ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

"ANALISIS DE LAS SOLUCIONES DEL CONTROL DE ACCESO A LA RED (NAC) PARA MEJORAR LA SEGURIDAD EXTERNA E INTERNA DE REDES CORPORATIVAS"

JULIO ROLANDO FLORES ALVAREZ

Trabajo de Titulación modalidad Proyecto de Investigación y Desarrollo presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH como requisito parcial para la obtención del grado de:

MAGISTER EN INTERCONECTIVIDAD DE REDES

Riobamba – Ecuador

Agosto 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo titulado "Análisis de las Soluciones de Control de Acceso a la Red (NAC) para mejorar la seguridad externa e interna de redes corporativas" de responsabilidad del Sr. Julio Rolando Flores Alvarez, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Fredy Proaño PhD	_____
PRESIDENTE	FIRMA
Ing. Vinicio Ramos MsC	_____
DIRECTOR	FIRMA
Lic. Raúl Lozada MsC	_____
MIEMBRO	FIRMA
Ing. Patricio Moreno MsC	_____
MIEMBRO	FIRMA

Riobamba, Agosto del 2017

DEERECHOS INTELECTUALES

Yo, Julio Rolando Flores Alvarez, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo**.**

_____

Julio Rolando Flores Alvarez

0603079104

DECLARACIÓN DE AUTENTICIDAD

Yo, Julio Rolando Flores Alvarez declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, Agosto de 2017

_____

Julio Rolando Flores Alvarez

0603079104

DEDICATORIA

Mi tesis la dedico con todo mi amor y cariño.

A ti DIOS que me diste la oportunidad de vivir y de regalarme una familia maravillosa que siempre me ha apoyado.

Con mucho cariño principalmente a mis padres Julio Cesar y Zoila María que me dieron la vida y han estado conmigo en todo momento. Gracias por todo papá y mamá por darme una carrera para mi futuro y por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón el que estén conmigo a mi lado.
Los quiero con todo mi corazón y este trabajo es para ustedes, solamente les estoy devolviendo lo que ustedes me dieron en un principio

A mi hermano Angel Leonel quien fue un gran apoyo emocional durante mi desarrollo de tesis.

A esposa Viviana, a mi hija Heidi que son lo mejor que Dios me dio en esta vida, que con su amor siempre me apoyaron para la culminación de mi MAESTRIA.

A todos ellos se los agradezco desde el fondo de mi alma. Para todos ellos hago esta dedicatoria.

Julio

AGRADECIMIENTO

A Dios por ser nuestro creador, a la Escuela Superior Politécnica de Chimborazo y a su benemérita Instituto de Posgrado y Educación Continua IPEC, por habernos educado para ser unos profesionales honestos y comprometidos con la sociedad.

A nuestros catedráticos insignes que nos han brindado generosamente sus conocimientos.
A mi gran amigo Javier quien de una forma desinteresada me ayudo a la culminación de mi tesis

Al Ing. Vinicio Ramos MSC, al Ing. Raúl Lozada MSC, al Ing. Patricio Moreno MSC estudiosos en las ciencias de la Informática, que con su erudición y calidad humana, fueron en todos momentos guías permanentes para el desarrollo de esta investigación.

A todos ellos, mi eterna GRATITUD

Julio

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

LISTA DE ANEXOS

RESUMEN

Se desarrolló un estudio de las soluciones del control de acceso a la red NAC para determinar la mejor alternativa de seguridad externa e interna de redes corporativas. La investigación analizó las distintas alternativas de solución del control de acceso a la red que se ofrecen en el mercado ya que los esfuerzos están en su mayoría enfocados a la actualización de antivirus en los equipos. La herramienta PacketFence de código abierto es una alternativa NAC para las redes corporativas que permiten enfrentar nuevas amenazas, es por ello que contar con la más reciente actualización es imprescindible. Para el levantamiento de la simulación de la red corporativa se tomó como referencia un nodo de red, se utilizó el software GNS3 junto con la herramienta NAC PacketFence, misma que cumplió con los estándares de seguridad propuestas como son la Autenticación, Integridad y Disponibilidad mediante la creación de un portal cautivo que realizó tareas de autenticación de usuarios y dispositivos de red en un 98% de efectividad en cuanto a la integridad de datos 99% y disponibilidad de servicios 99% de efectividad. La solución NAC debe ejecutar todos los componentes y dependencias necesarias para su buen funcionamiento, además de recordar que PacketFence se integra también con redes inalámbricas a través del módulo FreeRADIUS, esto permite asegurar sus redes inalámbricas.

Palabras claves: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <TECNOLOGÍA DE LA COMUNICACIÓN>, <INTERCONECTIVIDAD DE REDES>, <CONTROL DE ACCESO A LA RED>, < PACKETFENCE (SOFTWARE)>,<SEGURIDAD INFORMÁTICA>

ABSTRACT

It was developed a study of control solutions of NAC net access for determining the best alternative of internal and external security of corporative networks. The research analyzed the alternatives of control solution of network access offered in the market since the efforts are focused on the antivirus updating in the equipment. The PacketFence tool of opened cod is an alternative NAC for the corporative networks that allow facing new threats, for this reason, is essential to have with the most recent updating. For the requirement of simulation of corporative network, a network node was taken like reference, it was used a software GNS3 with the NAC PacketFence tool, which fulfilled with proposed security standards as authentication, integrity and availability. The NAC solution must execute all the components and dependencies for its good functioning, in addition, to recall that PacketFence is also integrated with wireless networks by FreeRADIUS module, allowing sure its wireless networks

Keywords: <TECHNOLOGY AND SCIENCE OF ENGINEERING>, < COMMUNICATION TECHNOLOGY>, <INTERCONECTIVITY OF NETWORKS>, < NETWORK ACCESS CONTROL>, < PACKETFENCE (SOFTWARE)>, < IT SECURITY >

INTRODUCCIÓN

El desarrollo tecnológico y la automatización de procesos ha puesto en relevancia la necesidad de la importancia del control de acceso a las redes debido al crecimiento empresarial que obliga a la apertura de nuevas sucursales, oficinas y centros de negocios repartidos en varios lugares en ubicaciones geográficas distintas.

El análisis de las soluciones del control de acceso a la red (NAC) para mejorar la seguridad externa e interna de redes corporativas, es un estudio que brida a éstas empresas y organizaciones la confiabilidad de acceder a su información utilizando distintos medios de acceso sin comprometer la integridad y confidencialidad de los mismos, esto debido al aparecimiento de nuevas amenazas o puntos débiles que requieren atención.

El presente estudio está divido en cinco capítulos en los cuales se desarrolló los aspectos más relevantes de la investigación así:

El Capítulo I, enuncia la problematización que tienen las redes corporativas y la necesidad de buscar alternativas de solución que permitan enfrentar los puntos críticos de debilidad en la red, así se determinó el estudio de las soluciones NAC.

El Capítulo II, es el marco teórico el fundamento que nos permite determinar que son las NAC, su importancia beneficios y herramientas existentes en el mercado informático.

El capítulo III, es la metodología de investigación empleada para el desarrollo del estudio de campo determinando los métodos, técnicas así como la determinación de la población y la muestra.

El Capítulo IV, tiene que ver con la tabulación de la información obtenida a través de la aplicación de los instrumentos respectivos para determinar la seguridad de las NAC con PacketFence con la prueba de CHI-Cuadrado de los indicadores propuestos tales como: Autenticación, Integridad, Disponibilidad.

El Capítulo V, está enfocado a la Propuesta Guía de Implementación de la tecnología NAC

Al término del trabajo de investigación se obtuvieron las correspondientes conclusiones y recomendaciones de este estudio.

CAPITULO I

1. ANTECEDENTES

El desarrollo de la tecnología en el mundo permitió al ser humano el informatizar y automatizar de muchas de sus actividades sus actividades a través de las computadoras, actividades que en años anteriores se realizaban de forma manual y con una pérdida de tiempo considerable, con el paso de los años la informática gracias a los avances del Internet y el constante ingreso de cibernautas han logrado tener alrededor del mundo un importante y significativo número de usuarios. (Administración y Seguridad en Redes, 2006)

Según León, Y. (2013) en su artículo "Internet y el mundo" manifiesta que algunas investigaciones empíricas apuntan a una visión diferente de Internet, no como una tecnología sino como una forma de vida. En 1993, cuando se liberó la web al mundo, sólo tenían acceso determinadas clases sociales especializadas o económicas; sin embargo, el crecimiento exponencial de la red, al pasar de menos de 2 millones de usuarios en 1994 a casi 2 mil 100 millones de cibernautas en 2011, demuestra que la red dejó de ser una tecnología para "una cultura sofisticada".

Los recientes datos estadísticos sobre la penetración de Internet demuestran que, a escala global, es utilizado por 30.2% de los habitantes del planeta, con una tasa de crecimiento anual de 480.4%. Las regiones con mayor número de internautas son Asia, con 922 millones; Europa, con 476 millones; Norteamérica, con 272 millones; Latinoamérica, con 215 millones; África, con 118 millones; y Oceanía, con 21 millones. (Aguirre, 2006)

Los avances en el área de informática y conocimiento se debe a la formación de redes o grupos de personas que bajo una idea, concepto o familiaridad forman redes o grupos de usuarios, si a ello se suman las instituciones gubernamentales, los negocios se tiene un importante número de usuarios conectados a la red pero cuán seguros se esté dentro de las redes, es muy común escuchar en la actualidad hablar de cyber ataques, el término hackers, que superan las "seguridades" impuestas para obtener información a través del uso que pueden obtener, un ejemplo claro de ellos son los "Wikileaks", sitio que a través de la violación de seguridades informáticas dan a

conocer al mundo datos, documentos, videos o elementos que pueden ser compartidos en la red y difundidos a escala mundial a un solo clic. (Carracedo, 2004)

1.1. Planteamiento del problema

El avance científico de la humanidad ha permitió el desarrollo de nueva tecnología que permita al usuario y sus organizaciones crear un sinnúmero de redes que se encuentran más distribuidas, con oficinas y centros de negocios repartidos en distintas ubicaciones geográficas, todos con la necesidad de acceso a la red y sistemas de la compañía utilizando distintos medios de acceso desde tecnologías inalámbricas, Internet, VPN, accesos remotos, etc.

Para Villalón, A. (2012) en su obra "Seguridad en redes", manifiesta que: "Se dice insegura a una red en la cual la privacidad de los datos sea limitada y que se encuentre en riesgo de ser interceptados, alterados o robados, así como propensas a transmitir información que dañe la red misma con virus, ya sea informáticos o de sistemas operativos, y por lo tanto la red se vuelva inestable, no brindando tranquilidad de un funcionamiento constante y óptimo, y en la que no se pueda contar con un ancho de banda variable hasta los límites de una velocidad en la que la transmisión de la información sea estable y aceptable, produciendo un debilitamiento en el rendimiento de la red, volviendo imposible la transmisión de datos; debido a que la red se ha vuelto sumamente lenta.

Los varios entornos de interconexión complejos han unido a la mayor criticidad de los datos que poseen las empresas y organizaciones, y a la necesidad de acceso a los mismos desde cualquier dispositivo y ubicación, todo ello sin comprometer la integridad y confidencialidad de la información, ha provocado la aparición de innumerables y nuevos puntos débiles de acceso. Estas circunstancias implican nuevos riesgos y amenazas ante los cuales las empresas demandan nuevas soluciones para solventarlas. (Nakhjir & Nakhjiri, 2002)

Las empresas y los usuarios domésticos aún no se han concientizado acerca de la seguridad que se necesita al trabajar en los ambientes informáticos ya que aún no han sido víctimas de "atracos en la web", que entro los más comunes están: transferencia ilícita de dinero, apropiación fraudulenta de datos personales, interceptación ilegal de datos, pornografía infantil, acoso sexual, entre otros.

Internet abrió el paso a esas nuevas formas de delincuencia común y organizada que pone en riesgo la información privada, la seguridad en la navegación y de las instituciones públicas y privadas.

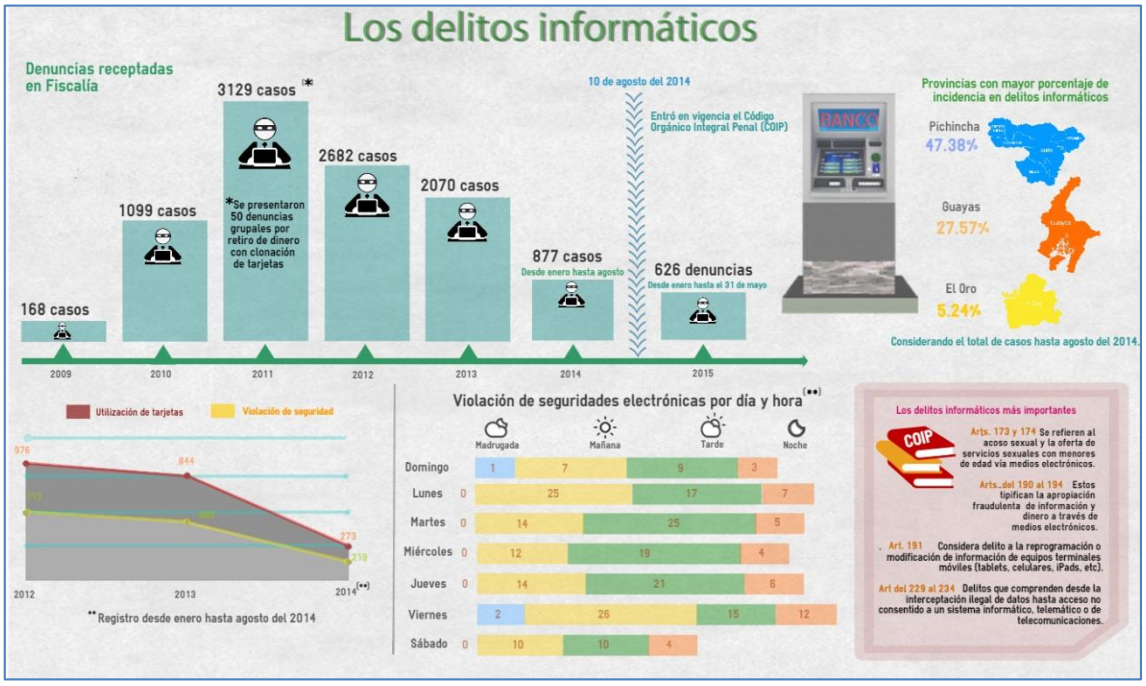

Figura 1-1: Delitos informáticos

Fuente: http://www.fiscalia.gob.ec/

De acuerdo a la Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 -cuando entró en vigencia el Código Orgánico Integral Penal.

Es por ello que se vuelve necesario e indispensable contar son sistemas de seguridad que permita la protección más valioso que posee el ser humano su identidad y sus datos.

1.2 Justificación

El avance tecnológico a escala mundial ha desarrollado variantes de tecnología de redes de computación ya que organizaciones y usuarias domésticos se siguen incluyendo dentro de una red, es por ello que los ataques hacia las redes corporativas públicas y privadas son el blanco de los ataques a través de programas antivirus, usuarios autentificados que vulneran las seguridades implementadas con el objetivo de sustraer información o dañar sistemas informáticos. Las

empresas tienen la necesidad de acceso a las redes corporativas utilizando distintos medios de acceso ya que las empresas tienen cada vez redes más distribuidas, con oficinas y centros de negocios repartidos en distintas ubicaciones geográficas. (Aguirre, 2006)

Es así que el control de acceso a la red es un concepto basado en los dispositivos de red y un conjunto de protocolos usados para definir como asegurar los nodos de la red antes de que estos accedan a la misma. NAC puede integrar el proceso de remedio automático detectando de forma temprana nodos que no cumplen las normativas antes de permitirles acceso, a través de la infraestructura de red como routers, switches y firewalls.

El presente estudio determina como un conjunto de herramientas basadas en tecnología NAC y el equipamiento informático del usuario final permiten asegurar que el sistema de información está operando de manera segura antes de permitir el acceso a la red.

El objetivo de la investigación es tener un acceso de control a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos a los que pueden acceder en la red los usuarios y dispositivos, y que pueden hacer en ella.

Es por ello que la investigación pretende determinar qué tipo de seguridades internas y externas poseen para determinar el grado de utilidad de tecnología NAC en los procesos internos y externos de la red corporativa.

Al finalizar, se puede recomendar varias alternativas de tecnología NAC que permita la seguridad interna y externa de las diferentes redes que conforman la institución.

1.3 Objetivos

1.3.1 *General*

Desarrollar un estudio de las soluciones del control de acceso a la red NAC para determinar la mejor alternativa de seguridad externa e interna de redes corporativas.

1.3.2 *Específicos*

- Documentar las diferentes soluciones de control de acceso a la red NAC.
- Determinar las herramientas de Seguridad Informática con las que cuenta institucionalmente una red corporativa en sus diferentes laboratorios de cómputo, mediante la aplicación de una encuesta a los administradores de Red, pretendiendo además conocer si utilizan soluciones NAC.
- Implementar un escenario de simulación con GNS3 para el control del tráfico HTTP con PacketFence, en la creación de portal cautivo con sus mecanismos de conexión, autenticación.
- Proponer una guía de implementación de la tecnología NAC para la seguridad externa e interna de las redes corporativas.

1.4 Hipótesis

La implementación de tecnología NAC permitirá mejorar la seguridad externa e interna de las redes corporativas.

CAPITULO II

2. REVISION DE LITERATURA

2.1 Antecedentes

En realidad, el fenómeno informático es la es la expresión de un crecimiento acelerado de la capacidad de procesar información por parte del género humano. Esta capacidad de procesamiento es la que convierte a la información en conocimiento. Es por ello que la Revolución informática es sólo la cobertura tecnológica de un proceso mucho más amplio definitorio: el desplazamiento de la humanidad hacia el concepto de la SOCIEDAD DEL SABER. (Peter, 2004)

Pero todo el conocimiento y la acumulación de información a través de los computadores ha desarrollado una serie de ataques tanto internos como externos para tratar de conseguir lo que es en la actualidad valioso para la empresa "su información", un bien intangible que le permite posicionarse en el mercado y estar a la vanguardia de los proceso a escala mundial.

Es así que La globalización y la dinamización de los negocios ha obligado a las empresas a que no pueden permitirse el lujo de tener pérdidas y sabotajes de la información que mermen su productividad y paralicen su actividad.

2.2 Seguridad

La seguridad en redes es mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales) control y autenticidad de la información manejada por computadora, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado. (Nakhjir & Nakhjiri, 2002)

Seguridad informática se puede definir como un conjunto de medidas que impidan la ejecución de operaciones no autorizadas sobre un sistema o red informática, estás medidas pueden ser un conjunto de reglas, planes, actividades y herramientas. Los efectos que puede tener una operación

no autorizada en un sistema informático, pueden conllevar daños sobre la información, comprometer su confidencialidad, autenticidad, integridad, también pueden disminuir el rendimiento de los equipos, desactivar los servicios o bloquear el acceso a los usuarios autorizados del sistema.

