipo de organizaciones, sin importar su tamaño o su actividad.

El conjunto de estándares de la familia ISO-27000, contiene entre otros:

ISO / IEC 27000, Sistemas de gestión de la seguridad de la información - Visión general y vocabulario.
ISO / IEC 27001, Sistemas de gestión de la seguridad de la información – Requisitos.
ISO / IEC 27002, Código de prácticas para los controles de seguridad de la información.
ISO / IEC 27003, Guía de implementación del sistema de gestión de la seguridad de la información.
ISO / IEC 27004, Gestión de la seguridad de la información – Medición
ISO / IEC 27005, Gestión de riesgos de seguridad de la información
ISO / IEC 27006, Requisitos para los organismos de auditoría y certificación de la seguridad de la información sistemas de gestión.

[24] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION –ISO. International Standards for Business, Government and Society. ISO/IEC 27000. Fourth edition 2016-02-15. [En línea]. ISO office Génova. s/f.

ISO / IEC 27007, Directrices para la auditoría de los sistemas de gestión de la seguridad de la información.

#### 2.2.6.3 Estándar ISO/IEC 18028-2:2006

Según ISO[25], Este estándar define una arquitectura de seguridad para redes, brindando seguridad de extremo a extremo a una red. La arquitectura puede ser empleada por varias clases de redes donde la seguridad extremo a extremo es una inquietud presente, esto es independiente de la tecnología con que haya sido implementada la red. Su objetivo es servir de base para el desarrollo de recomendaciones detalladas para la seguridad en redes punto a punto.

Este estándar ha sido revisado por el estándar ISO/IEC 27033-2:2012 que da directrices para que las organizaciones planifiquen, diseñen, implementen y documenten la seguridad de la red.

#### 2.2.6.4 ISO/IEC 15408 Common Criteria

El Committee of the Common Criteria Recognition Arrangement[26] libera el Criterio Común para la Valoración de la Seguridad en Tecnologías de la Información (abreviado como Criterio Común o CC), que es un estándar internacional usado para la certificación de la seguridad en computadoras.

El Criterio Común es un esquema de trabajo en el cual los usuarios de computadoras pueden detallar sus requisitos funcionales de seguridad y de garantía, para que los proveedores interesados puedan implementar y/o hacer solicitudes acerca de los atributos de seguridad de sus productos, y los laboratorios de prueba pueden verificar los productos para confirmar si en realidad satisfacen los requisitos.

[25] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION –ISO. ISO/IEC 18028-2:2006. Information technology -- Security techniques -- IT network security -- Part 2: Network security architecture. [En línea]. Génova. s/f.

[26] COMMITTEE OF THE COMMON CRITERIA RECOGNITION ARRANGEMENT. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements. [En línea] 2016.

La aplicación de este estándar garantiza que los procesos de especificación, implementación y evaluación de la seguridad de un producto de computación han sido realizados en una manera inflexible y estandarizada.

#### 2.2.6.5 Estándar ISO / IEC 21827: 2008

De acuerdo a la ISO[27], es un estándar internacional fundado en el Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas, mejorado por la Asociación Internacional de Ingeniería de Seguridad de la Información.

Especifica las características necesarias para el éxito del proceso de ingeniería de la seguridad de una organización, y es adaptable a todas las organizaciones de ingeniería de la seguridad, ya sean gubernamentales, comerciales o académicas.

No especifica una secuencia o proceso particular, en cambio captura las prácticas que están siendo aplicadas en la industria. El modelo es una métrica estándar para las prácticas de la ingeniería de seguridad. Cubre lo siguiente:

Ciclos estructurales de vida del proyecto, que contiene las actividades de desarrollo, operación, mantenimiento y desmantelamiento.
Trabajo paralelo con variadas disciplinas, como software y hardware, pruebas de ingeniería, gestión de sistemas, operación, mantenimiento y talento humano.
Todos los ámbitos de la organización, como las actividades de gestión, de organización y de ingeniería.
Normatividad sobre Seguridad de la Información

### 2.2.7 Estándares en Colombia

En Colombia, las normas internacionales en seguridad de la información, han sido adoptadas por el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC[28].

[27] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION –ISO. ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®). [En línea]. Génova. s/f.

[28] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS - ICONTEC. Organismo Nacional de Normalización de Colombia. [En línea] Colombia. 2016.

Por ejemplo, la norma NTC ISO/IEC 27001 fue liberada por el Instituto Colombiano de Normas Técnicas y Certificación en el año 2006. Esta norma permite implementar un sistema de gestión de seguridad de la información (SGSI) teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos. La norma emplea el modelo de procesos PHVA (Planificar-Hacer-Verificar-Actuar).

De otra parte, el Gobierno ha generado normas de control interno como MECI (basado en COSO) y de calidad como la NTCGP1000 (basado en ISO9001).

## 2.3. MARCO CONTEXTUAL

La Contraloría General de la República – CGR[29] es el máximo órgano de control fiscal en el país, cuya misión es fortalecer el control y la vigilancia de la gestión fiscal con enfoque preventivo en el marco de la Constitución y la Ley, para garantizar el buen manejo de los recursos públicos, en la búsqueda de la eficiencia y la eficacia de la gestión pública, con participación de la ciudadanía, para el logro de los fines del Estado.

En 1991 el control fiscal constitucionalmente da un giro de 180º. Se elimina el control numérico legal y se da paso al posterior y selectivo (Art. 267 C.P.) fundamentado en la eficiencia, la economía, la eficacia y la valoración de los costos ambientales. Se concibe la Contraloría como una entidad técnica con autonomía presupuestal y administrativa.

En 2000 el proceso de responsabilidad tiene un vuelco total mediante la Ley 610 se reduce a una sola etapa. Se define el concepto de gestión fiscal, los elementos para la responsabilidad fiscal, se fijan los términos para la caducidad y la prescripción y se extiende la responsabilidad fiscal a los herederos como consecuencia de la muerte del presunto responsable.

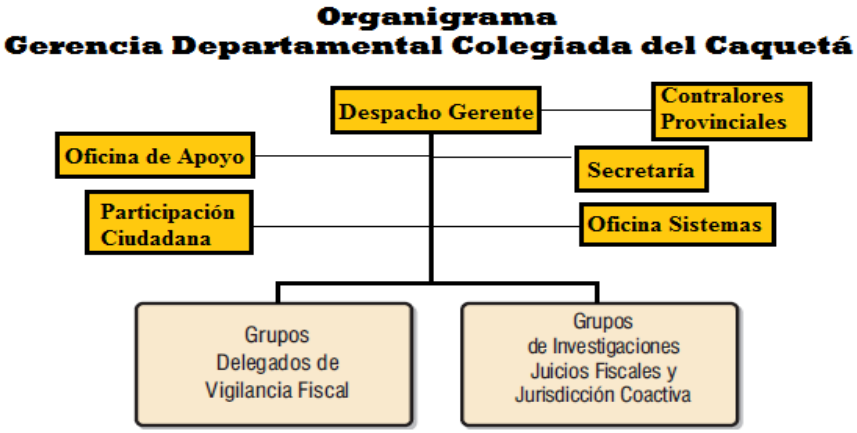
El 2 de julio 2002 la Contraloría General de la República recibió la certificación ISO 9001(versión 2000) otorgada por BVQI de Colombia Ltda (*Bureu Veritas*), con lo cual fueron avalados a nivel internacional la calidad de una buena parte de los procesos del ente de control.

[29] CONTRALORIA GENERA DE LA REPUBLICA. ¿Qué es la Contraloría? [En línea]. Bogotá. 2016.

Tiene en servicio un Portal Institucional integrado por dos sitios o ambientes: Intranet e Internet. El primero fue concebido como una herramienta de trabajo y de comunicación para todos los funcionarios, y el segundo como un lugar para mostrarle al Congreso de la República, a la ciudadanía y a los sujetos de control qué hace y cómo hace su labor la Contraloría.

Respecto a la Gerencia Departamental Colegiada del Caquetá, se aprecia su organigrama en la figura 2 y más adelante aspectos de la red de datos.

Figura *2*. Organigrama de la empresa




Fuente: El autor

La Gerencia Departamental Colegiada del Caquetá cuenta con los siguientes servicios de red:

Protocolo de Configuración Dinámica de Host (DHCP)
Protocolo Simple de Administración de Red (SNMP)
Correo electrónico
Domain Name System (DNS)
Protocolo de transferencia de archivos (FTP)
Impresión
VoIP
Bases de Datos

Se cuenta con cableado estructurado UTP Categoría 5 con capacidad para 48 computadores. Se ha incrementado la capacidad con la adquisición de nuevos Switch colocados en cascada.

El centro de cableado está ubicado en el bloque de Gerencia. La Red eléctrica cuenta con soporte de UPS de 20 KVA. Respecto a la comunicación telefónica, esta es directa con el nivel central Vía VozIP.

El acceso a internet, intranet, correo electrónico, aplicativos en línea y sistema de videoconferencia, se hace mediante banda ancha de 10 MB con fibra óptica en la última milla.

La seguridad de la información se basa en firewall, antivirus, software de seguridad del PC que bloquea la instalación de programas no autorizados, copias de seguridad.

Hay un esquema de carpetas compartidas, donde los funcionarios intercambian información. Eventualmente se tienen pasantes a los que se les asigna un equipo para trabar.

Hay intercambio de información con terceros a través de memorias USB, correo electrónico o almacenaje en la nube. Los funcionarios acceden a sus correos personales desde la oficina. Se tiene bloqueo de navegación a ciertas páginas que no estén relacionadas con la función de la Contraloría.

## 2.4. MARCO LEGAL

En las últimas dos décadas ha habido un fuerte desarrollo normativo a nivel mundial para hacer frente a la creciente ola de delitos informáticos que se presentan. Se enuncian a continuación algunas normas que se usan en otros países y posteriormente algunos de los desarrollos normativos en Colombia.

### 2.4.1 Normatividad internacional

Ramírez y Aguilera[30] abordan el tema de los delitos informáticos y su tratamiento en los diferentes países e indican que dada la enorme trascendencia que tiene el crimen transnacional, los gobiernos han realizado varias cumbres y llegado a

[30] RAMÍREZ, Egil y AGUILERA, Ana. Los Delitos Informáticos. Tratamiento internacional, en Contribuciones a las Ciencias Sociales, mayo 2009 [En línea]. Eumed.net 2009. p. 6.

acuerdos para compartir información y poder capturar a los delincuentes informáticos, algunos de ellos son:

El convenio de Berna
La convención sobre la Propiedad Intelectual de Estocolmo
La Convención para la Protección y Producción de Fonogramas de 1971
La Convención Relativa a la Distribución de Programas y Señales
Boletín de las Naciones Unidas sobre los delitos informáticos de 2002

En el tema de legislación de algunos países, se cuenta:

Acta Federal de Abuso Computacional de Estados Unidos de 1994
Convenio sobre cibercrimen del Consejo Europeo de 23 de noviembre de 2001
Ley Especial sobre los Delitos Informáticos de Venezuela de 2001
Ley de los Abusos Informáticos de Gran Bretaña de 1992
Ley número 88-19 de 1988 sobre el fraude informático en Francia
Ley de reforma del Código Penal de 1987 en Austria
Ley de los Delitos Informáticos de 1993 en Holanda
Segunda Ley contra la Criminalidad Económica de 1986 en Alemania

### 2.4.2 Normatividad de ámbito nacional.

El 5 de enero de 2009, el Congreso de la República de Colombia[31] promulgó la Ley 1273 que modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Dicha ley define los nuevos tipos penales relacionados con la seguridad de los sistemas computacionales, como son: Acceso abusivo a un sistema informático (artículo 269A), Obstaculización ilegítima de sistema informático o red de telecomunicación (artículo 269B), Interceptación de datos informáticos (artículo 269C), Daño informático (artículo 269D), Uso de software malicioso (artículo 269E),

[31] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 1273 DE 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47.223. p. 1-2.

Violación de datos personales (artículo 269F), Suplantación de sitios WEB para capturar datos personales (Artículo 269G).

Un punto importante a considerar es que el Artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
Por servidor público en ejercicio de sus funciones
Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
Revelando o dando a conocer el contenido de la información en perjuicio de otro.
Obteniendo provecho para sí o para un tercero
Con fines terroristas o generando riesgo para la seguridad o defensa nacional
Utilizando como instrumento a un tercero de buena fe

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

En el mismo sentido, el Capítulo II de dicha ley trata sobre los atentados informáticos y otras infracciones, tipificando los delitos de Hurto por medios informáticos y semejantes (Artículo 269I) y la Transferencia no consentida de activos (Artículo 269J).

# 3. METODOLOGÍA

## 3.1. TIPO DE INVESTIGACIÓN

Tomando como guía lo desarrollado por Gómez[32] el tipo de investigación que se aplicó para el desarrollo del presente proyecto se clasificó así:

Acorde con el método utilizado: Cuantitativa
Los procedimientos que se aplicaron y los resultados que se obtuvieron, usan magnitudes numéricas que son tratadas mediante herramientas del campo de la estadística, como el número de alertas, el número de equipos, entre otros.

Por el nivel de conocimientos que se adquirieron: Descriptiva
Con este proyecto se buscó conocer las generalidades de los IDS, sus tipos, sus características, su funcionamiento para hacer frente a los ataques informáticos.

Por las características de los medios utilizados para obtener datos: De campo
Se realizó en la red local de la Gerencia Departamental Colegiada del Caquetá, para acopiar o recoger material directo de la información en el lugar mismo donde se presenta el fenómeno.

Por las características externas de las fuentes: Investigación primaria
Los datos e información fueron recogidos directamente por el investigador, de cuyo proceso dependieron los resultados obtenidos.

