PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCION DE INTRUSOS (IDS) EN LA DIRECCION GENERAL SEDE CENTRAL DEL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO INPEC “PIDSINPEC”

GILBERZON GARZON PADILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD
ESCUELA DE CIENCIAS BÀSICAS TECNOLOGIA E INGENIERIA- ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
TUNJA
2015

PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCION DE INTRUSOS (IDS) EN LA DIRECCION GENERAL SEDE CENTRAL DEL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO INPEC“PIDSINPEC”

GILBERZON GARZON PADILLA

Trabajo de grado

Director

Ing. Rafael Pérez Holguín

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÀSICAS TECNOLOGIA E INGENIERIA-ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
TUNJA
2015

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Tunja, 07 de Mayo de 2015

DEDICATORIA

Primero que todo a Dios por cumplir sus promesas y darme el conocimiento y la sabiduría para sacar adelante mis proyectos. A mi esposa Janeth Cuadrado, mis hijos Yilber Daniel y Kristen Maylen por su paciencia, comprensión y apoyo en los momentos que más he necesitado.

AGRADECIMIENTOS

Al Instituto Nacional Penitenciario y Carcelario INPEC quien me facilito los medios e información necesaria para implementar y lograr los objetivos del proyecto. Al Ingeniero Arturo Erazo tutor del anteproyecto, ya que con sus conocimientos y consejos se dio inicio al estudio del presente trabajo. Al Ingeniero Rafael Pérez Holguín Director del proyecto quien con su ayuda, compromiso y profesionalismo se materializo y culmino con éxito este proyecto y por último a la Universidad Nacional Abierta y a Distancia UNAD por la oportunidad que da a sus estudiantes para seguir especializándose en las diferentes ramas del saber.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

.

LISTA DE ANEXOS

pág.

GLOSARIO

ATAQUES POR FUERZA BRUTA: Se utiliza para acceder de forma ilegal a un sistema, probando una gran cantidad de combinaciones posibles del teclado o contraseñas.

BACKBONE: Son conexiones troncales de Internet. Se compone de un número de routers gubernamentales y comerciales entre otros. Llevan datos mediante fibra óptica a través de países y continentes.

BOTS: Programa informático que imita el comportamiento de un ser humano. Pueden ejecutar cualquier orden, mejorando las técnicas de infección actualizando las vulnerabilidades que utilizan para propagarse.

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

CGI-BIN: Trasmite información hacia un compilador instalado en el servidor. Una de sus funciones es la de incrementarla interacción con los documentos web que se presentan de forma estática por medio del HTML.

CIBERNÉTICOS: Estudia los conceptos interdisciplinarios de la estructura de los sistemas reguladores. Está relacionada a la teoría de sistemas y de control.

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

CÓDIGO MALICIOSO: Lenguaje de código informático que incita a infracciones de seguridad para romper un sistema.

DNS: Es una nomenclatura jerárquica para computadoras, o cualquier recurso que esté conectado a Internet o a una red privada.

FIREWALLS: Comprueba la información que sale de internet o red y bloque o restringe el paso al sistema de acuerdo su configuración.

FTP: (Protocolo de Transferencia de Archivos) se basa en la arquitectura cliente servidor y es un protocolo que se usa para la transferencia de archivos entre sistemas conectados a una red.

HTTP: (Protocolo de transferencia de hipertexto) es un método de intercambio de información en la red, se transfieren las páginas web a una computadora.

ICMP: (Protocolo de Mensajes de Control de Internet) Se utiliza para enviar mensajes de error, mostrando que un servicio determinado no está accesible o que un router o host no puede ser encontrado.

LOGS: Es un registro de actividad de un sistema, que se guarda en un fichero de texto, al que se le van aumentando líneas a medida que se efectúan acciones sobre el sistema.

NETBIOS: Es una interfaz para el acceso a los servicios de la red, enlaza un SO de red con un hardware en particular.

NFS: (Sistema de archivos de red*)*, en el Modelo OSI es un protocolo de nivel de aplicación. Se utiliza para sistemas de archivos distribuido en un ambiente de red de área local.

PHISHING: (Suplantación de identidad) es un abuso informático en el cual se comete usando un tipo de ingeniería social intentando adquirir información confidencial de manera fraudulenta.[1]

PROXY: Es un servidor que se utiliza para intermediar entre las peticiones de recursos que se realiza entre un cliente a otro servidor.

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

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

SAMBA: Es una implementación libre del protocolo de archivos compartidos de Microsoft Windows, configura los directorios GNU/Linux como recursos para compartir a través de la red.

SMTP: (Protocolo para la transferencia simple de correo electrónico), es un protocolo de red que se utiliza para intercambiar mensajes de correo

[1] PHISHING. [en línea]. <http:www.etapa.net.ec/Portals/0/Productos%20y%20Servicios/Phishing.pdf > [citado en 7 de Mayo de 2015]

electrónico. Su funcionamiento se da en línea y opera en los servicios de correo electrónico.

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

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

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

VNC: (Computación Virtual en Red) Conocido como software de escritorio remoto y es un programa de software libre que se basa en una estructura cliente-servidor, permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente.[2]

ZOMBIES DE SPAM: Ordenador conectado a Internet colocado por un hacker, y se puede utilizar para realizar tareas potencialmente dañinas bajo la dirección remota.

[2]TEMAS DE INFORMATICA. VNC [en línea]. <https://miblogidiomas.wordpress.com/author/almondita21> [citado en 7 de Mayo de 2015]

RESUMEN

La seguridad en la información por ser uno de los activos más importantes hoy en día es una prioridad de las empresas e instituciones. Es por esto que la relevancia que tiene la seguridad informática es fundamental para el logro de los objetivos de cualquier entidad y ha traído consigo el desarrollo de investigaciones con el propósito de crear mecanismos de seguridad tanto para la prevención como la detección de intrusos.

La realización de la presente investigación pretende estudiar y conocer la estructura y aplicación de los sistemas de detección de intrusos (IDS), y de acuerdo a un análisis sobre los IDS que se encuentran disponibles comercialmente, hacer una propuesta denominada "PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCION DE INTRUSOS (IDS) EN LA DIRECCION GENERAL SEDE CENTRAL DEL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO INPEC (PIDSINPEC), a una entidad en particular y en nuestro caso la Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC, en donde al igual que muchas entidades están haciendo uso de las tecnologías de punta y esto ha traído consigo un incremento mayor del número de ataques e intrusiones en los sistemas informáticos.

La propuesta incluye el sugerir la implementación y el uso de uno de los principales exponentes dentro de las herramientas de detección de intrusos (IDS) como lo es Snort, siendo este IDS un software muy flexible ya que es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos y actualizaciones constantes además está disponible bajo licencia GPL.

Palabras Clave: SISTEMAS DE DETECCIÓN DE INTRUSOS, SNORT, ATAQUES INFORMÁTICOS, SEGURIDAD INFORMÁTICA.

ABSTRAC

The information security as one of the most important assets today is a priority for companies and institutions. That is why the relevance of computer security is essential for achieving the objectives of any entity and has brought the development of research in order to create security mechanisms for both prevention and intrusion detection.

The embodiment of the present research aims to study and understand the structure and implementation of intrusion detection systems (IDS), and according to an analysis of the IDS that are commercially available, make a proposal entitled "PROPOSAL FOR THE IMPLEMENTATION OF AINTRUSION DETECTION SYSTEM (IDS) IN GENERAL HEADQUARTERS OF THE NATIONAL PENITENTIARY AND PRISON INSTITUTE INPEC (PIDSINPEC) to a particular entity and in our case the Headquarters of the National Penitentiary and Prison Institute INPEC, where as many organizations are making use of advanced technologies and this has led to a greater increase in the number of attacks and intrusions in computer systems.

The proposal includes suggest the implementation and use of one of the leading exponents within the Tools intrusion detection (IDS) as it is Snort and this IDS a very flexible software because it is one of the most used and available a large number of predefined filters or patterns and constant updates is also available under the GPL.

Keywords: INTRUSION DETECTION SYSTEMS, SNORT, ATTACK COMPUTER, COMPUTER SECURITY.

1 INTRODUCCION

Actualmente con el avance de la tecnología y las telecomunicaciones, la seguridad informática se ha convertido en una pieza fundamental en el entramado empresarial, industrial y administrativo de las organizaciones quienes a diario corren el riesgo de verse vulneradas en la confidencialidad y disponibilidad de su información.

La seguridad en la información no es solo guardar los archivos en sitios estratégicos, sino mirar cómo está conformado su entorno, como está conformada su estructura, observar que posibles vulnerabilidades hay, como mitigar los riesgos, verificar si los equipos electrónicos que utilizamos realmente son seguros o si hay que realizar ajustes, algo muy indispensable es analizar y verificar qué tan resistentes son a los ataques informáticos y si la información que almacenamos va a estar segura o si va hacer volátil.

Se hará una exposición de los diferentes Sistemas de Detección de Intrusos (En adelante: IDS) que actualmente existen en el mercado, pretendiendo estudiar, analizar y razonar sobre los mismos y de acuerdo a esta disertación lograr determinar cuál de los IDS, que cumpla con los requerimientos y exigencias que necesita la Sede Central del Instituto Nacional Penitenciario y Carcelario (En adelante: INPEC) puede llegar a ser el más apropiado para implantarlo.

Es por esto que se presenta el proyecto denominado “PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCION DE INTRUSOS (IDS) EN LA DIRECCION GENERAL SEDE CENTRAL DEL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO INPEC (En adelante: PIDSINPEC), y en dicha propuesta se dará una idea de una implementación de un software, uno de los mecanismos de defensa más usados en el mercado para reducir el riesgo de ataques dirigidos hacia los bienes informáticos, así como su instalación, configuración y demás requerimientos y aplicaciones.

Además este proyecto se hace como requisito para acceder al título de Especialista en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD.

Se espera que con la propuesta presentada se pueda cumplir con los principios que tiene la seguridad informática que es mantener la confidencialidad, integridad y disponibilidad de la información.

2 FORMULACIÓN DEL PROBLEMA

La cantidad de accesos no autorizados a la información que existe en Internet, ha crecido durante los últimos años de una manera significativa, comprometiendo la estabilidad económica, social tanto a nivel empresarial como a nivel doméstico.

En Colombia, las instituciones de seguridad se están vinculando a la Estrategia TI para aumentar la capacidad del Estado de enfrentar las amenazas informáticas, pues en el momento presenta grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar sus efectos. Según estudios en 2011 en Colombia hubo más de 550 ataques exitosos a entidades del Estado, para 2013 los ataques aumentaron en 130[3].

Entre las instituciones o entidades del estado que menciona el estudio no puede quedar por fuera una de las más importantes, el INPEC en donde al igual que muchas por no decir todas las entidades del estado están haciendo uso de las tecnologías de punta y esto ha traído consigo un incremento mayor del número de ataques e intrusiones en los sistemas informáticos.

Para el INPEC la seguridad es algo primordial en el correcto funcionamiento de sus redes de datos, pues con ella se garantiza la confidencialidad, integridad y disponibilidad de la información. Una violación a su seguridad puede ocasionar severos daños a la integridad de sus redes de datos, las cuales son de vital importancia en la organización y pueden llegar a afectar datos relevantes para los usuarios que hagan uso de los diferentes sistemas de información.

El INPEC es la entidad que tiene a cargo la custodia y vigilancia del personal recluso del país y maneja tanto física como documental este tipo de perfil de usuarios (internos), y por esto no es ajena a cualquier tipo de ataques e intrusiones por parte de agentes internos y externos.

En Colombia y sus organismos estatales es muy preocupante la vulnerabilidad en cuanto a ciberseguridad se refiere, más aun cuando en estas instituciones se concentra la mayoría de los controles de los sistemas de información del país.

El INPEC está expuesto como la gran mayoría de las entidades gubernamentales y privadas a actividades maliciosas y ataques cibernéticos como son: amenazas, phishing, código malicioso, zombies de spam, computadoras infectadas por bots, orígenes de ataques a redes, etc.

[3]MINTIC. Seguridad TI. [en línea]. < http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html >[citado en 6 de junio de 2014]

La sofisticación del uso y estrategia de Tecnología de Información conlleva al INPEC a la necesidad y obligación de mejorar las herramientas de seguridad ya que la información que el INPEC maneja la realiza por medio de una red de informática que permite la consulta y actualización de los datos de los sindicados y condenados en los 138 establecimientos de reclusión del orden nacional, con la visión de enlazar y compartir información con diferentes entidades del gobierno.

Los ataques cibernéticos a que está expuesto el INPEC pueden ser de diferentes tipos:

- **Externo**

En la cual los ataques son realizados desde una ubicación en Internet en cualquier parte del mundo.

- **Interno**

En este caso el ataque es realizado directamente en las oficinas del INPEC, generado internamente en la organización.

Las posibles vulnerabilidades a las que están expuestos los sistemas son:

- Usuarios y contraseñas propias del sistema operativo.
- Permisos débilmente establecidos sobre archivos de sistema e incluso llaves de registro.
- Recursos compartidos.
- Revelación de información a través de protocolos inseguros (RCP, NetBIOS Shares).
- El robo de cuentas de usuarios (login y password) del sistema estudiado utilizando herramientas automáticas. (Passwords por defecto, ataques por fuerza bruta, diccionarios de passwords, etc).

A nivel de configuración de red los siguientes aspectos:

- ✓ Listado de servicios y puertos de red
- ✓ Aplicaciones inseguras
- ✓ Stack TCP/IP
- ✓ Vulnerabilidades sobre los servicios principales (Web, DNS, FTP, SMTP, SNMP)
- ✓ Accesos vulnerables (Telnet, Terminal Services, XWindows, VNC, NFS, cgi-bin, Samba).

El INPEC actualmente tiene implementado una serie de medidas técnicas que se han instalado en todos los medios para evitar la pérdida, mal uso, alteración, acceso no autorizado o robo de los datos. Una de estas medidas son los

firewalls que permiten de forma segura que los usuarios externos se puedan comunicar con la intranet del Instituto.

Estos firewall con una política correcta pueden minimizar el que numerosas redes queden expuestas y esto ha aliviado un poco el problema de inseguridad en la información, también se han implementado routers, proxy y antivirus, sin embargo los atacantes están evolucionando y aparecen nuevas técnicas como los troyanos, gusanos y escaneos silenciosos que atraviesan los firewall mediante protocolos autorizados como HTTP, ICMP o DNS. Los piratas informáticos están en la búsqueda de agujeros en los sistemas que se presentan en el firewall, realizando los ataques a los protocolos que éstos poseen enmascarándolos y logrando que la red quede expuesta.

Se plantea entonces la necesidad de realizar un estudio de las ventajas y alcances que tiene un IDS así como su aceptación con respecto a la infraestructura de la seguridad del Instituto y al realizar dicho estudio pasamos al siguiente planteamiento de cómo podemos implementarlo.

Con lo expuesto anteriormente se podrá responder al cuestionamiento. ¿Un IDS es realmente una estrategia de seguridad que garantice la protección del sistema, de las amenazas a las que se ve expuesta la información en la Dirección General Sede Central del INPEC?

3 JUSTIFICACIÓN

Debido al aumento del número de ataques informáticos que se producen en internet, así mismo el avance de la tecnología, y a que en la Sede Central del INPEC no se cuenta actualmente con un mecanismo de defensa ante los intentos de intrusión desde el interior o exterior de la red, se hace necesario realizar el presente proyecto denominado “PIDSINPEC”.

El sistema de información que maneja la Sede Central del INPEC necesita estar disponible todo el tiempo, debido a que el sistema es usado por los empleados de la Institución, lo que significa que una falla en el sistema debe ser subsanada de manera inmediata a fin de seguir con la continuidad y prestación del servicio.

La PIDSINPEC se hace necesario realizarlo, ya que con el desarrollo del mismo se propone utilizar los mecanismos necesarios que justifiquen su validez y ejecución, beneficiando el manejo de la información en cuanto a seguridad e integridad de la información y así dar pautas o recomendaciones para implementar un IDS en la Sede Central del INPEC, desarrollando una herramienta de detección de intrusos para la red, que permita proteger los activos reales de la información digitalizada.