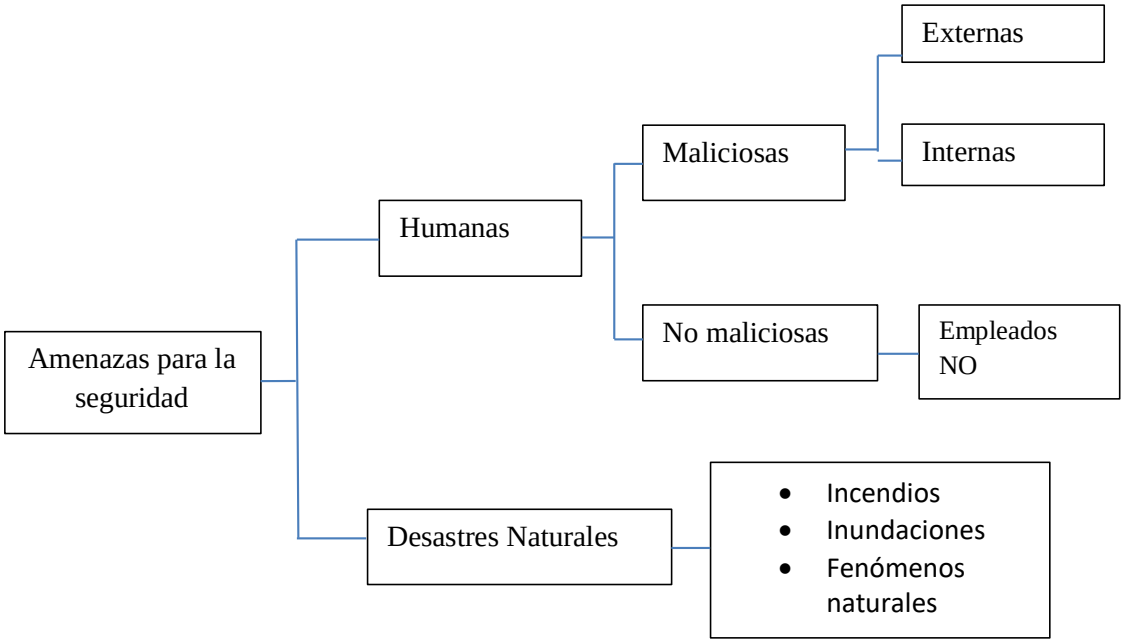

Figura 1-2: Tipos de Amenazas a la seguridad

Fuente: http://isvoc.com/download/ISO_27002_EN.pdf

2.2.1 *Tipos de seguridad*

Podemos clasificar a la seguridad en redes en 2 tipos, y de ellos se subdividen en la siguiente tabla donde más adelante se definirán. (Aguirre, 2006)

2.2.1.1. *Seguridad física.*

La seguridad física es la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial".

La seguridad física se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de computo así como los medios de acceso remoto del mismo; implementados para

proteger el hardware y medios de almacenamiento de datos. Es muy importante, que por más que nuestra organización sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc; la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

- Desastres
- Incendios
- Equipamiento
- Inundaciones
- Picos y ruidos electromagnéticos
- Cableado

2.2.1.2. *Seguridad Lógica*

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo. (Aguirre, 2006)

Después de ver como nuestra red puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un sitio de computo, no será sobre los medios físicos, sino, contra información por él almacenada y procesada.

Así, la seguridad física, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la seguridad lógica.

a. **Tipos de seguridad lógica**

- Controles de acceso
- Identificación
- Roles

- Transacciones
- Limitación a los servicios
- Control de acceso interno

b. Objetivos de la seguridad lógica

Los objetivos que se plantean para la seguridad lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.2.2 Seguridad Externa e Interna

Conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no sea conectada a un entorno externo no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre 60 y 80 por ciento de los incidentes de red son causados desde adentro de la misma. (Arquitectura de protección de acceso a la Red, 2005) Basado en esto podemos decir que existen 2 tipos de amenazas:

Amenazas internas

Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

- Los usuarios conocen la red y saben cómo es su funcionamiento.
- Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

- Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

(Carracedo, 2004) Entre las amenazas internas están:

Personal enterado.-personal que tiene acceso autorizado puede ser personal que labora en la actualidad o ex empleados que lo pueden hacer por revanchas personales o motivados por el dinero.

Curiosos.- Ingresan al sistema sin autorización motivados por aprender, curiosidad, desafío a personal, se debe tener bastante cuidado porque pueden causar daño no intencional incluso perdidas económicas.

Sabotaje.-consiste en reducir la funcionalidad del sistema por medio de acciones que impidan el normal funcionamiento por tanto daño de los equipos, interrupción de los servicios, en algunos casos provocando la destrucción completa del sistema.

Fraude.-actividad que tiene como fin aprovechar los recursos para obtener beneficios ajenos a la organización.

Ingeniería social.- obtener información social a través de la manipulación a los usuarios legítimos impulsándolos a revelar información sensible. De esta manera los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra antes que aprovechar de los agujeros de seguridad de los sistemas.

2.2.2.1. *Amenazas externas*

Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.
Entre las amenazas externas están:

Intrusos.- Se encarga de ingresar al sistema con un objetivo fijo, se debe tener precaución porque estas personas tienen la experiencia. Capacidad y herramientas para ingresar al sistema sin importar el nivel de seguridad que posea.
Terrorista.- Causar daño para diferentes fines.

Robo.- Extraer información en alguna unidad de almacenamiento, robo físico de hardware para otros fines.

Amenazas de hardware.-las amenazas se da por las fallas físicas del hardware ya sea defectos de fabricación o mal diseño de hardware que forma parte del sistema de cómputo

2.2.2.2. *Tipos de amenazas de hardware.*

Mal diseño.-cuando los componentes de hardware del sistema no cumple con los requerimientos necesarios.
Errores de fabricación.-cuando el hardware tienen desperfecciones de fabricación y fallan en el momento de usarse. Esto trae consecuencias negativas a la organización que a los fabricantes.

Suministro de energía.- las variaciones de voltaje provocan daños en los dispositivos, es por esto que debemos revisar las instalaciones de energía, que proporcionen el voltaje que se requiere de acuerdo al hardware caso contrario se acortara su vida útil.

Desgaste.- al usar el hardware se da un desgaste de este hasta que no se pueda utilizar.

Descuido y mal uso.-los componentes de hardware deben ser usados tomando en cuenta los parámetros establecidos de los fabricantes como son: Tiempo de uso, periodos y procedimientos

de mantenimiento, no tomar en cuenta esto provoca un mayor desgaste y reduce la vida útil de los recursos de hardware.

2.3 Control de Acceso a la Red (NAC)

2.3.1 *Concepto.*

NAC, (Network Access Control) es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades), usuario o sistema de autenticación y reforzar la seguridad de la red de acceso. (CISCO, 2006)

El control de acceso a red es un concepto de ordenador en red y conjunto de protocolos usados para definir como asegurar los nodos de la red antes de que estos accedan a la red. NAC puede integrar el proceso de remedio automático (corrigiendo nodos que no cumplen las normativas antes de permitirles acceso) en el sistema de red, permitiendo a la infraestructura de red como routers, switches y firewalls trabajar en conjunto con el back office y el equipamiento informático del usuario final para asegurar que el sistema de información está operando de manera segura antes de permitir el acceso a la red. (CISCO, 2006)

2.3.2 *Objetivos de las NAC.*

El objetivo del control de acceso a red es realizar exactamente lo que su nombre implica: control de acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos a los que pueden acceder en la red los usuarios y dispositivos y que pueden hacer en ella.

Entre ellos están:

- El control de acceso a red
- Mitigar ataques de día cero
- Refuerzo de políticas
- Administración de acceso e identidad

a. Control de Acceso

El control de acceso a red (NAC) representa una categoría emergente en productos de seguridad, su definición es controvertida y está en constante evolución. (Knipp & Brian, 2002)

b. Mitigar ataques de día cero

El propósito clave de una solución NAC es la habilidad de prevenir en los equipos finales la falta de antivirus, parches, o software de prevención de intrusión de hosts y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de gusanos informáticos.

c. Refuerzo de políticas

Las soluciones NAC permiten a los operadores de red definir políticas, tales como tipos de ordenadores o roles de usuarios con acceso permitido a ciertas áreas de la red, y forzarlos en switches y routers. (Knipp & Brian, 2002)

d. Administración de acceso e identidad

Donde las redes IPs convencionales refuerzan las políticas de acceso con base en direcciones IP, los dispositivos NAC lo realizan basándose en identidades de usuarios autenticados, al menos para usuarios finales de equipos portátiles y sobremesa.

2.3.3 *Pre-admisión y Post-admisión*

Existen dos filosofías de diseño predominantes en NAC, basadas en políticas de refuerzo antes de ganar acceso a la red o después de hacerlo.

2.2.1.3. *NAC Pre-admisión*

Las estaciones finales son inspeccionadas antes de permitirles el acceso a la red. Un caso típico de NAC pre-admisión sería el prevenir que equipos con antivirus no actualizados pudieran conectarse a servidores sensibles.

2.3.3.1 *NAC Post-admisión*

Crea decisiones de refuerzo basadas en acciones de usuario después de que a estos usuarios se les haya proporcionado el acceso a la red. Con agente vs sin agente La idea fundamental de la

tecnología NAC es permitir a la red tomar decisiones de control de acceso basadas en inteligencia sobre los sistemas finales, por lo que la manera en que la red es informada sobre los sistemas finales es una decisión de diseño clave. Una diferencia clave entre sistemas NAC es si requieren agentes software para informar de las características de los equipos finales, o si por el contrario utilizan técnicas de escaneo e inventariado para discernir esas características remotamente. (Control de Acceso a la Red, 2009)

Entre las soluciones podemos encontrar: cuarentena y portal cautivo, los administradores de sistemas y redes despliegan productos NAC con la esperanza de que a algunos clientes legítimos se les denegará el acceso a la red (si los usuarios nunca tuvieron antivirus desactualizados y sus sistemas están siempre actualizados, NAC no sería necesario). Por ello las soluciones NAC requieren de un mecanismo para remediar el problema del usuario final que le ha sido denegado el acceso a la red.

2.4 Términos y tecnologías.

Las soluciones NAC son diferentes pero pueden ser clasificadas en dos grupos:

- Clienless no necesita de ningún software instalado en los dispositivos.
- Client-based un componente de software es preinstalado en los dispositivos para poder asistir al proceso de NAC.

Existe un número de factores para decidir cuál tipo de solución es la más adecuada dependiendo de cómo está formada la organización, NAC basado en cliente provee más detalle del dispositivo pero también hay que tener en cuenta que requiere su instalación equipo por equipo. (Bello, 2002)

2.4.1. *Pre admisión NAC*

Determina que un dispositivo cumpla con ciertos criterios predeterminados antes de permitirle el acceso a la red. Si esos criterios no se cumplen, no permite que el dispositivo se conecte a la red, o le asigna un acceso restringido. (Arquitectura de protección de acceso a la Red, 2005)

La Pre-Admisión en NAC se encuentra en las siguientes soluciones:

- Microsoft NAP
- Cisco NAC

- Mobile NAC
- IPSec VPN
- SSL VPN

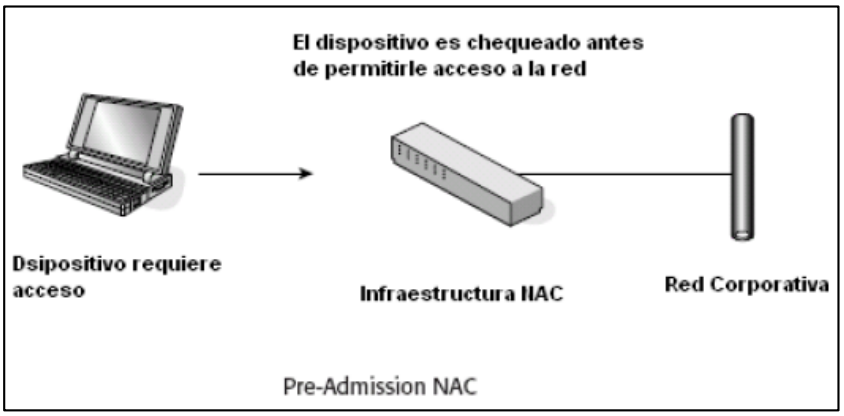

Figura 2-2: Pre Admisión NAC

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

2.4.2. *Estrategias.*

Existen tres estrategias de implantación de NAC basándonos en dónde se introduce el control de acceso a la red, así que uno debe decidir cuál de las tres se ajusta más a las características y particularidades de la organización. (Nakhjir & Nakhjiri, 2002)

Estas estrategias son:

2.4.2.1. *Control en el Perímetro (Edge Control)*

Introduce el control de acceso a la red en el exterior, es decir en el punto donde se conectan los sistemas a ésta, por ejemplo en el switch de una LAN, o en un concentrador VPN.

2.4.2.2. *Control Central (Core Control)*

El control de acceso se puede implantar en cualquier punto de acceso a la red, por ejemplo, a través de un dispositivo que se coloca en medio de la red por el que pasa el tráfico de los equipos cuyo acceso se quiere analizar.

2.4.2.3. *Control en el Cliente (Client Control)*

La implantación de las políticas de seguridad y control de acceso se realiza fundamentalmente en el usuario final, instalando en cada uno de los equipos y sistemas que se quiera gestionar y controlar todas las aplicaciones necesarias para realizar este control, como firewalls personales, aplicaciones de control del acceso inalámbrico, control de dispositivos USB, etc. (Aguirre, 2006)

2.5 Terminología utilizada en cada una de las arquitecturas

Dependiendo de la arquitectura de cada uno de los protagonistas la terminología se resume en la siguiente tabla:

Tabla 1-2: Terminología de tecnologías NAC

TERMINOLOGIA	IETF	TCG TNC	MICROSOFT NAP	CISCO NAC
Colector de estado	Posture Collector	Integrity Measurement Collector	System Health Agent	Posture Plug-in Applications
Agente intermedio	Client Broker	TNC Client	NAP Agent	Cisco Trust Agent
Módulo de peticiones de acceso	Network Access Requestor	Network Access Requestor	NAP Enforcement Client	Cisco Trust Agent
Punto de acceso y aplicaciones de políticas	Network Enforcement point	Policy Enforcement Point	NAP Enforcement Server	Network Access Device
Servidor de verificación de estado	Posture Validator	Integrity Measurement Verifier	System Health Validor	Policy Vendor Server
Modulo intermedio	Server Broker	TNC Server	NAP Administration Server	Access Control Server
Servidor de autorización de acceso	Network Access Authority	Network Access Authority	Network Policy Server	Access Control Server

Fuente:http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

2.6 Soluciones NAC en el mercado

En el mercado existen varias empresas que dedican sus aplicaciones y trabajo para ofrecer soluciones de seguridad completas como: seguridad por capas con protección antivirus, antispyware, anti spam, prevención de intrusiones IPS y filtrado de contenidos web.

Empresas que están especializadas en la asesoría, implantación, gestión y mantenimiento de todas las soluciones de seguridad en red con firewalls UTM y Wifi, las soluciones SSL VPN de Acceso Remoto Seguro, la seguridad de correo electrónico y anti spam, hasta las soluciones de Backup y copias de seguridad. Bajo la premisa que Internet ofrece muchas ventajas, pero también pone en riesgo la seguridad de las empresas (Carracedo, 2004)

Tabla 2-2: Soluciones existentes en el mercado y sus características

Producto	Descripción de la Solución	Tecnología
Cisco NAC Framework	Iniciativa propietaria de Cisco basada en la implantación de control de acceso dentro de la infraestructura de red.	Cisco NAC
Cisco NAC Appliance	Equipos Cisco que permiten una rápida implantación de políticas de control de acceso a la red.	Cisco NAC
ConSentry LANShield	Solución NAC de alto rendimiento pensada para ser desplegada de forma perimetral. Control de acceso basado en identidad, políticas y datos de usuario.	Basada en dispositivos propios, appliances creados por ConSentry
Elemental Security Platform	Sistema diseñado para monitorizar dispositivos de red, configuraciones, actividad de los usuarios, implementando políticas de seguridad basado en roles.	Propietaria, basada en un modelo de servidores y software de agentes.
ENDFORCE Enterprise	Solución basada en software, diseñada para redes heterogéneas, con la capacidad de extender las funcionalidades ofrecidas por las arquitecturas NAC, NAP y TNC.	Basada en estándares, compatible con CNAC, NAP y TNC
FireEye NAC Appliance	Basada en appliances que implanta el control de acceso basándose en la inspección del tráfico de los dispositivos de la red, y por tanto en la deyección de tráfico peligroso o dañino.	Propietaria, basada en dispositivos propios junto con la tecnología FACT

ForeScount CounterAct	Utiliza appliances propios, para realizar un despliegue transparente, no perjudicial para la red donde se realiza, combinando control de acceso que no utiliza clientes con prevención de intrusos para asegurar el correcto cumplimiento de la seguridad en los equipos.	Propietaria, basada en dispositivos propios junto con la tecnología FastPass.
InfoExpress CyberGatekeeper	La familia CyberGatekeeper ofrece productos, uno para implementar en entornos LAN, otro para sistemas remotos y el tercero que focaliza el control de acceso sobre el usuario final.	Propietaria, basada en dispositivos servidores y software de agentes y servidores.
Insightix NAC	Mantiene un inventario exhaustivo de todos los dispositivos conectados a la red, permitiendo, gracias a su tecnología de bloqueo y cuarentena única, implementar políticas de seguridad y control de acceso para cualquier dispositivo o tráfico.	Propietaria.
Juniper Networks Unified Access Control (UAC)	El control de Acceso Unificado 2.0 incluye varios elementos: Infranet Controller, agente UAC y puntos de aplicación de la política de seguridad. Funciona en gran variedad de entronos, incluyendo aquellos con 802.1X	Compatible con la arquitectura TNC
Lockdown Enforcer	Se trata de aplliences dinámicos de control de acceso a la red, que autentica de forma simultánea a usuarios y dispositivos y los analiza de forma periódica y también en caso de solicitud puntual, comprobando que cumplen las políticas de seguridad.	Propietaria, basada en appliances
Microsoft NAP	Iniciativa propietaria de Microsoft.	Microsoft NAC
Mirage Networks NAC	Familia de productos NAC, en la que las decisiones sobre qué políticas aplicar a los usuarios se toman en dispositivos diferentes a los que finalmente aplican la política, basada en escaneos de dispositivos y prevención de intrusos.	Propietaria, compatible con arquitecturas TNC y NAP
Nevis Networks LANenforcer	Esta solución se implementa sobre switches que son los que realizan el control de acceso de los usuarios, cada uno de los cuales se ubica en una DMZ personal donde se le protege de amenazas, y a la vez se protege a la red de las amenazas que pueda provocar dicho usuario.	Propietaria, basada en el uso de dispositivos propios (switches)

Nortel Secure Network Access	Solución de control de acceso a redes basada en la implementación de control en los switches LAN, routers y gateways SSL VPN de Nortel.	Propietaria
Senforce NAC & Endpoint Security Suite	Solución que integra la comprobación de que los usuarios finales están libres de amenazas, con la seguridad inalámbrica y el control de acceso a la red.	Compatible con la arquitectura Cisco NAC
StillSecure SafeAccess	Solución muy flexible, que ofrece cinco opciones de aplicación de políticas en diferentes entornos, por lo que se adapta muy bien a redes complejas y heterogéneas.	Compatible con la arquitectura Cisco NAC
Symantec Network Access Control	Ofrece una solución que permite aplicar control de acceso para dispositivos que se conectan a través de SSL VPNs, switches inalámbricos, aplicaciones basadas en Web, usando 802.1X, y casi cualquier infraestructura LAN o inalámbrica.	Compatible con la arquitectura Cisco NAC
Vernier EdgeWall	Appliances NAC, que validan a los usuarios mediante una mezcla de política de confianza y chequeo de vulnerabilidades.	Propietaria
Enterasys Secure Networks	Arquitectura basada en redes inteligentes, capaces de gestionar de forma individualizada cada usuario o dispositivo, permitiendo un control granular de usuarios, dispositivos y aplicaciones, ofreciendo una respuesta dinámica a intrusiones.	Basada en estándares, no propietaria
HP Procurve Networking Adaptative EDGE	Arquitectura que permite construir redes con inteligencia perimetral, que pone la inteligencia en el punto de conexión del usuario, permitiendo realizar en ese punto funciones como la priorización de tráfico, autenticación, reserva de ancho de banda y aplicación de políticas	Arquitectura propietaria