## 3.2. DISEÑO DE INVESTIGACIÓN

Para el cumplimiento del objetivo general y de cada uno de los objetivos específicos se aplicó un diseño de tipo preexperimento ya que no hubo grupo de control ni aleatoriedad, se siguieron los siguientes pasos:

[32] GÓMEZ, Susana. Lección 5: Investigación pura, investigación Aplicada, Investigación profesional, Curso Técnicas de Investigación. [En línea] Universidad Nacional Abierta y a Distancia- UNAD. Bogotá. 2008. p.14

Se estudiaron los manuales y características técnicas de algunos de los diferentes sistemas de detección de intrusos basados en red.
Se determinó cuál era el más apropiado para el presente proyecto

Se instaló y configuró el sistema de detección de intrusos seleccionado

Se realizó monitoreo de la red local durante los meses de septiembre a noviembre de 2016.

Se analizaron los resultados obtenidos para establecer la existencia o no de intrusos en la red local.

Se entregó un informe al representante legal de la Gerencia Departamental Colegiada del Caquetá, que contenía entre otros aspectos las evidencias del trabajo realizado y algunas recomendaciones para aumentar la seguridad de la red local y de la información en general.

## 3.3. POBLACIÓN Y MUESTRA

En este proyecto la población que se trabajó está conformada por cuarenta y un equipos de cómputo, que conforman la totalidad de la red local de la Gerencia Departamental Colegiada del Caquetá.

Teniendo en cuenta que todos los computadores están conectados en el mismo dominio, y por ende el tráfico de red es uno solo, se consideró que no era procedente realizar el proyecto sobre una muestra, en su lugar se tomó la totalidad del tráfico para ser analizado por el IDS, es decir, en este proyecto no se usó una muestra.

## 3.4. TÉCNICAS E INSTRUMENTOS PARA LA RECOLECCIÓN DE DATOS

Tomando como fundamento lo indicado por Collazos[33], la técnica utilizada en el presente proyecto fue la observación directa de las alertas generadas por el IDS Smooth-Sec, que fue la herramienta de medición del fenómeno estudiado.

[33] COLLAZOS, Hernán. Técnicas de Investigación. Contenido didáctico del curso Técnicas de Investigación. [En línea].UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA Bogotá. 2007.

El instrumento utilizado fue un diario de campo en archivo electrónico donde se registraban las capturas de pantalla de las alertas y se detallaba el correspondiente análisis. Este archivo electrónico sirvió de base para elaborar el informe final.

# 4. RESULTADOS

Para lograr el objetivo general propuesto se desarrollaron todos y cada uno de los objetivos específicos durante el tiempo establecido en el cronograma de trabajo. El cumplir a cabalidad con cada uno de los cuatro objetivos arrojó resultados importantes tanto para el conocimiento general del autor como para la entidad. En las líneas siguientes se detalla el desarrollo y resultados de los objetivos específicos.

## 4.1. SISTEMAS DE DETECCION DE INTRUSOS

Entre los más populares y mejores sistemas de prevención/detección de intrusos (IPS/IDS) gratuitos y/o de software libre, se mencionan los siguientes:

SNORT[34] es un sistema de prevención y detección de intrusiones de redes (IDS / IPS) de código abierto perfeccionado por Sourcefire. De Roesch y Green[35] se toma que la combinación de uso de firmas, el protocolo y el examen basado en anomalías, hacen que Snort sea la tecnología IDS / IPS de mayor aplicación a nivel mundial. Snort usa como complemento a BASE (*Basic Analysis and Security Engine*) que se fundamenta en el código de la consola de análisis de bases de datos de Intrusión del proyecto ACID. Esta aplicación suministra un *front-end web* para examinar y analizar las alertas originarias del sistema IDS Snort. BASE es desarrollado por los voluntarios de Secure Ideas[36].

OSSEC[37] (*Open Source SECurity*): Es un sistema de detección de intrusiones basado en host que efectúa análisis de registro, valida la comprobación de la integridad, hace seguimiento de políticas, realiza detección de *rootkits*, genera alertas en tiempo real y funcionalidad de respuesta activa. Se puede usar en la mayoría de sistemas operativos, incluyendo Linux, Mac OS, Solaris, HP-UX, AIX y Windows.

34 SNORT. Open source intrusion prevention system. [En línea] Organización Snort. 2016.

35 ROESCH, Martin y GREEN, Chris. The Snort Project. SNORT User's Manual 2.9.9. [En línea] Sourcefire, Inc. Cisco and/or its affiliates. 2003.

36 SECURE IDEAS, LLC. Independent security-consulting and penetration testing firm. [En línea] Jacksonville FL 32257, USA. 2016.

37 OSSEC. Bienvenido a la documentación de OSSEC. Equipo de Proyecto OSSEC. [En línea] Trend Micro, Inc. 2014.

SURICATA[38]: Es un IDS/IPS de gran rendimiento y motor de monitoreo basado en red. Es de código abierto y es propiedad de la Fundación Seguridad de la Información abierta (OISF), que es una fundación sin fines de lucro organizada y mantenida por una comunidad de seguidores. Suricata es perfeccionado constantemente por el OISF y expertos en pruebas de penetración.

SAMHAIN[39]: es un sistema de detección de intrusos basado en host (HIDS) facilita la comprobación de integridad de registros, así como el descubrimiento de *rootkits*, detección de los ejecutables que se les ha dado permisos de superusuario considerados malignos, supervisión de puertos, y procesos que están ocultos. Samhain se considera una aplicación multiplataforma de código abierto empleado en sistemas POSIX, Unix, Linux, Cygwin / Windows.

EASYIDS[40]: Es un sistema de detección de intrusos y es muy fácil de instalar basado en Snort. EasyIDS puede ser usado por principiantes de seguridad de red con práctica mínima de Linux. EasyIDS incluye Linux CentOS, Corral, Snort, MYSQL, NTOP, BASE, Arpwatch entre otras aplicaciones.

SMOOTH-SEC[41]: Es una distribución Linux basada en Debian que contiene un IDS/IPS totalmente listo y muy liviano. Contiene Snorby, Suricata, Snort, Pocilga y Pulledpork. Tiene un proceso de fácil configuración que admite desplegar en cuestión de minutos, un sistema IDS/IPS totalmente funcional, sin apoyo de expertos, incluso para los novatos de seguridad con experiencia pequeña de Linux.

PATRIOT NG[42]: es una sencilla aplicación que se ocupa de monitorear sistemas Windows. Este programa avisa de los cambios que se causan en el ordenador, dando la posibilidad de permitirlos o rechazarlos.

38 SURICATA. IDS / IPS Suricata. Entendiendo y configurando Suricata. [En línea]. Open Information Security Foundation (OISF), 2011.

39 WICHMANN, Rainer. The SAMHAIN file integrity / host-based intrusion detection system. [En línea]. Samhain Labs. 2006.

40 EASYIDS. Distribución de sistema de detección de intrusiones de código abierto basada en Snort. [En línea]. 2011.

41 SMOOTH-SEC. Smooth-Sec. Sistema IDS / IPS con motor Suricata e interface Snorby. [En línea]. Daboweb. 2011.

42 PATRIOT N.G. Host IDS tool. Monitoring of changes in Windows systems or Network attacks. [En línea] Security Projects. Julio 08, 2016.

TRIPWIRE[43]: es el IDS basado en host más aclamado para Linux. Asegura controles fundamentales para proteger a las empresas contra ataques cibernéticos junto con cumplimiento continuo y eficiencia operacional. Los desarrolladores de Tripwire Inc. liberaron últimamente el código fuente para la versión basada en Linux y fue licenciado bajo los términos de la Licencia Pública General GNU.

RPM COMO UN IDS: El Manejador de paquetes RPM[44] es otro programa que puede ser empleado como un IDS basado en host. Incluye varias opciones para examinar paquetes y sus contenidos. Dichas opciones de verificación son invalorables para un administrador que sospeche que sus archivos de sistema y ejecutables críticos hayan sido cambiados.

SWATCH[45]: Este programa trae archivos de registro generados por *syslog* (estándar para el envío de mensajes de registro en una red) para notificar a los administradores de las incoherencias en el registro del equipo, basándose en los registros de configuración del usuario. SWATCH fue planteado inicialmente para registrar cualquier evento que el usuario desee agregar en el archivo de configuración; sin embargo ha sido empleado ampliamente como un IDS basado en host.

LIDS[46]: El sistema de detección de intrusos Linux (*Linux Intrusion Detection System*) es un parche del *kernel* y es un útil instrumento de administración que adicionalmente puede vigilar la modificación de ficheros a través de las listas de control de acceso (ACLs) y preservar procesos y archivos, incluso del propio superusuario.

Aunque en el presente proyecto no se trabajó con IDS de Pago, es importante que se conozcan algunos de ellos creados por importantes compañías de tecnología, como por ejemplo: Cisco Systems, Computer Associates (CA), Enterasys Networks, Intrusión.com e Internet Security Systems (ISS).

[43] BRAVO, Diego. Guía breve Tripwire . [En línea]. Tripwire INC. Portland, OR 97204. 2007.

[44] RPM. RPM as an IDS. [En línea]. Red Hat, Inc. 2016.

[45] SWATCH. The Simple Log Watcher. A real time monitoring tool for your logs. [En línea] Linux Magazine. QuinStreet Inc. 2016.

[46] LIDS. Linux Intrusion Detection System. [En línea] Slashdot Media. 2016

En un análisis realizado por expertos de Networtworld[47], se indica que los mejores son Secure IDS de Cisco y RealSecure de ISS. El producto IDS Dragon de Enterasys obtuvo excelentes resultados en cuanto a rendimiento, pero su complicada instalación y configuración, así como algunos aspectos poco pulidos de su gestión, lo confinaron a la segunda posición. En oposición, eTrust, de CA, destacó por una poderosa gestión, así como por una estupenda funcionalidad. Su diligencia de gestión es lógica e intuitiva, aunque trae demasiadas aplicaciones separadas, lo que restringe su facilidad de uso. El último de los cinco, fue SecureNet Pro, de Intrusion.com, resultó el más sencillo de instalar (en 15 minutos estaba funcionando), pero exhibe algunos problemas de rendimiento, lo que contribuyó a reducir su puntuación global.

Luego de la breve revisión de todos estos programas de seguridad, se considera que es pertinente estudiar un poco más a fondo algunos de esos IDS de software libre, especialmente los basados en red, para determinar cuál es el más apropiado para realizar el análisis de la red de la Gerencia Departamental Colegiada del Caquetá. Los NIDS que se eligen son: SNORT, SURICATA, EASYIDS y SMOOTH-SEC, por cuanto son los más usados y/o por su facilidad de instalación.

### 4.1.1 SNORT

Este IDS implanta un lenguaje de creación de reglas flexibles, sencillas y potentes. Durante su instalación provee de cientos de filtros o reglas para *backdoor*, ataques web, Ddos, CGI (*Common Gateway Interface*), *finger* (protocolo que proporciona información de los usuarios de una máquina), escaneos Nmap, FTP, buffer *overflows*, escaneos de puertos *stealth* (invisibles), ataques a aplicaciones web, entre otros.

Puede marchar como *sniffer* (ver en consola y en tiempo real qué sucede en la red), registro de paquetes (guarda en un archivo los registros para su posterior examen) o como un IDS puro (es decir un NIDS).

La ubicación de Snort en la red puede realizarse según qué tráfico se quiere vigilar: paquetes que entran, dentro del firewall, paquetes salientes, fuera del firewall, y en realidad prácticamente donde se quiera.

[47] NETWORTWORLD. Sistemas de detección intrusiones. Comparativa. [En línea] España. 2001.

Una característica muy significativa e implementada desde hace pocas versiones es FlexResp que concede la posibilidad de dar de baja una conexión maliciosa, mediante el transporte de un paquete con la bandera RST (para reiniciar una conexión debido a paquetes corrompidos) con lo cual efectuaría funciones de firewall, cortando las conexiones que verifiquen ciertas reglas predefinidas.

Análisis del Proceso de instalación:

Snort puede ser instalado en una gran variedad de sistemas operativos, para el caso de Linux, se observa obviamente que hay que tener mucho cuidado de seleccionar el instructivo acorde a la distribución Linux que se use, de lo contrario, los comandos no servirán y se perderá gran cantidad de tiempo. De los manuales revisados se observa que se requieren gran cantidad de pasos y la ejecución de comandos complejos para hacerlo funcionar en Linux. Esta parte le da una calificación negativa a la hora de elegirlo como IDS, para las pruebas del presente proyecto.

La versión para Windows es más sencilla de instalar, sin embargo, se tiene el inconveniente que Snort requiere que el equipo donde se instale tenga dos tarjetas de red, una para administración y otra para capturar los paquetes de la red y analizarlo, esto puede ser un inconveniente en algunos casos.

### 4.1.2 SURICATA

En este NIDS el *Multi-Threaded Processing* se convierte en una de las características más importantes ya que permite la ejecución de muchos procesos y subprocesos de forma simultánea. Se puede asignar un número determinados de subprocesos por cada CPU. De esta forma está puede entre otras cosas, procesar una gran cantidad de paquetes de forma simultánea aumentando consecuentemente el rendimiento.

Este completo sistema cuenta con módulos de captura de paquetes, detección y comparación de firmas, decodificador, procesamiento de eventos y generación de alertas.

Adicional a los protocolos IP, TCP, UDP e ICMP, Suricata usa palabras claves para otros protocolos como HTTP, FTP, SMB, TLS. De esa forma se pueden estructurar reglas independientemente del puerto que use un protocolo determinado, ya sea por defecto o no, porque su detección es automática.

Suricata, independientemente de las alertas, vuelca todas las peticiones HTTP en un archivo para estadísticas y análisis de rendimiento. El registro de estas peticiones se almacena en formato de Log en un servidor Apache local.

Análisis del Proceso de instalación:

El proceso de instalación es común a las instalaciones sobre Linux: descargar paquetes, instalarlos, modificar los archivos de configuración de acuerdo a las necesidades y por tanto tiene la limitante de tener las versiones adecuadas, que se correspondan con los comandos que se estén usando. En la literatura estudiada, no se aprecia que tenga aplicación para facilitar el proceso de lectura e interpretación de las alarmas, en su lugar, en los manuales, se indica que se tiene que hacer un proceso manual, lo cual no es eficiente.

