DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED DE LA UNAD SEDE PUERTO COLOMBIA

MARIO AVILA PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2018

DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED DE LA UNAD SEDE PUERTO COLOMBIA

MARIO LUIS AVILA PEREZ

Proyecto aplicado

Asesor Temático

Francisco Javier Hilarión Novoa

Asesor de Proyecto

Francisco Javier Hilarión Novoa

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANQUILLA
2018

Nota de aceptación :

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Barranquilla, 01 de febrero de 2018

DEDICATORIA

A mi padre celestial y a mi familia.

AGRADECIMIENTOS

A Dios por darme la fuerza para continuar luchando por mis sueños, a mi familia por apoyarme durante todo este tiempo, por la paciencia de mi esposa y mis hijos.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

ANEXOS

pág.

GLOSARIO

AMENAZA: Es la causa potencial de un incidente no deseado que pudiera provocar daños en una organización.

AUDITORIA: Proceso sistemático y documentado mediante el cual se verifica que los procedimientos se están realizando de acuerdo con los lineamientos establecidos.

AUTENTICACIÓN: Es el proceso que tiene como finalidad validar la identificación de un actor dentro de un sistema.

IDS: Acrónimo de Sistema de detección de Intrusos.

LINUX: Sistema operativo de código abierto.

SGSI: Acrónimo de sistema de gestión de la seguridad informática.

SNORT: Sistema de detección de intrusiones de código abierto que se ha convertido en un estándar de facto.

VULNERABILIDAD: Es una debilidad susceptible de ser explotada o aprovechada por alguien para causar algún daño.

RESUMEN

En este documento se plantea una propuesta para el diseño de un sistema de detección de intrusos IDS en la red de la UNAD CCAV Puerto Colombia. Inicialmente se presenta la descripción, formulación y justificación del problema, se plantea el objetivo general y los objetivos específicos del proyecto, se presenta la descripción del marco teórico y contextual del proyecto, el cual abarca una reseña histórica, y la descripción o definición de los conceptos que se desarrollan en el proyecto. Se realiza un inventario de activos informáticos del centro y se hace el levantamiento de información sobre la topología de la red con el fin de seleccionar el tipo de IDS que se ajusta la necesidad planteada. Se presenta un plan de preparación de las máquinas virtuales para la simulación de un ambiente de red, se procede con la instalación del IDS y sus componentes, y la configuración del prototipo del sistema IDS, para finalmente poner en marcha un plan de pruebas en un ambiente simulado con máquinas virtuales.

PALABRAS CLAVES

IDS, REGLAS, ATAQUE, COMANDO, ESNIFFER, INFORMACION, ISO/IEC 27001, IPS, VULNERABILIDAD, TESTING, LINUX, RED, SNORT, BACKTRACK, SERVIDOR, PAQUETE, PLUGUIN, INTERFAZ

INTRODUCCIÓN

La seguridad de la información constituye un área de especial trascendencia para una organización, debido a las amenazas a las que se han visto expuestas las organizaciones, el aumento de vulneraciones es notorio y bastaría con hacer una búsqueda en el navegador Google acerca de reportes de incidencias para darnos cuenta del riesgo al que se está expuesto al tener equipos interconectados en redes públicas o privadas.

Por esta razón se hace necesario para las organizaciones estar a la vanguardia en el área de seguridad informática sin escatimar recursos que posibiliten el diseño, implementación y mantenimiento de sistemas que coadyuven a mantener los niveles de riesgo de vulneración en rangos razonablemente aceptables.

Partiendo desde esta perspectiva, se propone el diseño de un sistema de detección de intrusiones en la red de la UNAD CCAV Puerto Colombia con la finalidad de minimizar riesgos de intrusiones en la red.

1. TITULO

Diseño de un sistema de detección de intrusos en la red de la UNAD sede puerto Colombia.

AREA DEL CONOCIMIENTO: Seguridad Informática.

2. DEFINICION DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

El aumento de vulneraciones a personas y organizaciones es notorio y bastaría con hacer una búsqueda en el navegador Google acerca de reportes de incidencias para darnos cuenta del riesgo que implica conectarse a la red de Internet sin contar con las medidas de seguridad adecuadas.

Como toda organización pública la UNAD tiene unos activos informáticos importantes en cada una de sus sedes o centros y es importante mantenerlos resguardados del uso malintencionado o de actividades delincuenciales o mal intencionadas, máxime cuando los ataques han aumentado no solamente en cantidad sino también en calidad, siendo estos ataques cada vez más sofisticados y difíciles de detectar. También es importante la protección de la información que transita por la red de la institución, estos datos son el activo más importante de la organización y no se debe escatimar ningún esfuerzo en mantenerlos protegidos.

2.2 FORMULACION DEL PROBLEMA

¿Cómo diseñar un sistema de detección de intrusiones basado en red - NIDS óptimo para garantizar la disponibilidad, la confidencialidad y la integridad de la información en la red de datos de la UNAD?

2.3 DESCRIPCION DEL PROBLEMA

En el CCAV se han presentado evidencias de actividad maliciosa sobre todo en el uso de skype, específicamente envío de mensajes en las que el propietario de la cuenta afirma no haber enviado dichos mensajes y varios casos de malware y publicidad molestosa que aparentemente para los usuarios no representa un alto riesgo. Muy a menudo los usuarios de la red suelen conectarse a la red del CCAV

con sus dispositivos móviles y o computadores portátiles los cuales podrían estar infectados por software malicioso lo cual representaría riesgo de vulneración para la red y dispositivos interconectados.

El diseño de un sistema de detección de intrusiones en la red, constituye una herramienta importante que ayudaría a mitigar el riesgo de vulneración en una red. Para la UNAD CCAV Puerto Colombia sería muy importante contar con un sistema de sensores de actividad maliciosa que pueda monitorear , analizar y generar alertas tempranas de cualquier actividad sospechosa que se detecte en la red, proporcionando información valiosa para que los administradores de la red tomen las medidas pertinentes para evitar vulneraciones en los activos de la organización.

3. JUSTIFICACIÓN

Se ha dicho que la Información es el activo más importante de cualquier organización. Algunas organizaciones prestan la debida atención al tema de la seguridad; sin embargo algunas organizaciones no son conscientes del gran riesgo al que están expuestas. A menudo esto se debe al desconocimiento de metodologías de mitigación de riesgos que protejan los activos informáticos.

La Universidad Nacional Abierta y a Distancia está realizando enormes esfuerzos e inversiones para poner al servicio de la comunidad una infraestructura que garantice la disponibilidad, integridad y confidencialidad de la información, sin embargo, como ya se ha mencionado antes, el área de la seguridad informática es crítica en cualquier organización debido al aumento de incidencias y la sofisticación de los ataque por parte de la delincuencia informática, lo que hace necesario que se esté actualizando e innovando en el área de la seguridad.

Un sistema de detección de intrusiones (IDS), contribuye a garantizar La confidencialidad, la integridad y la disponibilidad de la información, las cuales son características con las que deben contar los activos de TI, estas características son consideradas esenciales para asegurar que la información sea accesible únicamente a los usuarios debidamente autorizados, previniendo el acceso no autorizado a la información ya sea de manera voluntaria o involuntaria, contribuyendo de esta manera al logro de los objetivos de la organización.

Los sistemas de detección de intrusos IDS son una herramienta muy potente que permite la detección temprana de actividad maliciosa en la red y como tal, para la UNAD sería muy importante contar con una herramienta de este tipo que coadyuve a garantizar la disponibilidad, confidencialidad e integridad de la información, las cuales podrían verse afectadas por alguna actividad maliciosa dentro de la red.

Generalmente cuando ocurre una vulneración dentro de la red los resultados suelen ser catastróficos, dependiendo del tipo de ataque. En ese punto por decirlo de alguna manera ya el daño está hecho, ya hubo pérdida de información, dicho de otra manera, lo que se observa es el resultado o fase final del ataque. Con la implementación de un NIDS es posible detectar la intrusión en su fase inicial lo que posibilita el uso de medidas preventivas que eviten el ataque.

El desarrollo de este proyecto pretende el diseño de un sistema de detección de intrusos en la red del CCAV Puerto Colombia como una medida para minimizar el riesgo de vulneración de la información en el centro. Esta herramienta constituiría un avance importante en el área de la seguridad como una medida adicional a las ya existentes para garantizar la disponibilidad, confidencialidad e integridad de la información.

4. OBJETIVOS

4.1 GENERAL

Diseñar un sistema de detección de intrusos para la red de la UNAD CCAV de Puerto Colombia con el fin de mitigar la materialización de las amenazas en los activos informáticos.

4.2 OBJETIVOS ESPECÍFICOS

1. Identificar la topología de la red del CCAV Puerto Colombia con el fin de determinar el inventario de activos informáticos.

2. Planificar el diseño del sistema de detección de intrusos para la red de la UNAD CCAV Puerto Colombia.

3. Diseñar un plan de pruebas de pentesting que garantice la funcionalidad del prototipo del sistema de detección de intrusos en una red aislada y controlada, externa a la red de la UNAD.

5. MARCO DE REFERENCIA

5.1 MARCO TEÓRICO

5.1.1 Historia de los sistemas de detección de intrusos IDS. La historia de los IDS se inicia en los años ochenta. James Anderson propuso por vez primera monitorear las amenazas de seguridad a través de auditorías En 1980. En 1987, Dorothy Denning presentó un modelo general de un IDS, analizando pistas de auditoría, creando perfiles de usuarios basados en sus actividades. En 1988, Robert T. Morris lanzó el primer gusano de Internet que desactivó alrededor de 6.000 estaciones de trabajo Sun y VAX. El mismo año se crearon tres IDS, *Intrusion Detection Expert System* (IDES) por SRI, Haystack por la Universidad de California Davis y *Multics Intrusion Detection and Alerting System* (MIDAS) por *National Computer* Security Center. En 1990, Network Security Monitor (NSM) analizó el tráfico de red para detectar comportamientos sospechosos. En 1991, Network *Anomaly* Detection and Intrusion Reporter (NADIR) y *Distributed Intrusion Detection System* (DIDS) recopilaron los datos de auditoría de varios hosts para detectar ataques coordinados contra un granja de hosts.
Para estos sistemas era complejo garantizar escalabilidad, mantenibilidad y eficiencia, lo que llevó a los investigadores de IDS a nuevos avances en esta área del conocimiento. En 1994, Mark Crosbie y Eugene Spafford en la Universidad de Purdue propusieron agentes autónomos para el manejo de estos inconvenientes. En 1996, el IDS Basado en Gráficos (GrIDS) posibilitó la revisión del tráfico de red mediante gráficas, permitiendo la detección de ataques automáticos o coordinados a gran escala. En 1998, Ross Anderson y Abida Khattak utilizaron técnicas de recuperación de información en IDS. Wenke Lee y Salvatore Stolfo aplicaron técnicas de minería de datos para construir automáticamente modelos IDS. En 1999, se lanzó el IDS de código abierto Snort (www.snort.org) en su primera versión. En 2000, los IDS se ampliaron a la red inalámbrica ad hoc.[1]

[1] YU, Zhenwei. TSAI, Jeffrey J.-P. Intrusion Detection: A Machine Learning Approach. 3rd ed: Imperial College Press, 2011. 41p.

5.1.2 Rastreadores de red. Según Baca [2] Los rastreadores de red permiten monitorear el tráfico en una red, interceptando los paquetes, los cuales a menudo no van encriptados a menos que se use el protocolo HTTPS, lo que deja a merced de un atacante datos importantes como número de tarjetas de créditos, claves, números de cuentas bancarias entre otros.

5.1.3 Intentos de intrusión. Los eventos o incidencias que pueden afectar negativamente a la confidencialidad, integridad y disponibilidad de la información de un sistema o que intentan evitar los mecanismos de seguridad que hay establecidos, se les denomina intentos de intrusión. Las intrusiones se ocasionan de varias maneras una de estas es la de usuarios no autorizados que acceden al sistema a través de la red, también usuarios que están autorizados pero que intentan ingresar a privilegios no autorizados. Otra forma muy usual son los usuarios autorizados que utilizan los privilegios otorgados con mala intención.
Los IDS pueden prevenir este tipo de intrusiones mediante el establecimiento de protección adicional a los activos informáticos de una organización frente a las amenazas que suelen presentarse durante la utilización de los sistemas computacionales internos y externos.[3]

5.1.4 Sistemas de detección de intrusos. Un sistema de detección de intrusos básicamente es un sensor ubicado estratégicamente en una red o en un segmento de red, el cual mediante una serie de técnicas y mecanismos es capaz de esnifar el tráfico de red dirigido a cualquier dispositivo que se encuentre conectado a esta, el IDS compara los paquetes capturados con una base de datos de firmas y si encuentra coincidencias con alguna genera una alerta.

El IDS monitorea el tráfico de la red para someterlo a un análisis con el propósito de detectar actividad sospechosa y de esta manera proceder a generar una alarma.

El análisis del tráfico de la red se realiza mediante la utilización de mecanismos de identificación de patrones y métodos estadísticos o de inteligencia artificial.

---

[2] BACA URBINA, Gabriel. Introducción a la seguridad informática. Distrito Federal: Grupo Editorial Patria. 2016. ProQuest Ebook Central. 155p.
[3] CHICANO TEJADA, Ester. Gestión de incidentes de seguridad informática , IC Editorial, 2014. 20p.

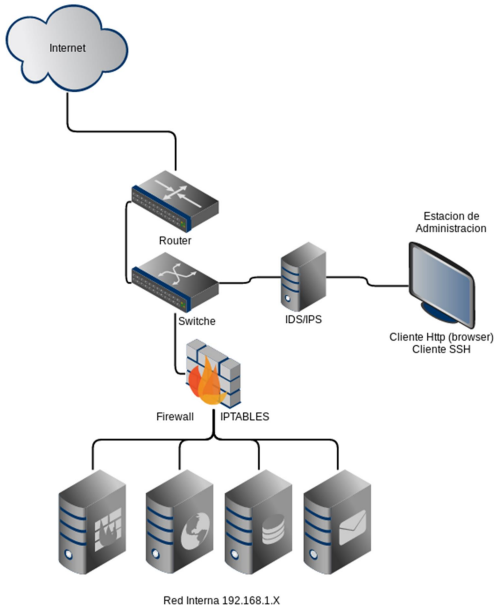
Los sistemas de detección de intrusos se fundamentan en tres pilares que son:

- Una fuente de información que proporciona eventos del sistema

- Un motor de análisis que busca evidencias de intrusiones

- Un mecanismo de respuesta que actúa según los resultados del motor de análisis

Figura 1. Esquema de la ubicación del IDS



Fuente. Autor

El objetivo de este sistema IDS es detectar acceso no autorizado a una red, esto se logra mediante el uso de snifer de red para obtener tráfico detallado de la red, se analiza este tráfico y se detecta actividad anormal que puede ser un intento de intrusión o una falsa alarma o falso positivo.

El análisis pormenorizado del tráfico de la red puede ser realizado mediante el uso de una base de firmas de ataques conocidos como puede ser escaneo de puertos, paquetes deformes, analizando el contenido y comportamiento de los paquetes.

Las bases de datos de firmas permiten al IDS distinguir entre el uso normal y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

5.1.5 Tipos de IDS. Los tipos de IDS que encontramos son:
HIDS (Host IDS): Este tipo de IDS está destinado a la protección de un servidor, PC o host. Básicamente consiste en la monitorización de los eventos que ocurren en el sistema monitorizado, determinando de manera precisa los usuarios y procesos involucrados en un evento, recolecta información de logs, archivos de sistema y recursos para analizarlos posteriormente en busca de actividad maliciosa.

NIDS (Net IDS): Se les denomina de esta manera por sus sigla (Network intrusion Detection System) Sistemas de detección de intrusos basados en red. Estos actúan en una red mediante la captura y análisis del tráfico que circula a través de la misma. Estos sniffers de red capturan y analizan los paquetes, buscando similitudes con su base de firmas que lo identifique como actividad maliciosa o sospechosa. Un IDS Se trata de un dispositivo de red configurado en modo promiscuo para capturar todos los paquetes que circulan por un segmento de red de todos los dispositivos de ese segmento.

Básicamente un IDS está constituido por la fuente: recolector de datos las cuales pueden ser un log, dispositivo de red o el propio sistema. Reglas y filtros sobre los datos y patrones para actividad sospechosa. Dispositivo generador de informes y alarmas.[4]

[4] COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014. p.137 ProQuest Ebook Central.

5.1.6 IDS – Snort. El IDS Snort es un sistema de detección de intrusos basado en red (NIDS). Consta de un motor de detección de ataques y barrido de puertos, Este sistema analiza el tráfico de paquetes de la red y lo compara con unos patrones y reglas previamente definidas en tiempo real generando alertas de actividad maliciosa en los casos que coincidan con estos patrones base de firmas. Snort (http://www.snort.org/) se distribuye bajo licencia GPL, y está disponible para sistemas operativos Windows y GNU/Linux. Es un IDS con mucha popularidad entre sus características más sobresalientes está la actualizaciones constantes de la base de datos de firmas.[5]

5.1.7 Elementos de un sistema de detección de intrusos.

5.1.7.1 Arquitectura. Un requisito mínimo que debe cumplir un sistema de detección de intrusos es que la información quede almacenada en un entorno diferente a los sistemas que se están protegiendo, con el fin de evitar que el intruso tenga la posibilidad de eliminar los registros de monitoreo.
Generalmente, a grandes rasgos un IDS está conformado por: la fuentes donde se realiza la recolección de datos, las reglas donde se describen los patrones para detección de anomalías en el sistema, los filtros que comparan la información recolectada con los patrones de las reglas, El motor de análisis y el generador de alertas e informes.

5.1.7.2 Las fuentes. Al diseñar un sistema uno de los factores más importantes es la fuente de información, una de las formas de clasificar estos sistemas es por su localización y se podrían agrupar en 4 categorías: host, red, aplicaciones y objetivo.

Los IDS basados en host (*host based*) recogen información generada por un computador u ordenador a nivel de sistema operativo.

Los IDS basados en red son llamados NIDS (*network intrusion detection*) en los que se implementa mediante un dispositivo de red promiscuo que escudriña los datos que transitan por la red monitoreada.

[5] COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014. p.138.

Los IDS basados en aplicaciones registran la actividad de una aplicación determinada, tal es el caso de los monitores de bases de datos.

Los IDS basados en objetivos (*target Based*) generan sus propios registros y utilizan cifrado para determinar alteraciones de su objetivo, son usados en sistemas que solo permiten este tipo de monitoreo.[6]

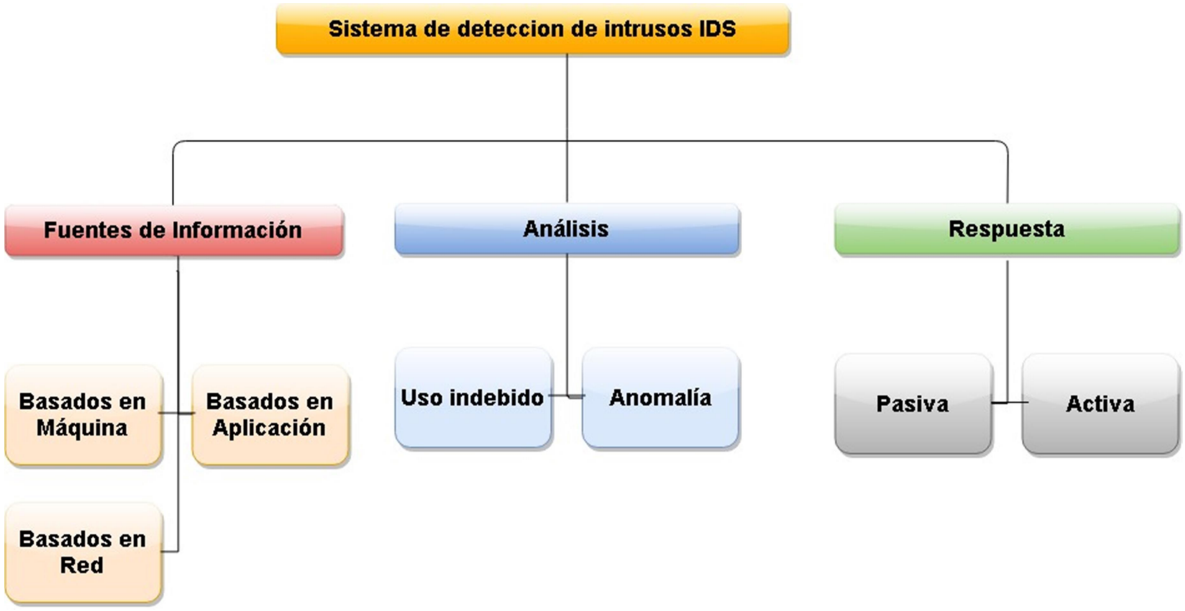
5.1.7.3 Tipos de análisis. Una vez recolectada la información esta se procesa por el motor de análisis. Puede ser procesada buscando usos indebidos "*misuse*" mediante el uso de firmas o patrones conocidos, o mediante estadísticas buscando anomalías mediante técnicas estadísticas para buscar comportamientos inusuales. En la actualidad es muy usual la combinación estas dos técnicas de análisis.

5.1.7.4 Reacción o respuesta. La reacción de un IDS ante una actividad maliciosa o sospechosa puede ser de tipo pasiva, en el caso en que simplemente se reporta la anomalía en el sistema y se genera la alarma. O activa en el caso de sistemas en los que se toman medidas para detener la actividad maliciosa o sospechosa, a este tipo de sistemas que tienen la capacidad de bloqueo de ataques se les llama IPS *(intrusion prevention System)*[7]

[6] GONZALES GOMEZ, diego. Sistemas de detección de intrusiones. {En línea}. {10 mayo de 2018} disponible en: (http://www.criptored.upm.es/descarga/IDS_v1.0.zip). p. 19

[7] GONZALES GOMEZ, diego. Sistemas de detección de intrusiones. {En línea}. {10 mayo de 2018} disponible en: (http://www.criptored.upm.es/descarga/IDS_v1.0.zip). p. 19

Figura 2. Clasificación de un IDS



Fuente: Autor.

5.1.8 El procesamiento de paquetes. El problema del análisis de paquetes en un sistema de detección de intrusos se realiza mediante el uso de algoritmos que utilizan inteligencia artificial, arboles de decisión y redes neuronales esto con la finalidad de identificar patrones maliciosos o inusuales en un sistema monitorizado.