El estudio que se pretende realizar es viable porque lo que se proyecta es dar una visión clara y precisa del porqué y cómo implementar un IDS en la sede central del INPEC, tomando como referencia estudios previos hechos en otras organizaciones, además se realizó una encuesta aplicada a los funcionarios que laboran en el área de sistemas, con lo que se demuestra la falta de información con respecto a la seguridad de la red y el funcionamiento de un IDS y con estos análisis se tomara como base para realizar esta disertación.

Esta investigación se realiza con la singularidad de proyecto factible, en donde se elabora una propuesta sustentada en una guía viable para satisfacer las necesidades de la Institución.

El impacto que genera el proyecto PIDSINPEC es relevante ya que el tema abordado implica un beneficio para la organización y se puede extender a las demás regionales que forman el INPEC y demás organizaciones que quieren mejorar la seguridad en sus comunicaciones.

Así mismo este proyecto PIDSINPEC es realizado con el fin de integrar y aplicar los conocimientos y competencias desarrolladas en el transcurso de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD y como requisito para acceder al título de Especialista en Seguridad Informática.

4 DELIMITACION DE LA PIDSINPEC

El INPEC cuenta con una red LAN a nivel nacional que es controlada a través de un servidor en la Dirección General o Sede Central, Direcciones Regionales y en los 138 establecimientos de reclusión a nivel nacional, facilitando la transferencia de información entre ellos y la Sede Central.

Los establecimientos de reclusión están dirigidos por las Direcciones Regionales y todos estos a su vez por la Dirección General o Sede Central ubicada en la Calle 26 No 27-48 en la ciudad de Bogotá y cuyo fin es optimizar la supervisión, verificación y control del cumplimiento de las políticas institucionales.

En la Sede Central se encuentra una base de datos centralizada, los servidores de datos, servidores de aplicaciones y estaciones cliente, accediendo a estos por medio de la red interna intranet únicamente con el nombre de usuario y contraseña y donde se administran y enlazan los establecimientos y regionales a nivel nacional, alimentando la base de datos y unificando de forma integral la información, para el control total de la población de internos.

Por las razones anteriormente expuestas la propuesta para la implementación de un IDS se realizara en la Dirección General o Sede Central, a raíz de unas pruebas a la red que se realizaran para verificar el estado de la misma y sus posibles vulnerabilidades, reconociendo las fallas de seguridad, para poder dar un veredicto sobre el IDS a implementar.

De la misma manera que es allí donde está la base de datos y las aplicaciones, soportadas con sistemas computacionales de punta, compatibles con el sector justicia y los estándares internacionales para el manejo de datos estadísticos y es la encargada de consolidar la totalidad de la información personal, familiar y jurídica inherente a cada interno ubicado en los establecimientos de reclusión del orden nacional, detención o prisión domiciliaria, control y vigilancia electrónica a cargo del INPEC, desde el momento en que ingresa al sistema penitenciario hasta que recupera su libertad.

.

5 OBJETIVO GENERAL PIDSINPEC

Realizar una PIDSINPEC, a través de un análisis realizado a la red de comunicaciones de la Sede Central del INPEC y de una indagación sobre los IDS y sus características, teniendo como finalidad un sistema integral más eficiente monitorizando los eventos que ocurren en el sistema o en la red, para analizarlos en busca de violaciones de políticas de seguridad.

5.1 OBJETIVOS ESPECIFICOS

Conocer que es un IDS, estudiar su historia, sus características, arquitectura y clasificación.

Reconocer las fallas de seguridad que actualmente tiene la red de comunicaciones de la Dirección General Sede Central del INPEC para así mismo determinar la ubicación del IDS en la red.

Estudiar los productos de uso comercial relacionados con los IDS y así poder determinar cuál de los productos estudiados se puede llegar a implementar en la red de la Sede Central del INPEC.

Exponer los beneficios de implantar un IDS en la red de la Sede Central del INPEC.

Dejar los conceptos claros y precisos al culminar el presente proyecto, para así poder ejecutar la implementación futura de un IDS en la Dirección General Sede Central del INPEC.

6 MARCO REFERENCIAL

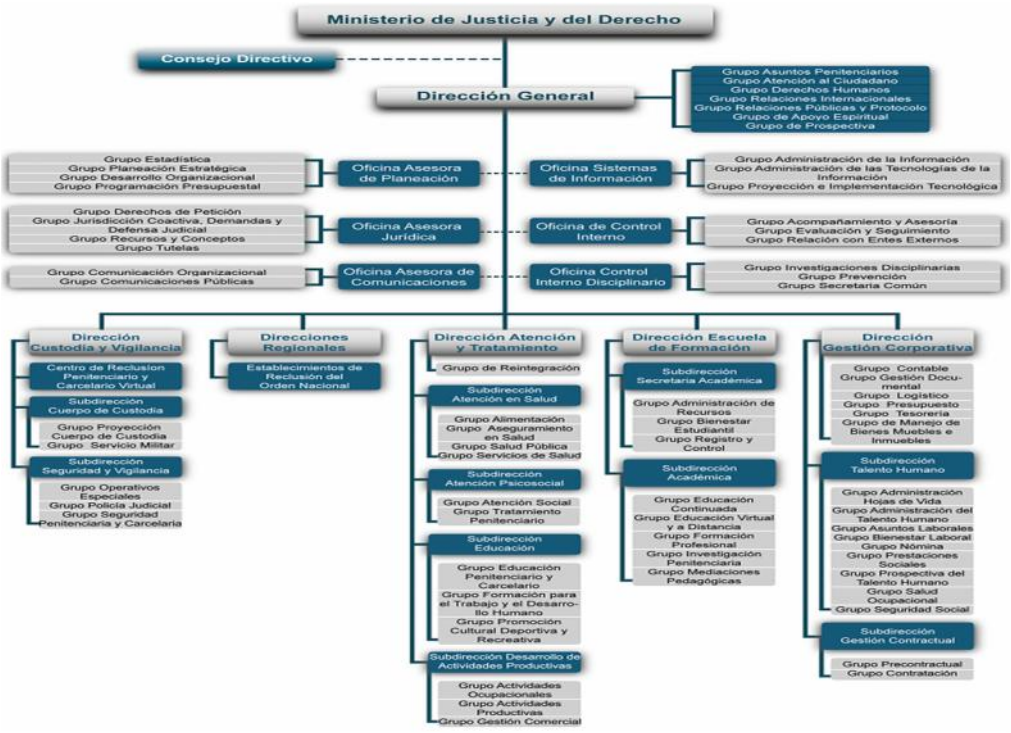
6.1 MARCO CONTEXTUAL

El INPEC es una institución del estado responsable de la ejecución de la pena y las medidas de seguridad de la totalidad de la población reclusa. Cuenta con 138 establecimientos de reclusión en las 06 regionales distribuidas a nivel nacional[4].

Además de manejar y administrar los centros de reclusión también es la encargada de la información tanto a nivel de personal adscrito a ésta, como de la población reclusa.

6.1.1 Organigrama

Figura 1: Organigrama del INPEC



Recuperado de
http://www.inpec.gov.co/portal/page/portal/Inpec/Institucion/Organizacion

[4]INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO. Organización. [en línea]. <http://www.inpec.gov.co/portal/page/portal/Inpec/Institucion/Organizacion/LOcalizacion> [citado en 06 de Junio de 2014]

6.1.2 Misión

Contribuir al desarrollo y resignificación de las potencialidades de las personas privadas de la libertad, a través de los servicios de tratamiento penitenciario, atención básica y seguridad, fundamentados en el respeto de los derechos humanos[5].

6.1.3 Visión

El INPEC será reconocido por su contribución a la justicia, mediante la prestación de los servicios de seguridad penitenciaria y carcelaria, atención básica, resocialización y rehabilitación de la población reclusa, soportado en una gestión efectiva, innovadora y transparente e integrada por un talento humano competente y comprometido con el país y la sociedad[6].

6.2 MARCO HISTÓRICO

La seguridad en los sistemas de información es un tema que ha sido objeto de estudio desde hace muchos años atrás, se podría decir que desde el momento que se implementan los sistemas informáticos en los diferentes entornos en el que se desarrolla el ser humano. Lo que hoy conocemos como el internet fue creado por el gobierno estadounidense para el desarrollo y defensa en el año de 1969 con el nombre de ARPAnet y su entorno en cuanto a seguridad era muy mínimo ya que la mayoría de datos que se intercambiaban no eran confidenciales y los usuarios muchos de ellos se conocían. Ahora por el contrario las redes globales requieren un mayor nivel de seguridad, manejando volúmenes grandes de información, intercambiando datos privados de forma independiente en varios países, siendo imprescindible cada vez más la seguridad[7].

El proceso de generar, revisar y almacenar los eventos de un sistema en orden cronológico, a esto se llama auditoria, y eran conocidas como sistemas de auditorías básico y su intención era medir el tiempo que dedicaban los operadores a utilizar los sistemas que monitorizaban, con una precisión casi exacta, y eran maquinas escasas y muy caras y su uso estaba restringido a técnicos e ingenieros especializados.

Monitor de referencias fue el concepto dado por James P. Anderson ya que fue el primero en documentar la necesidad de un mecanismo que automatizara la revisión de los eventos de seguridad, este estudio fue encargado por las

[5]INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO. Organización. [en línea]. <http://www.inpec.gov.co/portal/page/portal/Inpec/Institucion/FormulacionEstrategica> [citado en 06 de Junio de 2014]

[6]INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO. Organización. [en línea]. <http://www.inpec.gov.co/portal/page/portal/Inpec/Institucion/FormulacionEstrategica> [citado en 06 de Junio de 2014]

[7]DIEGO GONZALEZ GOMEZ. Sistemas de Detección de Intrusiones. Barcelona. 2003. P. 17-18

Fuerzas Aéreas de EEUU y en al año de 1980 se redactó un informe que sería el primero sobre los futuros trabajos sobre detección de intrusiones[8].

El primer sistema de intrusiones en tiempo real fue desarrollado entre 1984 y 1986 por Dorothy Denning y Peter Neumann, este proyecto proponía una correspondencia entre una actividad anómala y abuso o uso indebido.

En los años 80 aparecieron numerosos sistemas de detección de intrusiones, un grupo de desarrollo en Syteck dirigió un proyecto denominado "AutomatedAuditAnalysis" este proyecto recogía información a nivel de interfaz de comandos "shell" de un sistema UNIX para después compararlos con una base de datos y estos se analizaban estadísticamente para comprobar que se podían detectar comportamientos fuera de lo normal.

Multics Intrusion Detection and Alerting System (MIDAS, hecho por el National Computer Security Center (NCSC), utilizando un sistema hibrido, combinando la estadística de anomalías como reglas de seguridad de un sistema experto.

Se convirtió en el primer IDS conectado a internet y ayudó a mejorar la seguridad contra ataques externos a fortalecer los mecanismos de autenticación de usuarios y a seguir bloqueando intrusiones internas, publicado en la red en 1989.

En los años ochenta el Network Audit Director and Intrusion Reporter (NADIR) fue uno de los sistemas más exitosos, compuesta por unos 9.000 usuarios, usando técnicas de detección similares a los sistemas de su tiempo como el IDES o MIDAS, siendo su principal responsable Kathleen Jackson.

El primer sistema de detección de intrusiones que monitorizaba el tráfico en la red fue el Network System Monitor (NSM), trabajando en una estación UNIX de Sun, desarrollado en la Universidad de California[9].

A raíz del famoso gusano de internet en 1988 se unieron esfuerzos académicos y comerciales como el Centro de soporte Criptológico de las fuerzas aéreas de los EEUU, el laboratorio nacional de Lawrence Livermore, la Universidad de California y los laboratorios Haystackpara dar soluciones en seguridad dando fusión a los sistemas de detección basados en máquina y red originando el Distributed Intrusion Detection System (DIDS)[10].

[8] JORGE MAESTRE VIDAL. Sistema de Detección de Anomalías de red basado en el procesamiento de Payload. Madrid. 2012. Trabajo de grado [Ingeniero de software].Universidad Complutense Madrid. Facultad de Informática.

[9]MARIA ISABEL JIMENEZ GARCIA. Utilización de Sistemas de Detección de Intrusos como elemento de seguridad perimetral. Trabajo de grado [Ingeniero en Informática]. Universidad de Almería. Facultad de Informática.

[10]DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype.[en línea]. <http://seclab.cs.ucdavis.edu/papers/DIDS.ncsc91.pdf> [citado en 06 de Junio de 2014]

Este fue el primer sistema que logro monitorizar las violaciones e intrusiones de seguridad a través de las redes y el principal objetivo era facilitar canales que permitieran agrupar el control y publicación de resultados en un controlador central.

Alrededor del año 1990 aparecieron los primeros programas de detección de intrusiones de uso comercial como: Computer Watch, desarrollado por la empresa AT&T, el Information Security Officer´s Assistant (ISOA) de PRC y el Clyde VAX Audit por Clyde Digital.

Entre los años 1994 y 1996 se desarrolló el Sistema de Detección de Intrusos Adaptativo (AID), en la Universidad de Tecnología de Brandenburgo. Fue planteado para auditar las redes fundamentadas en la monitorización de los hosts presentes en una LAN y está siendo utilizado para la investigación de auditorías de privacidad.

6.3 MARCO CONCEPTUAL

Observando los análisis y estadísticas que se han realizado sobre las vulnerabilidades y los posibles ataques a los sistemas de información, se han venido realizando en los últimos años, programas para detectar las posibles debilidades tanto a los sistemas operativos como a los servicios de red.

Estos programas verifican las políticas de seguridad en búsqueda de agujeros y escanean las redes y problemas de seguridad encontrados presentes en los diferentes dispositivos que se conectan a la red.

Las vulnerabilidades afectan a sistemas que son tradicionalmente seguros, lo mismo que a los sistemas de seguridad como firewall.

6.3.1 ¿Qué es un Sistema de Detección de Intrusos? Un IDS (Intrusion Detection System) es una herramienta de seguridad, que se encarga de monitorizar los sucesos que resultan en un sistema informático en busca de intentos de intrusión.

Los IDS están compuestos por tres elementos fundamentales: Una fuente de información que proporciona eventos del sistema, un motor de análisis que busca evidencias de intrusiones y un mecanismo de respuesta que actúa según los resultados del motor de análisis[11].

6.3.1.1 Funciones de un IDS. Los IDS trabajan con otras herramientas como son los firewalls, que implantan métodos de trabajo.

[11]EMILIO JOSE MIRA ALFARO. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Trabajo de grado. [Ingeniero Informático]. Universidad de Valencia. Ingeniería Informática.

Las funciones de un IDS son:

- En el momento que el ataque está sucediendo o después, los IDS detectan esta intrusión.

- Automatización de la búsqueda de nuevos patrones de ataque, gracias a herramientas estadísticas de búsqueda y al análisis de tráfico anómalo.

- Monitorización y análisis de las actividades de los usuarios. De este modo se pueden conocer los servicios que usan los usuarios y estudiar el contenido del tráfico, en busca de elementos anómalos.

- Auditoría de configuraciones y vulnerabilidades de determinados sistemas.

- Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.

- Analiza el comportamiento que no es usual. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs pueden revelar una máquina comprometida o un usuario con su contraseña al descubierto[12].

- Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos y otros.

Los IDS comparten la información de otros sistemas como lo son firewalls, routers y switches configurando características de la red con los eventos que se generan. Así mismo permiten que se utilicen protocolos SNMP enviando notificaciones y alertas a otras máquinas de la red, recibiendo el nombre de interoperabilidad.[13]

La correlación es otra característica de los IDS, consistiendo en la capacidad de establecer relaciones lógicas entre eventos diferentes e independientes, permitiendo manejar eventos de seguridad complejos que pueden representar un riesgo alto en la seguridad del sistema.

