UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMATICOS

Seminario de Graduación: Seguridad Informática

Tema:

"SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA EL CONTROL DE LA VULNERABILIDAD EN LOS SERVIDORES DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO"

Trabajo de Graduación. Modalidad: Seminario presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Daniel Fernando Yánez Guevara

TUTOR: Ing. M.sc. David Omar Guevara Aulestia

Ambato - Ecuador

Abril-2013

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema "**SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA EL CONTROL DE LA VULNERABILIDAD EN LOS SERVIDORES DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO**", del señor DANIEL FERNANDO YÁNEZ GUEVARA, estudiante de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato Abril 25, 2013

EL TUTOR

_____

Ing. M.sc. David Guevara

AUTORÍA

El presente trabajo de graduación titulado "**SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA EL CONTROL DE LA VULNERABILIDAD EN LOS SERVIDORES DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO**". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Abril 25, 2013

_____

Daniel Fernando Yánez Guevara

CI: 1804487732

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Luis Solís e Ing. Renato Urvina, revisó y aprobó el Informe Final del trabajo de graduación titulado "**SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA EL CONTROL DE LA VULNERABILIDAD EN LOS SERVIDORES DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO**", presentado por el señor Daniel Fernando Yánez Guevara de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Edison Álvarez
PRESIDENTE DEL TRIBUNAL

Ing. Luis Solís
DOCENTE CALIFICADOR

Ing. Renato Urvina
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo se lo dedico a Dios por todas las oportunidades que me brinda día a día, a mi madre y hermanos que han estado conmigo en los buenos y malos momentos por ser un ejemplo en mi vida y enseñarme que con esfuerzo, perseverancia y dedicación nada es imposible, a Cristina por la paciencia, apoyo y ayuda brindada durante esta etapa de mi vida.

AGRADECIMIENTO

A la Facultad de Ingeniería en Sistemas, Electrónica e Industrial y a cada uno de los docentes que durante los años de estudio supieron brindarme con calidad el conocimiento necesario para hoy en día desempeñarme como un profesional, al ingeniero. David Guevara por la excelente enseñanza que supo compartir en las aulas y la colaboración para la culminación del presente proyecto, al ingeniero Eduardo Chazo por la apertura y colaboración brindada para la realización del presente proyecto

Daniel Fernando Yánez Guevara

ÍNDICE

ÍNDICE DE GRÁFICAS

INDICE DE TABLAS

RESUMEN EJECUTIVO

El tema del presente trabajo es sistema de detección y prevención de intrusos para el control de la vulnerabilidad en los servidores de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

El departamento de administración de redes de la FISEI es el ente encargado de las redes y equipos servidores que mantienen la información de sistemas y datos de la FISEI. Por tal motivo, en el presente trabajo de investigación se describe los pasos necesarios para la implementación de un sistema de detección y prevención de intrusos basados en software libre, el cual permite mantener un historial e información en tiempo real sobre posibles intentos de accesos o intentos de vulnerabilidad de los servidores por parte de usuarios no autorizados, mediante la configuración de reglas que se adapten a las necesidades reales del departamento de administración de Redes de la FISEI.

Para cumplir con el objetivo planteado, el presente proyecto se encuentra estructurado de seis capítulos que se detallan a continuación:

Capítulo I. EL PROBLEMA, como su nombre lo indica describe el problema en sí, su respectivo análisis y justificación como también los objetivos.

Capítulo II. MARCO TEÓRICO, contiene la fundamentación legal, las categorías fundamentales que es la base de la investigación y la hipótesis.

Capítulo III. METODOLOGÍA, se enfoca en el tipo de investigación, la Operacionalización de variables, la población y la muestra.

Capítulo IV. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS, presenta el análisis de resultados junto con su interpretación los resultados.

Capítulo V. CONCLUSIONES Y RECOMENDACIONES, muestra las conclusiones a junto con las respectivas recomendaciones de acuerdo al estudio realizado.

Capítulo VI. PROPUESTA, determina los pasos a seguir para el desarrollo de los objetivos.

Por último se encuentran los anexos con contienen el modelo de la encuesta aplicada para la investigación, el croquis de la ubicación en donde se realizó la investigación, instalación de CentOS y programas adicionales utilizados en el presente proyecto.

INTRODUCCIÓN

La seguridad de la información es un tema de vital importancia para el departamento de sistemas de cualquier institución, el crecimiento de la tecnología y la facilidad para obtener información hoy en día, obliga a las instituciones a tomar medidas de seguridad adicionales y prevenir posibles ataques por personas ajenas a la misma.

Los sistemas de detección y prevención de intrusos permiten vigilar y analizar la actividad de los usuarios de la red de datos y mantener un control sobre posibles intentos de intrusión en los sistemas de información; sirven como un complemento a las herramientas tradicionales utilizadas para la seguridad, permitiendo a los administrador detectar y prevenir posibles ataques en la red de datos.

Por este motivo es necesario la implementación de IDPS para mantener un mejor control y administración de la información alojada en los servidores de la FISEI y de esta manera detectar y prevenir vulnerabilidades en los quipos servidores que conforman parte de la misma.

CAPITULO I

1. EL PROBLEMA

1.1. Tema:

Sistema de Detección y Prevención de Intrusos para el control de la vulnerabilidad en los servidores de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

1.2. Planteamiento del Problema

1.2.1. Contextualización

En la actualidad a nivel mundial las empresas se enfrentan cada vez más con riesgos e inseguridades procedentes de una variedad de fuentes que pueden causar daños a gran escala en los sistemas de información y pueden poner en peligro la continuidad de un negocio.

Es cada vez más común que personal tanto externo como interno de una empresa, intente vulnerar los sistemas de información, con el objetivo de conseguir información importante que permitan de alguna manera sacar provecho de la información obtenida.

En la actualidad, ya no es suficiente la seguridades que nos brindan los routers, firewall y los antivirus tradicionales, debido al avance de la tecnología nuevos ataques siguen apareciendo y van a apareciendo nuevas maneras de vulnerar este tipo de herramientas, es por este motivo de la necesidad de nuevas herramientas de seguridad que permitan controlar, detectar, prevenir y responder a posibles ataques perpetuados por delincuentes informáticos.

"La seguridad de la información en Latinoamérica es, en términos generales y salvo excepciones en verticales como el sector financiero, el de tecnología, o el petrolero, algo inmadura y rezagada respecto a otras regiones del mundo, debido a que las organizaciones aún no le dan la importancia estratégica que ésta tiene."[1]

En Latinoamérica la seguridad de la información es considerada como parte exclusiva del área de tecnología, es por este motivo que latinoamérica es un mercado en crecimiento en el área de seguridad, que poco a poco va tomando la importancia que esta debe tener en la parte de aseguramiento de sistemas e infraestructura. Se puede considerar que en grandes empresas de sudamérica el tema de seguridad es considerado como importante sin embargo, en pequeñas y hasta incluso en algunas medianas empresas que no poseen departamentos de sistemas correctamente estructurados, la seguridad de la información no es considerada como una prioridad debido a los presupuestos que en ellas se manejan.

"*En el Ecuador Durante el año 2010 las estadísticas nos muestran que han existido 866 delitos informáticos, este número ha ido en aumento durante el presente año mostrando la mayor cantidad de ataques en las principales provincias del país como son Pichincha y Guayas con el 45% y 28% respectivamente y mostrando a Tungurahua como la cuarta provincia más afectada con un 3% por delitos informáticos."* [2]

Existen personas que aprovechan las herramientas informáticas y de la poca seguridad que se brinda a la información en entidades públicas, para poder adquirir la información que en ella se maneja. Es por esto la necesidad de resguardar este bien mediante la implementación de software que brinde la protección necesaria para los equipos.

La Facultad de Ingeniería en Sistemas Electrónica e Industrial almacena su información en los servidores alojados en el departamento de Redes. Este es el ente encargado del manejo de los datos y la correcta administración y servicios que brinda la FISEI a los estudiantes. En la actualidad cuenta con equipos servidores que manejan la información de estudiantes, docentes y personal administrativo que conforman la misma. No poseen adecuados sistemas de control de información, lo que hace que estén expuestos a ataques informáticos por posibles vulnerabilidades en los puertos, permitiendo el fácil acceso a la información de los docentes y estudiantes. De esta manera la información se encuentra amenazada, perdiéndose de esta manera la privacidad de los usuarios.

1.2.2. Árbol del Problema

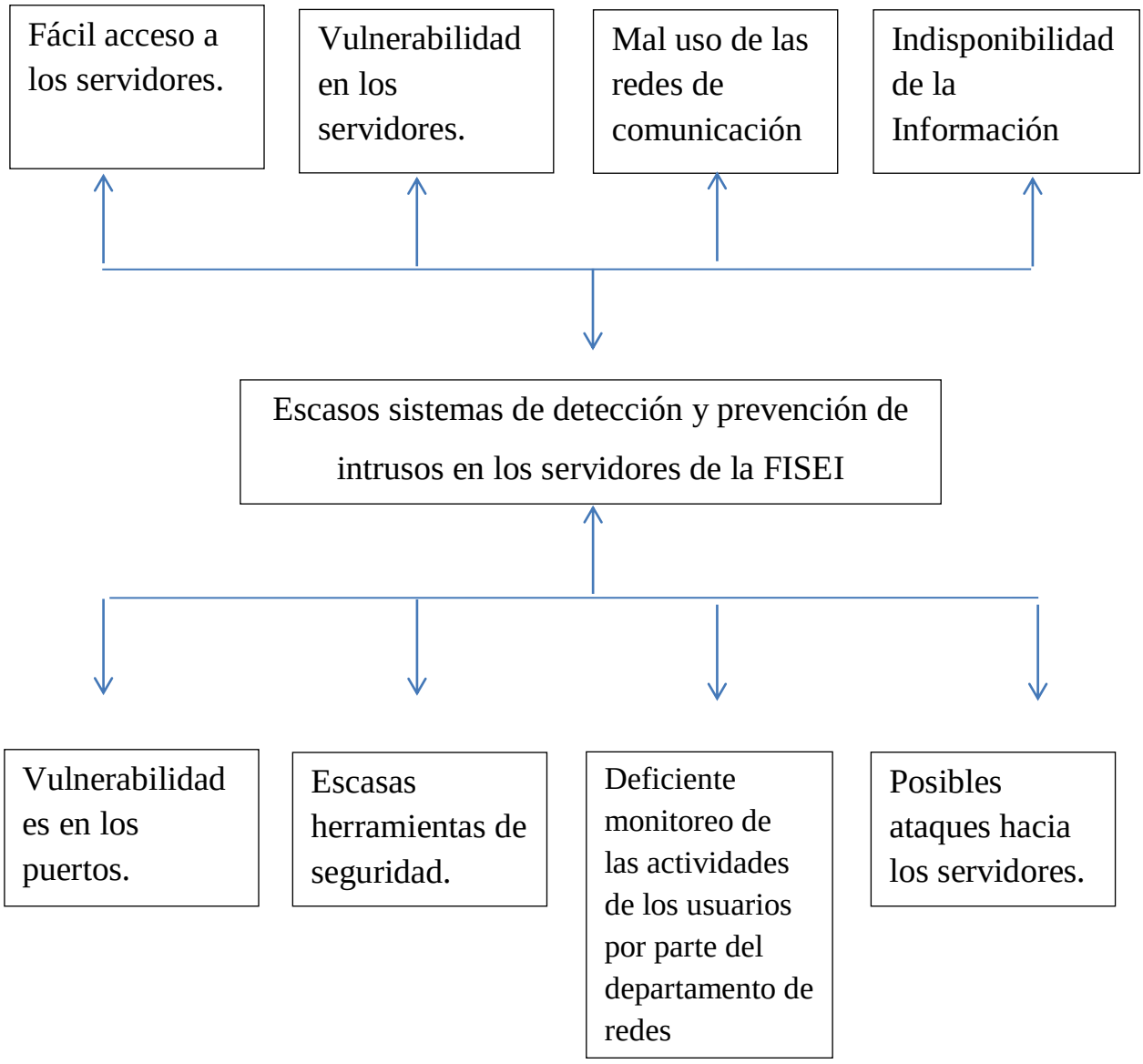


Gráfico 1.1 Árbol del Problema

1.2.3. Análisis Crítico

El constante cambio de la tecnología y la seguridad es un tema de vital importancia hoy en día en cualquier institución ya sea pública o privada. La información se considera como un recurso importante para el correcto

funcionamiento de cualquier entidad, es por esta razón que en las empresas hoy en día el mantener la información segura se convierte en una prioridad.

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato cuenta con equipos servidores, routers, switch, access point los cuales poseen herramientas que brindan seguridades a las redes, hoy en día encontramos gran cantidad de ataques que pueden vulnerar la seguridad de estas herramientas, es por este motivo que al existir escasas herramientas de seguridad en los servidores y redes de la FISEI puede ser una puerta de fácil acceso a los intrusos que poseen poco conocimiento. La falta de configuraciones de los equipos servidores provoca que cualquier persona ya sea estudiante o los mismo docentes, puedan alterar algún registro como puede ser en el sistema de control de docentes y administrativos, la misma que maneja el departamento de administración de redes.
Además esto implica que puedan existir vulnerabilidades en los puertos ya que no se tiene un control o escaneo periódicamente y esto puede provocar fácil acceso a los servidores.

Esto además del escaso monitoreo por parte de la administración hacia los usuarios produce que exista desconocimiento y poco control de las actividades que ellos realizan al momento de utilizar los equipos y de esta manera es propenso a ataques que con llevaría a la indisponibilidad de los datos al momento de ser necesarios.

1.2.4. Prognosis

En caso de no implementarse un Sistema de Detección y Prevención de Intrusos para el control de las vulnerabilidades en los Servidores de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial seguirán las inseguridades en los equipos servidores y la facilidad de acceso a los datos, lo cual al ser una facultad ligada al tema de sistemas y seguridades debe ser la primera en brindar

seguridades en sus redes de datos, ya que al existir ataques a la misma se podría dar un desprestigio de la misma en la Universidad.

1.2.5. Formulación del Problema

¿Como los escasos sistemas de detección y prevención de intrusos influyen en la vulnerabilidad de la información en los servidores de la FISEI?

1.2.6. Preguntas Directrices

- ¿Existen vulnerabilidades en la red de datos de la FISEI?
- ¿Qué Sistemas de Detección y Prevención de Intrusos de software libre se ajustan a las necesidades del Departamento de redes?
- ¿Qué configuraciones son necesarias para brindar seguridad a la red de datos de la FISEI?

1.2.7. Delimitación

Teórico:

- **Campo:** Seguridad Informática.
- **Área:** Seguridad de la Información.
- **Aspecto:** Sistemas de detección y prevención de intrusos

Espacio:

La presente investigación se desarrollara en el departamento de administración de redes de la FISEI.

Tiempo:

La investigación propuesta se desarrollara en un período de 12 meses a partir de la aprobación del proyecto.

1.3. Justificación

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial trabaja con servicios de internet, redes inalámbricas, redes físicas para la facilidad de obtener información por parte de estudiantes y docentes, desde cualquiera de las dos edificaciones que posee la misma, por este motivo es de gran importancia proteger la información de la institución mediante correctas configuraciones de herramientas de seguridad que nos brindan constante monitoreo de las redes ante posibles ataques y de esta manera detectar y ejecutar soluciones adecuadas al problema.

La FISEI cuenta con equipo servidores los cuales contienen información y aplicaciones almacenadas en las mismas, no posee herramientas de seguridad que nos permitan obtener información sobre posibles ataques o intentos de intrusión ni tampoco herramientas que nos permitan mantener un control sobre el uso que los usuarios (docentes, estudiantes y administrativos) dan a los servicios que proporciona la red, es por este motivo que existe la necesidad de realizar un análisis de vulnerabilidades que permitan identificar los puntos vulnerables de los servidores y de la misma manera permita corregir y controlar la información que los usuarios.

El departamento de administración de redes además de la Facultad de Ingeniería en Sistemas Electrónica e Industrial son los principales beneficiados con el presente proyecto ya que al ser una Facultad ligada al tema informático es importante mantener el prestigio que esta mantiene a nivel de la provincial y del país.

1.4. Objetivos

General

- Implementar un sistema de detección y prevención de intrusos mediante el uso de software libre que evite la vulnerabilidad de la información de los servidores de la FISEI.

Específicos

- Analizar la situación actual de la red de datos de la FISEI buscando vulnerabilidades de la información en los servidores.

- Estudiar un Sistema de Detección y Prevención de Intrusos basado en software libre que se ajuste a las necesidades del departamento de Redes de la FISEI.

- Plantear una solución que permita realizar la configuración de un sistema de detección y prevención de intrusos identificando las inseguridades que eviten la vulnerabilidad de la información de los servidores de la FISEI.

CAPITULO II

2. MARCO TEÓRICO

2.1. Antecedentes Investigativos

Revisando los archivos de la biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial se puede constatar que existen temas similares al que se está planteando el cual se detalla a continuación:

Autores: Leonor Margarita Carrillo Crespo
Tema: Sistema de Detección y Prevención de Intrusos para mejorar la seguridad de datos e información de UNIFINSA
Año: 2010
Lugar: Reposa en la Facultad de Ingeniería en Sistemas, electrónica e Industrial
Objetivo General: Establecer un Sistema de Detección y Prevención de Intrusos que mejor se ajuste a las Políticas de Seguridad de Datos e Información de UNIFINSA.

Esta tesis ha sido tomada en cuanta por haber sido realizada en la Universidad Técnica de Ambato y el resultado obtenido es la implementación de un Sistema de Detección y Prevención de Intrusos realizando un análisis de los problemas que presentan las seguridades de la institución y orientada a la realidad de la ciudad.

Revisando los repositorios virtuales de las universidades del país se puede constatar que existen temas similares al que se está planteando el cual se detalla a continuación:

Autores: Gabriela Torres, Diego LLanga
Tema: Estudio e Implementación de un sistema de Prevención de Intrusos en una red LAN.
Año: 2010
Lugar: Reposa en la Escuela Politécnica del Chimborazo
Objetivo General: Estudiar e identificar una metodología de prevención de intrusos en la red corporativa del M.I Municipio de Riobamba con el fin de proteger la información digital privada que allí se maneja.

Se ha tomado en cuenta esta tesis por tener relación con el tema planteado para la investigación, tomando en cuenta las distintas metodologías de IPS y está orientado a la realidad del Ecuador.

Revisando Bibliografía con la cuenta la Biblioteca de la FISEI, se utilizaron los libros Redes de Computadoras tercera Edición Tanembaum Editorial Prentice Hall además, Seguridad Informática y Criptografía de Jorge Ramiro Sexta Edición.

2.2. Fundamentación Legal

ARTÍCULOS DE LA CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DEL ECUADOR RELACIONADOS CON LA SEGURIDAD INFORMÁTICA Y EL USO DEL SOFTWARE LIBRE.

Decreto de Ley 1014

Política de Estado el uso de Software libre en Ecuador

Art. 1: Establecer como política pública para las entidades de administración Pública central la utilización del Software Libre en sus sistemas y equipamientos informáticos.

Art. 2: Se entiende por software libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan el acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas. Estos programas de computación tienen las siguientes libertades:

- Utilización de programa con cualquier propósito de uso común.
- Distribución de copias sin restricción alguna
- Estudio y modificación de programa (Requisito: código fuente disponible)
- Publicación del programa mejorado (Requisito: código fuente disponible.

Art. 3: Las entidades de la administración pública central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para este tipo de software. **Art. 4:** Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo de seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 386.- El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y particulares, empresas públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación y aquellas ligadas a los saberes ancestrales.

El Estado, a través del organismo competente, coordinará el sistema, establecerá los objetivos y políticas, de conformidad con el Plan Nacional de Desarrollo, con la participación de los actores que lo conforman.

Art. 387.- Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.

2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir,.

3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.

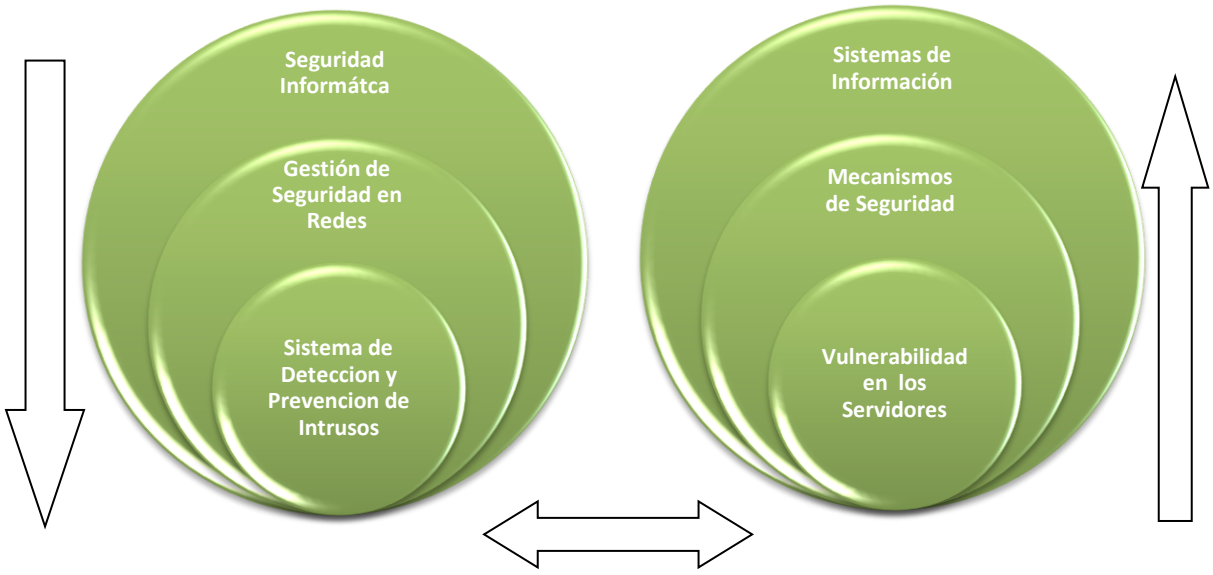
5. Reconocer la condición de investigador de acuerdo con la Ley.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

2.3. Categorías Fundamentales

Marco Conceptual

Categorías Fundamentales



Variable Independiente **Variable Dependiente**

Gráfico 2.2 Categorías Fundamentales

2.4. Constelación de Ideas

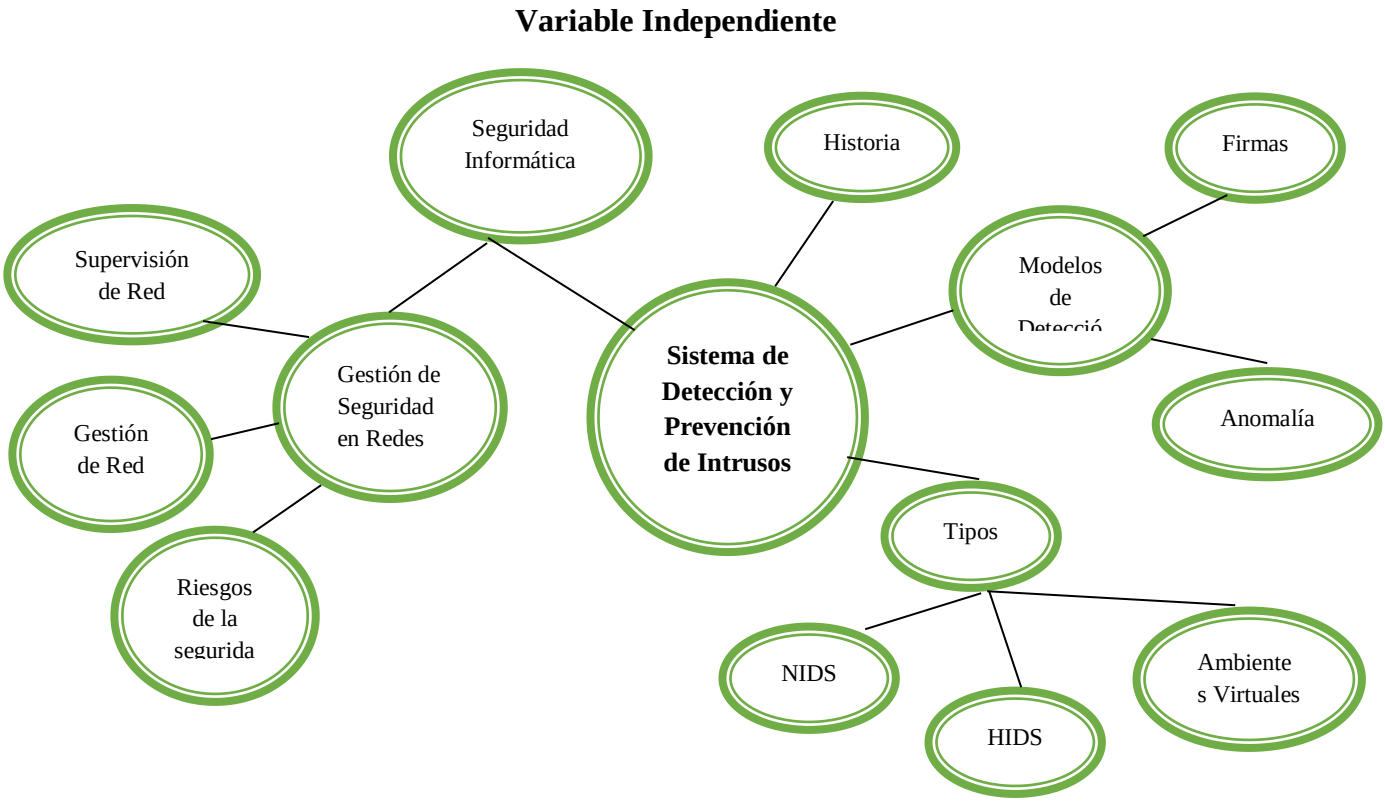


Gráfico 2.3 Constelación de la variable independiente

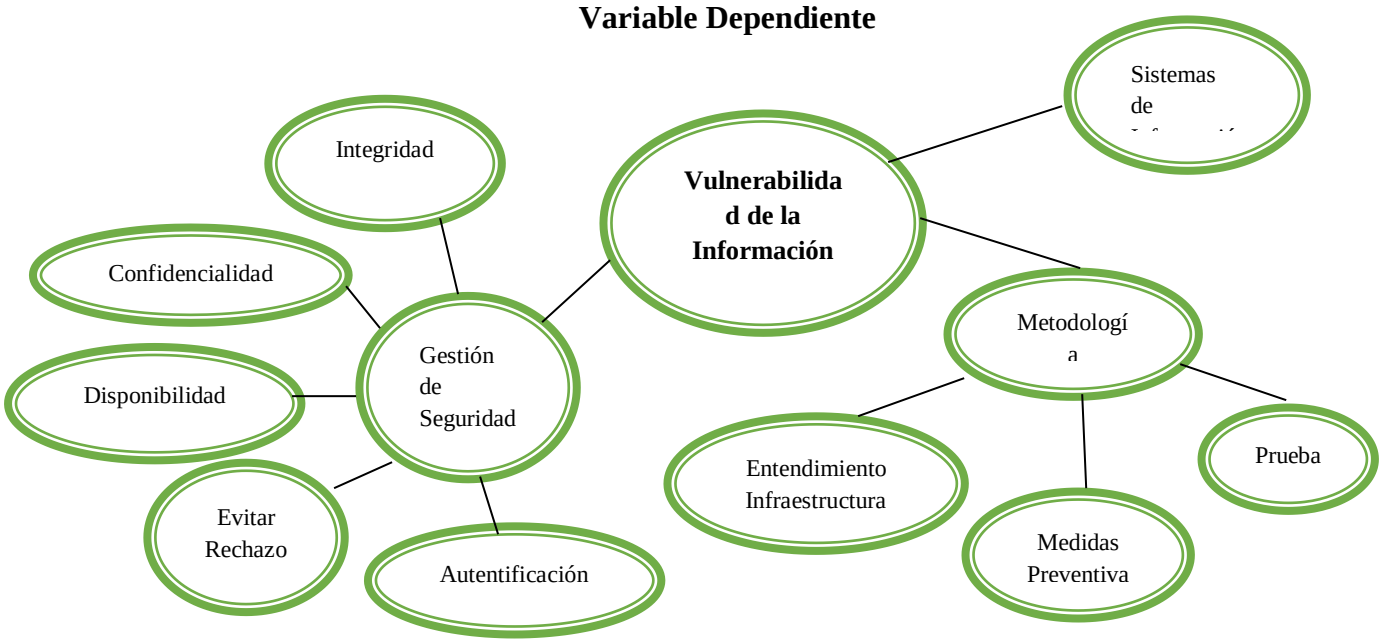


Gráfico 2.4 Constelación de la variable dependiente

2.5. Variable Independiente: Sistema de detección y prevención de Intrusos

2.5.1. Seguridad Informática

"Un sistema informático es seguro si su comportamiento es acorde con las especificaciones previstas para su utilización (dependability).

Seguridad es el estado de bienestar de la información y las infraestructuras, en las cuales la posibilidad que puedan realizarse con éxito y sin detectarse, el robo, alteración y parada del flujo de información, se mantienen en niveles bajos o tolerables." [3]

"Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática." [4]

La seguridad Informática es un área de la informática que se enfoca en la protección de la estructura computacional, nos permite tener confianza de que la información que estamos utilizando se encuentre en un lugar seguro y confiable.

2.5.2. Gestión de Seguridad en Redes

"La gestión se puede definir como el conjunto de actividades que controlan o vigilan el uso de los recursos en la red. Se debe proporcionar la posibilidad de supervisar el estado, medir el rendimiento, reconocer actividades anormales y recuperar el servicio.

Las funciones de red se suelen agrupar en dos categorías

- ***Supervisión de red.*** *Se considera una función de ``lectura'' y se encarga de observar y analizar el estado y el comportamiento de la configuración y componentes de la red.*

- ***Control de red.*** *Se le considera como una función de "escritura" y se encarga de alterar los parámetros de los distintos componentes de la configuración de la red y hacer que lleven a cabo las acciones que se determinen.*

En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales." [5]

Se puede decir, que la gestión de las redes y la seguridad son aquellas actividades que nos permiten mantener un controlar y supervisar el uso de la seguridad y la red de información.

"La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos." [6]

La seguridad informática según los autores citados es una disciplina que relaciona diversas técnicas, aplicaciones y dispositivos cuya principal funciones son

prevenir, proteger y resguardar la información para que siempre esté disponible cumplir los propósitos del usuario.

2.5.3. Riesgos de la Seguridad Informática

*"**Tipos de Riesgos***

Según la clasificación de Shirey se clasifican en 4 que son los siguientes:

- ***Revelación** (disclosure) : Acceso no autorizado a información*
- ***Engaño** (deception) : Admisión de datos falsos*
- ***Perturbación** (disruption) : Interrupción o prevención de correcta operación*
- ***Usurpación**: Control no autorizado de partes del sistema.*

Riesgos Comunes

- ***Fisgoneo (snooping):** Captura no autorizada de información (forma pasiva de revelación).*
  ***Solución:** Servicio de confidencialidad.*

- ***Modificación:** cambio no autorizado de información (engaño, perturbación, usurpación).*
  ***Solución:** servicio de integridad.*

- ***Enmascaramiento:** una entidad hace pasarse por otra (engaño, usurpación).*
  ***Solución:** servicio de integridad*

Una forma permitida de enmascaramiento: Delegación de Autoridad.

- ***Repudiación:*** *Falsa denegación de pertenencia a una entidad (engaño).*
  Solución: *servicio de integridad.*

- ***Denegación de recepción (engaño)***
  Solución: *servicio de integridad.*

- ***Denegación de servicio:*** *inhibición de servicio (usurpación, papel soporte en engaño). Retardo si es de corto plazo (caballos de troya).*
  Solución: *servicio de disponibilidad. "* [7]

Los riesgos son una eventualidad que imposibilita el cumplimiento de un objetivo. De manera cualitativa el riesgo es una medida de las posibilidades de incumplimiento o de exceso del objetivo planteado.

En lo relacionado con tecnología el riesgo, es referenciado como una amenaza que no permite cumplir con los objetivos.

2.5.4. Sistema de Detección y Prevención de Intrusos

Los IDPS son elementos (Hardware - Software) que tiene como objetivo detectar identificar y responder el acceso no autorizado de intrusos, cuyo único objetivo es comprometer la integridad, confiabilidad y disponibilidad de la información.

2.5.4.1. Historia

En el año de 1972 se realiza un informe en los Estados Unidos sobre la seguridad en los sistemas de información para las fuerzas armadas, a partir de aquí se empezaron a realizar estudios tratando de buscar la manera de mejorar la seguridad y vigilancia en los equipos de la institución. En 1980, aparece por primera vez una publicación por James P. Anderson, la cual consistía en una

teoría sobre lo que eran los sistemas de detección de intrusos y de esta manera buscaba automatizar los procesos que podrían llevar a cabo un control de la seguridad.