El procesamiento de paquetes en un NIDS basado en paquetes como lo es Snort es la columna vertebral del funcionamiento del IDS, y la mejor forma de entenderlo es hacer un seguimiento a un paquete desde el comienzo hasta el final.

Todo comienza con la adquisición de los paquetes, en SNORT se trata de colocar la interface de red en modo promiscuo para la obtención de todos los paquetes que transitan en la red monitoreada, una vez el paquete está dentro del IDS, se inicia la decodificación del paquete. Luego que se ha decodificado el paquete este pasa al preprocesador o motor de análisis, para el proceso de normalización y análisis estadísticos, en esta etapa se pueden aplicar algoritmos de inteligencia artificial tales como redes neuronales y árboles de decisión; una vez es terminado el preprocesamiento, el paquete pasa a al motor de detección donde es evaluado contra las reglas las cuales son cargadas previamente, y finalmente el

archivo es enviado hacia el plugin para la respectiva generación de la alerta, en el caso que este sea un paquete considerado como actividad maliciosa [8].

5.1.9 El preprocesador. Es uno de los elementos más importantes en el motor de análisis del IDS, este componente del sistema realiza importantes tareas como lo son detectar actividad anormal a través de un complejo código, para generar sus propias alertas. El preprocesador es una fracción de código compilado en el motor del IDS, cuyo objetivo es normalizar y o examinar el tráfico en busca de paquetes que tengan las características o patrón de un ataque o actividad maliciosa, comparando con las reglas previamente definidas. Esta operación involucra cierta complejidad, debido al uso de algoritmos que a menudo incluyen inteligencia artificial y árboles de decisiones.

La capa de preprocesamiento se compone de las siguientes actividades:
- Protocolo de comunicaciones
- Desfragmentación IP
-Se verifica que los paquetes sean parte o no de una sesión establecida
-Reensamblaje de las tramas TCP en pseudo-paquetes.
- Normalización de protocolos y de ser necesario se genera un evento de implementación incorrecta o un uso indebido del protocolo.
- Finalmente luego que transcurren estas etapas el paquete es pasado a la máquina de detección a través de reglas.

5.1.10 Las reglas. En Snort a las reglas también se les denomina firmas o *signatures* en inglés. En este contexto el término se puede usar como una forma o manera de referirse a una condición o estado de la red. Por ejemplo podríamos escribir la siguiente regla, en la que se intenta detectar un ataque al servidor web *Internet information Server*

alert tcp $RED_EXTERNA any -> $APACHE_WEB_SERVERS $HTTP_PORTS (msg:"/cmd.exe
going to the IIS Webserver"; flow:established,to_server; content:"/cmd.exe"; depth:30;)

Básicamente la regla establece que si la cadena de texto "/cmd.exe" es enviado desde la red externa, con destino a lo que se haya definido en la variable

[8]CASWELL, Brian; BEALE, Jay; BAKER, Andrew. Snort intrusion detection and prevention toolkit. Burlington: Syngress, 2007. p.219

$*APACHE_WEB_SERVERS ,* en una transmisión TCP, se debería generar una Alerta.

El entendimiento de una regla es fundamental para el buen funcionamiento de un IDS; una regla mal definida podría generar demasiados falsos positivos, de allí la importancia del afinamiento o refinamiento de estas para incrementar la efectividad del dispositivo IDS.

Es posible escribir las reglas al momento de la implementación del IDS, pero esto significaría un enorme gasto de tiempo, considerando que estas también pueden ser descargadas desde los principales repositorios, uno de ellos es el repositorio *Snort.org GPL rules set,* En este repositorio, el equipo de SNORT, que es un equipo compuesto por voluntarios, ha puesto a disposición de la comunidad un conjunto de reglas para ser descargado y utilizado. También existen otros repositorios destacados entre otros: VRT*, Bleeding Edge Threaths y Community Rules Set*.[9]

5.1.11 Descripción de una regla. Las reglas en SNORT se escriben con un lenguaje flexible y potente, pero es necesario comprender la sintaxis para la escritura de las reglas. Las reglas en SNORT están compuestas por dos partes principales: La cabecera y las Opciones

5.1.11.1 Header o cabecera de la regla. La cabecera de la regla está compuesta por La acción de la regla que puede ser disparar una alerta, El protocolo , La dirección IP de origen, puerto de origen, dirección IP destino, Puerto de destino y la dirección de la operación.

5.1.11.2 Las opciones de la regla. En las opciones de la regla se encuentra primeramente el Mensaje: msg y luego van una serie de opciones tales como *flags, ack, reference*, entre otras opciones.

[9] CASWELL, Brian; BEALE, Jay; BAKER, Andrew. Snort intrusion detection and prevention toolkit. Burlington: Syngress, 2007. p.297

5.1.12 Sistema de prevención de intrusos IPS. Consiste en un dispositivo que controla el acceso en una red informática protegiendo a los sistemas computacionales de ataques. La tecnología de Prevención de Intrusos se considera una extensión de los Sistemas de Detección de Intrusos (IDS), sin embargo otros autores consideran que es otro tipo de control de acceso, más cercano a las tecnologías de firewall. Los IPS representan una evolución relevante sobre las tecnologías de firewall tradicionales, al tomar decisiones de control de acceso basados en los contenidos de los paquetes, en vez de direcciones IP o puertos. Esto debido a su cercanía con los IDS.

Una de la manera más usada en la implementación de IPS es combinar el IDS con el firewall o trabajar conjuntamente con una pasarela o gateway. De esta forma se combina la inteligencia del IDS y la capacidad de bloqueo del firewall.

5.2 MARCO CONTEXTUAL

La historia de la UNAD se remonta al año 1981 con la presidencia de Belisario Betancur. Nació como un proyecto educativo con el nombre de UNISUR.

La UNAD surgió, mediante la Ley 52 de 1981, como un establecimiento público del orden nacional adscrito al Ministerio de Educación Nacional y transformada por el Congreso de la República mediante la Ley 396 del 5 de agosto de 1997 en la Universidad Nacional Abierta y a Distancia UNAD.[10]

Fue creada con el objeto de diseñar e implementar programas académicos de educación a distancia para pertinentes con las necesidades locales, regionales, nacionales e internacionales.[11]

Se puso en marcha en el año 1982, y desde entonces se ha caracterizado por su compromiso con la población sin oportunidades para la formación en educación superior, contribuyendo de esta manera a la recuperación del tejido social[12]

[10] UNAD “Transparencia y acceso a la información pública”. {En línea}. {10 abril de 2018} disponible en:(https://informacion.unad.edu.co).
[11] Ibid.
[12] Ibid.

5.3 MARCO ESPACIAL

MISION

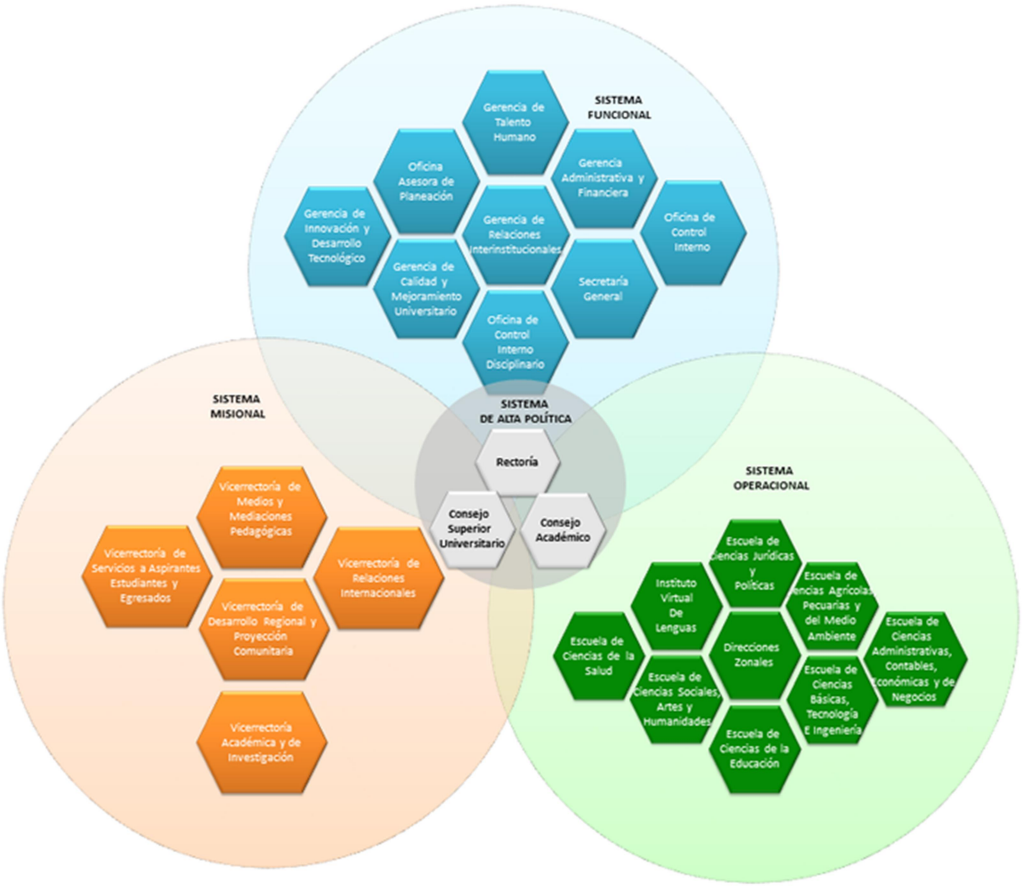
"La Universidad Nacional Abierta y a Distancia (UNAD) tiene como misión contribuir a la educación para todos a través de la modalidad abierta, a distancia y en ambientes virtuales de aprendizaje, mediante la acción pedagógica, la proyección social, el desarrollo regional y la proyección comunitaria, la inclusión, la investigación, la internacionalización y las innovaciones metodológicas y didácticas, con la utilización de las tecnologías de la información y las comunicaciones para fomentar y acompañar el aprendizaje autónomo, generador de cultura y espíritu emprendedor que, en el marco de la sociedad global y del conocimiento, propicie el desarrollo económico, social y humano sostenible de las comunidades locales, regionales y globales con calidad, eficiencia y equidad social".[13]

VISIÓN

"Se proyecta como una organización líder en Educación Abierta y a Distancia, reconocida a nivel nacional e internacional por la calidad innovadora y pertinencia de sus ofertas y servicios educativos y por su compromiso y aporte de su comunidad académica al desarrollo humano sostenible, de las comunidades locales y globales".[14]

[13] UNAD "Transparencia y acceso a la información pública". {En línea}. {10 abril de 2018} disponible en:(https://informacion.unad.edu.co).
[14] Ibid.

Figura 3. Estructura organizacional de la UNAD.



Fuente:https://informacion.unad.edu.co/images/acerca%20de%20la%20unad/gobierno%20corporativo/organigrama2.png.

5.4 MARCO LEGAL

Existe una gran cantidad de normas que regulan la utilización de los recursos informáticos, estas tienen como principal objetivo normalizar el uso de la TIC.

El gobierno colombiano preocupado por el aumento de la delincuencia informática, y debido a que en este campo no había mucha legislación se implementó las leyes que regularon el tema.

LEY 603 DE 2000, la cual se refiere a la protección de los derechos de autor en Colombia.

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008, Por la cual se dictan las disposiciones generales del Hábeas Data para regular el uso de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros .

LEY 1273 DEL 5 DE ENERO DE 2009

El 5 de Enero de 2009 se decretó la Ley 1273 de 2009, la cual añade dos nuevos capítulos al Código Penal Colombiano:[15]

Esta ley regula todo lo que tiene que ver con el acceso indebido a datos o equipos de cómputo sin la debida autorización, Adicionándose el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos".

Esta ley en su artículo I regula todo lo que tiene que ver con atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Por mencionar alguno de los artículos de esta ley, en su artículo 269ª, se penaliza el acceso abusivo a un sistema informático, el artículo dice textualmente:

> Artículo 269A: *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
>
> Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.[16]

[15] LEY 1273 DE 2009. {En línea}. {12 abril de 2018} disponible en:(http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf).
[16] LEY 1273 DE 2009. {En línea}. {13 abril de 2018} disponible en:(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492).

LEY 1341 DEL 30 DE JULIO DE 2009, Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del .

LEY ESTATUTARIA 1581 DE 2012

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, por la cual se obliga a las empresas a crear sus propias políticas internas de manejo de datos personales, y se establecen procedimientos para la atención de peticiones, quejas y reclamos.

DECRETO 1377 DE 2013 Protección de Datos, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

5.5 MARCO CONCEPTUAL

5.5.1 Seguridad de la información. La seguridad de la información abarca una gama de medidas preventivas, correctivas y reactivas que garantizan preservar niveles aceptables de calidad en términos de integridad, Disponibilidad y confidencialidad.
En la medida en que ha aumentado el uso masivo de las tecnologías de la información, ha aumentado el riesgo de vulneración de la información personal y de las organizaciones. La seguridad de la información es un campo muy amplio, que ha tomado auge a medida que aumentan los casos de vulneración, La seguridad de la información también abarca la Seguridad informática cuyo fin es mantener la e integridad, Disponibilidad y confidencialidad, pero desde el ámbito tecnológico. La seguridad de la información es un proceso continuo para mantener y adaptarse con el objetivo de minimizar vulnerabilidades y evitar que se conviertan en riegos[17].

5.5.2 Integridad. Esta propiedad propende porque la información sea exacta y esté completa, se busca garantizar que la información no sea alterada sin autorización, que sea la misma desde su emisión hasta su lectura.[18]

[17] MIFSUD, Elvira “Seguridad Informática, Introducción a la seguridad informática - Seguridad de la información / Seguridad informática”, {En línea}. {10 abril de 2018} disponible en:(http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1) p.2.
[18] LÓPEZ AGUILERA, Purificación. Seguridad informática. Editex, 2010. P.10

5.5.3 Disponibilidad. La información posee esta característica cuando puede ser accedida por los usuarios autorizados en cualquier momento. El avance en las tecnologías de la información y la comunicación ha permitido niveles de disponibilidad muy altos, Sin embargo un ataque de negación de servicio DOS, o la caída del servidor por una falla en el fluido eléctrico porque no se tiene un sistema alterno de alimentación pueden poner en riesgo que la información esté disponible para su uso o consulta.[19]

5.5.4 Confidencialidad. Se define la confidencialidad de la información como el hecho de que los datos puedan ser conocidos únicamente por las personas o entidades autorizadas como tal, en la forma y tiempo autorizado.[20]
La confidencialidad de la información se podría ver comprometida por una intrusión no autorizada en el sistema mediante mecanismos o técnicas que permitan acceder al sistema a usuarios no autorizados, las siguientes situaciones podrían aumentar la probabilidad de comprometer la confidencialidad en la organización :

- El uso de certificados de seguridad caducados.
- Suplantación de identidad.
- Mediante inyección o envenenamiento de la tabla ARP se puede colocar a un “hombre en el medio” y vulnerar este servicio.
- El uso de contraseñas débiles constituye una amenaza para este servicio.

[19] LÓPEZ AGUILERA, Purificación. Seguridad informática. Editex, 2010. P.10

[20] Ibíd., p.11.

6. DISEÑO METODOLÓGICO

Para la elaboración de este proyecto se han tomado en consideración unas etapas de desarrollo que conduzcan al logro del objetivo propuesto. Estas fases de desarrollo están encaminadas hacia la concepción del diseño de un sistema de detección de intrusos, teniendo como finalidad el monitoreo de la red para la detección temprana de actividad maliciosa dentro de la red, básicamente se planea la elaboración de un diseño pormenorizado en la modalidad de proyecto aplicado, de un sistema de detección de intrusiones.

6.1 METODOLOGIA DE DESARROLLO

La metodología que se plantea seguir para el desarrollo del proyecto, pasa por la planeación de los objetivos específicos para alcanzar el objetivo general del proyecto. Partiendo de la identificación de la topología de la red del CCAV Puerto Colombia y el levantamiento del inventario de activos informáticos, a partir de allí se planificará el diseño del sistema de detección de intrusos para la red. Incluyendo un plan de pruebas de *pentesting* que garantice la funcionalidad del prototipo del sistema de detección de intrusos, en una red aislada y controlada, externa a la red de la UNAD.

Las fases de desarrollo que se han planeado se ejecutarán de la siguiente manera:

La elaboración del cronograma de actividades con la asignación de los tiempos para el desarrollo de cada actividad.

Revisión documental de los temas que se han de desarrollar a lo largo del proyecto. Esta etapa comprenderá la selección de la bibliografía que se debe abordar para obtener las habilidades y conocimientos necesarios en los temas tales como sistema operativo Linux, redes, seguridad, IDS entre otros.

A continuación se listan las actividades que se deben ejecutar:

- ✓ Realizar inventario de activos informáticos del CCAV.
- ✓ Levantamiento de información sobre la topología de la red.
- ✓ Revisión documental de cuáles son los tipos de IDS
- ✓ Selección el tipo de IDS que se ajusta la necesidad del CCAV
- ✓ Preparación de la máquina para la instalación del IDS.

- ✓ Instalación del prototipo del sistema IDS.
- ✓ Preparación y configuración del set de pruebas.
- ✓ Puesta en marcha del prototipo de IDS una red aislada y controlada, externa a la red de la UNAD.
- ✓ Elaboración de los documentos o memorias del proyecto.

Se aclara que las pruebas no se realizaran sobre la red de la UNAD, estas se realizaran en una red externa, en un ambiente controlado, para demostrar la eficacia del IDS.

6.2 FUENTES Y TÉCNICAS DE RECOLECCION DE INFORMACION

6.2.1 FUENTES PRIMARIAS

Documentos originales
Diarios
Minutas
Entrevistas

6.2.2 FUENTES SECUNDARIAS

Revistas de resúmenes, y comentarios

Bibliografías

Fuentes de información citadas en el texto

6.3 DELIMITACIÓN Y ALCANCE

El alcance del proyecto está delimitado hacia la seguridad de la red de la UNAD en el CCAV de puerto Colombia

6.3.1 Técnicas de análisis de datos. En el presente proyecto se utilizaran técnicas de análisis de datos en mediante los algoritmos que implementa el IDS los cuales permitirán realizar un análisis sistemático de los paquetes que circulan por la red de tal manera que se pueda identificar y catalogar como actividad sospechosa o normal.

6.3.2 Técnicas de procesamiento de datos. Varias fuentes de información tales como libros, artículos, tesis tanto en medio físico como electrónico

6.4 ESQUEMA TEMATICO

- ✓ Levantamiento de información.
- ✓ Topología de la red del CCAV puerto Colombia.
- ✓ Dispositivos de red.
- ✓ Inventario de activos Aplicando magerit
- ✓ Direccionamiento IP
- ✓ Ataques informáticos usuales en Colombia
- ✓ Diseño del sistema de detección de intrusos para la red de la UNAD CCAV puerto Colombia
- ✓ Consideraciones generales del diseño.
- ✓ ¿Por qué Snort?
- ✓ Preparación de la máquina
- ✓ Instalación de Snort.
- ✓ Configuración de Snort como NIDS
- ✓ Instalación de vanyard2
- ✓ Instalación y configuración de pulledpork.
- ✓ Instalación de la interfaz gráfica para Snort
- ✓ BASE
- ✓ diseño del plan de pruebas de pentesting para garantizar la funcionalidad del IDS.
- ✓ instalación de kali Linux
- ✓ Pruebas de aplicación con agujeros.
- ✓ Ataque DOS
- ✓ Otros ataques
- ✓ Resultados
- ✓ Orígenes de las incidencias
- ✓ Tipos de hallazgos
- ✓ Falsos positivos

7. PERSONAS QUE PARTICIPAN EN EL PROYECTO.

7.1 PROPONENTE PRIMARIO

MARIO LUIS AVILA PEREZ nació en Corozal Sucre el 11 de mayo 1971. Se graduó de Bachiller académico en el año 1988. Se graduó en la Universidad Nacional Abierta y a Distancia, UNAD, en Ingeniería de Sistemas. Es especialista en Pedagogía para el desarrollo del Aprendizaje autónomo y se encuentra en la misma universidad cursando la especialización en Seguridad Informática. Experiencia en desarrollo de aplicaciones en varios lenguajes de programación como Java, Visual Basic, COBOL. Desarrollo de aplicaciones web en PHP y JSP. Actualmente se desempeña como Tutor de la escuela ECBTI CEAD Barranquilla

7.2 PROPONENTE SECUNDARIO

En el desarrollo de este proyecto participa el Ingeniero Francisco Javier Hilarión Novoa, Especialista en Seguridad Informática, Ingeniero Electrónico y Tecnólogo en Electrónica, certificado en competencias como E-mediador en Ambientes Virtuales de Aprendizaje y Desarrollo de aplicaciones móviles, Docente de la Universidad Nacional Abierta y a Distancia, de la Escuela de Ciencias Básicas, Tecnología e Ingeniería, Perteneciente al CEAD de Gachetá Cundinamarca, como director del proyecto.

8. RECURSOS DISPONIBLES

8.1 MATERIALES

Este proyecto se desarrolla financiado principalmente por el investigador, con recursos propios, sin embargo la UNAD contribuye facilitando algunos equipos que a continuación se mencionan los principales.

1. computador para la instalación del SNORT para implementar los sensores, core i7, con 8 GB de RAM.
2. Computador portátil para la elaboración de informes, realizar la monitorización del IDS y realizar los informes.
3. Conexión a internet ilimitada de 5 megas para la realización investigación, consulta de documentos especializados en el tema de IDS y revisión bibliográfica
4. El recurso Humano constituido por un ingeniero de sistemas Especialista en Seguridad Informática a cargo de la realización del proyecto.

8.2 INSTITUCIONALES

Computador para realizar la instalación de la maqueta del sistema para simulación de la red del CCAV, donde se instalarán las máquinas virtuales, incluida la instalación del SNORT para implementar los sensores, con las siguientes características: core i7, con 8 GB de RAM.

8.3 PRESUPUESTO

A continuación se presenta la Tabla 2. Donde se detalla un estimado de los recursos necesarios para el desarrollo del proyecto.

Tabla 1. Recursos.