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

2.6.1 *NAC de Cisco*

Es una arquitectura propietaria, que en el lado del cliente se compone de un agente denominado Cisco Trust Agent software gratuito descargable desde la página del fabricante y cuya función es la de recibir la información del estado de la seguridad del equipo a conectar a la red proporcionando toda la información recogida, para recopilar esta información pueden usarse aplicaciones de distintos fabricantes o una propietaria de Cisco, el Cisco Secure Access. Para el Trust Agent Cisco ha desarrollado un protocolo propietario el EAP, en dos versiones: una sobre UDP y otra sobre 802.1X. La diferencia entre ambas es que sobre UDP se hace solo validación y en 802.1X se hace validación y autenticación. Además no todos los equipos Cisco soportan todos los escenarios posibles a través del protocolo EAP, muchos switches y routers requieren de una actualización. En cuanto a servidores Cisco la implementa en base al Access Control Server que ha desarrollado para tal fin, completando con interfaces de verificación, auditoria y autenticación de otros fabricantes. Cisco también ofrece una solución basada en appliances permitiendo una más rápida implementación. Cisco define a NAC como: El control de la admisión de la red de Cisco (NAC) es una solución que utiliza la infraestructura en red para hacer cumplir políticas de seguridad en todos los dispositivos que intentan tener acceso a recursos de computación de la red NAC ayuda a asegurar que todos los hosts cumplan con las últimas políticas de seguridad corporativa, tales como antivirus, software de la seguridad, y patch (remiendo) del sistema operativo, antes de obtener el acceso de red normal. (CISCO, 2006)

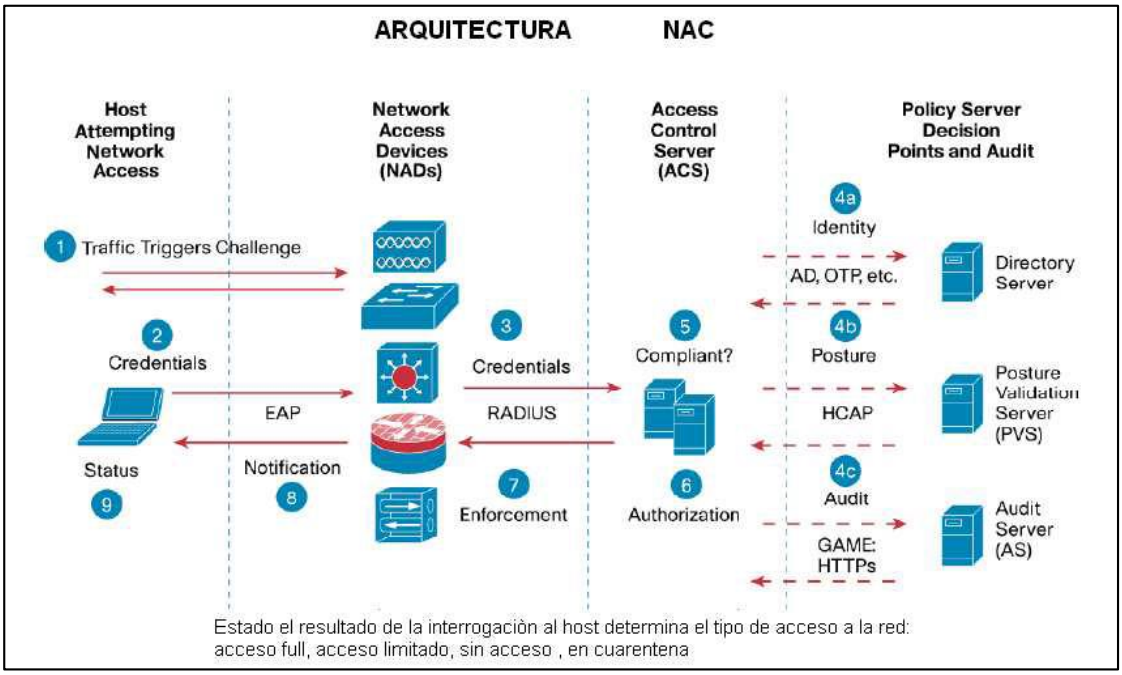

Figura 3-2: Implantación NAC de Cisco

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

2.6.1.1 *Secuencia Interna NAC de Cisco*

a. La validación de postura ocurre cuando un dispositivo de acceso a la red detecta que un host se quiere conectar o usar los recursos de la red.
b. Una vez detectado el nuevo dispositivo el NAD (dispositivo de acceso a la red) habilita una conexión entre el AAA server) servidor de autorización autenticación y auditoria y el Access control server ACS o server de control de acceso, una vez establecida el Server AAA requiere las credenciales de postura al host desde uno o más plugins de posturas.
c. El host responde a la petición con sus credenciales de postura desde los software compatibles con NAC
d. El server AAA valida la información de las posturas localmente, o puede delegar esta decisión a otros servers de validación de posturas
e. El server AAA agrega los resultados individuales de la postura, o símbolo (tokens) de postura, de todos los servers para determinar la conformidad total del host, o del símbolo de postura del sistema.
f. La autenticación de identidad y el token de postura del sistema son luego chequeadas por una red de autorización , que puede consistir en : server Radius, asignación de VLANs o listas de acceso descargables
g. Estas cualidades del Radius se envían al NAD para la aplicación en el host.
h. El CTA en el host envía el estado de su postura para notificar los plugins respectivos de su postura individual del uso así como la postura entera del sistema.
i. Se puede enviar opcionalmente un mensaje al usuario final usando el diálogo de la notificación de CTA's notificando el estado actual del anfitrión en la red.

2.6.1.2 *Secuencia Externa NAC de Cisco*

Muchas compañías no tienen un control de sus propias Pc’s, laptops del personal que accede desde afuera, oficinas remotas de la organización, aquí es necesaria la implementación de Firewall, IPS e IDS previenen de ataques de hackers (CISCO, 2006)

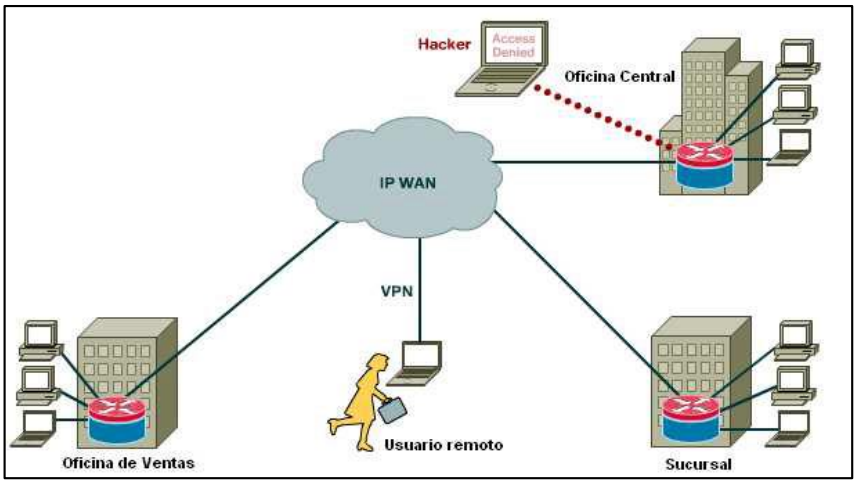

Figura 4-2: Acceso Externo a la red

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

Es necesario que los dispositivos que cumplen con las políticas de seguridad en todos los puntos de acceso a la red, quizás desde el primer momento en su acceso, NAC de Cisco permite tener una política global para todos aquellos usuarios que trabajan en la red, esto es una política de control de admisión de acceso. (CISCO, 2006)

Entre los factores que evalúa la tecnología Cisco está:

- ¿Qué y quien se conecta y por cuánto tiempo?
- ¿Cuáles son los requerimientos para garantizar un acceso seguro a la red?
- ¿Qué pasos se deben seguir para conseguir que se cumpla este acceso seguro?
- ¿Cuáles son los requerimientos son predeterminados y cuales son modificables?

Cisco introduce el concepto de NAC o Control de Admisión a la red NAC que permite dar seguridad la entera relación entre los puntos finales y la red.

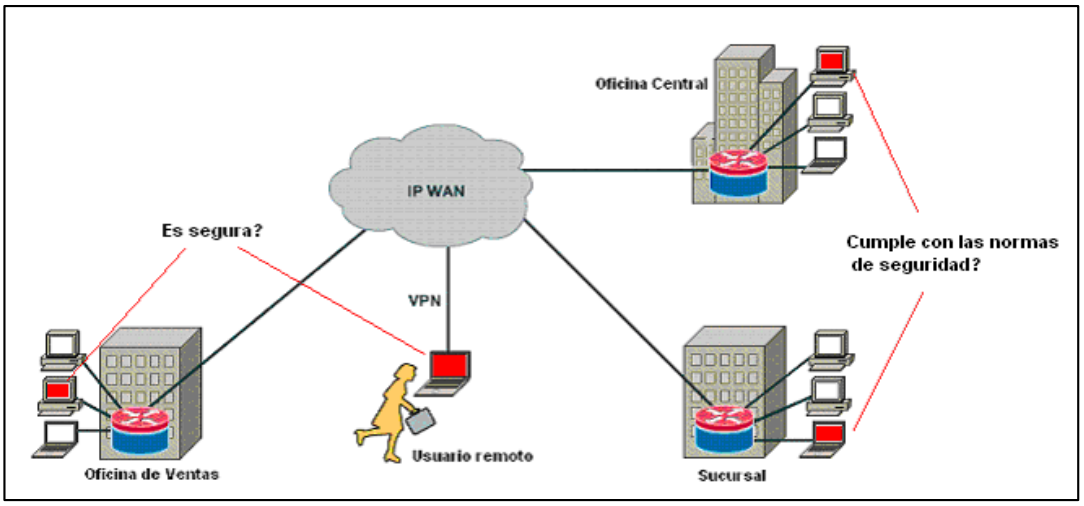

Figura 5-2: Escenario de una Red Externa

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

La solución NAC de Cisco permite:

- Autenticar e identificar accesos.
- Hacer cumplir la política de accesos, impidiendo aquellos no permitidos.
- Identificar e impedir el acceso a usuarios que no cumplan con la política de seguridad establecida.
- Eliminar o en su defecto mitigar la vulnerabilidad.

La solución NAC de Cisco permite controlar el acceso de los usuarios a la red en un punto de acceso verificado además de su identidad el cumplimiento de todas las políticas de seguridad establecidas por la organización, es decir que el equipo que trate de conectarse este actualizado, tenga todas las herramientas de seguridad exigidas por la empresa, etc. Se incluye además el control sobre lo que pueden hacer, a que contenidos e información pueden acceder estos usuarios y que sistemas o recursos son accesibles una vez admitidos en la red. (Knipp & Brian, 2002)

Un usuario se conecta a la red corporativa con su laptop, pero su sistema operativo es vulnerable.

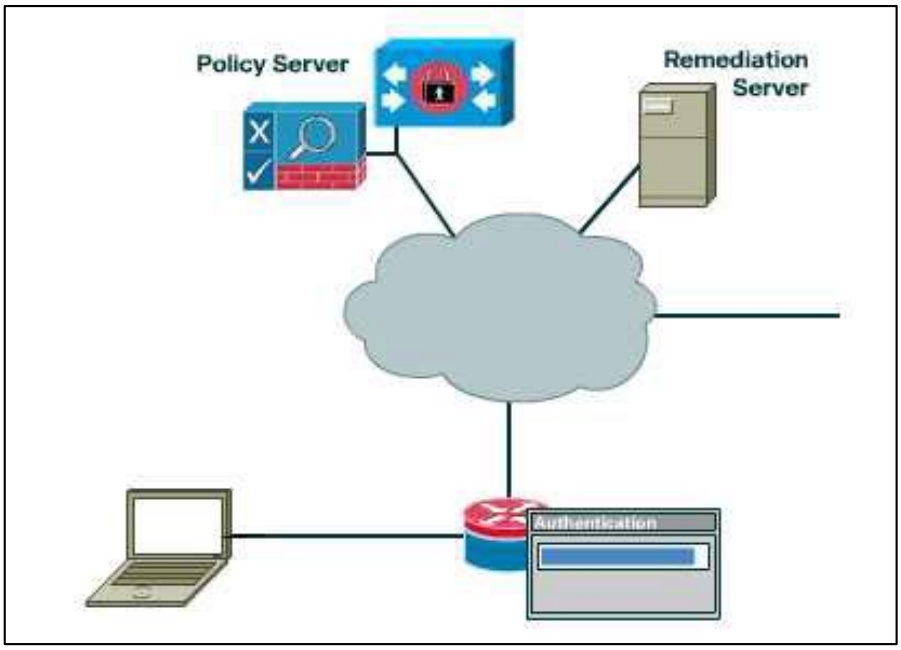

Figura 6-2: Usuario Autenticado

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

El sistema NAC de Cisco, mediante el control de admisión a la red escanea el dispositivo que se quiere conectar y encuentra que el sistema operativo del terminal puede o no ser vulnerable a un nuevo ataque.

2.6.1.3 *Políticas NAC-Cisco*

La solución Network Admission Control diseñada para proteger las empresas ante riesgos de seguridad de información provocados por usuarios o dispositivos que no cumplan las políticas de seguridad corporativas, está preparada para responder a los desafíos crecientes a los que se enfrentan las empresas provocados por amenazas cada vez menos predecibles, el dispositivo abunda en el concepto NAC de Cisco proporcionando políticas de seguridad en puntos de acceso a la red dentro de una empresa distribuida. Presenta capacidades significativas de imposición de políticas para proteger redes de área local (LAN) así como oficinas remotas, redes privadas virtuales (VPN) y puntos de acceso inalámbricos. (CISCO, 2006)

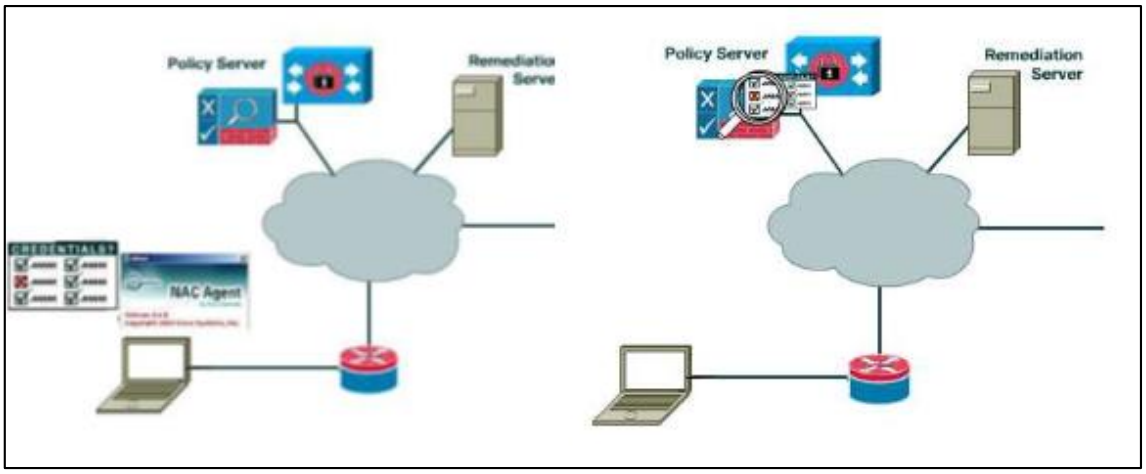

Figura 7-2: Políticas de Acceso NAC-Cisco

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

Esta vulnerabilidad es chequeada por el o los servers de políticas de validación. Si no cumple con lo estipulado sus credenciales no son aceptadas.

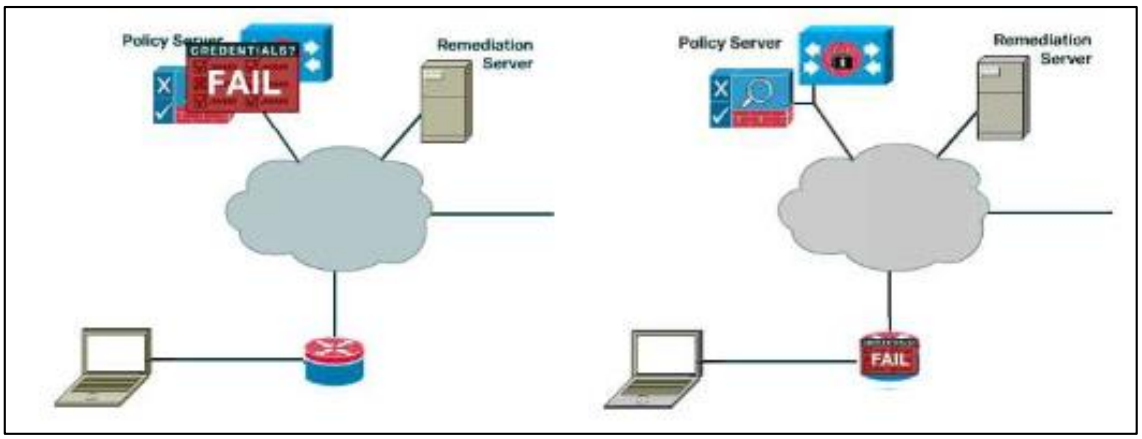

Figura 8-2: Acceso Denegado NAC-Cisco

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

2.6.1.4 *Solución NAC - Cisco*

El sistema re direcciona la conexión a un server llamado server de remediación, el cual actualiza el sistema operativo con los últimos fixes haciendo que el dispositivo cumpla con las normas de seguridad establecidas por la organización.

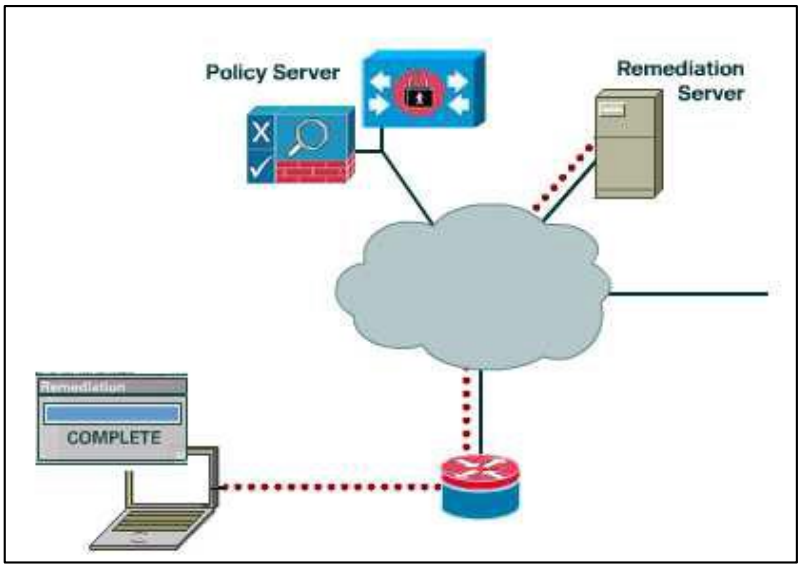

Figura 9-2: Solución NAC-Cisco

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

El dispositivo es nuevamente chequeado y ya remediado se le otorga las credenciales de acceso. (Knipp & Brian, 2002)

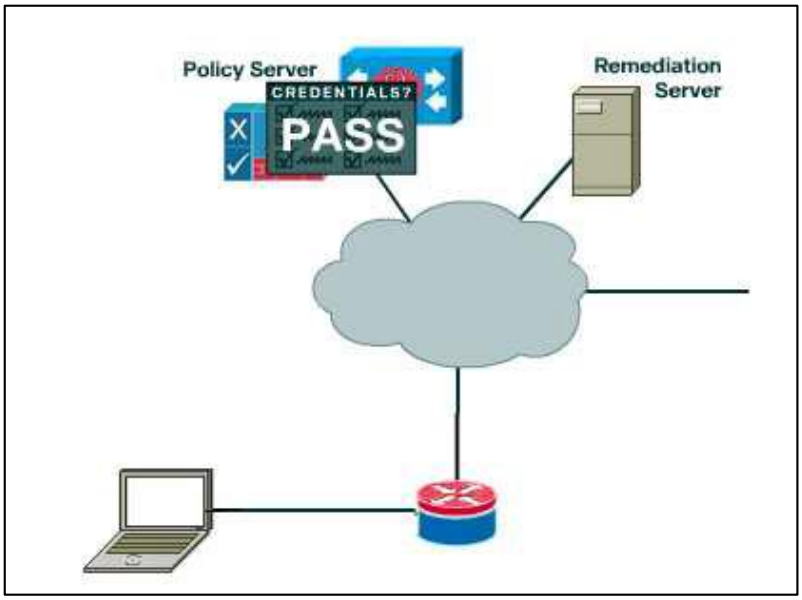

Figura 10-2: Acceso Concedido NAC-Cisco

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

2.6.2 NAP de Microsoft

NAP (Network Access Protection) es la solución propietaria de Microsoft, consta de una plataforma plataforma que proporciona componentes para la aplicación de políticas para ayudar

a asegurarse que las computadoras conectadas o a conectarse en una red cumplan con los requisitos para la salud del sistema de aplicación pensada para ser soportada por el sistema operativo de Windows Vista y el servidor Windows Longhom, requiere servers corriendo Windows Server 2008 y clientes corriendo Windows Vista o Windows XP service pack 3. (Nakhjir & Nakhjiri, 2002)

NAP protege las redes y dispositivos que componen la red aplicando políticas de confianza basadas en requerimientos de salud que deben cumplir los dispositivos al componer una red.