Entre los años 1984 y 1986 aparece el primer versión de los sistema de detección de intruso denominado IDES, Intrusión Detection Expert System que funcionaba en tiempo real, a partir de aquí se empezó a mejorar este proyecto hasta el año de 1990 que aparece oficialmente el primer Sistema de detección de Intrusos en la Universidad de California llamado NSM (Network Security Monitor), este sistema estaba orientado a trabajar solamente como protección de un computador, a partir de aquí se empieza a ampliar la idea y se lo orienta a las redes de computadores y empiezan a tomar fuerza a partir de la crisis de firewall en el año de 1995.

2.5.4.2. Sistema de Detección de Intrusos – IDS

Los Sistemas de Detección de Intrusos son aquellos que nos permiten identifica el mal uso de los recursos de la red u ordenador mediante el monitoreo de la información (Tráfico-Recursos), la detección (Anomalías e Intrusos) y alertas enviadas al administrador de la red.

Los IDS monitorean no solamente a los equipos sino también a la red de datos pudiendo estar ubicados en cualquier parte de la misma convirtiéndose de esta manera en una fuerte herramienta de seguridad.

2.5.4.3. Sistema de Prevención de Intrusos – IPS

Los sistemas de Prevención de Intrusos son una evolución de los IDS, son aquellos que nos permiten monitorear, detectar y reportar el mal uso de los recursos de una red de computadores con la diferencia que los IPS nos permiten adicionalmente prevenir los ataques de los intrusos. Los IPS realizan análisis más

completos del uso de la red adoptando un enfoque preventivo interviniendo activamente en caso de que en la red existan paquetes maliciosos o dañinos. Además necesita de configuraciones más complejas dependiendo de las políticas que maneje la empresa.

2.5.4.4. Firewall e IDPS

Tanto los IDPS como los firewalls son herramientas creadas para utilizarse en conjunto y ambas permiten proteger la información en tiempo real, Los IDPS son un complemento para los firewalls brinda mayor seguridad a los equipos. Los firewalls se encargan de bloquear a nivel de puertos y protocolos estando atento a los ataques de intrusos que se pueden dar desde el exterior pero no a los ataques que se ejecutan en la red interna. Los IDPS buscan ataques en el propio firewall ya que existen ataques que no son controlados por los firewalls.

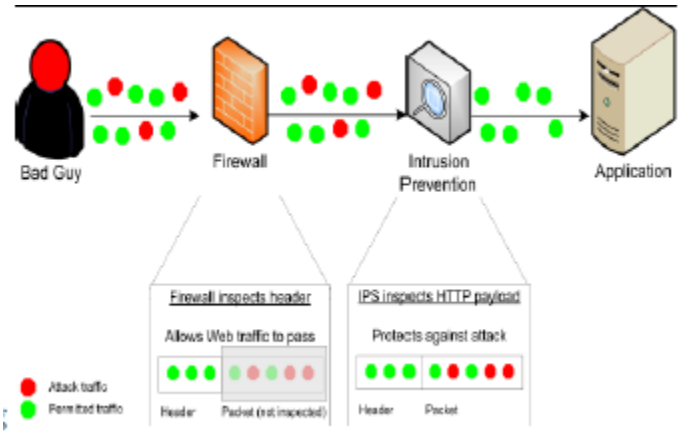


Gráfico 2.4 Firewall e IDPS

En la Gráfico 2.3 podemos observar cómo tanto el firewall como los IDPS son un complemento mutuo, En el ejemplo vemos que se envía un ataque en el cual los puntos de color verde es la información normal y los rojos es el contenido maligno, el firewall deja pasar el paquete ya que el encabezado del paquete es normal pero los IDPS verifica que el paquete contiene datos malignos y lo bloque para que no pueda pasar.

2.5.4.5. Modelos de Detección de los IDS

Se los clasifica de la siguiente manera:

2.5.4.5.1. Detección Basada en Firmas

Los IDS contienen una base de datos de firmas que se encargan de detectar si existe algo anormal estos tienen la capacidad de reconocer determinadas cadenas dentro de los paquetes que son enviados. Estas firmas deben ser actualizadas constantemente por los proveedores ya que si existen nuevos ataques deben generarse las firmas indicando la información de cómo actúa el ataque, para que los IDS puedan bloquearlo.

2.5.4.5.2. Detección Basada en Anomalías

Estos tipos de detección analizan el tráfico de la red para tomar una decisión. Se los puede clasificar en tres que son:

Perfiles Definidos: Son aquellos en los cuales ya vienen definidos por los proveedores.

Perfiles Estadísticos: El IDS analiza el tráfico que se genera en la red por un determinado tiempo y almacena esta base para posteriormente compararla. Cuando el tráfico cambia demasiado, se genera una alarma.

Perfiles Dinámicos: Son aquellos en los cuales el administrador es la persona quien define el patrón normal de tráfico, pero es susceptible a generar muchos falsos positivos.

Análisis de Estado de Protocolos: Verifican como determinados protocolos pueden ser usados o no.

2.5.4.6. Tipos de IDS

Esto hace referencia a la forma como vamos a utilizar los IDS en nuestra organización, este se divide en 4 grupos importantes que son los siguientes.

- Sistema de Detección de Intrusos Redes- NIDS
- Sistema de Detección de Intrusos Equipos - HIDS
- Sistema de Detección de Intrusos IDS en Ambientes Virtuales.

2.5.4.6.1. NIDS

Los IDS en las redes controlan todo el tráfico en los segmentos de las redes y también pueden controlar el tráfico y recolectando información en los equipos, analizan protocolos de red, aplicaciones y transporte en busca de actividades peligrosas, estos se presentan como equipos o como software.

2.5.4.6.2. HIDS

Los HIDS nos ayudan a controlar la información que se maneja en los equipos y son complementarios a los antivirus. Los HIDS van detectando las anomalías que existen en los sistemas para que los usuarios no roben información, este va chequeando la integridad de los sistemas, si archivos fueron modificados, monitoreando tráfico inalámbrico y algunos pueden controlar el tráfico cifrado de la red.

2.5.4.6.3. IDS en Ambientes Virtuales

En el caso de los IDS en Ambientes Virtuales estos son aplicados en nuevos escenarios como son los ambientes virtuales y cloud computing. Los ambientes virtuales están por fuera de las estructuras físicas de seguridad, estos ambientes

fomentan el ahorro de energía, baja costo en equipamiento y mantenimiento y reduce el espacio físico.

2.5.4.7. Uso de los IDPS

- Los IDPS se encargan del control de las políticas de seguridad.
- Los IDPS son un complemento para los Firewall.
- Los IDPS bloquean el paso de código maligno que no fue detectado por el firewall.
- Los IDPS llevan un registro de Logs de las amenazas detectadas.
- Comprender frecuencia y naturaleza de los ataques.
- Impedir que usuario violen las políticas establecidas por la institución.
- Educar a los administradores de sistemas.

2.6. Variable Dependiente: Vulnerabilidad de la Información en los Servidores

2.6.1. Sistemas de Información

"A través del procesamiento de información, una compañía crea valor, en especial si se trata de una empresa que ofrece servicios. Por lo tanto, en este caso, la información tiene un valor aún mayor porque ayuda a alcanzar los objetivos de la compañía.

*Un **sistema de información** (SI) representa todos los elementos que forman parte de la administración, el procesamiento, el transporte y la distribución de la información dentro de la compañía.*

En términos prácticos, el alcance del término "sistema de información" puede variar notablemente entre una organización y otra y, según el caso, puede abarcar todos o algunos de los siguientes elementos:

- *Bases de datos de la compañía.*
- *Software de gestión integral de empresas (ERP, por sus siglas en inglés).*
- *Herramienta para la Gestión de relaciones con los clientes (CRM, por sus siglas en inglés).*
- *Herramienta para la Gestión de la cadena de suministro (SCM, por sus siglas en inglés).*
- *Solicitudes de empleo.*
- *Infraestructura de red.*
- *Servidores de datos y sistemas de almacenamiento.*
- *Servidor de aplicaciones.*
- *Dispositivos de seguridad.” [8]*

*“Un **sistema de información** es un conjunto organizado de elementos, que pueden ser personas, datos, actividades o recursos materiales en general. Estos elementos interactúan entre sí para procesar información y distribuirla de manera adecuada en función de los objetivos de una organización.” [9]*

Los sistemas de Información es considerada como aquellos servicios que una empresa ofrece a sus empleados que pueden interactuar entre si para poder procesar, analizar y distribuir información para todos sus empleados y clientes.

2.6.2. Mecanismos de Seguridad

“Generalmente, los sistemas de información incluyen todos los datos de una compañía y también en el material y los recursos de software que permiten a una

compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos." [10]

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en cinco mecanismos principales:

- **Integridad**: garantizar que los datos sean los que se supone que son.
- **Confidencialidad**: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- **Disponibilidad**: garantizar el correcto funcionamiento de los sistemas de información.
- **Evitar el rechazo**: garantizar de que no pueda negar una operación realizada.
- **Autenticación**: asegurar que sólo los individuos autorizados tengan acceso a los recursos

2.6.2.1. Confidencialidad

Consiste en que la información solamente debe ser accedida por personal autorizado dentro de la institución.

Este puede ser el resultado de medidas de seguridad escasas o fugas de información por parte del personal. Un ejemplo de medidas de seguridad escasas

sería: el envío de un correo con información sensible y que llegue a una persona que no era la destinataria.

2.6.2.2. Integridad

Consiste en prevenir la modificación errónea de la información. Los usuarios autorizados son probablemente la causa más grande de errores, omisiones y alteración de información. El almacenamiento de información incorrecta dentro del sistema puede ser tan malo como perder información. Atacantes maliciosos también pueden medicar, eliminar o corromper información que es vital para la operación correcta de las funciones de negocios. Un ejemplo la encriptación MD5 para verificar que el software sea íntegro y no haya sido modificado con anterioridad.

2.6.2.3. Disponibilidad

Consiste en prevenir la retención no autorizada de información o recursos. Esto no sólo aplica al personal que retiene información. La información deberá estar tan libremente disponible como sea posible para los usuarios autorizados, las 24 horas del día.

2.6.3. Vulnerabilidad de la Información en los Servidores

Según Rodrigo Ferrer (Internet; 26/05/2011; 01/11/2011; 15:25) Una vulnerabilidad, se puede definir como un estado de un sistema (o conjunto de sistemas) que puede:

- Permitir a un atacante acceder a información confidencial.
- Permitir a un atacante modificar información.

- Permitir a un atacante negar un servicio.

Una de las preocupaciones más importantes de los profesionales de la seguridad de la información es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas tecnológicos, las cuales son el blanco predilecto de herramientas de software cada vez más poderosas en su capacidad de ocasionar daños a los sistemas de información y la infraestructura que los soporta.

2.6.4. Metodología para el análisis de vulnerabilidades

El análisis de vulnerabilidades el cual complementa el proceso de análisis de riesgo, es una actividad fundamental con el fin de orientarnos hacia un sistema de gestión de la seguridad de la información, el cual debería comprender las siguientes actividades:

2.6.4.1. Entendimiento de la Infraestructura

Se busca, identificar cada uno de los dispositivos de hardware o software residentes en la infraestructura que soportan los procesos del negocio. Esta selección debe iniciarse con los servicios prestados, continuar luego con los procesos asociados a estos servicios y de allí, determinar los activos o dispositivos que soportan estos procesos.

A manera de ejemplo, dentro de los posibles elementos de la infraestructura que un momento dado pudieran llegar a albergar vulnerabilidades a nivel de software tenemos los siguientes:

- Servidores
- Aplicaciones
- Estaciones de trabajo
- Bases de datos
- Firewalls

- Enrutadores

2.6.4.2. Pruebas

Se deberá realizar una clasificación de activos o dispositivos con base en la confidencialidad de la información que guardan y la importancia del activo.

Por medio del uso de herramientas para la detección de vulnerabilidades, las cuales pueden ser tanto de software para correr sobre sistemas operativos tradicionales o poseer un hardware específico.

Una vez seleccionada la herramienta, se debe tomar una decisión costo- beneficio. Se pueden crear categorías y agrupar servidores o estaciones de trabajo, siempre y cuando se cuente con la certeza que aquellos seleccionados para esta agrupación, comparten más de un 90 % de similitud en su configuración con los otros que no serán inspeccionados.

2.6.4.3. Medidas Preventivas

Una vez determinado el universo de la prueba se tomarán las medidas preventivas adecuadas para su ejecución, con el fin de prevenir efectos adversos sobre la prestación de los servicios; entre ellas, podemos resaltar:

- Definir hora adecuada de pruebas
- Horas de bajo tráfico
- Horarios de no prestación de servicios, si esto fuera posible
- Análisis sobre la no disponibilidad de activos críticos de la prueba
- Tomar algunas medidas de contingencia
- Realizar monitoreo de los servicios durante las pruebas
- Tiempos de respuesta excesivos
- Eventos o incidentes de seguridad
- Se debe informar a operaciones de la realización de las pruebas

- Se debe monitorear el tráfico de la red
- Utilización de los segmentos críticos
- Informar a los dueños de los activos

2.7. Hipótesis

La implementación de un sistema de detección y prevención de intrusos influirá en la seguridad de la información interna y confidencial de la FISEI.

2.8. Señalamiento de las Variables

Variable Independiente: Sistema de detección y prevención de Intrusos

Variable Dependiente: Vulnerabilidades en los servidores

CAPITULO III

3. METODOLOGÍA

3.1. Enfoque

El presente trabajo investigativo tomara un enfoque Cuali – Cuantitativo con las siguientes consideraciones:
Naturalista debido a que no atenta contra la naturaleza.
Participativo ya que en él se considera a las personas que trabajan en el medio y quienes están dentro del mismo.
Etnográfica debido a que se estudia las necesidades de acuerdo al trabajo diario realizado dentro del departamento de sistemas.
Normativa porque va a cumplir con ciertas normas.

3.2. Modalidades básicas de la investigación

La presente investigación tiene las siguientes modalidades:

Modalidad Bibliográfica o Documentada: Se ha considerado esta modalidad ya que se ha utilizado el internet como principal recurso para obtener información en los cuales se ha podido encontrar en documentos, revistas, tesis de grado de distintas universidades del país información acerca del tema propuesto.

Modalidad Experimental: Se ha considerado la relación de la variable independiente sistemas de detección y prevención de Intrusos y su influencia y relación en la variable dependiente vulnerabilidad en los servidores, para considerar sus causas y sus efectos.

Modalidad de Campo: se ha considerado esta modalidad ya que el investigador ira a recoger la información primaria directamente de los involucrados a través de una encuesta.

3.3. Tipos de Investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de la investigación ¿Como los escasos sistemas de detección y prevención de intrusos influyen en la vulnerabilidad en los servidores de la FISEI? Como de la misma manera ayudo a plantear la hipótesis la implementación de un sistema de detección y prevención de intrusos influirá en la seguridad de la información interna y confidencial de la FISEI.

Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar el tiempo y en espacio construyendo el análisis crítico la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación correlacional ya que ha permitido medir la compatibilidad de variable independiente sistema de detección y prevención de intrusos con la variable dependiente vulnerabilidad en los servidores.

3.4. Población y Muestra

La población considerada para la presente investigación son los beneficiaron del presente proyecto, el personal encargado del departamento de Administración de Redes de la FISEI la cual está conformada por 7 personas.

Cantidad	Cargo	Departamento
1	Administrador de Redes	Administración de Redes
4	Laboratorista Sistemas	Administración de Redes
1	Laboratorista Industrial	Administración de Redes
1	Laboratorista Electrónica	Administración de Redes

Tabla 3.1 Empleados Departamento de Sistemas

3.5. Operacionalización de variables

Hipótesis: La implementación de un sistema de detección y prevención de intrusos influirá en la seguridad de la información interna y confidencial de la FISEI.

Variable Independiente: Sistema de detección y prevención de Intrusos

Concepto	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
Los IDPS son elementos (Hardware - Software) que tiene como objetivo detectar identificar y responder el acceso no autorizado de intrusos.	Hardware	Servidores Estaciones de Trabajo Access Point Routers	¿Con que tipo de hardware cuenta la FISEI?	Encuesta a través de un cuestionario aplicado al departamento de Redes de la FISEI
	Software	Firewall Antivirus IDPS	¿Con que tipo de seguridades cuenta los servidores de la FISEI?	Encuesta a través de un cuestionario aplicado al departamento de Redes de la FISEI
	Acceso no	Estudiantes	Que control	

	autorizado de intrusos	Docentes Administrativos	posee el departamento de Administración de Redes sobre usuarios de la Red?	Encuesta a través de un cuestionario aplicado al departamento de Redes de la FISEI

Tabla 3.2 Operacionalización de Variables – Variable Independiente

Variable Dependiente: Vulnerabilidad en los servidores

Concepto	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
Son las debilidades que se presentan en equipos servidores debido a malas configuraciones que permiten a un atacante tener acceso a información o servicios.	Servidores	Capacidad Marca Cantidad Sistema Operativo	¿Con que tipo de servidores cuenta los la FISEI?	Encuesta a través de un cuestionario aplicado al departamento de Redes de la FISEI
	Configuraciones	Servidores Equipos Routers	¿Con que tipo de configuraciones cuenta la FISEI?	Encuesta a través de un cuestionario aplicado al departamento de Redes de la FISEI
	Atacante	Estudiantes Docentes Administrativos	¿Qué tipo de Ataques pueden ser realizados por los usuarios de la FISEI?	Encuesta a través de un cuestionario aplicado al departamento de Redes de la FISEI
	Información o Servicio	Servicio Web Servicio correo Servidor Proxy Servidor Base de Datos	¿Qué tipo de Servicios proveen los Servidores de la FISEI?	Encuesta a través de un cuestionario aplicado al

	departamento de Redes de la FISEI

Tabla 3.3 Operacionalización de Variables – Variable Dependiente

3.6. Recolección y análisis de la Información

Tipos de Investigación

SEGUNDARIA	PRIMARIA
Se recolecta la información de estudios realizados anteriores que reposan en tesis de grados. Se encuentra registrada en documentos y materiales impresos: libros, revistas, especializadas, informes técnicos, memorias de eventos científicos, tesis de grado, etc. Las fuentes de información son bibliotecas, archivos, centro de documentación, internet, etc.	Se recolecta directamente a través del contacto directo entre el sujeto investigador y el objeto de estudio, es decir, con la realidad

Tabla 3.4 Tipos de investigación

Técnicas de Investigación

BIBLIOGRAFICAS	DE CAMPO
Permite recolectar información secundaria que se encuentra registrada en: libros, revistas científicas, informes técnicos, memorias, internet, etc. Análisis de documentos (Lectura científicas) El fichaje	Permiten recolectar información primaria La observación, La entrevista, La encuesta.

Tabla 3.5 Técnicas de investigación

Recolección de la Información

PREGUNTAS	EXPLICACION

Para qué?	Recolectar Información primaria para comprobar y contrastar con la hipótesis
A que personas o sujetos?	Al departamento de redes de la Facultad de ingeniería en Sistemas, Electrónica e Industrial.
Sobre qué aspectos?	**VI.** Sistema de Detección y Prevención de Intrusos **VD.** Vulnerabilidad de los servidores
Quién?	**Investigador.** Daniel F. Yánez G.
Cuando?	De acuerdo al cronograma establecido
Lugar de recolección de la Información?	FISEI
Cuantas veces?	1 sola vez
Que técnicas de recolección?	Encuesta
Con que?	Cuestionario
En qué situación?	Situación normal y cotidiana

Tabla 3.6 Recolección de la Información

3.7. Procesamiento y Análisis de la Información

Revisión y codificación de la información.

Categorización y tabulación de la información.

- Tabulación manual.

Análisis de los datos.

Interpretación de los resultados.

- La presentación de los datos se dará a través de gráficos cuadros para analizar e interpretarlos.
- Redactar una síntesis general de los resultados.

CAPITULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En la presente investigación la información fue recopilada utilizando como técnica la Encuesta, la misma que fue aplicada a las personas responsables del Departamento de Administración de Redes de la FISEI (laboratoristas y administradores) el cual se encuentra detallado en la tabla 3.1 de acuerdo al modelo presentado en el Anexo 2. A continuación se presentan los resultados.

4.1. Análisis

1.- ¿Cuál es el nivel de importancia de la información que maneja el Departamento de Administración de Redes? Tomando en cuenta los indicadores como normal información que puede ser visualizada por cualquier persona y alta información que solamente puede acceder personal autorizado

literal	Indicador	Valores	%
A	Normal	3	43
B	Alta	4	57
	Total	7	100

Fuente: Estudio de campo
Autor: Daniel Yánez

Tabla 4.1 Tabulación de la Encuesta – Pregunta 1

Fuente: Estudio de campo
Autor: Daniel Yánez

Gráfico 4.1. Tabulación de la Encuesta – Pregunta 1

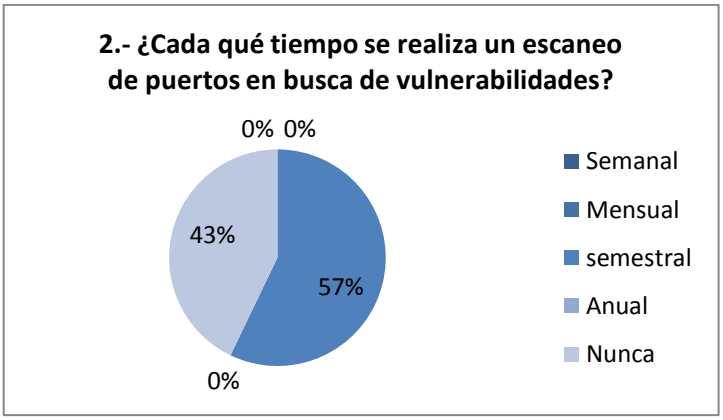
De los 7 encuestados que forman parte del departamento de sistemas dela FISEI, 3 encuestados que representan el 43%, indica que el nivel de importancia de la información es considerada como normal mientras que 4 encuestados que representa el 57% manifiestan que el nivel de importancia es alto.

2.- ¿Cada qué tiempo se realiza un escaneo de puertos en busca de vulnerabilidades?

literal	Indicador	Valores	%
A	Semanal	0	0
B	Mensual	0	0
C	Semestral	4	57
D	Anual	0	0
E	Nunca	3	43
	Total	7	100

Fuente: Estudio de campo
Autor: Daniel Yánez

Tabla 4.2 Tabulación de la Encuesta – Pregunta 2



Fuente: Estudio de campo
Autor: Daniel Yánez

Gráfico 4.2. Tabulación de la Encuesta – Pregunta 2

De los 7 encuestados que forman parte del departamento de sistemas dela FISEI, 4 encuestados que representan el 57%, indica que se realiza un escaneo de puertos en busca de vulnerabilidades semestralmente mientras que 3 encuestados que representa el 43% manifiestan que nunca se ha realizado un escaneo de puertos.

3.- ¿Qué nivel de seguridad poseen los equipos servidores de la FISEI?

Tomar en consideración la siguiente tabla para medir los indicadores

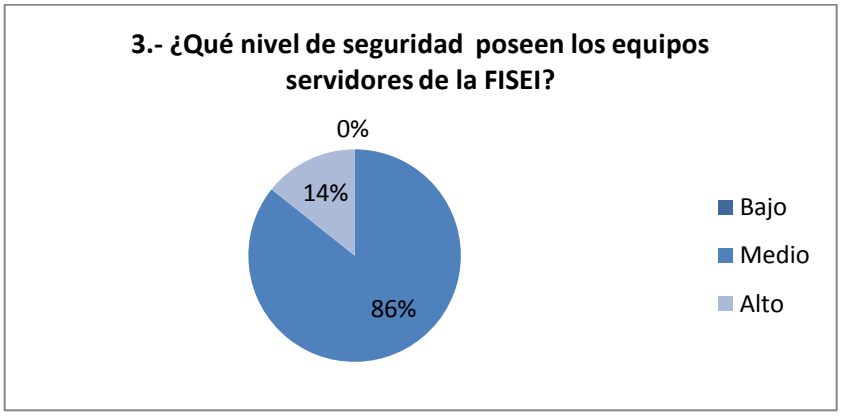
Niveles	Parámetros
Bajo	Cualquier usuario tiene acceso a los equipos físicos, red de datos e internet.
Medio	Solamente personal autorizado accede a los equipos servidores y usuarios accede a la red LAN, internet, aplicaciones mediante usuarios y contraseñas o algún tipo de autentificación
Alto	Solo personal autorizado accede a los equipos servidores, se mantiene historiales de acceso y uso de las redes, se posee herramientas de seguridad para control y administración de redes

Tabla 4.3 Indicadores – Pregunta 3

literal	Indicador	Valores	%
A	Bajo	0	0
B	Medio	6	86
C	Alto	1	14
	Total	7	100

Fuente: Estudio de campo
Autor: Daniel Yánez

Tabla 4.5 Tabulación de la Encuesta – Pregunta 3



Fuente: Estudio de campo
Autor: Daniel Yánez

Gráfico 4.3. Tabulación de la Encuesta – Pregunta 3

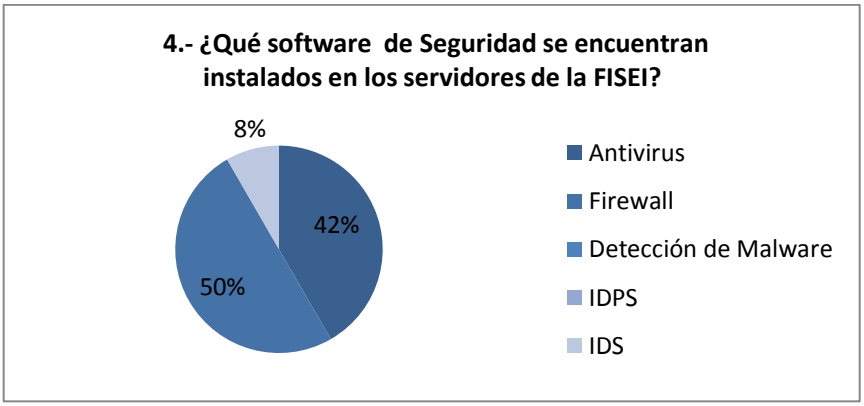
De los 7 encuestados que forman parte del departamento de sistemas de la FISEI, 6 encuestados que representan el 86%, indica que el nivel de seguridad poseen los equipos servidores es medio mientras que 1 encuestados que representa el 14% manifiestan que la seguridad es alto.

4.- ¿Qué software de Seguridad se encuentran instalados en los servidores de la FISEI?

literal	Indicador	Valores	%
A	Antivirus	5	42
B	Firewall	6	50
C	Detección de Malware	0	
D	IDPS	0	
E	IDS	1	8
	Total	12	100

Fuente: Estudio de campo
Autor: Daniel Yánez

Tabla 4.5 Tabulación de la Encuesta – Pregunta 4



Fuente: Estudio de campo
Autor: Daniel Yánez

Gráfico 4.4. Tabulación de la Encuesta – Pregunta 4

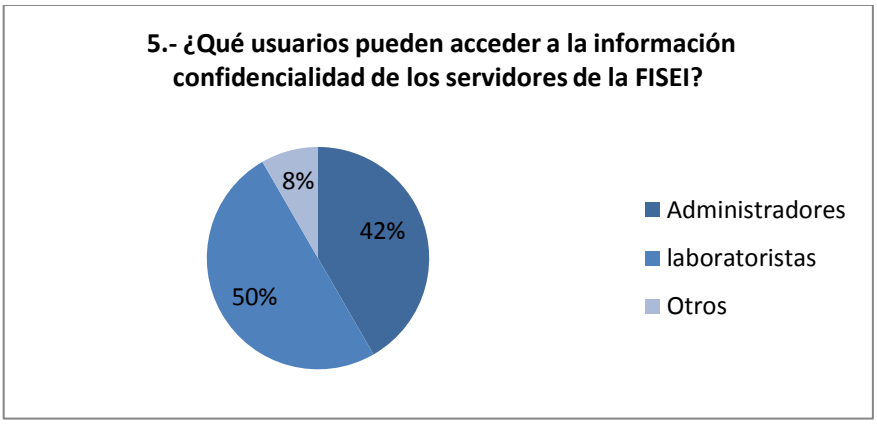
De los 7 encuestados que forman parte del departamento de sistemas dela FISEI, La pregunta 4 de opción múltiple, los encuestados señalaron la opción A) Antivirus por 5 ocasiones que representan el 42%, señalaron la opción b) Firewall por 6 ocasiones que representan el 50% y señalaron la opción e) IDS por 1 ocasión que representa el 8%.

5.- ¿Qué usuarios pueden acceder a la información confidencial de los servidores de la FISEI?

literal	Indicador	Valores	%
A	Administradores	5	42
B	Laboratoristas	6	50
C	Otros	1	8
	Total	12	100

Fuente: Estudio de campo
Autor: Daniel Yánez

Tabla 4.6 Tabulación de la Encuesta – Pregunta 5



Fuente: Estudio de campo
Autor: Daniel Yánez

Gráfico 4.5. Tabulación de la Encuesta – Pregunta 5

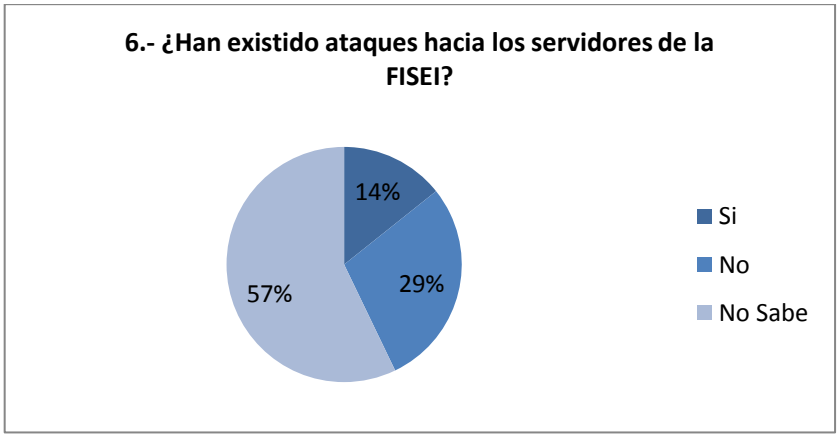
De los 7 encuestados que forman parte del departamento de sistemas de la FISEI, La pregunta 5 de opción múltiple, los encuestados señalaron la opción A) Administradores por 5 ocasiones que representan el 42%, señalaron la opción b) laboratoristas por 6 ocasiones que representan el 50% , y señalaron la opción e) Otros por 1 ocasión que representa el 8%.

6.- ¿Han existido ataques hacia los servidores de la FISEI?

literal	Indicador	Valores	%
A	Si	1	14
B	No	2	29
C	No Sabe	4	57
	Total	7	100

Fuente: Estudio de campo
Autor: Daniel Yánez

Tabla 4.7 Tabulación de la Encuesta – Pregunta 6



Fuente: Estudio de campo
Autor: Daniel Yánez

Gráfico 4.6. Tabulación de la Encuesta – Pregunta 6

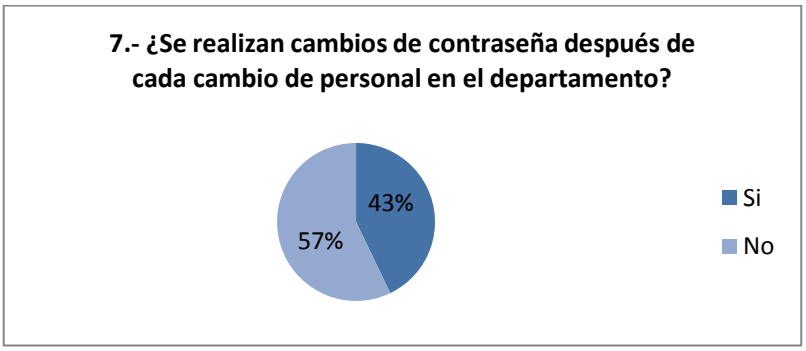
De los 7 encuestados que forman parte del departamento de sistemas de la FISEI, 4 encuestados que representan el 57%, indica que NO SABEN si han existido ataques a los servidores de la FISEI mientras que 2 encuestados que representa el 29% manifiestan que NO han existido ataques a los servidores de la FISEI y mientras que 1 encuestado que representa el 14%, indica que SI han existido ataques hacia los servidores de la FISEI.

7.- ¿Se realizan cambios de contraseña después de cada cambio de personal en el departamento?

literal	Indicador	Valores	%
A	Si	3	43
B	No	4	57
	Total	7	100

Fuente: Estudio de campo
Autor: Daniel Yánez

Tabla 4.8 Tabulación de la Encuesta – Pregunta 7



Fuente: Estudio de campo
Autor: Daniel Yánez

Gráfico 4.7. Tabulación de la Encuesta – Pregunta 7

De los 7 encuestados que forman parte del departamento de sistemas de la FISEI, 4 encuestados que representan el 57%, indica que NO se realiza cambios de contraseña después de cada salida del personal, mientras que 3 encuestados que representa el 43% manifiestan que SI se realiza cambios de contraseña después de cada salida del personal.