Para ser evaluada la utilidad de un sistema de detección de intrusos se debe tener en cuenta cuando en términos de probabilidad se analice, que el sistema

[12] MARIA ISABEL JIMENEZ GARCIA. Utilización de Sistemas de Detección de Intrusos como elemento de seguridad perimetral. Trabajo de grado [Ingeniero en Informática]. Universidad de Almería. Facultad de Informática.

[13] Seguridad Perimetral. < https://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf> [citado en 06 de Junio de 2014]

detecta un ataque y la de pronunciar falsas alarmas. Se debe analizar y tener muy presente el número inmenso de alertas generados y las falsas alarmas que se producen, haciendo esto una tarea dispendiosa para los administradores del sistema, requiriendo una constante supervisión.

6.3.1.2 Arquitectura de un IDS. Cuando se realiza una auditoria los logs o registros que son analizados deben quedar de forma segura guardados en una parte diferente a la del sistema, para evitar que esta información sea eliminada o se altere sin perjudicar el mecanismo IDS.

Los IDS se reconocen en dos grupos según el tipo de analizador o procesador de eventos que configuran el IDS: los que trabajan basados en normas, los que trabajan en la detección de uso indebido y los sistemas que se adaptan utilizando técnicas estadísticas trabajando en la detección de anomalías**.**

6.3.2 Clasificación de los IDSs

6.3.2.1 IDSs basados en red (NIDS). Existen varias fuentes de las que un IDS puede recoger eventos. Algunos IDSs analizan paquetes de red, capturados del backbone de la red o de segmentos LAN, mientras que otros IDSs analizan eventos generados por los sistemas operativos o software de aplicación en busca de señales de intrusión.[14]

La red es la base fundamental de los IDS. Los IDS detectan los ataques a los paquetes de la red, escuchando y analizando un segmento de ésta. Un NIDS logra monitorizar y proteger a los hosts que están conectados a un segmento de red.

Su complemento principal son los sensores, que están ubicados en diferentes localizaciones de la red, analizando el tráfico local e informando a la consola de gestión sobre los ataques que se producen.

Como los sensores están limitados a ejecutar el software de detección, pueden ser más fácilmente asegurados ante ataques. Muchos de estos sensores son diseñados para correr en modo oculto, de tal forma que sea más difícil para un atacante determinar su presencia y localización[15].

6.3.2.2 IDSs basados en host (HIDS). Los HIDS (NetworkIDS) fueron el primer tipo de IDSs desarrollados e implementados, operan sobre la información recogida desde dentro de una computadora, como pueden ser los

[14] MARIA ISABEL JIMENEZ GARCIA. Utilización de sistemas de Detección de intrusos como elemento de seguridad perimetral. Trabajo de grado. [Ingeniero en Informática]. Universidad de Almería. Ingeniería Informática.

[15]EMILIO JOSE MIRA ALFARO. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Trabajo de grado. [Ingeniero Informático]. Universidad de Valencia. Ingeniería Informática

ficheros de auditoría del sistema operativo. Esto permite que el IDS analice las actividades que se producen con una gran precisión, determinando exactamente qué procesos y usuarios están involucrados en un ataque particular dentro del sistema operativo.[16]

A diferencia de los NIDSs, los HIDSs puede ver el resultado de un intento de ataque, al igual que pueden acceder directamente y monitorizar los ficheros de datos y procesos del sistema atacado[17].

- **Tipo de análisis.** Existen dos tipos de análisis de eventos para la detección de ataques: detección de abusos y detección de anomalías.

  La detección de abusos la utilizan los sistemas comerciales y es la más usada por éstos.

  La detección de anomalías la utiliza un número reducido de IDSs de forma limitada, en busca de patrones que no son normales.

- **Detección de abusos o firmas.** De acuerdo a un esquema predefino o un ataque conocido, este sistema busca eventos que se ajusten a estos patrones.

Ventajas:

Evitar un número elevado de falsas alarmas, por la acción efectiva de los detectores de ataques.

Diagnosticar rápidamente y de manera exacta el uso de herramientas o una técnica de ataque en particular.

Permitir a los administradores de seguridad con o sin experiencia en esta materia, realizar seguimientos a los problemas de seguridad de sus sistemas.

Desventajas:

Siempre tienen que estar actualizados las firmas de los últimos ataques ya que únicamente detecta aquellos que conoce.

- **Detección de anomalías.** Crean perfiles que incorporan el comportamiento de los usuarios normalmente, basándose en medidas estadísticas

[16] EMILIO JOSE MIRA ALFARO. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Trabajo de grado. [Ingeniero Informático]. Universidad de Valencia. Ingeniería Informática

[17] Administración de Sistemas Operativos. IDS basados en hots (HIDS) [en línea]. < http://www.adminso.es/index.php/4.2.5._IDS_basados_en_host_%28HIDS%29> [citado en 06 de Junio de 2014]

parametrizadas y apoyándose en un periodo normal de operación observando por un determinado tiempo los datos históricos.

Ventajas:

Los IDSs basados en detección de anomalías detectan comportamientos inusuales. De esta forma tienen la capacidad de detectar ataques para los cuales no tienen un conocimiento específico. Los detectores de anomalías pueden producir información que puede ser utilizada para definir firmas en la detección de abusos.[18]

Desventajas:

Provoca un número significativo de falsas alarmas, por los comportamientos inusuales de usuarios y redes.

- **Respuesta.** El IDS reacciona ejecutando un evento cuando se realice un ataque y se agrupa en dos tipos como son: respuestas activas y respuestas pasivas.

- **Respuestas pasivas.** En este tipo de respuestas se notifica al responsable de seguridad de la organización, al usuario del sistema atacado o a algún CERT de lo sucedido. También es posible avisar al administrador del sitio desde el cual se produjo el ataque avisándole de lo ocurrido, pero es posible que el atacante monitorice el correo electrónico de esa organización o que haya usado una IP falsa para su ataque.[19]

- **Respuestas activas**. Son tareas automáticas que se ejecutan cuando se detectan cierto tipo de intrusiones.

  Se pueden establecer dos categorías distintas:

- **Recogida de información adicional:** Consiste en incrementar el nivel de sensibilidad de los sensores para obtener más pistas del posible ataque (por ejemplo, capturando todos los paquetes que vienen de la fuente que originó el ataque durante un cierto tiempo o para un máximo número de paquetes).[20]

[18] EMILIO JOSE MIRA ALFARO. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Trabajo de grado. [Ingeniero Informático]. Universidad de Valencia. Ingeniería Informática

[19] EMILIO JOSE MIRA ALFARO. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Trabajo de grado. [Ingeniero Informático]. Universidad de Valencia. Ingeniería Informática

[20] VANESSA VIÑES SANJUAN. Análisis de sistemas de detección de intrusiones. Ingeniería Técnica en Informática de Sistemas. Trabajo de grado. Universitat Rovira I Virgili

- **Cambio del entorno**: Otra respuesta activa puede ser la de parar el ataque; por ejemplo, en el caso de una conexión TCP se puede cerrar la sesión establecida inyectando segmentos TCP RST al atacante y a la víctima o filtrar en el router de acceso o en el firewall la dirección IP del intruso o el puerto atacado para evitar futuros ataques[21].

6.4 Productos comerciales

6.4.1 Dragon - Enterasys Networks. El IDS de Enterasys Networks, Dragon, toma información sobre las actividades sospechosas de un sensor llamado Dragon Sensor y de un módulo identificado como DragonSquire que es el encargado de monitorizar los logs de los firewalls y otros sistemas. Esta información es enviada a un producto llamado Dragon Server para futuros análisis y correlaciones. Cada componente tiene algunas ventajas que compensan con debilidades de otro, un ejemplo seria que el sensor Dragon Sensor es incapaz de interpretar tráfico codificado de una sesión web SSL, pero el producto DragonSquire es capaz de recocer los logs del servidor web y pasárselos a la máquina de análisis[22].

6.4.2 NetRanger - Cisco Systems. El sistema de detección de intrusos de Cisco, conocido formalmente por Cisco NetRanger, es una solución para detectar, prevenir y reaccionar contra actividades no autorizadas a través de la red.

Cisco IDS Host Sensor v2.0 es capaz de identificar ataques y prevenir accesos a recursos críticos del servidor antes de que ocurra cualquier transacción no autorizada. Esto lo hace integrando sus capacidades de respuesta con el resto de sus equipos, como veremos más adelante.

La versión más reciente actualmente del sensor de cisco es la v3.0, que incluye un mecanismo de actualización automática de firmas, un lenguaje robusto que permite a los clientes escribir sus propias firmas y extensiones al módulo de respuestas que añaden soporte para la familia de firewalls Cisco PIX y para los conmutadores Cisco Catalyst[23]

[21]EMILIO JOSE MIRA ALFARO. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Trabajo de grado. [Ingeniero Informático]. Universidad de Valencia. Ingeniería Informática.

[22] Intrusion Prevention System.
[en línea]. < http://www.extremenetworks.com/product/extreme-intrusion-prevention-system> [citado en 06 de Junio de 2014]

[23]ARMANDO BECERRA RODRIGUEZ. Sistemas Detección de Intrusos. Trabajo de grado. [Ingeniero Informático]. Universidad Francisco de Paula Santander. Facultad de Ingeniería

Sensor y Director son los dos componentes principales de Cisco Secure y gracias a la alta velocidad de sus herramientas de red los cuales establecen y autorizan el tráfico de los paquetes de forma individual.

El sensor de Cisco se presenta en tres formatos distintos dependiendo de las necesidades de la organización:

6.4.3 Módulo IDS Catalyst R 6000. Es el primero diseñado para integrar la funcionalidad IDS directamente dentro del conmutador permitiendo al usuario monitorizar tráfico directamente del backplane del conmutador en lugar de utilizar módulos software. Monitoriza 100 Mbps de tráfico y aproximadamente 47.000 paquetes por segundo.[24]

6.4.3.1 IDS- 4250. Soporta hasta 500 Mb/s sin paralelizar, monitoriza tráfico en una red Gigabit y para tráfico atravesando conmutadores usados para agregar tráfico entre numerosas subredes[25].

6.4.3.2 IDS-4210. Monitoriza entornos de 45 Mb/s aunque también es adecuado para múltiples T1/El, T3 y entornos Ethernet.

6.4.4 Internet Security Systems. Almacena en una BD los eventos que se derivan de la detección, prevención y respuesta, desde cualquier punto de la red.

De acuerdo a las necesidades de la red el sensor se acopla de forma casi inmediata, adaptando las alertas y firman que especifican los usuarios además la sintonización de firmas de ataque. Con la aplicación X-PressUpdate automáticamente las firmas se actualizan.

6.4.5 Symantec. Symantec adquirió Axent y así obtuvo las tecnologías NetProwler y su Intruder Alert.

Entre la gama de productos de Symantec [SYM04], están los modelos de seguridad de Gateway 320, 360 y 360R que no son vulnerables a los ataques de Denegación de Servicios, aunque sí lo son a ataques como servicios activos de identificación en la interfaz WAN, la exploración de los servicios y a la alteración del firewall.[26]

[24] CARLOS JIMENEZ GALINDO. Diseño y Optimización de un sistema de Detección de Intrusos Hibrido. [Ingeniero Informático].Universidad de Almeira
[25] ARMANDO BECERRA RODRIGUEZ. Sistema Detección de Intrusos. Universidad Francisco de Paula Santander
[26] CARLOS JIMENEZ GALINDO. Diseño y Optimización de un sistema de Detección de Intrusos Hibrido. [Ingeniero Informático].Universidad de Almeira

6.4.6 Enterasys. Es una compañía que elabora para los usuarios medidas de seguridad y aplicaciones para el hardware de red orientado a los servicios.

Un ejemplo de producto desarrollado por Enterasys es Secure Gigabit Ethernet Workgroup L2 Switch con Soporte de Políticas Opcional, llamado Enterasys D2.

Enterasys D2 proporciona 12 puertos Gigabit Ethernet (GbE) con conectividad de10/100/1000 Mbps RJ45 con opciones integradas Power sobre Ethernet (PoE) y soporte para potencia redundante[27].

6.4.7 Shadow. Fue desarrollado como respuesta a los falsos positivos de un IDS anterior, NID. La idea era construir una interfaz rápida que funcionara bien en una DMZ caliente (una DMZ que sufre muchos ataques). La interfaz permitiría al analista evaluar gran cantidad de información de red y decidir de qué eventos informar.

No es en tiempo real. Los diseñadores de Shadow sabían que no iban a estar disponibles para vigilar el sistema de detección de intrusos 7 días a la semana, 24 horas al día. Shadow almacena el tráfico de red en una base de datos y se ejecuta por la noche[28].

6.4.8 Ax3soft Sax2. Es un software utilizado para la detección y prevención de intrusiones profesional (IDS) y sobresale en la captura en tiempo real de paquetes, 24/7 es fácil de aislar, detecta vulnerabilidades a la red, identifica amenazas, además ofrece diferentes tipos de informes de análisis de intrusión.

6.4.9 Snort. Creado por Martin Roesch y bajo licencia GPL, se puede ejecutar en UNIX y Windows. Es el primero en IDS y cuanta con 1600 reglas para el análisis de las alertas.

Era flexible y muy pequeño, fue elaborado como prototipo, cumpliendo las exigencias de un IDS y con el tiempo creció y adopto funciones que tenían solo los IDS de marcas comerciales.

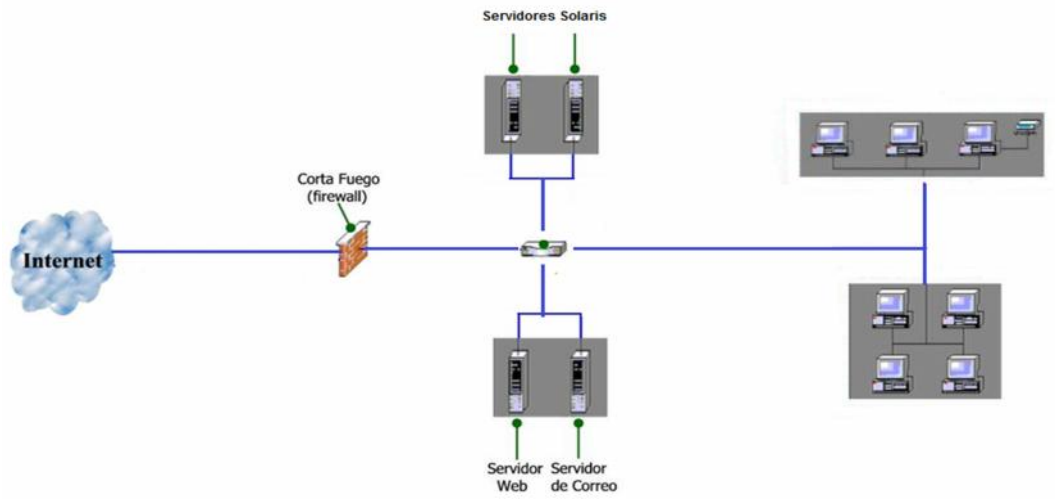
6.5 RED ACTUAL DEL INPEC EN LA REGIONAL CENTRAL

La Sede Central del INPEC cuenta actualmente con servidores de datos, servidores de aplicaciones, estaciones cliente en donde se administran y enlazan con los establecimientos y demás regionales a nivel nacional.