La mayor diferencia que presenta esta solución es que al no ser fabricante de equipos de networking Microsoft basa su despliegue de agentes y aplicaciones en el lado del cliente y en el uso de disitinto tipo de servidores en el lado de la red tanto para la verificación como para la admisión.

Microsoft define NAP como sigue: La protección del acceso de red (Network Access Protection NAP) es una plataforma que proporciona componentes para la aplicación de políticas para ayudar a asegurarse que las computadoras conectadas o a conectarse en una red cumplan con los requisitos para la salud del sistema.

Microsoft ofrece una variedad de tecnologías para el Acceso seguro a redes entras la que cuenta con:

- Microsoft Network Protection (NAP)
- 802.1X vía Microsoft
- Microsoft Network Access Quarantime Control (NAQC)

2.6.2.1 *Plataforma NAP.*

Los siguientes son los componentes de Microsoft NAP:

- NAP Agente.- Este mantiene el estado de la salud basado en estrada de las comunicaciones del SHA (sistema agente de salud) con el Enforcement Client Component (Cliente de la aplicación componentes). Este agente crea el SOH (declaraciones de la salud) basándose sobre esta información. (Nakhjir & Nakhjiri, 2002)

- System Health (SHA) agente de salud del sistema.- Este es un componente para cada tipo de requisito de salud. Por ejemplo, podía haber SHA para el antivirus y otros para las

actualizaciones del sistema operativo. (Estos son similares a los plugins de postura de NAC de Cisco)

- SHA Aplication Programming Interface (API) interfaz de programación.- Este permite que los vendedores creen e instales SHAs a medida o por encargo.

- Enforcement Client Components (EC) componentes del cliente de la aplicación.- Estas impiden el tipo de acceso a la red, pasan el estado de salud de la computadora a un punto de aplicación NAP que esté proporcionando el acceso de red, e indican el estado limitado o ilimitado del acceso de red del cliente NAP a otros componentes de la arquitectura.
- NAP EC API.- Esta permite que los vendedores creen y que instales ECs adicionales.

2.6.2.2 *Los componentes del server*

- NAP Enforcement Server servidor de la aplicación NAP(ES).- Este permite un nivel de acceso o de comunicación de red. Pasa estado de salud del cliente a un servidor de la política sanitaria y basado sobre esa regeneración, puede controlar el acceso de red. Es el punto de la aplicación para la solución NAP.

- NAP Administration Server. Servidor de Administración.- Esta obtiene el SoH del NAP es con el servicio de NPS. Distribuye el SoHs en la declaración del sistema de la salud (SSoH) al Sistem Health Validators del sistema. El Recoge la declaración de las respuestas de la salud (SoHRs) de la salud Validators del sistema y la pasa al servicio de NPS para la evacuación.

- Network Policy Servers Servidores de la Política de la red (NPS).- La respuesta en práctica de un servidor Radius y un proxy server Windows 2008. Esto proporciona la configuración de la política sanitaria y la evaluación centralizadas del estado de la salud del cliente NAP.

- System Health Validator de la salud del sistema (SHV).- Este recibe un SoH del servidor de la administración y compara la información del estado de salud del sistema en el SoH con estado requerido de la salud del sistema.

Microsoft NAP trabajará con infraestructura basada en Windows existente tal como Active Directory, Policy Group, Microsoft Systems Management Server (SMS), los servicios de actualización de Windows, y el servidor Microsoft Internet Segurity and Aceleation (ISA). (Control de Acceso a la Red, 2009)

Además, algunos componentes pueden ser proporcionados por otros vendedores. Microsoft ofrece dos APIs para que los vendedores provean la integración de sus productos.

2.6.3 Microsoft 802.1X

802.1X es una autenticación basada en el port que puede aplicarse tanto para redes alámbricas como inalámbricas, la autenticación comienza en el port de acceso y tiene dos componentes primarios:

- **Suplicante.-** Requiere el acceso a la red
- **Autenticador.-** Autentica suplicantes y decide o no darle acceso a red.

Para entender mejor 802.1X podemos hablar de ports controlados y ports no controlados. Un port controlado es aquel que nos habilita a ciertas direcciones de red. Un port no controlado nos permite un acceso irrestricto a la red.

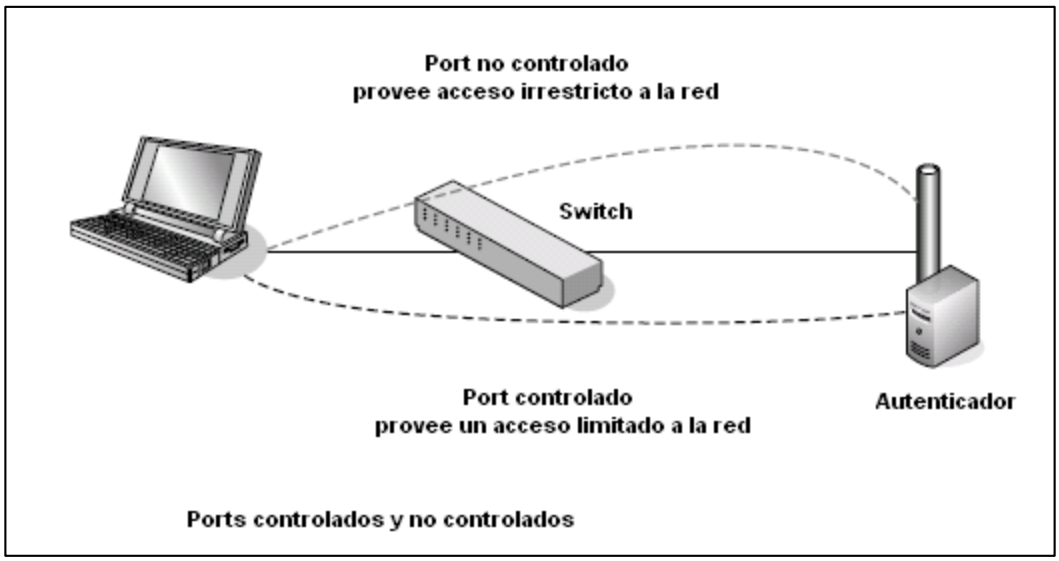

Figura 11-2: Ports Controlados

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

Teniendo todos los ports de la LAN con ports controlados el acceso a la red el dado por el Autenticador. Microsoft ofrece soluciones 802.1X desde Windows 2000, Windows Server 2003, Windows Xp y ediciones superiores.

2.6.3.1 *NAQC (Microsoft Network Access Quarantine Control)*

El control de la cuarentena del acceso de red (NAQC) es una herramienta de la inspección del acceso remoto que viene con el servidor 2003 de Windows. El propósito de esta tecnología era determinar que dispositivos pueden intentar conectividad remota a una LAN corporativa. Microsoft no quiere ninguna confusión entre NAQC y NAP.
Microsoft indica específicamente lo siguiente:
NAQC proporciona solamente protección agregada para las conexiones de acceso remoto. NAP proporciona la protección agregada para las conexiones virtuales (VPN), Configuración del protocolo de configuración de anfitrión dinámico (DHCP) y comunicaciones basadas en IPsec. (Carracedo Gallardo, 2004)

2.6.3.2 *Componentes*

- **Quarantime Compatible Remote Access Client.-** sistemas operativos que soportan esta función, tal como Windows XP, edición de Windows Millennium y superiores.
- **Remote Access Server.-** corriendo sobre el servicio Routing and Remote Access
- **Remote Access Policy.-** Corriendo sobre el Remote Access Server.

NAQC utiliza los scripts custom-written para analizar un sistema. Una vez que el script corre con éxito, la información se pasa a un componente notificador, que entonces se comunica con un servicio oyente en el servidor del acceso remoto. Si todo está bien, el servidor del acceso remoto lanza el requerimiento en la conexión. NAQC que viene con un número de componentes, incluyendo un componente del notificador rqc.exe y un servicio oyente notificador usando las herramientas del kit del recurso del servidor de Windows 2003. (Bello, 2002)

2.6.3.3 *Esfuerzos por estandarización TNC, IETF*

Las actuales tecnologías de control de accesos desaparecerán a medida que las empresas vayan adoptando sistemas de autenticación que operen en el extremo de las redes, de acuerdo con una reciente investigación de Forrester Research. Según la consultora, la complejidad y falta de interoperabilidad multimarca de estas tecnologías creará oportunidades de mercado a otros tipos de soluciones de autenticación y control de accesos más fáciles de implementar y gestionar.

Para Forrester, el mercado NAC se encuentra actualmente sumido en una gran confusión, debido en gran parte al amplio conjunto de soluciones y herramientas que engloba, que van desde sistemas de extremo a extremo sumamente complejos a aplicaciones de autenticación muchos

más simples. Esta gran diversidad se ve reflejada también en los propios suministradores activos en este negocio, cuyos perfiles van desde las típicas firmas de seguridad a los grandes fabricantes de infraestructura de red, como Cisco Systems y Juniper Networks, sin olvidar a Microsoft, que se está haciendo un hueco en este negocio. Y todos ellos siguen un enfoque NAC diferente, creando un entorno operativo y funcional heterogéneo que complica la elección de los usuarios.

Uno de los mayores problemas de los sistemas NAC actuales es que obligan a crear varias políticas para controlar los mismos procesos. En el estudio se asegura que, por ejemplo, no es infrecuente que clientes de tecnologías de acceso inalámbrico y remoto de Symantec utilicen productos Cisco para acceso de usuario local, l que da lugar a políticas dispares que impiden que el usuario disfrute de una experiencia consistente cuando intenta acceder desde la oficina o en remoto.

Así mismo, el informe mantiene que muchos de los productos NAC actuales son "meramente preventivos", limitándose a avisar a los usuarios de que sus ordenadores y dispositivos no cumplen las políticas de seguridad corporativas pero sin ofrecerles una solución efectiva para resolver el problema.

Una incapacidad que, para la consultora, representa una de las mayores carencias de estas tecnologías. Incluso la funcionalidad de puesta en "cuarentena" de los dispositivos que no cumplen las normas de seguridad un segmento de red donde quedan bloqueados los sistemas clientes hasta que logran cumplir las políticas de la empresa queda en entredicho en el estudio. Según Forrester, esto podría perjudicar la productividad de usuarios autorizados pero que son enviados a la zona de cuarentena, impidiendo asi un acceso a contenidos de su interés. Un inconveniente que favorecerá la adopción de aplicaciones NAC basadas en dispositivos o directamente en el extremo, donde residirá la inteligencia de seguridad, en lugar de en la propia red. "En muchos casos, las empresas ya disponen de la infraestructura de gestión y seguridad capaz de tratar esta función; sólo se trata de mejorar lo que ya está instalado". Esta tendencia provocará un proceso de consolidación en la industria de seguridad de extremo y de autenticación de red, puesto que los principales fabricantes tratarán de disponer de todas las piezas necesarias para crear productos que puedan trabajar de tal manera.

2.6.3.4 *TNC (Trusted Network Connect)*

TNC es una arquitectura abierta desarrollada por Trusted Computing Group. Se trata de una iniciativa que pretende ser una alternativa a las soluciones NAC propietarias, cuyo propósito

principal es posibilitar que cualquier organización pueda implementar políticas de integridad y control de acceso en todas sus redes y conexiones, además de ofrecer interoperabilidad entre los dispositivos finales de red de los distintos fabricantes. Por lo tanto, se trata de una iniciativa para ofrecer un estándar a todos los fabricantes y organizaciones que deseen acogerse a ella que les permita crear productos de control de acceso a la red compatibles unos a otros, y compatibles con las tecnologías y entronos ya existentes. Está especialmente diseñada para trabajar con el protocolo de control de acceso, autenticación y autorización 802.1X, aunque TNC no se ha limitado a este entorno y está desarrollando estándares para el resto de métodos de acceso y control como por ejemplo VPN. La meta de TNC es permitir que cualquier solución NAC/NAP pueda interactuar libremente. (CISCO, 2006)

El gran problema es conseguir el consentimiento de todos los involucrados. En Mayo de 2007 Microsoft y TCG anunciaron interoperabilidad en el evento Interop de Las Vegas. Básicamente, significa que los dispositivos que funcionan con el agente NAP de Microsoft se pueden utilizar en infraestructura de NAP y de TNC. De hecho, este agente será incluido en el sistema operativo de Microsoft en las versiones siguientes: Windows Vista, Servidor 2008 de Windows, Versiones futuras de Windows Xp.

En la lista de compañías que han anunciado compatibilidad con el estándar TNC o que tienen intención de hacerlo están:

- Microsoft
- Juniper
- Sygate
- Symantec

Por su parte Cisco lanza un programa para que terceras partes tengan interoperabilidad con su solución NAC. Hay una gran diferencia entre TNC y este programa de Cisco. Mientras TNC pretende ser un Estándar la intención de Cisco es que distintas compañías se acoplen a su solución NAC.

2.6.3.5 *IETF (Internet Engineering Task Force)*

El gran problema de las soluciones NAC hoy disponibles es la falta de estándares que las haga interoperativos. Una carencia que trata de suplir el IETF, que formó el grupo de trabajo Network Endpoint Assessment (NEA) para estandarizar los protocolos comunes de las actuales arquitecturas NAC. (Nakhjir & Nakhjiri, 2002)

Inicialmente, la prioridad está siendo la normalización de los protocolos encargados de transportar la información sobre el estado de seguridad de los sistemas que intentan acceder lo que NEA llama “posture attributes” entre los “collectors” situados en dichos clientes y los “validators” que corren en los servidores de políticas.

NEA creó un subgrupo que definió un primer borrador del documento donde se recogen la terminología propuestas, diversos escenarios de uso y un modelo de referencia que incluye los recolectores de información de estado (“posture collector”) y los “validators” de dicho estado respecto de componentes específicos de la política, como los antivirus, por ejemplo.
NEA propone estandarizar el protocolo PA (Posture Attribute), que pasa los atributos de estado del sistema cliente sobre un determinado componente de la política entre los “collectors” y los “validators”, y el protocolo PB (Posture Broker), encargado de transportar los mensajes de PA agregados de extremo a extremo. Además, estipula los requerimientos que deberían cumplir los protocolos encargados de pasar la información de estado de los mensajes PB entre el cliente NEA y el servidor NEA.

Es de resaltar que otras capacidades y protocolos que podrían afectar a la interoperatividad son obviados conscientemente de los objetivos actuales de NEA, especialmente los relacionados con la solución de problemas cuando el cliente no cumple las normas de seguridad de la empresa y el reforzamiento de políticas. Además, solo se propone estandarizar los protocolos NAC que afectan a la infraestructura, mientras que existen fabricantes que se apartan de este modelo, como por ejemplo, los que siguen el reforzamiento IPSec, que utilizan certificados de clave pública X.509. Estos certificados se obtienen de un servidor que actúa como autoridad de registro sobre el estado de seguridad y los utiliza posteriormente para establecer relaciones con otros servidores que actúan como iguales del primario.

Elegir una determinada arquitectura NAC depende de los objetivos que se persigan y de la estrategia global de seguridad de cada empresa. Si una organización se mueve en un entorno Cisco actualizado, lo mejor será adoptar la arquitectura de este fabricante, tan completa como cualquier otra. Para aquellos interesados en soluciones basadas en estándares, TNC es la única opción real, a pesar de sus riesgos. El enfoque de Microsoft, finalmente, resulta el más apropiado para rede más pequeñas donde se quiera controlar los PC de la empresa y la principal preocupación sean los virus y no tanto la autenticación y el control de accesos. (Arquitectura de protección de acceso a la Red, 2005)

2.6.4 Tecnologías con funcionalidad NAC/NAP: 802.1X, IPSec VPN y SSL VPN

Existen distintas tecnologías que componen todo el entramado de las soluciones NAC, entre las que se puede destacar la autenticación en el acceso a un punto "vivo" en la red tecnología estándar 802.1X. A pesar de ser un estándar ya consolidado que data del a2001 al contrario de lo que ocurre con la mayoría de que componen el control de acceso a la red, hay problemas con la integración con algunos sistemas operativos.

La IEE 802.1X es una norma del IEEE para el control de admisión de red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP-RFC 2284). El RFC 2284 ha sido declarado obsoleto a favor del RFC 3748.

802.1X está disponible en ciertos switches de red y puede configurarse para autenticar nodos que están equipados con un software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

Algunos proveedores están implementados 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corriendo fallas de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación sólo del cliente o más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

Windows XP y Windows Vista soporta 802.1X para todas las conexiones de red por defecto. Windows 2000 lo soporta como el último service pack. El Windows Mobile 2003 y sistemas operativos más últimos también vienen con un cliente nativo 802.1X.

Un proyecto para Linux conocido como Open1X produce a cliente abierto de la fuente. Xsupplicant. El wap_supplicant más general se puede utilizar para 802.11 en wireless y en redes cableadas. Ambos apoyan una gama muy amplia de EAP. MAC OS X ha ofrecido la ayuda nativa desde 10.3 mientras que iPhone y el iPod Touch lo soportarán en junio 2008.

Para algunas compañías, la ejecución de una verdadera solución NAC/NAP no esta en sus planes inmediatos. Al mismo tiempo pueden reconocer que los sistemas móviles plantean una amenaza

grave a su LAN y quisieran aprovecharse de una tecnología para asistir con este problema. Este es un ejemplo perfecto en donde usar tecnologías existentes tales como dispositivos VPN que pueden ayudar a agregar funcionalidad NAC. (Arquitectura de protección de acceso a la Red, 2005)

2.6.4.1 *Funcionalidad NAC en IPSec VPN*

IPsec (Protocolo de Seguridad de Internet) es un set de estándares abiertos desarrollados por el IETF. IPsec es ejecutado por un sistema de los protocolos criptográficos para asegurar tráfico IP. El marco de IPsec asegura el funcionamiento del tráfico IP en la capa 3 (capa de red) del modelo de OSI, así asegurando todos los usos de la red y las comunicaciones que utilizan la red del IP. Usando combinaciones de hashing, de llave simétrica, y de algoritmos criptográficos asimétricos, IPsec ofrece los servicios siguientes de seguridad:

- Peer Authentication Autentificación del par
- Data confidentiality Secreto de los datos
- Data integrity Integridad de datos
- Data origin Authentication Autentificación del origen de datos
- Replay detection Detección de la respuesta
- Access control Control de acceso
- Traffic flow confidentiality Secreto de circulación

2.6.4.2 *IPSec Request for Commets (RFCs)*

IPsec es un sistema de estándares abiertos que se documenta en varios RFCs. Originalmente, IPsec fue definido en una serie de RFCs 1825-1829, publicado en 1995. Mientras que la tecnología se desarrolló, éstos fueron puestos al día por más nuevas revisiones e hicieron obsoleto por RFCs 2401-2412 publicado en 1998. En 2005, una tercera generación de RFCs 4301-4309 (de 2401-2412) fue producido para incluir otros adelantos en este tema. IPsec tiene dos métodos para propagar los datos a través de una red:

Modo túnel: Protege datos en red-a-red o sitio-a-sitio Por ejemplo, la red A en el Site1 se conecta con la red B en Site2. En modo del túnel, IPsec protege datos a nombre de la otra red entidad-que es, cifra tráfico a través de los pares de IPsec. El modo del túnel encapsula y protege la carga útil

entera del paquete IP incluyendo el header original de IP y agrega un nuevo header IP. El header de IPsec se agrega según muestra el siguiente dibujo. (Carracedo Gallardo, 2004)

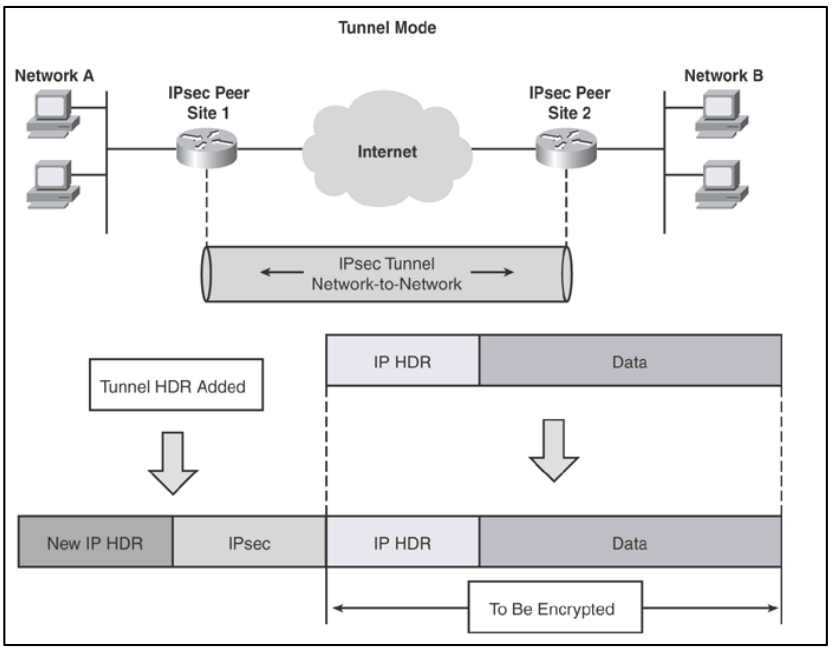

Figura 12-2: Modo Tunel

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

2.6.4.3 *IpSec modo transparente*

Protege datos en host –a-host o end to end Por ejemplo, el host A en el Site1 se conecta con el host B en Site2. En modo transparente, IPsec protege datos peer to peer., agrega un nuevo header IP entre el payload y el header original según muestra el siguiente dibujo.