4.2. Interpretación

Se ha tomado en cuenta las dos preguntas determinantes la número 2 y la pregunta numero 6 ya que los resultados arrojados, dicen que la red informática de la FISEI necesita tener un mayor control y mayores tipo de seguridad, ya que no se realizan análisis ni monitoreos frecuentes de los accesos hacia los servidores, lo cual puede provocar que existan vulnerabilidades por medio de los puertos y además existe desconocimiento por parte de las personas que conforman el departamento de redes sobre los niveles de seguridad que existen en los equipos.

4.3. Verificación de la Hipótesis

Para verificar la hipótesis se tratara la información utilizando el método estadístico conocido como t-student, que permitirá determinar si se aplica o no la propuesta en poblaciones pequeñas.

4.4. Modelo Lógico

"La implementación de un sistema de detección y prevención de intrusos influirá en la seguridad de la información interna y confidencial de la FISEI".

a) **Hipótesis Nula (H_0) =** "La implementación de un sistema de detección y prevención de intrusos SI influirá en la seguridad de la información interna y confidencial de la FISEI".

b) **Hipótesis Alterna (H_1) =** "La implementación de un sistema de detección y prevención de intrusos NO influirá en la seguridad de la información interna y confidencial de la FISEI".

Se calcula el intervalo de confianza en 95% asumiendo que para

H_0: μ1 - μ2 = 0

H_1: μ1 - μ2 ≠ 0

Nivel de significancia y regla de decisión

Se trabajará con un intervalo de confianza IC 95% para lo que se necesita calcular la varianza y el error estándar.

Elección de la prueba estadística

$$t = \frac{\overline{X}\ 1 - \overline{X}\ 2}{EE(\overline{X}\ 1 - \overline{X}\ 2)} = \frac{\overline{X}\ 1 - \overline{X}\ 2}{\sqrt{s^2\ (\frac{1}{n1} + \frac{1}{n2})}}$$

Donde:

t = t student

EE = Error Estándar

$\overline{X}$ = Media

n = Número de observaciones

S = Desviación estándar

Combinación de Frecuencias

Se combina dos preguntas de la encuesta con el fin de comprobar la hipótesis y representar gráficamente dicha combinación.

Se trabajará con las preguntas 6 y 7 de la encuesta, se tratará de establecer la relación que permita verificar la hipótesis según el grado de significancia.

Frecuencias Observadas

N°	Pregunta	Si	No	No sabe	Total
6	¿Han existido ataques hacia los servidores de la FISEI?	1	2	4	7
7	¿Se realizan cambios de contraseña después de cada cambio de personal en el departamento?	3	4	0	7
Totales		4	6	4	14

Fuente: Estudio de campo
Autor: Daniel Yánez

Tabla 4.9 Frecuencias Observadas

Con los datos de las frecuencias observadas se procede a calcular la medida para cada pregunta seleccionada partiendo de la formula.

$$\overline{X} = \frac{\sum x}{n}$$

De aquí según los tamaños muestrales n1 = 2 y n2 = 3 para la medida se tendría:

$$\overline{X}\ 1 = \frac{7}{2}$$

$$\overline{X}\ 1 = 3.5$$

$$\overline{X}\ 2 = \frac{7}{3}$$

$$\overline{X}\ 2 = 2.33$$

Una vez obtenidos estos datos se calcula la desviación típica para cada grupo de respuestas aplicando la fórmula:

$$S = \sqrt{\frac{1}{n-1}\sum(x - \overline{X})^2}$$

A partir de esta fórmula tendremos los valores en las desviaciones típicas para los grupos como S1 y S2.

Desviación estándar para S1:

$$S1 = \sqrt{\frac{1}{n1-1}\sum(x1 - \overline{X}\ 1)^2}$$

$$S1 = \sqrt{\frac{1}{2-1}[(3-3{,}5)^2 + (4-3.5)^2]}$$

$$S1 = \sqrt{\frac{1}{1}[(-0{,}5)^2 + (0.5)^2]}$$

$$S1 = \sqrt{\frac{1}{1}[0.25 + 0.25]}$$

$$S1 = 0{,}71$$

Desviación estándar para S2:

$$S2 = \sqrt{\frac{1}{n2-1}\sum(x2 - \overline{X}\ 2)^2}$$

$$S2 = \sqrt{\frac{1}{3-1}[(1-2.33)^2 + (2-2.33)^2 + (4-2.33)^2]}$$

$$S2 = \sqrt{\frac{1}{2}[(-1.33)^2 + (-0.33)^2 + (1.67)^2]}$$

$$S2 = \sqrt{\frac{1}{2}[1.77 + 0.11 + 2.79]}$$

$$S2 = 1{,}53$$

Se calculará la desviación típicas o desviación estándar.

$$S^2 = \frac{(n1-1)S_1^2 + (n2-1)S_2^2}{n1 + n2 - 2}$$

$$S^2 = \frac{(2-1)0{,}71^2 + (3-1)1{,}53^2}{2+3-2}$$

$$S^2 = \frac{(2-1)0{,}5041 + (3-1)2{,}3409}{2+3-2}$$

$$S^2 = 1{,}729$$

Con esto podemos calcular el error estándar:

$$EE = \sqrt{S^2(\frac{1}{n1}+\frac{1}{n2})}$$

$$EE = \sqrt{1{,}729(\frac{1}{2}+\frac{1}{3})}$$

$$EE = 1{,}2$$

Grados de libertad

$$G1 = (n1-1)(n2-1)$$

Donde:

G1 = Grado de libertad

n = Número de observaciones

Remplazando se tiene:

$$G1= (2-1)\ (3-1)$$

$$G1 = 2$$

De donde basándose en la tabla de distribución F para la distribución t se tiene que el grado de significancia es:

$$\infty= 2{,}92$$

Con este resultado se procede a buscar el intervalo de confianza IC 95% y se tiene:

$$IC = [(\overline{X}\ 1 - \overline{X}\ 2) \pm \infty EE(\overline{X}\ 1 - \overline{X}\ 2)]$$

$$IC95\% = [(3{,}5 - 2{,}33) \pm (2{,}92)(1{,}2)(3{,}5 - 2{,}33)]$$

$$IC95\% = 1{,}17 \pm 4{,}1$$

$$IC95\% = (5{,}27;\ -2{,}93)$$

Cálculo matemático

Se busca que no exista asociación entre variables, comprobando valores esperados a través de t-student. De donde se tiene según la graduación de niveles de las desviaciones estándar y la varianza para la distribución se tiene que:

G1 = 2	∞ = 2,92
$\overline{X}$ 1 = 3,5	$\overline{X}$ 2 = 2,33
n1 = 2	n2 = 3
EE = 1,2	S^2 = 1,53

Entonces aplicando la fórmula de t:

$$t = \frac{\overline{X}\ 1 - \overline{X}\ 2}{\sqrt{s^2\ (\frac{1}{n1} + \frac{1}{n2})}}$$

$$t = \frac{3,5 - 2,33}{\sqrt{1,53\ (\frac{1}{2} + \frac{1}{3})}}$$

$$t = 1,04$$

Regla de decisión

Dado que para H_0: μ1 - μ2 = 0 y para H_1: μ1 - μ2 ≠ 0, se hace referencia al grado de significancia de 2,92 según el resultado de t 1,04 se evalua según la regla general de aceptación dentro del intervalo de confianza IC (5,27; -2,93), si el valor se encuentra dentro del intervalo de confianza y el resultado t es menor al grado de significancia al referente a la hipótesis es aceptada caso contrario esta deberá rechazarse, en tal virtud la regla se cumple y la hipótesis se acepta.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

El presente capitulo comprende las conclusiones y recomendaciones fundamentales en los resultados presentados y analizados mediante la realización de la encuesta, conforme a los objetivos de estudio.

5.1. Conclusiones

- El nivel de seguridad que maneja el departamento de Administración de Redes, es considerada de nivel medio, tomando en cuenta los indicadores de la pregunta 3, la cual hace referencia a que el nivel de seguridad medio indica que solamente personal autorizado accede a los equipos servidores y usuarios accede a la red LAN, internet y aplicaciones mediante un usuario y contraseña o algún tipo de autentificación proporcionados por el departamento de administración de redes; es por este motivo que es necesario el mantener la información segura de tal manera que siempre esté disponible para las personas que la requieran y en el momento que sea necesario.

- Existe desconocimientos a cerca de los posibles ataques e intentos de acceso a la información existente en los equipo servidores de la FISEI como nos indica la pregunta 6 de la encuesta realizada al personal que trabaja en el departamento de administración de redes.

- Los equipos servidores que forman parte de la red de la FISEI cuentan con herramientas tradicionales de seguridad (antivirus y firewall) como nos indica en la pregunta 4 de la encuesta realizada, lo cual en la actualidad pueden no resultar suficientes para proteger los datos de nuevos y más avanzados ataques que busca el obtener el control de la información.

- La información que maneja los servidores de la FISEI es considerada por los encuestados de alto nivel (información que solamente puede acceder personal autorizado), esto es debido a que en los servidores se administran las aplicaciones para el control de docentes, aplicaciones para el control de inventario de equipos, encuestas para estudiantes y además el control de usuarios que pueden acceder a las redes inalámbricas.

5.2. Recomendaciones

- Se recomienda implementar herramientas de seguridad complementarias a las ya instaladas en los equipos y de esta manera se permita a los encargados del departamento de administración en redes, tener un mejor control de la información.

- Se sugiere implementar un software que permita mantener un control de los accesos y que emita una respuesta ante posibles ataques, además permita bridar a los administradores de la red respuestas oportunas en tiempo real ante posibles vulnerabilidades.

- Se aconseja establecer periodos para cambios de contraseña y de esta manera evitar el acceso hacia los equipos por parte del personal que trabajó anteriormente en el departamento de Sistemas y mantener un registro de la información de cada uno de ellos.

CAPITULO VI

6. PROPUESTA

6.1. Datos Informativos

- **Titulo**

  "Sistema de Detección y Prevención de Intrusos para el control de la vulnerabilidad en los servidores de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato."

- **Institución ejecutora**

  Facultad de Ingeniería en Sistemas, Electrónica e Industrial - UTA

- **Director de Tesis**

  Ing. M.sc. David Guevara

- **Beneficiario**

  Departamento de Administración de Redes FISEI

- **Ubicación**

Av. Los Chasquis y Río Guayabamba. (Universidad Técnica de Ambato).

- **Tiempo estimado para la ejecución**

    - Fecha de inicio: Enero de 2012
    - Fecha de Finalización: Enero de 2013

- **Equipo técnico responsable**

    - **Investigador:** Daniel Fernando Yánez Guevara
    - **Administrador Sistemas:** Ing. Eduardo Chaso

6.2. Antecedentes de la propuesta

En la actualidad ya no son suficientes las seguridades que nos brindan los equipos router, firewall y los antivirus tradicionales que se implementan en los equipos y servidores para protección de la información. Hoy en día debido al avance de la tecnología, empiezan a aparecer nuevos ataques cuyo objetivo es tratar de vulnerar las seguridades de los sistemas y equipos tradicionales, es por este motivo de la necesidad de nuevas herramientas de seguridad que permitan controlar, detectar, prevenir y responder a posibles ataques perpetuados por delincuentes informáticos.

Los Sistemas de Detección y Prevención de Intrusos son herramientas que actúan como un complemento de seguridad a las herramientas tradicionales, brindando de una manera más simple y sencilla un mejor manejo y control de las actividades que en ella se realizan; brindando al departamento de administración de redes una mayor seguridad a los usuarios y equipos que forman parte de la misma.

6.3. Justificación

La implementación de un sistema de detección y prevención de intrusos, permitiría al departamento de administración de redes mantener un correcto control de acceso y políticas de seguridad para poder optimizar los recursos de la institución, además de mantener un mayor grado de seguridad para la información que se encuentra almacenada en los equipo servidores

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial cuenta con la infraestructura necesaria y con información relevante para el control de los estudiantes y docentes que forman parte de la misma, esta información necesita ser asegurada y estar disponible el momento que los usuarios lo necesiten.

El alto conocimiento informático por parte de docentes y estudiantes, además del constante cambio del personal en el departamento de redes obliga a buscar alternativas de seguridad más eficientes que las normalmente utilizadas en cualquier tipo de institución.

La implementación de un sistema de detección de intrusos será beneficioso para la persona encargado del departamento de administración de redes ya que le permitirá mantener un historial de intentos de vulnerabilidad y además le permitirá actuar en tiempo real ente posibles ataques.

6.4. Objetivos

6.4.1. Objetivo General

- Implementar un sistema de detección y prevención de intrusos mediante el uso de software libre que evite la vulnerabilidad de la información de los servidores de la FISEI.

6.4.2. Objetivo Específico

- Realizar un análisis de servicios y software de los equipos servidores de la FISEI.

- Determinar un sistema de Detección y Prevención de Intrusos basado en software libre.

- Instalar y configurar de un sistema de Detección y Prevención de Intrusos para la FISEI.

6.5. Análisis de Factibilidad

6.5.1. Factibilidad Humana u Operativa

La implementación de un sistema de detección y prevención de intrusos brindara mayor seguridad al departamento de administración de redes; permitirá mejor el servicio que proporciona el personal que trabaja en él y mejorar los servicios para estudiantes, docentes y administrativos.

No ha existido ningún inconveniente con el personal a cargo del departamento de administración de redes, ha brindado las facilidades necesarias para realizar la encuesta y la puesta en marcha de la presente propuesta.

6.5.2. Factibilidad Técnica o Tecnológica

La factibilidad técnica o tecnológica consistió en realizar una evaluación de la tecnología existente en el departamento de administración de redes, éste estudio estuvo destinado a recolectar información sobre los componentes técnicos que

posee el departamento y la posibilidad de hacer uso de éstos en la implementación de Sistema de detección y prevención de intrusos, o adquirir de ser necesario nueva tecnología.

	Edificio Principal	**Edificio Posterior**
Access Point	3	2
Switch Capa3	1	Ninguno
Switch	12	4
Servidores	2	Ninguno

Tabla 6.1 Factibilidad Tecnológica

Posee un equipo servidor principal de virtualización o DOM0 el cual posee máquinas virtuales.

Las características de hardware y los servicios que brindan las máquinas virtuales son los siguientes:

Hardware - Servidor PROLIANT DL160 G6

MODELO	**HXQ123911FGF**
PROCESADOR	Intel® Xeon® E5620 (4 núcleos, 2,40 GHz, 12 MB L3, 80W)
PROCESADORES:	1
MEMORIA	8 GB
RANURAS DE MEMORIA	18 Ranuras DIMM
RANURAS DE EXPANSIÓN	2-

Tabla 6.2 Características Servidor 1

- Servicio de FREE RADIUS - CHILI SPOT
- Servicio PROXY
- Servicio de BASE DE DATOS.

La implementación de un sistema de detección y prevención de intrusos es factible ya que se cuenta con un equipo que posee las características necesarias

para poder realizar la implementación en una máquina virtual, además de la apertura y colaboración brindada por el personal que trabaja en el departamento de administración de redes.

6.5.3. Factibilidad Económica

La propuesta de implementar un sistema de detección y prevención de intrusos si es factible económicamente debido a que el departamento de administración de redes cuenta con los equipos necesarios para la implementación del mismo.

6.6. Fundamentación Teórica

6.6.1. Servidores

Es un computador que posee características superiores a los computadores normales denominados clientes y brinda servicios a los equipos que forman parte de una red de datos.

6.6.1.1. Tipos de Servidores

- **Servidor de impresión:** Permite controlar una o un conjunto de impresoras permitiendo imprimir documentos a los equipos clientes de la red de datos.

- **Servidor de correo**: Permite almacenar, enviar y recibir, correo electrónico a los clientes de la red de datos.

- **Servidor Proxy**: Es un programa o dispositivo que realiza acciones en representación de otro para aumentar y ganar funcionamiento de ciertas operaciones. Un Servidor Proxy proporciona servicios de seguridad y permite mantener un control y la administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.

- **Servidor del acceso remoto (RAS)**: Permite mantener un control de los canales de comunicación canales de comunicación de la red, de esta manera permitiendo a usuarios de la red peticiones para conectarse de una posición remota.

- **Servidor de uso**: Realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que se realicen las operaciones de un sitio de trabajo y sirviendo los resultados a su vez al sitio de trabajo, mientras que el sitio de trabajo realiza la interfaz operadora o la porción del GUI del proceso (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.

- **Servidor web**: Es un servicio que nos permite almacenar documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos que recibe peticiones por lado del cliente y las procesa en el lado del servidor.

- **Servidor de base de datos**: Es aquel que presta servicios de base de datos a otros programas o computadoras de la red (modelo cliente-servidor).

- **Servidor de Seguridad**: Son aquellos que poseen software que brinda seguridad a la red de información y permite detener intrusiones maliciosas, normalmente esta formado por antivirus, tienen antivirus, firewall, idps, antispyware, antiadware.

- **Servidor Free Radius:** Los servidores free radius nos permiten autentificar o validar un conjunto de datos provisto por el administrador de las redes y de esta manera bridar los servicios del proveedor de internet.

6.6.2. Software Libre

Es difícil encontrar una definición exacta al significado de software libre, pero en cada una de las definiciones encontradas se puede hacer referencia a cualquier software que respeta las propiedades de los usuarios y de la comunidad, dichos usuarios estipulas 4 libertades esenciales las cuales son las siguientes:

- La libertad de ejecutar el programa para cualquier propósito (libertad 0).
- La libertad de estudiar cómo funciona el programa, y la libertad de modificarlo para que cumpla con la función deseada. (libertad 1).
- La libertad de redistribuir copias (libertad 2).
- La libertad de distribuir copias de sus versiones modificadas a terceros (libertad 3).

6.6.3. Distribuciones Linux

Es una recopilación de programas y ficheros organizados y preparados para su instalación, estas distribuciones están basadas en un núcleo Linux, que poseen un conjunto de software generalmente libre aunque también pueden contener aplicaciones o controladores propietarios pero de manera minoritaria.

6.6.4. Centos

Es una plataforma muy estable y utilizada en grandes empresas por su eficiencia y estabilidad de trabajo; distribución LINUX de clase empresarial de fuentes libremente ofrecidas al público, y se encuentra basada en código fuente Red Hat Linux, es mantenido por una comunidad fortificada de usuarios que constantemente brindan soporte y están actualizando las versiones, Centos se encuentra disponible bajo licencia GNU GPL.

6.6.4.1. Requerimientos Mínimos:

- **RAM:** Mínimo 256Mb para modo gráfico.

- **Disco Duro:** 10 Gb.
- Procesador: Pentium III de 60 Mghz

6.6.5. Licencia GNU GPL

Es un tipo de licencia la cual fue creada por Free software Fundation y permite proteger la libre distribución, copia, modificación y uso del software. La idea es protegerlo de apropiación por parte de cualquier persona.

6.6.6. Snort

Gráfico 6.1. Snort Logo

La definición de Snort en la página oficial de la comunidad nos señala que "Snort es una red de código abierto de prevención y detección de intrusos (IDS / IPS) desarrollado por Sourcefire. La combinación del beneficio de la firma, el protocolo y la inspección de anomalías basado en Snort es la más utilizada tecnología en todo el mundo. Con millones de descargas y cerca de 400.000 usuarios registrados, Snort se ha convertido en el estándar para IPS."

Snort es una herramienta de seguridad de prevención y detección de intrusos basado en redes, el cual permite realizar un monitoreo y control de los eventos ocurridos en un sistemas informático en tiempo real. Snort realiza un barrido de puertos lo que permite registrar, alertar y responder ante cualquier irregularidad existente en la red de información permitiendo de esta manera generar o emitir

avisos y respuesta ante posibles ataque previamente definida en reglas o patrones.

La primera versión de Snort fue lanzada originalmente en 1998 por el fundador de Sourcefire Martin Roesch Inicialmente se lo denominaba lightweight.

Snort en la actualidad posee más de 4 millones de descargas y cerca de 400.000 usuarios registrados, por lo tanto es una de las tecnologías de detección y prevención de intrusos más utilizada en el mundo. Snort tiene tres usos principales: se utiliza como un analizador de paquetes, como un capturador de paquetes, o como un sistema de red para prevención de intrusiones.
Snort se encuentra disponible bajo la licencia GPL (proteger la libre distribución, modificación y uso de software), es multiplataforma a diferencia de su primera versión, puede ser instalado tanto en sistemas operativos de Windows como Unix/Linux. Al ser un sistema de código abierto posee una comunidad de desarrolladores experimentados muy amplia, esto debido al gran alcance y cantidad de usuarios que posee, los mismos que realizan pruebas periódicas para la revisión de reglas y motores que lo componen.

6.6.6.1. Elementos que componen Snort

El motor de Snort está dividido en varios componentes entre los cuales encontramos los siguientes:

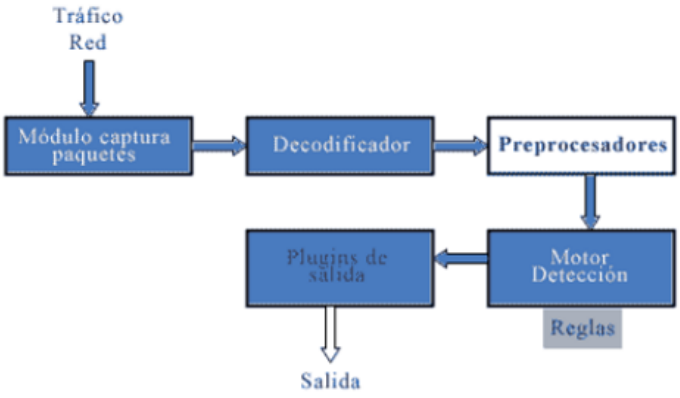


Gráfico 6.2. Snort Elementos

- Capturador de Paquetes
- Decodificador
- Preprocesadores
- Motor de Detección
- Plugins de Salida

6.6.6.1.1. Capturador de Paquetes

Permite analizar los paquetes enviados por la red y estructurarlo de manera que el paquete se encuentre bien formado y prepararlo para ser enviados al motor de detección.

Snort requiere una biblioteca de snnifing externa la misma que permite realizar la captura de tráfico que circula por la red esta librería se denomina **Libpcap**.

Libpcap posee independencia de plataforma con la cual este trabajando, de esta manera permite a snort trabajar bajo cualquier Sistema operativo.

Libpcap nos permite analizar paquetes raw, los cuales son paquetes capturados directamente desde la tarjeta de red, esto quiere decir que son paquetes sin modificar, estos paquetes dependen del sistema operativo. Snort utiliza la cabecera de estos paquetes para poder descifrar algunos tipos de ataques.

6.6.6.1.2. Decodificador

El decodificador permite buscar anomalías dentro de los paquetes capturados mediante Libpcap. Está formado por una serie de decodificadores que descifran elementos de protocolos específicos para posteriormente ser almacenados mediante una estructura de datos.

El decodificador analiza la información imponiendo orden sobre los datos que posee el paquete de datos iniciando desde el nivel más bajo hasta el más alto.

- Enlace de Datos (MAC, PPP)
- Red (IP)
- Transporte (TCP / UDP)

Gráfico 6.3. Decodificador

6.6.6.1.3. Preprocesadores

Los preprocesadores son módulos o plugins que permiten extender la funcionalidad de snort para tratar los paquetes o tramas que vienen desde el decodificador, Los preprocesadores se encargan de dar forma lógica a los paquetes para poder interpretar la información de una manera más simple.

Los preprocesadores pueden desfragmentar o realizar un análisis de la cabecera y cuerpo de las tramas además de ordenarlos decodificarlos y reensamblarlos para poder ser enviados hacia el motor de detección.

Pueden ser programados en Lenguaje C, estos programas son compilados junto a snort en forma de librerías y son configurados en el archivo etc/snort.conf.

Preprocesadores que posee SNORT

Snort trabaja con algunos preprocesadores entre los cuales se detallan posteriormente:

- frag3
- stream4 y stream4_reassemble
- flow
- stream5
- sfportscan
- rpc_decode
- Ssh

Procesadores	Objetivo	Función	Líneas de Configuración
frag3	Detección de evasión del IDS por fragmentación	Reensamblar paquetes Fragmentados	**Frag3_global**: global **Frag3_engine**:cada pila
stream4 y tream4_ reassemble	Detección de ataques basados en conexión	Guardar paquetes anteriores para reensamblarlos y detectar ataques repartidos en paquetes	**Detect_scans**: detectar intentos **Detect_state_problems:** número de secuencias **Max_sessions** número máximo de sesiones a analizar
Stream5	Permite la detección de anomalías dependiendo del S.O	Realiza un seguimiento de conexiones TCP, UDP, ICMP	**Global** configuraciones globales para TCP, UDP, ICMP **Configuración TCP** **Configuración UDP**

			Configuración ICMP
Sfportscan	Detectar escaneos TCP, UDP, IP Portscan, Decoy, distribuidos y barridos	Detectar el ataque me diante escaneo de puertos	**Scan_type:** Tipo de escaneo **Proto:** Protocolo a escanear **ignore scanners:** listas de IPs a escanear
rpc_decode	Permite normalizar múltiples registros RPC	Reemzamblar paquetes RPC en uno solo para facilitar el analisis	
Ssh	Detectar algunos exploits: Gobbles, CRC32, Secure CRT y Protocol Mismatch	Analizar el trafico ssh de servidores y clientes	**Server ports:** Puertos a escanear del servidor. **disable recognition:** detecta tráfico no SSH en puertos SSH

Tabla 6.6 Preprocesadores Snort

Los preprocesadores realizan el análisis de las tramas mediantes reglas lo cual se describe a continuación:

6.6.6.1.4. Reglas

Las reglas o firmas son los patrones que nos permiten buscar dentro de los paquetes enviados por los procesadores. Al existir coincidencias entre el contenido de los paquetes y las firmas generadas, snort emitirá una alerta informando de un posible ataque, estas reglas son utilizadas por el motor de detección

Snort provee en su página oficial un conjunto de reglas por defecto conocidas como VRT (Vulnerability Research Team) para ser utilizadas, pero hay que dejar en claro que estas reglas tienen costo, pero adicionalmente a ellas es necesario

registrarse en la página para poder acceder a ellas. Estas reglas deben ser actualizadas constantemente, esto debido a que diariamente aparecen una gran cantidad de ataques o vulnerabilidades. Estas reglas pueden ser añadidas o eliminadas en el archivo snort.conf.

Estructura de una Regla

Las reglas de snort son declaraciones de texto dentro del archivo de reglas, estas son escritas en una sola línea, las reglas de snort las podemos dividir en dos:

- Cabecera de una regla
- Opciones de una regla

Cabecera de una regla

Contiene la acción que va a ejecutar la regla, protocolo IP, máscaras de red, puerto de origen y destino del paquete.

Acción	Protocolo	Red Origen	Puerto Origen	Dirección	Red Destino	Puerto Destino
Alert	Tcp	$EXTERNAL_NET	ANY	->	$HOME_NET	53

Tabla 6.6 Estructura Cabecera

A continuación se describe cada parte de la estructura de una cabecera:

- Acción

Como su nombre lo indica, es la acción a realizarse sobre el paquete.

Tipo	Descripción
Alert	Genera alerta y registra el paquete

Log	Registra Paquete
Pass	Ignora Paquete
Actívate	Activa alerta y llama a una regla
Dynamic	Funciona cuando se activa una regla
Drop	Elimina el paquete cuando actúa como IPS
Reject	Rechasa paquete cuando actúa como IPS
Sdrop	Elimina el paquete sin registrar cuando actúa como IPS

Tabla 6.7 Tipos de Alertas

- Protocolo

Aquí se establece el protocolo de comunicación a utilizar, un protocolo es un conjunto de reglas que usan dos ordenadores para la comunicación entre si.

Tipo	Descripción
TCP	Este protocolo nos permite la transmisión de información en redes de ordenadores. Orientado a la conexión
UDP (User Datagram Protocol)	Se limita a recoger el mensaje y enviarlo por la red, NO orientado a la conexión
ICMP (Internet Control Message Protocol)	Protocolo de control y notificación de mensajes de error del protocolo IP
IP (Internet Protocol)	Es un protocolo que pertenece al nivel de red, tiene la misión de encaminar los datos sin comprobar la integridad de la información

Tabla 6.8 Tipos de Protocolos Soportados por SNORT

- Red de Origen y Destino

Establece el origen de la comunicación.

Formas de Señalar	Ejemplo

Directamente	192.168.0.5/24
Conjunto de Redes	[192.168.0.5 192.168.0.10]
Con variables	$HOME_NET (interna); $External_NET (Externa) y ANY (cualquiera)

Tabla 6.9 Formas de Señalar las redes en las reglas

- Puerto Origen y destino:

Establece puerto de Origen de la comunicación.

Puerto	Tipo	Nombre de protocolo o servicio	Nombre del servicio	Usado por/Información adicional
7	TCP/UDP	Echo	Echo	-
20	TCP	Protocolo de transferencia de archivos (FTP)	ftp-data	-
21	TCP	Control de FTP	ftp	-
22	TCP	Shell segura (SSH)	Ssh	-
23	TCP	Telnet	telnet	-
25	TCP	Protocolo simple de transferencia de correo (SMTP)	Smtp	Mail (para enviar correo electrónico);
53	TCP/UDP	Sistema de nombres de dominio (DNS)	Domain	MacDNS, FaceTime
80	TCP	Protocolo de transferencia de hipertexto (HTTP)	http	World Wide Web,
88	TCP	Kerberos	Kerberos	-

110	TCP	Protocolo de oficina de correos (POP3) Protocolo de oficina de correos autenticado (APOP)	pop3	Mail (para recibir correo electrónico)

Tabla 6.10 Protocolos más comunes

- **Dirección:**

Permite establecer el sentido de la comunicación.

Opciones de una regla

Las opciones de las reglas contienen la información necesaria para la toma de decisiones de una regla, se encuentran separadas entre si por (;) y las claves se encuentran separadas por (:).

Existen cuatro tipos de opciones las cuales son las siguientes:

- **Metadata:** Aquí se proporciona la información sobre la regla.
- **PayLoad:** Busca los patrones o las firmas dentro de los paquetes de la carga útil.
- **Non-Payload:** Busca patrones dentro del resto de paquetes como por ejemplo la cabecera.
- **Post-detection:** Activa reglas específicas, posteriores a la ejecución de una regla**.**

A continuación se indica cada una de las opciones que pueden ser configuradas para cada una de las diferentes categorías

Categorías	Opciones

Metadatos	msg, reference, sid, rev, classtype, priority
Payload	content, nocase, rawbytes, depth, offset, distance, within, uricontent, isdataat, pcre, byte_test, byte_jump, ftpbounce, regex y content-list
Non-payload	Fragoffset, ttl, tos, ipopts, fragbits, dzice, flags, flow, flowbits, seq, ack, Windows, iftype, icode, icmp_id, icmp_seq, rpc, ip_proto sameip
Post-Detection	Logto, sesión, resp, react, tag

Tabla 6.11 Opciones de las Reglas

6.6.6.1.5. Motor de Detección

El motor de detección es el responsable de detectar si existe alguna actividad maliciosa dentro de un paquete, esto lo realiza haciendo una comparación con las reglas previamente definidas y configuradas en los archivos de reglas, si existe una detección el motor ejecuta la regla especificada para dicho ataque, posteriormente la alerta emitida es almacenada en un log, caso contrario al no existir alguna similitud con las reglas el motor lo descarta.

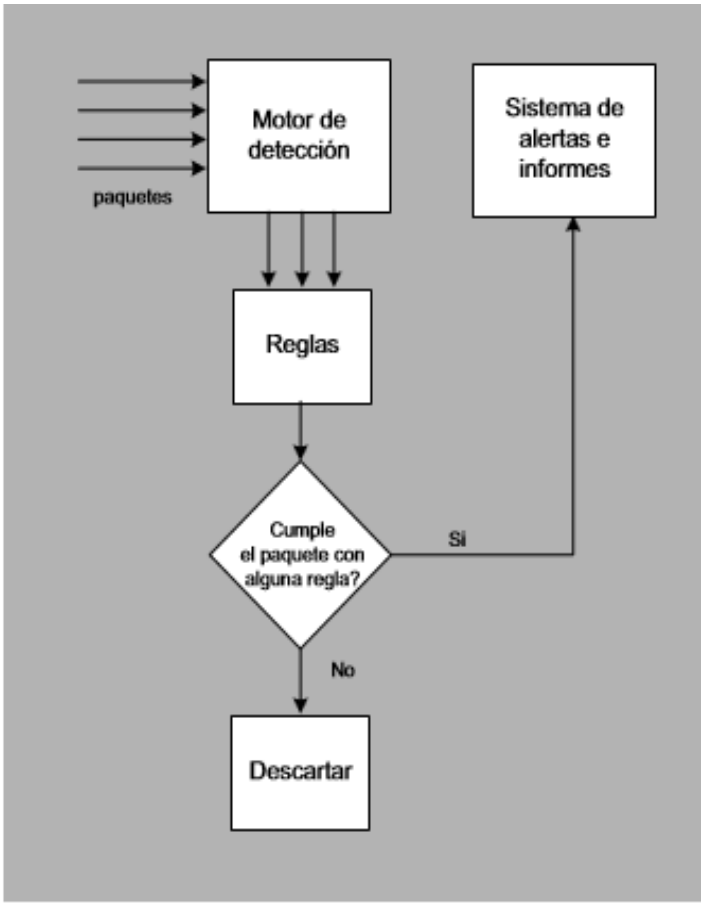


Gráfico 6.4. Comportamiento del Motor de Detección

6.6.6.1.6. Plugins o Módulos de Salida

Una vez analizada la información por el motor de detección, es necesario reportar la información ya sea en diferentes formatos y en diferentes equipos.
Cuando una alerta es lanzada por el motor de detección, esta alerta puede suponer la generar un fichero de registro (log), o puede ser enviado mediante un mensaje mediante SNMP o almacenarse en una base de datos.