### 4.1.3 EASYIDS

Es una distribución Linux basada en CentOS y que su propio nombre lo define como un IDS muy fácil de usar. Está basado en Snort que además viene con una cuenta con Ntop (monitoriza en tiempo real una red) y otras herramientas como Nmap (rastreo de puertos), Arpwatch (detección de anomalías en direcciones MAC), Stunnel (creación de túneles TLS/SSL) para sensores remotos, etc. Todo se administra a través de una interfaz desde la que se pueden configurar todas las herramientas, sus opciones, reglas, etc.

Luego de instalarlo usando el mismo equipo u otro cualquiera de la red y empleando un explorador de internet, se escribe la IP donde fue instalado y se accede a la interface gráfica. Para acceder se escribe el nombre y clave por defecto que son “admin” y “*password*” respectivamente. Es imperativo que estas claves se cambien en el primer inicio, de lo contrario, cualquiera podría entrar y alterar la configuración.

Ya ejecutando el programa, se observa que las secciones más importantes de esta interface gráfica de EasyIDS son *Analysis* y *Setting*. Con la primera se analiza el comportamiento de Snort a través de la interface BASE y así ver las actividades del sistema, las alertas generadas, etc. Con la segunda se pueden configurar los elementos más importantes del sistema como Arpwath, Stunnel, Barnyard (almacena y procesa las salidas binarias de Snort), Ntop y el propio Snort. Otra sección es Graphs, que genera gráficas del rendimiento de la red y de muchísimos

otros parámetros, como uso de la CPU, de la memoria, de las alertas por segundo, etc.

Otra no menos importante sección es la de Status, ya que permite comprobar el estado del sistema en general y advierte si algo no está funcionando bien. Por último la sección Tools, facilita las tareas de administración, ya que se encuentra la herramienta Nmap para escanear equipos y la herramienta *logviewer* para examinar los archivos de registro del sistema.

Análisis del Proceso de instalación:

Se descarga una imagen ISO de internet y se puede instalar rápidamente sobre un disco duro en blanco. Es muy sencillo todo el proceso de instalación, el proceso de configuración no es muy complicado tampoco. Tiene una interfaz gráfica para análisis de las alertas.

### 4.1.4 SMOOTH-SEC

Este es un sistema de detección/prevención de intrusiones IDS / IPS cuyo motor está basado en Suricata y con una interface Web Snorby para su gestión.

Se indica que Snorby es un front-end web, para la gestión de alertas IDS/IPS basado en sensores. En el caso de Smooth-Sec su interface gráfica es muy sencilla, que muestra de forma completa los diferentes tipos de alertas que va generando el sistema a medida que trabaja.

Está montado sobre Linux UBUNTU 10.04 LTS. Se trata de un sistema completamente configurado y listo para usarse.

Análisis del Proceso de instalación:

La instalación es muy sencilla e incluye las operaciones normales de una instalación Debian / Ubuntu, tales como configuración de particiones, guiadas o no, GRUB, etc. Una vez realizada la instalación se reinicia, se indica *password* para la cuenta *root*, se siguen las indicaciones de la instalación. Por último se configura la interface de red. Una pantalla indica, con base a la IP configurada, la forma de acceder a la interface web Snorby mediante HTTPS.

### 4.1.5 Comparativa de los cuatro IDS Preseleccionados

Al finalizar la revisión de la literatura de los anteriores IDS se establece que los criterios de selección deben ser los siguientes:
Plataforma Linux: por cuando es un Sistema Operativo seguro, la gran mayoría de los IDS vistos usan esta plataforma.
Basado en Red: Dado que se quiere detectar la presencia de terceros en la red local, se debe usar este tipo de IDS, además los basados en host implican instalar una copia del IDS en cada máquina, lo cual no es eficiente.
Facilidad de uso: dado que es probable que la entidad lo siga usando, se requiere un IDS que se pueda ser aprendido a operar fácilmente.
Facilidad de instalación: El IDS seleccionado debe ser fácil de instalar, ya que una instalación compleja da lugar a que se comentan errores de configuración.

Con esto en mente, se crea el cuadro 2 para realizar la comparación y seleccionar el IDS más adecuados al presente proyecto.

Cuadro 2. Comparación de los IDS

| | Snort | Suricata | EasyIDS | Smooth-Sec |
|---|---|---|---|---|
| Facilidad de instalación | | | X | X |
| Facilidad de uso | | | X | X |
| Basado en red | X | X | X | X |
| Para Linux | X | X | X | X |

Fuente: El autor

Este resultado se basa en que de la literatura consultada Snort y Suricata son IDS muy robustos, bastante completos en la detección de intrusos. Pero, aunque la instalación del Snort o Suricata es muy sencilla, ya que con tres o cuatro comandos queda instalado y ejecutándose, la dificultad grande se encuentra cuando se intenta configurar las herramientas adicionales como Barnyard2 o Snorby para obtener una interfaz gráfica para un análisis más cómodo de los resultados. Por ello no se califican como de fácil instalación o fácil uso

La principal causa de esto es que las instrucciones que se encuentran en internet no funcionan totalmente en determinadas distribuciones y por ello instalar Snort o Suricata sobre un sistema Linux preexistente puede resultar muy engorroso y al final no funcionar adecuadamente.

En consecuencia quedan dos IDS que tienen una mayor facilidad de instalación y de uso, además de estar basados en red y diseñados para plataformas Linux. En

vista de ello y para una mayor oportunidad de seleccionar el IDS más adecuado se opta por probar preliminarmente ambos programas: EasyIDS y Smooth-Sec.

## 4.2. INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA DE DETECCIÓN DE INTRUSOS

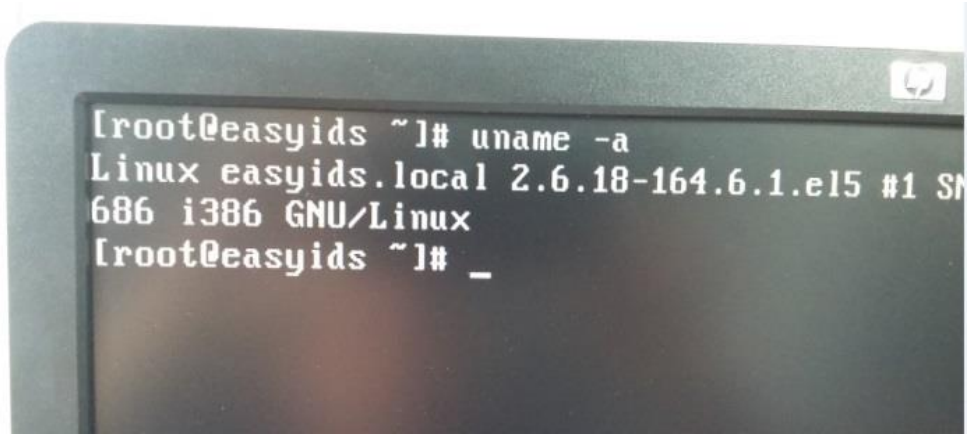
### 4.2.1 Determinación de cuál IDS es el más adecuado

De acuerdo a lo visto anteriormente, quedan preseleccionados EasyIDS y Smooth-Sec que tienen procesos de instalación muy sencillos y usan motores de detección robustos como son Snort y Suricata. Es importante indicar que estos dos programas cuentan con imágenes ISO que instalan un sistema Linux funcional y con la mayoría de parámetros ya configurados.

#### 4.2.1.1. Prueba de Instalación y funcionamiento de EasyIDS

Se instaló EasyIDS sobre un equipo dedicado, ver figura 3. En este equipo se hizo necesario instalar una segunda tarjeta de red, para que EasyIDS funcionara correctamente. La IP de la eth0 es 192.168.125.155 y la eth1 es 192.168.125.115.

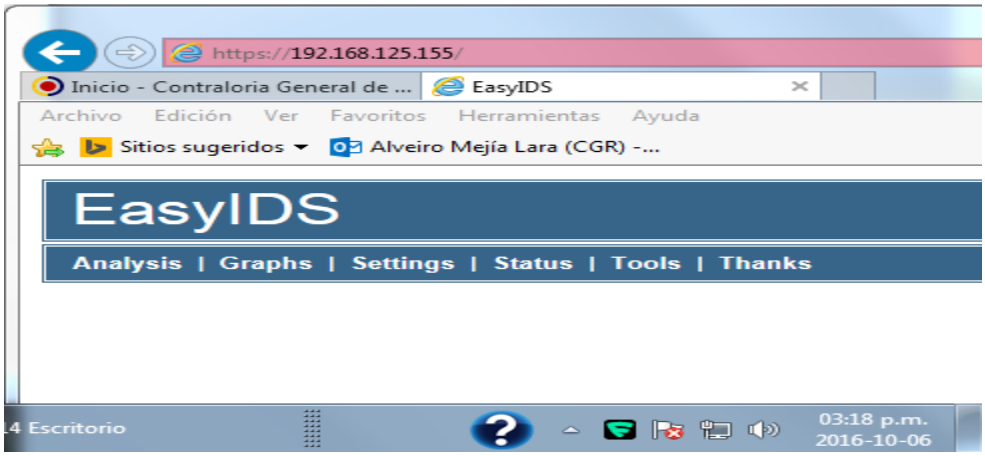
Figura 3. Equipo dedicado para EasyIDS




Fuente: El Autor

Para ejecutar EasyIDS se usa otro equipo de la red y se accede mediante la siguiente URL: https://192.168.125.155, el resultado se observa en la figura 4.

Figura 4. EasyIDS en funcionamiento




Fuente: El Autor

El usuario por defecto es “admin” y la clave de acceso es “password”, que obviamente hay que cambiar de inmediato. Luego pide cambiar la clave de Mysql.

En la figura 5 Se observa que todos los servicios de EasyIDS están en funcionamiento.

Figura 5. Servicios de EasyIDS

**System Status**

| Services | |
|---|---|
| Arpwatch | RUNNING |
| Barnyard | RUNNING |
| CRON server | RUNNING |
| MySQL | RUNNING |
| NTOP | RUNNING |
| NTP Server | RUNNING |
| Secure shell | RUNNING |
| Snort | RUNNING |
| Stunnel | RUNNING |
| Web server | RUNNING |

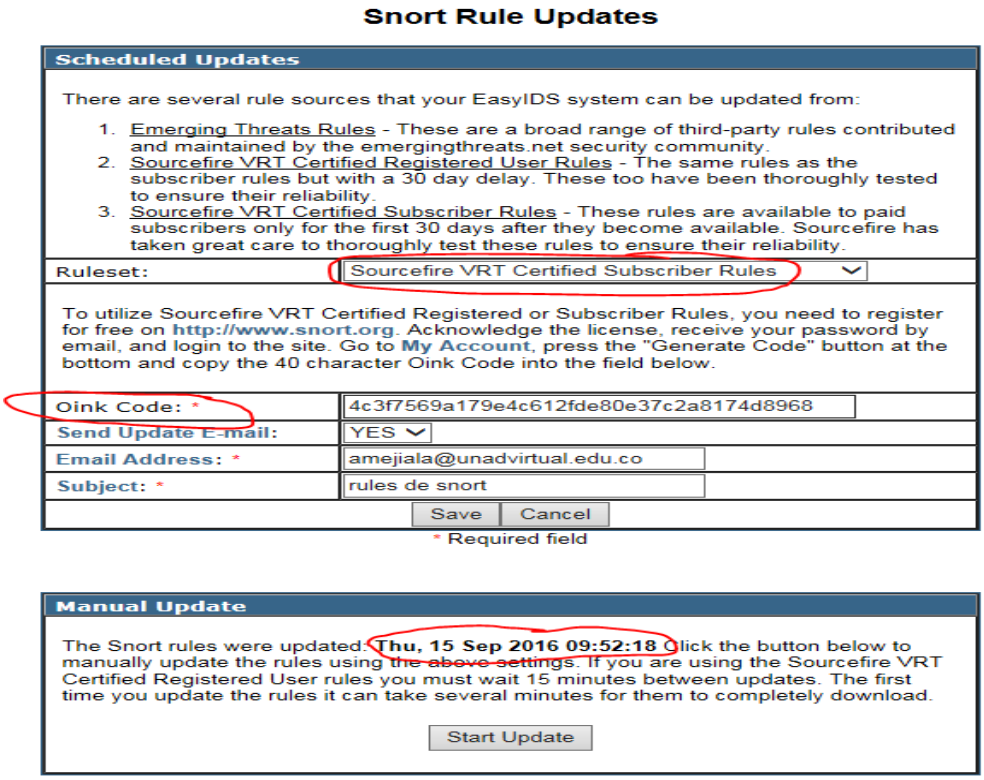
Fuente: El Autor

Lo primero que se hace es editar la línea del archivo /etc/snort/snort.conf para indicar que la red está en el rango 192.168.125.0/24.
Luego se actualizan las reglas, usando la ruta Setting > Snort > Rule Updates donde se especifica el juego de reglas, el Oinkcode y nos indica la fecha de la última actualización, tal como se observa en la figura 6.

Es importante indicar que las reglas o firmas son los patrones que se buscan dentro de los paquetes que son analizados por Snort, si encuentra una coincidencia genera una alerta, ya que la presencia de estos patrones puede indicar un posible ataque.

El Oinkcode es una clave única asociada a las cuentas de los usuarios que se registran en la página de Snort, esta clave permite descargar los paquetes de reglas actualizadas.

Figura 6. Actualización de reglas




Fuente: El Autor

Luego de lo cual, las reglas quedan actualizadas

Se lanzan los siguientes escaneos desde Kali Linux Virtualizado, estos escaneos son simples y sólo para captura de información.