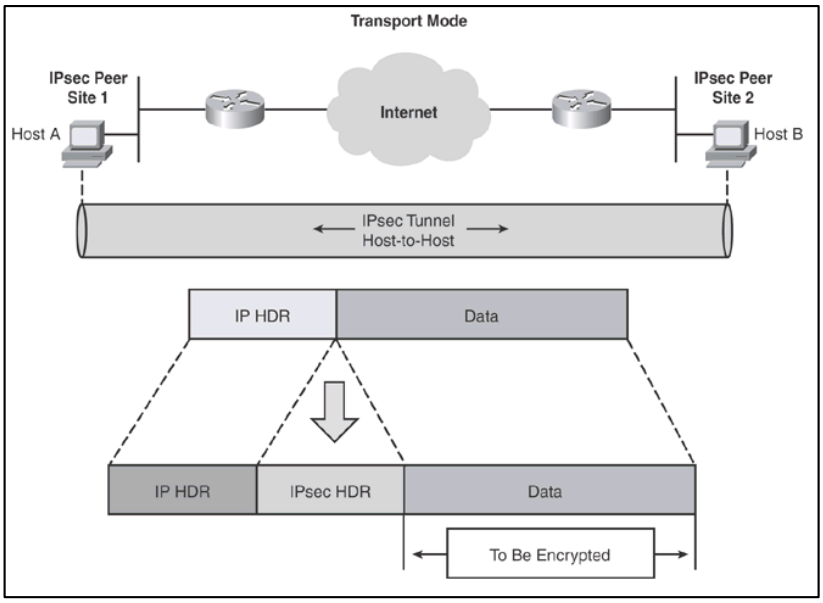

Figura 13-2: Modo de Transporte

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

Cuando los sistemas remotos intentan crear un VPN a la red corporativa con sus clientes de IPSec VPN, hay ventajas en la seguridad porque se determina el acceso para esos clientes antes de que se les permita acceso completo. Mientras que muchos dispositivos de IPSec VPN pueden realizar esta funcionalidad, centrémonos en la solución de VPN de Nortel.

Nortel introdujo la funcionalidad de Tunnel Guard (protector del túnel) a sus dispositivos de VPN. El protector del túnel es una aplicación relacionada con el cliente de IPSec VPN que comprueba si los componentes de seguridad requeridos están instalados y activos en la máquina del usuario remoto. Este chequeo ocurre mientras que el usuario intenta conectarse con el VPN

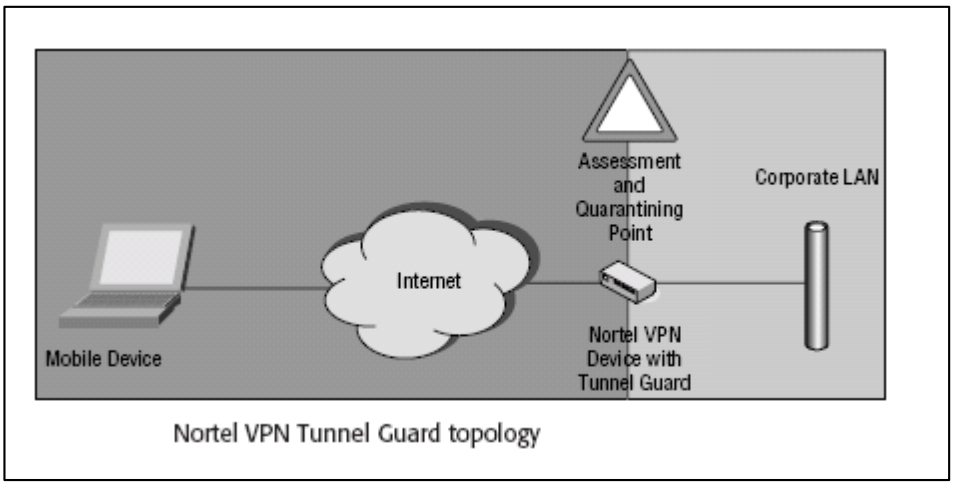

Figura 14-2: Protector de Túnel

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

El Túnel Guard debe buscar cuando el usuario se conecta las reglas predeterminadas de requisito de software (SRS). Si el dispositivo pasa estas reglas, entonces el acceso es proporcionado a la red según lo definido en su política del grupo. Si falla, su acceso puede ser limitado, o el túnel de VPN puede ser desconectado. El protector de túnel tiene en cuenta diversos elementos de seguridad para analizar en un sistema que intenta el acceso, incluyendo lo siguiente:

- Ejecutables
- archivos de .dll
- Archivos de configuración

El protector del túnel también tiene en cuenta la integración con los chequeos predefinidos de software de otros vendedores lo que le permite una fácil integración.

2.6.4.4 *Funcionalidad de NAC en SSL VPN*

Secure Sockets Layer : Protocolo de Capa de Conexión Segura- Muchos dispositivos VPN pueden actuar tanto como IPSec VPN y SSL VPN. Con SSL VPN no es necesaria la instalación de un cliente. El estándar primario en el espacio de VPN era IPSec, aunque algunos fabricantes utilizaran otros métodos, incluyendo el protocolo Layer 2 Tunneling (L2TP), y el Point-to-Point Tunneling Protocol (PPTP). SSL VPNs usa una diversa metodología de transportar datos confidenciales a través de Internet. (Carracedo Gallardo, 2004)

En vez de la confianza en el usuario final para tener un cliente configurado en una laptop de la compañía, SSL VPNs usa HTTPS que está disponible en todos los browsers Web como mecanismo de transporte seguro, sin la necesidad del software adicional. Con SSL VPN, la conexión entre el usuario móvil y el recurso interno sucede vía una conexión Web en la capa de aplicación, en comparación con el "túnel abierto" de IPSec VPNs en la capa de red.

El uso del SSL es ideal para el usuario móvil porque:

- SSL VPN no requiere software previamente instalado en el dispositivo que es utilizado para tener acceso a recursos corporativos.
- SSL VPN no necesita ser configurado en la máquina remota por un usuario o un administrador.
- SSL VPN está disponible de cualquier Web browser estándar, así que los usuarios no necesitan una laptop de la compañía.

Tabla 3-2: IPsec y SSL VPN Comparación

	IPsec VPN	**SSL VPN**
Opciones de usuarios	Habilita acceso desde desktops propias de la organización	Habilita acceso desde desktops propias de la organización, desktops de terceros desde Internet cybercafe
Métodos de acceso	Requiere usar un cliente VPN de software	Se inicializa a través de un web browser.
Requerimientos de software	Requiere preinstalar un cliente software propietario	No requiere un especial cliente de software VPN; solo es requerido un web browser
Software Updates	Puede hacer update automáticos, pero es más intrusivo y requiere la operación del usuario	No requiere software instalado; no requiere updates. El acceso es provisto por software instalado dinámicamente y el usuario no tiene que hacer updates
Configuración del acceso de los usuarios	Ofrece políticas de acceso granular pero no portables web	Ofrece políticas de acceso granular y portales web.

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

2.6.5 *Alternativas de Código Abierto*

Las comunidades NAC de código abierto aportan dos ventajas claves comunes a todas las comunidades de software libre:

a. La capacidad para encontrar fallas de seguridad rápidamente gracias al espíritu de colaboración con el que trabajan.
b. La ampliación progresiva de características y funcionalidades a medida que crece la demanda.

Existe bastante oferta de código abierto para NAC. Ciertamente el software de código abierto en general es propenso a la falta de apoyo técnico del creador, la falta de actualizaciones y la grave falta de interoperabilidad. Si uno llama a un soporte de Microsoft para recibir soporte y le dice que estaba en ejecución NAC de código abierto no obtendrá ningún tipo de soporte.

El potencial de la falta de apoyo técnico a su vez tiende a muchos usuarios de software de código abierto a invertir mucho tiempo tratando de solucionar temas de compatibilidad. (Opensource, 2012)

En la lista de proveedores de código abierto NAC se puede encontrar:

a. PacketFence Zero Effort NAC (ZEN)
b. FreeNAC
c. Netpass

2.6.5.1 *PacketFence Zero Effort NAC (ZEN)*

PacketFence es una red libre y de código abierto de control de acceso (NAC) del sistema. Esta aplicación basada en Linux principalmente proporciona un control de acceso de red, monitoreo y detección de intrusos. Te da varias funciones de protección de la red, que incluye lo siguiente:

- **Captive portal:** Se puede utilizar para solicitar a los usuarios hacer login antes de usar la red o para presentar instrucciones a un usuario en una página web, bloqueando todo el tráfico de la red, cuando se detecta un problema.
- **Detección de malware y alerta:** Además de funciones internas. PacketFence puede trabajar con sensores remotos como de Snort.
- **Escaneos de vulnerabilidades con Nessus:** Se puede utilizar el programa Nessus externo para ejecutar periódicamente análisis de vulnerabilidades.

- **El aislamiento de los dispositivos problemáticos:** Uno de los apoyos PacketFence aislamiento de varias técnicas es la VLAN aislada(VoIP), donde los clientes problemáticos serían trasladados a una VLAN designada.
- **Fingerprinting DHCP:** Se utiliza para permitir o no permitir automáticamente los tipos de dispositivos específicos (tales como VoIP o teléfonos Wi-Fi equipados)

PacketFence no es más que la última innovación entre alrededor de una docena de paquetes NAC básicos en software libre, la mayoría de ellos creados en reacción a los mismos problemas de seguridad, como los gusanos Sasser y Blaster, que empujan a las firmas comerciales a desarrollar sus soluciones. Y como sucede con el resto de software libre, precio e independencia de fabricantes son las principales razones por la que algunos usuarios se inclinan por este tipo de soluciones. (Opensource, 2012)

PacketFence es compatible con cualquier switch con soporte de SNMP, es decir prácticamente la totalidad de switches.

2.6.5.2 *FreeNAC*

Desarrollado por Swisscom, el operador dominante de Suiza. Su versión comercial incorpora algunas características no disponibles en la versión de código abierto que se pueden conseguir por una tasa de suscripción que incluye instalación y soporte.

El servicio se dirigirá inicialmente a empresas con infraestructura heterogéneas sin actualizar, como switches sin soporte de autenticación de puerto 802.1x, una exigencia de muchos productos NAC convencionales. Sin embargo, FreeNac, que, como otras herramientas de código libre, comenzó utilizando VMPS de Cisco para reforzar políticas, ahora también soporta 802.1X cubriendo así, entornos mixtos en proceso de actualización a soluciones comerciales. (Opensource, 2012)

FreeNAC proporciona fácil uso de VLANS, control de acceso de LAN para todo tipo de dispositivos de red (tales como servidores, estaciones de trabajo, impresoras, teléfonos IP, cámaras web,…) y gestión de la documentación. Permite revisión de cableado.

La solución FreeNAC desde el punto de vista de seguridad detecta los dispositivos ajenos a la red que están intentando obtener acceso a través de un conector de red Ethernet y a continuación, niega el acceso (y registra el evento).

Conocidos y registrados se habilitan a la LAN que se les atribuyen. Los visitantes (los dispositivos desconocidos), opcionalmente pueden tener acceso a una zona llamada VLAN de default/ guest VLAN. Esto puede ser útil, por ejemplo, para las organizaciones que deseen permitir acceso a los visitantes Web/VPN de acceso por Internet, pero que no tienen acceso a las redes internas.

Funcionamiento FreeNAC:

Un switch detecta una nueva PC y pide la autorización de FreeNAC que comprueba su base de datos y se niega o concede el acceso a la red basdo en la dirección MAC. FreeNAC es una versión muy mejorada de “OpenVMPS” y directamente puede sustituir a otras soluciones VMPS con importantes mejoras en la facilidad de uso.

Las principales características de FreeNAC son:

- ❖ Asignación dinámica de VLAN, es decir, se asigna VLAN basada en la dirección MAC del dispositivo, no se basa en el puerto switch, los dispositivos pueden moverse y seguir perteneciendo a la misma VLAN asignado.
- ❖ Una interfaz de usuario amigable para la gestión.
- ❖ Se puede vincular con bases de datos externas.

- ❖ Documentación de cableado y presentación de informes.
- ❖ El uso de una base de datos MySQL proporciona escalabilidad, flexibilidad, facilidad de integración y permite hacer consultas de inventario de red.

Beneficios

- ❖ No se necesita software de los dispositivos finales.
- ❖ Código abierto y extensible.
- ❖ Se ejecuta en hardware estándar y los sistemas operativos (Linux / Unix)
- ❖ Mejor utilización de los puertos de switch (eficiencia, ahorro de costes)
- ❖ Puede ser configurado por el apoyo de nivel 1 de Helpdesk.
- ❖ Cambiar la configuración más sencilla, ya que los puertos son dinámicos.
- ❖ Menor número de cambios en el cableado durante reorganizaciones.

La arquitectura FreeNAC se compone de un servidor con la base de datos master y programas de control.

Opcionalmente, uno o varios servidores esclavos para la redundancia y distribución de la carga.

2.6.5.3 *NetPass*

NetPass es un proveedor neutral de entorno de red para poner en cuarentena a los clientes que se considere que de conformidad con su política de red.

NetPass funciona mediante la asignación de puertos de cliente en una de las dos VLANS. El valor predeterminado es el puerto para estar en la cuarentena estado VLAN. En este estado, todo el tráfico desde el cliente se dirige hacia el servidor de validación NetPass.

La intercepta el tráfico VPN web, realiza comprobaciones de cumplimiento, facilita la autocorrección y mueve el puerto del cliente para la el estado unquarantiden una vez que el cumplimiento está asegurado. (Opensource, 2012)

La Auto-recuperación se logra mediante la correlación de fallas específicas de cumplimiento con la documentación sobre la forma de llevar el equipo cliente en el cumplimiento. Una vez que los pasos son seguidos, el cumplimiento se comprobará de nuevo.

NetPass está diseñado para ofrecer una identificación modular. Cualquier parte de su infraestructura existente puede ser usado para activar una cuarentena de un cliente. Por ejemplo, su servidor de correo podría detectar un cliente en particular el envío de correo electrónico cargado de virus, una señal segura de que el cliente esta infectado. Ese mismo servidor de correo

puede instruir a las VPN en cuarentena al cliente. Como parte de la transacción, el servidor de correo le diría a los VPN por la que el cliente en cuarentena. Esta información se utiliza para ayudar al cliente en el proceso de auto-corrección.

NetPass incluye la comprobación del cumplimiento de módulos para Snort y Nessus además de una API para integrar otros sistemas de identificación. NetPass también incluye una interfaz web para fines administrativos que le permite manualmente hosts cuarentena cuando sea necesario.

NetPass está diseñado para ser flexible y ofrece varias opciones de implementación lo que le permite decidir cómo riguroso quieres estar en la identificación de cuando poner en cuarentena un puerto.

2.6.5.4 *¿Qué es y para qué sirve GNS3?*

GNS3 es un simulador gráfico para el diseño de topología de red complejas es de uso libre básicamente para la interconexión en lo que permisible a un entorno real sin la implementación de Hardware que puede ser costoso la adquisición de estos equipos.

El simulador permite instalar router por medio de IOS (Sistema Operativo para redes), para ser configurados útil para la realización de prácticas con equipos ciertamente apegados a la realidad, al igual que permite añadir dispositivos, crear topologías, en general para habituarse al funcionamiento el GNS3 con equipos Cisco, incluso a sus errores habituales. (Microsoft, 2005, https://msdn.microsoft.com/es-es/library/cc778605%28v=ws.10%29.aspx).

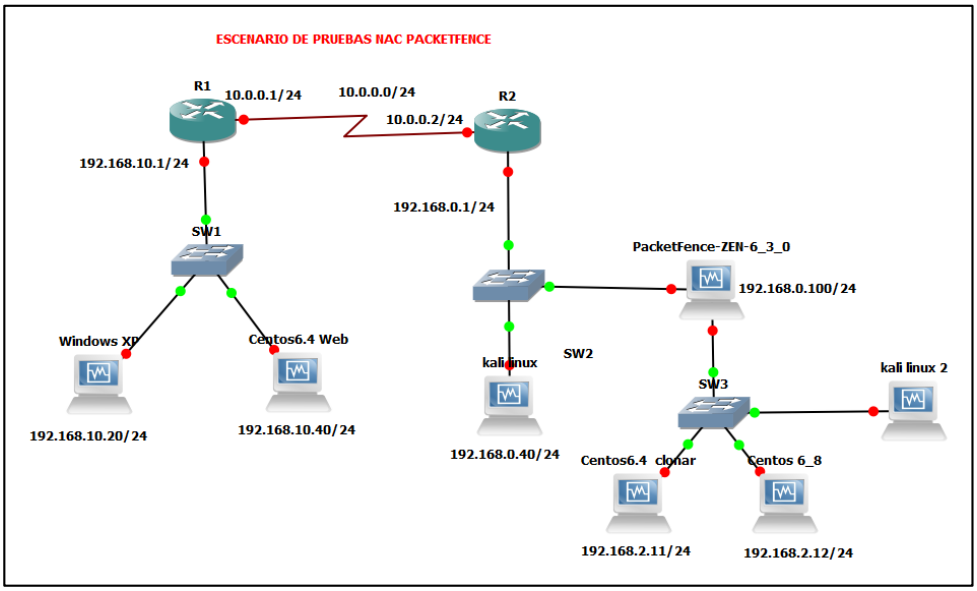

Figura 15-2: Topología GNS3

Realizado: Julio Flores

Esta herramienta se puede descargar directamente de la red, los enlaces para descargas son variados, sitios de entrenamiento que colaboran con diferentes IOS para la creación de topologías.

2.6.5.5 Ataque DDos

Un ataque DoS o DDoS (depende de cómo se lleve a cabo) no es más que un número exageradamente elevado de peticiones a una dirección IP. Tal es así que el servidor es incapaz de gestionar dichas peticiones causando un error en el sistema y la detención o reinicio del servicio, dejando este inaccesible al resto de usuarios.

Se refiere a un servidor, ya que dependiendo del objetivo del ataque y de la intensidad del mismo, podríamos hablar de inhabilitar un servicio.

La diferencia entre un ataque DoS (Denial of Service o Denegación de Servicio) y un ataque DDoS (Distributed Denial of Service o Denegación de Servicio Distribuido) la encontramos en los significados de sus anagramas.