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Ingeniero de Sistemas especialista en seguridad informática, Asesor de proyecto	4.200.000
Equipos y Software	1. computador para la instalación del SNORT para implementar los sensores, core i7, con 8 GB de RAM. 2. Computador portátil para la elaboración de informes, realizar la monitorización del IDS y realizar los informes.	2.000.000
Viajes y Salidas de Campo		0
Materiales y suministros	Impresora Láser, Resma para impresión	1.000.000
Bibliografía	Documentación consultada en internet	0
		TOTAL $7.000.000

Fuete: El autor

8.4 RESULTADO E IMPACTO ESPERADO

Al finalizar el presente proyecto aplicado se espera tener una propuesta de diseño para un IDS basado en red, que se ajuste a las necesidades de la organización, y que contribuya a la disminución del riesgo de materialización de amenazas en la plataforma de la red del CCAV Puerto Colombia.

Con este proyecto se pretende afianzar los conocimientos que se tienen sobre IDS, las clases y tipos de IDS, las metodologías de diseño. Se busca la mejora en la utilización de herramientas y paquetes de software que se distribuyen bajo el modelo de licenciamiento de software libre, especialmente las GPL, como un marco de herramientas robustas y ampliamente recomendadas por la comunidad de desarrolladores, organizadas y alineadas con el objetivo de configurar dispositivos avanzados de protección de redes.

9. LEVANTAMIENTO DE INFORMACIÓN.

9.1 TOPOLOGÍA DE LA RED DEL CCAV PUERTO COLOMBIA

A continuación se describen las principales características de la red del CCAV puerto Colombia, Información recolectada mediante trabajo de campo en el campus de la Universidad Nacional Abierta y A Distancia. La recolección de la información de la red se realizó de la mano de la persona encargada del área de TI.

9.1.1 Dispositivos de red. La red de datos del CCAV de Puerto Colombia está soportada por una topología tipo estrella, en la cual hay 5 *swiches* en cascadas distribuidos en los 2 edificios como se aprecia en la figura 4. En el campus existen 5 racks de comunicaciones los cuales están distribuidos así:
2 Racks en el edificio Administrativo y 3 racks en el edificio académico.

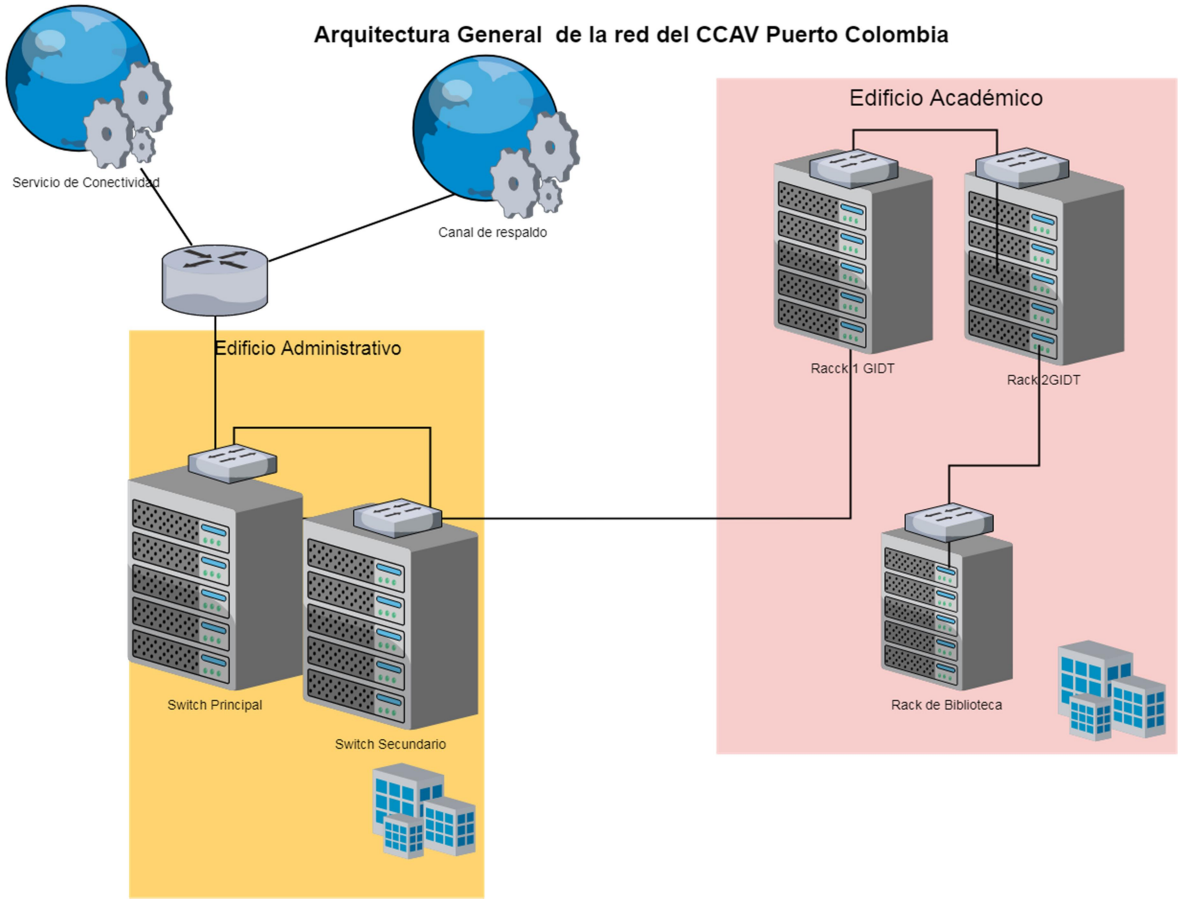
En estos 5 racks se encuentran distribuidos 5 swiches, como se observa en la figura 4.

Tabla 2. Dispositivos de Red del CCAV Puerto Colombia

Dispositivo	Marca
Módems de fibra óptica	Sin información
Módems de fibra óptica	Sin información
Enrutador	Sin información
Enrutador	Sin información
Switch 24 Puertos	Hp Aruba 2530
Switch 24 Puertos	Hp Aruba 2530
Switch 48 Puertos	Hp Aruba 2930
Switch 48 Puertos	Hp Aruba 2930
Switch 48 Puertos	Hp Aruba 2930

Fuente: El autor.

Figura 4. Esquema general de la red



Fuente: El autor.

La conectividad es suministrada por el proveedor de internet Movistar, el cual suministra un canal de 10Mb y un canal de respaldo de 1Mb. Estos canales son soportados por medio de fibra óptica.

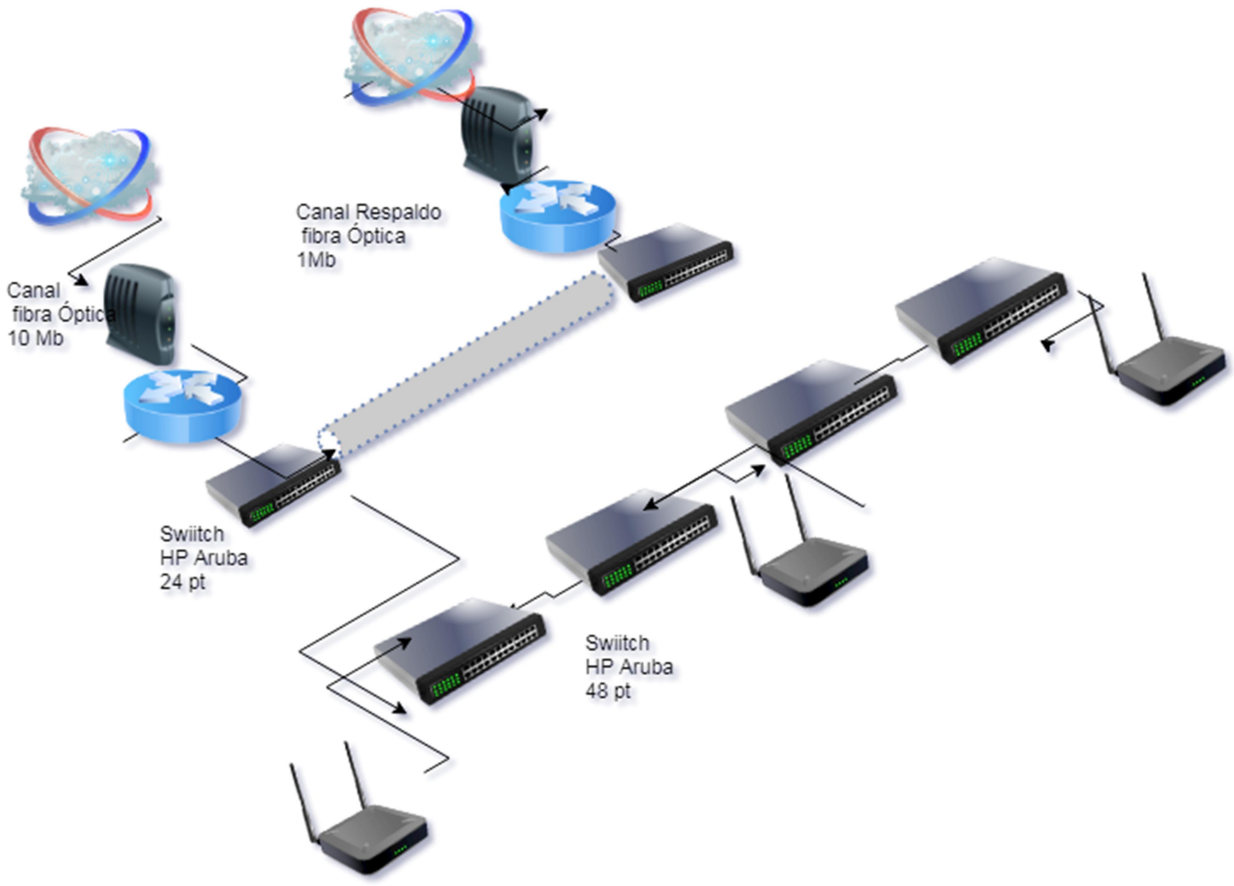
9.1.2 Inventario de activos aplicando Magerit. En el anexo A se relaciona el inventario de equipos que se encuentran activos para la comunidad académica y administrativa del CCAV Puerto Colombia. Este inventario se realizó gracias a la colaboración del personal GIDT encargado del soporte tecnológico en el CCAV.

9.1.3 Direccionamiento IP.
A continuación se presenta el esquema de direccionamiento de la red del CCAV Puerto Colombia, incluyendo los equipos que se encuentran interconectados.

Como se puede apreciar en las figuras 5, 6 y 7 , Existen dos VLAN las cuales consisten en redes de área local virtual; La disposición de estas dos VLAN posibilitan la optimización de las prestaciones de la red evitando de esta manera inundaciones de broadcast.

En la figura 5 se puede apreciar el esquema de configuración, se aprecia el canal principal de fibra óptica, el cual al momento de la recolección de la información tienen una capacidad de 10 Mbps, pero se planea ampliar a 20 Mbps en los próximos meses. En la figura 5 se aprecia El canal de respaldo de 1Mps y la distribución de los switches.

Figura 5. Esquema de red de canales de datos



Fuente: El autor

Estas dos redes VLAN se han denominado Red Administrativa también conocido por el personal de soporte como la red 134, identificada de esta manera porque 134 es el tercer octeto de las direcciones IP de los equipos que se conectan a dicha red.

En la tabla 3 se puede apreciar el esquema de direccionamiento IP, para la red cableada.

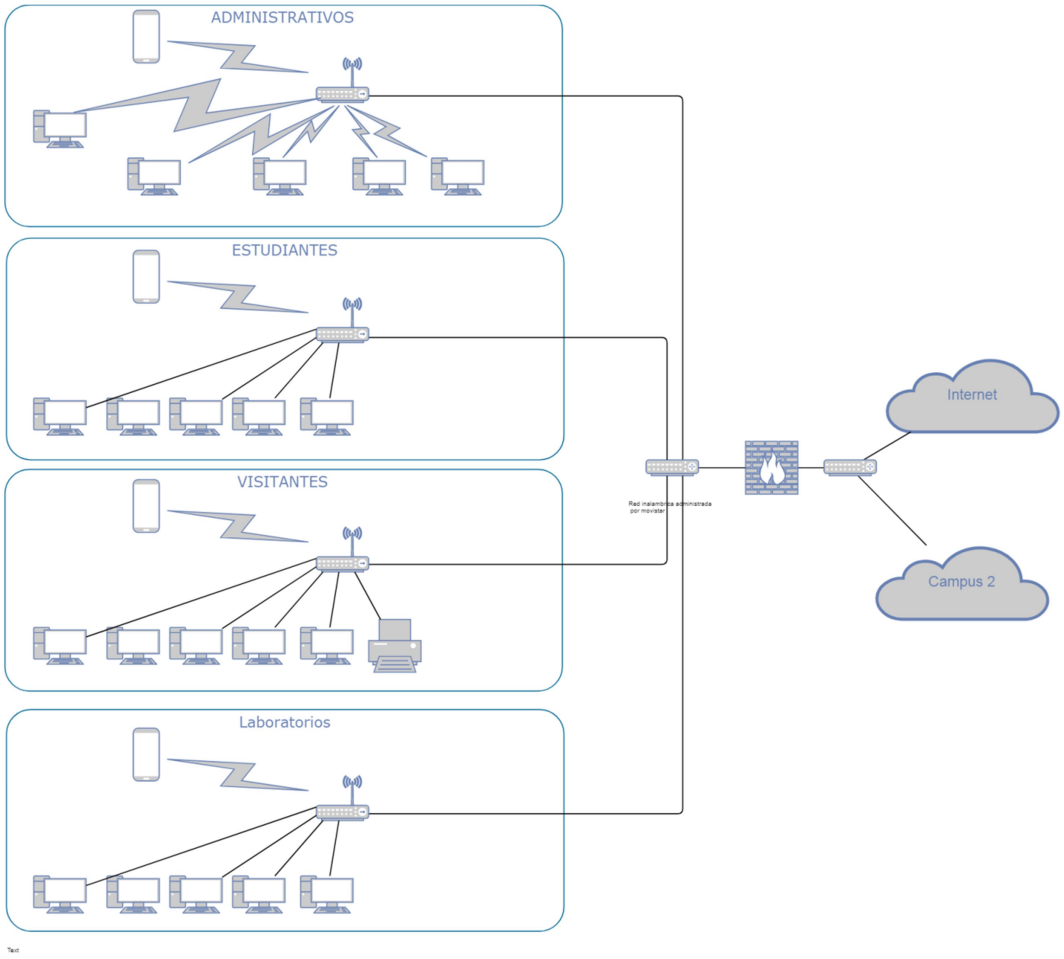
Tabla 3. Direccionamiento IP.

Nombre VLAN	Dirección IP	Mascara de sub red	Gateway
Administrativos	192.168.134.0	255.255.255.128	192.168.134.1
Estudiantes	192.168.133.0	255.255.255.128	192.168.133.1

Fuente: El autor

Existen otras 3 redes VLAN para los dispositivos inalámbricos. Esta redes esta soportada por 5 dispositivos AP CISCO, con protocolo seguro de autenticación. Cabe anotar que estas redes inalámbricas son administradas por el proveedor movistar, el cual se encarga de la gestión de configuración, lo cual está contemplado dentro de la contratación de servicios de internet.

Figura 6. Esquema de redes inalámbricas del CCAV



Fuente: El autor

En el Centro se cuenta con un equipo de altas prestaciones el cual aloja los servicios de DHCP (Dynamic host control protocol) y se planea usar para configuración de directorio activo con Windows Server.

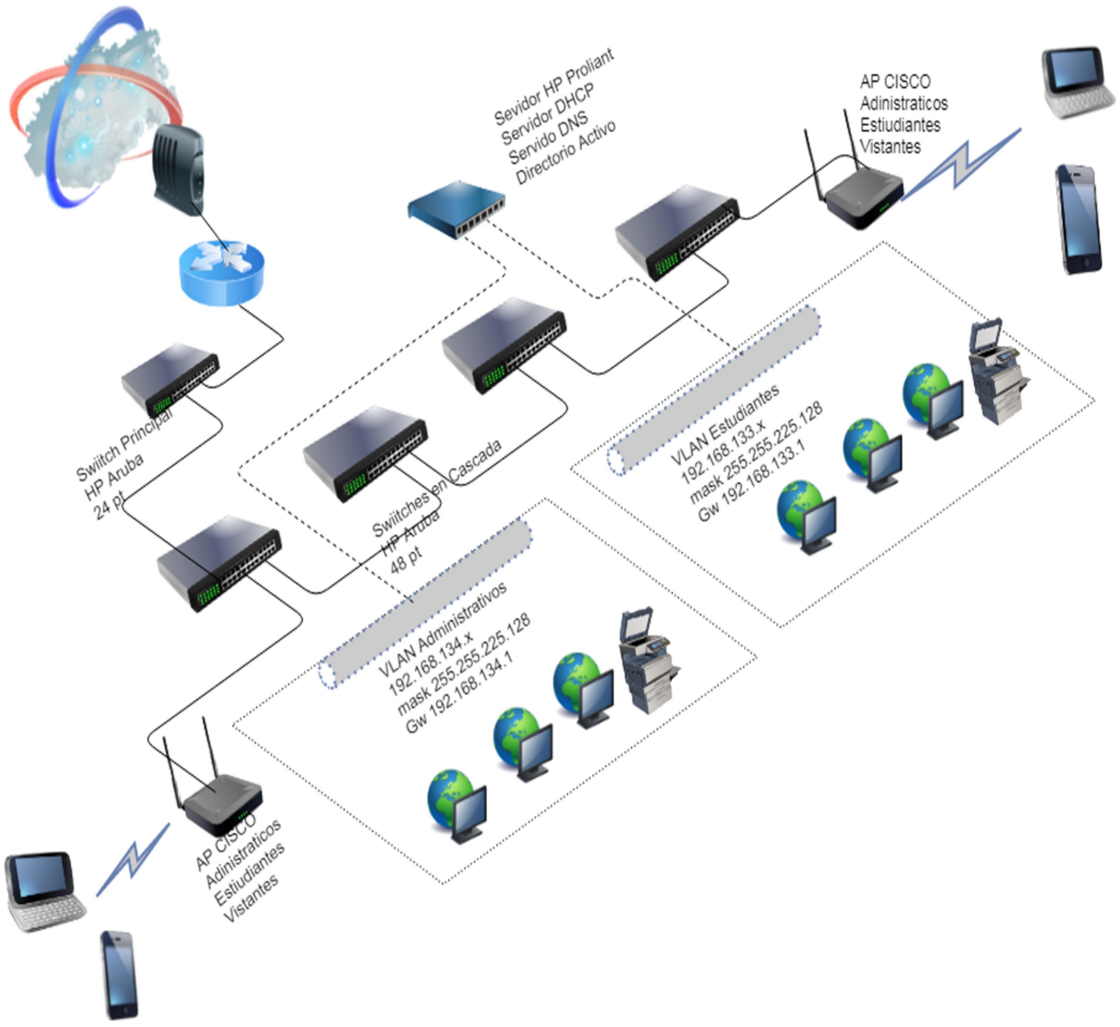
Tabla 4. Servidor en la red.

Dispositivo	Marca
Servidor tipo Rack	Hp Proliant

Fuente: El autor

En la figura 7 se pude observar una descripción más detallada de la red, destacándose las dos redes VLAN y su disposición lógica dentro del esquema de direccionamiento IP.

Figura 7. Esquema detallado de la red del CCAV.



Fuente: El autor

9.2 INCREMENTO DE DELITOS INFORMATICOS EN COLOMBIA

Al consultarse las estadísticas acerca de noticias de delitos informáticos en Colombia, en el sistema de información de la fiscalía, se nota un incremento significativo en los últimos años. Con estos alarmantes aumentos, nos encontramos ante un panorama bastante crítico en materia de seguridad informática.

Por ejemplo para el delito "Acceso abusivo a un sistema informático art 269A ley 1273 de 2009" se observa que para el periodo comprendido entre 2016-12 y 2018-05, se presenta un incremento de aproximadamente 54.3%, como se puede apreciar en la figura 8.[21]

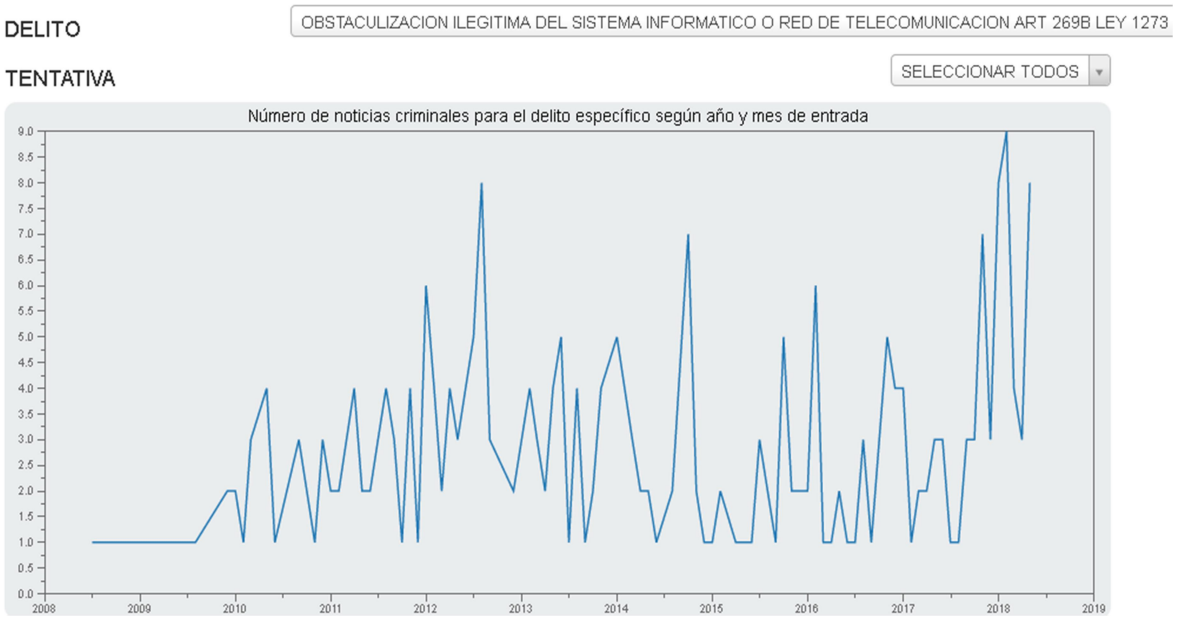
Figura 8. Noticias criminales para el delito "Acceso abusivo a un sistema informático art 269A ley 1273 de 2009".