Existen varios tipos de salida de información los cuales se detallaran en el siguiente cuadro:

Tipos	Descripción
Syslog	Envia alarmas al Syslog
Alert_Fast	Devuelve información sobre tiempo, mensaje, clasificación, prioridad, ip, puerto origen y destino
Alert_Full	Modo de alerta más completa que alert_fast añadiendo información sobre las cabeceras de los paquetes
Alert_Smb	Envia mensaje de alerta a host Windows
Alert_unixsock	Enviar alertas a través de socket
Log_tcpdump	Asocia paquetes a un archivo con formato tcpdump
Base de datos	Almacena la información en una base de datos snort soporta 3 tipos de salida: • MySql • PostgreSQL • Oracle
CSV	Escribe los datos en formatos CSV
Unified	Formato Binario básico
Log Null	No se almacena en archivos Log.
Eventlog	Registra alerta y se visualiza en S.O Windows.

Tabla 6.12 Tipos de Módulos de Salidas

6.6.6.2. Tipos de Errores

Dentro del análisis y estudio de Snort y en general de los IDPS existen 2 tipos de errores:

6.6.6.2.1. Falsos positivos

Son aquellos que hacen referencia a un fallo de detección en un sistema de alertas. Generalmente esto puede suceder cuando el sistema posee demasiadas reglas o seguridades en las cuales el sistema todo lo que detecta lo analiza como una amenaza.

6.6.6.2.2. Falsos negativos

Sucede cuando un intruso intenta acceder a nuestra red o equipos y pudo pasar las seguridades de nuestro IDPS.

6.6.6.3. Comandos Básicos de Snort

El siguiente cuadro muestra los comandos Básicos para poner en funcionamiento snort.

Comandos	Descripción
snort –W	Permite conocer las interfaces físicas
snort -v -i interface	Permite usar snort como sniffer
snort -T -c ruta_completa_fichero_snort.conf	Permite mostrara un reporte del estado de nuestro fichero de configuración
snort -c ruta_completa_fichero_snort.conf -i interface	Permite poner snort en funcionamiento como sistema de intrusión IDS
snort -D -c ruta_completa_fichero_snort.conf -i interface	Snort como un daemon en un sistema linux para que arranque al comienzo del sistema

Tabla 6.13 Comandos Básicos Snort

6.6.6.4. Requerimientos para implementación de Snort

6.6.6.4.1. Sistema Operativo

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial posee instalado en sus laboratorios y biblioteca sistemas operativos Windows. En su servidor principal posee un servidor CentOS el cual brinda los servicios mencionados anteriormente en el análisis de la Red de la FISEI y adicionalmente será el sistema operativo en el cual se instalara el software necesario para la Implantación de SNORT.

6.6.6.4.2. Pre-requisitos necesarios para instalar Snort

Snort requiere de varios paquetes adicionales para su funcionamiento, y son los siguientes:

- GCC
- FLEX
- BISON
- ZLIB
- LIBPCAP
- PCRE
- LIBDNET
- TCPDUMP

6.6.6.4.3. Back-End

Snort no permite almacenar la información en archivos Log, archivos CSV, Base de datos, etc. Esta información se la puede encontrar en los puntos explicados anteriormente.

Para la presente propuesta vamos a almacenar la información en una base de datos que permita al administrador de Sistemas obtener la información en tiempo real y además tener históricos de ataques para su posterior estudio o prevenir taques futuros.

Las bases de datos que podemos utilizar con snort son las siguientes:

- MySql
- PostgreSQL

- **MySQL**

“Es un sistema de gestión de bases de datos relacional, licenciado bajo la GPL de la GNU. Su diseño multadillo le permite soportar una gran carga de forma muy eficiente. MySQL fue creada por la empresa sueca MySQL AB, que mantiene el copyright del código fuente del servidor SQL, así como también de la marca**”**

- **POSTGRESQL**

“Fue el pionero en muchos de los conceptos existentes en el sistema objetorelacional actual, incluido, más tarde en otros sistemas de gestión comerciales. PostGreSQL es un sistema objeto-relacional, ya que incluye características de la orientación a objetos, como puede ser la herencia, tipos de datos, funciones, restricciones, disparadores, reglas e integridad transaccional. A pesar de esto, PostGreSQL no es un sistema de gestión de bases de datos puramente orientado a objetos.”

Postgresql a diferencia de MYSQL es una base de datos más robusta pero la sintaxis no es tan intuitiva a diferencia de MYSQL. Postgresql es utilizado en gran cantidad de proyectos comerciales. MYSQL es una excelente base de datos de gran acogida y generalmente es utilizada para proyectos pequeños, sin embargo esto no quiere decir que no pueda trabajar en proyectos grandes.

En el análisis de red realizado anteriormente podemos ver que se encuentra instalada la base de datos MYSQL, por motivo de facilidad para los administradores al ya conocer el funcionamiento de esta base de datos y al ajustarse a las necesidades del presente proyecto se utilizara la base de datos MYSQL.

6.6.6.4.4. Front-End

Para presentar la información se utilizó BASE, es una herramienta que permitirá visualizar la información en tiempo real de snort, es una versión mejorada de ACID, que fue una de las primeras interfaces de manejo y uso de snort.

6.6.7. SnortSam

Para poder mejorar la seguridad que nos brinda snort como IDS es recomendable que al recibir un intento de vulnerabilidad por parte de un atacante a nuestro servidor, se pueda realizar una acción bloqueante mediante la ayuda de un Firewall para que al ser detectada inmediatamente se realice el bloqueo de dicho ataque.

Existe un plugins que permite realizar esta combinación y mejora la seguridad que proporciona snort cuyo nombre es SNORTSAM.

SnortSam es un agente de código abierto que permite bloquear las conexiones al existir ataques, esto se logra enviando peticiones al firewall para reconfigurar las diferentes ACLs (listas de control de acceso) por un determinado tiempo.

6.6.7.1. Componentes de SnortSam

SnortSam consta de dos componentes los cuales se denominan:

- El Agente de Snort
- El plug-in de Salida

El Agente de Snort el cual permite automatizar el bloqueo además de la interacción entre snort y el firewall, y acepta los comandos enviados por el plug-in de salida.

El plug-in de Salida es implementado mediante un parche en snort y envía comandos para el filtrado de direcciones según las reglas que tengamos en nuestro IDS, las reglas de snort deberán ser modificadas para permitir el plug-in enviar información hacia el agente para que pueda bloquear las peticiones de ataques.

6.6.7.2. Firewall que trabajan con SnortSam

- Checkpoint Firewall-1
- Cisco Cisco PIX firewalls
- Cisco Routers (usando ACL o nulos Routes-)
- Netscreen anterior, ahora Juniper firewalls
- Filtro IP (IPF), disponible para varios Unix OS'es como FreeBSD
- FreeBSD IPFW2
- OpenBSD Packet Filter (PF)
- Ipchains Linux
- IPtables Linux
- Ebtables Linux
- WatchGuard Firebox firewalls
- 8signs Windows
- MS ISA Server firewall proxy Windows
- CHX
- Ali Basilea Rastreador de SNMP a través del plugin de interfaz SNMP-down

6.7. Metodología

Para poder realizar la implementación de un sistema de detección y prevención de intrusos, vamos a describir a continuación los pasos que seguiremos para poder obtener el objetivo señalado, los pasos son los siguientes:

- Análisis de Hardware
- Análisis de Software y Servicios
- Análisis de Sistema de Detección y Prevención de Intrusos
- Implementación
- Pruebas
- Capacitación

Estos son los pasos que se realizaran en el presente proyecto.

6.8. Modelo Operativo

El modelo operativo consiste en aplicar cada uno de los pasos necesarios para la implementación de la metodología expuesta anteriormente y de esta manera, cumplir con la solución propuesta

6.8.1. Análisis de Hardware

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial cuenta con equipos servidores, equipos inalámbricos, repetidores, switch y routers distribuidos en las dos edificaciones con las cuales se encuentran repartidas de la siguiente manera:

	Edificio Principal	**Edificio Posterior**
Access Point	3	2
Switch Capa3	1	Ninguno

Switch	12	4
Servidores	2	Ninguno

Tabla 6.14 Equipos FISEI

En el edificio principal los Access Points se encuentran distribuidos: uno en las oficinas administrativas, uno en la biblioteca y uno en el tercer piso, el switch de 3 capas se encuentra ubicado en la oficina de administración de redes de la FISEI al igual que los dos servidores.

En el edificio posterior se encuentra ubicado los Access points uno en el segundo piso y uno en el tercer piso, los mismos que permiten que exista la conexión a internet a los estudiantes y docentes que se encuentran en la edificación posterior, de la misma manera permiten la cobertura total de la FISEI, para que un estudiante que pase de una edificación a otra no pierda la conexión inalámbrica.

Además la estructura cableada se encuentra en buen estado, la FISEI cuenta con un cableado UTP categoría 5 el cual se encuentra cubierto por canaletas para aproximadamente a 15 centímetros de distancia del suelo lo cual cumple con los estándares en el diseño de una red cableada, tanto cableado como canaletas se encuentra en buen estado.

Se cuenta con un rack principal ubicado en el departamento de administración de redes el mismo en el cual se encuentran los switch que salen a cada laboratorio.

6.8.2. Análisis de Software y Servicios de Servidores

La FISEI cuenta con dos equipos servidores de los cuales solamente uno se encuentra funcionando mientras que el segundo servidor en la actualidad no se encuentra brindando ningún servicio a la red de datos de la FISEI, por este motivo solamente haremos mención de la existencia del mismo y nos centraremos en el

servidor que se encuentra funcionando el mismos que poseen las siguientes características:

Servidor PROLIANT DL160 G6

MODELO	**HXQ123911FGF**
PROCESADOR	Intel® Xeon® E5620 (4 núcleos, 2,40 GHz, 12 MB L3, 80W)
PROCESADORES:	1
MEMORIA	8 GB
RANURAS DE MEMORIA	18 Ranuras DIMM
RANURAS DE EXPANSIÓN	2

Tabla 6.15 Características Servidor 1

El servidor posee instalado el Sistema Operativo Centos 6.0, en el cual se encuentran levantados y funcionando los servicios:

- Servicio de FREE RADIUS - CHILI SPOT
- Servicio PROXY
- Servicio de BASE DE DATOS.
- Servicio SSH

Fue necesario conocer las versiones de los paquetes instalados en el S.O, esto lo se realizó utilizando el comando:

Comando: rpm –aq o rpm –aq –last

Al ingresar este comando indica los paquetes instalados en este caso se centró en encontrar las versiones de los servicios que se encuentran funcionando:

PAQUETE	**VERSION**

MySQL	5.1.52-1.el6_0.1.x86_64
Chillispot	1.1.0-1.i386
Freeradius	2.1.10-5
Dalo Radius	0.9-8
Apache	2.2.15-5.el6.centos.x86_64

Tabla 6.16 Versiones de Paquetes Instalados

Para poder conocer un poco más a fondo que posee el equipo servidor, se realizó una conexión SSH al servidor mediante un usuario y contraseña facilitada por el Laboratorista encargado del departamento de Administración de redes.

Para esto se utilizó el comando **NETSTAT** que permite controlar el estado actual de la Red y buscar todos los puertos abiertos:

Comando: netstat –anp –udp –tcp | grep LISTEN

```
[laboratorista@serverFisei ~]$ netstat -anp --udp --tcp | grep LISTEN
(No info could be read for "-p": geteuid()=501 but you should be root.)
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN      -
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      -
tcp        0      0 192.168.122.1:53            0.0.0.0:*                   LISTEN      -
tcp        0      0 172.168.0.1:3990            0.0.0.0:*                   LISTEN      -
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      -
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      -
tcp        0      0 0.0.0.0:46558               0.0.0.0:*                   LISTEN      -
tcp        0      0 127.0.0.1:1344              0.0.0.0:*                   LISTEN      -
tcp        0      0 :::111                      :::*                        LISTEN      -
tcp        0      0 :::8080                     :::*                        LISTEN      -
tcp        0      0 :::80                       :::*                        LISTEN      -
tcp        0      0 :::47668                    :::*                        LISTEN      -
tcp        0      0 :::22                       :::*                        LISTEN      -
tcp        0      0 :::443                      :::*                        LISTEN      -
tcp        0      0 :::5989                     :::*                        LISTEN      -
[laboratorista@serverFisei ~]$
```

Gráfico 6.5. Captura Comando netstat

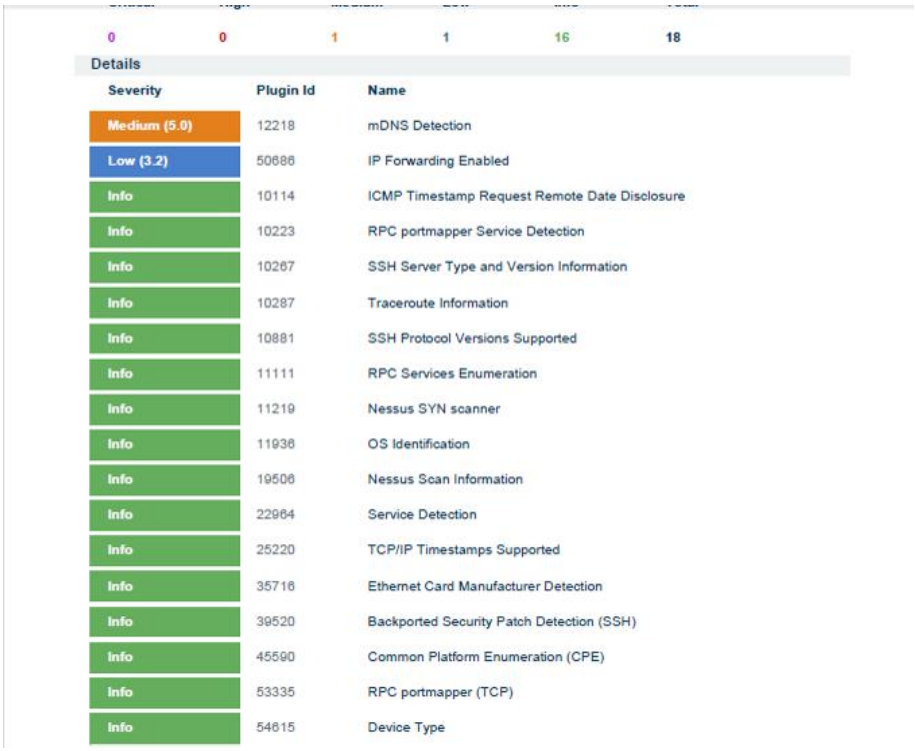
En la imagen que se muestra anteriormente se pudo observar la lista de puertos que el servidor principal está escuchando, estos puertos son los siguientes:

- **Puerto 111:** Portman(8).
- **Puerto 8080:** Servicio web HTTP alternativo al puerto 80
- **Puerto 80:** Servicio webHTTP

- **Puerto 22:** Servicios de acceso remoto SSH,
- **Puerto 443:** Servicio web HTTPS.

Esta información permitió tener una idea clara sobre los servicios y posibles vulnerabilidades que posee nuestro servidor, además demostró que el servidor no posee ningún tipo de seguridades implementadas en el caso de Firewall o antivirus ni tampoco posee ninguna herramienta que permita mantener algún control sobre la información y posibles accesos a la misma.

Para profundizar la información de los servidores se realizó un escaneo utilizando Nessus en el cual encontramos la siguiente información:



0	0	1	1	16	18

Details

Severity	Plugin Id	Name
Medium (5.0)	12218	mDNS Detection
Low (3.2)	50686	IP Forwarding Enabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10223	RPC portmapper Service Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type

Gráfico 6.6. Reporte de Vulnerabilidades con NESSUS

Permitió mostrar las vulnerabilidades que posee el servidor entre los cuales destaca 1 vulnerabilidad con nivel medio, y 1 con nivel bajo las cuales debe ser tomado en cuenta con precaución por parte de adminitrador de la FISEI, estas vulnerabilidades se las describen a continuacion:

mDNS Detection

Esta vulnerabilidad hace referencia a la ejecucion ejecucion RendezVous ("también conocido como ZeroConf o mDNS"). Esta vulnerabilidad permite a los usuarios obtener información de servidor, lista de servicios, etc.

IP Forwarding Enabled

El host remoto tiene habilitado el reenvío IP. El servidor tiene habilitado el reenvío de IP's, este permite que un atacante pueda utilizar los paquetes a través del servidor, y potencialmente, pasar por alto algunos firewalls o routers.

6.8.3. Análisis de los Sistemas de Detección y Prevención de Intrusos.

Existen en el mercado gran cantidad de Sistemas de Detección y Prevención de Intrusos los cuales se los puede clasificar ya sea por el tipo si son basados en software libre o software propietario, si son multiplataforma, si son de host o de red y además si se basa en firmas o anomalías además de equipos completos hardware y software.

De un gran número de posibilidades, se escogió cuatro IDS/IPS para realizar una comparación de cada uno de ellos que se describen en el siguiente cuadro. Se tomó en consideración el decreto 1014 el cual indica la utilización de software libre como política de estado, de esta manera se pudo encontrar una herramienta que se ajuste a las necesidades de la FISEI. Para este análisis y comparación se ha tomado en cuenta la información proporcionada en artículos o documentos que se encuentran en el internet.

Las opciones que más destacan son las siguientes:

- OSIRIS
- PRELUDE
- SNORT.

- SHADOWN

IDS / IPS	Modelo de Detección	Tipos	Plataformas	Detalle
OSIRIS	Basado en Firmas	HIDS	Windows Mac OS x Solaris OpenBSD FreeBSD Linux	• Monitorea cambios en la red de información
PRELUDE	Anomalías	Hibrido	Mac OS x Solaris OpenBSD FreeBSD Linux	• Recoge, normaliza, clasifica, agrega, correlaciona y relata todos los eventos generados en un sistema.
SNORT	Basado en Firmas	Hibrido	Windows Unix / Linux	• Se puede modificar código fuente. • Se combina con elemento para mejor funcionamiento. • Posee gran cantidad de módulos que se adaptan a las necesidades del cliente
SHADOWN	Anomalías	NIDS	Windows Linux	• Procesa los archivos de Log Tcpdump. • Similar a Snort con la diferencia que no actúa en tiempo real

Tabla 6.17 Resumen de IDS/IPS

En base al resumen señalado en el cuadro anterior se pudo observar que OSIRIS trabaja un HIDS, al utilizar este sistema cuando se desea realizar un análisis de la información de la totalidad de la red OSIRIS no sería de mucha utilidad. Adicionalmente OSIRIS forma parte del proyecto OSSIM que es un IDS que trabaja con sensores de Snort.

Shadown posee un funcionamiento similar a Snort la principal desventaja es que no trabaja en tiempo real por lo tanto no beneficiará ya que se desea obtener información continua.

Prelude es un sensor de máquina que complementa protección que brinda snort, ya que utiliza su motor para la detección de ataques en red.

Snort es un sistema muy completo que brinda una cantidad de módulos para adaptarse a las necesidades que posea un administrador de sistemas para el manejo de la red. Snort es el sistema más descargado y utilizado a nivel mundial a diferencia de otras herramientas.

De las herramientas anteriormente mencionadas para la realización del presente trabajo se utilizó SNORT por los siguientes motivos:

- Es software libre
- De código abierto lo cual permite la manipulación de acuerdo a las necesidades y ataques detectados para su actualización
- Posee un excelente equipo de soporte en su portal web.
- Es un proyecto que se está actualizando continuamente.
- Brinda las posibilidades de trabajar con S.O Linux y Windows los cuales se encuentran instalados en la FISEI.
- Es la herramienta de seguridad más utilizada y descargada a nivel mundial.

6.8.4. Implementación de Solución Snort y SnortSam

Para la implementación y configuración de Snort y SnortSam, se trabajó en entornos virtuales, debido a que el departamento de Sistemas de la FISEI cuenta con un servidor de Virtualización.

A continuación se detallara cada uno de los pasos y configuraciones que se realizaron para la implementación de la solución.

6.8.4.1. Configuración de Tarjeta de Red y Firewall

6.8.4.1.1. Configuración Tarjeta de Red

Ya instalada la máquina se procedió a la configuración de la tarjeta de red, con el comando usado en la siguiente imagen.

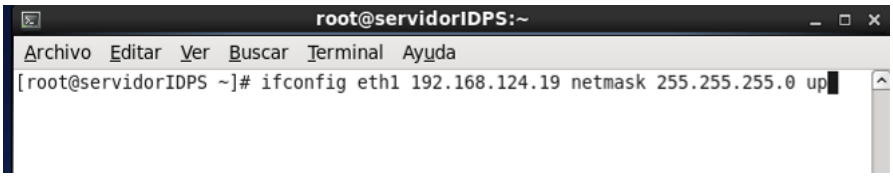


Gráfico 6.7. Configuración Tarjeta de Red

Se verificó la configuración de la tarjeta de Red.

Gráfico 6.8. Configuración de la Red

6.8.4.1.2. Deshabilitar Firewall

Adicionalmente se deshabilitó el cortafuegos de nuestro sistema operativo, esto se realizó con el comando setup en un terminal, se seleccionó configuración de cortafuegos y se lo deshabilito.

Gráfico 6.9. Configuración de cortafuegos

6.8.4.2. Instalación de Pre-Requisitos para SNORT

Se instalaron las librerías necesarias para poder instalar Snort, la versión a instalar fue snort-2.9.4.tar.gz, debido a que Snort al ser un elemento de seguridad es necesario que siempre se encuentre actualizado y la versión mencionada anteriormente fue liberada a finales del mes de noviembre.

6.8.4.2.1. Paquetes GCC y sus dependencias

La instalación del Paquete se lo realizó utilizando el comando yum. Primero se verificó que el paquete no se encuentre instalado, este paquete no se encuentra instalado por lo tanto procedemos a instalar el paquete gcc y sus dependencias

Comando yum install gcc

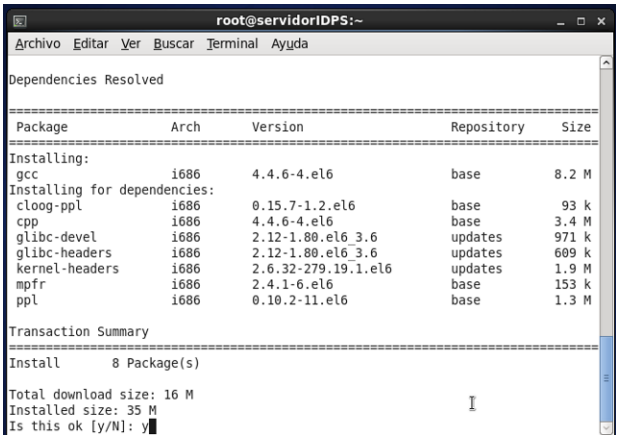


Gráfico 6.10. Snort Instalación gcc

También se instaló el paquete gcc-c++

Comando yum install gcc-c++

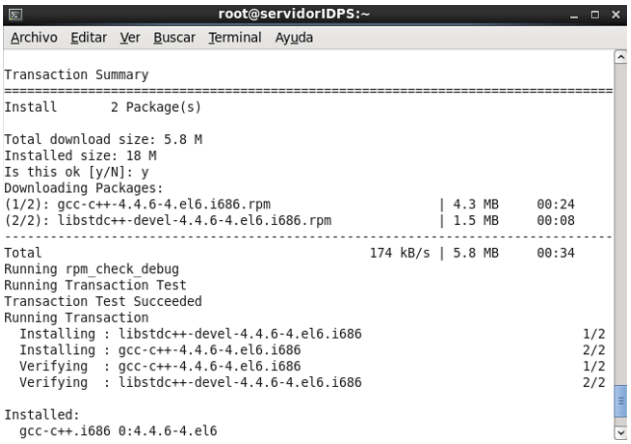


Gráfico 6.11. Snort Instalación gcc-c++

Para consultar las versiones de los paquetes se lo realizó con el comando rpm –q. La versión instalada es gcc 4.4.6.4.

6.8.4.2.2. Paquetes FLEX

Se verificó que el paquete no se encuentre instalado y de no estarlo se procedió a la instalación.

Comando: yum install flex

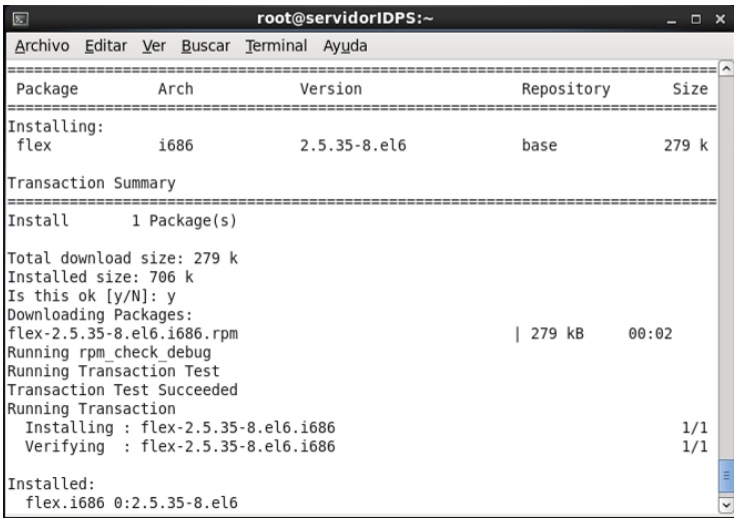


Gráfico 6.12. Snort Instalación flex

La versión que se instaló fue flex-2.5.35.8.

6.8.4.2.3. Paquete BISON

Se comprobó que no se encuentre instalado en el sistema y se procedió a la instalación del Paquete, se lo realizó utilizando el siguiente comando.

Comando: yum install bison

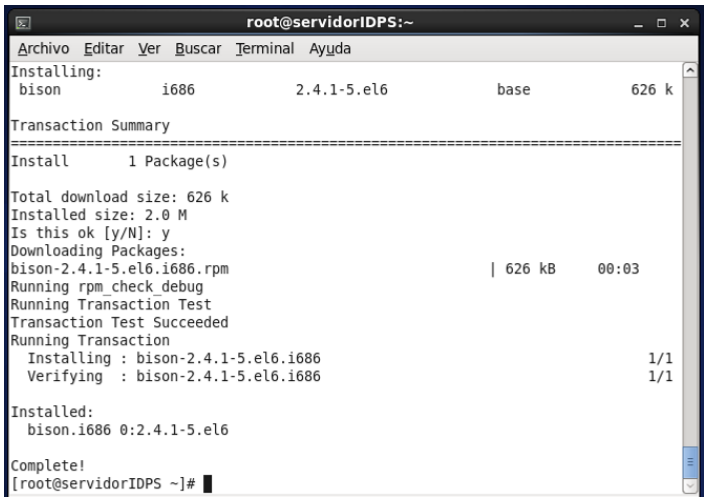


Gráfico 6.13. Snort Instalación Bison

La versión que se instaló fue Bison-2.4.1-5.

6.8.4.2.4. Paquete ZLIB

Al intentar instalar el paquete el sistema mostró que este paquete ya fue instalado.

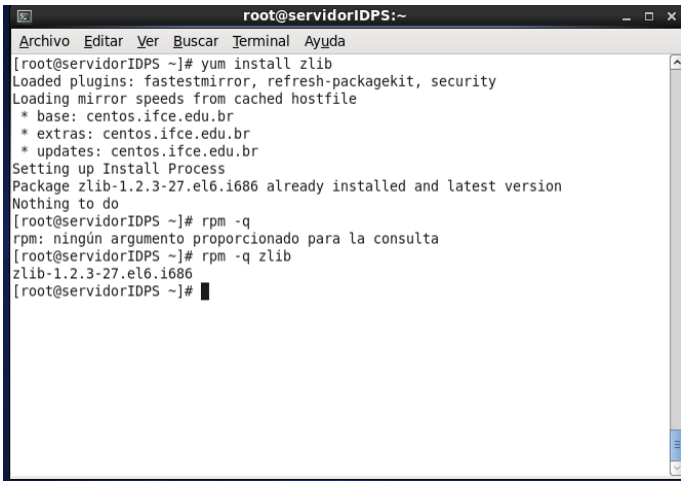


Gráfico 6.14. Snort Información ZLIB

La versión instalada fue zlib-1.2.3-27. Después se procedió a verificar adicionalmente si se encuentra instado el paquete zlib-devel, se encontró que esta dependencia no se encuentra instalada y se pudo continuar con su instalación.

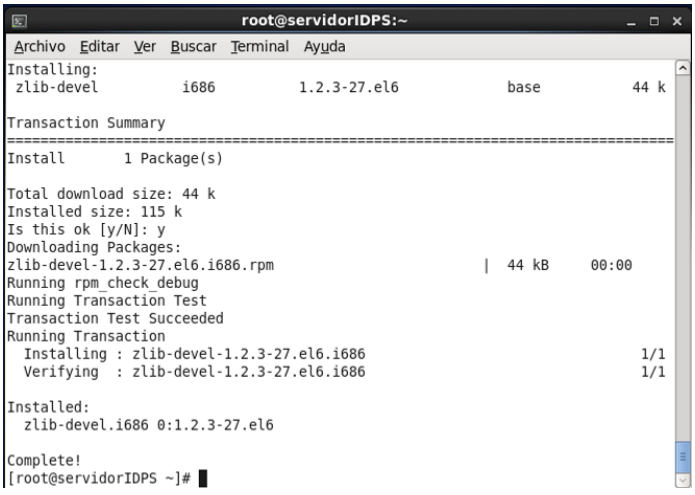


Gráfico 6.15. Snort Instalación ZLIB-devel

La versión que se instaló fue zlib-devel-1.2.3-27.

6.8.4.2.5. Paquete PCRE

El paquete ya estaba instalado por lo tanto no fue necesaria su instalación.

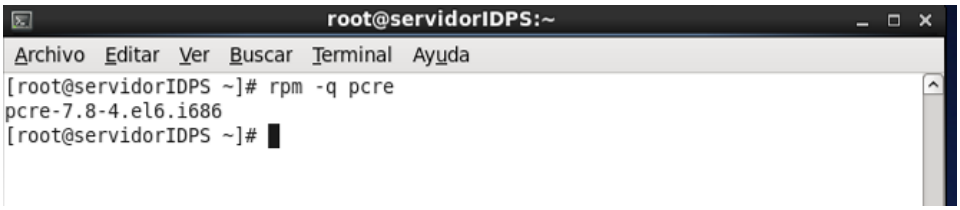


Gráfico 6.16. Snort Versión PCRE

Se instaló adicional el paquete pcre-devel.

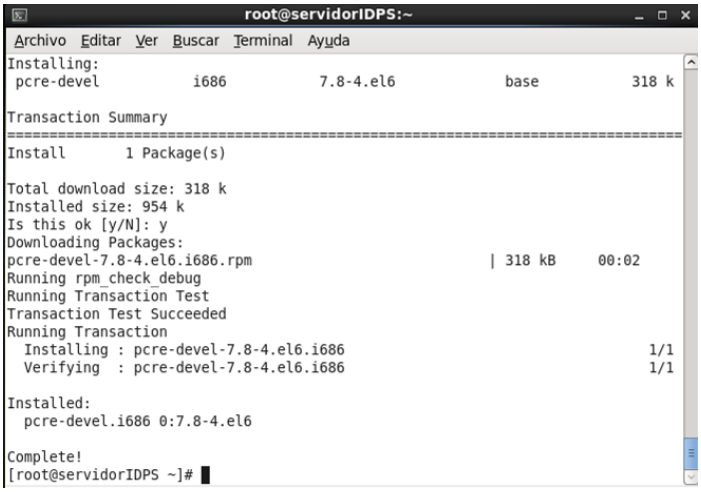


Gráfico 6.17. Snort Instalación PCRE-DEVEL

La versión que se instaló fue pcre-devel-7.8.4.

6.8.4.2.6. Paquete LIBPCAP

Primero se comprobó que el paquete no se encuentre instalado, en este caso el paquete ya se encontraba instalado.

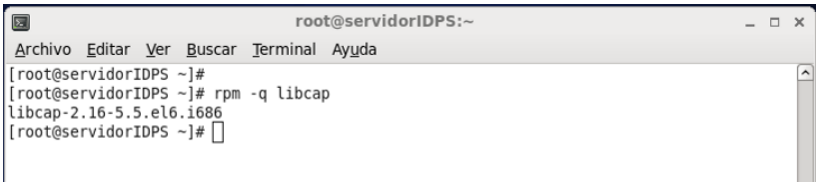


Gráfico 6.18. Snort Versión Libpcap

También se confirmó si el paquete Libpcap-Devel se encuentra instalado, en este caso no se encontraba por lo tanto se procedió a su instalación.