En el primero nos encontramos con un atacante que cuenta con un único equipo, mientras que para el ataque distribuido se usarán múltiples máquinas simultáneamente. Por lo general todas pertenecerán a redes de equipos controlados por un único atacante.

Los ataques DDoS, no todos tienen por qué tener un atacante tras ellos, se puede dar perfectamente cuando hemos estructurado un servicio para albergar 100 usuarios simultáneos y se incrementa el volumen de tráfico hacia este equipo queriendo acceder al mismo 200 usuarios.

Un claro ejemplo es cuando una pequeña academia crea una plataforma de formación online con un presupuesto ajustado, eligiendo un servidor económico, sin tener en cuenta el volumen máximo de usuarios que gestionará dicho servidor. Si esta academia comienza a vender cursos sin establecer un límite, se puede dar tal cantidad de usuarios queriendo acceder al aula virtual que generarán inconscientemente un DDoS.

2.7 Estudio comparativo de control de acceso a la red NAC parámetros

La tabla 4-2 se realiza un cuadro comparativo de los soluciones de acceso a la red, con licencia NAC de Cisco y NAP de Microsoft y sin licencia Open Source FreeNAC y PacketFence

Tabla 4-2: Estudio comparativo de control de acceso a la red NAC parámetros

PARAMETROS		**SOLUCIONES PROPIETARIO**		**SOLUCIONES OPEN SOURCE**	
		CISCO NAC	**MICROSOFT NAP**	**FREENAC**	**PACKETFENSE**
REQUERIMIENTO DEL NEGOCIO PARA EL CONTROL DE ACCES	**Política de control de acceso**	Cisco Clean Manager para crear políticas de seguridad y gestionar los usuarios conectados, puede hacer la función de servidor de autenticación Proxy hacia los servidores de autenticación del back end. Este dispositivo gestiona y se comunica con el servidor Cisco Clean Access que es el dispositivo que se encarga de permitir o no el acceso desde la red	Servidor de políticas NAP para evaluar el estado de salud de los clientes de esta manera permitir o no el acceso SHVs viene incorporado dentro de las políticas de red, y determina la acción a tomar basándose en el estado de salud del equipo que se conecta	Son políticas definidas por la Institución una de ellas sería que mientras un usuario no este registrado en la base de datos no puede tener acceso a la red.	Se debe cumplir una política de uso aceptable, los usuarios no pueden habilitar el acceso a la red, sin antes haberse autenticado

GESTIÓN DE ACCESO AL USUARIO	**Registro de usuario**	Servidor de Directorio. Un servidor de directorio centralizado para registro de usuario y / o autenticación. Los servicios de directorio posibles son: LightweightDirectory Access Protocol**(LDAP),** Microsoft ActiveDirectory (AD), Novell DirectoryServices (NDS), y por una sola vez servidores de tokens OTP (contraseña).	Active directory	Freenac permite realizar un registro de usuarios en la base de datos mysql.	Packetfence permite un registro de usuario y un registro de dispositivos conectados a la red, tanto un registro de archivos planos como un registro de usuarios en la base de datos OpenLdap, para dicho registro se ha creado una aplicación amigable para ingresar los datos de los usuarios, así como sus respectivas contraseñas
	Gestión de privilegios	Servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como EAP sobre 802.1X	WSv Protege a las VM del sistema operativo host y viceversa, al permitir que las VM se ejecuten en una cuenta de servicio sólo con los privilegios necesarios	Permite determinar privilegios el momento de crear los usuarios.	Todos los usuarios que tenga los privilegios para acceder a la red serán registrados en OpenLdap, usuario que no esté registrado no podrá acceder a la red, a los usuarios se les asigna el privilegio como Administrador o invitado
	Gestión de claves secretas de los usuarios	Cisco TrustSec ofrece controles de acceso a la red basados en una política uniforme para los usuarios (incluidos empleados, contratistas o usuarios temporales), los dispositivos terminales (equipos portátiles, teléfonos IP, impresoras) y los dispositivos de	Mediante la herramienta IPsec está implementado por un conjunto de protocolos criptográficos para asegurar el flujo de paquetes, garantizar la autenticación mutua y establecer parámetros criptográficos	El momento de crear los usuarios se utiliza mecanismos criptográficos de autenticación como peap. Eap.	Se registrará un usuario y una contraseña, dichos usuarios serán almacenados en OpenLdap, donde las contraseñas de cada uno de los usuarios serán almacenas de manera segura, es decir cifradas-

		red (switches, routers, etc.). Cisco TrustSec es capaz de controlar el modo en que se le otorga acceso a un usuario o dispositivo, las políticas de seguridad que deben cumplir los dispositivos terminales, como el cumplimiento de una postura, y los recursos de red que un usuario está autorizado a usar dentro de la red			
	Revisión de los derechos de acceso del usuarios	Cisco TrustSec protege el acceso a la red y los recursos, así sea una red cableada, inalámbrica o VPN, y se asegura de que los dispositivos terminales tengan autorización y se mantengan en buen estado	NPS como un servidor RADIUS para procesar solicitudes de conexión, así como para realizar la autenticación, la autorización y la administración de cuentas para conexiones inalámbricas 802.11	Freenac emite informes detallados de los usuarios que acceden a la red	Para la revisión de los derechos de acceso de los usuarios al intentar conectarse a la red se revisará en la base de datos que el usuario suplicante está registrado, caso contrario el usuario no puede ingresar a la red
RESPONSABILIDADES DEL USUARIO	**Uso de claves secretas**	Servidor de directorios	Active directory Combinación de Kerberos, LDAP, Samba NIS(YP) and NIS+ para autenticar usuarios en la red	Se debería concientizar a los clientes sobre el uso de las claves secretar su importancia etc.	Se debe recomendar a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas, sin embargo al ingresar los usuarios a la base de datos las contraseñas están validadas para que las mismas cumplan con un cierto grado de seguridad.

	Equipo de usuario **desatendido**	No cumple	No cumple	No cumple	Una vez que el usuario se autentique, si este deja a su equipo desatendido por un lapso
	Política de escritorio y pantallas limpios	No cumple	No cumple	No cumple	No cumple
CONTROL DE ACCESO A LA RED	**Políticas sobre el uso de los servicios de red**	Configuración en los servidores de políticas, de puntos de decisión y de Auditoria	NPS permite crear y aplicar políticas de acceso a la red para toda la organización referidas al estado de salud de los equipos clientes, y los requisitos de autenticación y autorización para la conexión. Se usan políticas (orientada a objetos), con funciones pre y post conexión. Con Freenac se Establecen una fecha de validez para cada dirección MAC	Los usuarios deberían basarse en las políticas de control de acceso	Los usuarios deberán cumplir con la política de acceso a la red, es decir todos los usuarios necesitan autenticarse.
	Autenticación del usuario	Cisco dispone de un servidor de	Switches con autenticación basada en protocolo 802.1x	No cumple	

	para las conexiones externas	autenticación propio denominado Cisco Security Access que soporta tanto RADIUS como TACACS	NPS para habilitar el proceso de autenticación segura de passwords con protocolo PEAP Protected Extensible AuthenticationProtocol (PEAP)-MS-CHAP v2 para conexiones inalámbricas servicio Routing and Remote Access Service (RRAS) disponen de los servicios de enrutamiento para red de área local (LAN) y redes de área extensa (WAN) utilizados para conectar segmentos de red en entornos de conexión remota o infraestruturas de redes de oficina certificados X.509		
	Identificación del equipo en las redes	Servidor de autorización autenticación y auditoria Servidor de control de acceso	SHVs (SystemHealthValidators) para analizar el estado de salud del equipoSHAServidor de cumplimiento NAP	El momento que una maquina accede se registra la dirección MAC de la maquina por tanto se tiene un registro de acceso a la red	Todos los equipos una vez autenticados serán identificados por su dirección MAC
	Protección del puerto de diagnostico y configuración remota	Basado en una autenticación	Secure Sockets Layer (SSL) 802.1X podemos hablar de ports controlados y ports no controlados. Un port controlado es aquel que nos habilita a ciertas direcciones de red.	No cumple	No cumple

			Un port no controlado nos permite un acceso irrestricto a la red.		
	Segregación de redes	No cumple	Se puede crear bosques mediante el active directory Un bosque de Active Directory tiene el esquema ampliado con las extensiones de esquema del Administrador de configuración, y se dotará de un contenedor de administración del sistema en al menos un dominio.	Permite crear vlan.	PacketFence es el servidor que asigna la VLAN a un dispositivo. Esta VLAN puede ser una de sus VLAN o puede ser una VLAN especial donde PacketFence actúa como un servidor DHCP / DNS / HTTP en el que se ejecuta el portal cautivo. Vlans, permiten crear redes lógicamente independientes dentro de una misma red física lo que permiten una administración de la red separando segmentos lógicos de una red de área local
	Control de conexión a la red	Una vez detectado el nuevo dispositivo el NAD (dispositivo de acceso a la red) habilita una conexión entre el Servidor AAA, el servidor de autorización autenticación y auditoria y el access control server ACS o server de control de acceso, una vez establecida la conexión con el	Permitir el acceso a la red Permitir el acceso a la red por tiempo limitado Permitir el acceso limitado Si un servidor que ejecuta NPS es miembro de un dominio de Active Directory®, NPS usa el servicio de directorio como su base de datos de cuentas de usuario y forma parte de una solución de inicio de sesión		PacketFence es completamente compatible, confiable de código abierto, sistema de control de acceso(a la red NAC), basados en la norma 802.1x que permiten la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o

		Server AAA se requiere las credenciales para la respectiva conexión	único. El mismo conjunto de credenciales se usa para controlar de acceso a la red (autenticación y autorización del acceso a una red) y para iniciar sesión en un dominio de Active Directory. Debido a esto, se recomienda usar NPS con los Servicios de dominio de Active Directory (AD DS)		previniendo el acceso por ese puerto si la autenticación falla
	Control de enrutamiento a la red	No cumple	No cumple	No cumple	No cumple
CONTROL DE ACCESO AL SISTEMA OPERATIVO	Procedimiento para un registro seguro		WSv Protege a las VM del sistema operativo host y viceversa, al permitir que las VM se ejecuten en una cuenta de servicio sólo con los privilegios necesarios	No cumple	
	Identificación y autenticación del usuario	Los servicios de directorio posibles son: LightweightDirectory Access Protocol**(LDAP),** Microsoft ActiveDirectory (AD), Novell DirectoryServices (NDS), usando servidor RADIUS comprueba que la información es correcta utilizando esquemas de	Active directory NPS como un servidor RADIUS para procesar la autenticación, la autorización y la administración de cuentas inalámbricas, alambricas, VPN	Se realiza la autenticación por medio de protocolo de autenticación 802.1x	Todos los usuarios tendrán un identificador único, para poder ingresar a la red, es decir cada usuario tendrá que autenticarse antes de ingresar a la red

		autenticación como EAP sobre 802.1X R			
	Sistema de gestión de contraseñas	Configuración dentro del servidor de control de acceso, políticas de control de acceso	Active directory	Las contraseñas al momento de ser almacenadas en OpenLdap serán validadas para que las mismas sean de calidad, es decir cumplan con ciertas condiciones de seguridad, además dichas contraseñas serán almacenadas en	formatos protegidos(encriptación)
	Uso de las utilidades del sistema	Servidor de Control de Acceso usando servidores Radius			
	Cierre de una sesión por inactividad				
	Limitación del tiempo de conexión				Packetfence permite limitar los tiempos de conexión, es decir asignar un tiempo específico para su conexión.
CONTROL DE ACCESO A	**Restricción de acceso a la información**		Trafico protegido mediante (IPsec) Secure Sockets Layer (SSL)		

	Aislar el sistema confidencial				
	Trabajo remoto	El papel de NAC Appliance 4.0 de Cisco Systems responde al acceso a la red en todos los segmentos de la misma de una empresa: alámbricos, inalámbricos y conexiones remotas			

Fuente: http://postgrado.info.unlp.edu.ar/Especializaciones/Redes_y_Seguridad/Esmoris.pdf

CAPITULO III

3. MARCO METODOLÓGICO

3.1 Diseño de la investigación

La investigación utilizará un diseño de la investigación cuasi experimental que consiste en determinar la seguridad de PacketFence en una red corporativa en base a los siguientes indicadores Autenticación, Integridad, Disponibilidad, para de esta forma verificar la validez o el rechazo de la hipótesis de estudio lo que permitió determinar si las soluciones del control de acceso a la red (NAC) mejoran la seguridad externa e interna de redes corporativas.

3.2 Tipo de la investigación

Este trabajo investigativo será de tipo descriptiva y aplicada, lo cual permitirá determinar los efectos de seguridad de PacketFence en el ambiente de simulación propuesto.

3.3 *Métodos*

Los métodos a utilizarse en la investigación son los siguientes:

3.3.1 *Deductivo*

El método deductivo parte de premisas generales a concluir en consideraciones particulares o específicas para una investigación, que para el estudio de la seguridad de acceso a la red. se fundamenta en los beneficios de la tecnología NAC para mejorar la seguridad interna y externa de las redes corporativas.

3.3.2 *Inductivo*

La seguridad interna y externa de las redes corporativas, se desarrolla a través de políticas internas que son adoptadas de acuerdo a las necesidades de las empresas pudiendo ser éstas de software libre o con licenciamiento de una forma particular, es decir iniciando de forma individual para

luego generalizarlo ya que al implementar las NACs como estrategia de seguridad favorecerá el control interno y externo dentro de la red.

3.3.3 *Analítico*

Durante el desarrollo de la investigación se analizarán las políticas de seguridad de la NAC a través de un estudio comparativo en ambientes de simulación con el uso de PacketFence y sin él.

3.4 Técnicas e instrumentos de recolección de datos

Se utilizan para la recolección de información las siguientes técnicas que se detallan a continuación:

- Observación
- Revisión y estudio de Documentación
- Recopilación de información
- Análisis comparativo

3.5 Validación de instrumentos

Para la validación de instrumentos se tomará en cuenta las siguientes herramientas:
Se plantea la elaboración del ambiente de simulación de una red corporativa en el simulador gráfico de redes (GNS3) para equipos CISCO, este es un software gráfico para el diseño de redes y topologías complejas y poner en marcha simulaciones sobre ellos. Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.
- Dynagen, un front – end basado en texto para Dynamips
- Quemu y VirtualBox, para permitir utilizar máquinas virtuales como un firewall PIX
- VPCS, un emulador de PC con funciones básicas de networking
- IOU (IOS on Unix), compilaciones especiales de IOS provistas por Cisco para correr directamente en sistemas UNIX y derivados

GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes de Cisco o las personas que quieren pasar sus CCNA, CCNP, CCIE DAC o certificaciones.

Se utilizara la herramienta VirtualBox excelente programa que sirve para virtualizar y que más que un programa se lo considera una herramienta, porque con VirtualBox podemos virtualizar hasta Servidores, Sistemas de monitoreo, se considera que es excelente, además que la compatibilidad no solo está con Windows podemos encontrar el VirtualBox en Linux. VirtualBox tiene otra gran ventaja la cual es que tiene licencia GPL (General Public Licence) lo cual nos indica que es libre podemos descargarlo sin ningún costo adicional, distribuirlo con los que queramos y sin tener claves de compra, además de eso VirtualBox tiene la gran ventaja de que los desarrolladores sacan una nueva versión cada cierto tiempo el cual es un periodo de tiempo corto, tener una aplicación, estable, útil, libre y fácil de usar

Los sistemas operativos a utilizar son CentOS 6.8 utilizado para levantar el servicio web, al igual que los clientes para la validación y pruebas de seguridad. El software que se utiliza para la seguridad de las NAC es el PacketFence versión 6.3.0 es un aplicación de tipo OpenSource PacketFence es una solución NAC basada en código abierto y gratuito. Esta solución nos ofrece un conjunto de características como por ejemplo un portal cautivo en donde los usuarios se autentificaran para su debido registro.

Para las pruebas de seguridad se utilizó Kali Linux 2.0 ya que está orientado a pruebas de penetración profesional y auditorías de seguridad. El tiempo estimado para cada ataque es de una hora.

Para la realización de los ataques se ha utilizado las herramientas:

MACCHANGER, el objetivo de esta herramienta es cambiar el hardware original de la tarjeta de red por una dirección de MAC falsa.

AIREPLAY-NG, **s**irve para crear y/o inyectar tráfico dentro de una red inalámbrica. De por sí sirve para realizar varios ataques rápidos y simples como la desautentificación o la falsa autentificación.

MACOF se utilizó para inundar una red local con direcciones MAC, el objetivo es interrumpir su flujo regular de datos entre sus puertos lo que permite pasar los datos por todas las tarjetas de red excepto a la que estaba destinada.

Para realizar ataques de Integridad se utilizaron herramientas como:

SQLMAP es una herramienta de pruebas de penetración de código abierto que automatiza el proceso de detectar y explotar los errores de inyección SQL y toma de carga de los servidores de bases de datos. Viene con un potente motor de detección, muchas características de nicho para el probador de penetración máxima y una amplia gama de interruptores que duran de toma de huellas dactilares de base de datos, ir a buscar a través de datos de la base de datos, para acceder al sistema

de archivos subyacente y ejecutar comandos en el sistema operativo a través de fuera conexiones de banda.

SQLSUS es una herramienta de pruebas de penetración de código abierto que automatiza el proceso de detectar y explotar los errores de inyección SQL,

SQLNINJA, el objetivo principal es conseguir acceso interactivo a nivel de sistema operativo en el servidor remoto DB y para utilizarlo como un punto de apoyo en la red de destino. Como una característica experimental, también se puede explotar las vulnerabilidades de inyección SQL en aplicaciones web.

Para realizar ataques de Disponibilidad es utilizaron las siguientes herramientas:
METASPLOIT es una suite o conjunto de programas. Está diseñada para explotar las vulnerabilidades de los equipos y es sin duda el programa más usado por los mejores hackers del mundo. Dentro de MetaSploit, disponemos de multitud de herramientas y programas para ejecutar en las diferentes vulnerabilidades de cada equipo, a cada una de estas aplicaciones se le llama sploit.

HPING3, hping es una línea de comandos orientado TCP / ensamblador de paquetes IP / analizador. La interfaz está inspirada en el ping, pero hping no sólo es capaz de enviar peticiones de eco ICMP. Soporta TCP, UDP, ICMP y protocolos RAW-IP, tiene un modo traceroute, la posibilidad de enviar archivos entre un canal cubierto, y muchas otras características.
PING OF DEATH Por norma general una petición ping tiene un tamaño de 32 bytes (incluida la cabecera) y los servidores no tienen ningún problema para gestionar las peticiones y enviar la respuesta correspondiente legítimas. Con el conocido como “Ping de la muerte” (Ping of Death o PoD), lo que hacemos es enviar paquetes mediante ping, pero con un tamaño mucho mayor y a mayor frecuencia de lo normal.

Dada los requerimientos para la simulación de la red, creación de los varios clientes fue necesario contar con un equipo robusto en características de Hardware para que soporte estas exigencias así tenemos un equipo con procesador corei7 con una memoria RAM de 12GB con un disco duro de 1TB.

3.6 Población y Muestra

3.6.1 *Población*

La población es el conjunto de todos los elementos que pueden ser evaluados, en la presente investigación resulta no muy adecuado tomar en cuenta las soluciones propietarias sea de hardware o de software ya que se trata de averiguar las posibles falencias de la tecnología NAC. Tomando en cuenta esto se definirá un aspecto para su desarrollo:

- Vulnerabilidades Existentes

Vulnerabilidades Existentes.

En el presente apartado, se describirán los modos de ataques que podrían ocurrir más frecuentemente en las redes de información que son: Autenticación, Integridad y Disponibilidad, mismos que al ser quebrantados generan vulnerabilidades (a la que se asocia un ataque), ya que son apropiados y convenientes para los fines de esta investigación. Esta población se seleccionó basándose en los documentos de la NIST (Nacional Institute of Estándar and Tecnology) con respecto a la seguridad en redes.