[27] Introduccion a los IDS. [en línea]. < http://www.adminso.es/images/0/03/Pfc_Carlos_cap1.pdf> [citado en 06 de Junio de 2014]
[28] Intercomunicación y seguridad en redes. [en línea]. < http:// lordratita.wordpress.com/2012/07/page/2/ > [citado en 06 de Junio de 2014]

- 2 Servidores Solaris Versión 10 (Incluye sistema Operativo, bases de datos y demás herramientas informáticas instaladas).
- 1 Servidor Linux.
- 7 PC‘s
- 1 Switch Cisco Catalyst 4705.
- 1 Servidor correo (Hosting en ETB)

Figura 2: Red Interna Sede Central



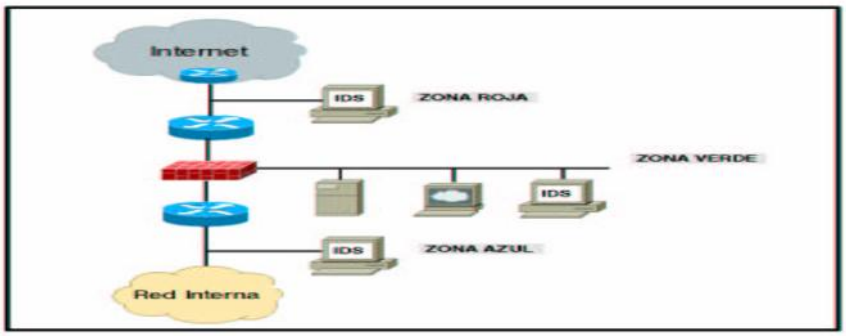
Recuperado: Archivo particular INPEC

La decisión depende del equipo que usemos, el software IDS y la BD y esto nos da los fundamentos para saber dónde localizar el IDS, que es lo primero que hay que tener en cuenta para tomar la decisión de instalar un IDS.

6.6 DONDE COLOCAR UN IDS

Existen principalmente tres zonas en las que se podría poner un sensor.

Figura 3: Donde instalar un IDS



- **Zona roja**. Zona con un índice de riesgo elevado, por esta razón el IDS debe ser configurado de forma sensible, ya que el tráfico en la red tanto de entrada como de salida se verá y esto genera más alarmas.

- **Zona verde.** En esta zona la sensibilidad es mayor a la roja, es por eso que se debe configurar el IDS. Aparecen menos falsas alarmas que la zona roja y los servidores se podrán solo acceder desde esta zona.

- **Zona azul.** Esta es la zona de confianza. Cualquier tráfico anómalo que llegue hasta aquí debe ser considerado como hostil. En este punto de la red se producirán el menor número de falsas alarmas, por lo que cualquier alarma del IDS debe de ser inmediatamente estudiada[29].

6.7 MODELO DE REFERENCIA OSI

Después de la especificación de SNA (Systems Network Architecture) por parte de IBM cada fabricante importante definió su propia arquitectura de redes; así la evolución de los productos de comunicaciones estaba garantizada, pero no se había resuelto el problema de la interoperabilidad entre diferentes fabricantes. Debido a la posición de hegemonía que IBM disfrutaba en los años 70 y principios de los ochenta la compatibilidad con IBM era un requisito necesario, por lo que la mayoría de los fabricantes tenían implementaciones de los protocolos SNA para sus productos, o estas estaban disponibles a través de

[29]EMILIO JOSE MIRA ALFARO. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Trabajo de grado. [Ingeniero Informático]. Universidad de Valencia. Ingeniería Informática

terceros. Así, la forma más sencilla de interconectar dos equipos cualesquiera era conseguir que ambos hablaran SNA.[30]

En 1977 la ISO (International OrganizationforStandardization) consideró que esta situación no era la más conveniente, por lo que entre 1977 y 1983 definió la arquitectura de redes OSI con el fin de promover la creación de una serie de estándares que especificaran un conjunto de protocolos independientes de cualquier fabricante. Se pretendía con ello no favorecer a ninguno a la hora de desarrollar implementaciones de los protocolos correspondientes, cosa que inevitablemente habría ocurrido si se hubiera adoptado alguna de las arquitecturas existentes, como la SNA (Systems Network Architecture) de IBM o la DNA (Digital Network Architecture) de Digital.

Seguramente la aportación más importante de la iniciativa OSI ha sido precisamente su arquitectura. Ésta ha servido como marco de referencia para describir multitud de redes correspondientes a diversas arquitecturas, ya que la arquitectura OSI es bien conocida en entornos de redes, y su generalidad y no dependencia de ningún fabricante en particular le hacen especialmente adecuada para estos fines. Por este motivo generalmente a la arquitectura OSI se la denomina Modelo de Referencia OSI, o también OSIRM (OSI Reference Model). Por extensión hoy en día se utiliza a menudo el término modelo de referencia para referirse a una arquitectura de red; así oímos hablar del Modelo de Referencia TCP/IP, el Modelo de Referencia ATM, etc.[31].

El modelo OSI estandariza la representación de las redes a través de capas. El modelo contempla el uso de siete capas. Los principios que se aplicaron para llegar a las siete capas son las siguientes[32].

Los límites de las capas deben elegirse a modo de minimizar el flujo de la información a través de las interfaces.

La cantidad de capas debe ser suficiente para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

6.7.1 Capas presentes en el modelo OSI

- **Capa Física.** Es el encargado de la transmisión de bits por un canal de comunicación.

[30]Administración de Sistemas Operativos. IDS basados en hots (HIDS) [en línea]. <http://www.adminso.es/index.php/Modelo_OSI> [citado en 06 de Junio de 2014]

[31]EL MODELO DE REFERENCIA OSI.[en línea].<http://www2.rhernando.net/modules/tutorials/doc/redes/osi.html> [citado en 06 de Junio de 2014]

[32] Red LAN para el centro local Amazonas Universidad Nacional Abierta y a Distancia. .[en línea]<http://biblo.una.edu.ve/docu.7/bases/marc/texto/t37250.pdf>

- **Capa de Enlace de Datos.** Encargado de transformar sin errores un medio de trasmisión.

- **Capa de Red**. El funcionamiento de la subred es controlado por esta capa también pueden enrutar al destino los paquetes de la fuente.

- **Capa de Transporte**. Los datos de la capa de sesión son aceptados y los divide en unidades mínimas y éstas son pasadas a la capa de red, asegurando la llegada a su destino.

- **Capa de Sesión.** Las sesiones de los usuarios son establecidas por diferentes maquinas.

- **Capa de Presentación.** Realiza ciertas funciones que se le piden con suficiente frecuencia como para garantizar la búsqueda de una solución general para ellas, en lugar de dejar que cada usuario resuelva los problemas.

- **Capa de Aplicación**. Sus protocolos son variados y se utilizan para la transferencia de archivos, manejo de terminales diversos, presentación de líneas de texto, etc.

7 DISEÑO METODOLÓGICO PRELIMINAR

7.1 Tipo de investigación

El tipo de investigación que se propone en el presente trabajo de grado es la descriptiva proporcionando la información necesaria de una muestra para analizar la propuesta que permita implementar un IDS en la Sede Central del INPEC ya que el objetivo es llegar a conocer y comprender los componentes y procesos de un IDS describiendo e identificando los elementos que intervienen en el planteamiento de la investigación, su historia, características y demás aspectos lógicos de acuerdo a la descripción que se realiza en los diferentes contornos en los que se desarrolla dicho sistema y como se puede implementar en la Sede Central del INPEC para así lograr los objetivos que se proponen. Los datos o la información de interés se obtuvieron de forma directa por parte del investigador.

7.2 Método

Para la realización de la investigación el método a utilizar es el cuantitativo, ya que sus resultados pueden ser medibles en términos numéricos en cuanto a cantidad de información de conexiones a la red recibidas y monitoreadas por un archivo de auditoría a través de períodos distintos de valoración.[33]

7.3 Población

Tamayo y Tamayo (1996), en su libro El Proceso de la Investigación Científica, define la población como “La totalidad de individuos o elementos en los cuales presentarse determinada característica susceptible de ser estudiada”. En la “PIDSINPEC” este proyecto la población que se ha definido estará conformada por 10 usuarios con nivel administrativo y soporte técnico sobre los servidores de la red y equipos de informática del INPEC Sede Central.

7.4 Muestra

Según el análisis de Méndez Morales (1996), en su libro Metodología de la Investigación, nos dice que la muestra es “Parte o subconjunto de la población”. En este caso el investigador representará la muestra por la misma cantidad de población, es decir, 10 personas, ya que esto representa una muestra finita y medible.

[33] PROPUESTA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA RED (DETECCIÓN DE INTRUSOS – REDES DE TRAMPA) CASO: INSTITUTO DE LAS ARTES ESCÉNICAS Y MUSICALES (IAEM). 2008 - 2009. [en línea]. <http://saber.ucv.ve/xmlui/bitstream/123456789/3670/1/T026800003889-0-43CesarVallez-000.pdf> [citado en 07 de Mayo de 2015]

7.5 Técnicas e instrumentos para la recolección de datos

Una de las técnicas para la recolección de datos hallamos que Carlos Sabino (1994) define la entrevista como "... desde el punto de vista del método científico es una forma específica de interacción social que tiene por objeto recolectar datos para la indagación.[34] El investigador formula preguntas a las personas capaces de aportarle datos de interés." De la misma manera Pérez (2002), clasifica la observación científica según los medios en "... no estructurada: Aquella en la cual el investigador reconoce, estudia y analiza los hechos de manera libre no utiliza ningún tipo de técnicas; y estructurada: Aquella que permite observar los fenómenos en forma sistemática... "y según la participación del Investigador la clasifica en "... participante:

El investigador se involucra directamente con el grupo o comunidad, y no participante: el investigador está en contacto con la comunidad sin participar. Se comporta como un espectador."

Para la recolección de datos se utilizaron las técnicas de entrevistas y observación no estructurada.

La información para esta investigación fue recogida mediante la implementación de un instrumento de medición (el cuestionario), el cual se elaboró con preguntas que hacen referencia a los fundamentos de esta investigación. Así mismo las respuestas sirvieron de soporte para identificar los objetivos proyectados en esta investigación.

Con la información recolectada de acuerdo al orden de los indicadores, se realizaron los análisis cualitativos de los datos arrojados en la investigación y se elaboraron cuadros estadísticos y representaciones gráficas.

[34]Como hacer una tesis. [en línea]. http://www.unicauca.edu.co/ai/Investigacion/TesisDoctorales.pdf > [citado en 06 de Marzo de 2015

8 RESULTADO Y ANALISIS DE LA ENCUESTA

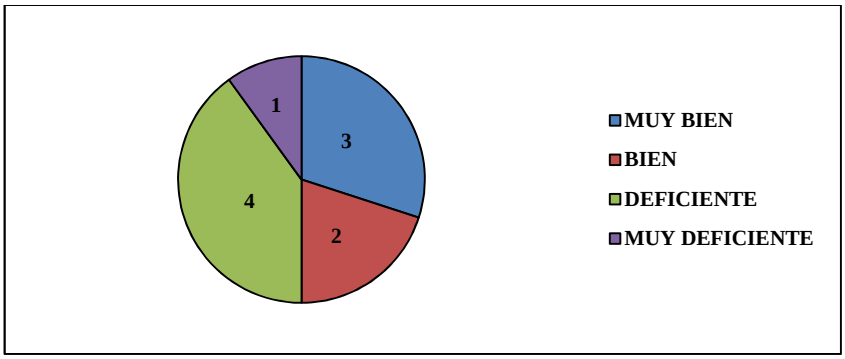
¿Cómo cree usted que la red del sistema de la Sede Central en cuanto a seguridad funciona actualmente?

TABLA 1 Funcionamiento actual del sistema

MUY BIEN	BIEN	DEFICIENTE	MUY DEFICIENTE	TOTAL
3	2	4	1	10

Fuente: Autor

Figura 4 Grafico funcionamiento actual del sistema



Fuente: Autor

Se puede observar que los funcionarios encuestados la mitad de ellos están conformes y la otra mitad no creen que la seguridad de la red del sistema sea segura o piensan que la red presenta deficiencias o puede estar expuesta a cualquier ataque informático.

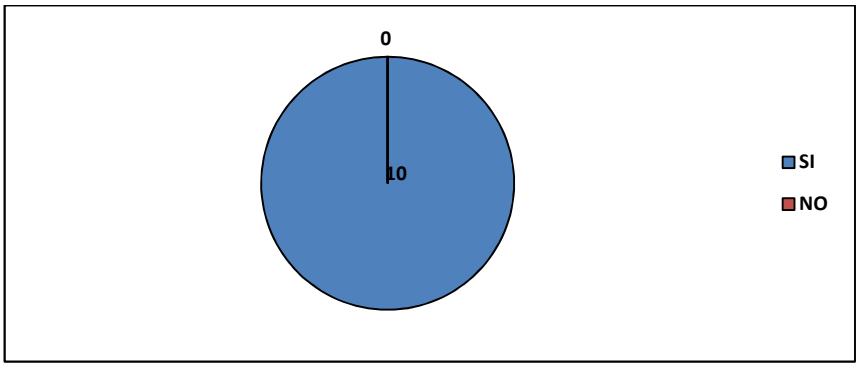
¿Usted sabe que es un ataque informático?

TABLA 2 Conocimiento ataques informáticos

SI	NO	TOTAL
10	0	10

Fuente: Autor

Figura 5 Grafico conocimiento ataques informáticos



Fuente: Autor

Se puede observar que la totalidad de los encuestados saben que es un ataque informático, al menos tal vez porque lo han leído, o lo han visto por noticias, pero hasta el momento no lo han experimentado.

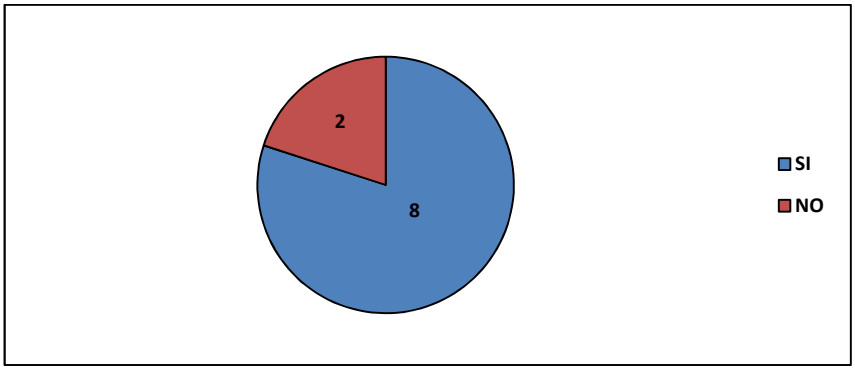
Tiene conocimiento si existe algún procedimiento sobre el mantenimiento al hardware y software de la red.

TABLA 3 Conocimiento mantenimiento hardware y software

SI	NO	TOTAL
8	2	10

Fuente: Autor

Figura 6 Grafico conocimiento mantenimiento hardware y software



Fuente: Autor

La mayoría de los encuestados saben que existen estos procedimientos, lo ideal debería ser que fuera en su totalidad, ya que las políticas de la Institución exige que todos sus empleados manejen y apliquen estos procedimientos.

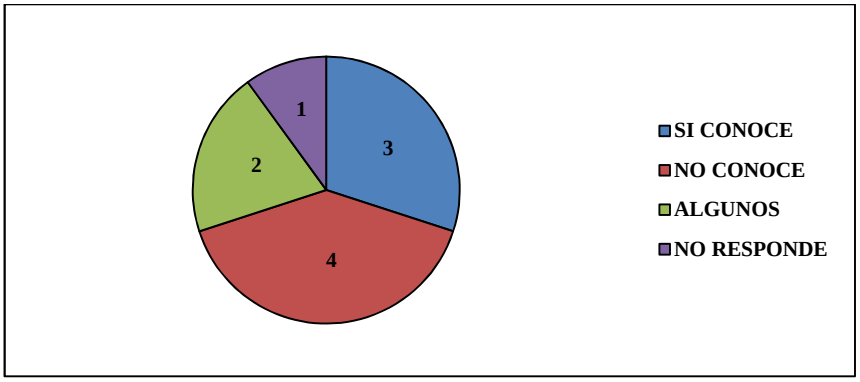
¿Conoce los diferentes ataques a los que puede estar expuesto un sistema o red?

TABLA 4Conocimiento ataques a un sistema o red

SI CONOCE	NO CONOCE	ALGUNOS	NO RESPONDE	TOTAL
3	4	2	1	10

Fuente: Autor

Figura 7 Grafico del conocimiento ataques a un sistema o red.



Fuente: Autor

Al responder a este interrogante se evidencia la contrariedad con respecto al conocimiento de los ataques informáticos, porque al preguntarse sobre un tema en particular que es la red, la mitad de ellos coincide que desconoce dichos ataques.