Gráfico 6.19. Snort Instalación Lipcap-devel

6.8.4.2.7. Paquete LIBDNET

Se confirmó que el paquete no se encuentre instalado, y se continuó con la instalación.

1. Se descargó la librería de la página http://libdnet.sourceforge.net/

2. Se copió la librería a la dirección /usr/local/src y se ubicó en dicha carpeta

   [root@servidorIDPS ~]# cp -r /home/FISEI/Escritorio/libdnet-1.11.tar.gz /usr/local/src/

   [root@servidorIDPS ~]# cd /usr/local/src/

3. Se descomprimió el archivo libdnet

   [root@servidorIDPS src]# tar -zcvf libdnet-1.11.tar.gz

4. Y se procedió a ubicar en la carpeta libnet-1.11, se configuró, compiló e instaló.

   [root@servidorIDPS src]# cd libdnet-1.11
   [root@servidorIDPS libdnet-1.11]# ./configure --with-pic && make && make install

6.8.4.2.8. Paquete TCPDUMP

Primero se verificó que el paquete no se encuentre instalado, pero este paquete si encuentra instalado por lo que se verifica la versión.

La versión instalada fue tcpdump-4.0.0.3.

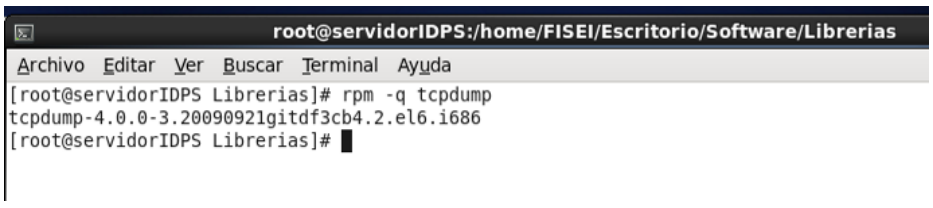


Gráfico 6.20. Snort Versión TCPDUMP

6.8.4.3. Instalación Daq

Se creó una carpeta en el escritorio llamada Software y dentro de esta se creó la carpeta denominada Snort.

[root@servidorIDPS /]# mkdir /home/FISEI/Escritorio/Software/Snort

En esta carpeta se almacenaron los archivos descargados y necesarios para la instalación.

La instalación de Snort se realizó de forma manual, debido a que fue necesario conocer y modificar ciertos archivos para optimizar el rendimiento del mismo, primero se descargó Snort de la página Oficial www.snort.org. Los dos archivos a descargar son SNORT y DAQ.

"Data AcQuisition library (DAQ), para el paquete de I/O. El DAQ sustituye llamadas directas en las librerías, como PCAP con una capa de abstracción que hacen que sea fácil añadir software adicional o implementaciones de hardware de captura de paquetes. "

1. Se descargó DAQ.

   Link: http://www.snort.org/snort-downloads/

2. Se procedió a copiar a la carpeta usr/local/src y posterior se ubicó en dicha carpeta.

   [root@servidorIDPS snort]# cp –r daq-2.0.0.tar.gz /usr/local/src/
   root@servidorIDPS ~]# cd /usr/local/src/

3. Después se descomprimió el archivo DAQ.

   [root@servidorIDPS src]# tar -zxvf daq-2.0.0.tar.gz

4. Se configuró, compiló e instaló DAQ.

   [root@servidorIDPS daq-2.0.0]#./configure && make && make install

6.8.4.4. Instalación Snort

1. Se descargó SNORT.

   Link: http://www.snort.org/snort-downloads/
   Link versiones anteriores:
   http://sourceforge.net/projects/snort.mirror/files/

2. Se copió a la carpeta usr/local/src.

   [root@servidorIDPS snort]# cp –r snort-2.9.4.tar.gz /usr/local/src/

3. Se procedió a descomprimir el archivo SNORT-2.9.4.

   [root@servidorIDPS src]# tar -zxvf snort-2.9.4.tar.gz

4. Finalmente se configuró, compiló e instaló SNORT.

   [root@servidorIDPS snort-2.9.4]# ./configure --enable-sourcefire && make && make install

6.8.4.5. Creación de carpetas para funcionamiento de Snort

Al instalar snort el paquete de instalación creó las siguientes carpetas para el funcionamiento de snort:

- Se creó la carpeta SNORT la cual será el directorio principal o de trabajo en donde se guardaran todos los archivos de configuración de snort **etc/snort.**

- Se creó la carpeta SNORT_DYNAMICRULES en el directorio **/usr/local/lib/.**

  [root@servidorIDPS lib]# cd /usr/local/lib/snort_dynamicrules

- Adicionalmente se creó una nueva carpeta que se llamara barnyard2 aquí se almacenaran los logs para posteriormente trabajaran con la base de datos.

  [root@servidorIDPS /]# mkdir -p /var/log/barnyard2

6.8.4.6. Incorporación de Reglas

El paquete de reglas se lo puede encontrar en la página www.snort.org, Snort posee un paquete de reglas VTR para poder descargarlas se debe tener una suscripción de tipo personal o empresarial, el precio difiere para cada una de ellas, pero también al registrarse en la página se puede tener acceso a las mismas reglas pero de un mes atrás.

1. Se descargó las reglas de la página.

   Link: http://www.snort.org/snort-rules

2. Se copió a la carpeta de descargas **usr/local/src.**

   [root@servidorIDPS snort]# cp –r snortrules-snapshot-2940.tar.gz /usr/local/src/

3. Se descomprimió el paquete con las reglas de snort.

   [root@servidorIDPS src]# tar –zxvf snortrules-snapshot-2940.tar.gz

4. Se copió las reglas de la carpeta **usr/local/src** a la carpeta **etc/snort.**

   [root@servidorIDPS src]# cp –rf rules/ so_rules/ etc/ prepoc_rules/ /etc/snort

5. Se procedió a crear dos archivos dentro de la carpeta rules denominados **white_list_rules** y **black_list_rules.**

   [root@servidorIDPS /]# touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules

6. Se movió los archivos dentro de la carpeta **/etc** que acabamos de copiar a la carpeta **/etc/snort**.

   [root@servidorIDPS etc]# mv -r classification.config reference.config snort.conf unicode.map gen-msg.map sid-msg.map threshold.conf /etc/snort

6.8.4.7. Creación de Usuario y Permisos

Se creó el Grupo Snort y dentro de este grupo el usuario snort.

[root@servidorIDPS /]# groupadd -g 40000 snort

[root@servidorIDPS /]# useradd snort -d /var/log/snort -s /sbin/nologin -c SNORT_IDS -g snort

Se colocó en la carpeta snort y se asignó permisos a todas las carpetas que se encuentran dentro de la misma.

[root@servidorIDPS /]# cd /etc/snort
[root@servidorIDPS snort]# chown -R snort:snort *

Tendrá los permisos sobre la carpeta **/var/log/snort** y se agregó los permisos a las siguiente carpetas **/var/log/barnyard2.**

[root@servidorIDPS snort]# chown -R snort:snort /var/log/snort
[root@servidorIDPS snort]# chown -R snort:snort /var/log/barnyard2

Se verificó que las carpetas mencionadas tengan los permisos del usuario snort con el siguiente comando:

[root@servidorIDPS src]# ls – al

Se colocó en la carpeta /usr/local/lib y se le dio permisos de grupo y usuario snort 700 a las carpetas /snort /snort_dynamicengine /snort_dynamicpreprocessor.

[root@servidorIDPS /]#cd /usr/local/lib
[root@servidorIDPS lib]# chown -R snort:snort snort*
[root@servidorIDPS lib]# chown -R snort:snort snort_dynamic*
[root@servidorIDPS lib]# chown -R snort:snort pkgconfig
[root@servidorIDPS lib]# chmod -R 700 snort*
[root@servidorIDPS lib]# chmod -R 700 pkgconfig

Se dirigió a la carpeta /usr/local/bin y se asignó permisos de grupo y usuario snort 700 a las carpetas /snort /snort_dynamicengine /snort_dynamicpreprocessor
[root@servidorIDPS bin]# cd /usr/local/bin

[root@servidorIDPS bin]# chown -R snort:snort daq-modules-config

[root@servidorIDPS bin]# chown -R snort:snort u2*

[root@servidorIDPS bin]# chmod -R 700 daq-modules-config

[root@servidorIDPS bin]# chmod 700 u2*

Después se ubicó en la carpeta /etc y se asignó permisos de grupo y usuario snort 700 a las carpetas /snort /snort_dynamicengine /snort_dynamicpreprocessor

[root@servidorIDPS etc]# chown -R snort:snort snort

[root@servidorIDPS etc]# chmod –R 700 snort

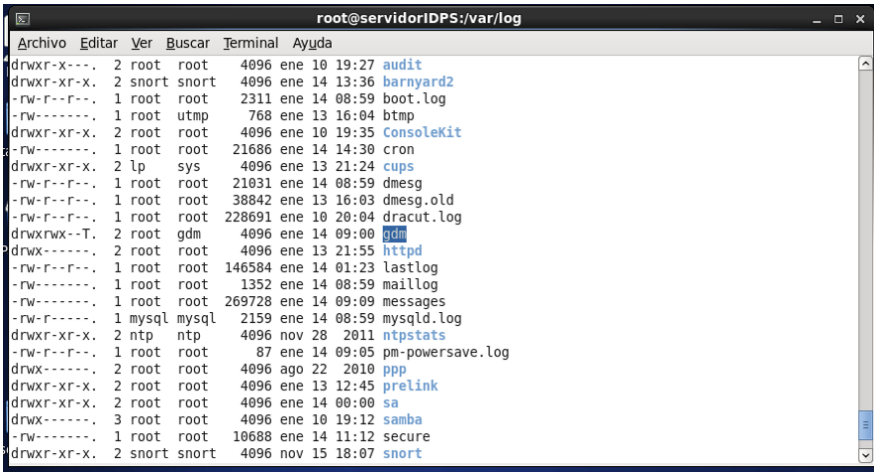


Gráfico 6.21. Permisos Usuarios

6.8.4.8. Configuración Archivo Snort.conf

1. Se descomentó y poner la red que se iba a monitorear.

   ipvar HOME_NET 192.168.X.X/24

2. Se descomentó y escribió la palabra any para que detecte cualquier red externa.

ipvar EXTERNAL_NET any

3. Se agregó los puertos que se encontró en el análisis de la red para que fueran asegurados con la opción portvar dependiendo el servicio que cada uno de ellos brinde.

   # List of ports you run web servers on portvar HTTP_PORTS []

4. También se descomentó y seleccionar la ubicación correcta donde se encuentre las carpetas de las reglas y preprocesadores con los cuales trabaja snort en las siguientes líneas.

   var RULE_PATH /etc/snort/rules
   var SO_RULE_PATH /etc/snort/so_rules
   var PREPROC_RULE_PATH /etc/snort/preproc_rules

5. Se descomentó he ingresó la ubicación de los dos archivos que se crearon junto con las reglas.

   var WHITE_LIST_PATH /etc/snort/rules
   var BLACK_LIST_PATH /etc/snort/rules

6. Se descomentó la línea de salida para el intérprete de información barnyard2 de tipo unified2.

   output unified2: filename snort.log. limit 128

7. Y se comentó todas las líneas **$RULE_PATH** y solamente se dejó la línea **$RULE_PATH/local.rules**, aquí se procedió a crear una regla para realizar una prueba con Snort para posteriormente des comentar las líneas que se necesitan.

8. Finalmente se añadió la siguiente regla dentro de **local.rules** la cual permitió verificar si Snort está captando tráfico.

[root@servidorIDPS src]# nano etc/snort/rules/local.rule

Regla: alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:1;)

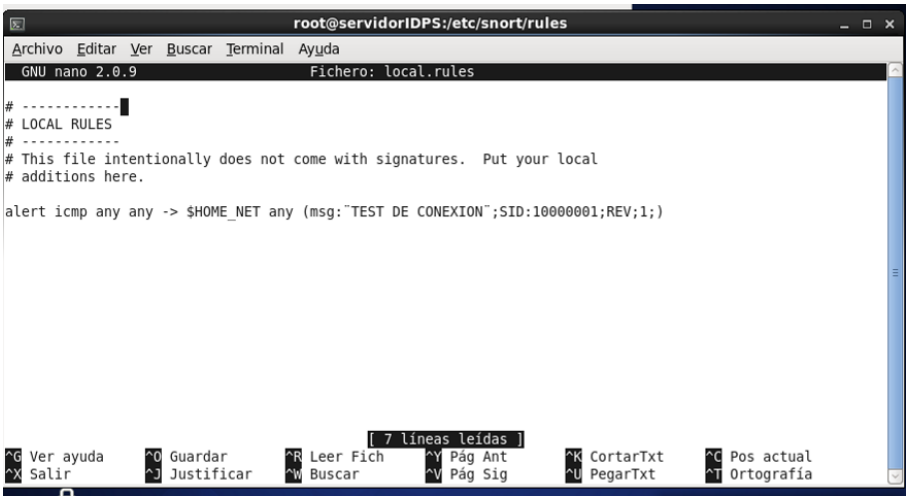


Gráfico 6.22. Agregando regla rule.local a Snort.conf

Esta es la configuración básica de snort, que posteriormente se agregará configuraciones según la información de la red de la FISEI.

6.8.4.9. Script para iniciar el servicio

Para que Snort pueda funcionar se necesitó un script que permitió iniciar, reiniciar, parar, el servicio de snort, este script se lo pudo encontrar en la página web de snort www.snort.org y existe para varias versiones de Linux se los puede escoger dependiendo del sistema operativo.

Se necesitó crear dos archivos con el nombre:

1. Un archivo se creó en el directorio /etc/init.d/.

[root@servidorIDPS init.d]# cd etc/init.d/

[root@servidorIDPS init.d]# nano snort

Y se procedió a copiar el siguiente script:

```
#!/bin/bash
#
# snort                 Start up the SNORT Intrusion Detection System daemon
#
# chkconfig: 2345 55 25
# description: SNORT is a Open Source Intrusion Detection System
#              This service starts up the snort daemon.
#
# processname: snort
# pidfile: /var/run/snort_eth0.pid

### BEGIN INIT INFO
# Provides: snort
# Required-Start: $local_fs $network $syslog
# Required-Stop: $local_fs $syslog
# Should-Start: $syslog
# Should-Stop: $network $syslog
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: Start up the SNORT Intrusion Detection System daemon
# Description:       SNORT is an application for Open Source Intrusion Detection.
#                            This service starts up the Snort IDS daemon.
### END INIT INFO

# source function library
. /etc/rc.d/init.d/functions

# pull in sysconfig settings
[ -f /etc/sysconfig/snort ] && . /etc/sysconfig/snort

RETVAL=0
prog="snort"
lockfile=/var/lock/subsys/$prog

# Some functions to make the below more readable
SNORTD=/usr/local/bin/snort
#OPTIONS="-A fast -b -d -D -i eth0 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort"
#PID_FILE=/var/run/snort_eth0.pid
```

```
# Convert the /etc/sysconfig/snort settings to something snort can
# use on the startup line.
if [ "$ALERTMODE"X = "X" ]; then
  ALERTMODE=""
else
  ALERTMODE="-A $ALERTMODE"
fi

if [ "$USER"X = "X" ]; then
  USER="snort"
fi
if [ "$GROUP"X = "X" ]; then
  GROUP="snort"
fi

if [ "$BINARY_LOG"X = "1X" ]; then
  BINARY_LOG="-b"
else
  BINARY_LOG=""
fi

if [ "$LINK_LAYER"X = "1X" ]; then
  LINK_LAYER="-e"
else
  LINK_LAYER=""
fi

if [ "$CONF"X = "X" ]; then
  CONF="-c /etc/snort/snort.conf"
else
  CONF="-c $CONF"
fi

if [ "$INTERFACE"X = "X" ]; then
  INTERFACE="-i eth0"
  PID_FILE="/var/run/snort_eth0.pid"
else
  PID_FILE="/var/run/snort_$INTERFACE.pid"
  INTERFACE="-i $INTERFACE"
fi

if [ "$DUMP_APP"X = "1X" ]; then
  DUMP_APP="-d"
else
  DUMP_APP=""
fi

if [ "$NO_PACKET_LOG"X = "1X" ]; then
  NO_PACKET_LOG="-N"
```

```
else
  NO_PACKET_LOG=""
fi

if [ "$PRINT_INTERFACE"X = "1X" ]; then
  PRINT_INTERFACE="-I"
else
  PRINT_INTERFACE=""
fi

if [ "$PASS_FIRST"X = "1X" ]; then
  PASS_FIRST="-o"
else
  PASS_FIRST=""
fi

if [ "$LOGDIR"X = "X" ]; then
  LOGDIR=/var/log/snort
fi

# These are used by the 'stats' option
if [ "$SYSLOG"X = "X" ]; then
  SYSLOG=/var/log/messages
fi

if [ "$SECS"X = "X" ]; then
  SECS=5
fi

if [ ! "$BPFFILE"X = "X" ]; then
  BPFFILE="-F $BPFFILE"
fi

runlevel=$(set -- $(runlevel); eval "echo \$$#" )

start()
{
        [ -x $SNORTD ] || exit 5

        echo -n $"Starting $prog: "
        daemon --pidfile=$PID_FILE $SNORTD $ALERTMODE $BINARY_LOG
$LINK_LAYER $NO_PACKET_LOG $DUMP_APP -D $PRINT_INTERFACE
$INTERFACE -u $USER -g $GROUP $CONF -l $LOGDIR $PASS_FIRST $BPFFILE
$BPF && success || failure
        RETVAL=$?
        [ $RETVAL -eq 0 ] && touch $lockfile
        echo
        return $RETVAL
}
```

```
stop()
{
        echo -n $"Stopping $prog: "
        killproc $SNORTD
        if [ -e $PID_FILE ]; then
           chown -R $USER:$GROUP /var/run/snort_eth0.* &&
           rm -f /var/run/snort_eth0.pi*
        fi
        RETVAL=$?
        # if we are in halt or reboot runlevel kill all running sessions
        # so the TCP connections are closed cleanly
        if [ "x$runlevel" = x0 -o "x$runlevel" = x6 ] ; then
           trap " TERM
           killall $prog 2>/dev/null
           trap TERM
        fi
        [ $RETVAL -eq 0 ] && rm -f $lockfile
        echo
        return $RETVAL
}

restart() {
        stop
        start
}

rh_status() {
        status -p $PID_FILE $SNORTD
}

rh_status_q() {
        rh_status >/dev/null 2>&1
}

case "$1" in
        start)
                rh_status_q && exit 0
                start
                ;;
        stop)
                if ! rh_status_q; then
                        rm -f $lockfile
                        exit 0
                fi
                stop
                ;;
        restart)
                restart
                ;;
        status)
```

```
                rh_status
                RETVAL=$?
                if [ $RETVAL -eq 3 -a -f $lockfile ] ; then
                        RETVAL=2
                fi
                ;;
        *)
                echo $"Usage: $0 {start|stop|restart|status}"
                RETVAL=2
esac
exit $RETVAL
```

2. Se agregó un enlace simbólico.

[root@servidorIDPS sbin]# cd usr/sbin/

[root@servidorIDPS sbin]# ln -s /usr/local/bin/snort snort

3. El segundo archivo se creó en el directorio /etc/sysconfig.

[root@servidorIDPS /]# cd etc/sysconfig/

[root@servidorIDPS init.d]# nano snort

Y se copió el siguiente script:

```
# /etc/sysconfig/snort
# $Id: snort.sysconfig,v 1.8 2003/09/19 05:18:12 dwittenb Exp $

#### General Configuration

INTERFACE=eth0
CONF=/etc/snort/snort.conf
USER=snort
GROUP=snort
PASS_FIRST=0

#### Logging & Alerting

LOGDIR=/var/log/snort
ALERTMODE=fast
DUMP_APP=1
```

BINARY_LOG=1
NO_PACKET_LOG=0
PRINT_INTERFACE=0

4. Se asignó permisos del grupo snort con permiso 700.

[root@servidorIDPS sysconfig]# chown -R snort:snort snort
[root@servidorIDPS sysconfig]# chown -R 700 snort

6.8.4.10. Validación de configuración, inicialización y prueba de Snort

Para realizar la inicialización de Snort se realizó los siguientes pasos:

Se dirigió a la carpeta **/usr/sbin.**

[root@servidorIDPS lib]# cd /usr/sbin

Se inicializó el servicio de SNORT y se verificó que se encuentre correctamente instalado con el siguiente comando.

[root@servidorIDPS sbin]# ./snort -T -i eth0 -u snort -g snort -c /etc/snort/snort.conf

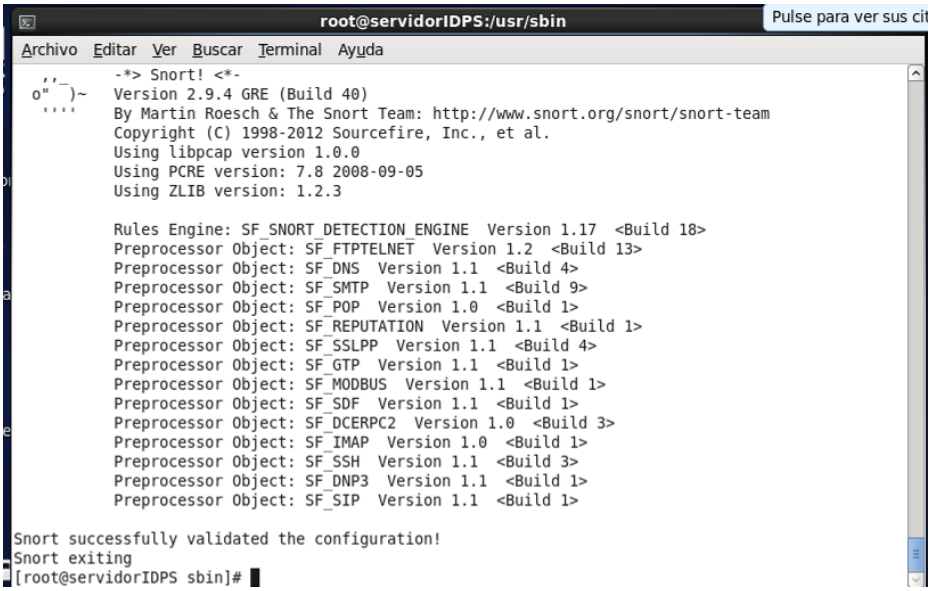


Gráfico 6.23. Configuración Satisfactoria

En la imagen anterior se pudo observar que la configuración de snort fue realizada con éxito, snort ya se encuentra funcionando en la red de la FISEI como un IDS, a continuación se realizó la primera prueba, la cual consiste en verificar el funcionamiento de snort en modo snnifer.

En las configuraciones iniciales, se agregó una regla al archivo /snort/rules/local.rule solicitando que se genere una alerta cuando se realice un ping a cualquier máquina de la red de la FISEI y nos muestre el mensaje “test de conexión ICMP”

Se realizó un ping desde la maquina 192.168.0124.12 hacia la maquina 192.168.124.19

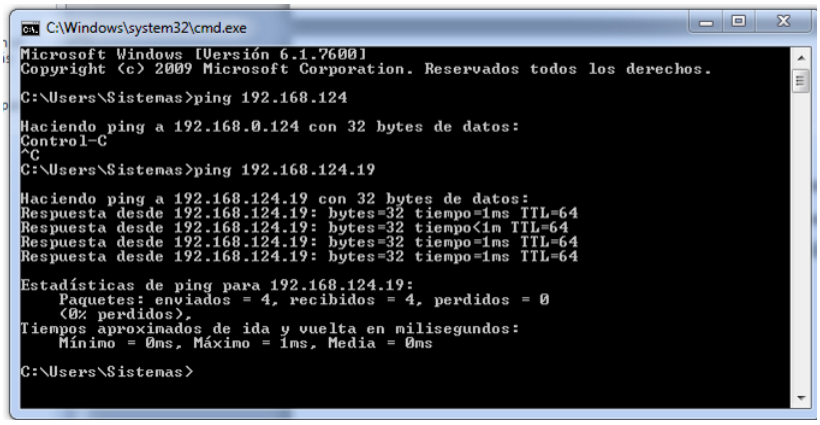


Gráfico 6.24. Prueba Snort Ping

Se ingresó el siguiente comando para que SNORT capture el tráfico que circula por la red y aplique la regla configurada.

[root@servidorIDPS sbin]# ./snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

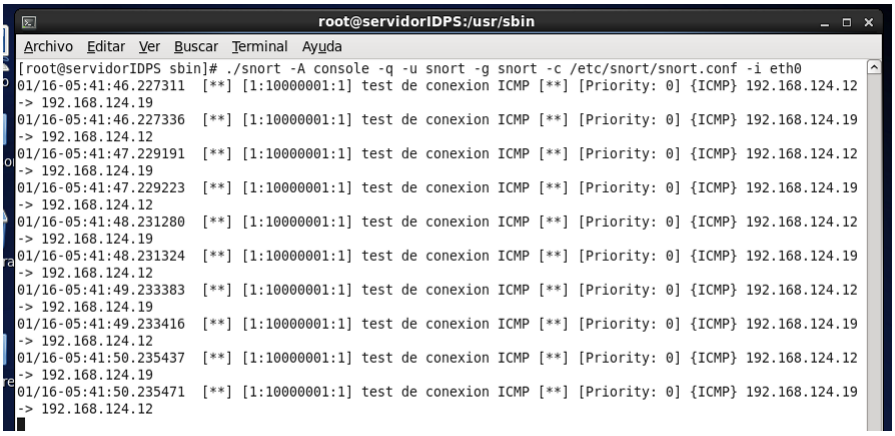


Gráfico 6.25. Generación de alerta snort

6.8.4.11. Back end - MYSQL

La base de datos permitirá almacenar la información generada por snort, se procedió a instalar la base de datos MySql, en la cual se generó un usuario

específicamente para snort, se creó una base de datos denominada snort la cual se encuentra dentro del paquete de instalación de barnyard2.

6.8.4.11.1. Instalación Mysql

Para instalar MySql y sus dependencias o paquetes necesarios se utilizó el siguiente comando.

[root@servidorIDPS /]# yum install mysql mysql-bench mysql-server mysql-devel mysqlclient10

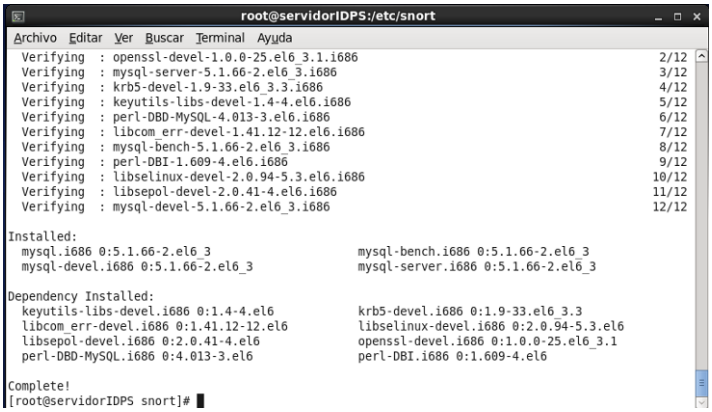


Gráfico 6.26. Instalación Mysql

La versión instalada de Mysql fue mysql-5.1.66-2.

Gráfico 6.27. Versión Mysql

Se inició el servicio.

[root@servidorIDPS /]# service mysqld start

Se configuró para que mysql se inicie inmediatamente después de apagar o reiniciar el sistema

[root@servidorIDPS /]# chkconfig mysqld on

6.8.4.11.2. Configuración y creación de base de datos SNORT

Se creó un usuario denominado snort junto con la base de datos con el mismo nombre y se le asignó los privilegios totales.

1. Se conectó al servidor MySQL:

   [root@servidorIDPS /]# mysql -u root

2. Se asignó privilegios y una contraseña al usuario root.

   mysql> GRANT ALL PRIVILEGES ON mysql.*TO 'root'@'localhost' IDENTIFIED BY 'contraña';

3. Se creó la base de datos donde se almacenará la información que genere snort.

   mysql> CREATE DATABASE snort;

4. Se creó un usuario denominado snort el cual tendrá todos los privilegios sobre la base de datos snort.

   mysql> GRANT ALL PRIVILEGES ON snort.*TO 'snort'@'localhost' IDENTIFIED BY 'contraseña';

   set password for 'snort'@'localhost' = password('snortbdd!');

5. Para salir de MySQL se ejecutó el siguiente comando.

   mysql> exit.

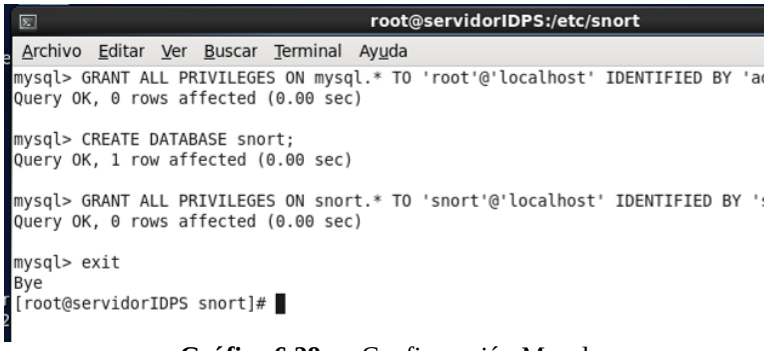


Gráfico 6.28. Configuración Mysql

6.8.4.12. Front-End - BASE

Para la visualización de información de manera gráfica se instaló la herramienta BASE.

6.8.4.12.1. Requisitos de BASE

Para instalar de manera adecuada la herramienta Base se debe tener instalado:

- Apache
- PHP
- Barnyard2

6.8.4.12.1.1. Instalación de Apache

Para instalar apache se utilizó el comando.

[root@servidorIDPS /]# yum install httpd

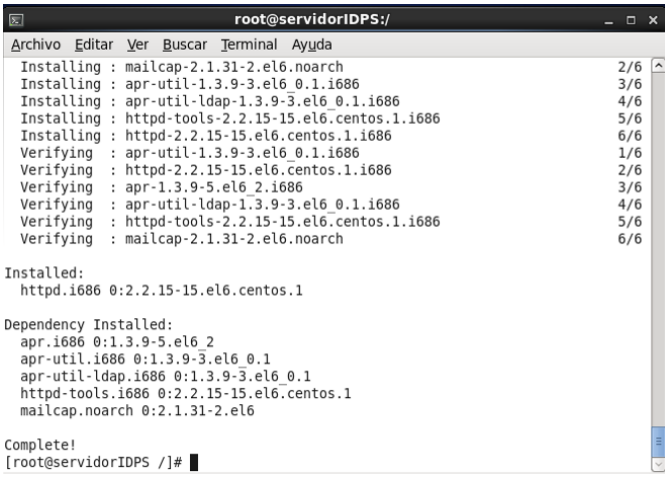


Gráfico 6.29. Instalación Apache

La versión instalada fue: httpd-2.2.15-15.el6

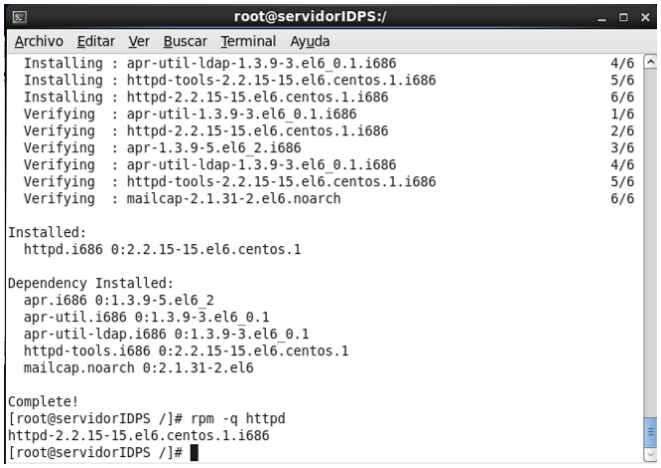


Gráfico 6.30. Versión de Apache

Se inició el servicio.

[root@servidorIDPS /]# service httpd start

Se configuró para que apache se inicie inmediatamente después de apagar o reiniciar el sistema.

[root@servidorIDPS /]# chkconfig httpd on

Para comprobar que apache fue instalado correctamente se creó un archivo en var/www/html llamado index.html el cual contiene la siguiente información.

Gráfico 6.31. Código HTML para prueba Apache

Se escribió en el navegador http://localhost y mostró la página index.html indicando que apache se instaló correctamente.

Gráfico 6.32. Página Web de prueba

6.8.4.12.1.2. Instalación de PHP

Se instaló php y sus dependencias, además se agregó la librería gd que ayudará para la visualización de imagen mediante php.