3.6.2 *Muestra*

En vista de que la población involucrada en el proyecto de investigación, es pequeña, se considera para la muestra a toda la población para la presente investigación es decir 180 ataques realizados a la red simulada con PacketFence y sin PacketFence, distribuidos en 60 ataques para la autenticación, 60 para integridad, 60 para disponibilidad que son los suficientes y necesarios al vulnerar un principio de seguridad, basados en los documentos de la ARCERT(Coordinación de Emergencia en Redes Teleinformáticas).

Tabla 1-3: Muestra de Vulnerabilidades

Principios	**Ataques**
Autenticación	MACCHANGER, AIRCRACK, MAOF
Integridad	SQLMAP, SQLSUS, SQLNINJA
Disponibilidad	METASPOLIT, HPING3, PING OF DEATH

Realizado por: Julio Flores.

3.7 Planteamiento de la hipótesis

La implementación de tecnología NAC permitirá mejorar la seguridad externa e interna de las redes corporativas.

3.8 Determinación de las variables

Las variables de estudio se detallan a continuación

- **Variable Independiente:** Tecnología NAC
- **Variable Dependiente:** Seguridad externa e interna de las redes corporativas

3.9 Operacionalización de variables

- Operacionalización Conceptual

En la siguiente tabla 2-3: esta la definición conceptual de las variables Independiente, Dependiente utilizadas en esta investigación.

Tabla 2-3: Operacionalización Conceptual

VARIABLE	TIPO	DEFINICIÓN
Tecnología NAC	Independiente	Para qué sirve la tecnología NAC
Seguridad	Dependiente	Seguridad de un portal cautivo

Realizado por: Julio Flores.

- Operacionalización Metodológica

En la tabla 2-3; se detalla a continuación los indicadores que se utilizarán para la validación de la hipótesis.

- Autenticación: Es un procedimiento que permite asegurar que un usuario en un sitio web es auténtico o es quien dice ser.
- Integridad: Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no solo la que esta almacenada directamente en los sistemas de cómputo sino también se deben considerar elementos menos obvios como respaldo, documentación, tránsitos en una red, esto comprende cualquier tipo de modificaciones:

- Causadas por errores de hardware y/o software
- Causadas de forma intencional
- Causadas de forma accidental

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados.

- Disponibilidad: De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por lo tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

Tabla 3-3: Operacionalización Metodológica

HIPÓTESIS	**VARIABLES**	**INDICADORES**	**INSTRUMENTOS**
La implementación de la tecnología NAC permitirá mejorar la seguridad externa e interna de las redes corporativas.	**V. Independiente** Tecnología NAC	Trafico HTTP	- Manuales técnicos - PacketFence - GNS3
	V. Dependiente Seguridad	- Autenticación - Integridad - Disponibilidad	- ClonarMAC, AIRCRACK,CBC-MAC - SQLMAP, SSCANNER SQL-NINJA - METASPLOIT, HPING3, PING OF DEAD

Realizado por: Julio Flores.

3.10 Escenarios para las pruebas

El escenario planteado para la investigación con software libre PacketFence para la implementación de la tecnología NAC en GNS3 se muestra en la figura 1-3.

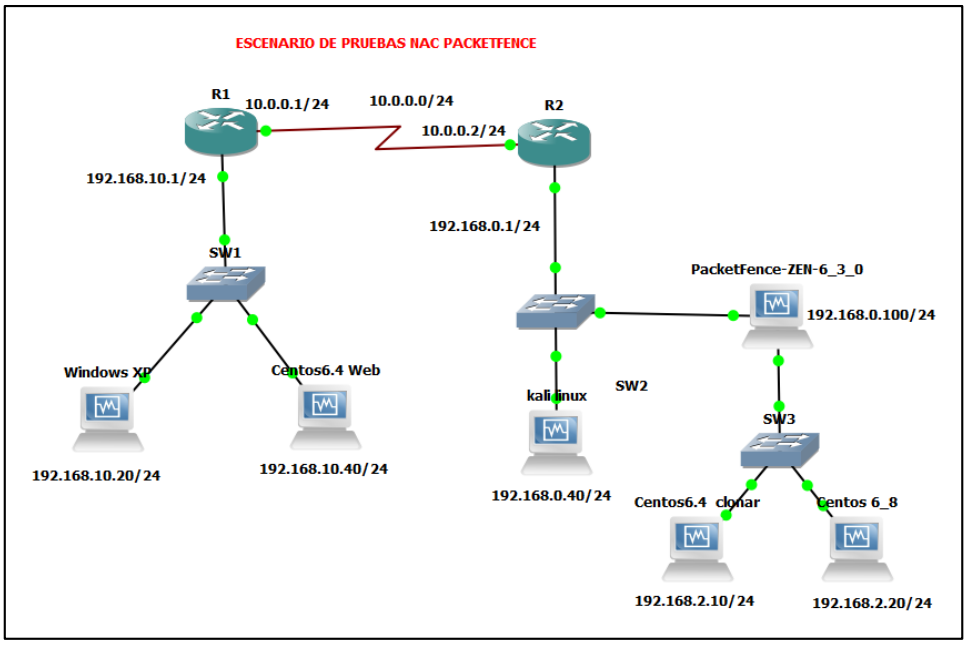

Figura 1-3: Escenario de conexión de red

Realizado por: Julio Flores

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Análisis y procesamiento de la información

En esta investigación se plantea el uso del PacketFence con medida de seguridad para el establecimiento de la comunicación utilizando portal cautivo el escenario planteado de la simulación con GNS3 para equipos Cisco utilizados en la interconectividad de la red y el PacketFence levantado sobre CentOS permitiendo la salida de las maquinas a un servidor web.

La seguridad se analiza en base al control de acceso a la red (NAC), al igual que se realizará pruebas con el ataque al servidor de PacketFence probando su repudio al no tener acceso ya que esta herramienta cuenta con un descriptor gráfico que identificará si existe o no ataques de vulnerabilidad.

4.2 Análisis y presentación de resultados variable dependiente

En cuanto a la variable dependiente, se toma en cuenta el ambiente de pruebas en el escenario planteado, indicando que la categoría siempre que representa el 100% indica que se pudo hacer el ataque y que la categoría nunca que representa el 0% indica que nunca se pudo realizar el ataque, las otras categorías estarán en función del tiempo que se demora en realizar el ataque. Para la cuantificación de los indicadores se utilizó un valor que se muestra la siguiente tabla 1-4 de la Escala Cualitativa de cuantificación de indicadores.

Tabla 1-4: Escala cualitativa de cuantificación de indicadores variable dependiente

CATEGORIA	ABREVIATURA	VALORACIÓN	PORCENTAJE
Siempre	S	4	100 %
Casi siempre	CS	3	75 %
A Veces	AV	2	50 %
Pocas veces	PV	1	25 %
Nunca	N	0	0 %

Fuente: Adaptada de la Guía de Autoevaluación con fines de acreditación. CONEA (2005: 41).

4.2.1 Indicador 1: Autenticación

Tabla 2-4: Autenticación

PacketFence				Sin PacketFence		
N° Ataques	**MACCHANGER**	**AIRCRACK**	**MACOF**	**MACCHANGER**	**AIRCRACK**	**MACOF**
1	0	0	0	3	4	4
2	0	0	0	3	4	4
3	0	0	0	3	4	4
4	0	0	0	3	4	4
5	0	0	0	3	4	4
6	0	0	0	3	4	4
7	0	0	0	3	4	4
8	0	0	0	3	4	4
9	0	1	1	3	4	4
10	0	0	0	3	4	4

Realizado Por: Julio Flores.

Tabla 3-4: Porcentaje del Promedio de Interacciones de la Autenticación

	PacketFence			**Sin PacketFence**		
	MACCHANGER	**AIRCRACK**	**MACOF**	**MACCHANGER**	**AIRCRACK**	**MACOF**
PI (Promedio Interacciones)	0	0,1	0,1	3	4	4
TOTAL	4	4	4	4	4	4
PORCENTAJE	0%	3%	3%	75%	100%	100%

Realizado Por: Julio Flores.

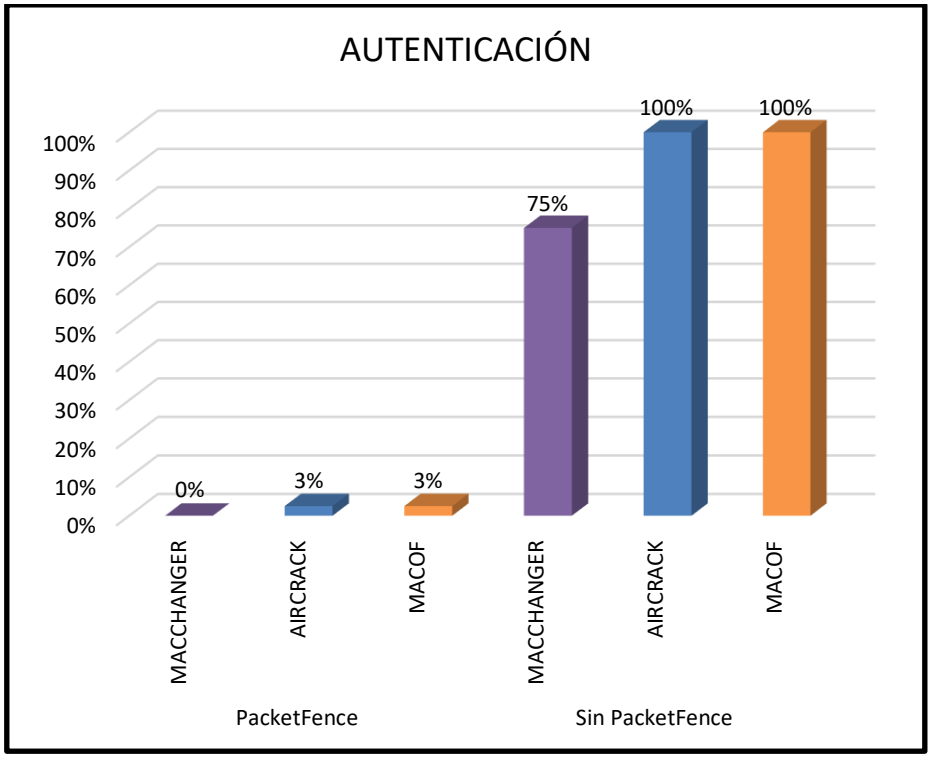

Gráfico 1-4: Autenticación

Realizado por: Julio Flores

En la tabla 2-4 se presenta los resultados de los ataques realizados con MACCHANGER, AIRCRACK Y MACOF en el escenario propuesto con la herramienta PacketFence y sin la herramienta PacketFence, se puede observar que los ataques realizados con MACCHANGER a la herramienta PacketFence tomaron valores de cero que representa el 0% en los 10 ataques, que indica que no se pudieron realizar dichas vulnerabilidades; con AIRCRACK tomaron valores de cero y en pocos casos tomaron el valor de 1 que representa el 3% tomando como referencia el tiempo que demoró más del intervalo predefinido en realizar dicho ataque (la demora se debe a la virtualización de la red con respecto al hardware de la máquina anfitrión); con MACOF tomaron valores de cero y en pocos casos tomaron el valor de 1 que representa el 3% de la misma manera tomando como referencia el tiempo que demoró más del intervalo predefinido en realizar dicho ataque.

Cuando se realizaron ataques sin la herramienta PacketFence, se puede observar que los ataques realizados con MACCHANGER tomaron valores de 3 en los 10 ataques que representa el 75% que indica que se pudieron efectuar dichas vulnerabilidades; con AIRCRACK tomaron valores de 4 que representa el 100% de vulnerabilidad y con MACOF tomaron valores de 4 que representa el 100% de vulnerabilidad, es decir, siempre se pudo atacar.

En la tabla 3-4 se presenta los resultados de los porcentajes de interacción de los 10 ataques realizados, el total representa el valor de 4 esperado con respecto al promedio de las herramientas evaluadas.

En el gráfico 1-4 se puede evidenciar que con la herramienta de ataque MACCHANGER en PacketFence representa un 0% que no puede ser vulnerado frente a un 75% de vulnerabilidad sin la herramienta PacketFence; con AIRCRACK en PacketFence representa un 3% que no puede ser vulnerado frente a un 100% de vulnerabilidad sin la herramienta PacketFence y con MACOF en PacketFence representa un 3% que no puede ser vulnerado frente a un 100% de vulnerabilidad sin la herramienta PacketFence, esto en cuanto al indicador Autenticación.

4.2.2 Indicador 2: Integridad

Tabla 4-4: Integridad

	PacketFence			Sin PacketFence		
N° Ataques	**SQL MAP**	**SQLSUS**	**SQL NINJA**	**SQL MAP**	**SQLSUS**	**SQL NINJA**
1	0	0	0	4	4	4
2	0	0	0	4	4	4
3	0	0	0	4	4	4
4	0	0	0	4	4	4
5	0	0	0	4	3	4
6	0	0	0	4	3	4
7	0	0	0	4	4	3
8	0	0	0	4	4	4
9	0	0	0	3	4	3
10	0	0	0	3	3	3

Realizado Por: Julio Flores.

Tabla 5-4: Porcentaje del Promedio de Interacciones de la Integridad

	PacketFence			Sin PacketFence		
	SQL MAP	**SQLSUS**	**SQL NINJA**	**SQL MAP**	**SQLSUS**	**SQL NINJA**
PI (Promedio Interacciones)	0	0	0	3,8	3,7	3,7
TOTAL	4	4	4	4	4	4
PORCENTAJE	0%	0%	0%	95%	93%	93%

Realizado Por: Julio Flores.

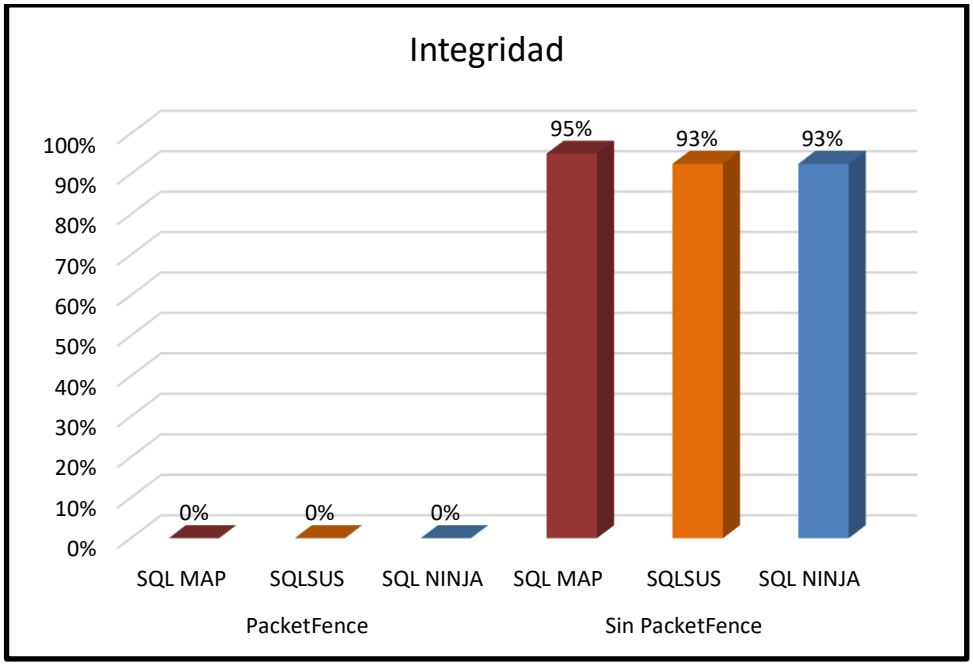

Gráfico 2-4: Integridad

Realizado por: Julio Flores

En la tabla 3-4 se presenta los resultados de los ataques realizados con SQL MAP, SQLSUS y SQL NINJA en el escenario propuesto con la herramienta PacketFence y sin la herramienta PacketFence, se puede observar que los ataques realizados con SQL MAP a la herramienta PacketFence tomaron valores de cero que representa el 0% en los 10 ataques esto nos indica que no se pudieron realizar dichas vulnerabilidades; con SQL SUS tomaron valores de cero que representa el 0% en los 10 ataques tomando esto indica que no se pudieron realizar dichas vulnerabilidades; con SQL NINJA tomaron valores de cero que representa el 0% en los 10 ataques indicando que no se pudo atacar a la herramienta PacketFence.

Cuando se realizaron ataques sin la herramienta PacketFence, se puede observar que los ataques realizados con SQL MAP tomaron valores de 4 y de 3 que indica que siempre y casi siempre se pudo atacar a la herramienta PacketFence en los 10 ataques que representa el 95% de vulnerabilidad; con SQL SUS tomaron valores de 4 y de 3 que indica que siempre y casi siempre se pudo atacar a la herramienta PacketFence en los 10 ataques que representa el 93% de vulnerabilidad Y CON SQL NINJA tomaron valores de 4 y de 3 que indica que siempre y casi siempre se pudo atacar a la herramienta PacketFence en los 10 ataques que representa el 93% de vulnerabilidad es decir, siempre se pudo atacar, tomando como referencia el tiempo en que se demoró en realizar el ataque.

En la tabla 5-4 se presenta los resultados de los porcentajes de interacción de los 10 ataques realizados, el total representa el valor de 4 esperado con respecto al promedio de las herramientas evaluadas.

En el gráfico 2-4 se puede evidenciar que con la herramienta de ataque SQL MAP en PacketFence representa un 0% que no puede ser vulnerado frente a un 95% de vulnerabilidad sin la herramienta PacketFence; con SQL SUS en PacketFence representa un 0% que no puede ser vulnerado frente a un 93% de vulnerabilidad sin la herramienta PacketFence y con SQL NINJA en PacketFence representa un 0% que no puede ser vulnerado frente a un 100% de vulnerabilidad sin la herramienta PacketFence, se evidencia que con PacketFence la Integración de los datos no es vulnerada, es decir, toman valores de 0%, en cambio que sin PacketFence los valores de porcentaje son altos indicando que existe un 94% de vulnerabilidad.

4.2.3 Indicador 3: Disponibilidad

Tabla 6-4: Disponibilidad

	PacketFence			Sin PacketFence		
N° Ataques	**METASPLOIT**	**HPING 3**	**PING OF DEATH**	**METAEXPLOIT**	**HPING 3**	**PING OF DEATH**
1	0	0	0	4	4	4
2	0	0	0	4	4	3
3	0	0	0	4	4	3
4	0	0	0	3	4	3
5	0	0	0	3	4	3
6	1	0	0	3	4	3
7	1	0	0	4	4	3
8	0	0	0	3	4	3
9	0	0	0	3	4	3
10	0	0	0	3	4	3

Realizado Por: Julio Flores.

Tabla 7-4: Porcentaje del Promedio de Interacciones de la Disponibilidad

	PacketFence			Sin PacketFence		
	METASPLOIT	HPING 3	PING OF DEATH	METAEXPLOIT	HPING 3	PING OF DEATH
PI (Pormedio Interacciones)	0,2	0	0	3,4	4	3,1
TOTAL	4	4	4	4	4	4
PORCENTAJE	5%	0%	0%	85%	100%	78%

Realizado Por: Julio Flores.