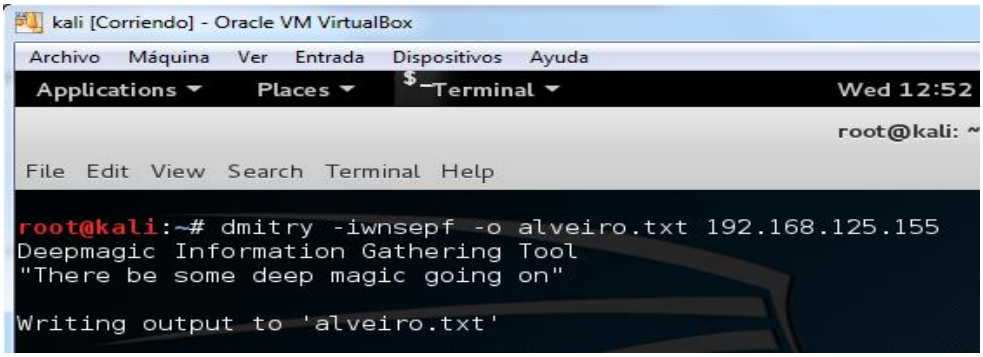
Escaneo 1**: *dmitry -iwnsepf -o alveiro.txt 192.168.125.155***

Dmitry[48] (*Deepmagic Information Gathering Tool*) es una herramienta de Recopilación de Información de Deepmagic, es una aplicación de línea de comando de Linux. Esta herramienta reúne tanta información como sea posible sobre la máquina víctima, tales como subdominios posibles, direcciones de correo electrónico, exploración de puertos TCP, información de tiempo de actividad, consultas de Whois y más. En la figura 7 se aprecia el comando que tiene las siguientes opciones.

-i Realiza una búsqueda Whois en la dirección IP 192.168.125.155
-w Realiza una búsqueda Whois en el nombre de dominio de un host
-n Recupera de Netcraft.com información sobre la máquina indicada
-s Realiza una búsqueda de posibles subdominios
-e Realiza una búsqueda de posibles direcciones de correo electrónico
-p Realiza una exploración de puerto TCP en 192.168.125.155
-f Realizar un escaneo de puerto TCP mostrando informes de salida
-o Guarda la salida del host en el archivo alveiro.txt indicado

Todas estas acciones, las debería detectar Snort y ser mostrada por BASE

Figura 7. Escaneo con dmitry desde Kali




Fuente: El Autor

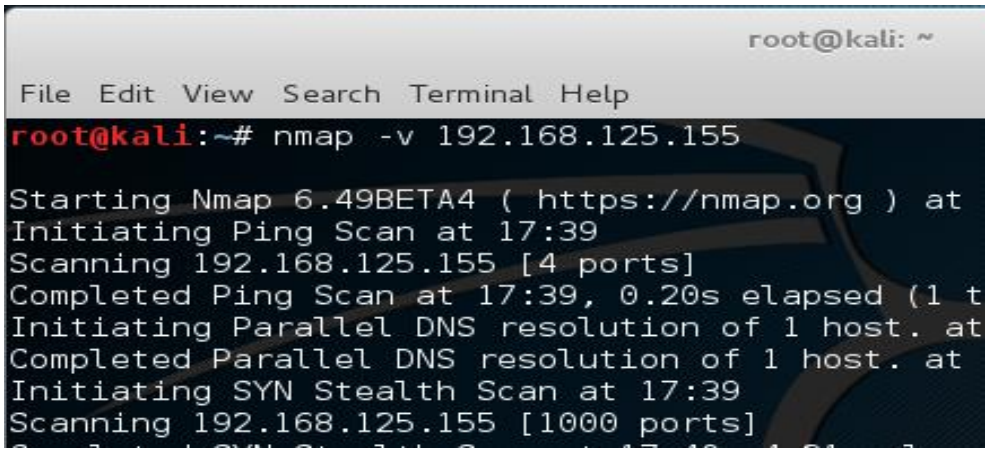
Escaneo 2: *nmap -v 192.168.125.155*

[48] KALITOOLS. Kali Linux Penetration Testing Tools. DMitry Package Description. [En Línea] 2014.

Nmap[49] es un programa de código abierto que se usa en línea de comandos de Linux, para efectuar rastreo de puertos.

En la figura 8 se aprecia que se usa nmap con la opción –v para activar el modo detallado (también llamado verboso).

Figura 8. Escaneo con nmap desde Kali



Fuente: El autor

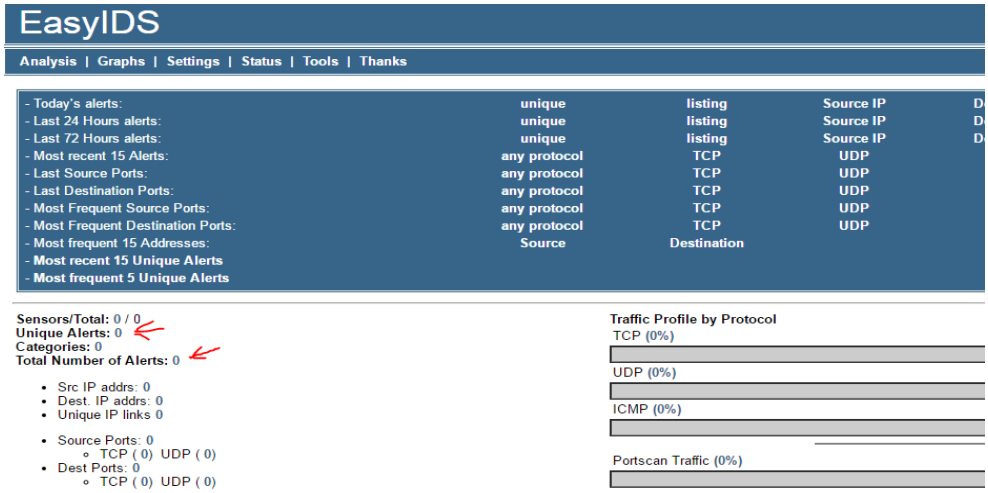
Se observa en la figura 9, que BASE no mostró advertencias sobre estos escaneos (dmitry y nmap) por lo que se supone que hay algunas características que quedaron sin configurar, pese a seguir todos los instructivos encontrados.

Esto es un punto negativo, ya que se supone que es un sistema listo para usar y sin embargo hay que configurarle demasiadas opciones e introducir muchos parámetros manualmente.

En vista de esto se procede a evaluar otro IDS que según la literatura encontrada es muy práctico.

[49] NMAP. Open source utility for network discovery and security auditing [En línea] EE.UU. 2016.

Figura 9. BASE no detecta los escaneos.



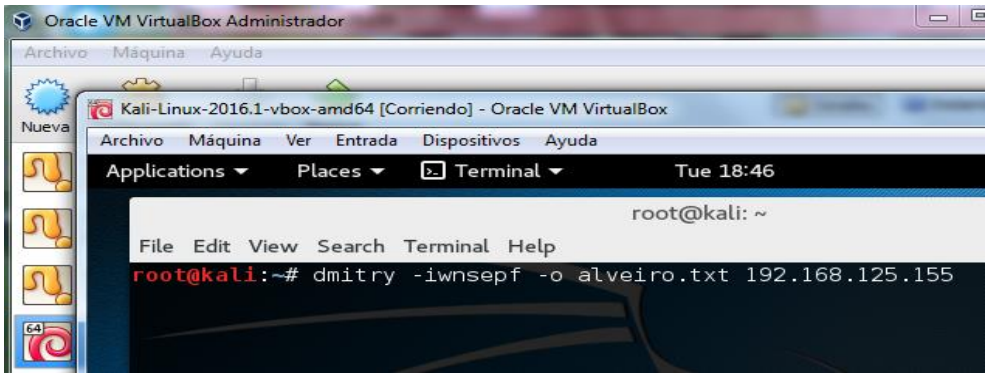

Fuente: El autor

### 4.2.1.2. Prueba de instalación y configuración de Smooth-Sec

El proceso de instalación y configuración de Smooth-Sec es muy rápido y en menos de 10 minutos está funcionando, solo hay que parametrizar aspectos globales de fácil entendimiento, por lo que es muy amigable para usuarios que no tengan mucha experiencia en estos temas.

Igualmente se pudo realizar una prueba de detección, usando los mismos comandos indicados arriba (nmap y dmnitry), que salió satisfactoria contrario a lo que sucedió con EasyIDS. Se observa en la figura 10, el lanzamiento del escaneo, para probar que el sensor esté funcionando adecuadamente.

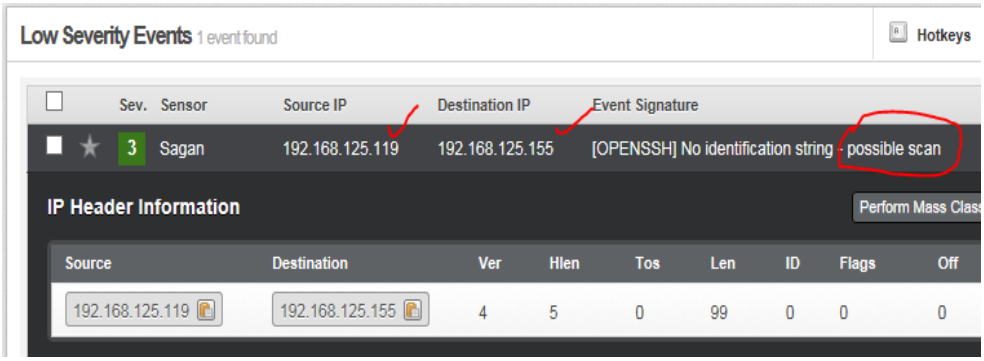
Figura 10. Escaneo desde Kali Linux usando dmitry.




Fuente: El Autor

Este comando hace un escaneo en busca de puertos abiertos y otra información sobre la máquina objetivo, lo cual es detectado por Suricata y mostrado por Snorby, ilustrado esto en la figura 11.

Figura 11. Detalle de la alerta




Fuente: El Autor

Dado que la prueba de detección del posible ataque, en este caso un escaneo, es exitosa, se selecciona a Smooth-Sec como el IDS que será instalado en la Gerencia Departamental Caquetá de la Contraloría General de la República, para el desarrollo del presente proyecto.

### 4.2.2 Instalación y Configuración del IDS Seleccionado

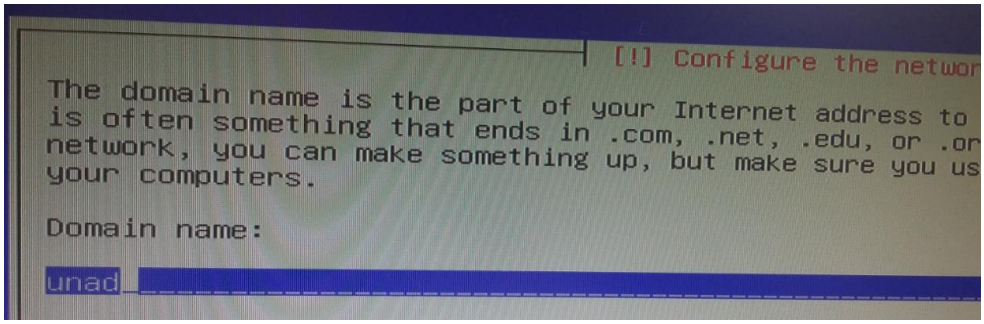
Se descarga la imagen ISO desde sourceforge.net que tiene fecha de actualización 28 de enero de 2014. Luego, con el CD se procede a instalar Smooth-Sec sobre la misma máquina en la que antes se instaló EasyIDS borrándolo completamente. En la Figura 12 se observa la pantalla inicial de instalación.

Figura 12. Instalación de Smooth-Sec


Fuente: El Autor

Luego de algunas selecciones básicas como idioma, distribución de teclado, nombre del equipo y otras, nos pregunta el nombre del dominio, dado que es una prueba se coloca el nombre “unad”.  En la figura 13 observamos este paso

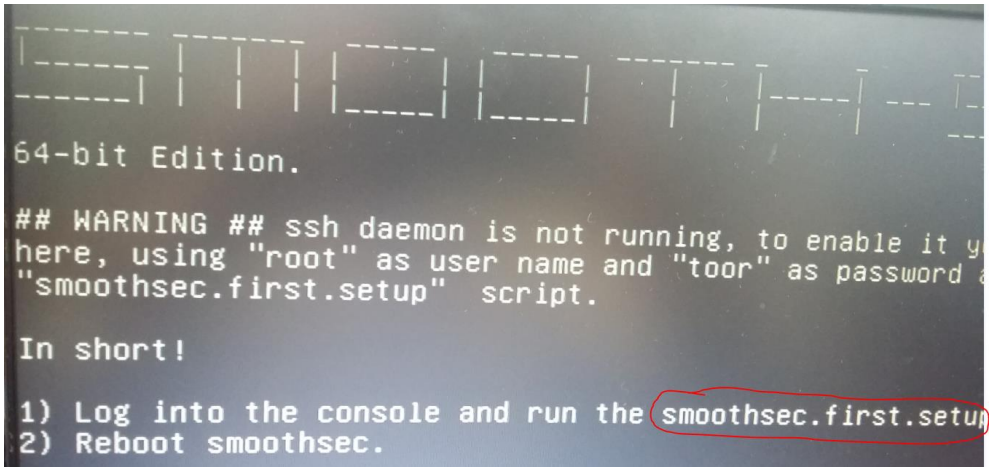
Figura 13.  Nombre de dominio




Fuente: El Autor

Luego de que se termina todo el proceso de instalación del Linux Debian 3.2, pide que ejecutemos el script que ayudará a configurar smooth-sec. En la figura 14 se observa cómo el script se llama smooth-sec.first.setup.