[root@servidorIDPS /]# yum install gd php php-mysql php-pear php-gd

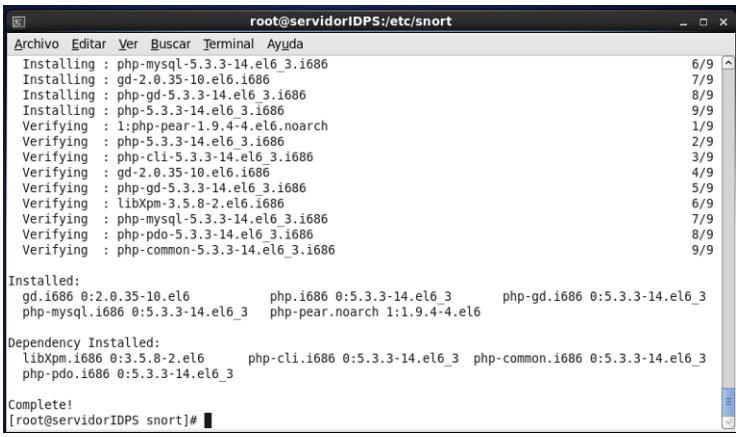


Gráfico 6.33. Instalación PHP y GD

La versión instalada fue: php -5.3.3-14.el6_3.i686.

Gráfico 6.34. Versión PHP

6.8.4.12.1.3. Instalación de Barnyard2

Para la instalación seguimos los siguientes pasos:

1. Se descargó Barnyard2 de su página

   http://www.securixlive.com/barnyard2/download.php

2. Se copió a la carpeta usr/loca/src donde se encontraban los archivos de instalación y se tubo que ubicar en dicha carpeta.

[root@servidorIDPS /]# cp -p home/FISEI/Escritorio/barnyard2-1.9.tar.gz /usr/local/src/

[root@servidorIDPS /]# cd usr/local/src/

3. Se descomprimió la carpeta barnyard2-1.9.

   [root@servidorIDPS src]# tar -zxvf barnyard2-1.9.tar.gz

4. Posteriormente se configuró, compiló e instaló barnyard2

   [root@servidorIDPS src]# cd barnyard2-1.9
   [root@servidorIDPS barnyard2-1.9]# ./configure --with-mysql && make && make install

5. Se copió el archivo de configuración barnyard.conf a la carpeta de snort.

   [root@servidorIDPS barnyard2-1.9]# cp -p etc/barnyard2.conf /etc/snort/

6. Se creó la base de datos con la que funciona snort que se encuentra dentro de la carpeta barnyard2-1.9/schemas.

   [root@servidorIDPS barnyard2-1.9]# mysql -u root -p snort </usr/local/src/barnyard2-1.9/schemas/create_mysql
   Enter password:

7. Se verificó que se haya creado las tablas.
   [root@servidorIDPS barnyard2-1.9]# mysql -u root -p snort
   Enter password:
   mysql> use snort;

Database changed

mysql> show tables;

mysql> exit

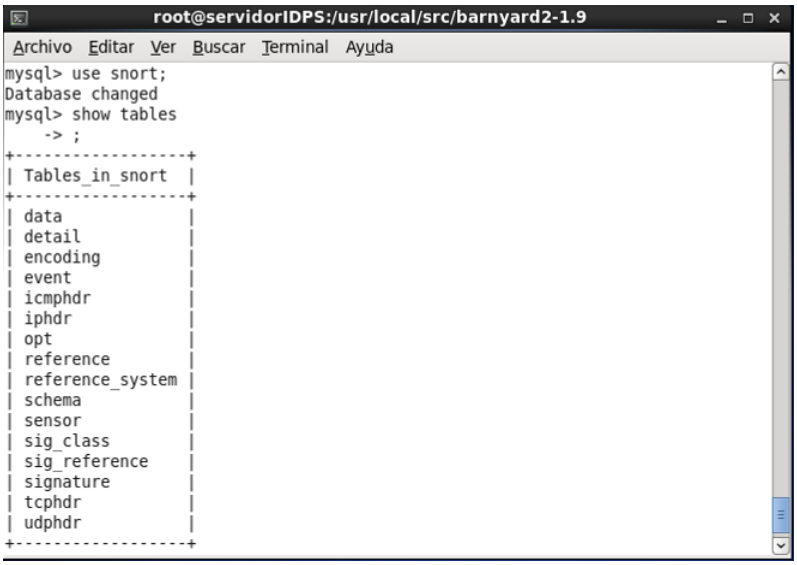


Gráfico 6.35. Tablas creadas en la base de datos SNORT

8. Se configuró el archivo /etc/snort/barnyard.conf para que pueda envir la informacion de snort hacia la base d datos mysql

   [root@servidorIDPS snort]# nano barnyard2.conf

   config hostname: localhost
   config interface: eth0
   input unified2
   output database: log, mysql, user=snort password=****** dbname=snort **host**=localhost

9. Se visualizó los archivos que se generearon en var/log/snort/, se procedió a crear un archivo barnyard.waldo y se agregó la línea con el log generado dentro de /var/log/snort.

   [root@servidorIDPS snort]# cd var/log/snort/

[root@servidorIDPS /]# nano var/log/snort/barnyard.waldo

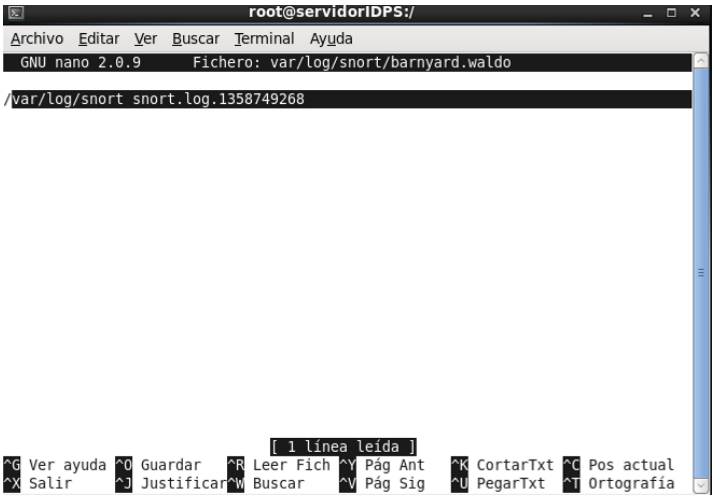


Gráfico 6.36. Configurcion Barnyard2

10. Se descargó y copió el archivo para inicializar los daemons de barnyard y se convertió en un archivo ejecutable.

    [root@servidorIDPS src]# wget http://www.internetsecurityguru.com/barnyard

    [root@servidorIDPS init.d]# cp barnyard /etc/init.d/

    [root@servidorIDPS init.d]# chmod +x /etc/init.d/barnyard

    [root@servidorIDPS init.d]# chkconfig barnyard on

11. Se ingreso el siguiente comando para ejecutar barnyar2 en modo continuo y especificamos los ficheros para que puedan ser traducidos los generadores

    [root@servidorIDPS /]# /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map -d /var/log/snort -f snort.log -w /var/log/snort/barnyard.waldo

snort.log.1359385044

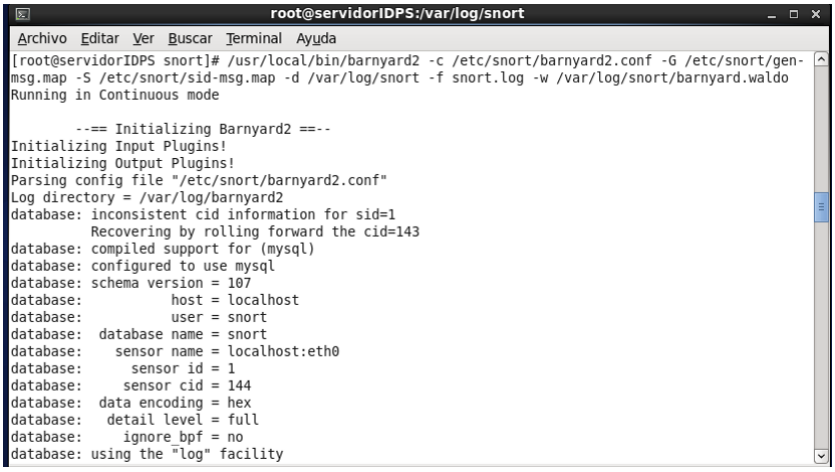


Gráfico 6.37. Barnyard2 Inicializando

12. Se visualizó la base de datos en la tabla eventos y se verificó que se este registrando la información

[root@servidorIDPS /]# mysql -u root –p

Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.1.66 Source distribution

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use snort;
Reading table information for completion of table and column names

You can turn off this feature to get a quicker startup with -A

Database changed

mysql> select * from event

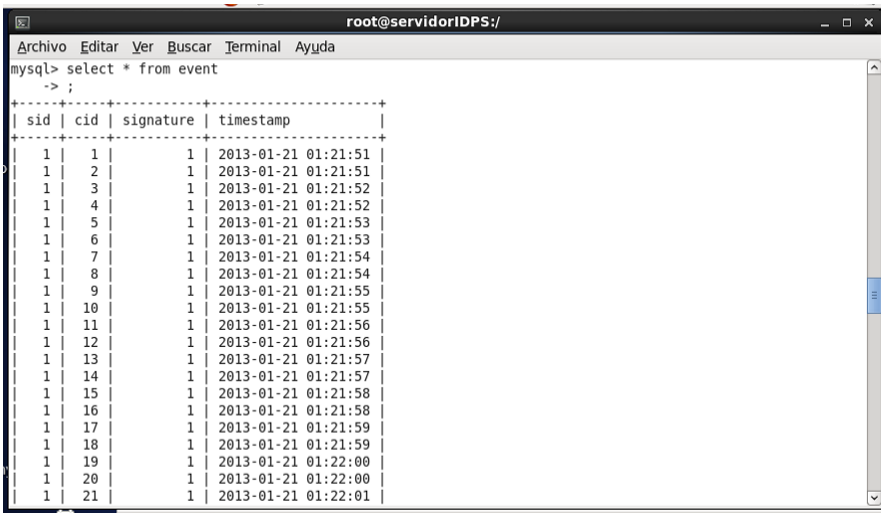


Gráfico 6.38. Información de Eventos almacenados en MySql

6.8.4.12.2. Instalación de BASE

1. Se instaló las dependencias de pear que necesita base para mostrar gráficos, textos ,etc.

   [root@servidorIDPS /]# pear install Image_Color
   [root@servidorIDPS /]# pear install Image_Canvas-alpha
   [root@servidorIDPS /]# pear install Image_Graph-alpha
   [root@servidorIDPS /]# pear install Numbers_Roman

2. Descargamos ADOBD y BASE de los siguientes links

   - http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/

- http://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-518-for-php5/

3. Se descomprimió los archivos dentro de la carpeta usr/local/src,

   [root@servidorIDPS src]# tar -zxvf base-1.4.5.tar.gz
   [root@servidorIDPS src]# tar -zxvf adodb518a.gz

4. Se ingresó a la carpeta a /var/www/html y se renombro el archive base-1.4.5 por base y copiamos la carpeta de adobd5

   [root@servidorIDPS html]# mv /usr/local/src/base-1.4.5 base
   [root@servidorIDPS html]# cp -rf /usr/local/src/adodb5 /var/www/html/

5. Se ingresó en la carpeta /base y se copió el archivo base_conf.php.dist, se le dió el nuevo nombre base_conf.php este archivo es el principal de base para la configuración

   [root@servidorIDPS html]# cd base/
   [root@servidorIDPS base]# cp base_conf.php.dist base_conf.php

6. Se configuró el archivo de base base_conf.

   Se cambiamó el idioma para la instalación a español

   - $BASE_Language = 'spanish';

   Se ingresó la dirección en donde se encuentra ubicado BASE.

   - $BASE_urlpath = '/base';

   Se ingresó la dirección en donde se encuentra ubicado ADOBD.

- $DBlib_path = '/adodb5';

Se configuró la información sobre MySql.

- $DBtype = 'mysql';
- $alert_dbname = 'snort';
- $alert_host = 'localhost';
- $alert_port = '';
- $alert_user = 'snort';
- $alert_password = 'snortbdd!';

7. Se modificó el nivel de reporte para php que no de problemas al mostrar la información.

   [root@servidorIDPS /]# nano etc/php.ini

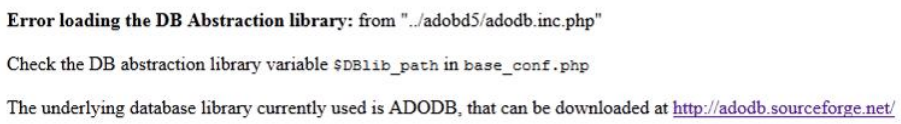
   Se modificó la línea error_reporting.
   error_reporting = E_ALL & ~E_NOTICE

8. Se restauró el servicio de apache.

   [root@servidorIDPS base]# service httpd restart

9. Se ingresó en la página web para iniciar con la configuración.

   http://192.168.124.19/base/base_main.php



Error instalación Base

Apareció el error anterior ya que se encuentra mal el nombre de la carpeta adobd5, se corregió con el nombre correcto adodb5.

Gráfico 6.39. Configuración de Base

10. Se seleccionó la opción de página de configuración y nos aparecerió la opción para crear la base de datos

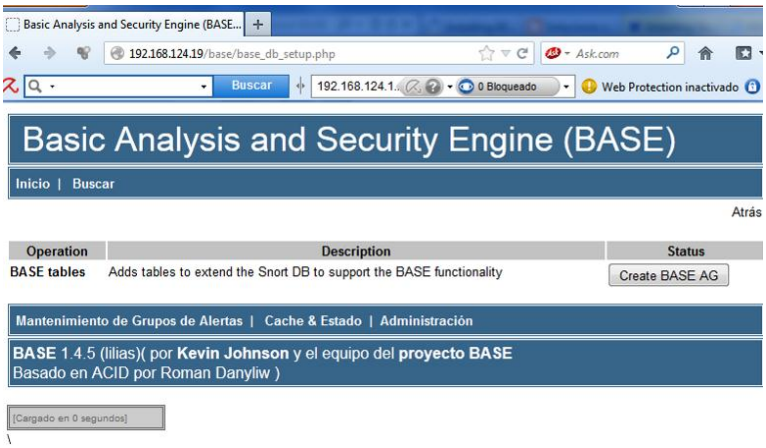


Gráfico 6.40. Instalación Base – Creación de Tablas

11. Se seleccionó en crear la base de AG y nos aparecerió un la imagen indicando las tablas que fueron creadas

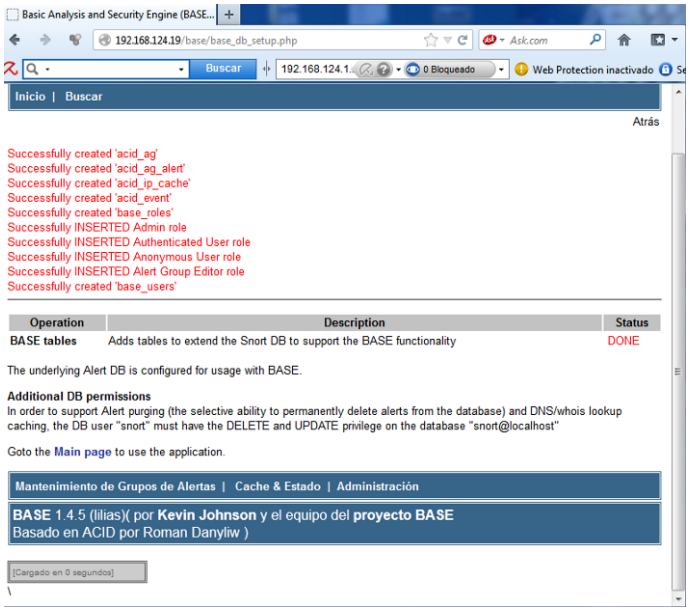


Gráfico 6.41. Instalación Base – Tablas Creadas

Se tubo que dirigir a la página principal y así ya se pudo obtener información de snort mediante la interfaz base.

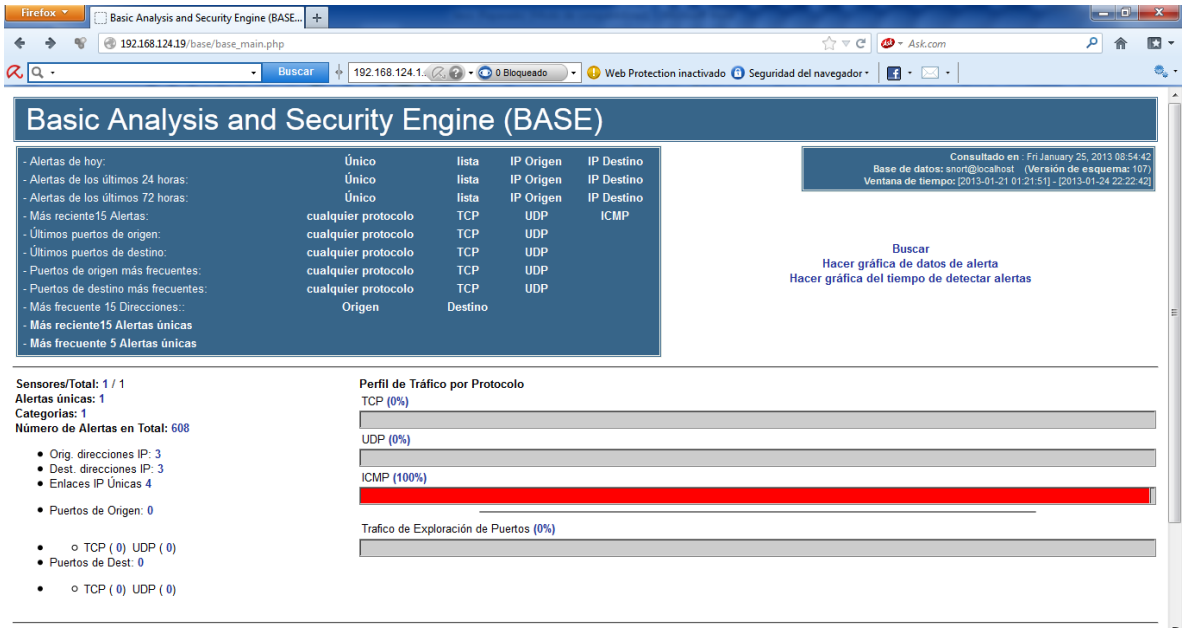


Gráfico 6.42. Instalación Base - Página Principal

6.8.4.13. Instalación de SNORTSAM (IPS)

Para la configuración de SnortSam es necesario como requisito tener instalado y funcionando SNORT y descargar los componentes necesarios para su instalación.

6.8.4.14. Descarga de componentes SnortSam

Se descargó los componentes necesarios para la instalación de la página web oficial, en los cuales se destaca que no existe aún SnorSam para la versión de snort 2.9.4 así que se descargó la versión de SnortSam 2.9.2.2. y se reinstalo snort siguiendo los mismos pasos para la versión 2.9.2.2

Link descarga Agente: http://www.snortsam.net/files/snortsam/
Link descarga Parche: ftp://ftp.snortsam.net/snort-plugin/

6.8.4.15. Instalación de Agente SnortSam

1. Se descomprimió el agente el archive en la carpeta /usr/local/src, y se dio los permisos para de ejecución al usuario root y se compiló el archivo makesnortsam.sh.

[root@servidorIDPS /]# cd usr/local/src/
[root@servidorIDPS src]# tar -zxvf snortsam-src-2.70.tar.gz
[root@servidorIDPS src]# cd snortsam
[root@servidorIDPS snortsam]# chmod 700 makesnortsam.sh
[root@servidorIDPS snortsam]# ./makesnortsam.sh

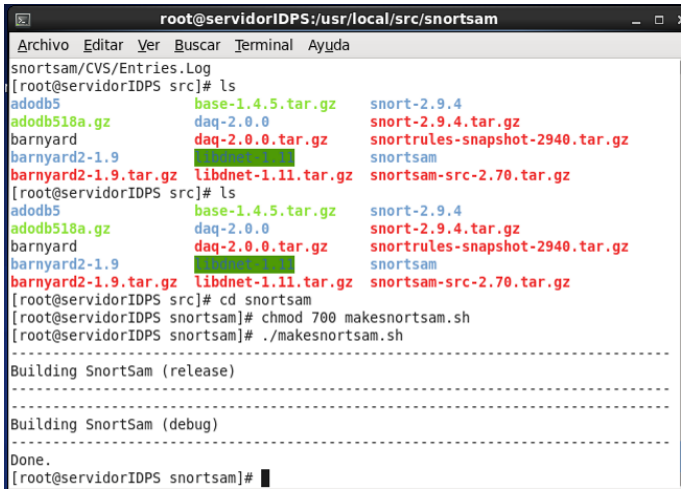


Gráfico 6.43. Compilación SnortSam Agente

2. Con el procedimiento anterior fueron creados en la carpeta de sortsam dos archivos binarios con el nombre snortsam y snortsam-debug, y se copió los archivos binarios a la carpeta a /usr/local/bin.

   [root@servidorIDPS src]# cp /usr/local/src/snortsam/snortsam /usr/local/bin/
   [root@servidorIDPS src]# cp /usr/local/src/snortsam/snortsam-debug /usr/local/bin/

3. Se copió el archive snorsam.conf.sample a la carpeta etc/ y se la renombró a snortsam.conf.

   [root@servidorIDPS snortsam]# mv conf/snortsam.conf.sample /etc/snortsam.conf

6.8.4.16. Instalación de Plug-in de Salida SnortSam

1. Se descomprimió el archivo en la carpeta /usr/local/src.

   [root@servidorIDPS src]# gzip -d snortsam-2.9.2.2.diff.gz

[root@servidorIDPS src]# cd snort-2.9.2.2

[root@servidorIDPS snort-2.9.4]# patch -p1 <../snortsam-2.9.2.2.diff

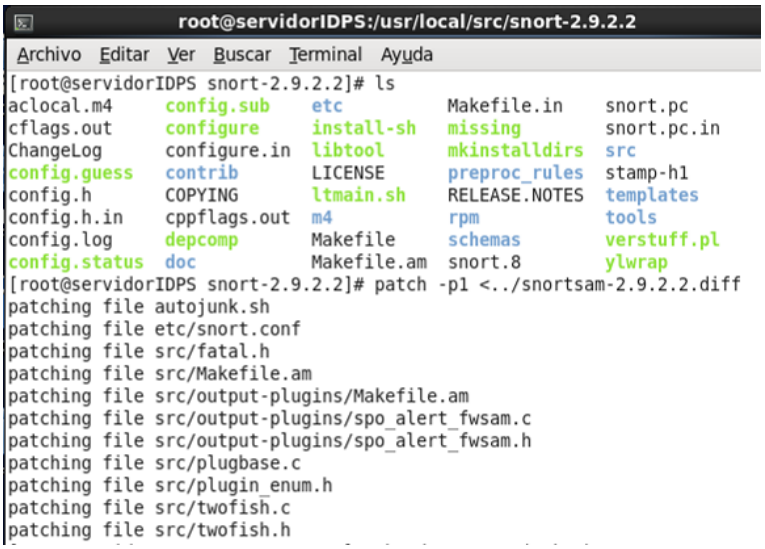


Gráfico 6.44. Parchando SnortSam

2. Se creó en la carpeta un archivo denominado autojunk.sh, se le dió permiso de ejecución y fue compilado.

   [root@servidorIDPS snort-2.9.4]# chmod 700 autojunk.sh
   [root@servidorIDPS snort-2.9.4]# ./autojunk.sh

3. Al intentar compilar autojunk.sh mostró un mensaje de error que no se ha podido localizar los siguientes archivos aclocal, autoheader autoconf y automaker instalados, para corregir este error se instaló el paquete libtool.

   [root@servidorIDPS ~]# yum install libtool

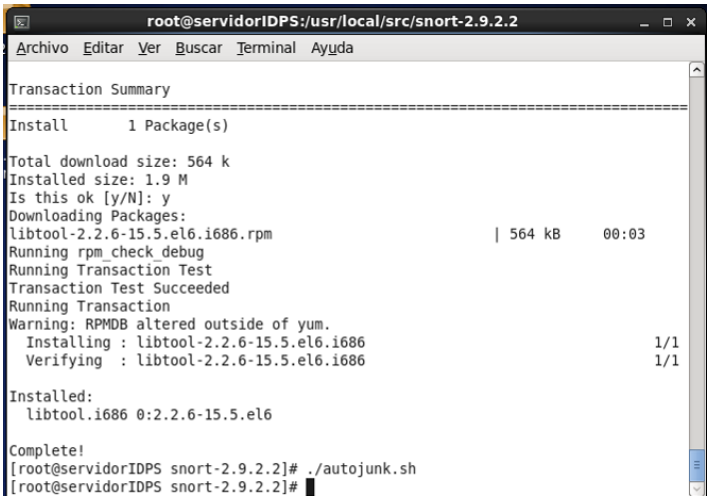


Gráfico 6.45. Instalación Libtool

4. Se volvió a parchar snort y ya no apareció el error y se ejecutó el archivo autojunk.sh.

[root@servidorIDPS snort-2.9.4]# ./autojunk.sh

Gráfico 6.46. Parche snort sin error

5. Se recompiló nuevamente snort.

[root@servidorIDPS snort-2.9.4]# ./configure --enable-sourcefire && make && make install

6.8.4.17. Configuración archivo snort.conf (Agente)

1. Se ingresó al archivo de configuración en la carpeta /etc.

   [FISEI@servidorIDPS etc]$ nano snortsam.conf

2. Se configuró las siguientes líneas del archivo:

   Descomentamos y agregamos el puerto por donde escuchara snortsam, colocamos el puerto por defecto de snortsam:

   - **Port** 899

```
#
 port 899
#
#   This set's the listening port to <port>.
#
#   Example:   port 666
#
#   It defaults to 898 if this line is omitted.
#
```

Gráfico 6.47. Puerto Snortsam

Se indicó la dirección de donde se encuentra ubicado el sensor de snort, en este caso se encuentra instalado en la misma máquina asignamos la dirección IP, no necesariamente puede ser uno ya que snortsam nos brinda la facilidad de instalar separado los componentes, y además pueden existir varios sensores que trabajen en diferentes partes de la red.

- **accept** 192.168.124.19/24

```
accept 192.168.124.19/24
#
#   This option lists Snort sensors that SnortSam is accepting packets from.
#   You can specify hostname, IP address, IP address and network mask, and
#   optionally an encryption key used configured for that host or network.
#
#   Examples:  accept 10.10.0.0/16, officepassword
#              accept snort1, hostpassword
#              accept 192.168.1.1
#
#   If the password is omitted, the default key specified with DEFAULTKEY will
#   be used. You can only specify one host per line, but you can supply
#   unlimited lines.
```

Gráfico 6.48. Ubicación sensor Snortsam

Se especificó el archivo donde se almacena las alertas

- **Logfile** /var/log/snortsam.log

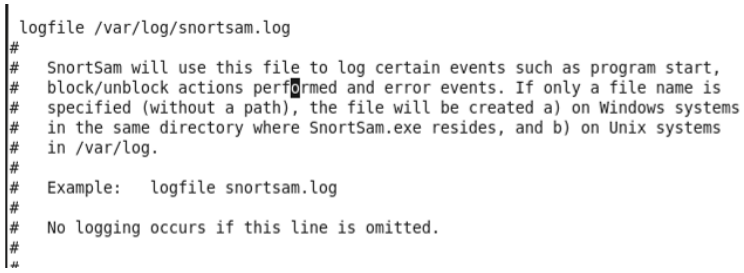


Gráfico 6.49. Archivo de almacén alertas

Se especificó la dirección del IPS en la opción bindip, en este caso es la ip de servidor IDPS.

- **Bindip** 192.168.124.19

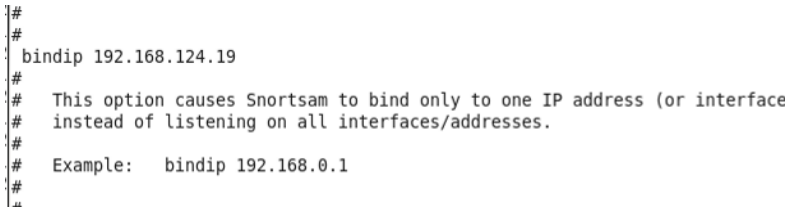


Gráfico 6.50. IP del IPS

Se especificó el firewall que vamos a utilizar

- **Fwsam** 192.168.124.19

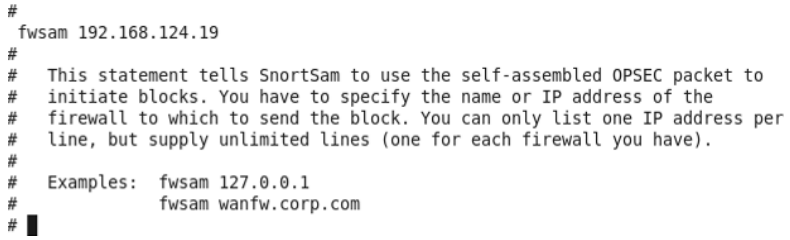


Gráfico 6.51. Especificacion de Firewall

Se escogió la opción de iptables y la tarjeta con la cual se va a trabajar

- **Iptables** eth0

```
# iptables eth0
#
#   This plugin will call the iptables executable in order to block the host by
#   adding a rule to the active rule set. You have to specify the adapter to
#   block on (for example, eth0) and you can optionally add a log option.
#
#   Example:   iptables eth0 syslog.info
#
```

Gráfico 6.52. Plugin Utilizado

6.8.4.18. Configuración archivo snort.conf

1. Se ingresó al archivo de configuración en la carpeta /etc/snort

   [FISEI@servidorIDPS snort]$ nano snort.conf

2. Se aumentó la línea para la alerta de SnortSam acompañado de su puerto

   - **output alert_fwsam**: 192.168.124.19:899

6.8.4.19. Modificación de las reglas de Snort

Para que snort y snortsam puedan funcionar se modificó las reglas aumentando los campos que permitieron a snortsam envíen los bloqueos hacia el firewall, para esto se realizó lo siguiente:

1. Se ingresó a los archivos de configuración de reglas que se encuentran en: /etc/snort/rules y se aumentó los siguientes parámetros:

firewall: [elemento a bloquear][sentido{opcional}], [tiempo de bloque]

En este caso se realizó un bloqueo por un tiempo de 20 minutos amentando a las reglas la siguiente línea: **fwsam:src, 20 minutes.**

Como en el siguiente ejemplo

Regla de snort

alert icmp any any -> $HOME_NET any (msg:"Prueba de Conexion"; sid:10000001; rev:1;)

Reglas de SnortSam para bloqueo

alert icmp any any -> $HOME_NET any (msg:"Prueba de conexion"; sid:10000001; rev:1; fwsam:src; fwsam:src,20 minutes;)

El procedimiento de actualización de las reglas se lo realizó de forma manual aumentando en las reglas los campos anteriormente mencionado.

6.8.5. Pruebas SNORT y SNORTSAM

En esta sección se realizara las pruebas de funcionamiento de la solución implementada, SNORT como IDS y SNORTSAM como IPS.

6.8.5.1. Pruebas SNORT IDS

Para la realización de pruebas sobre nuestro IDS SNORT se generó un análisis de vulnerabilidades mediante NESSUS, el cual es un programa que permite realizar

un escaneo de puertos de cualquier equipo que se encuentre en la red, además de mostrar las vulnerabilidades presenta mediante su interfaz web y posibles soluciones para corregir los errores.

Para proceder a instalar Nessus es necesario tener instalado el servidor web apache, la instalación de apache ya se lo mostro anteriormente, la instalación de Nessus la podemos encontrar en el ANEXO 4.

6.8.5.1.1. Preparación de las máquinas (Atacante - ServidorIDPS)

Para ejecutar el funcionamiento de snort, se utilizó un computador portátil que posee instalado el sistema operativo CentOS, este fue conectado a la red de la FISEI mediante cableado.

La dirección Ip de la máquina es la 192.168.124.55

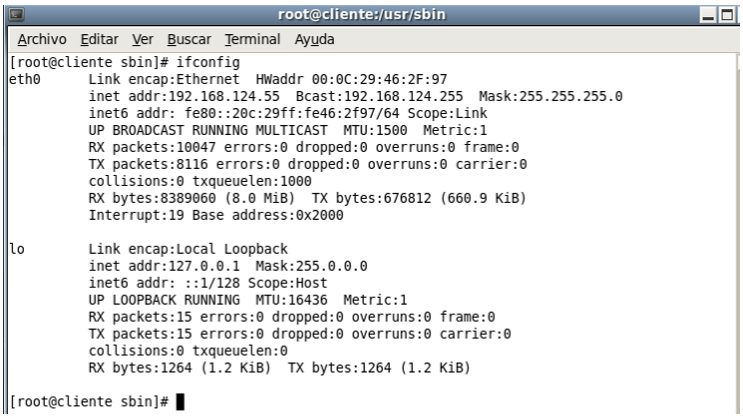


Gráfico 6.53. Ip Máquina Cliente

Se verificó que exista conectividad realizando un ping a cualquier máquina de la red, en este caso haremos un ping a nuestro servidor IDPS.