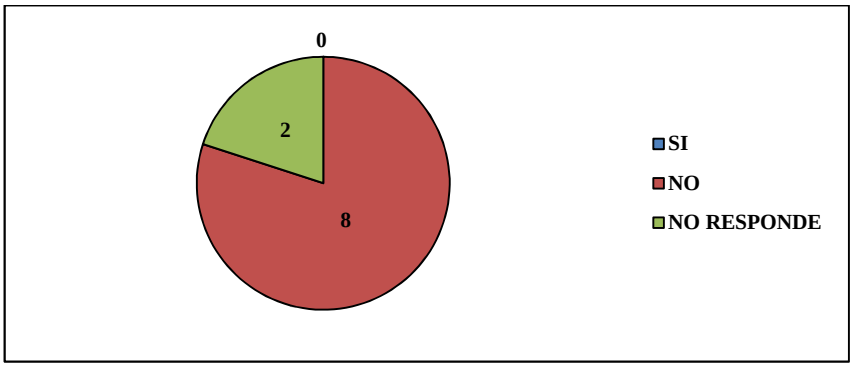
¿Sabe cuándo un sistema informático está siendo atacado?

TABLA 5 Conocimiento ataque informático

SI	NO	NO RESPONDE	TOTAL
0	8	2	10

Fuente: Autor

Figura 8 Grafico del Conocimiento ataque informático



Fuente: Autor

La falta de preparación, el desinterés o el hecho de que en el lugar de trabajo de ellos no haya ocurrido un suceso informático, nos indica que los encuestados no tienen el conocimiento necesario para conocer cuando su sistema está siendo atacado.

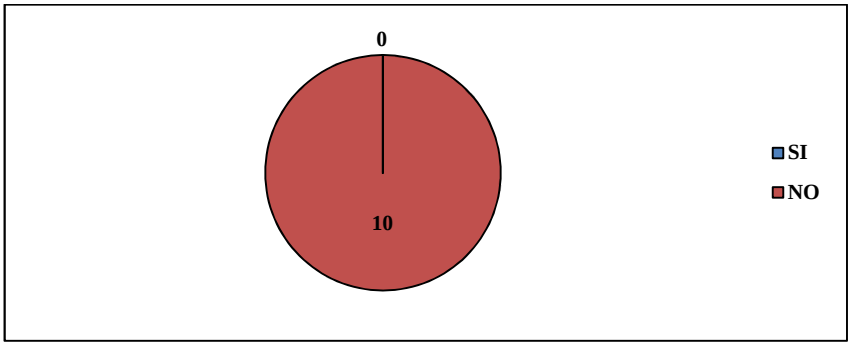
¿En caso de sospechar cuando el sistema está siendo atacado sabe realmente que hacer?

TABLA 6 Actuación frente a un ataque

SI	NO	TOTAL
0	10	10

Fuente: Autor

Figura 9 Grafico Actuación frente a un ataque



Fuente: Autor

Los encuestados en su totalidad coinciden que no tienen ni la más remota idea de cómo actuar en el caso de que su sistema se vea atacado, esto sumándole el hecho de que no saben cuándo un sistema está siendo víctima de un intruso.

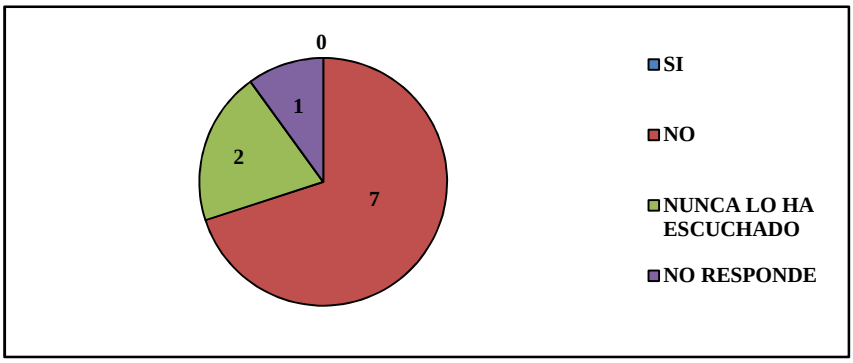
¿Sabe usted que es un Sistema de Detección de Intrusos (IDS) y para qué sirve?

TABLA 7 Que es un Sistema de Detección de Intrusos (IDS)

SI	NO	NUNCA LO HA ESCUCHADO	NO RESPONDE	TOTAL
0	7	2	1	10

Fuente: Autor

Figura 10 Grafico que es un Sistema de Detección de Intrusos (IDS) y para qué sirve.



Fuente: Autor

Se desconoce uno de los sistemas que las empresas actualmente están utilizando para incrementar la seguridad en las redes los Sistemas de Detección de Intrusos (IDS) y como el resultado de la entrevista se evidencia que los usuarios del sistema en su mayoría tienen poco conocimiento sobre seguridad informática y mucho menos la forma como se podría mitigar o evitar los ataques al sistema.

9 PROPUESTA

9.1 Propuesta de IDS a implementar

Teniendo como base los resultados obtenidos en un pen test realizado a la red y al evidenciar los resultados que se presentan en ella, se propone implementar la herramienta Snort como medida de prevención contra intrusos, ya que éste es un sistema de detección de intrusiones basado en red (NIDS). Snort genera unas alertas para cuando estas vulnerabilidades se presentan, registrando el análisis obtenido y almacenándolo en su base de datos.

Snort está disponible bajo licencia GPL, es gratuito y funciona bajo plataformas Windows y GNU/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, y actualizaciones constantes.

❖ **Elementos del sistema Snort**

Los elementos que componen el esquema básico de su arquitectura son:

- **Módulo de captura del tráfico**. Es el encargado de capturar todos los paquetes de la red utilizando la librería libpcap.

- **Decodificador**. Se encarga de formar las estructuras de datos con los paquetes capturados e identificar los protocolos de enlace, de red, etc.

- **Preprocesadores**. Permiten extender las funcionalidades preparando los datos para la detección. Existen diferentes tipos de preprocesadores dependiendo del tráfico que se quiere analizar (por ejemplo, existen los preprocesadores http, telnet).

- **Motor de Detección.** Analiza los paquetes en base a las reglas definidas para detectar los ataques.

- **Archivo de Reglas**. Definen el conjunto de reglas que regirán el análisis de los paquetes detectados.

- **Plugins de detección.** Partes del software que son compilados con Snort y se usan para modificar el motor de detección.

- **Plugins de salida.** Permiten definir qué, cómo y dónde se guardan las alertas y los correspondientes paquetes de red que las generaron. Pueden ser archivos de texto, bases de datos, servidor syslog, etc.

- **Módulo de captura de datos**. El módulo de captura de paquetes del sensor se encarga, tal y como su propio nombre indica, de realizar la captura del tráfico que circula por la red, aprovechando al máximo los

recursos de procesamiento y minimizando por tanto la pérdida de paquetes a tasas de inyección elevadas.

Para que los preprocesadores y posteriormente el motor de detección puedan conseguir paquetes se deben realizar algunas tareas previas. Snort no tiene ninguna facilidad nativa de paquetes aún; por lo que requiere de una biblioteca de sniffing de paquetes externa: libpcap. Libpcap fue escogida para la captura de paquetes por su independencia de plataforma. Puede ser controlada sobre todas las combinaciones de hardware y S.O; e incluso sobre WIN32 con winpcap.

Debido a que Snort usa la biblioteca libpcap para capturar paquetes por la red, puede utilizar su transportabilidad para ser instalado en casi todas partes. La utilización de libpcap hace que Snort tenga un uso realmente independiente de plataforma.

La responsabilidad de capturar paquetes directamente de la tarjeta de interfaz de red pertenece a libpcap. Esto hace que la facilidad de captura para “paquetes raw”proporcionados por el sistema operativo esté disponible a otras aplicaciones.

- **Preprocesadores**

El protocolo TCP/IP es un protocolo que se basa en capas y cada capa del protocolo tiene una función determinada y para trabajar correctamente necesita una información.

Los datos a la hora de trasmitirse por la red en paquetes de forma individual, llegan a su destino de forma desordenada, siendo el receptor el que se encarga de ordenar los paquetes y darles un sentido.

Snort tiene que leer todo el tráfico que pasa por la red y lo interpreta, además tiene que llevar un control de todos los paquetes que se envían por la red y así Snort le da forma a la información.

Los preprocesadores son componentes de Snort que no dependen de las reglas ya que el conocimiento sobre la intrusión depende del módulo Preprocesador. Se llaman siempre que llegue un paquete y se les puede aplicar reglas que estén cargadas en Snort. Así pues, se encargan de coger la información que viaja por la red de una manera caótica y darle forma para que pueda ser interpretada la información. De esta forma una vez que tenemos los datos ordenados que viajan por la red aplicaremos las reglas (rules) para buscar un determinado ataque.

Esta arquitectura de preprocesadores que tiene Snort radica en pequeños programas en C que toman decisiones sobre qué hacer con los paquetes. Estos programas se compilan junto a Snort en forma de librería. Estos

preprocesadores son citados después que Snort realice la decodificación, y después se llama al motor de detección. Si el número de preprocesadores es muy alto el rendimiento de Snort puede caer considerablemente.

Las configuraciones predeterminadas para estos subsistemas son muy generales, a medida que experimentemos con Snort, podremos ajustarlas para obtener un mejor rendimiento y resultados.

- **Reglas.** Las reglas o firmas son los patrones que se buscan dentro de los paquetes de datos. Las reglas de Snort son utilizadas por el motor de detección para comparar los paquetes recibidos y generar las alertas en caso de existir coincidencia entre el contenido de los paquetes y las firmas. El archivo snort.confpermite añadir o eliminar clases enteras de reglas. En la parte final del archivo se pueden ver todos los conjuntos de reglas de alertas. Se pueden desactivar toda una categoría de reglas comentando la línea de la misma.[35]

❖ **Categorías de reglas Snort**

Existen cuatro categorías de reglas para evaluar un paquete. Estas cuatro categorías están divididas a su vez en dos grupos, las que tienen contenido y las que no tienen contenido.

Hay reglas de protocolo, reglas de contenido genéricas, reglas de paquetes mal formados y reglas IP.

- **Reglas de Protocolo.** Las reglas de protocolo son reglas las cuales son dependientes del protocolo que se está analizando, por ejemplo en el protocolo Http está la palabra reservada uricontent.

- **Reglas de Contenido Genéricas.** Este tipo de reglas permite especificar patrones para buscar en el campo de datos del paquete, los patrones de búsqueda pueden ser binarios o en modo ASCII, esto es muy útil para buscar exploits los cuales suelen terminar en cadenas de tipo “/bin/sh”.

- **Reglas de Paquetes Malformados.** Este tipo de reglas especifica características sobre los paquetes, concretamente sobre sus cabeceras las cuales indican que seestá produciendo algún tipo de anomalía, este tipo de reglas no miran en el contenido ya que primero se comprueban las cabeceras en busca de incoherencias u otro tipo de anomalía.

- **Reglas IP.** Este tipo de reglas se aplican directamente sobre la capa IP, y son comprobadas para cada datagrama IP, si el datagrama luego es

[35]María Isabel Giménez García, Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. Ingeniero en Informática. Universidad de Almería

Tcp, Udp o Icmpse realizará un análisis del datagrama con su correspondiente capa de protocolo, este tipo de reglas analiza con contenido y sin él.

❖ **Personalización de reglas**

La manera más fácil de limitar el tráfico de las alertas es desactivar las reglas que no se aplicaran en el sistema, esto se hace ingresando en la configuración deSnort. El directorio */etc/snort/rules/* contiene muchos archivos con la extensión *.rules*.

Se puede deshabilitar una clase entera de reglas comentándola en el archivo de configuración o se puede deshabilitar reglas individuales si se requiere de la protección del resto de reglas de la clase. Para comentar una regla concreta, se busca en los archivos*.rules* apropiados y se inserta un comentario delante de la línea de dicha regla.

Hay que tener en cuenta que normalmente es mejor deshabilitar una sola regla que toda la clase, a no ser que ésta no se aplique en una determinada configuración. El motor de detección es realmente el corazón de la funcionalidad de Snort. Snortusa un lenguaje de descripción simple y flexible para indicar cómo se deben de manejarlos datos. Para que Snort pueda coger las últimas vulnerabilidades, se debe de actualizar nuestras reglas.

Aunque los conjuntos de reglas estándar incluidos en Snort proporcionan una protección adecuada contra armas de ataques conocidas, se puede diseñar algunas reglas personalizadas específicas para que la red obtenga el mejor rendimiento del IDS.

Snort permite mucha versatilidad para crear nuevas reglas. Modificando las propias reglas, minimizaremos los falsos positivos. Las reglas que abarcan muchos casos generales suelen poseer altos índices de falsos positivos, mientras que las particulares no. La idea es crear nuevas reglas avanzadas, en función de los servicios que se desean monitorizar.

Se pueden escribir reglas para:

- ✓ Registrar el acceso hacia o desde determinados servidores.
- ✓ Buscar determinados tipos de nombres de archivos en nuestra organización.
- ✓ Vigilar determinados tipos de tráfico que no pertenecen a nuestra propia red.

La escritura de reglas de Snort es fácil de aprender y nos permite añadir funcionalidades al programa, sin muchos conocimientos de programación.

Como se ha podido comprobar, las reglas de Snort son simplemente declaraciones de texto dentro de un archivo de reglas.

Si se desea que Snort busque un comportamiento único que debería ser sospechoso en nuestra red, se puede codificar rápidamente una regla y probar el resultado. El formato de una regla de Snort es básicamente una sola línea de texto que empieza con una acción (normalmente *alert*) seguida por diversos argumentos. Se pueden añadir múltiples líneas simplemente añadiendo una barra inclinada (/) al final de cada línea[36].

También se puede llamar a otros programas utilizando una declaración de inclusión para obtener una regla más compleja.

En su forma básica, una regla de Snort consta de dos partes:

- ✓ Un encabezado
- ✓ Las opciones

- **El motor de detección.** El motor de detección es la parte más importante de Snort. Su responsabilidad es descubrir cualquier actividad de intrusión existente en un paquete. Para ello, el motor de detección emplea las reglas de Snort. Las reglas son leídas en estructuras de datos internas o cadenas donde son comparadas con cada paquete[37]. Si un paquete empareja con cualquier regla, se realiza la acción apropiada. De lo contrario el paquete es descartado. Las acciones apropiadas pueden ser registrar el paquete o generar alarmas.

El motor de detección es la parte de tiempo crítico de Snort. Los factores que influyen en el tiempo de respuesta y en la carga del motor de detección son los siguientes:

- Las características de la máquina.
- Las reglas definidas.
- Velocidad interna del bus usado en la máquina Snort.
- Carga en la red.

[36] SNORT. [en línea]. < http://www.adminso.es/images/4/48/Pfc_Marisa_Capitulo2.pdf.> [citado en 07 de Mayo de 2015]

[37]SNORT. Sistemas de Detección de Intrusos [en línea]. <https://snortudenar.wordpress.com/snort-2/> [citado en 06 de Mayo de 2015]

Estos factores son muy importantes ya que por ejemplo, si el tráfico en la red es demasiado alto, mientras Snort está funcionando en modo NIDS, se pueden descartar paquetes y no se conseguirá una respuesta en tiempo real. Así pues, para el diseño delIDS habrá que tener en cuenta estos factores.

El motor de detección puede aplicar las reglas en distintas partes del paquete.

Estas partes son las siguientes:

- **La cabecera IP.** Puede aplicar las reglas a las cabeceras IP del paquete.

- **La cabecera de la capa de Transporte**. Incluye las cabeceras TCP, UDP eICMP.

- **La cabecera del nivel de la capa de Aplicación**. Incluye cabeceras DNS, FTP, SNMP y SMPT.

- **Payload del paquete.** Esto significa que se puede crear una regla que el motor de detección use para encontrar una cadena que esté presente dentro del paquete.

El motor de detección de Snort funciona de forma diferente en distintas versiones deSnort.