Fuente: Fiscalía General https://www.fiscalia.gov.co/colombia/delitos/

[21] FISCALÍA "Estadística de delitos". {En línea}. {7 de julio de 2018} disponible en:(https://www.fiscalia.gov.co/colombia/delitos/)

Para el delito “Obstaculización ilegitima del sistema informático o red de telecomunicación”, se observa que para lo que va corrido del 2018, con respecto al primer semestre del 2017, se presenta un incremento del 44.4%, en este tipo de delitos, como se puede apreciar en la figura 9.[22]

Figura 9. Noticias criminales para el delito “Obstaculización ilegitima del sistema informático o red de telecomunicación”



Fuente: Fiscalía General https://www.fiscalia.gov.co/colombia/delitos/

Muy a menudo encontramos en las noticias el aumento en incidencias de ataques informáticos. Según un informe de la compañía de seguridad informática rusa Kaspersky, américa latina ha sufrido un incremento del 30% anual entre 2014 y 2016 en los ataques de *ransomware*, y se espera que esta tendencia se mantenga o aumente para el 2017 y 2018.[23]

[22] FISCALÍA “Estadística de delitos”. {En línea}. {7 de julio de 2018}. disponible en:(https://www.fiscalia.gov.co/colombia/delitos/).

[23] KASPERSKY, Lab. “Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina”. {en línea}.{13 de marzo de 2018} Disponible en(https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america).

10. DISEÑO DEL SISTEMA DE DETECCIÓN DE INTRUSOS

10.1 CONSIDERACIONES GENERALES DEL DISEÑO

A continuación se mencionan los elementos a considerar para un diseño adecuado del NIDS.

Uno de los elementos más importantes es la arquitectura de la red con la que cuenta el CCAV, las redes VLAN existentes hace necesario que el dispositivo NIDS cuente con dos interfaces de red para monitorear el tráfico de VLAN ADMINISTRATIVOS y la VLAN ESTUDIANTES. También hay que tener en cuenta que si se desea administrar remotamente el dispositivo IDS, se haría necesaria una tercera tarjeta de red.

Sin embargo se puede optar por colocar el IDS en el switche principal, usando la funcionalidad de puerto espejo, con la que cuentan los switches modernos y de esta manera monitorizar todo el tráfico de la red con una sola interfaz de red.

Además de las consideraciones mencionadas, es necesario tener en cuenta los siguientes aspectos:

- Los activos tecnológicos a proteger
- El tipo de software o plataformas de los equipos a proteger
- Hay que tener en cuenta las modalidades de ataques que suelen presentarse en la zona de Latinoamérica, con el fin de reforzar las reglas de seguridad apuntando a un tipo específico de ataques, sin descuidar los otros tipos.

10.2 SNORT COMO MOTOR IDS.

Básicamente un dispositivo NIDS, es un *sniffer* o sensor que examina todo el tráfico que pasa a través de la red. Existen varias soluciones pagas tales como *fortinet*, las soluciones de CISCO tales como *Cisco Intrusion Detection System 4200 Security Appliance*[24]. Pero estas soluciones tienen un costo considerable.

[24] CISCO “Cisco Network-Based Intrusion. Capítulo 8”, {En línea}.{abril 20 de 2018} Disponible en(https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/8_NIDS.pdf).

Las versiones comerciales de NIDS poseen muchas facilidades y herramientas que facilitan el trabajo de administración y configuración. Como ejemplo de estas utilidades se pueden mencionar un software de administración web remota del sistema, delegación de la administración entre otras.

En el universo del software libre encontramos a Snort, el cual es un proyecto que funciona bajo licencia Open GL, cuenta un desarrollo progresivo continuo. Este proyecto ha ido evolucionando hasta convertirse en una opción robusta confiable y estable.

En este orden de ideas, la clave para decidir qué infraestructura de IDS implementar, radica en la capacidad de integrarse con el menor traumatismo posible a la arquitectura ya existente en la organización, que sea escalable y que permita reducir el riesgo de materialización de amenazas en la organización, que tenga facilidades de administración remota. En este sentido Las herramienta Libres se puede afirmar que algunas como Snort están a la altura de las versiones comerciales ofreciendo versatilidad a la hora de la implementación, a un menor costo. Esto en el caso de las organizaciones del sector público como lo es la UNAD, en las cuales los presupuestos deberían ser optimizados y el costo es una variable muy importante a tener en cuenta. Herramientas como SNORT tienen mucho soporte, pero es menor al soporte que ofrece por ejemplo CISCO o FortiNet.

En conclusión basados en los argumentos expuestos y dependiendo de factores como la infraestructura ya existente en la organización y la arquitectura de red, para esta entidad pública se recomienda herramientas de software libre, en este caso Snort.

10.3 PREPARACIÓN DE LA MÁQUINA

La computadora seleccionada para la instalación del NIDS es una computadora HP, Core i7 con 8GB de RAM, la cual es una configuración que satisface los requerimientos del sistema Linux, para NIDS.

Durante la ejecución del proyecto se configuró esta máquina con software de virtualización para simular la red objeto de estudio y de esta manera poder operar en un ambiente controlado aislado de la red de la UNAD para poder operar el sistema con seguridad y realizar las pruebas pertinentes.

Para la virtualización del sistema se utilizó el software *VirtualBox*, el cual es un software de Oracle que permite la instalación de diferentes máquinas virtuales con diferentes sistemas operativos.

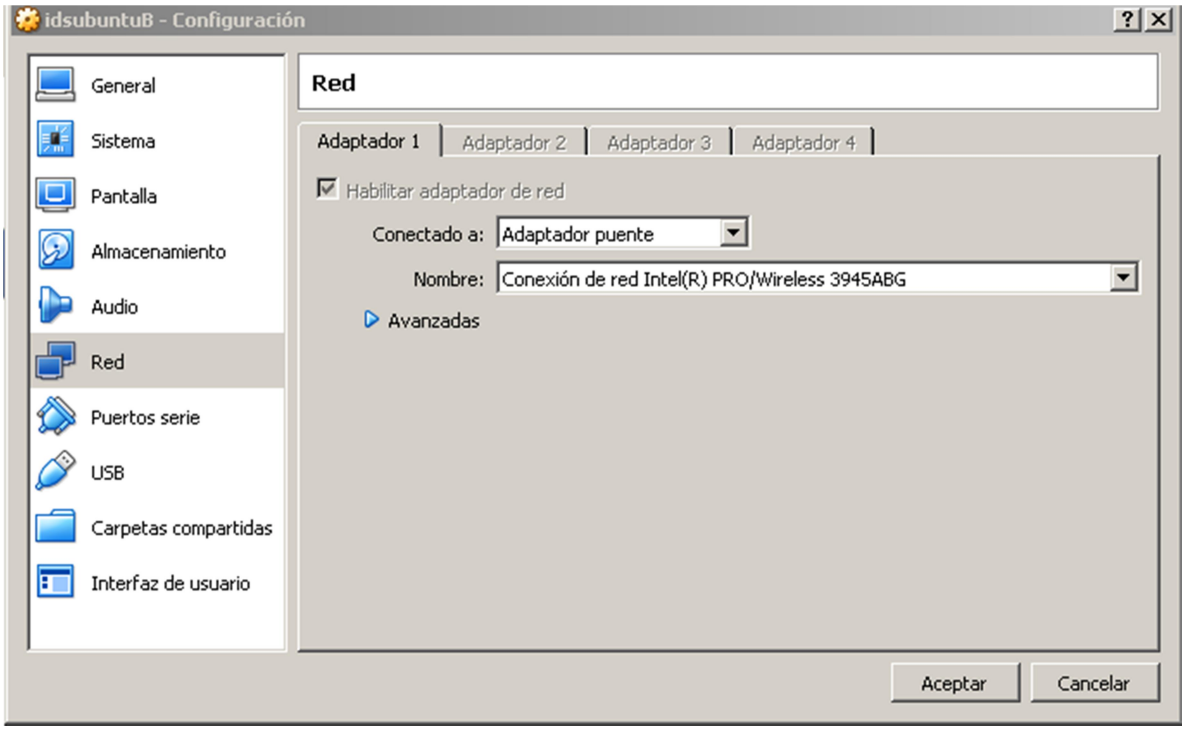
Una vez instalado el software *VirtualBox*, se descargó e instaló la versión 16 de 32 bits de *Ubuntu Server*, instalada en una máquina virtual, configurada con 2 GB de RAM y un disco de 20 GB, para la realización de las pruebas. En la escogencia de paquetes para la instalación de *Ubuntu server* se selecciona el Open ssh Server, para poder administrar la máquina de manera remota.

Se procede a actualizar Linux Ubuntu:

```
mario@IDSubuntu:$ sudo apt-get update
sudo apt-get dist-upgrade -y
sudo apt-get install -y openssh-server
sudo reboot
```

Todas las tarjetas de red de las máquinas virtuales que se utilizaran en este ambiente simulado y controlado para las pruebas del IDS deben estar configuradas en modo puente, este es un requerimiento obligatorio para que se puedan configurar direcciones IP estáticas, para lograrlo se ingresa desde *VirtualBox* por la opción de configuración de la máquina virtual, luego red, y en la opción *conectado a* se selecciona *adaptador puente*.

Figura 10. Configuración de red en VirtualBox.



Fuente: El autor

Una vez se ha instalado Ubuntu server, se procede con la configuración de la tarjeta de red de la máquina Linux en donde se alojará el IDS.

Para lo cual se edita el archivo */etc/network/interfaces,* para agregar la configuración de modo estático y agregar los parámetros de dirección IP, como son: mascara, puerta de enlace, broadcast y DNS, como se aprecia a continuación, para la interface *enp0s3,* que sería la que en versiones anteriores de *Ubuntu* o *Debían* llamaríamos *eth0*.

```
mario@IDSubuntu:~$ cat /etc/network/interfaces
source /etc/network/interfaces.d/*
# The primary network interface
auto enp0s3
iface enp0s3 inet static
        address 192.168.1.251
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        gateway  192.168.1.1
        dns-nameserver 8.8.8.8
```

Otro aspecto que se debe tener en cuenta a la hora de configurar las tarjetas o interfaces de red, es que algunos autores recomiendan que las opción GRO y LRO deben ser desactivadas en la configuración de las tarjetas para evitar inconvenientes con el reensamblado de paquetes.

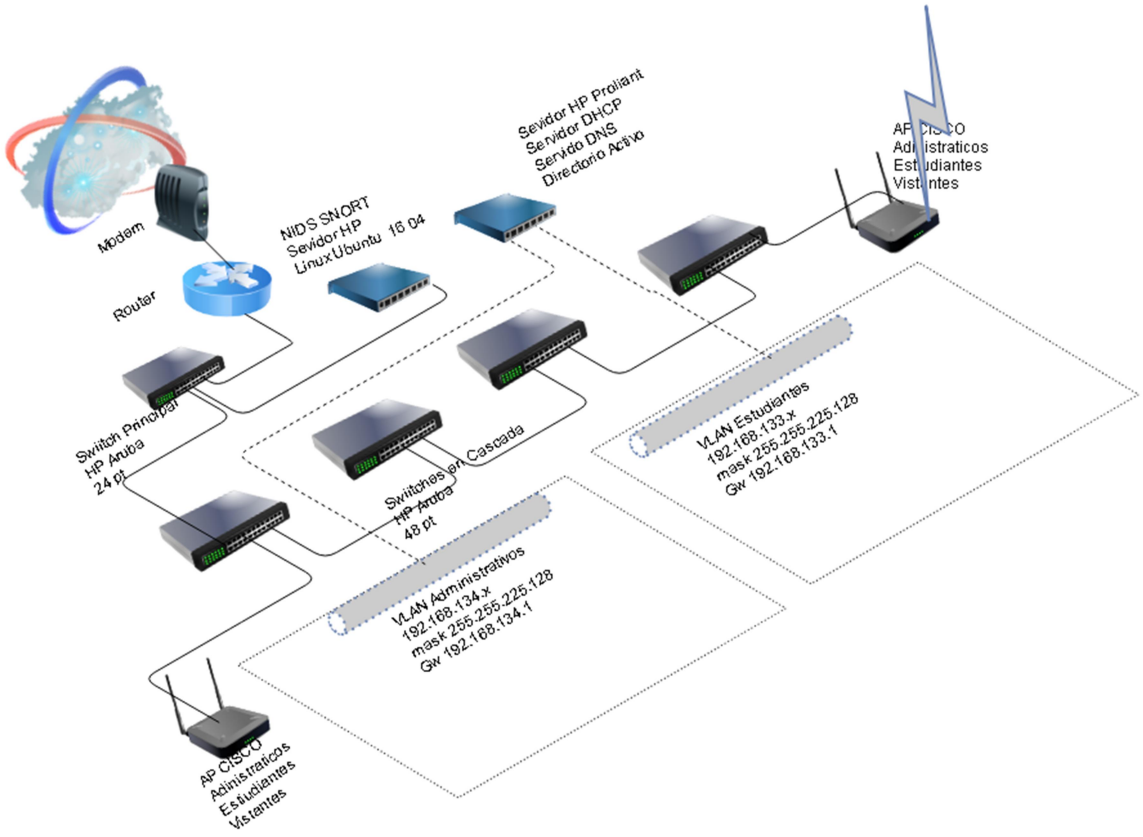
10.4 INSTALACION DE SNORT

Uno de los aspectos básicos a resolver es el lugar estratégico donde debe ubicarse el NIDS, para lo cual se deben tomar en consideración varios factores. Uno de estos factores es que el lugar debe ser estratégico para que pueda ser esnifado todo el tráfico que hace tránsito a través de la red.

En este orden de ideas en el diseño propuesto se plantea que NIDS quede conectado directamente al primer switch, que el HP Aruba de 24 puertos, y se plantea la opción de hacer transitar o direccionar todo tráfico hacia el NIDS, este objetivo se puede alcanzar ya sea colocando una de las tarjetas del NIDS en modo promiscuo o configurando un puerto espejo "mirror" en el switch hacia el que se copian todos los paquetes que transitan por la red. La disposición de los dispositivos se puede apreciar en la figura 11, donde se observa claramente la ubicación del NIDS.

Para la maqueta en la que se realizarán las pruebas la disposición de cada elemento de la red es más sencilla debido a que se utilizan máquinas virtuales para simular un ambiente similar y comprobar la efectividad del NIDS como se verá más adelante.

Figura 11. Ubicación del NIDS en la red.



Fuente: El autor

Snort es un sistema de detección de intrusos muy popular, es de libre distribución y por esta razón se ha seleccionado para la configuración de NIDS.

El software de Snort se distribuye bajo licencia GPL (General Public License) es un software robusto y entre sus características se destacan la escalabilidad, dispone de una gran cantidad de filtros y patrones definidos y actualizaciones constantes de la base de reglas o firmas.

No obstante existen distribuciones de Linux con Snort en las que ya viene mucho del trabajo de instalación realizado, incluso viene preconfigurada su interfaz gráfica. En este proyecto se configurará SNORT desde cero, con el fin de profundizar más en el funcionamiento y configuración de sus componentes y el engranaje de cada elemento.

Para el proceso de instalación de SNORT se procede de acuerdo a las indicaciones de la guía proporcionada en la documentación del proyecto Snort[25]

Se realiza la descarga de paquetes y se siguen las instrucciones proporcionadas en la documentación de SNORT, iniciando con los prerrequisitos que se deben tener instalados:

build-essential, libpcap-dev, libpcre3-dev, libdumbnet-dev, bison, flex

Estos paquetes se descargan e instalan desde los repositorios de Ubuntu utilizando la herramienta *apt-get.*

Se procede siguiendo los pasos de la guía que aparece en la documentación de snort.org (DIETRICH, Noah). Se crea un directorio en $HOME/snort_src.

También es necesario instalar la librería DAQ (Data AdQuisition), para lo cual se descarga el programa fuente, se descomprime, se compila y se instala, procediendo de la siguiente manera:

```
cd ~/snort_src
wget https://snort.org/downloads/snort/daq-2.0.6.tar.gz
tar -xvzf daq-2.0.6.tar.gz
cd daq-2.0.6
./configure
make
sudo make install
```

La librería DAQ crea una capa de abstracción para evitar las llamadas directas a la librería *pcap* facilitando el trabajo con *Snort*.

Existe otro prerrequisito que se debe instalar para Snort, la librería de compresión zlibg, junto con otras librerías que mejoran la funcionalidad en la descompresión

[25] DIETRICH, Noah “Snort 3 on Ubuntu 14 and 16”. {en línea}. {13 de marzo de 2018} disponible en: (https://www.snort.org/documents/snort-3-0-for-ubuntu-14-and-16).

de contenidos swf (adobe flash).[26] La cual se descarga e instala con apt-get desde los repositorios de Ubuntu:

```
sudo apt-get install -y zlib1g-dev liblzma-dev openssl libssl-dev
```

Se instala las librerías que implementan el algoritmo de compresión de cabeceras HPAC.

```
sudo apt-get install -y libnghttp2-dev
```

Ya se tienen instalados los prerrequisitos, entonces se procede con la instalación de Snort, para lo cual se descarga el paquete de los programas fuentes, se descomprimen, compilan e instalan, y para la compilación se habilita la opción *--enable-sourcefire* la cual facilita el monitoreo del preprocesador.

Una vez se ha instalado hay que ejecutar el comando *ldconfig* para actualizar las librerías compartidas, y finalmente es recomendable crear un enlace simbólico al archivo ejecutable para que pueda ser ejecutado desde cualquier ubicación.

```
cd $HOME/snort_src
wget https://snort.org/downloads/snort/snort-2.9.9.0.tar.gz
tar -xvzf snort-2.9.9.0.tar.gz
cd snort-2.9.9.0
./configure --enable-sourcefire
make
sudo make install

sudo ldconfig
sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

Para verificar que la instalación de Snort quedó correcta se ejecuta el comando snort con la opción *–v*

[26] DIETRICH, Noah “Snort 3 on Ubuntu 14 and 16”. {en línea}. {13 de marzo de 2018} disponible en: (https://www.snort.org/documents/snort-3-0-for-ubuntu-14-and-16).

```
mario@IDSubuntu:~/snort_src$ snort -V

   ,,_     -*> Snort++ <*-
  o"  )~   Version 3.0.0 (Build 243) from 2.9.11
   ""      By Martin Roesch & The Snort Team
           http://snort.org/contact#team
           Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using DAQ version 2.2.2
           Using LuaJIT version 2.0.4
           Using OpenSSL 1.0.2g  1 Mar 2016
           Using libpcap version 1.7.4
           Using PCRE version 8.38 2015-11-23
           Using ZLIB version 1.2.8
           Using FlatBuffers 1.8.0
           Using Hyperscan version 4.6.0 2018-02-17
           Using LZMA version 5.1.0alpha
```

10.5 CONFIGURACION DE SNORT COMO NIDS

Por razones de seguridad no es recomendable la ejecución de Snort ni de ninguna aplicación con el usuario *root* por tal motivo es necesario adecuar el sistema para la ejecución desde otro usuario, para lo cual se necesitan hacer los siguientes ajustes:

Se crea un usuario y un grupo sin privilegios de *root* para el usuario *snort:snort*, se crean algunos directorios y archivos requeridos y se ajustan los permisos de ciertos archivos.

```
sudo chown -R snort:snort /etc/snort
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

Se crea el usuario y algunos directorios necesarios:

```
mario@IDSubuntu:~$ sudo groupadd snort
mario@IDSubuntu:~$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g
snort
mario@IDSubuntu:~$ sudo mkdir /etc/snort
mario@IDSubuntu:~$ sudo mkdir /etc/snort/rules
mario@IDSubuntu:~$ sudo mkdir /etc/snort
mario@IDSubuntu:~$ sudo mkdir /etc/snort/rules/iplists
mario@IDSubuntu:~$ sudo mkdir /etc/snort/preproc_rules
mario@IDSubuntu:~$ sudo mkdir /usr/local/lib/snort_dynamicrules
mario@IDSubuntu:~$ sudo mkdir /etc/snort/so_rules
```

Se algunos archivos que son necesarios para las listas de IP.

```
mario@IDSubuntu:~$ sudo touch /etc/snort/rules/iplists/black_list.rules
mario@IDSubuntu:~$ sudo touch /etc/snort/rules/iplists/white_list.rules
mario@IDSubuntu:~$ sudo touch /etc/snort/rules/local.rules
mario@IDSubuntu:~$ sudo touch /etc/snort/sid-msg.map
mario@IDSubuntu:~$ # Crear  directorios para logs :
mario@IDSubuntu:~$ sudo mkdir /var/log/snort
mario@IDSubuntu:~$ sudo mkdir /var/log/snort/archived_logs
mario@IDSubuntu:~$ # ajustes de permisos:
mario@IDSubuntu:~$ sudo chmod -R 5775 /etc/snort
mario@IDSubuntu:~$ sudo chmod -R 5775 /var/log/snort
mario@IDSubuntu:~$ sudo chmod -R 5775 /var/log/snort/archived_logs
mario@IDSubuntu:~$ sudo chmod -R 5775 /etc/snort/so_rules
mario@IDSubuntu:~$ sudo chmod -R 5775
/usr/local/lib/snort_dynamicrules/usr/local/lib/snort_dynamicrules
```

Es necesario cambiar de propietario a ciertos archivos para garantizar que el usuario snort pueda abrirlos.

Snort necesita varios archivos de configuración y preprocesadores dinámico los cuales se encuentran en el paquete de distribución descargado, y es necesario copiarlos al directorio /etc/snort.[27]

Es necesario pasar los siguientes archivos:

- ✓ classification.config
- ✓ file magic.conf
- ✓ reference.config
- ✓ snort.conf
- ✓ threshold.conf
- ✓ attribute table.dtd
- ✓ gen-msg.map
- ✓ unicode.map

Se copian los archivos de la siguiente manera:

```
cd ~/snort_src/snort-2.9.9.0/etc/
sudo cp *.conf* /etc/snort
sudo cp *.map /etc/snort
sudo cp *.dtd /etc/snort
cd ~/snort_src/snort-2.9.9.0/src/dynamic-
preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/
```

[27] DIETRICH, Noah “Snort 3 on Ubuntu 14 and 16”. {en línea}. {13 de marzo de 2018} disponible en: (https://www.snort.org/documents/snort-3-0-for-ubuntu-14-and-16).