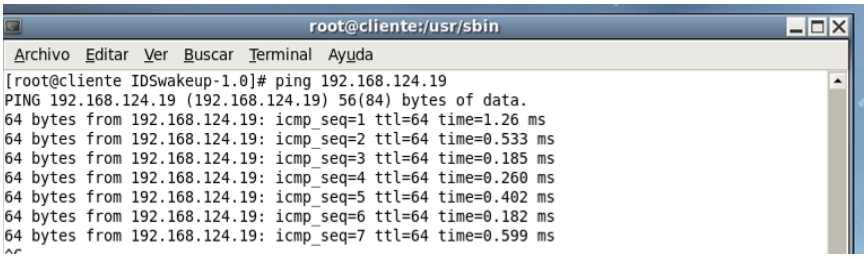


Gráfico 6.54. Verificación de conextividad

En la máquina donde reside SNORT lo primero que se realizó fue descomentar dentro del archivo snort.conf las reglas que fueron comentadas en el proceso de instalación, se dejaron solamente las reglas que se aplican a los servicios que se encuentra levantados en el servidor de la FISEI para no generar demasiados falsos positivos.

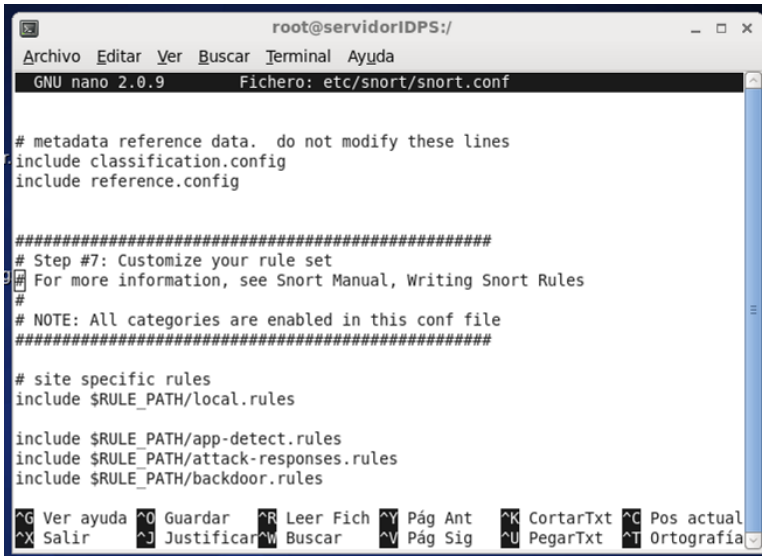


Gráfico 6.55. Reglas de Snort

6.8.5.1.2. Puesta en Marcha de Snort y Barnyard2

Se abrió un terminal, se procedió a cambiar de usuario root y se ubicó en la carpeta /usr/sbin/ para poner en marcha snort en modo IDS.

[root@servidorIDPS /]# su –

[root@servidorIDPS ~]# cd /

[root@servidorIDPS /]# cd usr/sbin/

[root@servidorIDPS sbin]# ./snort -c /etc/snort/snort.conf -i eth0

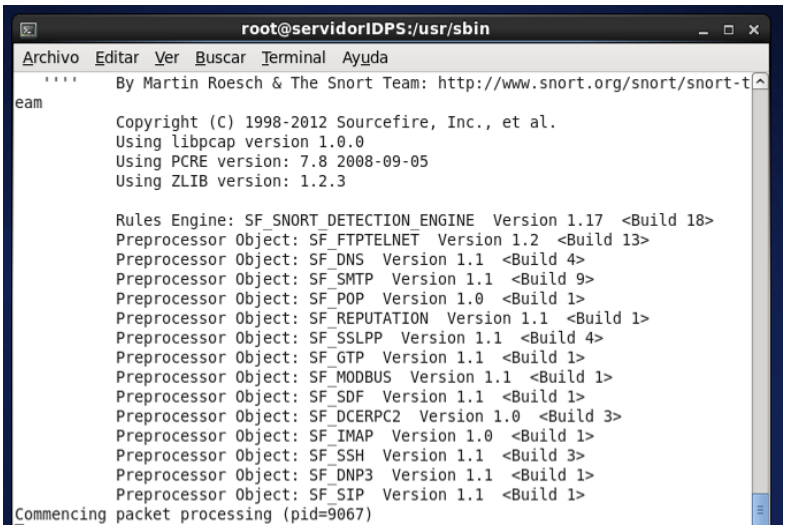


Gráfico 6.56. Puesta en Funcionamiento de Snort

Se abrió un nuevo terminal se cambió a usuario root y se pone en funcionamiento a barnyard2 con snort.

[root@servidorIDPS /]# /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map -d /var/log/snort -f snort.log -w /var/log/snort/barnyard.waldo

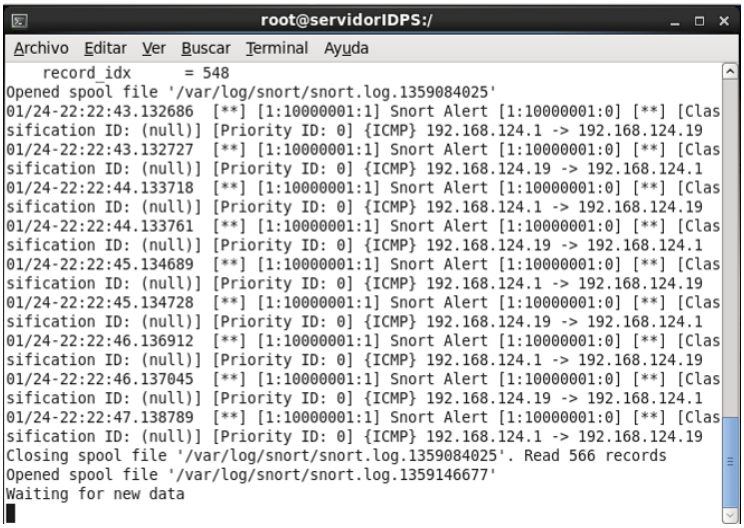


Gráfico 6.57. Funcionamiento de Barnyard2 y Snort

6.8.5.1.3. Generando Análisis con Nessus a servidor IDPS

En la maquina Atacante se ingresó con el usuario y clave asignados en la parte de configuracion de Nessus.

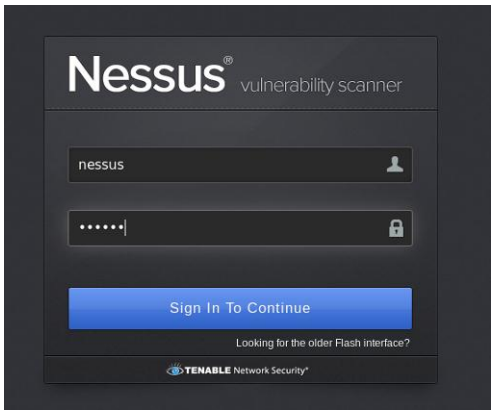


Gráfico 6.58. Usuario y Contraseña - Nessus

1. Se seleccionó la opción escanear y en nuevo escaneo.

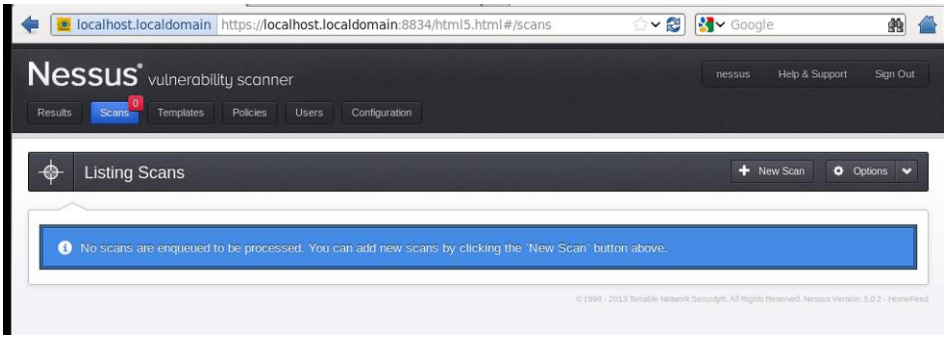


Gráfico 6.59. Nessus Escaneo

2. Se procedió a llenar los datos para el nuevo escaneo en este caso se realizó un escaneo de puertos al servidor IDPS.

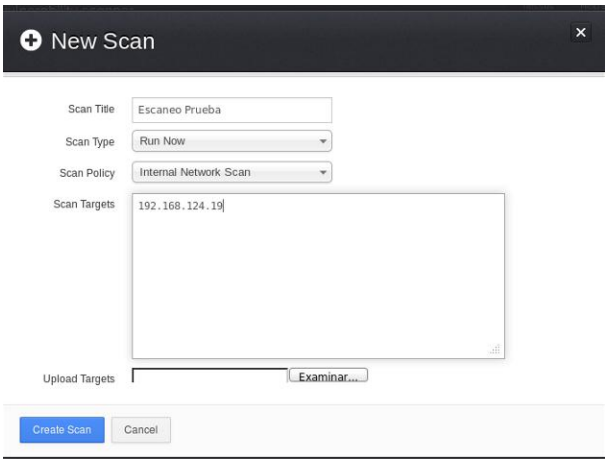


Gráfico 6.60. Nuevo Escaneo - Nessus

3. La imagen muestra la carga mientras se realizó el escaneo.

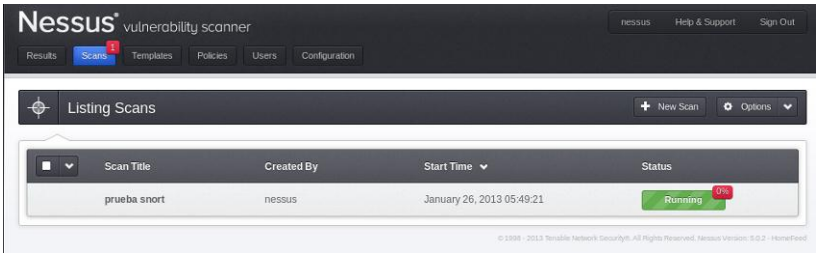


Gráfico 6.61. Escaneo de Servidor IDPS

4. Se verificó la terminal y visualizó que snort empieza a detectar el escaneo de Nessus.

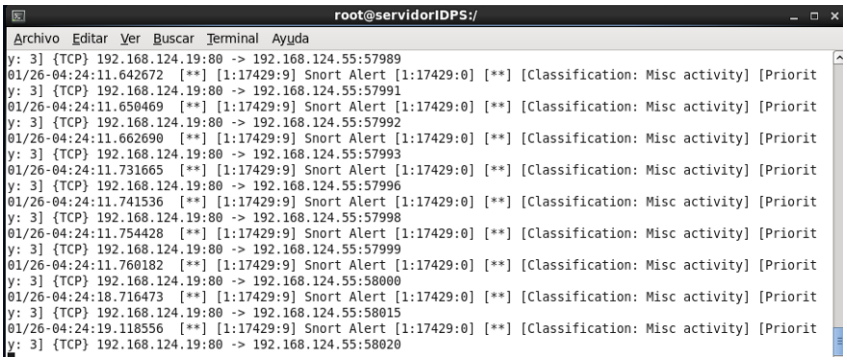


Gráfico 6.62. Visualización de Reglas Generadas por Nessus

6.8.5.1.4. Análisis de Resultados

La información generada en el análisis de los puertos del servidor se pudo visualizar mediante la interfaz web BASE, en primera instancia se observó que se encuentran generadas 1140 alertas y que es mediante los protocolos TCP e ICMP.

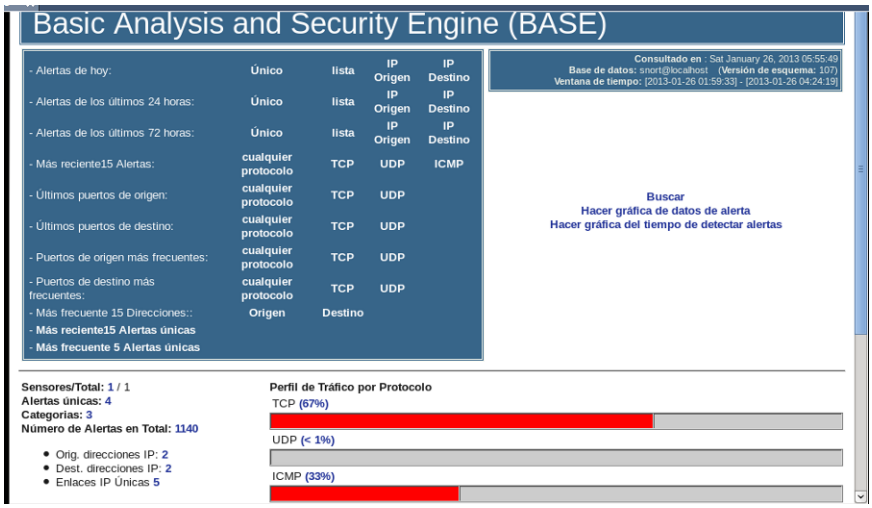
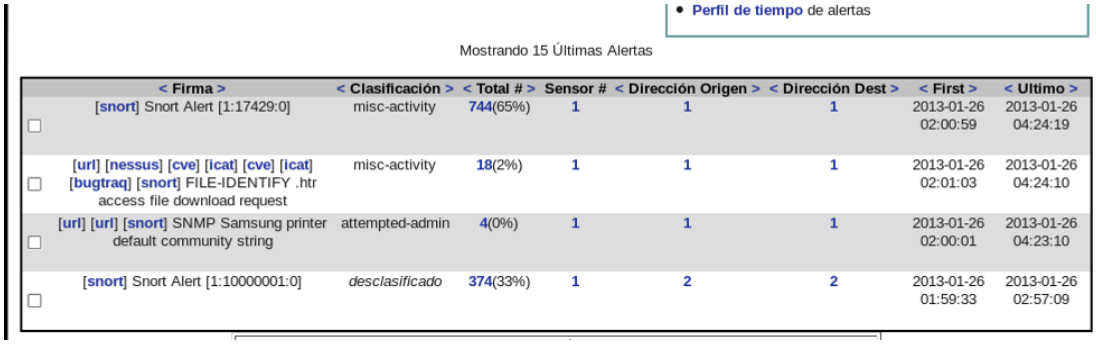


Gráfico 6.63. Pagina Inicial – Alertas Generadas

El tráfico por ICMP hace referencias a las alertas generadas con la regla creada en el archivo local.rule, esta regla permitió conocer en una instancia si SNORT se

encontraba detectando el trafico mediante una regla que al hacer ping nos generaba una alerta.

El tráfico por TCP hace referencia al escaneo generado por Nessus, para tener una información un poco más detallada, se visualizaron las últimas 5 alertas generadas.



• Perfil de tiempo de alertas

Mostrando 15 Últimas Alertas

	< Firma >	< Clasificación >	< Total # >	Sensor #	< Dirección Origen >	< Dirección Dest >	< First >	< Ultimo >
☐	[snort] Snort Alert [1:17429:0]	misc-activity	744(65%)	1	1	1	2013-01-26 02:00:59	2013-01-26 04:24:19
☐	[url] [nessus] [cve] [icat] [cve] [icat] [bugtraq] [snort] FILE-IDENTIFY .htr access file download request	misc-activity	18(2%)	1	1	1	2013-01-26 02:01:03	2013-01-26 04:24:10
☐	[url] [url] [snort] SNMP Samsung printer default community string	attempted-admin	4(0%)	1	1	1	2013-01-26 02:00:01	2013-01-26 04:23:10
☐	[snort] Snort Alert [1:10000001:0]	*desclasificado*	374(33%)	1	2	2	2013-01-26 01:59:33	2013-01-26 02:57:09

Gráfico 6.64. Ultimas 15 Alertas Generadas

[snort] Snort Alert [1:17429:0] misc-activity

Esta es una lista completa de las alertas que se generan cada día. El sensor snort se encuentra en un puerto que escucha a palmo cada pedazo de tráfico que entra y sale de nuestra red.

[url] [nessus] [cve] [icat] [cve] [icat] [bugtraq] [snort] FILE-IDENTIFY .htr access file download request

Está firma indica que atacantes remotos leen el código fuente de los programas ejecutables del servidor web.

[url] [url] [snort] SNMP Samsung printer default community string

Esta detección señala que el software está tratando de obtener privilegio de administrador.

Se ha verificado que snort se encuentra funcionando correctamente. Se realizaron dos pruebas, la primera en el proceso de instalación generando una alerta cuando

un usuario realiza un ping hacia cualquier máquina de la Red y la segunda prueba fue un escaneo mediante Nessus. Se pudo visualizar mediante consola y mediante la interface de BASE las alertas generadas, en los diferentes protocolos en tiempo real.

6.8.5.2. Prueba SnortSam IPS

Para verificar que nuestro IDPS SNORT-SNORTSAM esté funcionando correctamente se realizó una prueba simple la cual consistió en generar un ping desde una máquina en este caso se utilizó la misma máquina para las pruebas que se realizaron para el IDS y que SnortSam nos bloque la conectividad por un lapso de 2 minutos.

6.8.5.2.1. Puesta en Marcha de Snort, SnortSam y Barnyard2

Se abrieron 3 terminales en cada terminal inicializó un servicio como se muestra a continuación:

Inicializando Snort

[root@servidorIDPS /]# su –

[root@servidorIDPS /]# cd usr/sbin/

[root@servidorIDPS sbin]# ./snort -c /etc/snort/snort.conf -i eth0

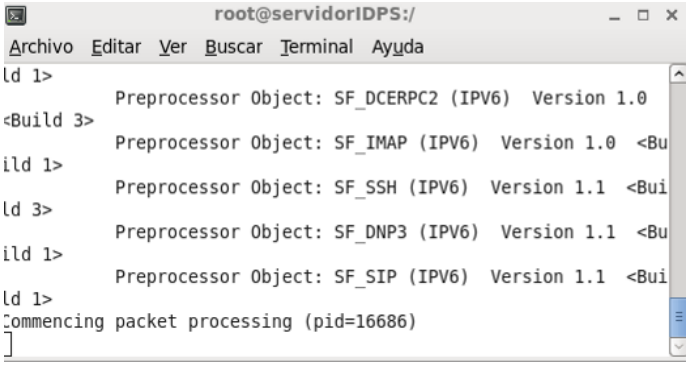


Gráfico 6.65. Inicializando Snort – Prueba IDPS

Inicializando Barnyard

[root@servidorIDPS /]# /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map -d /var/log/snort -f snort.log -w /var/log/snort/barnyard.waldo

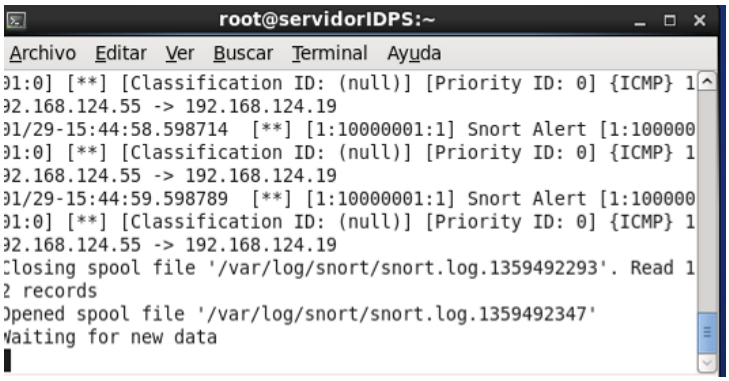


Gráfico 6.66. Inicializando Snort – Prueba IDPS

Inicializando SnortSam

[root@servidorIDPS /]# /usr/local/bin/snortsam /etc/snortsam.conf

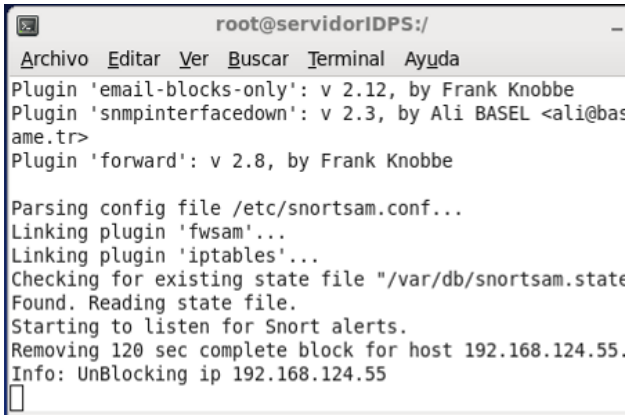


Gráfico 6.67. Inicializando SnortSam – Prueba IDPS

6.8.5.2.2. Ejecutando Prueba de conectividad

Se generó un ping desde la máquina 192.168.124.55 hacia la máquina 192.168.124.19 servidor IDPS

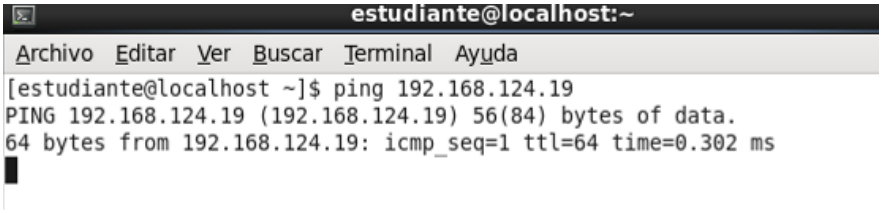


Gráfico 6.68. Ping Maquina Servidor IDPS – Prueba IDPS

El servidor IDPS no permite que se realice el ping de conexión ya que se ha configurado una regla para que al existir un test de conexión, Snortsam se comunique con el firewall y bloquee el intento de conexión por un tiempo estimado de 2 minutos lo cual se puede ver en la siguiente imagen

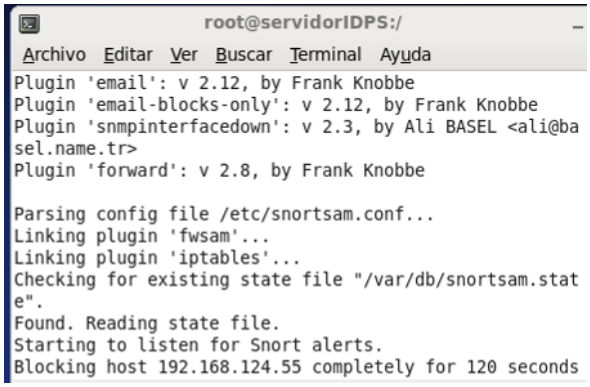


Gráfico 6.69. Generacion de bloqueo de SnortSam

En la tercera terminal se puedo observar que snortsam seguia generando las alertas que se envian por la accion del ping, de la misma manera pueden ser observada por la interfaz visual mediante el frontal “base”.

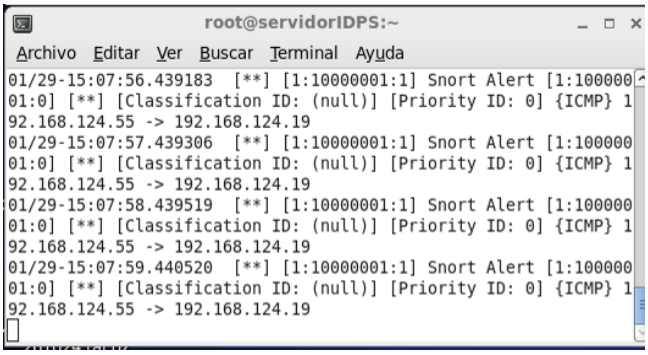


Gráfico 6.70. Generación de Aletas de Snort Consola

Al haber realizado un test de conectividad cada dos minutos se ejecutara un un nuevo bloqueo por tal motivo para comprobar el funcionamiento del Sistema de detección y prevención de intrusos se finalizaron los servicios de snort, snortsam y barnyard y al lapso de dos minutos el test de conectividad ya pudo concluirse como se muestra en la siguiente imagen.

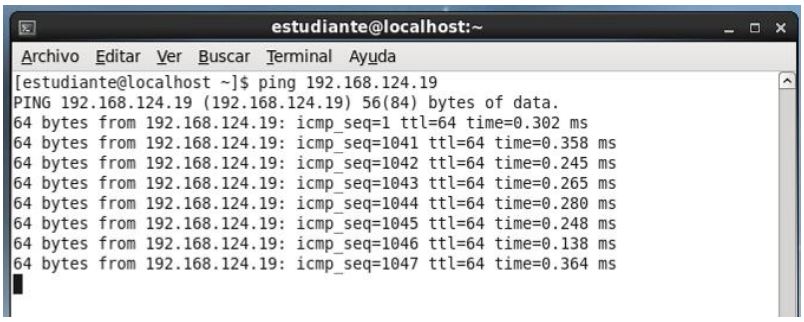


Gráfico 6.71. Termino de bloqueo test de conectividad

Y por último se verificó con el comando iptables –L para que nos muestre las reglas que se encuentran ejecutadas

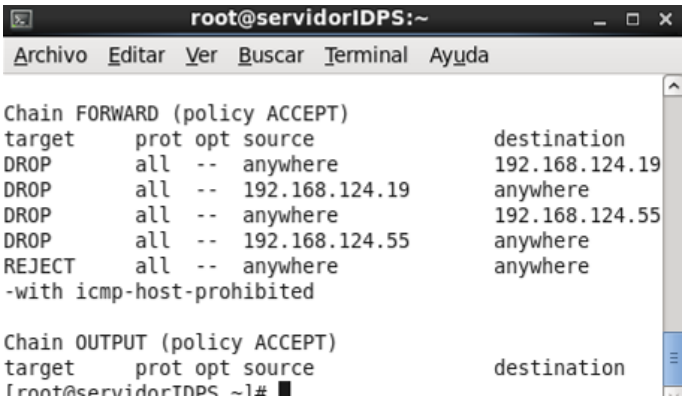


Gráfico 6.72. Reglas Generadas en Iptables

6.8.6. Capacitación

La capacitación para el uso del sistema de detección y prevención de intrusos mediante la herramienta de software libre Snort y el complemento SnortSam se la realizó al encargado del departamento de Sistemas de la Facultad de Ingeniería en sistema el Ing. Eduardo Chazo del 4 al 8 de Enero del 2013, siguiendo el cronograma que se adjunta a continuación.

CRONOGRAMA DE CAPACITACIÓN		
Fecha: 4 al 8 de Enero de 2013		
Días	**Horas**	**Contenido**
Lunes 4	2	Instalación de Dependencias
Martes 5	2	Instalación de Snort
Miércoles 6	2	Instalación de Frontend y Backend
Jueves 7	2	Instala de SnortSam
Viernes 8	2	Puesta en Marcha Snort y SnortSam

Tabla 6.18 Cronograma de Capacitación

6.9. Conclusiones y Recomendaciones

6.9.1. Conclusiones

- La implementación de Snort como sistema de detección y prevención de intrusos permite mantener un control sobre posibles intentos de vulnerabilidad de la información que se posee en los servidores de la FISEI en tiempo real mediante terminal o mediante la interfaz web “base”.

- El sistema de detección y prevención de intrusos nos permite almacenar un historial de información sobre posibles intentos de

vulnerabilidad en la base de datos, para poder visualizarlo en el momento que sea necesario y tomar medidas de prevención ante posibles intentos de ataques futuros.

- La instalación de módulo SnortSam permite obtener un mayor grado de seguridad ya que realiza bloqueos al encontrarse ejecutando un ataque mediante las reglas de snort que pueden ser fácilmente reconfiguradas.

- La implementación de herramientas de un IDPS basado en software libre nos brinda facilidad al configurar y adaptar el sistema de acuerdo a las necesidades de la red de información de la FISEI.

6.9.2. Recomendaciones

- Establecer políticas de manejo y uso de sistema de detección y Prevención de Intrusos para poder mantener un mayor control sobre intentos de vulnerabilidad de los equipos.

- Mantener actualizadas el paquete de reglas de acuerdo a las necesidades y cambios que se vayan presentando en los equipos que conforman la facultad de Ingeniería en sistemas, Electrónica e Industrial.

- Establecer políticas para el respaldo de la información debido al nivel de importancia que esta posee para el departamento de administración de redes de la FISEI.

6.10. Referencias

[1] Arbaláes, R., (2008). *"La Seguridad de la Información en Latinoamérica aún no tiene un carácter estratégico"*. Recuperado el 21 de mayo de 2012, de http://www.tecnologiahechapalabra.com/salud/enlaces/articulo.asp?i=2729.

[2] Cuenca, A., (2012). "*El delito informático en el Ecuador*". Recuperado el 08 de junio de 2012, de http://www.egov.ufsc.br/portal/sites/default/files/el_delito_informatico_en_el_ecuador_una_tendencia_criminal_del_siglo_xxi-alexander_cuenca.pdf.

[3] Arronategui U, Mayordomo E, Tricas F., (2009). "*Seguridad Informática - Un post diferente*". Recuperado el 18 de mayo de 2012, de http://webdiis.unizar.es/~ftricas/Asignaturas/seguridadD/Transparencias/1-IntroduccionSeguridadInformatica.pdf.

[4] Pumarino, A., (2006). "¿Qué es la *Seguridad Informática?*". Recuperado 10 de febrero de 2012, de http://pumarino.blogspot.com/2006/06/qu-es-la-seguridad-informtica.html.

[5] Murillo, S., (2001). "*Conceptos básicos de la seguridad informática*". Recuperado el 15 de enero de 2012, de http://catarina.udlap.mx/u_dl_a/tales/documentos/msp/murillo_c_sr/capitulo1.pdf.

[6] Diccionario informático, (2008). "*Definición de Seguridad Informática*". Recuperado el 23 de febrero de 2012, de http://www.alegsa.com.ar/Dic/seguridad%20informatica.php.

[7] Arronategui U, Mayordomo E, Tricas F., (2009). "*Seguridad Informática - Un post diferente*". Recuperado el 18 de mayo de 2012, de http://webdiis.unizar.es/~ftricas/Asignaturas/seguridadD/Transparencias/1-IntroduccionSeguridadInformatica.pdf.

[8] Kioskea.net, (2012). "*Noción de Sistema de información*". Recuperado el 04 de marzo de 2012, de http://es.kioskea.net/contents/systeme-d-information/si-systeme-d-information.php3.

[9] Ecuared, (2011). "*Sistemas de Información*". Recuperado el 09 de febrero de 2012, de http://www.ecured.cu/index.php/Sistema_de_Informaci%C3%B3n.

[10] Kioskea.net, (2008). "*Introducción a la Seguridad Informática*". Recuperado el 07 de marzo de 2012, de http://es.kioskea.net/contents/secu/secuintro.php3.

6.11. Bibliografía

Libros

- TANEMBAUM, Andrew. (2000). *Redes de Computadoras.* (3ra ed.). México: Pearson Educación.

- RAMIÓ, Jorge. (2006). *Seguridad Informática y Criptografía*. (6ta ed.). Madrid.

Internet

- ARRONATEGUI, Unai. (2009). *Administración de Sistemas Informáticos.* Recuperado el 20 de diciembre de 2011, de http://izaro.cps.unizar.es/asignaturas/asi/teoria/Tema20SeguridadInformatica.pdf

- DICCIONARIO DE INFORMATICA. (2008). *Definición de Seguridad Informática*. Recuperado el 07 de enero de 2012, de http://www.alegsa.com.ar/Dic/seguridad%20informatica.php

- KIOSKEA.NET. (2008). *Introducción a la Seguridad Informática*. Recuperado el 16 de enero de 2012, de http://es.kioskea.net/contents/systeme-d-information/si-systeme-d-information.php3

- ANONIMO. (2008). *Definición Sistema de Información. SF*. Recuperado el 16 de enero de 2012, de http://definicion.de/sistema-de-informacion/

- REVELO, Hector. (2010). *Derecho Informático. Estadísticas.* Recuperado el 17 de enero de 2012, de http://www.abogados.ec/tag/estadisticasde-delitos-informaticos-2010/

- WARE, Charles. (2011). *Sistema de Detección y Prevención de Intrusos. Estado del Arte*. Recuperado el 17 de enero de 2012, de http://www.asiap.org/AsIAP/images/stories/JIAP/jiap2011/Presentaciones/Azul/A1917_IBM.pdf

- KIOSKEA.NET. (2008). *Noción de sistema de información*. Recuperado el 16 de enero de 2012, de http://es.kioskea.net/contents/secu/secuintro.php3

- FERRER, Rodrigo. (2010). *Metodología recomendada para el análisis de vulnerabilidades*. Recuperado el 21 de mayo de 2012, de http://www.sisteseg.com

- MAESTROS DEL WEB. (2003). *Sistemas de detección de Intrusos y Snort*. Recuperado el 21 de mayo de 2012, de http://www.maestrosdelweb.com/editorial/snort/

- PAGINA OFICIAL SNORT. (2013). *Snort.* Recuperado el 16 de julio de 2012, de http://www.snort.org/

- JIMENEZ Carlos, GOMEZ Julio. (2009). *Diseño y Optimización de un Sistema de Detección de Intrusos Híbrido*. Recuperado el 16 de julio de 2012, de http://es.scribd.com/doc/68731192/PFC-carlos

- GARCIA, Joaquín. *Detección de Intrusos en Red Basado con Snort*. Recuperado el 16 de julio de 2012, de http://www.deic.uab.es/material/26118-snort.pdf

- INTERIANO Eduardo, MONTES Faustino. *Redes de Computadoras - Protocolos PPP.* Recuperado el 21 de julio de 2012, de http://www.ie.itcr.ac.cr/faustino/Redes/Clase6/3.2PPP.pdf

- Anónimo. (2011). *SNORT*. Recuperado el 22 de julio de 2012, de http://lordrna.blogspot.com/2011/01/snort.html

- MORENO, Javi. (2009). *Sistemas de Detección de intrusos Snort y sus Amigos.* Recuperado el 22 de julio de 2012, de http://vierito.es/wordpress/wp-content/uploads/2009/08/ids_cp2k9.pdf

- SYSTEMADMIN.ES. (2012). *Instalación de un IDS.* Recuperado el 22 de julio de 2012, de http://systemadmin.es/2009/11/instalacion-de-un-ids-snort-con-base-y-las-reglas-de-emerging-threads

- PALACIOS GONZALES, Elias. *Noticias de Linux y Tecnología - El Sistema de Detección de Intrusos: Snort.* Recuperado el 25 de julio de 2012, de http://www.linux-party.com/index.php/57-seguridad/6000-el-sistema-de-deteccion-de-intrusos-snort--windows-y-linux-

- TORRES VARGAS, Daniel. (2012). *Instalación Configuración y Funcionamiento del IDS SNORT.* Recuperado el 05 de agosto de 2012, de http://seguridadinformaticaufps.wikispaces.com/file/view/1150214.pdf

- ANONIMO. *Tipos de Protocolos.* Recuperado el 05 de agosto de 2012, de http://arturocasupa.galeon.com/

- PECOS, Daniel. *PostGreSQL vs. MySQL.* Recuperado el 16 de agosto de 2012, de http://danielpecos.com/docs/mysql_postgres/x57.html

- THE CENTOS PROJECT. *CentOS 6.3 Notas de la versión.* Recuperado el 16 de agosto de 2012, de http://wiki.centos.org/Manuals/ReleaseNotes/CentOS6.3/Spanish

- ANONIMO. *Artículo, Snort, Apache, SSL, PHP, MySQL, Barnyard y BASE Instalado en RHEL 5*. Recuperado el 01 de septiembre de 2012, de http://solucionalinux.blogspot.com/2009/11/snort-apache-ssl-php-mysql-barnyard-y.html.