9.2 Propuesta de la base de datos a implementar

9.2.1 MySQL. Lo mismo que para la gestión de los incidentes se debe optar por usar una base de datos relacional que permita hacer consultas complejas y facilitara el análisis al responsable de la seguridad. En esta propuesta se recomienda situar la base de datos en una maquina distinta a la que corre Snort por razones de eficiencia, ya que Snort solo puede utilizar un procesador simultáneamente quedando el otro procesador libre.

La base de datos que se presenta es MySQL ya que es un sistema de administración de bases de datos. Es totalmente gratuito, por lo que es una buena alternativa en sistemas como SQL Server u Oracle. El servidor de bases de datos MySQL es muy rápido, seguro, y fácil de usar por lo que es la solución adecuada para la implementación de Snort con un modelo de base de datos que permita tener un registro y control del análisis del tráfico.

MySQL es la base de datos relacional que se debe utilizar para controlar y almacenar los registros de las alertas o capturas que Snort realice[38].

[38]MySQL. [en línea]< http:// www.mysql.com/downloads/ > [citado en 30 de Marzo de 2015]

❖ Instalación

Por cuestiones de compatibilidad con diferentes equipos, se sugiere la instalación por separado del driver ODBC para MySQL.

Para instalarlo únicamente se debe de ejecutar el programa de instalación, y dar clic en instalar. La instalación será de forma automática.

Usualmente dentro del archivo comprimido de MySQL se encuentra el archivo de instalación llamado setup.exe. Al momento de ejecutarlo aparece la ventana de bienvenida, se da clic en Next.

Posteriormente aparece la ventana de información. Si se desea instalar MySQL en otro directorio diferente de C:\MySQL, se debe de crear un archivo de inicialización, la ventana de información describe el proceso. Para continuarse presiona el botón Next.

Una vez indicada la ruta en donde se instaló MySQL, se tomará como referencia de MySQLPath.

❖ Configuración

Para empezar a utilizar MySQL es necesario realizar algunas configuraciones iniciales y para hacerlo se debe desplazar a la carpeta MySQLPath\bin y ejecutar el siguiente comando:

Winmysqladmin

Al hacer esto se abre la consola gráfica de administración de la base de datos y solicita configuración para la autenticación. Se puede utilizar cualquier nombre de usuario y contraseña que se desee y se presiona el botón OK.

Debe aparecer un icono de semáforo en la parte inferior derecha con la luz verde encendida, esto indica que el servidor MySQL puede ser utilizado y que arrancó de forma adecuada, en caso de que no sea así y la luz sea de color rojo, es necesario revisar la configuración del archivo my.ini en %systemroot% (C:\Windows para XP y C:\WinNT para 2000) o desde la consola gráfica de administración en la pestaña my.ini Setup.

Una vez que MySQL funciona adecuadamente, es necesario configurarlo para que pueda trabajar con los datos de Snort. Antes es recomendable verificar que en la pestaña StartCheck de la consola de administración, la línea de my.ini tenga un yes como valor y las líneas siguientes indiquen OK. Esto indica de forma más clara que MySQL funciona apropiadamente.

El primer paso para configurar MySQL para trabajar con Snort es agregar un poco de seguridad, con lo cual se cambia la contraseña de administrador.

En el directorio MySQLPath\bin se debe ejecutar el siguiente comando:

Mysql -u root -p

Y se introduce el password del usuario root, en caso de que no tenga el password se omite la opción -p. De esta forma se accede con el cliente al servicio de MySQL.

Para realizar el cambio de contraseña, ya una vez ingresado se ejecuta el siguiente comando:

mysql>update user set password=PASSWORD('clave') where user='root';
mysql> FLUSH PRIVILEGES;

Ahora es necesario eliminar cuentas y bases de datos predeterminadas para evitar posibles problemas de seguridad.

Primero se indica el uso de la base de datos de administración:
usemysql;

- **Para eliminar usuarios y equipos:**

delete from user where host = "%";
delete from user where host = "%";

Al ejecutar select * fromuser; únicamente debe existir el usuario root.

Para eliminar bases de datos, el comando show databases; debe mostrar las bases de datos actuales.

Únicamente debe de quedar mysql como base de datos, así que para eliminar las demás se ejecuta:

DropdatabaseBaseDeDatos;

Por último, se crea la base de datos para Snort, así como un usuario que pueda acceder a ella.

mysql>createdatabasesnort;

Desde MySQLPath\binse indica que utilice el formato de creación de la base de datos de Snort.

C:\mysql -D snort <SnortPath\contrib\create_mysql

- **Para crear el usuario:**

mysql> grant insert,select,update,create,delete on Dbname.* to User@YourHostName identified by 'clave';

- **Para verificar estos permisos:**

Show grantsforUser@YourHostName;

Por último se verifica su funcionamiento junto con Snort, y para esto se levanta el servicio de Snort ya ingresado en el registro desde el commandprompt.

net start snort

- **Para detenerlo:**

net stop snort

Posteriormente se desplaza a MySQLPath\bin y se trata de ingresar con el usuario User y se ingresa la contraseña.

mysql -D snort -h YpurHostName -u User –p

- **Password:**

*mysql>select * event;*

En la tabla event se guardan los índices de los eventos. Si no hay ninguno, se debe esperar algunos minutos a que Snort identifique un posible ataque.

9.3 Propuesta de aplicaciones a implementar

9.3.1 ACID. Así mismo se recomienda implementar ACID ya que es una consola de análisis Web que permite al administrador del sistema analizar los datos que fueron generados por Snort y almacenarlos en una base de datos (en este caso MYSQL), permitiendo ver la dirección IP del atacante, la fecha, el tipo de ataque, etc. ACID genera gráficos y estadísticas, basados en tiempo, sensores, vulnerabilidad, protocolo, dirección IP, puertos TCP/UDP.[39]

Para la instalación de ACID es necesario únicamente copiar todo el contenido del archivo comprimido de ACID en un directorio llamado ACID, dentro de la raíz del servidor Web (para que sea accesible vía Web) y modificar acid_conf.php con los siguientes datos.

[39]ACID en las bases de datos. [en línea]< http:// /www.dosideas.com/noticias/base-de-datos/973-acid-en-las-bases-de-datos.html> [citado en 30 de Marzo de 2015]

$DBlib_path = "SnortPath\adodb";
$alert_dbname = "Dbname";
$alert_host = "YourHostName";
$alert_port = "3306";
$alert_user = "User";
$alert_password = "Password";
$ChartLib_path = "SnortPath\phplot"

ACID crea tablas adicionales para que el usuario pueda archivar alertas importantes. Se puede indicar otro usuario para acceder a ellas.

/ Archive DB connectionparameters */*
$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort";
$archive_password = "snort";

Se reinician los servicios para prevenir posibles errores y se accede al servidor Web con la siguiente ruta (localhost si está en equipo local o dirección IP del servidor):

http://localhost/acid/index.html

La primera vez que se accede indica un error pues todavía no crea las nuevas tablas. Para hacerlo se seleccionaSelectSetup Page y luego Create ACID AG, esto debe de crear las tablas adicionales y desplegar correctamente la página inicial.

En caso de desplegar correctamente la página de ACID y tener levantados los servicios Snort y MySQLdebidamente, el sistema de Snort ya puede ser utilizado para analizar el tráfico en la red.

9.3.2 WinPcap. Es un driver de captura de paquetes, esto significa que WinPcap puede tomar paquetes de una red y colocarlo en Snort.

Sus funciones son:

- Obtener una lista de adaptadores de red y salvar esa información.
- Sniffer de paquetes usando más de un adaptador seleccionado.
- Almacenar paquetes en disco duro (En este caso a Snort)

Para su instalación se ejecuta únicamente el programa de instalación (WinPcap_2_3.exe). Se da clic en el botón Next y automáticamente se instalará en donde corresponde.

Snort llama a WinPcap de forma automática, por lo tanto si al momento de ejecutar Snort, éste no funciona adecuadamente, puede ser que WinPcap no haya sido debidamente instalado.

9.4 Propuesta de requerimientos e implementación

Para el correcto funcionamiento de Snort se aconseja el S.O Windows 2000 Professional ó Windows XP Professional aunque la configuración sencilla de Snort corre en prácticamente en cualquier versión de 32 bits de Windows, Windows 2000 Pro y XP Pro son más seguros y estables, esto ocurre principalmente por la falta de características como el sistema de archivos NTFS, el servidor Web IIS para ACID y soporte de más de un procesador.

Se recomienda utilizar como mínimo dos particiones, una con el sistema operativo y la otra para almacenar los resultados de la captura; su tamaño dependerá de la cantidad de datos que se recopilen, así como del tamaño de la red a analizar.

9.4.1 Propuesta para la protección del equipo

- ✓ Limitar acceso físico. Colocar Snort en un área segura, accesible sólo por el personal autorizado.
- ✓ Configurar el sistema para que inicie sólo desde disco duro.
- ✓ Control de acceso. Limitar el número de usuarios que pueden ingresar al sistema utilizando una directiva de contraseñas adecuada.
- ✓ Instalar únicamente componentes necesarios para el funcionamiento del sistema operativo y no instalar componentes adicionales.
- ✓ Terminar todos los servicios que no se desean utilizar.
- ✓ Deshabilitar protocolos de red no necesarios.
- ✓ Establecer comunicaciones remotas si son necesarias con protocolos y aplicaciones seguras como IPSecó SSH.
- ✓ Aplicar actualizaciones de seguridad, parches, Services Pack.

9.5 Instalación de Snort

Para la instalación, Snort.org tiene una distribución de instalación automática para Windows, la cual puede ser utilizada de forma sencilla.

Se ejecuta el programa de instalación (snort.exe) y aparece la ventana de la Licencia Pública GNU. Se da click en I agree.

En la ventana Installation Options se debeseleccionar I do not plan to log to a database, or I am planning to log to one of the databases listed above. Se presiona el botón Next para continuar.

Esta opción es la adecuada si desea utilizar el soporte para la base de datos Mysql.

Posteriormente aparece la ventana ChoseComponents. Se selecciona los componentes que se desean instalar; de preferencia se instalan todas las opciones posibles.

Una vez hecho esto, se debe de indicar el lugar donde se instalará Snort, la opción predeterminada es en "C:\Snort", esta ruta se considera como SnortPath. Se presiona IInstall.

De esta forma queda instalado Snort en el equipo, ahora es necesario configurar Snort para poder trabajar adecuadamente.[40]

Configuración de Snort. Para que Snort comience a trabajar es necesario modificar algunos archivos especiales ubicados en SnortPath.

Se localiza el archivo SnortPath\etc\snort.conf y se abre con algún editor de texto que no corrompa el formato original como Notepad o Wordpad.

- **Configuración de red**

De forma predeterminada Snort.conf contiene la siguiente línea, la cual indica el rango de monitoreo.

var HOME_NET any

Para monitorear una IP o un segmento específico, se inserta el rango de direcciones IP y la subred de la red del host en snort.conf. Para hacer esto se remplaza la configuración de esta forma:

var HOME_NET IPAddressRange/Subnet

[40]SNORT [en línea]< http://www.snort.org// > [citado en 30 de Marzo de 2015]

- **Configuración de reglas**

Para que Snort detecte y avise sobre posibles intentos de ataques es necesario que se le diga un conjunto de reglas a seguir. De forma predeterminada la base de estas reglas está en SnortPath\rules.

Para indicar esto, en el archivo snort.conf, se remplaza la línea

*varRULE_PATH*por:
var RULE_PATH SnortPath\rules

- **Configuración de salida**

La configuración de la salida de Snort es muy importante ya que define cómo se presenta la información al usuario. Existen muchas características sobre la salida de Snort, pero para esta implementación se utilizará la salida de una alerta en una base de datos.

Para configurarlo se debe localizar la siguiente línea:

 # outputlog_tcpdump; tcpdump.log

Modificarla de la siguiente forma:

outputalert_fast: alert.ids

- **Configuración para la integración con la base de datos**

Para poder utilizar las características de almacenamiento en MySQL es necesario contar con la siguiente información antes de poder continuar.

- ✓ **User.** Usuario MySQL de la base de datos donde Snort almacenará información.
- ✓ **Password**. Contraseña del usuario.
- ✓ **Dbname.** Nombre de la base de datos en MySQL donde Snort almacenará las alertas.
- ✓ **YourHostName.** Nombre del host del servidor de base de datos.
- ✓ **Port.** Puerto en el cual se establecerá la comunicación Snort–MySQL.
- ✓ **Sensor_name**: Nombre del sensor de Snort.

Es posible obtener el nombre del host (hostname) con el comando hostname en el commandprompt (símbolo del sistema).

Se debe recordar no usar nombres de usuarios, bases de datos y passwords predeterminados para evitar ser comprometido.

Una vez obtenida esta información, localizar en el archivo snort.conf la siguiente línea:

 # output database: log, mysql, user=root password=test dbname=db host=localhost

Utilizando su propia información, se modifica la línea para que quede de la siguiente forma:

output database: log, mysql, user=User password=Password dbname=Dbname host=YourHostNameport=Port sensor_name=Sensor_name
output database: log, mysql, user=snortusr password=P@zzm0Rd dbname=snortdb host=localhost port=3006sensor_name=snort_sensor

- **Incluir archivos especiales**

Dos archivos de configuración deben ser referenciados para que Snort pueda clasificar y generar alertas adecuadas. Estos son classification.config y reference.config.

Para incluirlos se debe localizar la siguiente línea en snort.conf
Includeclassification.config

- **Modificar de la siguiente forma:**

IncludeSnortPath\etc\classification.config

De igual forma localizar en snort.conf

Includereference.config

- **Modificar de la siguiente forma:**

IncludeSnortPath\etc\reference.config

❖ **Propuesta de implantación del IDSSnort en la Sede Central del INPEC**

La colocación de Snort en la red de la Sede Central del INPEC se debe de realizar en función del tráfico que se quiere vigilar: paquetes entrantes, salientes, dentro del firewall, fuera del firewall.

Se debe de colocar el IDS Snortde forma que se garantice la interoperabilidad y la correlación en la red. Así la interoperabilidad permite que el sistema IDS Snort pueda compartir u obtener información de otros sistemas como firewalls,

routers y switches, lo que permite reconfigurar las características de la red de acuerdo a los eventos que se generan.

Se puede colocar el IDS Snortde las siguientes formas:

- **Delante del firewall.** De esta forma el IDS Snort puede comprobar todos los ataques producidos, aunque muchos de ellos no se hagan efectivos. Genera gran cantidad de información en los logs, que puede resultar contraproducente.

- **Detrás del firewall**. Snort colocado detrás del firewall suele ser la ubicación característica, puesto que permite analizar, todo el tráfico que entra en la red (y que sobrepasa el firewall).

Además, permite vigilar el correcto funcionamiento del firewall. Monitoriza únicamente el tráfico que haya entrado realmente en la red y que no ha sido bloqueado por el firewall. Con lo cual la cantidad de logs generados es inferior a la producida en el caso anterior.

Dentro de esta ubicación, se puede situar el IDS Snortatendiendo a los siguientes esquemas:

a) IDSSnort colocado tras un Hub (concentrador que une conexiones y no altera las tramas que le llegan).

b) IDS Snortcolocado tras un switch con un puerto replicador. El switch almacena la trama antes de reenviarla hacia Snort.

c) IDSSnort colocado en modo bridge. De esta forma se establece una comunicación directa entre los dos adaptadores de red.

- **Combinación de los dos casos**. Combinando la colocación del IDS Snortdelante y detrás del firewall el control que se ejerce es mayor. Se puede efectuar una correlación entre ataques detectados en un lado y otro. El inconveniente es que se necesitan dos máquinas para implementarlo.

- **Firewall/NIDS.** Otra opción es usar una única máquina que haga las funciones de firewall y de NIDS a la vez.

- **Combinaciones avanzadas**. Se utilizan para cubrir necesidades de seguridad más altas. Por ejemplo si se necesita que cada NIDS monitorice un segmento de red o hosts individuales.