La estructura de directorios de /etc/nort debe lucir de la siguiente manera:

```
mario@IDSubuntu:~$ tree /etc/snort
/etc/snort
├── attribute_table.dtd
├── classification.config
├── file_magic.conf
├── gen-msg.map
├── preproc_rules
├── reference.config
├── rules
│   ├── iplists
│   │   ├── black_list.rules
│   │   └── white_list.rules
│   └── local.rules
├── sid-msg.map
├── snort.conf
├── so_rules
├── threshold.conf
└── unicode.map

4 directories, 12 files
```

Para que snort se ejecute en modo NIDS es necesario modificar el archivo */etc/snort/snort.conf*.

También es necesario que se comenten (agregar un # delante de cada línea) todas las reglas del archivo */etc/snort/snort.conf.*

```
sudo sed -i "s/include \$RULE\_PATH/#include \$RULE\_PATH/" /etc/snort/snort.conf
```

Se modifica el archivo en el archivo */etc/snort/snort.conf* la variable *ipvar* HOME_NET, la cual queda así:

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.0/24
```

En este caso la red de prueba en que estamos configurando el NIDS es 192.168.1.0/24.

Continuando con el mismo archivo en el archivo */etc/snort/snort.conf,* hay que asegurarse que las siguientes líneas que generalmente comienzan en la 104 estén apuntando a los archivos correctos:

```
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
```

Una vez se termina de ajustar el archivo *etc/snort/snort.conf* se puede iniciar con la prueba de snort con la opción –T para indicar que se ejecutará en modo prueba, -i la interface donde escuchara y –c el archivo de configuración:

```
mario@IDSubuntu:~$ sudo  snort -T -i enp0s3 -c /etc/snort/snort.conf

(...)
Snort successfully validated the configuration!
Snort exiting
mario@IDSubuntu:~$
```

Para comprobar el funcionamiento se crea una regla para detectar tráfico en Facebook, esto con el fin de comprobar el funcionamiento inicial de nuestra instalación, para lo cual se crea un archivo *sudo vi /etc/snort/rules/local.rules,* y se agrega la siguiente regla.

```
alert tcp any any -> any any ( msg:"Facebook trafic Seen"; appids:"Facebook";sid:10000001; )
```

Se procede a la ejecución de snort para que escuche en la tarjeta de red *enp0s3* que es la tarjeta Ethernet de la máquina IDS.

```
mario@IDSubuntu:~/snort_src$ sudo /opt/snort/bin/snort -c
/opt/snort/etc/snort/snort.lua -R /etc/snort/rules/local.rules -i enp0s3 -A alert_fast
-s 65535 -k none
```

Desde otra terminal se ejecutó el comando *wget facebook.com* para generar tráfico hacia y desde el sitio facebook, lo que ocasiona que la alarma que se acaba de colocar se dispare mostrando lo siguiente:

```
03/30-18:32:37.739967 [**] [1:10000001:0] "Facebook trafic Seen" [**] [Priority: 0] [AppID:
Facebook] {TCP} 157.240.14.35:443 -> 192.168.1.251:40412
03/30-18:32:37.739998 [**] [1:10000001:0] "Facebook trafic Seen" [**] [Priority: 0] [AppID:
Facebook] {TCP} 192.168.1.251:40412 -> 157.240.14.35:443
03/30-18:32:37.810073 [**] [1:10000001:0] "Facebook trafic Seen" [**] [Priority: 0] [AppID:
```

10.6 INSTALACION DE BANYARD2

Para que las alarmas que snort genera se guarden en una base de datos como MySql es necesario para que Barnyard2 esté instalado y correctamente configurado en la misma máquina junto con Snort. Para esto se instalan los prerrequisitos, entre ellos mysql:

```
sudo apt-get install mysql-server libmysqlclient-dev mysql-client autoconf libtool -y
```

Se configura Snort para que guarde en formato binario los datos, para hacerlo se edita el archivo /etc/snort/snort.conf y en la línea 521 se adiciona la siguiente línea

```
output unified2: filename snort.u2, limit 128
```

Se procede con la descarga e instalación Barnyard2 2.1.14 desde el repositorio *github*:

```
cd ~/snort_src wget https://github.com/firnsy/barnyard2/archive/master.tar.gz -
O barnyard2-Master.tar.gz
tar zxvf barnyard2-Master.tar.gz
cd barnyard2-master
autoreconf -fvi -I ./m4
```

Barnyard2 necesita tener accesos a la librería *dnet.h*, la cual ya fue instalada antes en el paquete *libdumbnet*. Pero como Barnyard2 lo busca con un nombre diferente entonces es necesario crear un enlace simbólico de *dnet.h* a *dubmnet*.[28]

```
sudo ln -s /usr/include/dumbnet.h /usr/include/dnet.h
sudo ldconfig
```

Se apunta la instalación a la librería correcta de MySQl:

```
./configure --with-mysql --with-mysql-libraries=/usr/lib/i386-linux-gnu
```

Se compila e instala barnyard2:

```
make
sudo make install
```

[28] DIETRICH, Noah “Snort 3 on Ubuntu 14 and 16”. {en línea}. {13 de marzo de 2018} disponible en: (https://www.snort.org/documents/snort-3-0-for-ubuntu-14-and-16).

Se comprueba que haya quedado correctamente instalado:

```
mario@IDSubuntu:~/snort_src/barnyard2-master$  /usr/local/bin/barnyard2 -V

  _______   -*> Barnyard2 <*-
 / ,,_  \  Version 2.1.14 (Build 337)
 |o"  )~|  By Ian Firns (SecurixLive): http://www.securixlive.com/
  + "" +  (C) Copyright 2008-2013 Ian Firns <firnsy@securixlive.com>
mario@IDSubuntu:~/snort_src/barnyard2-master$
```

Banyard requiere unos archivos y directorios, a continuación se crean:

```
sudo cp ~/snort_src/barnyard2-master/etc/barnyard2.conf /etc/snort/
sudo mkdir /var/log/barnyard2
sudo chown snort.snort /var/log/barnyard2
sudo touch /var/log/snort/barnyard2.waldo
sudo chown snort.snort /var/log/snort/barnyard2.waldo
```

Se ingresa a MySql para realizar las configuraciones necesarias como creación de la base de datos Snort un usuario *snort* con *password* y ciertos privilegios:

```
mario@IDSubuntu:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
mysql> create database snort;
Query OK, 1 row affected (0.00 sec)

mysql> use snort;
Database changed
mysql> source ~/snort_src/barnyard2-master/schemas/create_mysql
Query OK, 0 rows affected (0.09 sec)
Query OK, 1 row affected (0.10 sec)
(…)
Query OK, 0 rows affected (0.06 sec)
```

Se crea el usuario Snort para que el NIDS se conecte a la base de datos.

```
mysql> CREATE USER 'snort'@'localhost' IDENTIFIED BY 'MySqlSNORTpassword';
Query OK, 0 rows affected (0.01 sec)

mysql> grant create, insert, select, delete, update on snort.* to 'snort'@'localhost';
Query OK, 0 rows affected (0.01 sec)
mysql>
```

Se edita el archivo /etc/snort/barnyard2.conf, para indicar a banyard2 los parámetros de conexión a la base de datos, agregando la siguiente línea al final del archivo:

```
# output alert_fwsam: 192.168.0.1/borderfw  192.168.1.254/wanfw
#
output database: log, mysql, user=snort password=MySqlSNORTpassword dbname=snort host=localhost sensor name=sensor01
```

Se comprueba que Snort este escribiendo las alertas en un archivo binario y que banyard2 las esté leyendo y guardando en mysql, para comprobarlo se ejecuta Snort:

```
mario@IDSubuntu:~$ sudo /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3
```

Se comprueban los archivos:

```
mario@IDSubuntu:~$ ls -l /var/log/snort/
total 12
drwsrwxr-t 2 snort snort 4096 Mar 30 23:13 archived_logs
-rw-r--r-- 1 snort snort    0 Mar 31 07:50 barnyard2.waldo
-rw------- 1 snort snort 2538 Mar 31 00:11 snort.log.1522472988
-rw------- 1 snort snort 2008 Mar 31 08:13 snort.u2.1522501915
mario@IDSubuntu:~$
```

Ahora se ejecuta banyard2 para procesar los archivos:

```
mario@IDSubuntu:~$ sudo barnyard2 -c /etc/snort/barnyard2.conf -d
/var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo \
> -g snort -u snort
Running in Continuous mode
        --== Initializing Barnyard2 ==--
Initializing Input Plugins!
Initializing Output Plugins!
```

Se pulsa *control+c* para terminar el proceso y se comprueba mediante una consulta a la base de datos que todas las alertas han sido guardadas en mysql:

```
mario@IDSubuntu:~$ mysql -u snort -p -D snort -e "select count(*) from event"
Enter password:
ERROR 1045 (28000): Access denied for user 'snort'@'localhost' (using
password: YES)
mario@IDSubuntu:~$ mysql -u snort -p -D snort -e "select count(*) from event"
Enter password:
+----------+
| count(*) |
+----------+
|       11 |
```

10.7 INSTALACION Y CONFIGURACION DE PULLEDPORK

El proceso de actualización de las reglas de NIDS podría resultar un trabajo sumamente engorroso pero la herramienta PulledPork ahorra una enorme cantidad de tiempo en mantener el sistema NID actualizado.

Se instalan los prerrequisitos:

```
sudo apt-get install -y libcrypt-ssleay-perl liblwp-useragent-determined-perl
```

Se procede a descargar e instalar la última versión de *PulledPork* desde los repositorios:

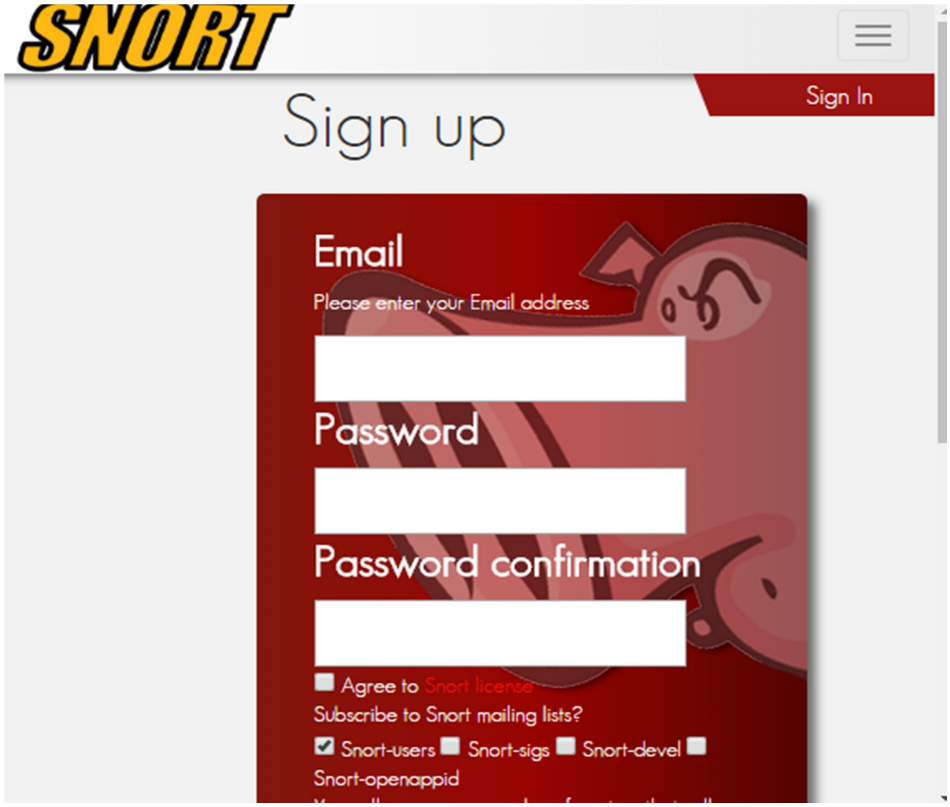
```
cd ~/snort_src
wget https://github.com/shirkdog/pulledpork/archive/master.tar.gz -O
pulledpork-master.tar.gz
tar xzvf pulledpork-master.tar.gz
cd pulledpork-master/
sudo cp pulledpork.pl /usr/local/bin
sudo chmod +x /usr/local/bin/pulledpork.pl
```

Para asegurarse que pulledpork está ejecutándose correctamente, se ejecuta el siguiente comando:

```
mario@IDSubuntu:~$ /usr/local/bin/pulledpork.pl -V
PulledPork v0.7.4 - Helping you protect your bitcoin wallet!
```

PulledPork puede descargar algunas reglas desde algunos repositorios como por ejemplo listas negras de *Talos* y las *free community ruleset* de Snort, pero es muy recomendable que se cree una cuenta gratuita en snort.org para obtener el *oinkcode* y descargar las reglas regulares y la documentación para esas reglas, para lo cual se ingresa a página https://www.snort.org/users/sign_up, como se observa en la figura 12.

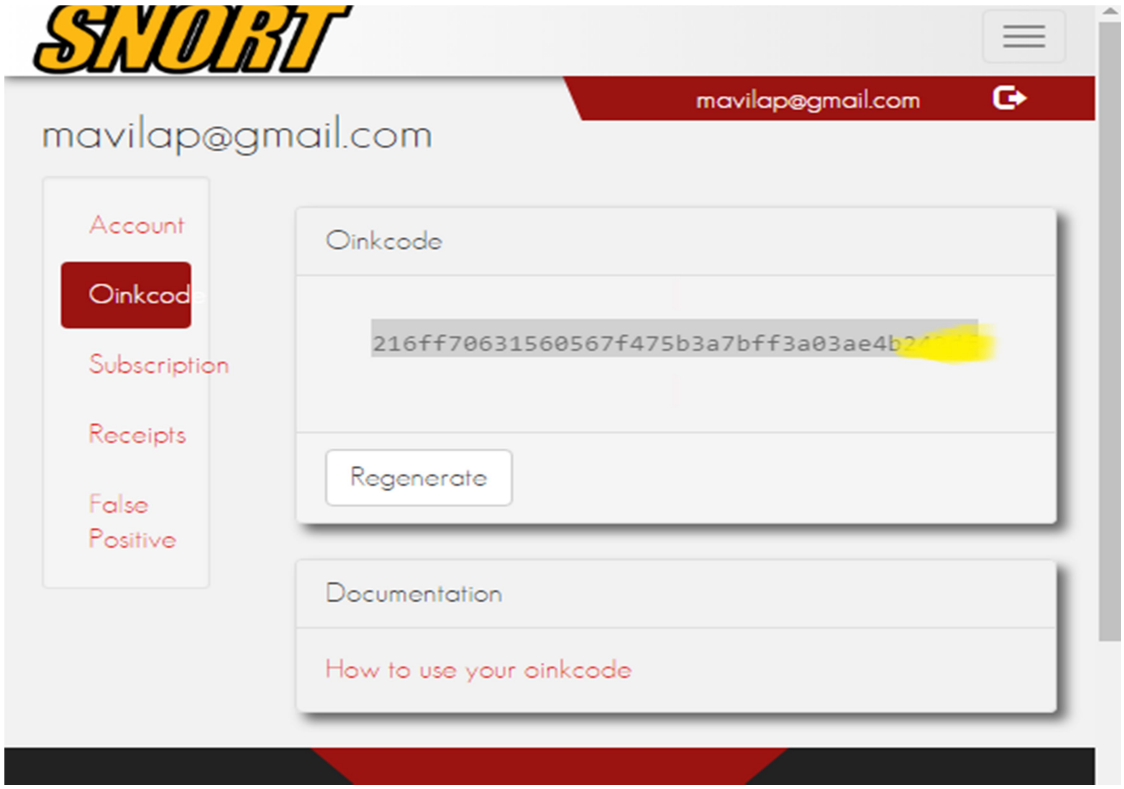
Figura 12. Creación de cuenta en snort



Fuente: El autor

Luego que se ingresa se puede obtener el *Oinkcode,* como se observa en la figura 13.

Figura 13. Oinkcode



Fuente: El autor

Se procede a configurar el archivo de configuración editando /etc/snort/pulledpork.conf y modificando las siguientes líneas:

Línea 19: ingrese su oinkcode Línea 29: Descomentar Línea 74: cambiar a : rule_path=/etc/snort/rules/snort.rules Línea 89: cambiar a: local_rules=/etc/snort/rules/local.rules Línea 92: cambiar a: sid_msg=/etc/snort/sid-msg.map Línea 96: cambiar a: sid_msg_version=2 Línea 119 cambiar a: config_path=/etc/snort/snort.conf Línea 133: cambiar a: distro=Ubuntu-12-04 Línea 141: cambiar a: black_list=/etc/snort/rules/iplists/

Se prueba PulledPork manualmente usando las opciones: -l para guardar logs en /var/log -c /etc/snort/snort.conf para comprobar que se ejecuta correctamente:

```
mario@IDSubuntu:~$ sudo /usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf -l
(…)
Rule Stats...
        New:-------57125
        Deleted:---0
        Enabled Rules:----28617
        Dropped Rules:----0
        Disabled Rules:---28508
        Total Rules:------57125
IP Blacklist Stats...
        Total IPs:-----1626
Done
Please review /var/log/sid_changes.log for additional details
Fly Piggy Fly!
```

Para que Snort use las reglas que PulledPork dejó en /etc/snort/rules/snort.rules.

```
include $RULE_PATH/snort.rules
```

Es posible configurar PulledPork para que se ejecute periódicamente y mantenga actualizadas las reglas del NIDS. También es recomendable que tanto snort como Banyard2 se configuren para ejecutarse como servicio cuando la maquina se inicie, esta configuración implica la realización de los script necesarios para ser ejecutados por *systemd init system.*[29]

```
[Unit]
Description=Barnyard2 Daemon
After=syslog.target network.target
[Service]
Type=simple
ExecStart=/usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -q -w /var/log/snort/barnyard2.waldo -g snort -u snort -D -a /var/log/snort/archived_logs
[Install]
```

[29] DIETRICH, Noah “Snort 3 on Ubuntu 14 and 16”. {en línea}. {13 de marzo de 2018} disponible en: (https://www.snort.org/documents/snort-3-0-for-ubuntu-14-and-16).

Al ejecutar el Snort como servicio se muestra la siguiente salida por consola, donde aprecia el status de la ejecución del programa:

```
mario@IDSubuntu:~$ sudo systemctl start snort
mario@IDSubuntu:~$ systemctl status snort
● snort.service - Snort NIDS Daemon
   Loaded: loaded (/lib/systemd/system/snort.service; enabled; vendor preset: en
   Active: active (running) since Sat 2018-03-31 10:19:03 -05; 24s ago
 Main PID: 25700 (snort)
    Tasks: 1
   Memory: 168.8M
      CPU: 23.745s
   CGroup: /system.slice/snort.service
           └─25700 /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort

Mar 31 10:19:03 IDSubuntu systemd[1]: Started Snort NIDS Daemon.
...skipping...
● snort.service - Snort NIDS Daemon
   Loaded: loaded (/lib/systemd/system/snort.service; enabled; vendor preset: en
   Active: active (running) since Sat 2018-03-31 10:19:03 -05; 24s ago
```

Al ejecutar el bantyard2 como servicio se muestra la siguiente salida por consola, donde aprecia el status de la ejecución del programa

```
mario@IDSubuntu:~$ sudo systemctl start barnyard2
mario@IDSubuntu:~$ systemctl status barnyard2
● barnyard2.service - Barnyard2 Daemon
   Loaded: loaded (/lib/systemd/system/barnyard2.service; enabled; vendor preset
   Active: active (running) since Sat 2018-03-31 12:23:11 -05; 13s ago
 Main PID: 25793 (barnyard2)
    Tasks: 1
   Memory: 7.5M
      CPU: 13.217s
   CGroup: /system.slice/barnyard2.service
           └─25793 /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var

Mar 31 12:23:11 IDSubuntu systemd[1]: Started Barnyard2 Daemon.
Mar 31 12:23:11 IDSubuntu barnyard2[25793]: Running in Continuous mode
Mar 31 12:23:11 IDSubuntu barnyard2[25793]:
```

10.8 INSTALACION DE LA INTERFAZ GRÁFICA PARA SNORT

10.8.1 BASE. Es una interfaz simple para Snort, llama mucho la atención su simplicidad y la facilidad de instalación además de otras virtudes que presenta la herramienta.
Para la instalación se procede con la instalación de los prerrequisitos:

```
sudo add-apt-repository ppa:ondrej/php
sudo apt-get update
sudo apt-get install -y apache2 libapache2-mod-php5.6 php5.6-mysql php5.6-cli php5.6 php5.6-common \ php5.6-gd php5.6-cli php-pear php5.6-xml
```

Se instala la aplicación Pear image Graph

```
sudo pear install -f --alldeps Image_Graph
```

Se procede con la instalación de ADODB:

```
cd ~/snort_src
wget https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-520-for-php5/adodb-5.20.8.tar.gz
tar -xvzf adodb-5.20.8.tar.gz
sudo mv adodb5 /var/adodb
sudo chmod -R 755 /var/adodb
```

Se procede a descargar descomprimir e instalar BASE al directorio root de apache:

```
cd ~/snort_src
wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
tar xzvf base-1.4.5.tar.gz
sudo mv base-1.4.5 /var/www/html/base/
```

Se crea un archivo de configuración de BASE a partir de la distribución descargada:

```
cd /var/www/html/base sudo cp base_conf.php.dist base_conf.php
```

Se edita el archivo de configuración y se modifican las siguientes lineas para que queden de la siguiente manera:

```
$BASE_urlpath = '/base'; # linea 50
$DBlib_path = '/var/adodb/'; # linea 80
$alert_dbname = 'snort'; # linea 102
$alert host = 'localhost';
$alert_port = '';
$alert_user = 'snort';
$alert_password = 'MySqlSNORTpassword'; # linea 106
//$graph_font_name = "Verdana"; //$graph_font_name = "DejaVuSans"; linea 506
 //$graph_font_name = "Image_Graph_Font"; $graph_font_name = "";
```

Se ajustan algunos permisos y se reinicia el servidor apache:

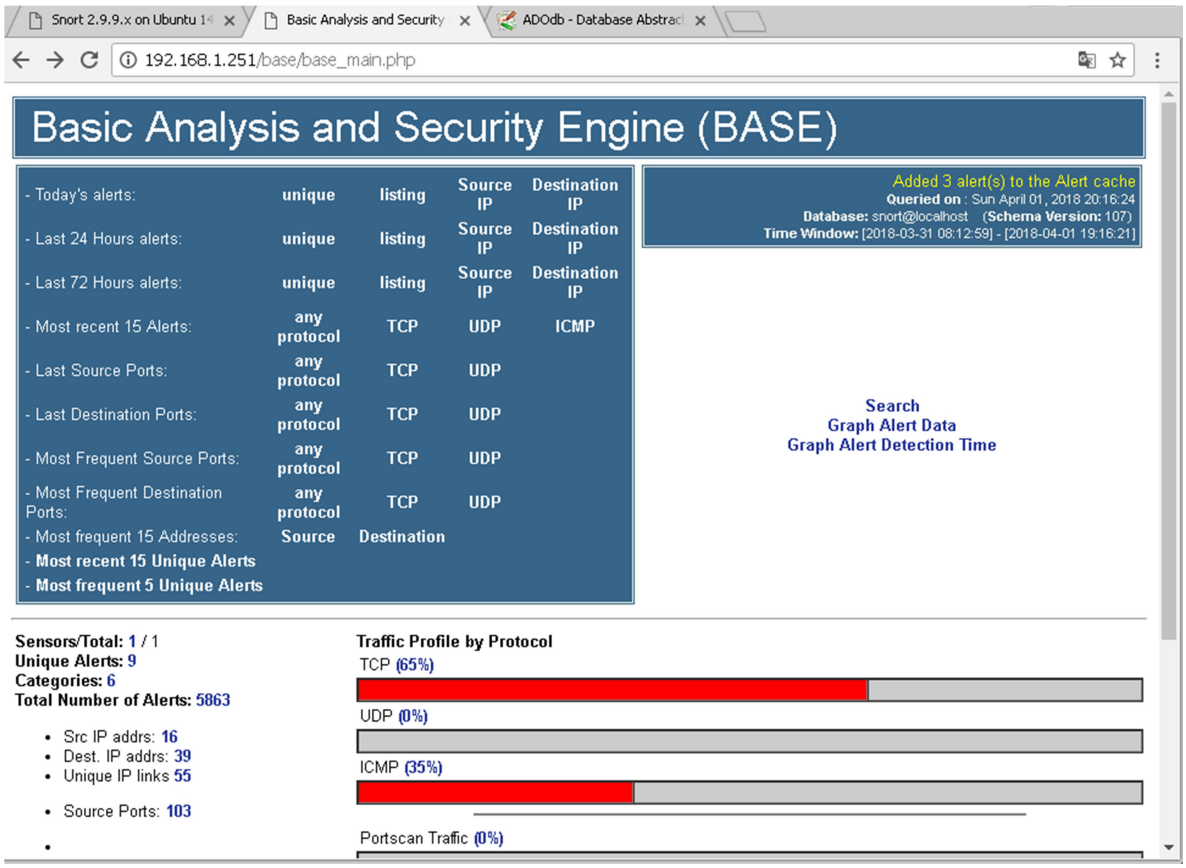
```
sudo chown -R www-data:www-data /var/www/html/base
sudo chmod o-r /var/www/html/base/base_conf.php
sudo service apache2 restart
```

El resto de la configuración de BASE se realiza desde el navegador, como se observa en la figura 14.

Para ello abrimos un navegador y digitamos la dirección IP de la máquina NIDS

1. http://192.168.1.251/base/index.php y click em *setup page link*
2. Click en el boton *Create BASE AG*
3. Click en *Main page line*

Figura 14. Instalación de BASE.



Fuente. El autor

11. PLAN DE PRUEBAS DEL IDS

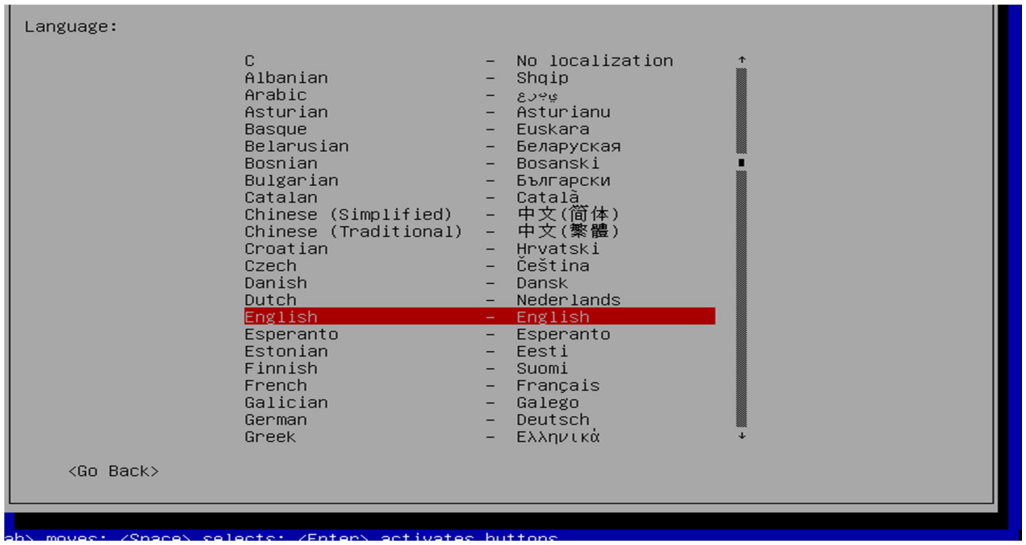
11.1 INSTALACION DE KALI LINUX

Kali Linux es una distribución Linux que trae instaladas una gran gama de herramientas para pruebas de vulnerabilidades en diferentes sistemas. Esta distribución está basada en debían y es la sucesora de la clásica distribución Backtrak, que era las distribución más popular para la realización de pruebas de seguridad en diversos sistemas. Ahora ese lugar lo ostenta la distribución *kali linux* [30].

Para la instalación se procedió con la descarga del archivo ISO para la distribución Kali Linux, y se configuró la máquina para que arranque desde la ISO, luego se inició la instalación en modo texto.

Se seleccionó el idioma inglés como se observa en la figura 15.

Figura 15. Instalación de Kali Linux

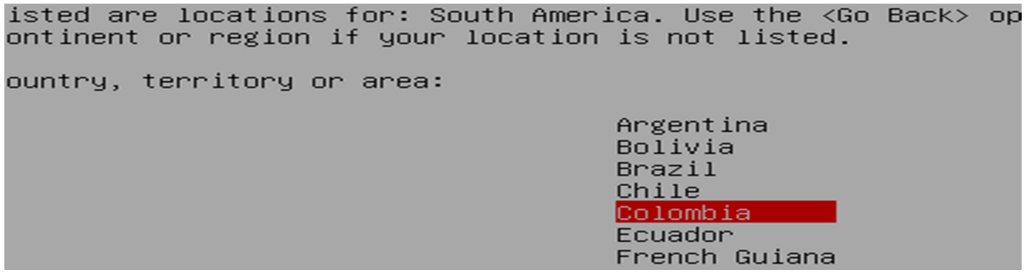


Fuente. El autor

[30] KALI LINUX "Official Documentation". {En línea}. {abril 15 de 2018} Disponible en: (http://es.docs.kali.org/installation-es/instalacion-de-kali-linux-en-un-disco-duro).

Luego se selecciona el país, como se observa en la figura 16.

Figura 16. Instalación de kali, selección del país

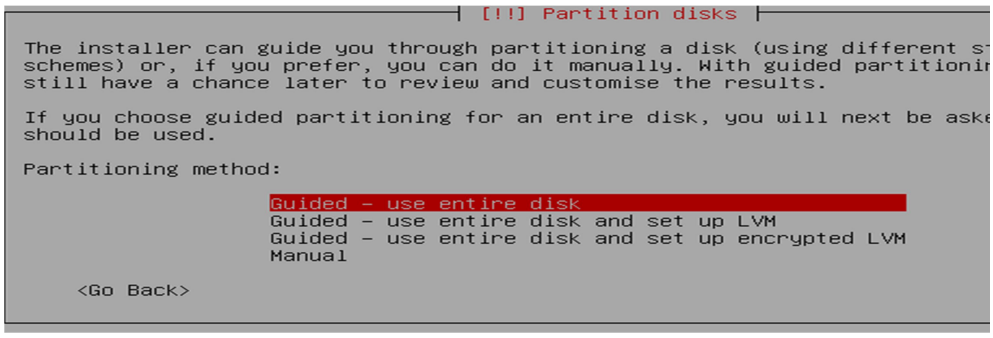


Fuente: El autor

Se asignó el nombre de la máquina: mariol en este caso, con el dominio mariol.com y luego se procedió a la creación de clave de root y usuario operador.

Se selecciona la opción de particionar todo el disco haciendo que el script de instalación utilice todo el almacenamiento disponible, como se observa en la figura 17.

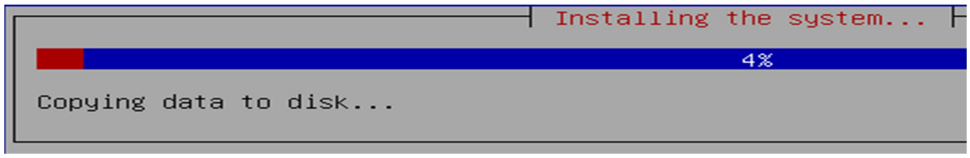
Figura 17. Instalación de kali Linux, Opción de disco



Fuente. El Autor

Luego de esto comienza la instalación hasta terminar como se observa en la figura 18.

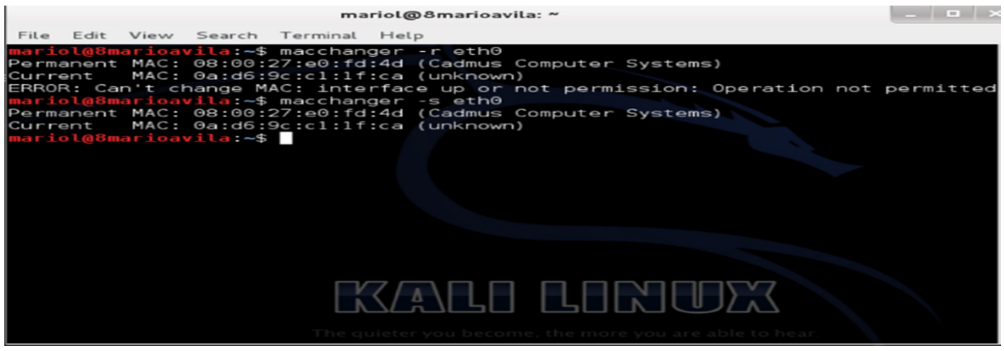
Figura 18. Instalando de kali linux



Fuente el autor

Finalmente se configuró la opción de GRUB para instalarse el disco, en el MBR. Una vez instalado el sistema se inició como se puede apreciar en la figura 19.

Figura 19. Kali linux



Fuente. El Autor

11.2 CONFIGURACION DE FEDORA PARA PRUEBAS

Se procede a la instalación de una máquina con la distribución Linux Fedora, para que sirva de huésped para hospedar la aplicación DVWA, la cual consiste en una aplicación web con agujeros la cual se describe brevemente en los siguientes apartados.

Luego de la instalación de la maquina Linux Fedora, se procede a la preparación de todos los componentes necesarios para la realización de los test. Se configuró

la máquina virtual Fedora con bajos niveles de seguridad, para lo cual fue necesario deshabilitar Selinux y el firewall de iptables para lo cual se siguen los siguientes pasos:

Se procede a editar el archivo de configuración de SElinux, colocando la variable SELINUX="disable" y se apaga el firewall para facilitar la prueba, con los siguientes comandos

 # vi /etc/selinux/config

 # chconfig iptables off

Se instalan con el comando *yum*, desde la cuenta *root* los paquetes de *apache* y *MySQL*

#yum install mysql mysql-server

Se inicia el servicio con el comando service.

#service mysqld start

Se le asigna una clave al usuario *root* de mysql para luego ingresar y crear La base de datos DVWA.

Una vez que se tiene listo el servidor mysql se procede a la instalación de PHP y otras librerías necesarias:

#yum install php php-mysql php-pear php-pear-DB wget

11.3 PRUEBAS DE APLICACIÓN CON AGUJEROS

DVWA es una aplicación con agujeros, la cual nos facilita realizar algunas pruebas del NIDS, donde se busca demostrar que el dispositivo está generando las alarmas correspondientes, al momento de intentar aprovechar las vulnerabilidades de esta aplicación.

Para la instalación de DVWA fue necesario hacer previamente la preparación de la máquina, lo cual se aprecia en el apartado ...11.2...

La descarga de la aplicación se puede hacer desde el sitio web *http://www.dvwa.co.uk/.*

Se procede a descargar el paquete por cualquiera de los medios disponibles, ya sea con *wget* o desde el navegador web.

Luego de descomprimir la carpeta, se copia el archivo a la carpeta *root* del servidor http.

#cp -R DVWA /var/www/html/dvwa*

Se edita el archivo: config.inc.php, pero es recomendable hacer una copia de seguridad del mismo:

#nano /var/www/html/dvwa/config/config.inc.php

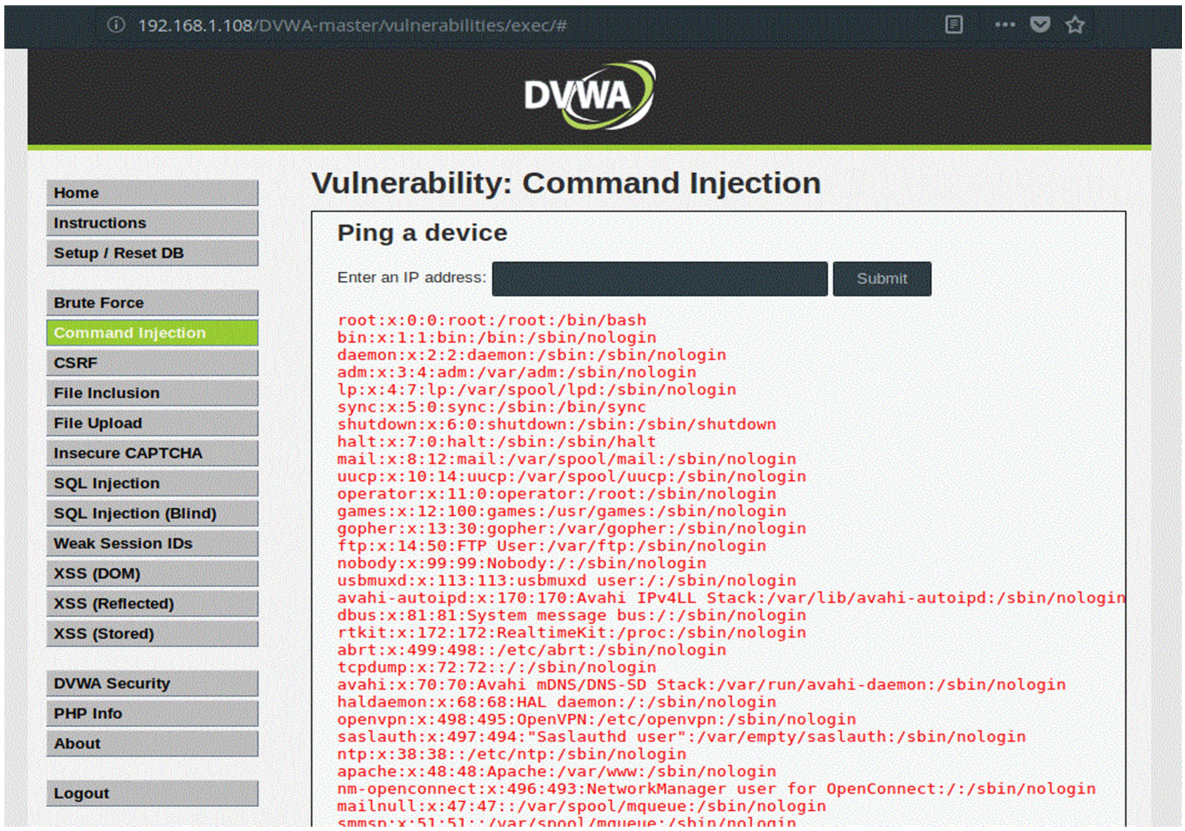
Se configura el acceso al servidor MySQL, y se cambia el propietario de la carpeta dvwa para finalmente reiniciar el servidor apache:

#chown -R apache: /var/www/html/dvwa

#/etc/init.d/httpd restart

Para ingresar a la aplicación, se hace desde un navegador, colocando la dirección IP, en este caso 192.168.1.108, que fue asignada para esta máquina.

Figura 20. Inicio de la aplicación DVWA



Fuente: El autor.

11.4 ATAQUE DOS

En el set de pruebas del NIDS, configurado como máquina virtual se realizaron simulacros de ataques de denegación de servicios DoS, se realizaron pruebas con las herramientas *hping3* y *ettercap* respectivamente.

11.4.1 Ataque DoS con hping3.

Para la realización de esta prueba se procedió de la siguiente manera:
Se utilizó una maquina atacante con *kali* con IP *192.168.1.3* y una maquina victima con IP 192.168.1.2

Este ataque con hping3 consiste en inundar la victima de mensajes SYN aprovechándose del funcionamiento del protocolo TCP, el cual para iniciar conexión, una de las partes inicia enviando un SYN, la otra parte responde con SYN+ACK, y quien comenzó la comunicación responde ACK. Para este ataque se envían muchas peticiones SYN con el comando *hping3,* se deja sin la respuesta ACK lo que dejará a la víctima esperando y consumiendo una cantidad exagerada de recursos hasta degradar el servicio.

root@8marioavila:/home/mariol# hping3 -p 80 -S --flood 192.168.1.108

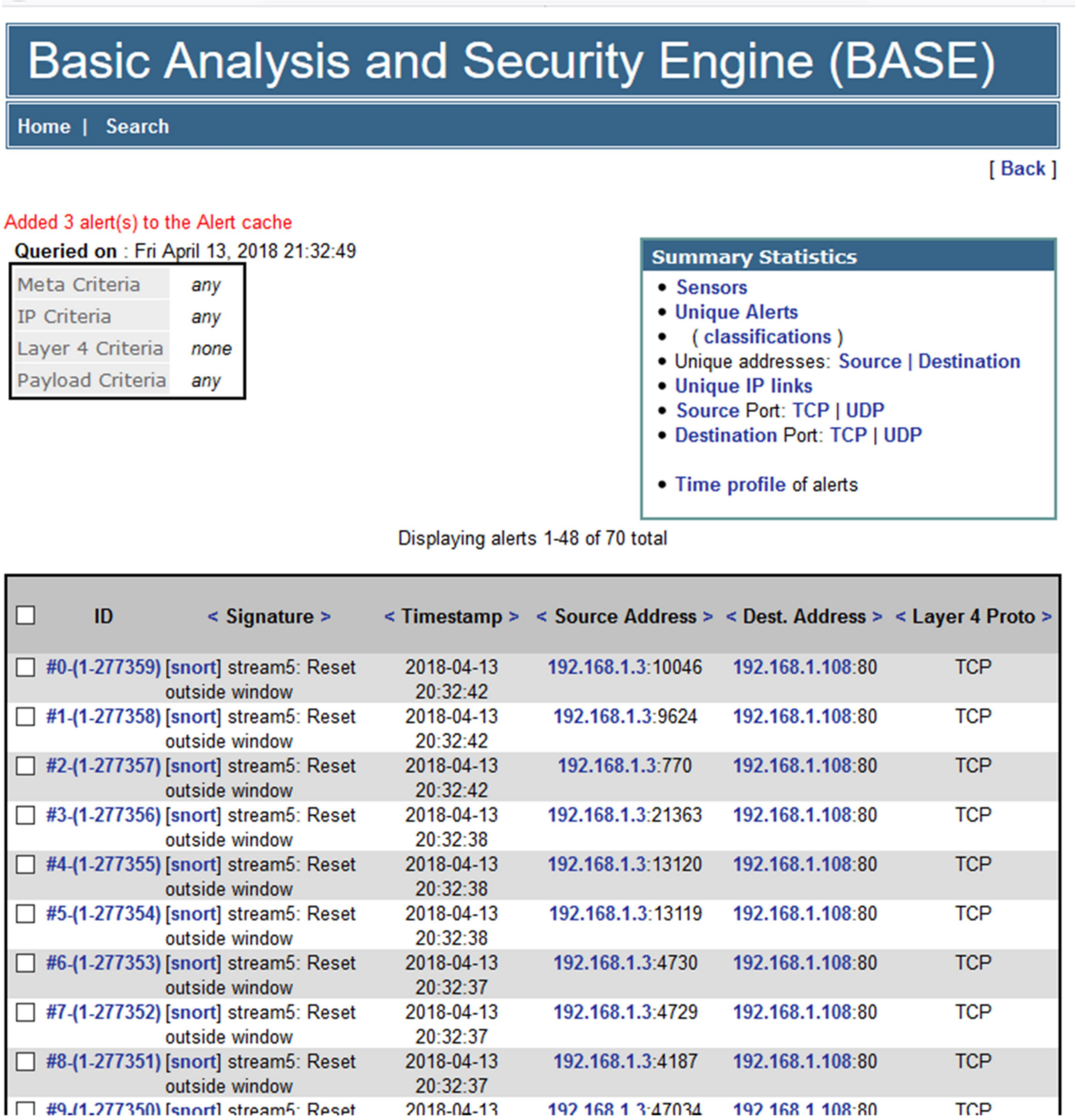
HPING 192.168.1.108 (eth0 192.168.1.108): S set, 40 headers + 0 data bytes

hping in flood mode, no replies will be shown

En el anterior comando se usa el comando hpin3 para simular un ataque de negación de servicios por inundación SYN, dirigido a la maquina 192.168.1.108 con, en el puerto 80, la opción –S para indicar el tipo SYN, y –flood para indicar que es a la máxima velocidad posible.

Al revisar la interfaz gráfica de Snort se pueden apreciar un aumento exagerado de alarmas de las dos máquinas involucradas en la prueba. Como se aprecia en la figura 21.

Figura 21. Actividad detectada por snort en prueba de inundación por SYN



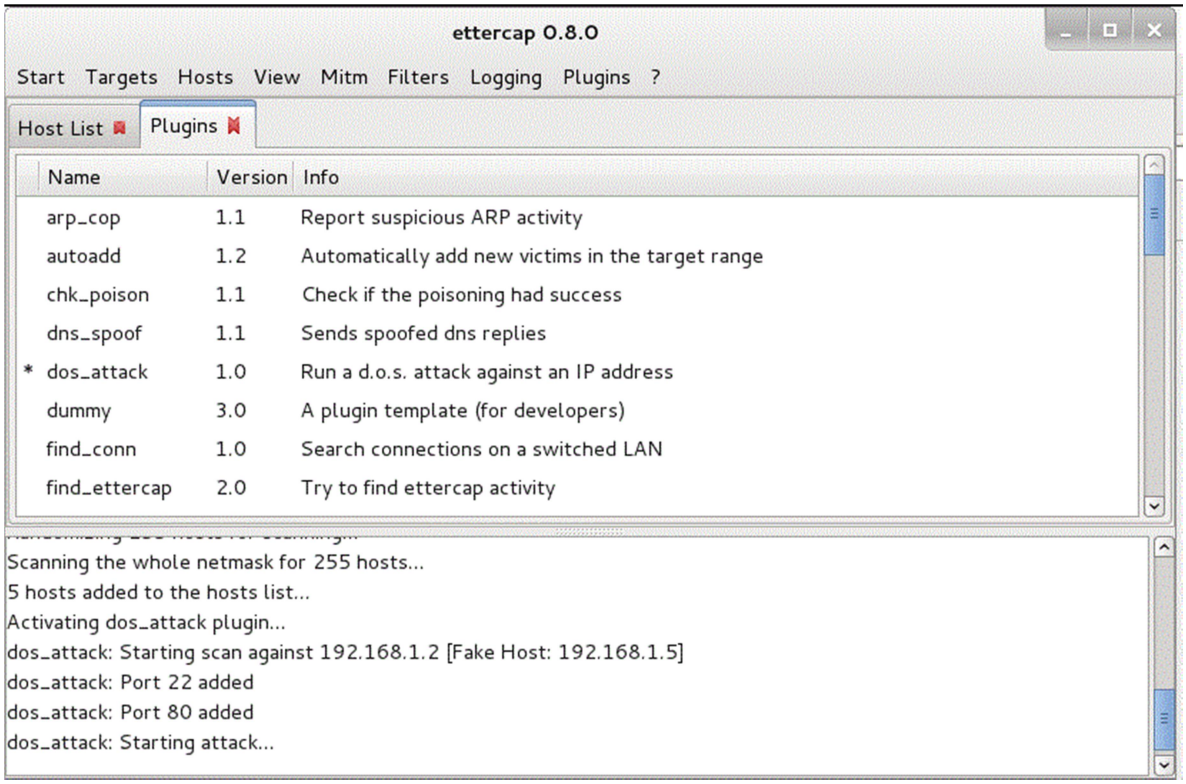
Fuente: El autor

11.4.2 Ataque DoS(denial of service) con *ettercap*. Ettercap es una herramienta que posibilita capturar el flujo de datos entre dos dispositivos, es usado principalmente para ataques tipo MITM (Man In The Middle en Ingles), el cual básicamente consiste en ubicar la tarjeta de red en modo promiscuo entre los dos equipos, y de esta manera capturar información como usuarios, contraseñas o certificados de acceso.

Para esta prueba se utilizó el plugins *dos_atack* que se encuentra presente en la herramienta ettercap, la cual está incluida en las distribuciones de kali linux.

Para la realización de la prueba se inicia la herramienta ettercap dese la consola, se utiliza el plugin *dos_atack* como se observa en la figura 22.

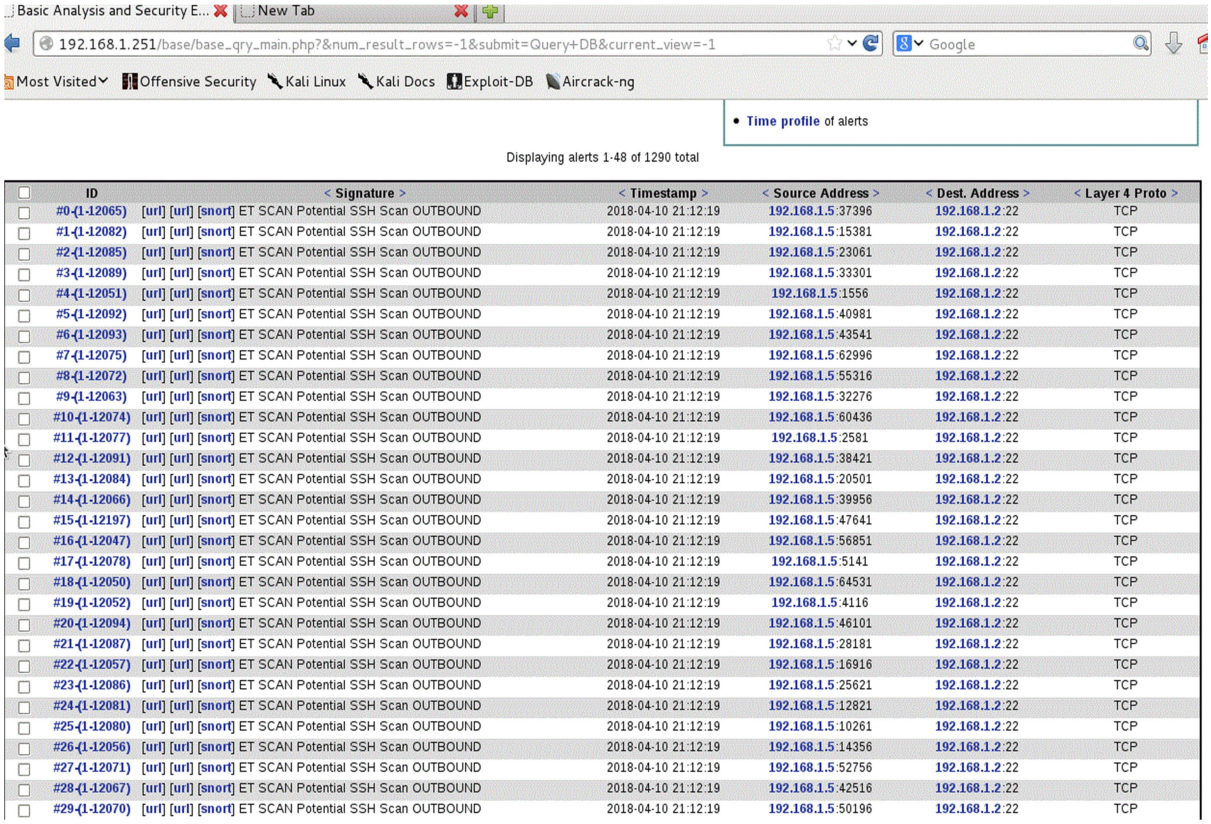
Figura 22. Ataque DoS desde ettercap



Fuente: El autor

Una vez se inicia el ataque se procede a revisar la el monitor del NIDS, observándose un aumento significativo de tráfico desde la IP de la maquina kali, con destino a la IP del servidor Fedora, como se aprecia en la figura 23.

Figura 23. Actividad detectada por snort en prueba de ataque con ettercap



ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-12065)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:37396	192.168.1.2:22	TCP
#1-(1-12082)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:15381	192.168.1.2:22	TCP
#2-(1-12085)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:23061	192.168.1.2:22	TCP
#3-(1-12089)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:33301	192.168.1.2:22	TCP
#4-(1-12051)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:1556	192.168.1.2:22	TCP
#5-(1-12092)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:40981	192.168.1.2:22	TCP
#6-(1-12093)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:43541	192.168.1.2:22	TCP
#7-(1-12075)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:62996	192.168.1.2:22	TCP
#8-(1-12072)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:55316	192.168.1.2:22	TCP
#9-(1-12063)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:32276	192.168.1.2:22	TCP
#10-(1-12074)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:60436	192.168.1.2:22	TCP
#11-(1-12077)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:2581	192.168.1.2:22	TCP
#12-(1-12091)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:38421	192.168.1.2:22	TCP
#13-(1-12084)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:20501	192.168.1.2:22	TCP
#14-(1-12066)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:39956	192.168.1.2:22	TCP
#15-(1-12197)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:47641	192.168.1.2:22	TCP
#16-(1-12047)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:56851	192.168.1.2:22	TCP
#17-(1-12078)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:5141	192.168.1.2:22	TCP
#18-(1-12050)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:64531	192.168.1.2:22	TCP
#19-(1-12052)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:4116	192.168.1.2:22	TCP
#20-(1-12094)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:46101	192.168.1.2:22	TCP
#21-(1-12087)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:28181	192.168.1.2:22	TCP
#22-(1-12057)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:16916	192.168.1.2:22	TCP
#23-(1-12086)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:25621	192.168.1.2:22	TCP
#24-(1-12081)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:12821	192.168.1.2:22	TCP
#25-(1-12080)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:10261	192.168.1.2:22	TCP
#26-(1-12056)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:14356	192.168.1.2:22	TCP
#27-(1-12071)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:52756	192.168.1.2:22	TCP
#28-(1-12067)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:42516	192.168.1.2:22	TCP
#29-(1-12070)	[url] [url] [snort] ET SCAN Potential SSH Scan OUTBOUND	2018-04-10 21:12:19	192.168.1.5:50196	192.168.1.2:22	TCP

Fuente: El autor

11.5 OTROS ATAQUES

Una de las primeras actividades que realizan los delincuentes informáticos o personas mal intencionadas consiste en escanear puertos, para verificar cuales están abiertos en los servidores o equipos que se encuentran en una red.

A continuación se realiza un prueba usando la herramienta nmap, desde la maquina 192.168.1.3 con kali lunux, hacia la maquina 192.168.1.250

root@8marioavila:/home/mariol# nmap 192.168.1.250

Starting Nmap 6.46 (http://nmap.org) at 2018-05-07 15:03 COT

Nmap scan report for 192.168.1.250

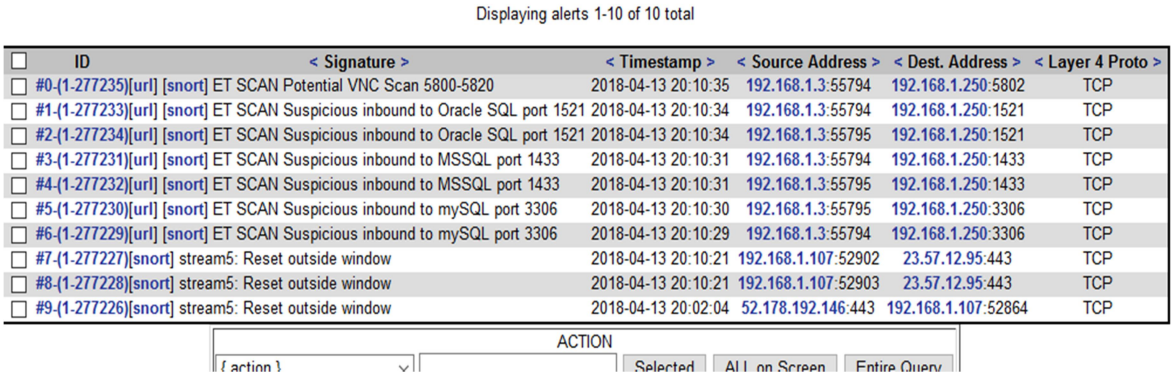
Host is up (0.00035s latency).

All 1000 scanned ports on 192.168.1.250 are filtered

MAC Address: 08:00:27:5A:97:6A (Cadmus Computer Systems)

Arrojando el siguiente resultado en el NIDS, que se aprecia en la figura 24.

Figura 24. Alertas de escaneo de puertos en snort



Displaying alerts 1-10 of 10 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-277235)[url] [snort]	ET SCAN Potential VNC Scan 5800-5820	2018-04-13 20:10:35	192.168.1.3:55794	192.168.1.250:5802	TCP
#1-(1-277233)[url] [snort]	ET SCAN Suspicious inbound to Oracle SQL port 1521	2018-04-13 20:10:34	192.168.1.3:55794	192.168.1.250:1521	TCP
#2-(1-277234)[url] [snort]	ET SCAN Suspicious inbound to Oracle SQL port 1521	2018-04-13 20:10:34	192.168.1.3:55795	192.168.1.250:1521	TCP
#3-(1-277231)[url] [snort]	ET SCAN Suspicious inbound to MSSQL port 1433	2018-04-13 20:10:31	192.168.1.3:55794	192.168.1.250:1433	TCP
#4-(1-277232)[url] [snort]	ET SCAN Suspicious inbound to MSSQL port 1433	2018-04-13 20:10:31	192.168.1.3:55795	192.168.1.250:1433	TCP
#5-(1-277230)[url] [snort]	ET SCAN Suspicious inbound to mySQL port 3306	2018-04-13 20:10:30	192.168.1.3:55795	192.168.1.250:3306	TCP
#6-(1-277229)[url] [snort]	ET SCAN Suspicious inbound to mySQL port 3306	2018-04-13 20:10:29	192.168.1.3:55794	192.168.1.250:3306	TCP
#7-(1-277227)[snort]	stream5: Reset outside window	2018-04-13 20:10:21	192.168.1.107:52902	23.57.12.95:443	TCP
#8-(1-277228)[snort]	stream5: Reset outside window	2018-04-13 20:10:21	192.168.1.107:52903	23.57.12.95:443	TCP
#9-(1-277226)[snort]	stream5: Reset outside window	2018-04-13 20:02:04	52.178.192.146:443	192.168.1.107:52864	TCP

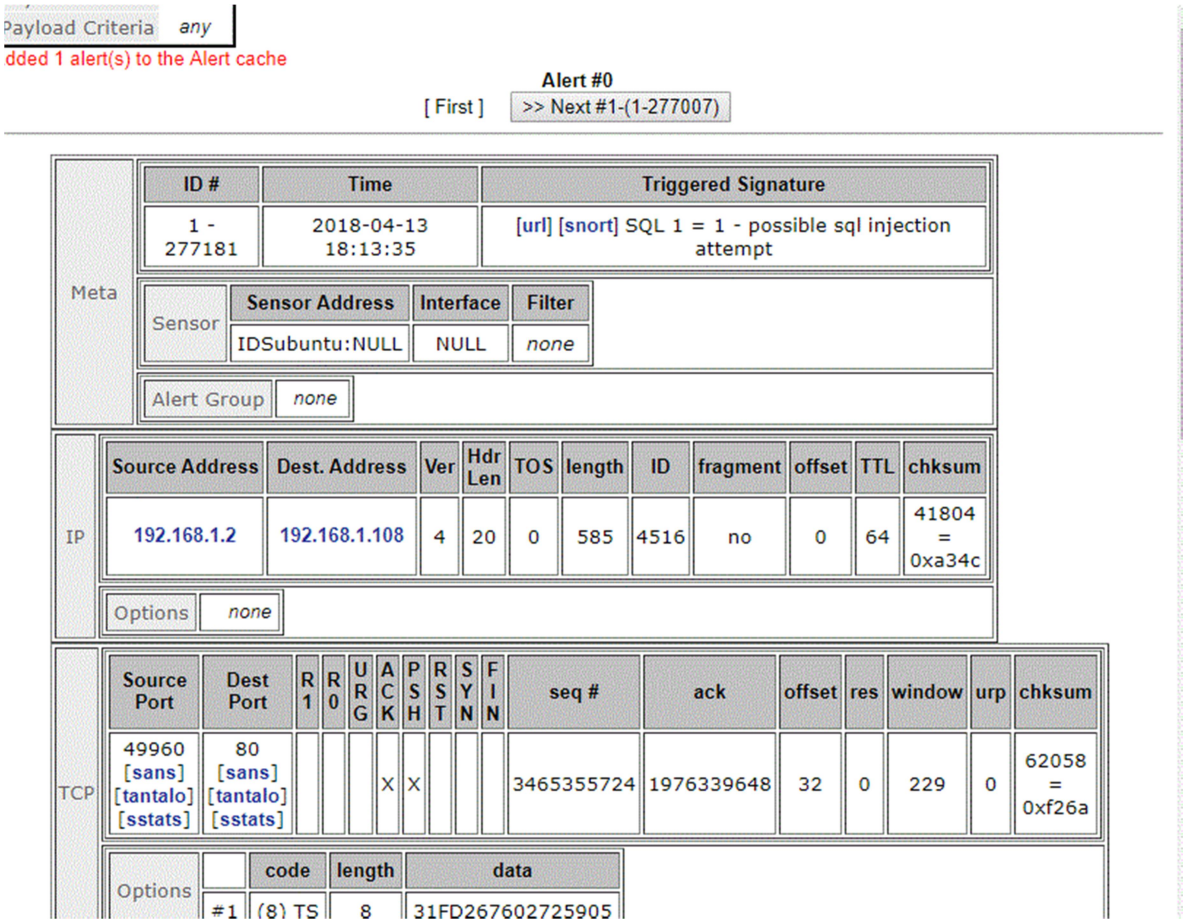
ACTION

{ action } Selected ALL on Screen Entire Query

Fuente: autor

Se realizó prueba utilizando SQL-injection, para lo cual se utilizó la herramienta DVWA que ya se había instalado previamente y configurado para nivel bajo de seguridad, se colocó en el formulario un dato y la cadena “WHERE 1= 1”, provocando que saltaran varias alarma en el IDS, las cuales se observan un poco más detallado en la figura 25.

Figura 25. Salida de comando para SQL Injection.



Payload Criteria any

dded 1 alert(s) to the Alert cache

Alert #0

[First] >> Next #1-(1-277007)

Meta

ID #	Time	Triggered Signature
1 - 277181	2018-04-13 18:13:35	[url] [snort] SQL 1 = 1 - possible sql injection attempt

Sensor	Sensor Address	Interface	Filter
	IDSubuntu:NULL	NULL	none

Alert Group	none

IP

Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	fragment	offset	TTL	chksum
192.168.1.2	192.168.1.108	4	20	0	585	4516	no	0	64	41804 = 0xa34c

Options	none

TCP

Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	seq #	ack	offset	res	window	urp	chksum
49960 [sans] [tantalo] [sstats]	80 [sans] [tantalo] [sstats]				X	X				3465355724	1976339648	32	0	229	0	62058 = 0xf26a

Options		code	length	data
	#1	(8) TS	8	31FD267602725905

Fuente: Autor.

11.6 RESULTADOS

Tal como se aprecia en cada una de las actividades realizadas en los apartes de este documento, el NIDS diseñado monitorea el tráfico de la red, de manera adecuada, generando las alarmas para cada una de las actividades maliciosas realizadas en este ambiente de red controlado.

Como resultado de este proyecto se destacan los siguientes productos:

-Documento del trabajo de grado donde se describe detalladamente la metodología de implementación de un IDS con la herramienta Snort.

-Un apartado donde se detalla un plan de pruebas que garantiza el funcionamiento del sistema de detección de intrusiones.

- Una tabla con el inventario de activos informáticos del CCAV puerto Colombia.
- Diagramas detallados de la topología de la red del CCAV Puerto Colombia.

11.7 FALSOS POSITIVOS

Un falso positivo se presenta cuando se dispara una alarma por un evento a una actividad que es reportada como sospechosa dentro de la operación del IDS, el IDS la reporta como actividad maliciosa, pero en realidad no son actividades maliciosas ni perjudícales para la operación de la red.

Es sabido que esta es tal vez la mayor desventaja de los NIDS, debido a que los falsos positivos podrían significar un desgaste en prestaciones tanto para el sistema como para los administradores de la red, debido a la cantidad recursos que se deben disponer para escudriñar el origen e incidencia de estas “anomalías” ; empeorando el asunto si la configuración de snort es en modo IPS, debido que se podrían presentar afectación de ciertos protocolos o servicios por bloqueo del IPS.