- ANONIMO. *Gestión de permisos, usuarios y grupos en Linux*. Recuperado el 01 de septiembre de 2012, de http://albertux75.wordpress.com/2008/08/01/capitulo-vi-gestion-de-permisos-usuarios-y-grupos-en-linux/

- HACKPLAYERS. *Aumentando el rendimiento de Snort con Barnyard2*. Recuperado el 07 de septiembre de 2012, de http://www.hackplayers.com/2011/03/aumentando-el-rendimiento-de-snort-con.html

Revistas

- Anónimo. (2002). *Seguridad Informática ¿Qué, porqué y para qué?*. Revista red. Recuperado el 03 de marzo de 2012, de http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm.

Cursos

- MICROSOFT. (2010). *Principio de Seguridad Informática. Mecanismos de Seguridad. Curso Certificaciones MTA*.

6.12. Glosario de Términos

Barnyard2: “Es un sistema de salida de snort, Snort creó un formato binario de salida llamado unified, Barnard2 lee este archivo y a continuación vuelve a enviar los datos a una base de datos.”

BASE: “Base es un analizador básico de seguridad. Se basa en el código de la Consola de Análisis para bases de datos de intrusión (ACID) proyecto. Esta aplicación proporciona un front-end web para consultar y analizar las alertas que vienen de un sistema IDS Snort.”

BISON: “Generador del programa de análisis de GNU”

FLEX: “Es una herramienta para generar programas capaces de reconocer patrones de texto. Su versatilidad permite establecer las reglas de búsqueda, erradicando la necesidad de desarrollar un programa especializado”

GCC: “El paquete GCC contiene compiladores GNU. Es útil para compilar programas escritos en C, C++, Fortran, Java, Objective C y Ada.”

LIBDNET: “Proporciona un interfaz simplificado, portable a varias rutinas de bajo nivel de una red.”

LIBPCAP: “Proporciona funciones para la captura de paquetes a nivel de usuario, utilizada en la monitorización de redes de bajo nivel.”

PCRE: “Contiene librerías de expresiones regulares compatibles con Perl. Son útiles para implementar búsquedas de patrones de expresiones regulares usando las misma sintaxis y semántica que Perl 5.”

TCPDUMP: "Es un herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.**"**

ZLIB: "Paquete para compresión librerías**"**

6.13. Anexos

6.13.1. Anexo 1: Croquis de la Universidad Técnica de Ambato

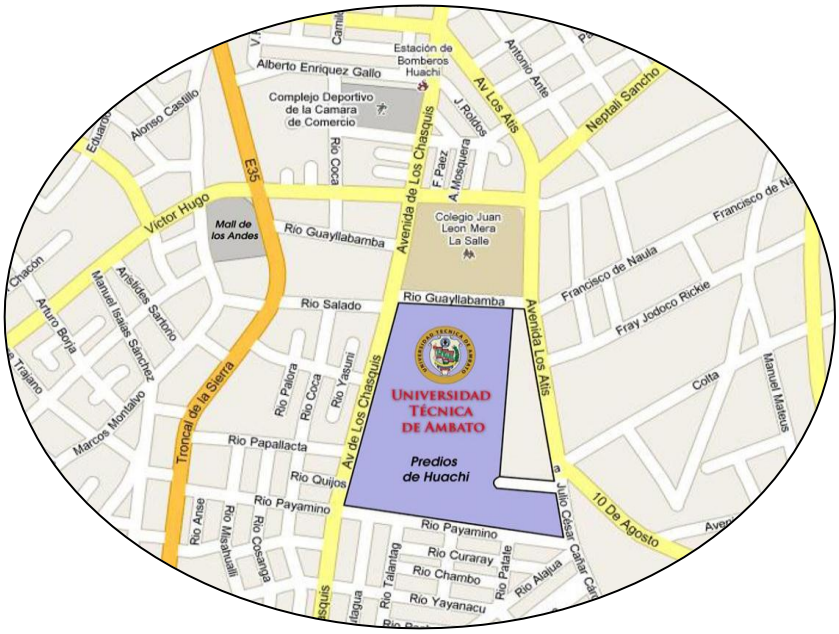


Gráfico 6.73. Predios Huachi

6.13.2. Anexo 2: Encuesta

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

LUGAR A ENCUESTAR: FISEI

OBJETIVO DE LA ENCUESTA: Obtener información real que permita justificar la investigación y demostrar las necesidades del departamento de administración de redes referente a la seguridad de la información.

Señores, su veracidad en las respuestas permitirá al investigador desarrollar un trabajo real y efectivo. Agradecemos su colaboración y garantizamos absoluta reserva de su información.

CUESTIONARIO

1.- ¿Cuál es el nivel de importancia de la información que maneja el Departamento de Administración de Redes? Tomando en cuenta los indicadores como normal información que puede ser visualizada por cualquier persona y alta información que solamente puede acceder personal autorizado

a) Normal ☐

b) Alta ☐

2.- ¿Cada qué tiempo se realiza un escaneo de puertos en busca de vulnerabilidades?

a) Semanal ☐

b) Mensual ☐

c) Semestral ☐

c) Anual ☐

d) Nunca ☐

3.- ¿Qué nivel de seguridad poseen los equipos servidores de la FISEI?

Tomar en consideración la siguiente tabla para medir los indicadores

Niveles	Parámetros
Bajo	Cualquier usuario tiene acceso a los equipos físicos, red de datos e internet.
Medio	Solamente personal autorizado accede a los equipos servidores y usuarios accede a la red LAN, internet, aplicaciones mediante usuarios y contraseñas o algún tipo de autentificación
Alto	Solo personal autorizado accede a los equipos servidores, se mantiene historiales de acceso y uso de las redes, se posee herramientas de seguridad para control y administración de redes

a) Bajo ☐
b) Medio ☐
c) Alto ☐

4.- ¿Qué software de Seguridad se encuentran instalados en los servidores de la FISEI?

a) Antivirus ☐
b) Firewall ☐
c) Detección de Malware ☐
d) IDS ☐
e) IPS ☐

5.- ¿Qué usuarios pueden acceder a la información confidencial de los servidores de la FISEI?

a) Administrador ☐
b) Laboratoristas ☐
c) Otros ☐

6.- ¿Han existido ataques hacia los servidores de la FISEI?

a) Si ☐
b) No ☐
c) No Sabe ☐

7.- ¿Se realizan cambios de contraseña después de cada cabio de personal en el departamento?

a) Si ☐

b) No ☐

GRACIAS POR SU COLABORACIÓN

Fecha de aplicación:

……

6.13.3. Anexo 3: Instalación de CentOS 6.3

1. Se insertó el Disco de Instalación el cual muestra 5 opciones que se detallan a continuación, usando la tecla TAB se puede mover entre cada una de ellas.

- Instalar o Actualizar un Sistema Operativo Existente.
- Instalar el Sistema con Driver Básicos de Video
- Recuperación de Sistema
- Arrancar desde el Disco Local
- Prueba de memoria

2. Se seleccionó la primera Opción y se presionó la tecla Enter.

Gráfico 6.74. Tipo de Instalación

3. Apareció una ventana en la cual indica si se desea realizar una verificación del disco para descartar que existan errores en la instalación. Si no esta seguro que el instalador este correcto es recomendable dar click en OK, caso contrario se selecciona en SKIP.

Gráfico 6.75. Comprobación del Disco

4. Se mostró la pantalla de bienvenida para la instalación de Centos 6.3 y se dió click en siguiente.

Gráfico 6.76. Pantalla de Bienvenida

5. Luego, apareció una ventana, la cual permitió escoger el idioma para el proceso de Instalación, se eligió Español (Español) o Español (Ecuador). Esto servirá para para que a partir de la siguiente ventana todos los textos que aparezcan sean en idioma Español.

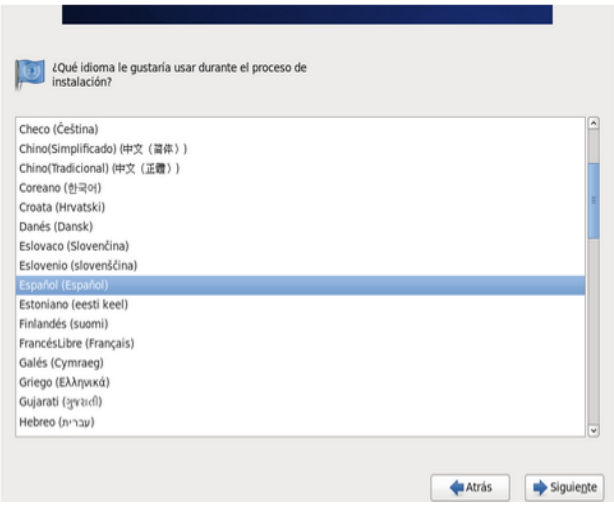


Gráfico 6.77. Selección de Idioma

6. La siguiente ventana preguntó si se desea instalar en un dispositivo de almacenamiento básico o especializado. Almacenamiento básico es cuando vamos a realizar una instalación normal en un disco duro, y Almacenamiento especializado cuando poseemos arreglas de discos duros RAID y necesita particionalmente especializado. En nuestro caso se seleccionó una instalación Normal.

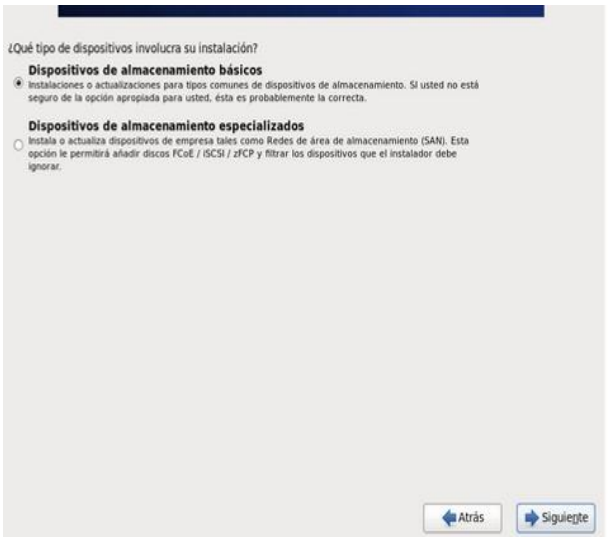


Gráfico 6.78. Tipo de Almacenamiento

7. Luego apareció una advertencia indicando que el disco duro debe ser inicializado en el caso de ser nuevo o haber sido borrado, y se eligió reinicializar todo.

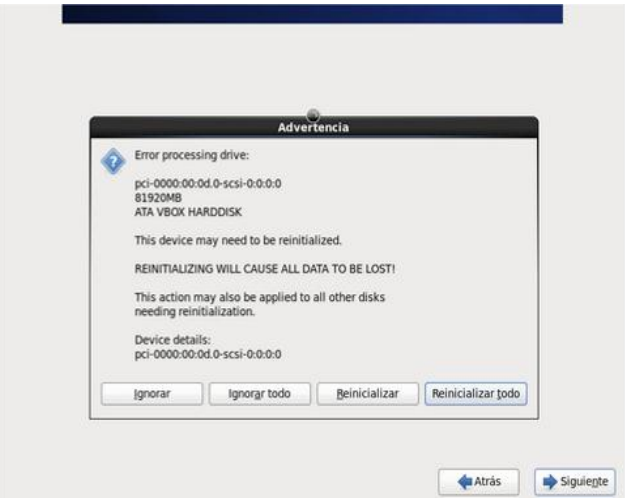


Gráfico 6.79. Advertencia de Eliminación de datos

8. En la siguiente ventana solicitó ingresar el nombre del computador, este nombre está formado generalmente en la primera parte por el nombre del equipo luego un punto (.) y el nombre del dominio del equipo, en este caso se lo llamo ServidorIDPS y se dió click en siguiente.

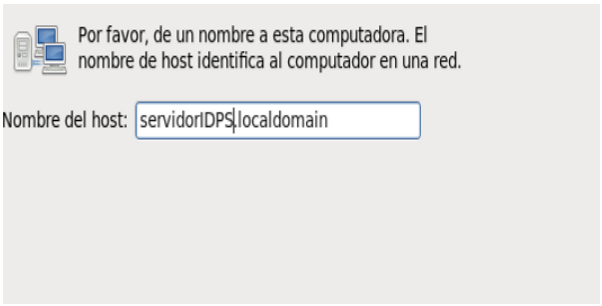


Gráfico 6.80. Nombre Servidor

9. A continuación se seleccionó la zona horaria, esto se lo realizó indicando en el mapamundi el lugar en donde se encuentra, en este caso la zona horaria es

Ecuador (Guayaquil) y se dejó seleccionado la casilla del reloj del sistema, ya que utiliza UTC y esto significa que utiliza Tiempo Universal Coordinado.

Gráfico 6.81. Situación Geográfica

10. Se procedió a ingresar la contraseña del usuario administrador o root, tomando en cuenta las recomendaciones de seguridad básica, como por ejemplo poner una contraseña que posea por lo menos 8 caracteres entre mayúsculas, minúsculas, números y caracteres especiales.

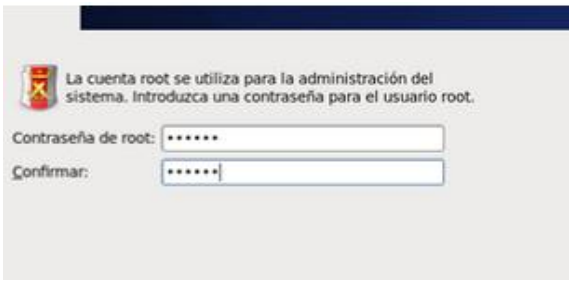


Gráfico 6.82. Contraseña Root

11. Se eligió el tipo de instalación que se deseaba hacer, Centos 6.3 brinda 5 opciones de instalación que son las siguientes:

- **Usar todo el espacio.-** Elimina cualquier partición que exista en el disco duro incluyendo de otros sistemas operativos.

- **Remplazar Sistema Linux Existente.-** Busca y elimina particiones Linux existentes en el disco

- **Achicar el Sistema Actual.-** Cambia el tamaño de particiones existentes, para tener espacio para la nueva partición.

- **Usar el espacio Libre.-** No modifica nada del disco duro y solamente utiliza el espacio disponible para la instalación.

- **Crear Diseño Personalizado.-** Permite crear de forma manual las particiones que necesitamos para instalar nuestro sistema.

Gráfico 6.83. Particionamiento del disco

Se creó una partición personalizada de la siguiente manera:

- Swap 1GB
- Boot 200 MB
- / el resto de espacio del disco

Este tipo de personalización se utilizó para optimizar el rendimiento del sistema.

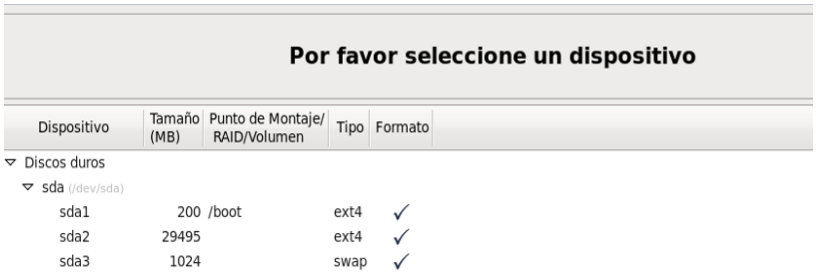


Gráfico 6.84. Particionamiento personalizada del disco

12. Después de seleccionar la partición para el disco duro nos aparecerá una advertencia indicando los cambios que se van a realizar al disco duro. Seleccionamos en Escribir cambios al Disco.

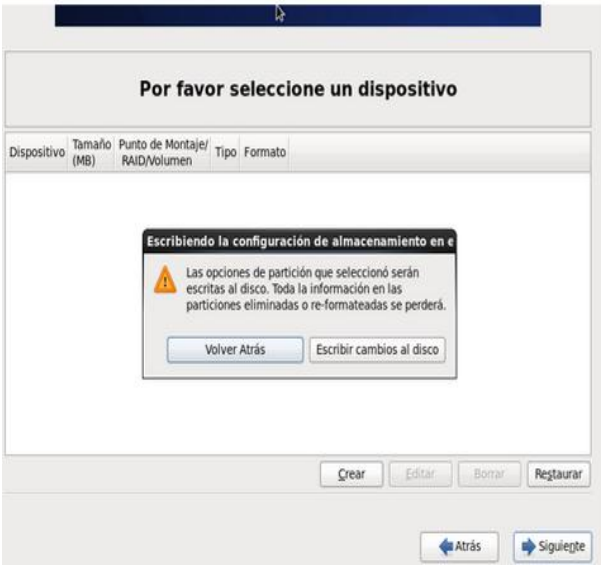


Gráfico 6.85. Escribir cambios en disco

13. Posteriormente apareció la opción para asignar una clave al sector de arranque por cuestiones de seguridad, en este caso se lo dejó en blanco.

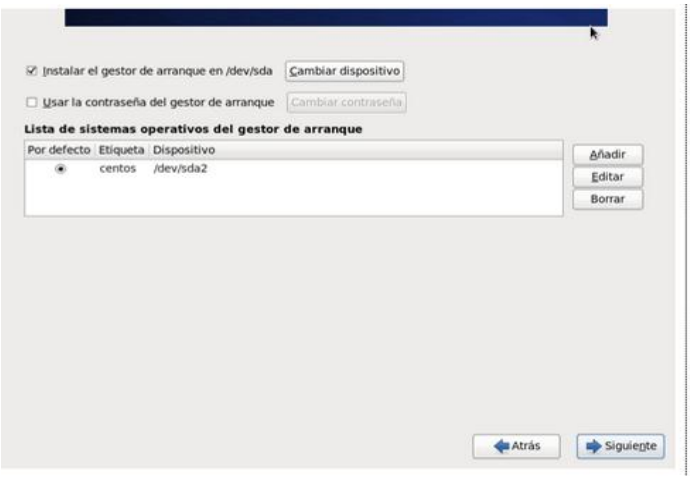


Gráfico 6.86. Contraseña GRU

14. A continuación se seleccionó el tipo de instalación, en este caso fue una Instalación de Escritorio Mínima y se eligió personalizar el software para instalar solamente lo necesario, se escogió este tipo de instalación, esta configuración es la que ya que tiene programas básicos y también se instala en modo gráfico.

Gráfico 6.87. Tipo de Instalación

15. Posteriormente se instalaron los paquetes seleccionados y se terminó la instalación.

Gráfico 6.88. Instalación de Paquetes

Posteriormente al finalizar la instalación se realizó un update para tener los paquetes actualizados. A continuación el comando usado.

Comando: yum update

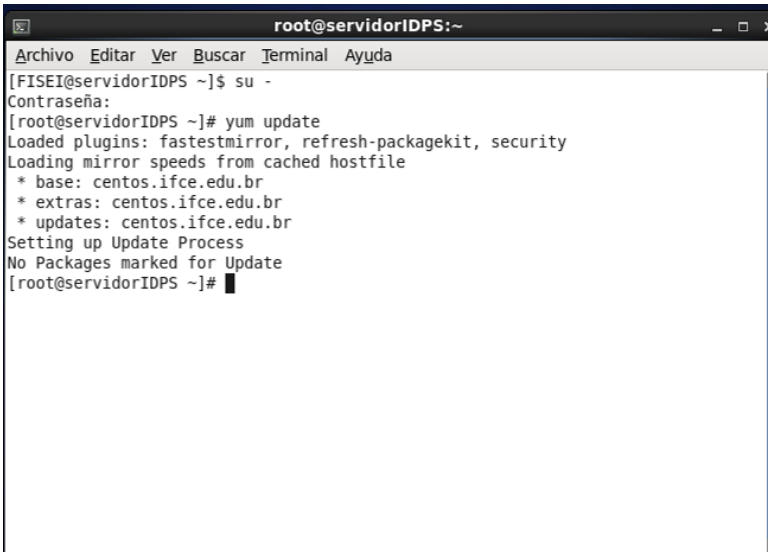


Gráfico 6.89. Paquetes Actualizados

6.13.4. Anexo 4: Instalación Nessus

1. Se descargó de la página oficial de Nessus el paquete y se aceptó los términos de uso.

   http://www.tenable.com/products/nessus/nessus-download-agreement

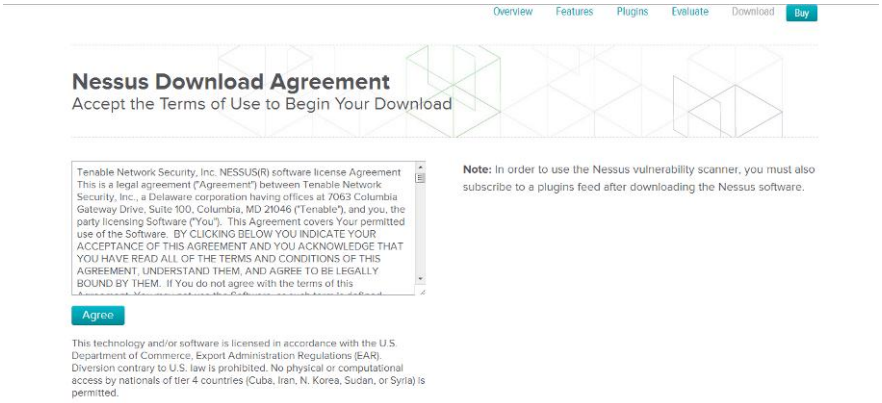


Gráfico 6.90. Descarga Nessus – Terminos de Uso

2. Se seleccionó el paquete en la opción descargar, en este caso se escogió para CentOS 6.

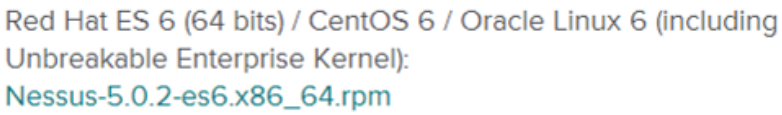


Gráfico 6.91 Paquete de Instalacion para Centos

3. Se instaló el paquete rpm.

[root@localhost /]# rpm -ivh Nessus-5.0.2-es6.x86_64.rpm

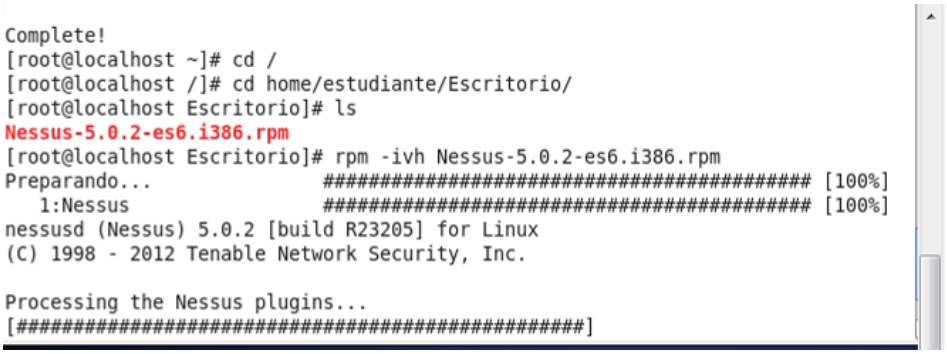


Gráfico 6.92. Instalación paquete rpm Nessus

4. Se añadió el nombre de usuario con su respectiva contraseña con el siguiente comando.

[root@localhost /]# /opt/nessus/sbin/nessus-adduser

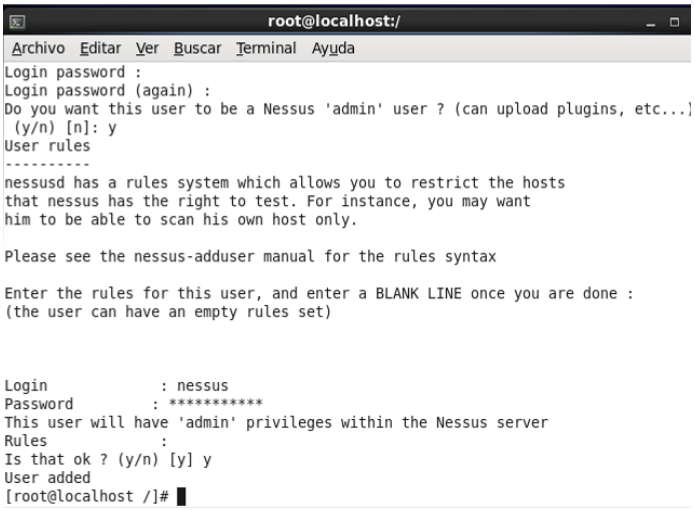


Gráfico 6.93. Añadiendo Usuario Nessus

5. Después se registró Nessus, siguiendo el siguiente enlace y se seleccionó la opción gratuita y de uso personal.

http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code

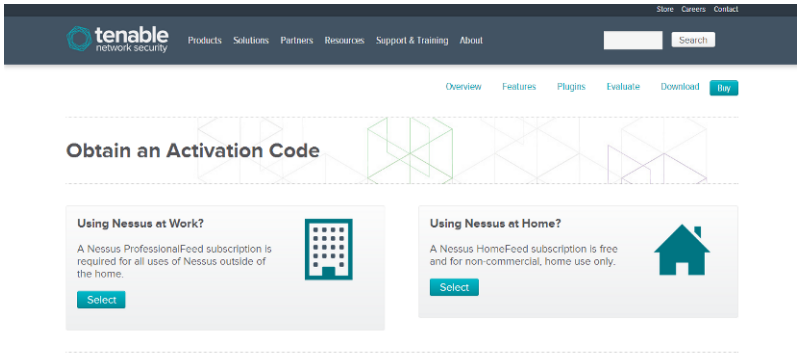


Gráfico 6.94. Código de Activación Nessus

6. Se procedió a llenar los datos (nombre, apellido y correo) para el registro de activación de código.

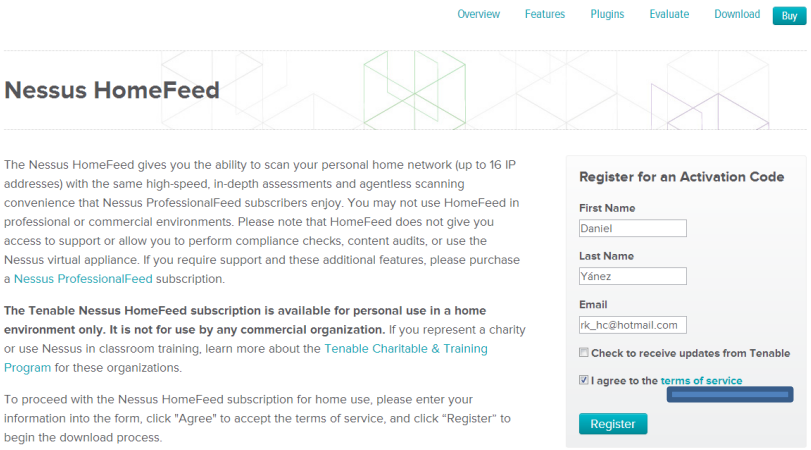


Gráfico 6.95. Datos para Código de Activación Nessus

7. Al dar click en Register se mostró la siguiente pantalla.

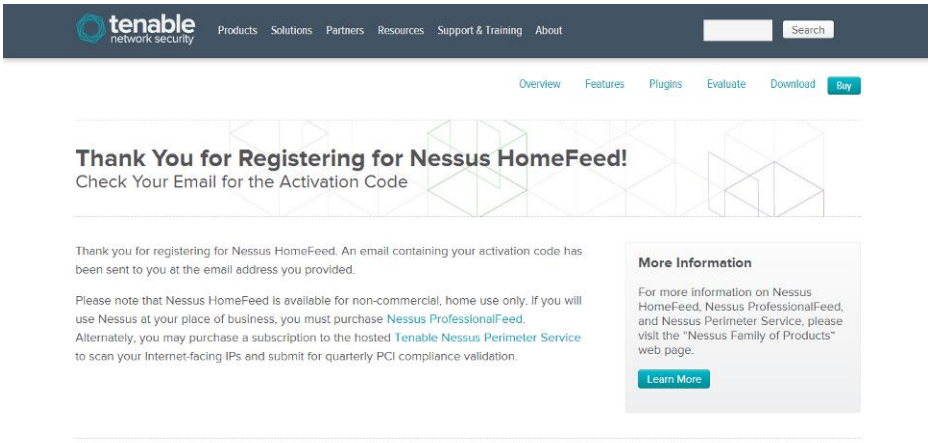


Gráfico 6.96. Confirmación de Registro Nessus

8. A continuación se revisó el correo electrónico para ver el código de activación.

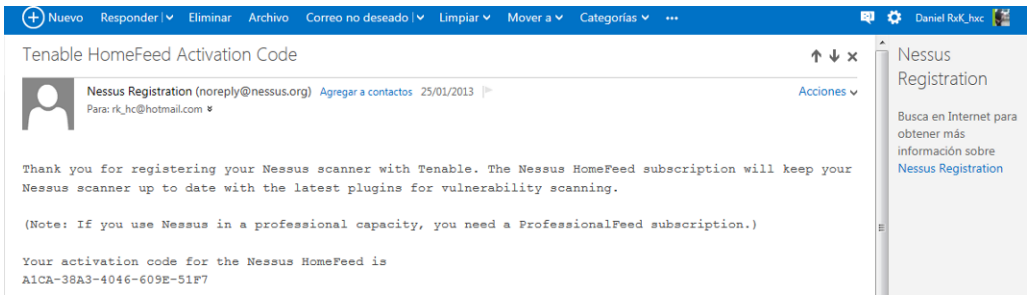


Gráfico 6.97. Código de Activación de Nessus

9. Se utilizó el siguiente comando para la activación de la clave. Este proceso tarda unos minutos, debido que actualiza todos los plugins de nessus.

   [root@localhost /]# /opt/nessus/bin/nessus-fetch –register xxx-xxx-xxx-xxxx

10. Al terminar el proceso se procedió a iniciar por primera vez nessus.

    [root@localhost /]# /sbin/service nessusd start

11. Para finalizar se procedió a ingresar vía web al panel administrativo colocando la siguiente dirección https://localhost:8834, se añadió el nombre de usuario y contraseña.

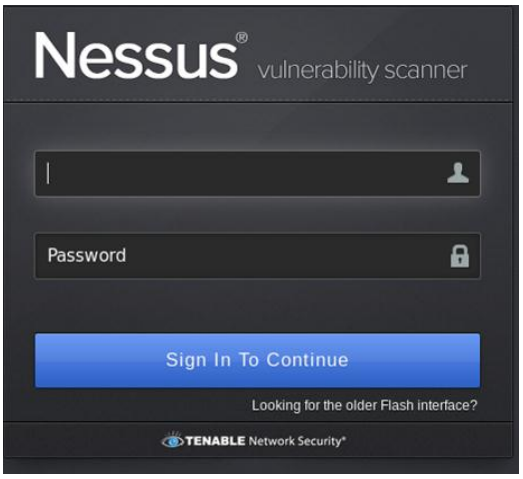


Gráfico 6.98. Pagina Inicial Nessus