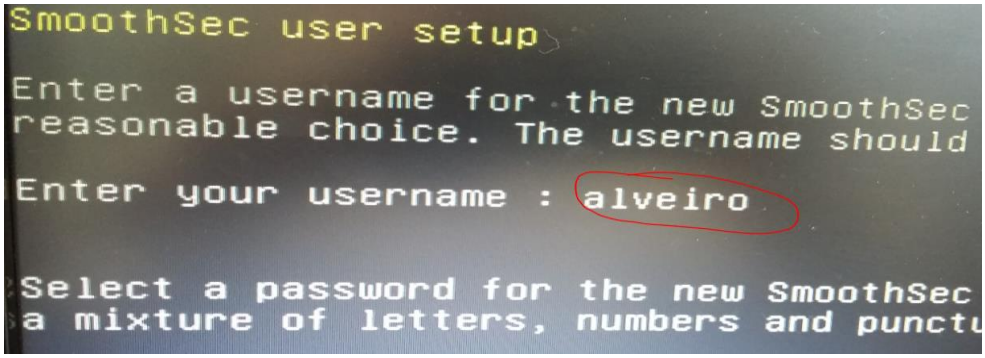
Figura 14.  Smooth-sec.first.setup




Fuente: El Autor

Este script ayuda a seleccionar el tipo de instalación de Smooth-Sec, la tarjeta que estará en modo promiscuo, definir la subred, definir nombre de usuario  (alveiro, c123) y demás parámetros necesarios para un buen funcionamiento. En la figura 15 se observa que se ha colocado el nombre del autor del presente proyecto.

Figura 15. Definición de Usuario




Fuente: El Autor

Es importante indicar que Smooth-Sec puede ser configurado en equipos con una sola tarjeta de red en los modos estándar, consola o sensor. Seleccionar estándar porque incluye el sensor y a la vez Snorby que es la interface gráfica para poder ver y entender los resultados de las detecciones.

Adicionalmente, Smooth-Sec puede ser configurado como IPS, es decir, sistema de prevención de intrusos, para lo cual se requeriría que la máquina tuviera tres tarjetas de red y los modos serían IPS- estándar, IPS- console e IPS- sensor. Algo importante que se debe mencionar es que se puede seleccionar el sensor que será utilizado.

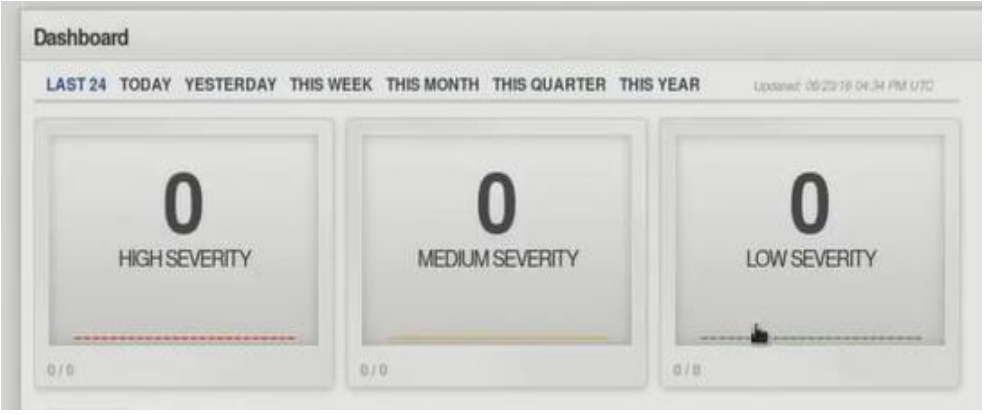
Al terminar todo este proceso de configuración se reinicia el sistema y ya se puede acceder a Smooth-sec desde otra máquina, usando un navegador y la dirección https://192.168.125.155. En la figura 16 se observa la pantalla de ingreso a Snorby. Se usa el correo electrónico suministrado en la instalación como usuario y la clave correspondiente.

Figura 16. Inicio de Snorby


Fuente: El Autor

En la primera ejecución, nos muestra la página inicial o *Dashboard* donde lo más relevante es un contador con las amenazas detectadas de acuerdo a su severidad, tal como se ilustra en la figura 17.

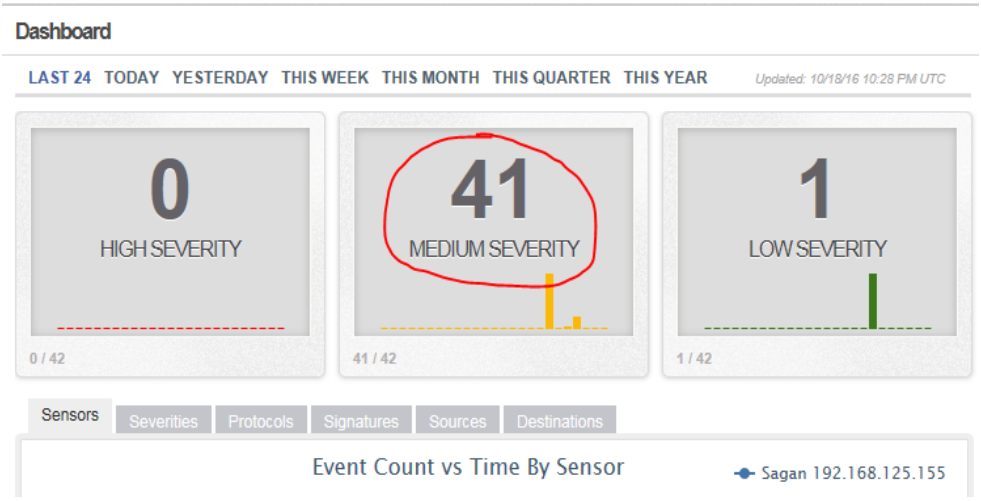
Figura 17. Dashboard




Fuente: El Autor

Como se aprecia, no se ha detectado ninguna amenaza o intento de intrusión, pero luego de un tiempo se generan alertas. Como se aprecia en la figura 18 se generaron 41 alertas.

Figura 18. Alertas por detección de equipos




Fuente: El Autor

El detalle de estas detecciones se aprecia en la figura 19. La mayoría se debe a que el sensor está identificando los equipos que pertenecen a la red local y su

correspondiente dirección IP. Esta alerta es muy importante para detectar equipos que se conecten a la red sin autorización.

Figura 19. Alertas por detección de equipos

| | | |
|---|---|---|
| 192.168.125.150 | 192.168.125.155 | [ARP] arpalert - Detected new machine on the network |
| 192.168.125.158 | 192.168.125.155 | [ARP] arpalert - Detected new machine on the network |
| 192.168.125.119 | 192.168.125.155 | [ARP] arpalert - Detected new machine on the network |
| 192.168.125.127 | 192.168.125.155 | [ARP] arpalert - Detected new machine on the network |
| 192.168.125.132 | 192.168.125.155 | [ARP] arpalert - Detected new machine on the network |
| 192.168.125.108 | 192.168.125.155 | [ARP] arpalert - Detected new machine on the network |
| 192.168.125.126 | 192.168.125.155 | [ARP] arpalert - Detected new machine on the network |
| 192.168.125.109 | 192.168.125.155 | [ARP] arpalert - Detected new machine on the network |

Fuente: El Autor

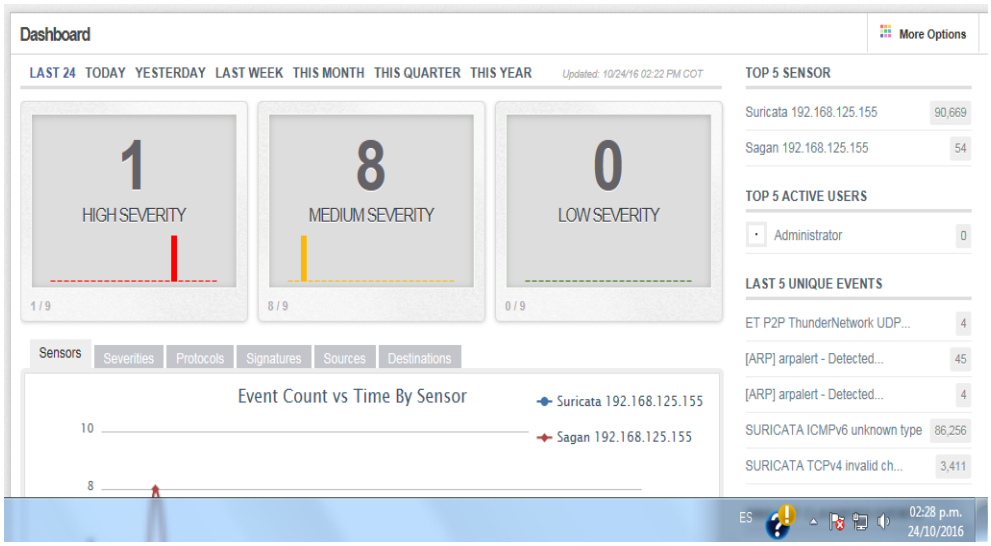
Hasta aquí llega la fase de instalación y configuración del IDS Smoothset, que como se ha evidenciado funciona correctamente, alertando sobre las situaciones que va encontrando, como un escaneo de puertos o la detección de los equipos que están conectados a la red local.

## 4.3. ESTABLECER LA EXISTENCIA O NO DE INTRUSOS

Para determinar la existencia o no de intrusos en la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República se monitoreó la red local con el IDS Smooth-sec durante parte del mes de septiembre hasta parte del mes de noviembre, obteniéndose algunos datos que se ilustran con sus respectivas imágenes.

El 23 de octubre se detectó un evento de alta severidad y ocho de mediana severidad, ilustrados en la figura 20.

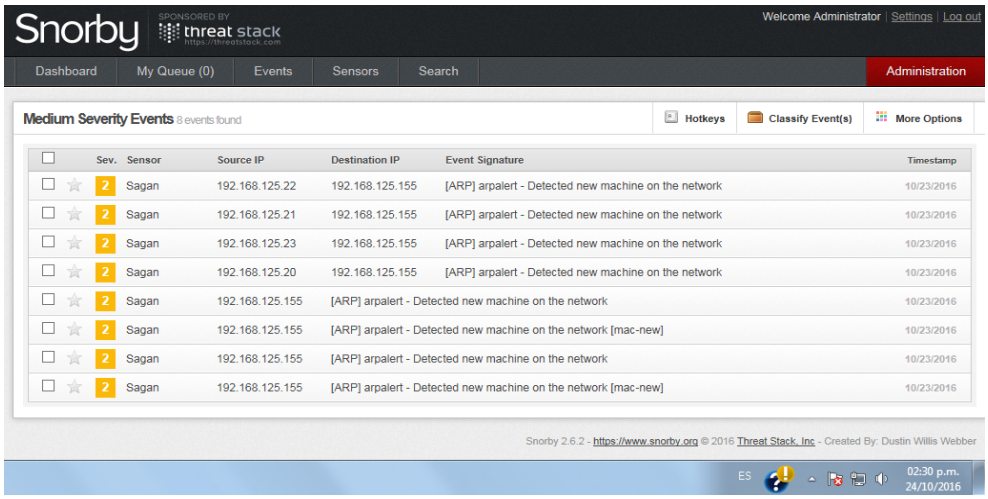
Figura 20. Detección del 23 de octubre de 2016




Fuente: El autor.

Primero se revisaron las de mediana severidad y se encontró que obedecía a detecciones de nuevos equipos en la red, equipos que son legales por lo cual se omitió el análisis de esta alerta. En la figura 21 se observa el detalle de esta alerta.

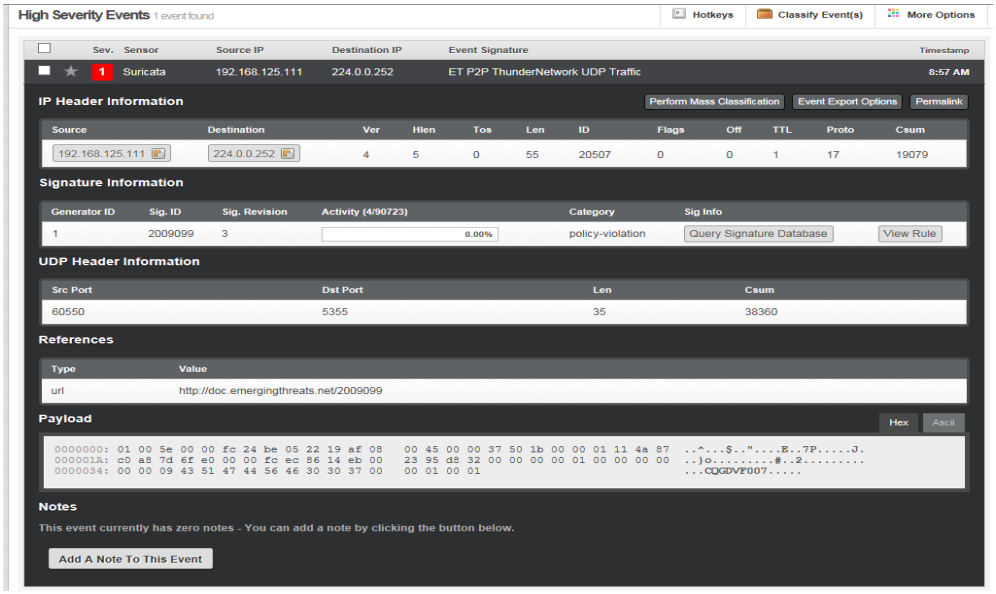
Figura 21. Detalle de alertas de mediana severidad




*Fuente: El autor.*

Posteriormente se analizó la alerta de alta severidad cuyo detalle se muestra en la figura 22, la cual a primera vista sí es preocupante porque al parecer un equipo está enviando información a una dirección IP fuera del rango de la red institucional.

Figura 22. Detalle de alertas de alta severidad

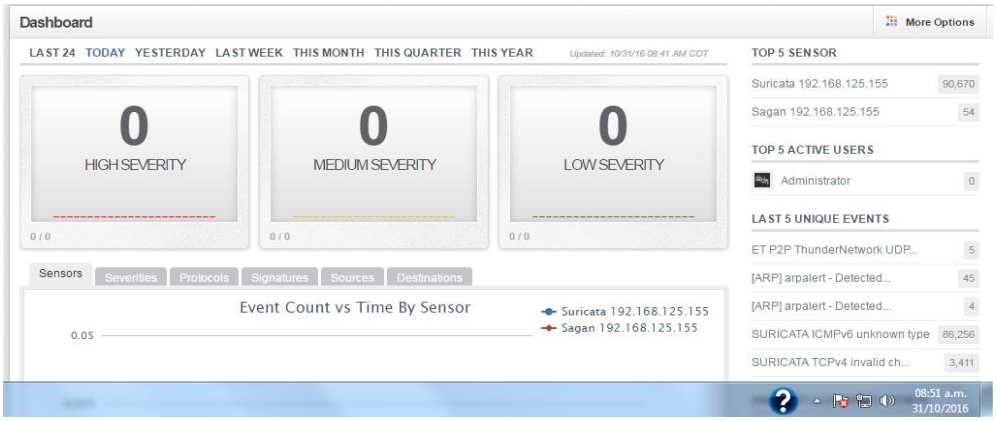



Fuente: El autor.