❖ **Los IDS y las políticas de Seguridad**. El IDS Snort debe ser tratado como un elemento complementario en las políticas de seguridad de la Institución,

pero antes de implementar o instalar el IDS Snortse recomienda analizar la política de seguridad y ver cómo encajaría el IDS Snort en ella:

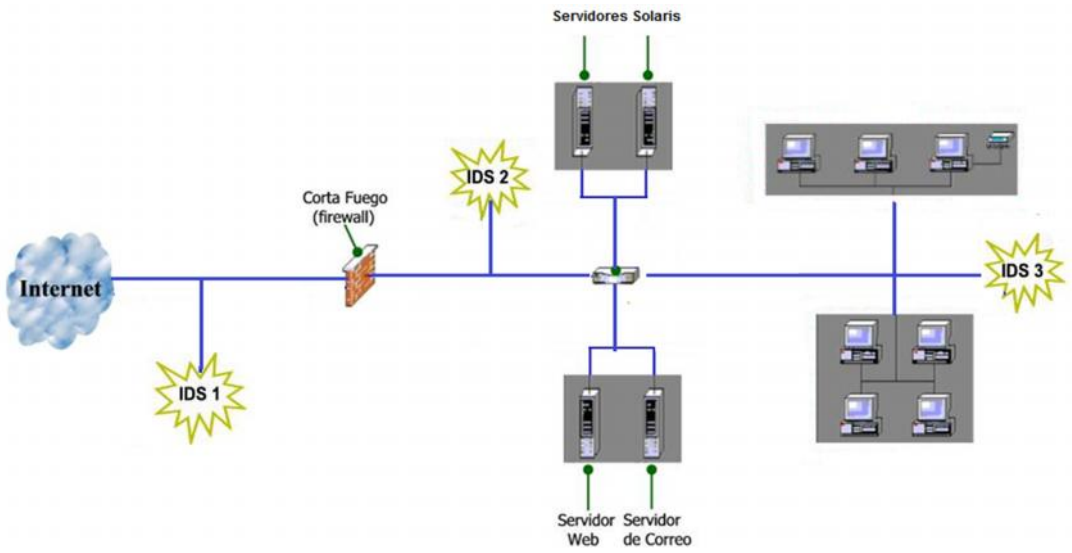
- ✓ Se recomienda una política de seguridad bien definida y a alto nivel, que cubra lo que está y lo que no está permitido en el sistema y red de la Sede Central del INPEC.

- ✓ Procedimientos documentados para que proceda el personal si se detecta un incidente de seguridad.

- ✓ Auditorías regulares que confirmen que las políticas de seguridad de la red en Sede Central del INPEC están en vigencia y las defensas son adecuadas.

- ✓ Personal capacitado o soporte externo cualificado.

Figura 11: Propuesta de la instalación gráfica del IDS Snort en la Sede Central del INPEC



Recuperado: Archivo particular INPEC

Si se sitúa el IDSSnort antes del cortafuegos exterior permitiría detectar el rastreo de puertos de reconocimiento que señala el comienzo de una actividad hacking y se obtendrá como ventaja un aviso prematuro. Sin embargo, si los rastreos no son seguidos por un ataque real, se generará un gran número de alertas innecesarias con el peligro de comenzar a ignorarlas.

Si se opta por colocar el IDSSnort en la Zona Desmilitarizada (DMZ) se tendría como ventaja la posibilidad de adecuar la base de datos de atacantes del NIDS para considerar aquellos ataques dirigidos a los sistemas que están en la Zona Desmilitarizada (DMZ) (servidor web y servidor de correo y servidores Solaris) y configurar el cortafuegos para bloquear ese tráfico.

Así mismo, un NIDS dentro de la red, se podría monitorear todo el tráfico para fuera y dentro de esa red. Este NIDS no debería ser tan poderoso como los otros IDS, puesto que el volumen y el tipo de tráfico es reducido.

El IDS1 se encargaría de avisar del rastreo de puertos, y si es reactivo podría enviar un "aviso" tanto al que está rastreando (por ejemplo un ping a la dirección que emite el paquete) como al encargado de la seguridad de la organización. El IDS2 se encargaría de vigilar la zona desmilitarizada y analizar el tráfico que reciben tanto el servidor web como el servidor de correo y los servidores Solaris. El otro IDS se encargaría de la red interna, este NIDS interno (el IDS3) podría ser un sensor que recoge la información y la envía a una consola dónde se realizarían los cálculos[41].

9.6 Propuesta de recursos tecnológicos

Para la tecnología propuesta para la implementación del IDS Snort en la Sede Central del INPEC se mantendrán los servicios que existen actualmente ya que está compuesta por la plataforma tecnológica sobre la que se sustenta la propuesta formada por los mismos servidores desde el punto de vista del hardware de la Institución y la implantación del software seleccionado que cumple con los estándares de software libre y no requiere de la adquisición de licencias propietarias.

[41]VANESSA ELEANA GONZALEZ MARQUEZ. Detector de intrusos basado en sistema experto. Trabajo de grado.[Maestro en ciencias en ingeniería de computo con opción en sistemas digitales]. Instituto Politécnico Nacional de México. Centro de Investigación en computación.

10 RECURSOS DISPONIBLES

Los recursos materiales utilizados para la realización de este proyecto, son por cuenta del investigador, entre los principales se destacan:

1. Uso de 01 computador portátil para la trascripción de los borradores y los capítulos del Trabajo de Investigación, implementación de las prácticas para poner en marcha la propuesta y ejecución de la versión definitiva del proyecto.

2. Uso de Internet (tiempo de navegación indefinido), para la consulta de referencias en la web.

3. Material digital, fotocopiado y libros especializados en la seguridad de la Información para las referencias bibliográficas consultadas.

11 COSTOS DEL PROYECTO

RECURSO HUMANO

TABLA No 8 Costos de personal

Nombres y Apellidos	Titulo		Función	Horas por Semana	Valor Hora	Dedicación [Semanas]	TOTAL
	Formación básica	Posgrado					
Gilberzon Garzón Padilla	Ingeniero de Sistemas	-	Investigador Principal	5	$30.000	16	2.400.000
SUBTOTAL							$2.400.000

Fuente: Autor

El esfuerzo de tiempo y costos del proyecto para el éxito del mismo, como son viáticos, gastos de alojamiento, manutención entre otros, están incluidos en la tabla de costos de personal reflejados en el valor de horas y estos estarán a cargo por cuenta del investigador.

EQUIPOS

TABLA No 9Costos de utilización de equipos

Concepto	Cantidad	Total
Computador Portátil	1	1.200.000
Impresora	1	200.000
SUBTOTAL		$1.400.000

Fuente: Autor

En la tabla de costos de utilización de equipos que se necesitan para el desarrollo del proyecto corren por cuenta esencialmente del investigador.

MATERIALES E INSUMOS

TABLA No 10Costos de materiales e insumos

Concepto	Total [$]
Papelería y Fotocopias	120.000
Digitación e impresión	200.000
SUBTOTAL	$320.000

Fuente: Autor

Al igual en la tabla de costos de materiales e insumos necesarios para el análisis y desarrollo del proyecto y por ser para un trabajo de grado, los costos los colocará el investigador

BIBLIOGRAFIA

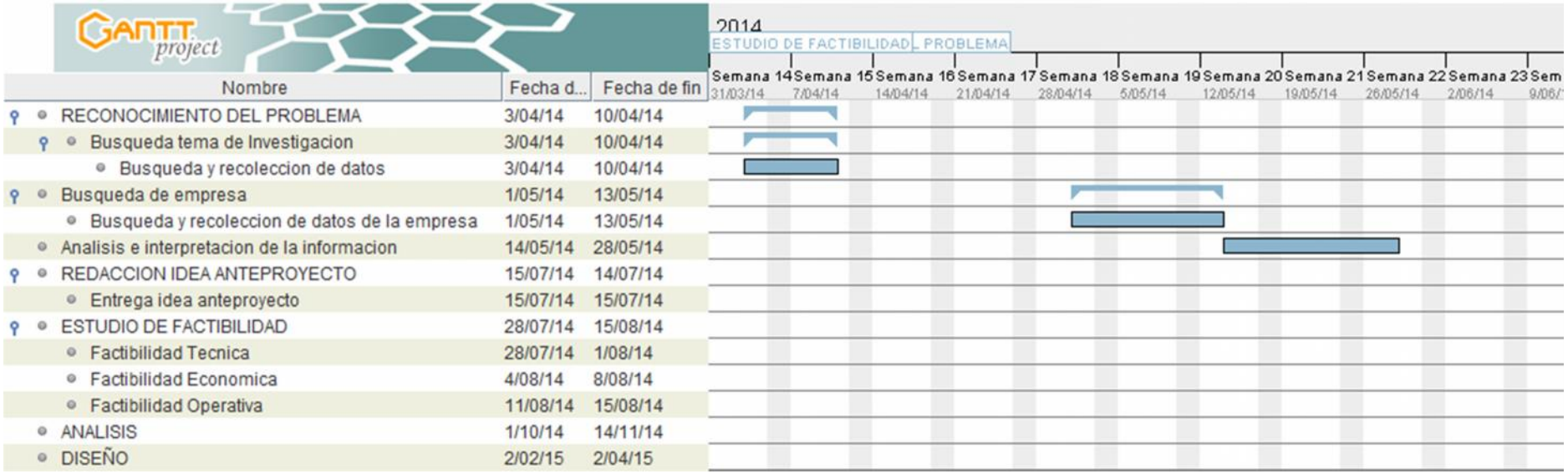
TABLA No 11Costos acceso a bibliografía

Concepto	Total [$]
Acceso a Internet	540.000
Libros	100.000
SUBTOTAL	$640.000

Fuente: Autor

En la tabla de costos acceso a bibliografía en donde el investigador extracta la información para el análisis del proyecto estará a cargo del mismo ya que son instrumento fundamental para el análisis y creación del proyecto.

12 CRONOGRAMA



Nombre	Fecha d...	Fecha de fin
RECONOCIMIENTO DEL PROBLEMA	3/04/14	10/04/14
Busqueda tema de Investigacion	3/04/14	10/04/14
Busqueda y recoleccion de datos	3/04/14	10/04/14
Busqueda de empresa	1/05/14	13/05/14
Busqueda y recoleccion de datos de la empresa	1/05/14	13/05/14
Analisis e interpretacion de la informacion	14/05/14	28/05/14
REDACCION IDEA ANTEPROYECTO	15/07/14	14/07/14
Entrega idea anteproyecto	15/07/14	15/07/14
ESTUDIO DE FACTIBILIDAD	28/07/14	15/08/14
Factibilidad Tecnica	28/07/14	1/08/14
Factibilidad Economica	4/08/14	8/08/14
Factibilidad Operativa	11/08/14	15/08/14
ANALISIS	1/10/14	14/11/14
DISEÑO	2/02/15	2/04/15

Tabla 12 Cronograma de actividades

El presente cronograma se realizó con base en el ciclo de vida de un proyecto informático, describiendo las fases que se tuvieron en cuenta para la realización del proyecto, desde la búsqueda y reconocimiento del problema, pasando por la propuesta del anteproyecto, el análisis y terminando con el diseño de la propuesta presentada en el proyecto.

12.1 ANALISIS EXPLICATIVO CRONOGRAMA

12.1.1 Reconocimiento del problema

Lo primero que se hizo fue buscar un tema de investigación (Sistemas de Detección de Intrusos IDS) y en el que se pudiera aplicar los conocimientos adquiridos en la Especialización de Seguridad Informática.

Se recolecto información sobre el tema de investigación, antecedentes, proyectos, tesis, en Internet, biografías, libros, etc.

Después se buscó una empresa o Institución en donde se pudiera implementar un IDS tema de investigación y que además existieran problemas o inconvenientes informáticos y encontramos al Instituto Nacional Penitenciario y Carcelario INPEC.

Se realizó la búsqueda y recolección de datos de la Institución y se pudo determinar que la red de información de la Sede Central del INPEC estaba expuesta a los diferentes ataques y vulnerabilidades informáticos.

Al tener la información requerida se realizó la interpretación de la información.

Por último se redactó la idea del anteproyecto el cual fue entregado para su revisión al Director de Proyecto I de la Especialización en Seguridad Informática.

12.1.2 ESTUDIO DE FACTIBILIDAD

Para darle continuidad y viabilidad al proyecto se estudiaron tres aspectos en el estudio de factibilidad de la investigación que son:

- ***Factibilidad Técnica:*** En esta etapa se verifica que la propuesta del software a implementar sea práctica y que se encuentre disponible ya que encontramos casos similares en varios entornos empresariales y de Instituciones conocidas pudiéndola implementar en la red de la Sede Central.

- ***Factibilidad Económica****:* En esta etapa se estudia que por ser un proyecto de investigación como opción grado para la culminación de la Especialización en Seguridad Informática, el proyecto económicamente es viable y se puede ejecutar ya que los costos de desarrollo del sistema, son por parte del investigador, además el software propuesto es gratuito.

- ***Factibilidad Operativa:*** La propuesta que se plantea trae beneficios a la Institución, además ofrece un tiempo de respuesta adecuado a los posibles inconvenientes que se presentan. Además se explotan al

máximo los recursos disponibles con los que cuanta l Sede Central del INPEC.

12.1.3 ANALISIS

De acuerdo a la necesidad que se quiere subsanar en la Institución y con la recolección de información y análisis de datos, se realiza el diseño de la propuesta consistente en la implantación del IDS en la red de la Sede Central del INPEC. Verificando qué hace el sistema, qué características se quieren y los requerimientos para el nuevo sistema, cotejando la información recogida sobre los IDS comerciales y estudiando cual cumple con las especificaciones exigidas.

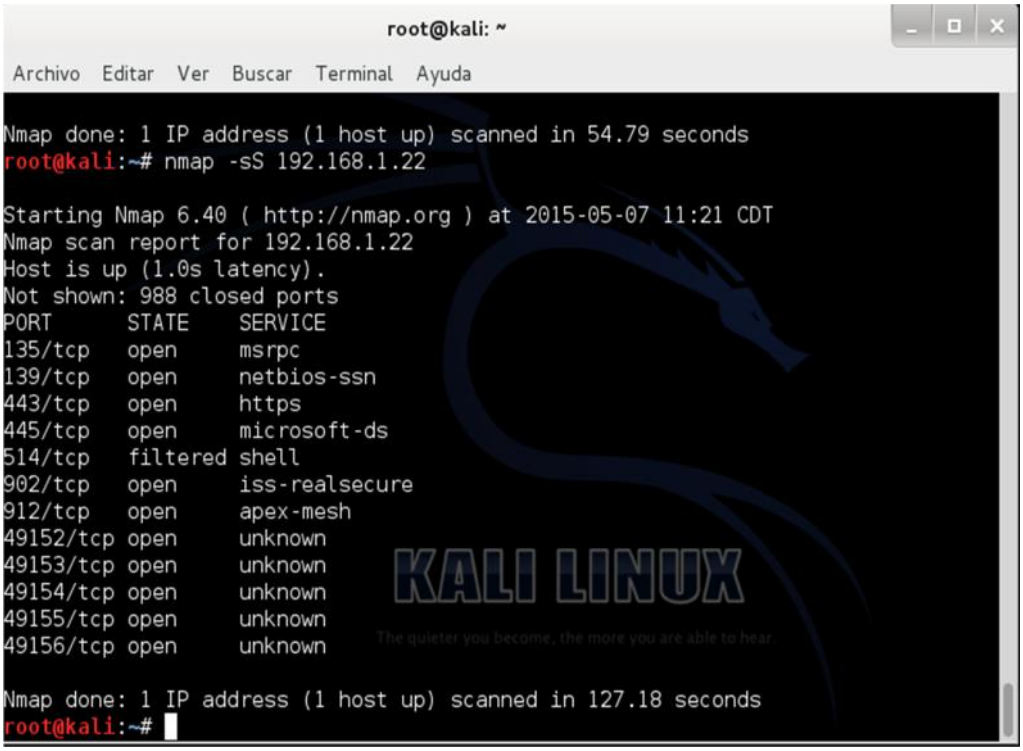
12.1.4 DISEÑO

En esta fase se organiza de forma adecuada la información suministrada por el análisis hecho previamente y se opta por realizar la propuesta de la implementación del IDS Snort, y se plasma una exposición detallada de la estructura interna del programa, su implementación, ejecución y aplicaciones requeridas para su funcionamiento además se hace una propuesta para la colocación en la red de la Institución del IDS Snort.