11.8 RECOMENDACIONES

Hoy día el fomento de la cultura de la seguridad debe ser una de las actividades primordiales de las organizaciones, sin embargo a menudo en algunas organizaciones esta suele estar descuidada.

Se sabe que la delincuencia opera cuando se baja la guardia o cuando se está demasiado confiado. La cultura de la seguridad es una de las barreras más efectivas para mantener la información a salvo de la delincuencia informática.

Se sabe de las bondades de tener un IDS como uno de los dispositivos de seguridad avanzados en un sistema de seguridad informática, y lo que puede significar como herramienta de protección para contribuir a garantizar la disponibilidad, integridad y confidencialidad de la información en la organización, no obstante esta poderosa herramienta no tendría mayor relevancia en la organización si no se dispone del personal debidamente entrenado para revisar , analizar y tomar decisiones en base a los log o historiales de actividades sospechosas detectadas y almacenadas por snort.

También es importante que se garantice que las actualizaciones de reglas se estén aplicando periódicamente y así disponer de una barrera de protección para la defensa en contra de las últimas modalidades de ataques.

Un IDS es una medida de seguridad que debe ser implementada en todas las redes para mitigar el riesgo de vulneración de la red.

Para disminuir el alto tráfico debido a las actualizaciones de los sistemas operativos Windows, se debe considerar la implementación de un servidor de actualizaciones para garantizar la prestación del servicio de conectividad en un nivel óptimo.

No es recomendable la desactivación del sistema de actualización de los sistemas Windows bajo ningún punto de vista.

Para futuros proyectos se recomienda determinar la viabilidad de un IPS, que estaría en capacidad no solamente de generar alarmas, sino de detener ataques.

11.9 DIVULGACIÓN

Este trabajo de grado se divulgará a través una ponencia en el SENA, en el marco del convenio SENA – UNAD, y queda abierta la posibilidad de que este proyecto sea socializado en los canales institucionales de la Universidad Abierta y a Distancia, y en los diferentes eventos académicos donde se exponen proyectos relacionados con las tecnologías de la información.

También se planea la elaboración de un artículo para publicarse en una revista científica.

CONCLUSIONES

1. Con el desarrollo de este proyecto se logró hacer el levantamiento de la información del CCAV Puerto Colombia, lográndose determinar que el centro cuenta con una infraestructura de red moderna, segmentada en 2 VLANs, soportada por 5 switchs que proveen un servicio de conectividad robusto. Los diagramas de la topología de la red, la configuración y distribución de los dispositivos realizados permitieron concebir el diseño del sistema de detección de intrusos NIDS adecuado para el centro. La realización de este proyecto evidencia un inventario de activos informáticos muy moderno y actualizado, para el cual se diseñó el IDS, administrado localmente por el personal de TI, con el fin de detectar tempranamente actividad ilícita o anomalías que pudieran impactar negativamente la disponibilidad, integridad y confidencialidad de la información que transita por cada uno de los canales, además de dejar un log de registro de las actividades sospechosa que pudiera proporcionar un registro en el tiempo para posteriores estudios.

2. Para el diseño del IDS se planteó un esquema basado en máquinas virtuales, en las cuales se instalaron las herramientas requeridas para la puesta en marcha del IDS, en un ambiente controlado. Se logró la implementación del sistema, mediante una metodología pormenorizada de cada componente o *plugins* de Snort, posibilitando la consolidación del conocimiento que se adquirió en el manejo del sistema Snort, configurado como NIDS. Se comprobó que la instalación y configuración de Snort es viable para ser instalado en ámbitos de redes diversas, contribuyendo a disminuir el riesgo de vulneración al proporcionar alertas sobre actividad maliciosa. Se observó que Snort se ha convertido en un estándar de facto, constituyéndose en una herramienta robusta de código abierto que cuenta con mucho soporte.

3. Se logró La planeación y diseño del sistema de detección de intrusos basado en red NIDS, esta fue una tarea bastante compleja que requirió conocimientos en muchas áreas de la ingeniería computacional. Para este proyecto se utilizó la versión 2.9 instalado sobre un sistema operativo Linux Ubuntu Server 16 04, la instalación se realizó componente por componente en un entorno aislado y controlado, lo que supuso una gran dosis de horas de trabajo y paciencia, ya que a pesar de que la documentación de los paquetes es clara, hubo detalles no contemplados, y a menudo se encontraron inconvenientes en la instalación de los componentes del snort que fueron resueltos durante la ejecución del proyecto.

4. Durante la ejecución del proyecto se realizaron simulacros de ataques de diversos tipos y se comprobó la efectividad del NIDS para detectar y generar alarmas para varios tipos de ataques, de tal manera que se garantiza la funcionalidad del NIDS, haciendo la salvedad de que la garantía de efectividad de esta sistema de protección requiere de las actualizaciones periódicas del sistema, de actualización de firmas o reglas y en este sentido el componente o herramienta PulledPork es un aliado imprescindible para encargarse de la tarea de la actualización de las firmas o reglas.

BIBLIOGRAFÍA

BACA URBINA, Gabriel. Introducción a la seguridad informática. Distrito Federal: Grupo Editorial Patria. 2016. ProQuest Ebook Central. 155p.

CISCO “Cisco Network-Based Intrusion. Capítulo 8”, {En línea}.{abril 20 de 2018} Disponible en:(https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/8_NIDS.pdf).

CASWELL, Brian; BEALE, Jay; BAKER, Andrew. Snort intrusion detection and prevention toolkit. Burlington: Syngress, 2007. p.219, p.297.

CHICANO TEJADA, Ester. Gestión de incidentes de seguridad informática , IC Editorial, 2014. 20p. .

COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014. p.137- 138. ProQuest Ebook Central.

DIETRICH, Noah “Snort 3 on Ubuntu 14 and 16”. {en línea}. {13 de marzo de 2018} disponible en: (https://www.snort.org/documents/snort-3-0-for-ubuntu-14-and-16).

FISCALÍA “Estadística de delitos”. {En línea}. {7 de julio de 2018}. disponible en:(https://www.fiscalia.gov.co/colombia/delitos/).

GONZALES GOMEZ, diego. Sistemas de detección de intrusiones. {En línea}. {10 mayo de 2018} disponible en: (http://www.criptored.upm.es/descarga/IDS_v1.0.zip). p. 19

KALI Linux “Official Documentation”. {En línea}. {abril 15 de 2018} Disponible en: (http://es.docs.kali.org/installation-es/instalacion-de-kali-linux-en-un-disco-duro).

KASPERSKY, Lab. “Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina”. {en línea}.{13 de marzo de 2018} Disponible en: (https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america).

LEY 1273 DE 2009. {En línea}. {12 abril de 2018} disponible en:(http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf).

LEY 1273 DE 2009. {En línea}. {13 abril de 2018} disponible en:(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492).

LÓPEZ AGUILERA, Purificación. Seguridad informática. Editex, 2010. P.10

MIFSUD, Elvira “Seguridad Informática, Introducción a la seguridad informática - Seguridad de la información / Seguridad informática”, {En línea}. {10 abril de 2018} // disponible en:(http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1) p.2.

UNAD “Transparencia y acceso a la información pública”. {En línea}. {10 abril de 2018} disponible en:(https://informacion.unad.edu.co).

YU, Zhenwei. TSAI, Jeffrey J.-P. Intrusion Detection: A Machine Learning Approach. 3rd ed: Imperial College Press, 2011. 41p.

ANEXO A. Definición y desglose de inventario de activos acorde a la metodología Magerit versión 3 en CCAV puerto Colombia (*leasing*)

CÓDIGO GRUPO DE ACTIVO	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
Computadoras del área GIDT			
[host]	grandes equipos	[serv]	Servidor HP Proliant
[mobile]	informática móvil	[portatile1]	Computadores portátiles Utilizados para diferentes actividades académicas y
[mobile]	informática móvil	[portatile2]	Computadores portátiles Utilizados para diferentes
[mobile]	informática móvil	[portatile3]	Computadores portátiles Utilizados para diferentes
[mobile]	informática móvil	[portatile4]	Computadores portátiles Utilizados para diferentes
[mobile]	informática móvil	[portatile5]	Computadores portátiles Utilizados para diferentes
Computadoras de la sala de Tutores			
[pc]	informática personal	[PCAIO1]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO2]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO3]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO4]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO5]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO6]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne 600
[pc]	informática personal	[PCAIO7]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO8]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO9]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO10]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO11]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO12]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne

ANEXO A. (continuación)

CÓDIGO GRUPO DE	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[pc]	informática personal	[PCAIO13]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO14]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO15]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO16]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO17]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO18]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO19]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO20]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO21]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO22]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO23]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO24]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO25]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO26]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO27]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO28]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
Computadoras de la Suite Virtual			
[pc]	informática personal	[PCAIO1]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO2]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO3]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO4]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO5]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO6]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne

ANEXO A. (Continuación)

CÓDIGO GRUPO DE	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[pc]	informática personal	[PCAIO7]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO8]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO9]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO10]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO11]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO12]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO13]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO14]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO15]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO16]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO17]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO18]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO19]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO20]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO21]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO22]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO23]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO24]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO25]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO26]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO27]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO28]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO29]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne

ANEXO A. (Continuación)

CÓDIGO GRUPO DE	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[pc]	informática personal	[PCAIO30]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
Computadores de Biblioteca			
[pc]	informática personal	[PCAIO1]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO2]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO3]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO4]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO5]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO6]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO7]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO8]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO9]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO10]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO11]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO12]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO13]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO14]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO15]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO16]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO17]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO18]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO19]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO20]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO21]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne

ANEXO A. (Continuación)

CÓDIGO GRUPO DE	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[pc]	informática personal	[PCAIO22]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO23]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO24]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO25]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO26]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO27]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO28]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO29]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO30]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO31]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO32]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO33]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO34]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO35]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO36]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO37]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO38]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO39]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO40]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
Computadores en el área de GIDT			
[pc]	informática personal	[PCAIO1]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO2]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO3]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne

ANEXO A. (Continuación)

CÓDIGO GRUPO DE	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[pc]	informática personal	[PCAIO4]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO5]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
AULAVIRTUALES 4-5-6 Y LABORATORIO DE ELECRONICA			
[pc]	informática personal	[PCAIO1]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO2]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO3]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO4]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO5]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO6]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO7]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO8]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO9]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO10]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
TUTORIA 1, TUTORIA 2, TUTORIA 3			