Al consultarse sobre esta alerta, Aragón[50] indica que la conexión a 224.0.0.252 con el protocolo UDP es utilizada por Windows para la resolución de nombres de multidifusión locales de vínculo (LLMNR) que buscan los equipos de la red local. Con lo cual esta alerta se puede obviar, dado que es un proceso normal del sistema operativo.

En la semana siguiente, es decir la correspondiente al 30 de octubre no se detectó actividad sospechosa y esto se muestra en la figura 23.

Figura 23. Actividad del 31 de octubre de 2016

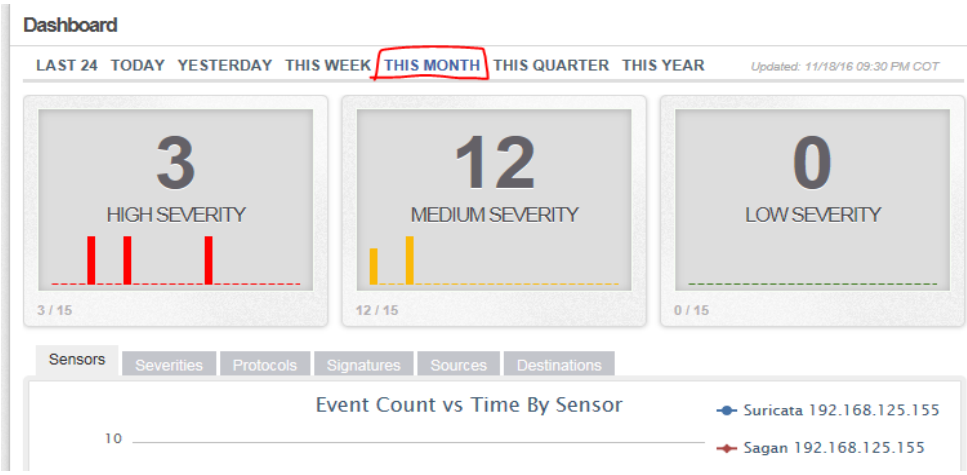



50 ARAGON. Jean. Why am I seeing lots of traffic to 224.0.0.22? Foro de WhireShark. 2011

Fuente: El autor.

Durante el mes de noviembre se detectaron tres eventos de alta severidad y 12 de mediana severidad, esto se ilustra en la Figura 24.

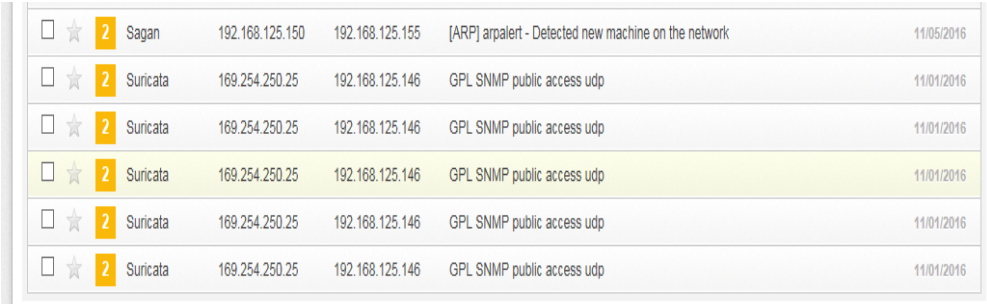
Figura 24. Detección de Noviembre de 2016




Fuente: El autor.

Se evidenció que de las doce alertas de mediana severidad siete eran por equipos nuevos válidos, pero las otras cinco eran debido a un acceso desde la IP externa 169.254.250.25 a uno de los equipos de la LAN, el 192.168.125.146. Se ilustra en la figura 25. Esta alerta es genérica y puede deberse a múltiples situaciones, porque básicamente se debe a intercambio de información de administración entre dispositivos de red.

Figura 25. GPL SNMP Public Access UDP

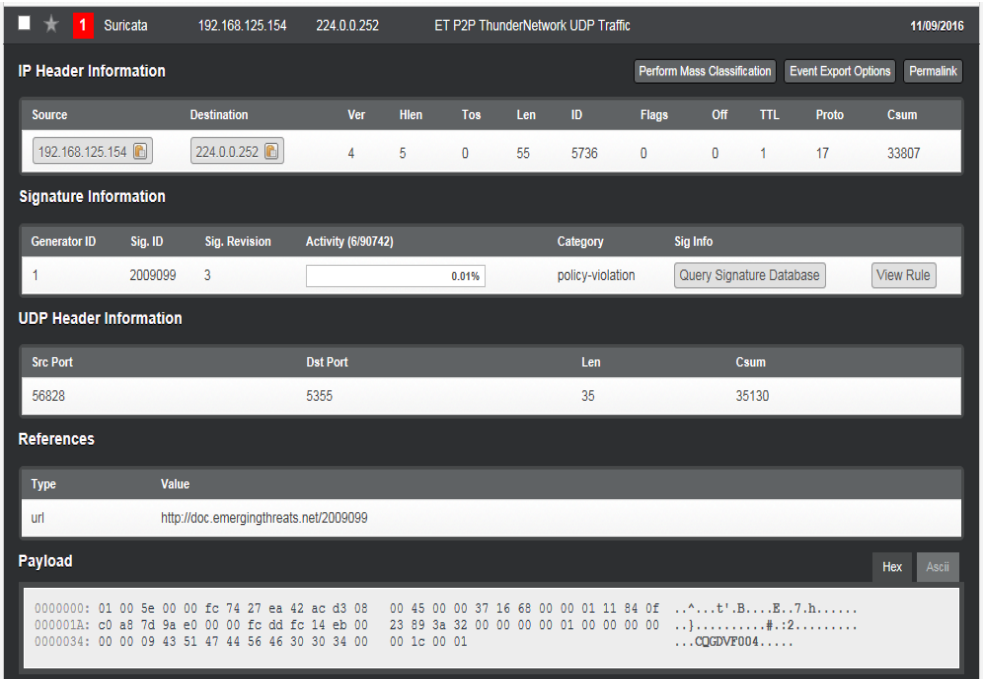



Fuente: El autor.

En cuanto a las tres alertas de alta severidad, dos eran por acceso físico al servidor donde está instalado el IDS, acceso válido. Pero el tercero, ver figura 26, se debe a

la misma actividad detectada en octubre pero desde otro equipo, se puede obviar su análisis porque es un proceso normal del sistema operativo.

Figura 26. Detección de alta severidad




Fuente: El autor.

Finalmente, después de aproximadamente tres meses de monitoreo con SMOOTH-SEC, se pudo tener una visión completa de las alertas generadas por los distintos sensores Suricata, se detectaron alertas de baja, mediana y alta severidad.

Estas actividades detectadas de baja y mediana severidad, en su gran mayoría eran equipos que se encendían luego de la instalación del IDS y que éste los registraba como nuevos equipos; otras eran accesos al servidor para realizar algún ajuste del mismo IDS.

Respecto a las alertas de alta severidad, en un principio no se sabía a qué obedecían, pero luego de un análisis se encontró que la conexión a 224.0.0.252 con el protocolo UDP era utilizada por Windows para la resolución de nombres de multidifusión locales de vínculo (LLMNR) que buscan los equipos de la red local. Con lo cual esta alerta se puede obviar, dado que es un proceso normal del sistema operativo.

Durante el tiempo de ejecución del proyecto, no se encontró evidencia de actividad fuera de lo normal como accesos desde equipos externos, navegación a deshoras, equipos que se encendieran solos, envío de paquetes a direcciones externas, etc.

Por lo anterior se puede afirmar que no hay evidencia para indicar que la red local de la Gerencia Departamental Colegiada del Caquetá haya estado bajo ataque de un intruso en los meses de ejecución del proyecto. Sin embargo, dado que un ataque se puede presentar en cualquier momento, se sugiere a la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, que deje funcionado de manera permanente este IDS o instalen otro según sus preferencias, para que puedan contar con una herramienta que les informe si se presentan eventos sospechosos en su red local.

## 4.4. RECOMENDACIONES A LA GERENCIA

El cuarto objetivo consiste en la presentación de recomendaciones a la dirección de la Gerencia Departamental Colegiada del Caquetá, con base en los resultados obtenidos. Como no se detectó evidencia que indique que actualmente la entidad esté bajo el ataque de terceros, las recomendaciones se centran en que la Entidad debe realizar actividades preventivas y no correctivas. En el Anexo B se presenta el informe respectivo y a continuación las recomendaciones presentadas:

Institucionalizar el uso de un IDS para que opere de manera permanente y en lo posible que sea usado en toda la entidad, no solamente en la Gerencia Caquetá.

Se deben analizar periódicamente las alertas que el IDS vaya generando, porque de nada serviría tener un IDS si no se revisan las alertas.

Se recomienda que adquieran un IDS comercial, por cuanto las versiones gratuitas pueden no estar totalmente actualizadas, además con una versión de pago, se tiene acceso a soporte y a capacitación para un óptimo uso de esta herramienta.

El costo de adquirir una de estas herramientas es insignificante si se compara con el beneficio que representa el evitar que intrusos puedan acceder a la red local de la Gerencia.

Adquirir e instalar programas de seguridad, como por ejemplo el PCSecure de la empresa PCtechSoft, que permitan una mayor protección de los equipos como evitar que cualquier usuario instale aplicativos, para evitar navegación en sitios maliciosos, para evitar descargar adjuntos sospechosos de correos, entre muchas otras políticas de control. Este

tipo de software también evita que los usuarios accedan a zonas sensibles del sistema operativo, como las carpetas de Windows o las de Program Files.

Inmunizar todas las USB que usan los funcionarios, para evitar que virus se copien a sus carpetas raíz. Este procedimiento es fácil y rápido y disminuye la probabilidad que usuarios traigan virus ocultos en sus archivos de uso cotidiano.

Revisar a profundidad todas las USB, con antivirus y antimalware, cada vez que las conecten a los equipos de la Gerencia. El malware día a día es más sofisticado y es necesario ser más cuidadosos.

Realizar charlas periódicas a los funcionarios sobre temas de seguridad informática, para que estén atentos y no sean víctimas de ataques de ingeniería social. Está demostrado que una de las brechas de seguridad más grande son los descuidos de los propios funcionarios.

Fortalecer el esquema de copias de seguridad de la información, usando programas que automaticen esta labor, como Cobian Backup, y en consecuencia si se presenta un ataque que dañe la información, se tenga la certeza que ésta pueda ser recuperada en su totalidad.

Asegurar que tienen actualizado, en todas las máquinas, el antivirus y demás software antimalware.

Revisar la configuración del firewall en todas las máquinas, bloqueando todos los puertos que no se usen.

# CONCLUSIONES

Existe gran variedad de IDS de software libre algunos más amigables que otros en cuanto a su configuración y uso, para el presente proyecto se determinó que el más adecuado era Smooth-sec, precisando que esto no indica que este sea el mejor ni mucho menos, simplemente, fue el que más fácil se pudo poder a funcionar.

La cuestión primera a dilucidar en la ejecución del proyecto, fue saber si el NIDS estaba funcionando y correctamente configurado, lo cual se evidenció positivamente cuando Smooth-sec detectó los escaneos de prueba que se lanzaron desde Kali, con las herramientas dmitry y nmap.

Posteriormente, se observó que Smooth-sec empezó a crear un listado con los equipos de red encontrados y generando las respectiva alertas, lo cual es muy positivo, porque en la eventualidad que alguien conectara un equipo no autorizado en la red, esto sería detectado inmediatamente.

En el periodo de análisis se detectaron muchas alertas, la gran mayoría normales por el mismo funcionamiento de la red local, pero otras alertas de alta severidad generaron cierta preocupación porque al principio no se podía establecer su origen, pero luego de consultar en varias fuentes, se encontró que eran procesos normales de los protocolos de red, propios de los sistemas operativos al interior de la entidad.

Aparte de lo anterior, no se detectó actividad de la red fuera del horario laboral, no se detectó que se encendieran equipos remotamente, no se detectó trasferencia de archivos hacia el exterior de la red, no se detectó escaneos ni dentro de la red ni de origen externo. De parte de los usuarios ninguno reportó situaciones anormales y los antivirus no detectaron amenazas de ningún tipo.

Terminado el proyecto, se pudo constatar que en la red local de la Gerencia Departamental del Caquetá, de la Contraloría General de la República, no existen evidencias de ningún tipo que puedan sugerir que durante el tiempo de ejecución del presente proyecto ocurrieran ataques por parte de un intruso.