13 PRUEBAS

Se realiza un escaneo a un equipo de la red con la IP 192.168.1.22 utilizando la herramienta NMAP de KALI LINUX

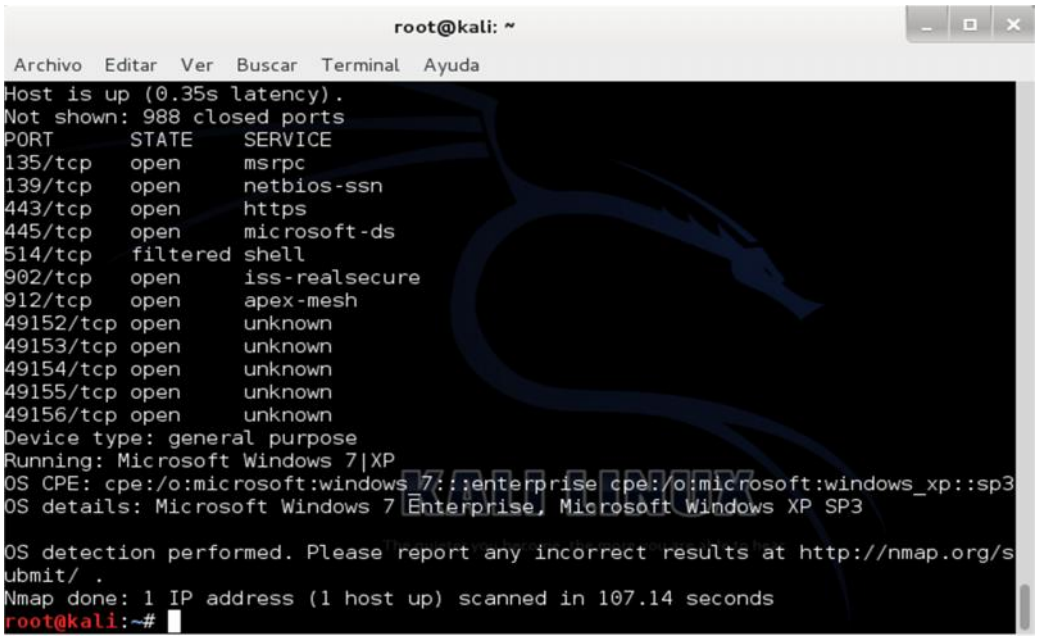
Figura 12 Prueba de la red con Nmap



Fuente: Autor

Nmap genera el reporte del escaneo de la red encontrando varios puertos tcp abiertos, reportando que la red es vulnerable a ataques informáticos.

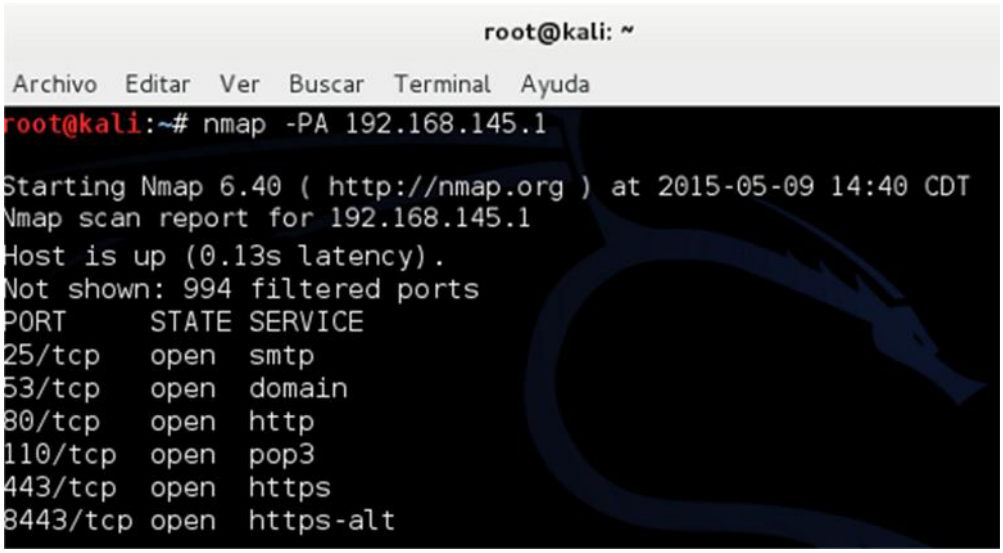
Figura 13 Prueba 2 de la red con Nmap



Fuente: Autor

También al realizar el escaneo a la red con Nmap se puede observar los servicios que se están utilizando en la maquina escaneada. En este caso la maquina está utilizando el SO Microsoft Windows 7.

Figura 14 Prueba 3 de la red con Nmap

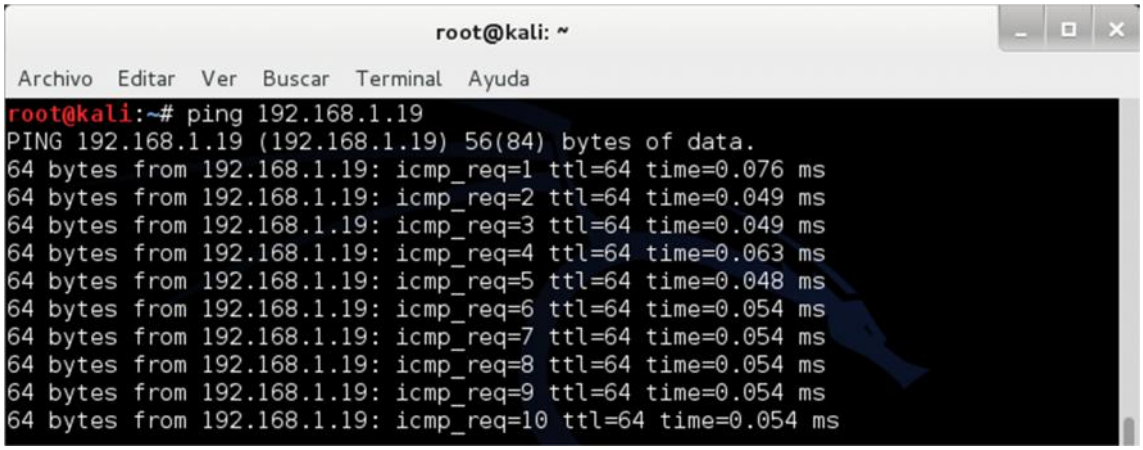


Fuente: Autor

Al hacer un Ping a otra máquina de la red con la IP 192.168.145.1 se evidencia que se encuentran varios puertos abiertos entre ellos está el puerto 80 y el puerto 25.

Con el puerto 80 abierto los atacantes pueden sacar nombres de usuarios y contraseñas de una base de datos. Y con el puerto 25 abierto los piratas informáticos tendrán a su merced el uso de los servidores de correo electrónico permitiendo así el paso de virus y spam.

Figura 15 Prueba ping de la red



Fuente: Autor

Al realizar una prueba ping a otra máquina de la red con la IP 192.168.1.19 se puede observar los paquetes ICMP enviados al host de destino y se certifica la disponibilidad de la máquina.

13.1 Resultados de las pruebas y análisis

Se puede observar que al utilizar la herramienta Nmap que es una herramienta para exploración de puertos y servicios de red, se evidencian los problemas que presenta la red en cuanto a seguridad y se detectan falencias en los puertos tcp de una de las máquinas de la red.

Entre los puertos abiertos más significativos que se muestran son: el puerto 135 Servicio RPC que se utiliza para asistencia de acceso remoto telefónico y es utilizado para espiar la actividad de los usuarios y regular la transferencia del ancho de banda.

Así mismo está abierto el puerto 139 que es un dispositivo de programación en red. Se utiliza como una aplicación en un computador remoto y es asignado a NetBIOS utilizado para el intercambio de archivos. Al estar este puerto abierto

hace que la red sea vulnerable por los virus Chode, el Gusano Mensaje de Dios, Netlog, Msninit, Qazsadmind, Red y SMB Relay.

Al efectuar el comando ping se evidencia que la conexión de la maquina atacante con la maquina destino es exitosa y esto se facilitaría para que los atacantes hicieran un ataque masivos de ping, generando que la maquina se dedique a responder estos paquetes y el resto de servicios quedaría sin recursos.

Al implementar la herramienta Snort en la red como medida de prevención contra intrusos, Snort genera alertas para cuando estos puertos se encuentran abiertos y cuando se está realizando un ping al host, registrando el análisis y almacenándolo para un posterior análisis más detallado y así poder obtener la dirección IP del computador de donde se realiza el ataque entre otras opciones de análisis.

En Snort se pueden habilitar las reglas con los servicios para detectar ataques como dns, ftp, ataque de denegación de servicios, virus, ataques web, etc.

El motor de detección de Snort, su versatilidad en los diferentes entornos de la red, los análisis de logs y las opciones de configuración, además la gran cantidad de filtros, patrones predefinidos y también la constante actualización de sus actividades nos dan las pautas para decir que éste es una de las mejores alternativas para la detección de intrusos que se pueden implementar.

CONCLUSIONES

El proyecto se desarrolló con el fin de hacer una propuesta para la implementación del IDS en la Sede Central del INPEC.

Se hizo un estudio de seguridad en la red que maneja la Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC utilizando el software para auditoria de redes Nmap y se pudo determinar que la red está a la merced de ataques e intrusiones que pueden llevar a una pérdida importante de su activo más valioso la información.

En el desarrollo del trabajo se realizó un breve estudio de las características, clasificación y arquitectura de un IDS.

Se han hecho propuestas de localización del IDS colocándolo en varios puntos de la red, para que en un futuro puedan instalarlos cuando la Institución opte por este sistema de seguridad en sus redes.

La utilización del IDS, Snort es una parte importante para mejorar la seguridad de la red, pero no es suficiente por sí solo, es necesario combinarlo con otro tipo de dispositivos de seguridad y con otras aplicaciones, como antivirus además se debe mantenerse actualizado, todo el software instalado.

Se consultaron los diferentes productos de uso comercial relacionados con los sistemas de detección de intrusos además se ejecutó una prueba a la red y se pudo determinar que la propuesta que se ha escogido fue SNORT ya que este software es de gran aceptación, potente y gratuito, multiplataforma y de código abierto.

BIBLIOGRAFÍA

ACID en las bases de datos. Recuperado. Marzo de 2015 de http://www.dosideas.com/noticias/base-de-datos/973-acid-en-las-bases-de-datos.html

Administración de Sistemas Operativos. *IDS basados en hots (HIDS).* Recuperado Junio de 2014 de http://www.adminso.es/index.php/4.2.5._IDS_basados_en_host_%28HIDS%29

AGUILAR MARTÍNEZ, Gustavo. *Sistema Detección de Intrusos para una red inalámbrica de una PyME*. Recuperado de: http://tesis.ipn.mx:8080/xmlui/handle/123456789/5863

Como hacer una tesis. Recuperado Marzo de 2015 http://www.unicauca.edu.co/ai/Investigacion/TesisDoctorales.pdf > [citado en 06]

DIDS (Distributed Intrusion Detection System) − *Motivation, Architecture, and An Early Prototype*. Recuperado Junio de 2014 de: http://seclab.cs.ucdavis.edu/papers/DIDS.ncsc91.pdf

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Subdirección de Seguridad de la Información/UNAM-CERT. Instalación de Snort, MySQL y ACID para Windows. Universidad Nacional Autónoma de México

EL MODELO DE REFERENCIA OSI Recuperado Junio de 2014 de http://www2.rhernando.net/modules/tutorials/doc/redes/osi.html

GONZALEZ GOMEZ, Diego. Sistemas de Detección de Intrusiones. Barcelona. 2003. P. 17-18

GONZALEZ MARQUEZ, Vanessa Eleana. Detector de intrusos basado en sistema experto. Trabajo de grado. [Maestro en ciencias en ingeniería de cómputo con opción en sistemas digitales]. Instituto Politécnico Nacional de México. Centro de Investigación en computación.

INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO (2014). Recuperado Mayo 2014 de: http://www.inpec.gov.co/portal/page/portal/Inpec Intercomunicación y seguridad en redes. Recuperado Junio de 2014 de http:// lordratita.wordpress.com/2012/07/page/2/

JIMENEZ GARCIA, María Isabel. Utilización de sistemas de Detección de intrusos como elemento de seguridad perimetral. Trabajo de grado. [Ingeniero en Informática]. Universidad de Almería. Ingeniería Informática

MAESTRE VIDAL, Jorge. Sistema de Detección de Anomalías de red basado en el procesamiento de Payload. Madrid. 2012. Trabajo de grado [Ingeniero de software].Universidad Complutense Madrid. Facultad de Informática.

MAYO QUEVEDO, Roberto. (2009). *Implementación de un Sistema de Prevención de Intrusos (ips) basado en Linux Fedora en la Base Aérea Lago Agrio.* Recuperado de http://repositorio.utc.edu.ec/handle/27000/1125

MINTIC. *Seguridad TI*. Recuperado Junio de 2014 de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html

MIRA ALFARO, Emilio José. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. Trabajo de grado. [Ingeniero Informático]. Universidad de Valencia. Ingeniería Informática.

MONTAÑA, Rogelio. (2014).*Proyecto Final de Carrera. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia.* Recuperado de http://webcache.googleusercontent.com/search?q=cache:btBFGTPfGhIJ:www.rediris.es/cert/doc/pdf/ids-uv.pdf+&cd=1&hl=es&ct=clnk&gl=co

MySQL.Recuperado Marzo de 2015 de http:// www.mysql.com/Enterprise Edition. (commercial)/

SNORT. Recuperado Marzo de 2015 de http://www.snort.org//. 2015 Cisco and/or its affiliates

ANEXOS

ANEXO A.

PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCION DE INTRUSOS (IDS) EN LA DIRECCION GENERAL SEDE CENTRAL DEL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO INPEC"PIDSINPEC"

CUESTIONARIO

Autor: Gilberzon Garzón Padilla

Fecha:

Nombre:

Cargo:

Dependencia:

INSTRUCCIONES

- ***Por favor lea cuidadosamente cada una de las preguntas y solamente luego de que las haya comprendido, proceda a marcar con una X.***
- ***A cada pregunta le corresponde solo una alternativa de respuesta.***
- ***Si marca dos o más alternativas se invalida la respuesta.***
- ***Si aparecen tachones o borrones se invalida la repuesta.***

PREGUNTA No 1
¿Cómo cree usted que la red del sistema de la Sede Central funciona actualmente?

MUY BIEN ☐ **BIEN** ☐ **DEFICIENTE** ☐ **MUY DEFICIENTE** ☐

PREGUNTA No 2
¿Usted sabe que es un ataque informático?

SI ☐ **NO** ☐

PREGUNTA No 3
Tiene conocimiento si existe algún procedimiento sobre el mantenimiento al hardware y software de la red.

SI ☐ NO ☐

PREGUNTA No 4
¿Conoce los diferentes ataques a los que puede estar expuesto un sistema o red?

SI ☐ NO ☐ ALGUNOS ☐ NO RESPONDE ☐

PREGUNTA No 5
¿Sabe cuándo un sistema informático está siendo atacado?

SI ☐ NO ☐ NO RESPONDE ☐

PREGUNTA No 6
¿En caso de sospechar cuando el sistema está siendo atacado sabe realmente que hacer?

SI ☐ NO ☐

PREGUNTA No 7
¿Sabe usted que es un Sistema de Detección de Intrusos (IDS) y para qué sirve?

SI ☐ NO ☐ NUNCA LO HE ESCUCHADO ☐ NO RESPONDE ☐