[pc]	informática personal	[PCAIO1]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO2]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO3]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO4]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO5]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO6]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO7]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO8]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO9]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO10]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO11]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne

ANEXO A. (Continuación)

CÓDIGO GRUPO DE	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[pc]	informática personal	[PCAIO12]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO13]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO14]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO15]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO16]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO17]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO18]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO19]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
AULA VIRTUAL 1, 2 Y 3			
[pc]	informática personal	[PCAIO1]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO2]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO3]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO4]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO5]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO6]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO7]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO8]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO9]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO10]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO11]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO12]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO13]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO14]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO15]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO16]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne

ANEXO A. (Continuación)

CÓDIGO GRUPO DE	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[pc]	informática personal	[PCAIO17]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO18]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
[pc]	informática personal	[PCAIO19]	Pc Tutores HP ALL IN ONE PRO ONE 600 HP ProOne
REDES DE COMUNICACIONES			
[wifi]	red inalámbrica	[R_ap1]	Ap para Red Inalámbrica
[wifi]	red inalámbrica	[R_ap2]	Ap para Red Inalámbrica
[wifi]	red inalámbrica	[R_ap3]	Ap para Red Inalámbrica
[wifi]	red inalámbrica	[R_ap4]	Ap para Red Inalámbrica
[wifi]	red inalámbrica	[R_ap]5	Ap para Red Inalámbrica
[LAN]	Red local	[R_Local]	Red local
[Internet]	Internet	[Internet]	Canal dedicado de Internet
[LAN]	Red local	[c_cabl]	Cableado para soportar la red LAN
[LAN]	Red local	[c_switch]	Switch 24 Puertos Hp Aruba 2530
[LAN]	Red local	[c_switch]	Switch 24 Puertos Hp Aruba 2530
[LAN]	Red local	[c_switch]	Switch 48 Puertos Hp Aruba 2930
[LAN]	Red local	[c_switch]	Switch 48 Puertos Hp Aruba 2930
[LAN]	Red local	[c_switch]	Switch 48 Puertos Hp Aruba 2930
[LAN]	Red local	[c_patch]	Patch Panel
[LAN]	Red local	[c_patch]	Patch Panel
[LAN]	Red local	[c_patch]	Patch Panel
[LAN]	Red local	[c_patch]	Patch Panel
[LAN]	Red local	[c_patch]	Patch Panel
[LAN]	Red local	[c_Rack1]	Rack de comunicaciones
[LAN]	Red local	[c_ Rack2]	Rack de comunicaciones
[LAN]	Red local	[c_ Rack3]	Rack de comunicaciones

ANEXO A. (Continuación)

CÓDIGO GRUPO DE	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[LAN]	Red local	[c_ Rack4]	Rack de comunicaciones
[LAN]	Red local	[c_ Rack5]	Rack de comunicaciones
[print]	medios de impresión	[E_Impresoras]	Impresoras Láser Tutores
[print]	medios de impresión	[E_Impresoras]	Impresoras Láser RyC
[print]	medios de impresión	[E_ImpresorasT]	Impresoras Láser GIDT
[router]	encaminadores	[R_enrutadores]	Enrutadores
SOFTWARE			
[os]	sistema operativo	[win10]	Windows 10
[os]	sistema operativo	[winServ]	Windows Server
[os]	sistema operativo	[linux]	Linux
[office]	ofimática	[officce]	Microsoft Office
[office]	ofimática	[WEB1]	CUTEPDF
DATOS/INFORMACIÓN			
[files]	Archivos	[acuerdos]	Información de Acuerdos de Homologaciones
		[Estadisticas]	Datos Estadisticos
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información
[password]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de usuarios del sistema
CLAVES CRIPTOGRÁFICAS			
[encrypt]	Claves de cifra	[sign1]	Claves de cifra
INVENTARIO DE SERVICIOS			
[ext]	A usuarios externos	[S_U_Externo]	Servicios prestados a usuarios externos

ANEXO A. (Continuación)

CÓDIGO GRUPO DE ACTIVO	NOMBRE GRUPO DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE ACUERDO A LA ENTIDAD	NOMBRE ACTIVO DE ACUERDO A LA ENTIDAD
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los funcionarios.
[email]	Correo electrónico	[S_correo]	Manejo de correoselectrónicos
SOPORTES DE INFORMACIÓN ALMACENAMIENTO ELECTRÓNICO			
[cd]	DiscosDuros DD	[A_DD]	Almacenamientos en Disco Duro
[usb]	Memoria USB	[A_Memoria]	Almacenamiento en Memoria USB
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD
SOPORTES DE INFORMACIÓN ALMACENAMIENTO NO ELECTRÓNICO			
		C_HistoriasA	Carpetas de Historias Académicas
		C_SoportesH	Carpetas de Homologciones
INSTALACIONES			
[building]	Edificio	[E_Edificio]	Instalacion física de la entidad
[site]	[site] recinto	[S_Auditorio]	Recinto del Auditorio
PERSONAL			
[ui]	Usuariosinternos	[U-Sistemas]	Personal de soporte TI
[adm]	Administradores de sistemas	[A_sistemas]	Funcionario de GIDT

Fuente: El autor.

ANEXO B. RESUMEN ANALÍTICO RAE

TEMA	Infraestructura tecnológica y seguridad en redes, Seguridad Informática. Sistemas de detección de intrusiones.
TÍTULO	Diseño de un sistema de detección de intrusos en la red de la UNAD sede Puerto Colombia.
AUTORES	Mario Luis Avila Pérez.
FUENTES BIBLIOGRÁFICAS	BACA URBINA, Gabriel. Introducción a la seguridad informática. Distrito Federal: Grupo Editorial Patria. 2016. ProQuest Ebook Central. 155p. CISCO "Cisco Network-Based Intrusion. Capítulo 8", {En línea}.{abril 20 de 2018} Disponible en :(https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/8_NIDS.pdf). CASWELL, Brian; BEALE, Jay; BAKER, Andrew. Snort intrusion detection and prevention toolkit. Burlington: Syngress, 2007. p.219, p.297 . CHICANO TEJADA, Ester. Gestión de incidentes de seguridad informática , IC Editorial, 2014. 20p. . COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014. p.137- 138. ProQuest Ebook Central. DIETRICH, Noah "Snort 3 on Ubuntu 14 and 16". {en línea}. {13 de marzo de 2018} disponible en: (https://www.snort.org/documents/snort-3-0-for-ubuntu-14-and-16). FISCALÍA "Estadística de delitos". {En línea}. {7 de julio de 2018}. disponible en:(https://www.fiscalia.gov.co/colombia/delitos/).. GONZALES GOMEZ, diego. Sistemas de detección de intrusiones. {En línea}. {10 mayo de 2018} disponible en: (http://www.criptored.upm.es/descarga/IDS_v1.0.zip). p. 19 [Publicación periódica]. KALI Linux "Official Documentation". {En línea}. {abril 15 de 2018} Disponible en: (http://es.docs.kali.org/installation-es/instalacion-de-kali-linux-en-un-disco-duro). KASPERSKY, Lab. "Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina". {en línea}.{13 de marzo de 2018} Disponible en(https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-. LEY 1273 DE 2009. {En línea}. {12 abril de 2018} disponible en:(http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf). LEY 1273 DE 2009. {En línea}. {13 abril de 2018} disponible en:(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492). LÓPEZ AGUILERA, Purificación. Seguridad informática. Editex, 2010. P.10 MIFSUD, Elvira "Seguridad Informática, Introducción a la seguridad informática - Seguridad de la información / Seguridad informática", {En línea}. {10 abril de 2018} // disponible en:(http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1) p.2.. UNAD "Transparencia y acceso a la información pública". {En línea}. {10 abril de 2018} disponible en:(https://informacion.unad.edu.co). [Publicación periódica]. YU, Zhenwei. TSAI, Jeffrey J.-P. Intrusion Detection: A Machine Learning Approach. 3rd ed: Imperial College Press, 2011. 41p.
AÑO	2018
RESUMEN	Este proyecto plantea un diseño de un sistema de detección de intrusos IDS en la red de la UNAD CCAV Puerto Colombia. Inicialmente se presenta la descripción, formulación y justificación del problema, se plantea el objetivo general y los objetivos específicos del proyecto. Se realizó un estudio para Identificar la topología de la red del CCAV Puerto Colombia con el fin de determinar las características y el inventario de activos informáticos. Utilizando la caracterización de la red, se elaboró el plan del diseño del sistema de detección de intrusos para la red de la UNAD CCAV Puerto Colombia, para lo cual se utilizó el sistema de código libre snort en su versión 2.9. Se diseña y ejecuta un plan de pruebas de con la finalidad de garantizar

	la funcionalidad del NIDS, haciendo la salvedad que estas pruebas se realizaron en una red aislada y controlada, externa a la red de la UNAD. Para estas pruebas se utilizó un set de herramientas de software libre.
PALABRAS CLAVES	IDS, reglas, ataque, comando, esniffer, información, iso/iec 27001, IPS, vulnerabilidad, testing, linux, red, snort, backtrack, servidor, paquete, plugins, interfaz
CONTENIDOS	
DESCRIPCION DEL PROBLEMA	Muy a menudo los usuarios de la red suelen conectarse a la red del CCAV con sus dispositivos móviles y o computadores portátiles los cuales podrían estar infectados por software malicioso lo cual representaría riesgo de vulneración para la red y dispositivos interconectados. El diseño de un sistema de detección de intrusiones en la red, constituye una herramienta importante que ayudaría a mitigar el riesgo de vulneración en una red. Para la UNAD CCAV Puerto Colombia sería muy

	importante contar con un sistema de sensores de actividad maliciosa que pueda monitorear , analizar y generar alertas tempranas de cualquier actividad sospechosa que se detecte en la red, proporcionando información valiosa para que los administradores de la red tomen las medidas pertinentes para evitar vulneraciones en los activos de la organización.
OBJETIVOS	OBJETIVO GENERAL Diseñar un sistema de detección de intrusos para la red de la UNAD CCAV de Puerto Colombia con el fin de mitigar la materialización de las amenazas en los activos informáticos. OBJETIVOS ESPECÍFICOS 1. Identificar la topología de la red del CCAV Puerto Colombia con el fin de determinar el inventario de activos informáticos. 2. Planificar el diseño del sistema de detección de intrusos para la red de la UNAD CCAV Puerto Colombia. 3. Diseñar un plan de pruebas de pentesting que garantice la funcionalidad del prototipo del sistema de detección de intrusos en una red aislada y controlada, externa a la red de la UNAD.
METODOLOGÍA	El presente proyecto de diseño de un sistema de detección de intrusos en la UNAD, CCAV de Puerto Colombia, corresponde a un proyecto aplicado, el cual contempla las siguientes actividades para cumplir los objetivos específicos del proyecto. - Realizar inventario de activos informáticos del CCAV. - Levantamiento de información sobre la topología de la red. - Revisión documental de cuáles son los tipos de IDS - Selección el tipo de IDS que ajusta la necesidad del CCAV - Preparación de la máquina para la instalación del IDS. - Instalación del prototipo del sistema IDS. - Preparación y configuración del set de pruebas. - Puesta en marcha del prototipo de NIDS una red aislada y controlada, externa a la red de la UNAD. - Elaboración de los documentos para presentar resultados.
PRINCIPALES REFERENTES TEÓRICOS	NIDS (Net IDS): Se les denomina de esta manera por sus sigla (Network intrusion Detection System) Sistemas de detección de intrusos basados en red. Estos actúan en una red mediante la captura y análisis del tráfico que circula a través de la misma. Estos sniffers de red capturan y analizan los paquetes, buscando similitudes con su base de firmas que lo identifique como actividad maliciosa o sospechosa. Un IDS Se trata de un dispositivo de red configurado en modo promiscuo para capturar todos los paquetes que circulan por un segmento de red de todos los dispositivos de ese segmento. Básicamente un IDS está constituido por la Fuentes recolector de datos las cuales pueden ser un log, dispositivo de red o el propio sistema. Reglas y filtros sobre los datos y patrones para actividad sospechosa. Dispositivo generador de informes y alarmas.
PRINCIPALES REFERENTES	IDS – snort. El IDS snort es un sistema de detección de intrusos basado en red (NIDS). Consta de un motor de detección de ataques y barrido de

CONCEPTUALES	puertos, Este sistema analiza el tráfico de paquetes de la red y lo compara con unos patrones y reglas previamente definidas en tiempo real generando alertas de actividad maliciosa en los casos que coincidan con estos patrones base de firmas. Snort (http://www.snort.org/) se distribuye bajo licencia GPL, y está disponible para sistemas operativos Windows y GNU/Linux. Es un IDS con mucha popularidad entre sus características más sobresalientes está la actualizaciones constantes de la base de datos de firmas.
RESULTADOS	Como resultado de este proyecto se destacan los siguientes productos: -Documento del trabajo de grado donde se describe detalladamente la metodología de implementación de un IDS con la herramienta Snort. -Un apartado donde se detalla un plan de pruebas que garantiza el funcionamiento del sistema de detección de intrusiones. - Una tabla con el inventario de activos informáticos del CCAV puerto Colombia. - Diagramas detallados de la topología de la red del CCAV Puerto Colombia.
CONCLUSIONES	1. Con el desarrollo de este proyecto se logró hacer el levantamiento de la información del CCAV Puerto Colombia, lográndose determinar que el centro cuenta con una infraestructura de red moderna, segmentada en 2 VLANs, soportada por 5 switchs que proveen un servicio de conectividad robusto. Los diagramas de la topología de la red, la configuración y distribución de los dispositivos realizados permitieron concebir el diseño del sistema de detección de intrusos NIDS adecuado para el centro. La realización de este proyecto evidencia un inventario de activos informáticos muy moderno y actualizado, para el cual se diseñó el IDS, administrado localmente por el personal de TI, con el fin de detectar tempranamente actividad ilícita o anomalías que pudieran impactar negativamente la disponibilidad, integridad y confidencialidad de la información que transita por cada uno de los canales, además de dejar un log de registro de las actividades sospechosa que pudiera proporcionar un registro en el tiempo para posteriores estudios. 2. Para el diseño del IDS se planteó un esquema basado en máquinas virtuales, en las cuales se instalaron las herramientas requeridas para la puesta en marcha del IDS, en un ambiente controlado. Se logró la implementación del sistema, mediante una metodología pormenorizada de cada componente o plugins de Snort, posibilitando la consolidación del conocimiento que se adquirió en el manejo del sistema Snort, configurado como NIDS. Se comprobó que la instalación y configuración de Snort es viable para ser instalado en ámbitos de redes diversas, contribuyendo a disminuir el riesgo de vulneración al proporcionar alertas sobre actividad maliciosa. Se observó que Snort se ha convertido en un estándar de facto, constituyéndose en una herramienta robusta de código abierto que cuenta con mucho soporte. 3. Durante la ejecución del proyecto se realizaron simulacros de ataques de diversos tipos y se comprobó la efectividad del NIDS para detectar y generar alarmas para varios tipos de ataques, de tal manera

	que se garantiza la funcionalidad del NIDS, haciendo la salvedad de que la garantía de efectividad de esta sistema de protección requiere de las actualizaciones periódicas del sistema, de actualización de firmas o reglas y en este sentido el componente o herramienta PulledPork es un aliado imprescindible para encargarse de la tarea de la actualización de las firmas o reglas.