## BIBLIOGRAFÍA


ABAD LIÑAN, José Manuel. Los dispositivos de Apple sufren el mayor ciberataque de su historia. Diario el País, Sección Tecnología. [En línea]. Madrid. 2015. [Citado en 2016-03-22]. Disponible en: < http://tecnologia.elpais.com/tecnologia/2015/09/21/actualidad/1442823415_104653.html>

AMAYA, Eduardo y QUIROGA, Laura. Evaluación del Piloto de la Herramienta de Monitoreo Alienvault en la Plataforma Tecnológica de TELECOM. [En línea] Universidad de San Buenaventura. Bogotá. 2012 [Citado en 2016-03-22]. Disponible en <http://biblioteca.usbbog.edu.co:8080/Biblioteca/BDigital/ 66647.pdf>

ANDERSON, James. Computer security threat monitoring and surveillance. [En Línea] Fort Washington, Pa. February 26, 1980. [Citado en 2016-04-15] Disponible en < http://csrc.nist.gov/publications/history/ande80.pdf >

BRAVO ESTRADA, Diego. Guía breve Tripwire . [En línea]. Tripwire INC. Portland, OR 97204. 2007. [Citado en 2016-03-22]. Disponible en <http://es.tldp.org/Tutoriales/GUIA_TRIPWIRE/guia_tripwire.pdf >

BRITOS, José. Detección de intrusiones en redes de datos con captura distribuida y procesamiento estadístico. Tesis de Maestría en Redes de Datos [En línea] Universidad Nacional de La Plata, Argentina. 2010. 156 p. [Citado en 2016-04-12]. Disponible en http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Britos_Jose_Daniel.pdf

COLLAZOS, Hernán. Técnicas de Investigación. Contenido didáctico del curso Técnicas de Investigación. [En línea].UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA Bogotá. 2007. [Citado en 2016-03-22]. Disponible en <http://datateca.unad.edu.co/contenidos/100104/1001004-MODULO-TI-2014-1.pdf>

COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 1273 DE 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47.223. p. 1-2.

COMMITTEE OF THE COMMON CRITERIA RECOGNITION ARRANGEMENT. Common Criteria for Information Technology Security Evaluation. Part 3: *Security*

*assurance requirements*. [En línea] 2016. [Citado en 2016-03-05]. Disponible en: <https://www.commoncriteriaportal.org/files/ccfiles/ccpart3v21.pdf>

CONTRALORIA GENERA DE LA REPUBLICA. ¿Qué es la Contraloría? [En línea]. Bogotá. 2016. [Citado en 2016-03-22]. Disponible en: < ria.gov.co/web/guest/que-es-la-cgr >

COTARELO, Genmota. Sistema de Detección de Intrusos. [En línea]. *Resumos e Trabalhos* México. 2011. 56 p. [Citado en 2016-03-22]. Disponible en: http://web.iti.upv.es/actualidadtic/2005/02/2005-02-intrusos.pdf >

DULAUNOY, Alexandre. RFC 2196 (Site Security Handbook) with ISO 27001 and other annotations. [En línea]. s/f. [Citado en 2016-03-25]. Disponible en: < http://rfc2196.foo.be/>

EASYIDS. Distribución de Sistema de Detección de Intrusiones de código abierto basada en Snort. [En línea]. 2011. [Citado en 2016-03-22]. Disponible en < http://www.skynet-solutions.net/development/our-software/easyids/

EL ESPECTADOR. Hackearon la página de la Procuraduría por decisión contra Petro. [En línea] Bogotá 03-ago-2011. [Citado en 2016-04-10]. Disponible en http://www.elespectador.com/noticias/judicial/hackearon-pagina-de-procuraduria-decision-contra-petro-articulo-463244

ENTER. Hackers atacan páginas del Ejército Nacional. [En línea] Bogotá 28-abr-2014. . [Citado en 2016-04-15] Disponible en /seguridad/anonymous-ataca-sitios-web-del-ejercito-de-colombia-y-mindefensa/

FLOREZ, Cesar. Hacker roba información en Bucaramanga con falso correo de la Fiscalía. Diario Vanguardia Liberal – Sección Judicial. [En línea]. Bucaramanga. 2015. [Citado en 2016-03-22]. Disponible en <http://www.vanguardia.com/judicial/ 326133-hacker-roba-informacion-en-bucaramanga-con-falso-correo-de-la-fiscalia >

GARZON, Gilberzon. Propuesta para la implementación de un Sistema de Detección de Intrusos (IDS) en la Dirección General Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC “PIDSINPEC”. [En línea] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Tunja. 2015. 78 p. [Citado en 2016-03-22]. Disponible en < http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3494/3/86057594.pdf >

GÓMEZ, Susana. Lección 5: Investigación pura, investigación Aplicada, Investigación profesional, Curso Técnicas de Investigación. [En línea] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD. Bogotá. 2008. [Citado en 2016-03-22]. Disponible en <http://datateca.unad.edu.co /contenidos/100104/100104_EXE/leccin_5_investigacin_pura_investigacin_aplicada_investigacin_profesional.html >

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS - ICONTEC. Organismo Nacional de Normalización de Colombia. [En línea] Colombia. 2016. Citado en 2016-03-18]. Disponible en < http://www.icontec.org/Paginas/Home.aspx>

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION –ISO. International Standards for Business, Government and Society. ISO/IEC 27000. Fourth edition 2016-02-15. [En línea]. ISO copyright office Génova. s/f. [Citado en 2016-03-18]. Disponible en < c066435_ISO_IEC_27000_2016(E).zip>

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION –ISO. ISO/IEC 18028-2:2006. Information technology -- Security techniques -- IT network security -- Part 2: Network security architecture. [En línea]. Génova. s/f. [Citado en 2016-03-24]. Disponible en <http://www.iso.org/iso/catalogue_detail.htm? csnumber=40009>

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION –ISO. ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®). [En línea]. Génova. s/f. [Citado en 2016-03-29]. Disponible en < http://www.iso.org/iso/ catalogue_ detail.htm?csnumber=44716>

KALITOOLS. Kali Linux Penetration Testing Tools. DMitry *Package Description*. [En Línea] 2014. [Citado en 2016-03-23]. Disponible en <.kali.org */information-gathering/dmitry>*

LARRIEU, Cyrille. Sistema de Detección de Intrusiones (IDS). Introducción a los sistemas de detección de intrusiones. [En línea] CCM Benchmark Group. 2003. 4 p. [Citado en 2016-03-22]. Disponible en < http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids>

LEMAÎTRE,Damien. La cuenta de Twitter de ‘Le Monde’, pirateada por activistas pro-El Asad. [En línea] Diario El País Internacional . Washington. 2015. [Citado en 2016-03-22]. Disponible en < http://internacional.elpais.com/internacional /2015/01/21/ actualidad/ 1421817872_541533.html >

LIDS. Linux Intrusion Detection System. [En línea] Slashdot Media. 2016. [Citado en 2016-03-22]. Disponible en <https://sourceforge.net/projects/lids/>

MIRA, Emilio. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. [En línea] Universidad de Valencia. España. 2012. [Citado en 2016-03-22]. Disponible en < http://rediris.es/cert/doc/pdf/ids-uv.pdf >

NETWORTWORLD. Sistemas de detección intrusiones. Comparativa. [En línea] España. 2001. [Citado en 2016-03-5]. Disponible en <http://www.networkworld.es/archive/sistemas-de-deteccion-intrusiones>

NMAP. Open source utility for network discovery and security auditing [En línea] EE.UU. 2016 [Citado en 2016-05-05] Disponible en <https://nmap.org/>

OSSEC. Bienvenido a la documentación de OSSEC. Equipo de Proyecto OSSEC. [En línea] Trend Micro, Inc. 2014. [Citado en 2016-03-22]. Disponible en < https://ossec-docs.readthedocs.io/en/latest/>

PATRIOT N.G. Host IDS tool. Monitoring of changes in Windows systems or Network attacks. [En línea] *Security Projects*. Julio 08, 2016. [Citado en 2016-03-5]. Disponible en <http://www.security-projects.com/?Patriot_NG>

PEREDA, Cristina. Piratas informáticos atacan la red del Ejército de EE UU. Diario El País- Sección Internacional. [En línea]. El País. Washington 2015. [Citado en 2016-03-22].Disponible en

RAMÍREZ, Egil y AGUILERA, Ana. Los Delitos Informáticos. Tratamiento internacional. Contribuciones a las Ciencias Sociales [En línea]. Eumed.net Mayo de 2009. [Citado en 2016-03-22] Disponible en <http://www.eumed.net/rev/cccss/04/rbar2.htm> ISSN: 1988-7833

ROBAYO, Eduard. Detección de intrusos en redes de telecomunicaciones IP usando modelos ocultos de Markov. [En línea] Tesis de Maestría presentada para optar al título de Magíster en Ingeniería de Telecomunicaciones. Universidad Nacional de Colombia. Bogotá, 2009. [Citado en 2016-05-05] Disponible en < http://www.bdigital.unal.edu.co/2409/1/299726.2009.pdf>

ROESCH, Martin y GREEN, Chris. The Snort Project. SNORT User's Manual 2.9.9. [En línea] Sourcefire, Inc. Cisco and/or its affiliates. 2003. [Citado en 2016-03-29]. Disponible en < >

RPM. RPM as an IDS. [En línea]. Red Hat, Inc. 2016. Citado en [2016-03-22]. Disponible en <pri se _Linux/4/html/Security_Guide/s2-ids-host-rpm.html>

SECURE IDEAS, LLC. Independent security-consulting and penetration testing firm. [En línea] Jacksonville FL 32257, USA. 2016. Citado en [2016-04-15]. Disponible en <https://www.secureideas.com/index.php>

SEMANA. Otro ataque informático a una página del Estado colombiano. [En línea] Bogotá 03-ago-2011. [Citado en 2016-03-19] Disponible en

SMOOTH-SEC. Smooth-Sec. Sistema IDS / IPS con motor Suricata e interface Snorby. [En línea]. Daboweb. 2011. [Citado en 2016-03-22]. Disponible en <https://www.daboweb.com/2011/03/14/smooth-sec-sistema-ids-ips-con-motor-suricata-e-interface-snorby/>

SNORT. Open source intrusion prevention system. [En línea] Organización Snort. 2016- Disponible en <https://www.snort.org/>

SURICATA. IDS / IPS Suricata. Entendiendo y configurando Suricata. Parte I [En línea]. *Open Information Security Foundation* (OISF), 2011. [Citado en 2016-03-22]. Disponible en < https://suricata-ids.org/

SWATCH. The Simple Log Watcher. A real time monitoring tool for your logs. [En línea] Linux Magazine. QuinStreet Inc. 2016. [Citado en 2016-03-01]. Disponible en <http://www.linux-mag.com/id/7807/>

WICHMANN, Rainer. The SAMHAIN file integrity / host-based intrusion detection system. [En línea]. Samhain Labs. 2006. [Citado en 2016-03-22]. Disponible en <http://www.la-samhna.de/samhain/.2006>

# ANEXOS

## ANEXO A. RESUMEN ANÁLITICO RAE

| | |
|---|---|
| Título de Documento. | IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED LOCAL DE LA GERENCIA DEPARTAMENTAL COLEGIADA DEL CAQUETÁ DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA |
| Autor | MEJIA LARA, Alveiro |
| Palabras Claves | IDS, Intrusion, Detection, Detección, Intrusos, LAN |
| Descripción<br><br>Proyecto aplicado para analizar el tráfico de la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, para detectar la existencia o no de intrusos. | |
| Fuentes Bibliográficas | BRITOS, José. Detección de Intrusiones en redes de datos con captura distribuida y procesamiento estadístico. Tesis de Maestría en Redes de Datos [En línea] Universidad Nacional de La Plata, Argentina. 2010. 156 p. [Citado en 2016-04-12]. Disponible en http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Britos_Jose_Daniel.pdf<br><br>GARZON, Gilberzon. Propuesta para la implementación de un Sistema de Detección de Intrusos (IDS) en la Dirección General Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC “PIDSINPEC”. [En línea] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD. Tunja. 2015. [Citado en 2016-03-22]. Disponible en <http://repository.unad.edu.co /bitstream/10596/3494/3/86057594.pdf ><br><br>MIRA, Emilio. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. [En línea] Universidad de Valencia. España. 2012. [Citado en 2016-03-22]. Disponible en < http://rediris.es/cert/doc/pdf/ids-uv.pdf > |

| | |
|---|---|
| | SMOOTH-SEC. Smooth-Sec. Sistema IDS / IPS con motor Suricata e interface Snorby. Qué es Smooth-Sec. [En línea]. Daboweb. 2011. [Citado en 2016-03-22]. Disponible en https://www.daboweb.com/2011/03/14/smooth-sec-sistema-ids-ips-con-motor-suricata-e-interface-snorby/ . 2011<br><br>SURICATA. IDS / IPS Suricata. Entendiendo y configurando Suricata. Parte I [En línea]. *Open Information Security Foundation* (OISF), 2011. [Citado en 2016-03-22]. Disponible en <https://seguridadyredes. wordpress.com/2011/02/22/ids-ips-suricata-entendiendo-y-configurando-suricata-parte-i/.> |

Contenido:

En la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, es posible que se presenten ataques de terceros interesados en obtener información sobre las auditorías y los procesos de responsabilidad fiscal que allí se adelantan.

Pese a que se cuenta con los sistemas de protección estándar como antivirus, firewall, software de seguridad del PC, filtrado WEB, esporádicamente se ha detectado malware almacenado en algunos de los computadores de la gerencia, lo que hace presumir que existen fallas en esos mecanismos de control y que además la red pueda estar bajo ataque.

En el evento que actualmente se esté perpetrando un ataque informático y éste no sea detectado y detenido mediante la implementación de un sistema de detección de intrusos, podría caer en manos de personas inescrupulosas información reservada perteneciente a las auditorias o a los procesos de responsabilidad fiscal que se adelantan en dicho ente de control.

Se requiere implementar un sistema de detección de intrusos que determine si hay intrusos actuales y disminuya la posibilidad de ataques futuros a la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República.

Para lograr esto, los objetivos fueron: estudiar algunos de los diferentes Sistemas de detección de intrusos de software libre y determinar cuál es el más apropiado para la situación particular, instalar y configurar el sistema de detección de intrusos

| |
|---|
| seleccionado, establecer la existencia o no de intrusos y finalmente presentar recomendaciones con base en los resultados del monitoreo a la red local.<br><br>Se instaló y configuró el sistema de detección de intrusos Smooth-sec que es un sistema de detección/prevención de intrusiones IDS / IPS cuyo motor está basado en Suricata y con una interface Web Snorby para su gestión. Una vez en funcionamiento Smooth-Sec, se realizó monitoreo de la red local durante los meses de septiembre a noviembre de 2016.<br><br>Se analizaron los resultados y se pudo establecer que no hay evidencia de ocurrencia de ataques informáticos durante el tiempo de ejecución del proyecto.<br><br>Finalizado el estudio se entregó un informe al representante legal de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, que contiene entre otros aspectos las evidencias del trabajo realizado y algunas recomendaciones para aumentar la seguridad de la red local y de la información en general. |
| Metodología:<br><br>Para el cumplimiento de cada uno de los objetivos particulares se siguieron los siguientes pasos:<br><br>Se estudiaron algunos sistemas de detección de intrusos basados en red.<br><br>Se determinó cuál era el más apropiado para el presente proyecto<br><br>Se instaló y configuró el sistema de detección de intrusos seleccionado<br><br>Se realizó monitoreo de la red local durante los meses de septiembre a noviembre de 2016.<br><br>Se analizaron los resultados obtenidos para establecer la existencia o no de intrusos en la red local.<br><br>Se entregó un informe a la Gerencia con recomendaciones generales, para mejorar la seguridad de la red local. |
| Conclusiones:<br><br>Existe gran variedad de IDS gratuitos en internet, algunos más amigables que otros en cuanto a su configuración y uso, para el presente proyecto se determinó que el más adecuado era Smooth-sec, precisando que esto no indica que este sea el mejor ni mucho menos, simplemente, fue el que más fácil se pudo poner a |

funcionar.

La cuestión primera a dilucidar en la ejecución del proyecto, fue saber si el NIDS estaba funcionando y correctamente configurado, lo cual se evidenció positivamente cuando Smooth-sec detectó los escaneos de prueba que se lanzaron desde Kali Linux, con las herramientas dmitry y Nmap.

Posteriormente, se observó que Smooth-sec empezó a crear un listado con los equipos de red encontrados y generando las respectiva alertas, lo cual es muy positivo, porque en la eventualidad que alguien conectara otro equipo en la red, esto sería detectado inmediatamente.

En el periodo de análisis se detectaron muchas alertas, la gran mayoría normales por el mismo funcionamiento de la red local, pero otras alertas de alta severidad generaron cierta preocupación porque al principio no se podía establecer su origen, pero luego de consultas en varias fuentes, se encontró que eran procesos normales de los protocolos de red, propios de los sistemas operativos al interior de la entidad.

Aparte de lo anterior, no se detectó actividad fuera del horario laboral, no se detectó que se encendieran equipos remotamente, no se detectó trasferencia de archivos hacia el exterior de la red, no se detectó escaneos ni dentro de la red ni de origen externo. De parte de los usuarios nadie reportó situaciones anormales y los antivirus no detectaron amenazas de ningún tipo.

Terminado el proyecto, se pudo constatar que en la red local de la Gerencia Departamental del Caquetá, de la Contraloría General de la República, no existen evidencias de ningún tipo que puedan sugerir la ocurrencia de un ataque por parte de un intruso.

Recomendaciones:

Institucionalizar el uso de un IDS para que opere de manera permanente y en lo posible que sea usado en toda la entidad, no solamente en la Gerencia Caquetá.

Se debe crear un espacio para analizar las alertas que el IDS vaya generando, porque de nada serviría tener un IDS si no se revisan las alertas.

Se recomienda que adquieran un IDS comercial, por cuanto las versiones gratuitas pueden no estar totalmente actualizadas, además con una versión de pago, se tiene acceso a soporte y a capacitación para un óptimo uso de esta herramienta.

El costo de adquirir una de estas herramientas es insignificante si se compara con el beneficio que representa el evitar que intrusos puedan acceder a la red local de la Gerencia.

Adquirir e instalar programas de seguridad, como PCSECURE de la empresa PCtechSoft, que permitan una mayor protección de los equipos, para evitar por ejemplo, que cualquier usuario instale aplicativos, para evitar navegación en sitios maliciosos, para evitar descargar adjuntos sospechosos de correos, etc. Este tipo de software también evita que los usuarios accedan a zonas sensibles del sistema operativo, como las carpetas de Windows o las de *Program Files*.

Inmunizar todas las USB que usan los funcionarios, para evitar que virus se copien a sus carpetas raíz. Este procedimiento es fácil y rápido y disminuye la probabilidad que usuarios traigan virus ocultos en sus archivos de uso cotidiano.

Revisar a profundidad todas las USB, con antivirus y antimalware, cada vez que las conecten a los equipos de la Gerencia. El malware día a día es más sofisticado y es necesario ser más cuidadosos.

Realizar charlas periódicas a los funcionarios sobre temas de seguridad informática, para que estén atentos y no sean víctimas de ataques de ingeniería social. Está demostrado que una de las brechas de seguridad más grande son los descuidos de los propios funcionarios.

Fortalecer el esquema de copias de seguridad de la información, usando programas que automaticen esta labor, y se tenga la certeza que si hay un ataque que dañe la información, esta pueda ser recuperada en su totalidad.

Asegurar que tienen actualizado, en todas las máquinas, el antivirus y demás software antimalware.

Revisar la configuración del firewall en todas las máquinas, bloqueando todos los puertos que no se usen.

**ANEXO B. INFORME A LA CONTRALORÍA GENERAL DE LA REPÚBLICA**

*Florencia, noviembre 28 de 2016*

*Señor*
*GERENTE DEPARTAMENTAL CAQUETA*
*CONTRALORIA GENERAL DE LA REPUBLICA*
*Ciudad*

*Asunto: Entrega informe detección de intrusos.*

*Una vez terminado el proceso de detección de intrusos en la red local de la Gerencia Departamental Colegiada del Caquetá de la Contraloría General de la República, me permito presentar el informe correspondiente, abordando los siguientes apartes:*

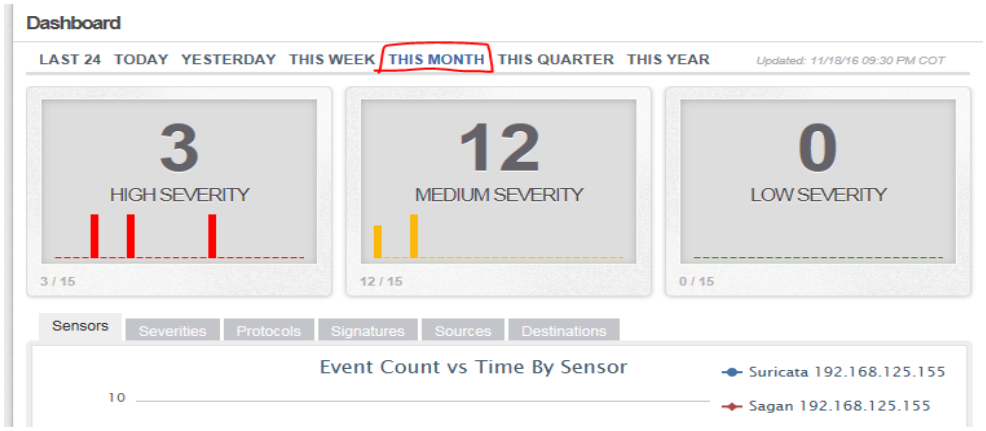
*Evidencias de la instalación del sistema de detección de intrusos*

*Se instaló el IDS Smooth-Sec en una máquina dedica, como se muestra en la imagen de abajo, el IDS realizó el monitoreo por espacio de dos meses. Este software es gratuito y no hay inconvenientes con la licencia.*

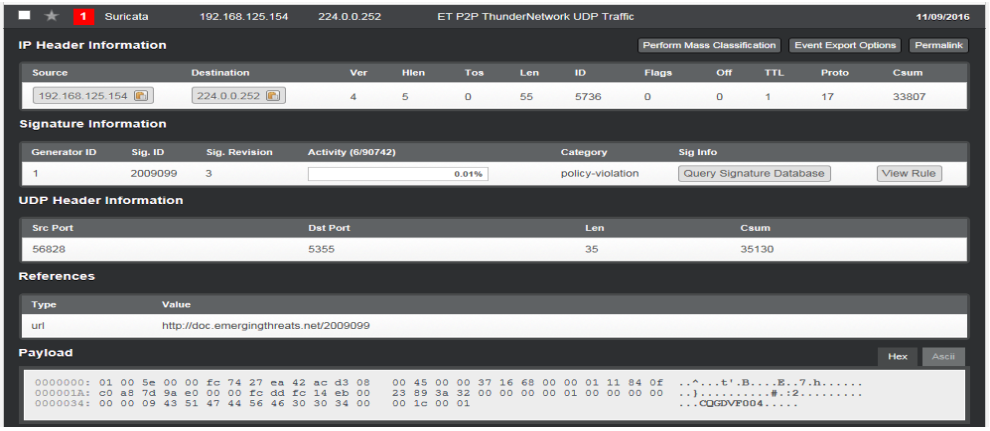

*Análisis del tráfico de red y las alertas sobre posible presencia de intrusos en la red local.*
*Se analizó el tráfico de la red local, esto de manera transparente a los usuarios y respetando la privacidad y confidencialidad de la misma, es decir, en ningún momento se leyó el contenido de la información que viaja por la red, solamente*

*se analizó por los motores del IDS si había evidencia de firmas conocidas como ataques.*

*Como se observa en la imagen de abajo, hubo varias alertas de actividades sospechosas, al analizarlas se constató que la mayoría eran causadas por eventos normales, es decir, que eran actividades propias de los funcionarios y no representaban amenazas.*




*Pero hubo una actividad que consistía en el envío de pequeños paquetes de información a una dirección por fuera de la red institucional, como se observa más abajo.*




*Sin embargo, dado que el paquete era muy pequeño como para contener información valiosa y que ocurrió solamente dos veces con muchos días de separación entre cada evento, se concluye que puede ser parte del proceso de actualización de algunos programas. Si fuera un ataque de un tercero, sería más repetitivo y con envíos de información mucho mayor.*

*Al consultarse sobre esta alerta, se encontró que la conexión a 224.0.0.252 con el protocolo UDP es utilizada por Windows para la resolución de nombres de multidifusión locales de vínculo (LLMNR) que buscan los equipos de la red local. Con lo cual esta alerta se puede obviar, dado que es un proceso normal del sistema operativo.*

*Conclusión del análisis*

*Realizar este proyecto fue enriquecedor de cuya realización se extraen las siguientes conclusiones:*

*Existe gran variedad de IDS gratuitos en internet, algunos más amigables que otros en cuanto a su configuración y uso, mientras la Gerencia adquiere uno comercial, podrían explorar varios de ellos.*

*Algunos IDS vienen preinstalados en distribuciones Linux, en formato ISO, listos para instalar, lo cual es un punto a favor en cuanto a su facilidad de instalación y esto favorece que la Gerencia tome la decisión de instalar uno permanentemente.*

*No todas las alertas que detectan los motores como Snort o Suricata, significan una amenaza, por ello, se deben estudiar a conciencia para establecer si su origen es malicioso o no. Esto adicionalmente acrecienta el conocimiento sobre redes, del personal de sistemas.*

*En la red local de cualquier empresa, se genera tráfico por el normal uso de los diferentes aplicativos por parte de los usuarios, pero también existe tráfico que generan de forma autónoma algunos programas del sistema operativo, que si no se tiene un analizador de tráfico, permanecerían totalmente desconocidas por el administrador de la red.*

*Durante los meses de análisis del tráfico de red, se detectaron varias alertas, que después de un riguroso análisis, se concluyó que no eran amenazas sino tráfico normal de los protocolos de red del Sistema Operativo y por ello se pudo constatar que en la red local de la Gerencia Departamental del Caquetá, de la Contraloría General de la República, no existen evidencias de un ataque por parte de un intruso.*

*Recomendaciones*

*Una vez terminado todo el proceso de revisión y análisis, de manera respetuosa se hacen las siguientes recomendaciones:*

*Institucionalizar el uso de un IDS para que opere de manera permanente y en lo posible que sea usado en toda la entidad, no solamente en la Gerencia Caquetá.*

*Se debe crear un espacio para analizar las alertas que el IDS vaya generando, porque de nada serviría tener un IDS si no se revisan las alertas.*

*Se recomienda que adquieran un IDS comercial, por cuanto las versiones gratuitas pueden no estar totalmente actualizadas, además con una versión de pago, se tiene acceso a soporte y a capacitación para un óptimo uso de esta herramienta.*
*El costo de adquirir una de estas herramientas es insignificante si se compara con el beneficio que representa el evitar que intrusos puedan acceder a la red local de la Gerencia.*

*Adquirir e instalar programas de seguridad, como PCSECURE de la empresa PCtechSoft, que permitan una mayor protección de los equipos, para evitar por ejemplo, que cualquier usuario instale aplicativos, para evitar navegación en sitios maliciosos, para evitar descargar adjuntos sospechosos de correos, etc. Este tipo de software también evita que los usuarios accedan a zonas sensibles del sistema operativo, como las carpetas de Windows o las de Program Files.*

*Inmunizar todas las USB que usan los funcionarios, para evitar que virus se copien a sus carpetas raíz. Este procedimiento es fácil y rápido y disminuye la probabilidad que usuarios traigan virus ocultos en sus archivos de uso cotidiano.*

*Revisar a profundidad todas las USB, con antivirus y antimalware, cada vez que las conecten a los equipos de la Gerencia. El malware día a día es más sofisticado y es necesario ser más cuidadosos.*

*Realizar charlas periódicas a los funcionarios sobre temas de seguridad informática, para que estén atentos y no sean víctimas de ataques de ingeniería social.*

*Está demostrado que una de las brechas de seguridad más grande son los descuidos de los propios funcionarios.*

*Fortalecer el esquema de copias de seguridad de la información, usando programas que automaticen esta labor, y se tenga la certeza que si hay un ataque que dañe la información, esta pueda ser recuperada en su totalidad.*

*Asegurar que tienen actualizado, en todas las máquinas, el antivirus y demás software antimalware.*

*Revisar la configuración del firewall en todas las máquinas, bloqueando todos los puertos que no se usen.*

*Atentamente*

*ALVEIRO MEJIA LARA*
*Ingeniero de Sistemas*
*Esp. En Seguridad Informática*