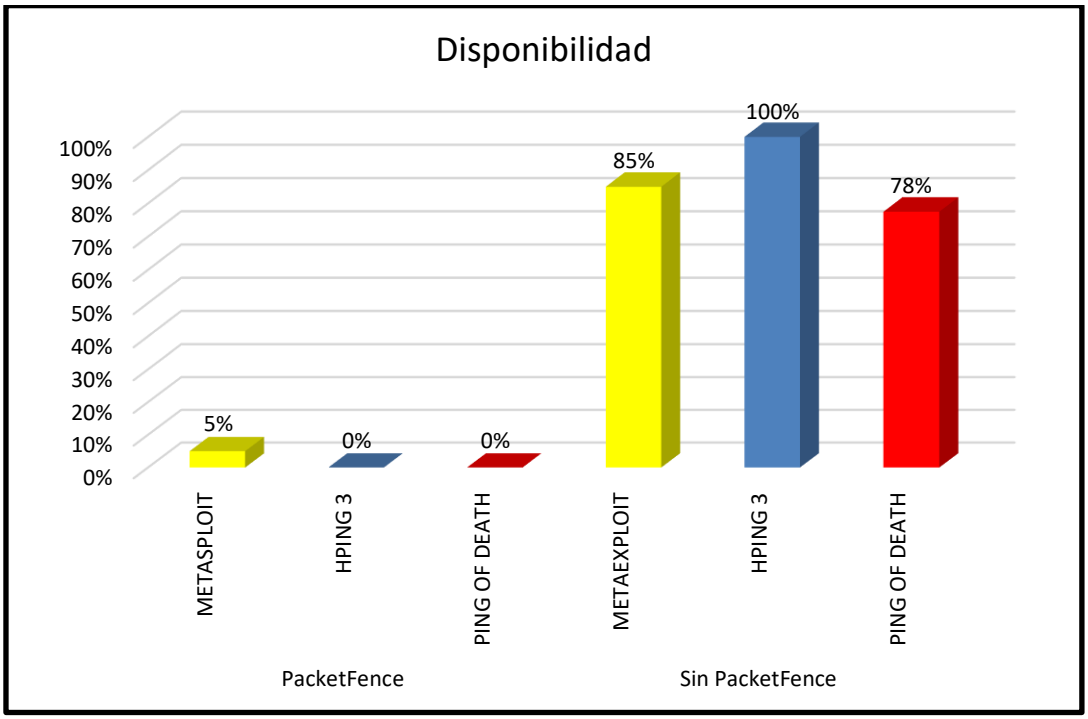

Gráfico 3-4: Disponibilidad

Realizado por: Julio Flores

En la tabla 6-4 se presenta los resultados de los ataques realizados con METASPLOIT, HPING3 y PING OF DEATH en el escenario propuesto con la herramienta PacketFence y sin la herramienta PacketFence, se puede observar que los ataques realizados con METASPLOIT a la herramienta PacketFence tomaron valores de 0 y en algunos casos valores de 1 que representa el 5% en los 10 ataques esto nos indica que el nivel de vulnerabilidad es bajo; con HPING3 tomaron valores de cero que representa el 0% en los 10 ataques esto indica que no se pudieron realizar dichas vulnerabilidades; con PING OF DEATH tomaron valores de cero que representa el 0% en los 10 ataques indicando que no se pudo atacar a la herramienta PacketFence.

Cuando se realizaron ataques sin la herramienta PacketFence, se puede observar que los ataques realizados con METASPLOIT tomaron valores de 4 y de 3 que indica que siempre y casi siempre se pudo atacar a la herramienta PacketFence en los 10 ataques que representa el 85% de vulnerabilidad; con HPING 3 tomaron valores de 4 que indica que siempre se pudo atacar a la herramienta PacketFence en los 10 ataques que representa el 100% de vulnerabilidad y con PING OF DEATH tomaron valores de 4 y de 3 que indica que siempre y casi siempre se pudo atacar a la herramienta PacketFence en los 10 ataques que representa el 78% de vulnerabilidad es decir, casi siempre se pudo atacar, tomando como referencia el tiempo en que se demoró en realizar el ataque.

En la tabla 5-4 se presenta los resultados de los porcentajes de interacción de los 10 ataques realizados, el total representa el valor de 4 esperado con respecto al promedio de las herramientas evaluadas.

En el gráfico 3-4 se puede evidenciar que con la herramienta de ataque METASPLOIT en PacketFence representa un 5% que no puede ser vulnerado frente a un 85% de vulnerabilidad sin la herramienta PacketFence; con HPING 3 en PacketFence representa un 0% que no puede ser vulnerado frente a un 100% de vulnerabilidad sin la herramienta PacketFence y con PING OF DEATH en PacketFence representa un 0% que no puede ser vulnerado frente a un 78% de vulnerabilidad sin la herramienta PacketFence, se evidencia que la Disponibilidad de servicios de la herramienta PacketFence no es vulnerada, es decir, toman valores de 0 y del 5 %, que indica que nunca se cayeron los servicios, en cambio que sin la herramienta PacketFence los valores de porcentaje son altos indicando que existe un 100 % de vulnerabilidad, llegando a la conclusión que la disponibilidad de los servicios permanecen estables con la herramienta PacketFence.

4.3 Resultados Generales

Tabla 8-4: Análisis General de los Ataques

	PacketFence			**Sin PacketFence**		
INDICADORES	**Ataque 1**	**Ataque 2**	**Ataque 3**	**Ataque 1**	**Ataque 2**	**Ataque 3**
Autenticación	0	0,1	0,1	3	4	4
Integridad	0	0	0	3,8	3,7	3,7
Disponibilidad	0,2	0	0	3,4	4	3,1
P.I.	0,07	0,03	0,03	3,4	3,9	3,6
TOTAL	4	4	4	4	4	4
PORCENTAJE	**2%**	**1%**	**1%**	**85%**	**98%**	**90%**

Realizado Por: Julio Flores.

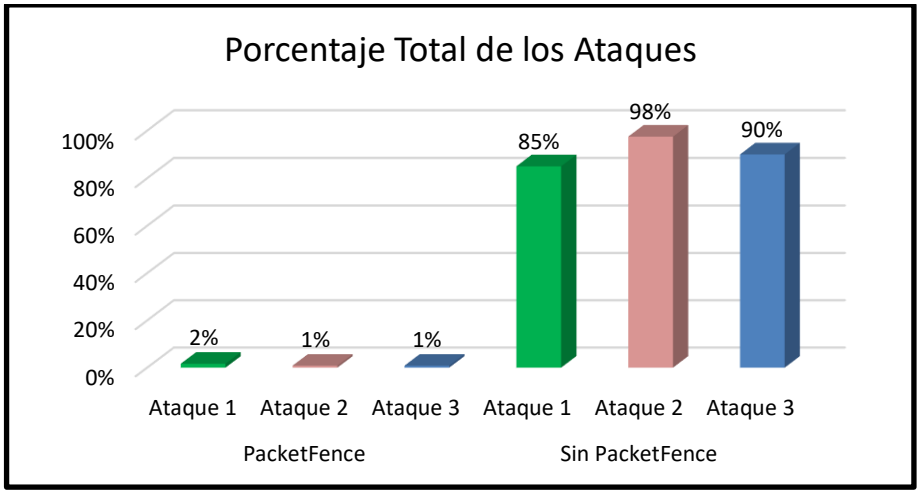

Gráfico 4-4: Porcentaje Total de los Ataques

Realizado por: Julio Flores

En la tabla 8-4 se presenta los resultados totales de los ataques realizados a nuestro escenario con PacketFence y sin PacketFence en referencia a los indicadores de estudio que es la Autenticación, Integridad y Disponibilidad, se puede evidenciar que, el Promedio de Interacciones del Ataque 1con PacketFence obtuvo un porcentaje del 2% de vulnerabilidad frente al 85% sin PacketFence; el Ataque 2 con PacketFence obtuvo un porcentaje del 1% de vulnerabilidad frente al 98% sin PacketFence y el Ataque 3 con PacketFence obtuvo un porcentaje de 1% de vulnerabilidad frente al 90 % sin PacketFence. Los resultados obtenidos demuestran que la red protegida con PacketFence presenta niveles de seguridad del 98.67%, mientras que, sin la herramienta demostró ser del 9%.

4.4 Valorización de los Resultados.

En la tabla 9-4 se realiza el respectivo análisis sobre los ataques realizados en nuestro escenario de prueba, con PacketFence y sin PacketFence.

Tabla 9-4: Análisis General de los ataques

		TECNOLOGIA NAC									
		PacketFence					Sin PacketFence				
Indicador	**INDICES**	**0**	**1**	**2**	**3**	**4**	**0**	**1**	**2**	**3**	**4**
Autenticación	**Clonar MAC**	x								x	
	AIRCRACK		X								X
	CBC-MAC		X								X
Integridad	**SQL MAP**	x							X		
	OSSCANNER	x									X
	SQL NINJA	x								x	
Disponibilidad	**METAEXPLOIT**		X							x	
	HPING3	x									X
	PING OF DEATH	x								x	
	TOTAL	**6**	**3**	**0**	**0**	**0**	**0**	**0**	**1**	**4**	**4**

Realizado por: Julio Flores

Para la valorización veamos un ejemplo: Si la tecnología NAC ha obtenido una calificación de 1 en la escala de 0 al 4, este valor equivale al 25%, y si el estándar tuviera una ponderación de 3, éste representaría el 100%, entonces necesitamos saber cuánto representa el 25% de 3; es decir; 0.75, entonces se realizaría así:

PacketFence

Ponderización	3
Valor en la escala	1 = 25%
Valor numérico	25% de 3 = 0.75

Además se debe indicar que para representar el acceso seguro se considera los siguientes aspectos que se describe en la tabla 10 – 4

Tabla 10-4: Consideraciones Acceso Seguro

CATEGORIA	VALORACIÓN	DESCRIPCIÓN	ABREVIATURA
Nunca	0	Acceso Seguro Alto	ASA
Pocas Veces	1		
A Veces	2	Acceso Seguro Moderado	ASM
Casi Siempre	3	Acceso Seguro Bajo	ASB
Siempre	4		

Realizado por: Julio Flores

En la Tabla 11 – 4 se realizó los respectivos cálculos de la valorización de nuestra variable dependiente aplicando las consideraciones de Acceso Seguro.

Tabla 11-4: Consideraciones Acceso Seguro

PacketFence					Sin PacketFence				
0	**1**	**2**	**3**	**4**	**0**	**1**	**2**	**3**	**4**
6	3	0	0	0	0	0	1	4	4
0	0.75	0	0	0	0	0	1	3	4
0.75		0	0		0		1	7	
ASA		**ASM**	**ASB**		**ASA**		**ASM**	**ASB**	

Realizado por: Julio Flores

4.5 Prueba de la Hipótesis.

Las hipótesis científicas son sometidas a prueba para acordar si son apoyadas o refutadas de acuerdo con lo que el investigador observa, no podemos probar que una hipótesis sea verdadera o falsa sino argumentar que fue apoyada o no de acuerdo con ciertos datos obtenidos en la investigación

Por consiguiente no existe un método que nos permita saber con precisión que una desviación es el resultado propio del azar, sin embargo hay pruebas estadísticas que admiten determinar algunos límites de confianza. Una de estas es la prueba del Chi – cuadrado (X^2) que permite calcular la probabilidad de obtener resultados que únicamente por efecto del azar se desvíen de las expectativas en la magnitud observada si una solución a un problema es correcta.

El establecimiento de las hipótesis nula y alternativa es el inicio de la comprobación de la hipótesis del trabajo de investigación. La hipótesis nula se denota como Ho, y constituye lo que queremos desacreditar; mientras que la hipótesis alternativa es una afirmación de la característica investigada, su símbolo es Hi.

Con lo anteriormente mencionado las hipótesis son:

Ho (Hipótesis Nula): Mediante la implementación de políticas NAC no mejorará la seguridad de las redes corporativas.

Hi (Hipótesis Alternativa): Mediante la implementación de políticas NAC si mejorará la seguridad de las redes corporativas.

Nivel de significación:

$$\alpha = 0.05$$

Criterio

$$\text{Rechace la } H_0 \text{ si } X_C^2 \geq X_t^2$$

X_C^2 = chi cuadrado calculado

X_t^2 = chi cuadrado de la tabla

En la Tabla 12 – 4 es la tabla de contingencia de lo observado

Tabla 12-4: Tabla de contingencia de lo Observado

INDICES	PACKECTFENCE	SIN PACKETFENCE	Total
Acceso Seguro Alto	0,75	0	0,75
Acceso Seguro Mediano	0	1	1
Acceso Seguro Bajo	0	7	7
Total	0,75	8	8,75

Realizado por: Julio Flores

La frecuencia esperada de cada celda, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas.

$$f_e = \frac{(total\ fila)(total\ columnas)}{N}$$

Donde N es el número total de frecuencias observadas.

Para la primera celda la frecuencia esperada sería:

$$f_e = \frac{(0,75)(0,75)}{8,75} = 0,064285714$$

En la Tabla 13 – 4 es la tabla de frecuencias de lo esperado

Tabla 13-4: Tabla de contingencia de lo Esperado

INDICES	PACKECTFENCE	SIN PACKETFENCE	Total
Acceso Seguro Alto	0,064285714	0,685714286	0,75
Acceso Seguro Mediano	0,085714286	0,914285714	1
Acceso Seguro Bajo	0,6	6,4	7
Total	0,75	8	8,75

Realizado por: Julio Flores

En base a la tabla de lo esperado y de lo observado obtenemos la tabla de Chi – Cuadrado (X_C^2) con la siguiente fórmula:

$$X_C^2 = \Sigma \frac{(O-E)^2}{E}$$

Donde:

O = el número observado

E = el número esperado, y

Σ = es la sumatoria de todos los valores posibles de $(O - E)^2 / E$

Obteniendo el resultado $X_C^2 = 0{,}846724399$

Determinar los grados de libertad que se obtiene del número de filas y el número de columna de la tabla de contingencia.

Donde:	En nuestro caso:
k = número de filas	k = 3
j = número de columnas	j = 4
v = (k-1)(j-1)=grados libertad	v=(3-1)(4-1)=6 grado de libertad

Decisión

Como $X_C^2 = 0{,}846724399$ cae en el área de rechazo de H_0, se rechaza la hipótesis nula y se acepta H_1, es decir la Hipótesis de Investigación como se demuestra en el Gráfico 5 – 4

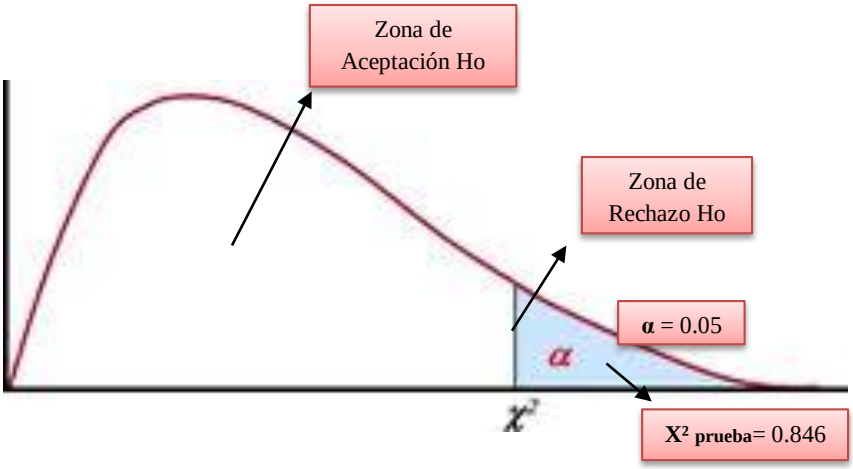

Gráfico 5-4: Gráfico de Aceptación / Rechazo H_0

Realizado por: Julio Flores

CAPITULO V

5. Propuesta de Guía de implementación de la tecnología NAC para la seguridad externa e interna de las redes corporativas

5.1. Descripción de la Infraestructura de la Solución NAC

La seguridad es una parte integral de la implementación de cada red en estos días, ante la necesidad de tener redes bien seguras y confiables, toda empresa debe implementar servicios de seguridad diseñados dentro de la red. La mayoría de las redes están conectadas a Internet y expuestas a amenazas de virus y ataques, las empresas deben tomar medidas para proteger su infraestructura de red, los datos de los usuarios y la información sobre los clientes.

La herramienta PacketFence será quien actué como servidor permite realizar una autenticación, es decir se podrá acceder a la red siempre y cuando sea un usuario autorizado, este usuario estará registrado con sus datos y su contraseña, las mismas que serán almacenadas en una base datos MySQL, en el servidor PacketFence se registra la dirección MAC la hora de conexión de cada usuario que desee acceder a la red.

5.2. Análisis de Requisitos de Hardware y Software

5.2.1. Análisis de requerimientos de Hardware

Para la implementación del PacketFence se recomienda un servidor robusto con las siguientes características:

- Servidor HPE ProLiant ML150 Gen9
- Procesador Intel® Xeon® E5-2600 v4
- Memoria RAM 512 GB
- Controlador de almacenamiento RAID (SATA 6Gb/s / SAS 12Gb/s)
- 2 tarjetas de red

5.2.2. Análisis de requerimientos de Software

- CentOS 6x de 64 bits
- PacketFence v5.0.0
- DHCP Server
- DNS Server

- Servidor de Base de Datos Mysql
- Web Server Apache

5.3. Análisis de Impacto

El análisis de soluciones de acceso a la red, permite indagar sobre la utilidad de una herramienta de software libre que realiza el control de acceso para ser implementada en una red corporativa, con el fin de restringir los accesos, identificar a los usuarios, registrar horas y tiempos de conexión, asignar los privilegios, la herramienta que se utiliza es PacketFence.

PacketFence ofrece el control de acceso a la red, protege la red, información que se almacena contra amenazas que pueden representar los usuarios y los dispositivos que acceden a ella. La tecnología NAC realiza tres funciones principales:

- Verificación de identidades con la autenticación de usuarios y equipos.
- Los computadores, equipos son evaluados para acceder a la red asegurándose que estén libres de virus y cumplan los criterios de seguridad configurados en el PacketFence.
- Autorización de acceso a la información, con la imposición de políticas para impedir el acceso no autorizado a otros datos.

La herramienta PacketFence protege datos corporativos mediante la restricción o el control del acceso no autorizado a la red. Verifica que se cumplan los requisitos mediante el control del acceso a datos y la posterior entrega de informes integrales sobre la actividad del usuario.

5.4. Optimizaciones.

PacketFence controla el libre acceso a la red, incluye un portal cautivo para el registro y la gestión centralizada por cable o por red inalámbrica, este permite el aislamiento de capa 2 (Enlace de Datos) de dispositivos problemáticos, la integración con IDS (Sistema de Detección de Intrusos), escáneres de vulnerabilidad y los servidores de seguridad; PacketFence se puede utilizar para asegurar de manera eficaz las redes, desde pequeñas a grandes redes corporativas.

De acuerdo al análisis de los ataques realizados a nuestro escenario PacketFence con el Indicador *Autenticación* la herramienta de ataque MACCHANGER representa un 0% que no puede ser vulnerado frente a un 75% de vulnerabilidad sin la herramienta PacketFence; con AIRCRACK en PacketFence representa un 3% que no puede ser vulnerado frente a un 100% de vulnerabilidad sin la herramienta PacketFence y con MACOF en PacketFence representa un 3% que no puede ser vulnerado frente a un 100% de vulnerabilidad sin la herramienta PacketFence.

Con el Indicador *Integridad* se puede evidenciar que con la herramienta de ataque SQL MAP en PacketFence representa un 0% que no puede ser vulnerado frente a un 95% de vulnerabilidad sin la herramienta PacketFence; con SQL SUS en PacketFence representa un 0% que no puede ser vulnerado frente a un 93% de vulnerabilidad sin la herramienta PacketFence y con SQL NINJA en PacketFence representa un 0% que no puede ser vulnerado frente a un 100% de vulnerabilidad sin la herramienta PacketFence, se evidencia que con PacketFence la Integración de los datos no es vulnerada, es decir, toman valores de 0%, en cambio que sin PacketFence los valores de porcentaje son altos indicando que existe un 94% de vulnerabilidad.

Con el Indicador *Disponibilidad* se puede evidenciar que con la herramienta de ataque METASPLOIT en PacketFence representa un 5% que no puede ser vulnerado frente a un 85% de vulnerabilidad sin la herramienta PacketFence; con HPING 3 en PacketFence representa un 0% que no puede ser vulnerado frente a un 100% de vulnerabilidad sin la herramienta PacketFence y con PING OF DEATH en PacketFence representa un 0% que no puede ser vulnerado frente a un 78% de vulnerabilidad sin la herramienta PacketFence, se evidencia que la Disponibilidad de servicios de la herramienta PacketFence no es vulnerada, es decir, toman valores de 0 y del 5 %, que indica que nunca se cayeron los servicios, en cambio que sin la herramienta PacketFence los valores de porcentaje son altos indicando que existe un 100 % de vulnerabilidad, llegando a la conclusión que la disponibilidad de los servicios permanecen estables con la herramienta PacketFence.

5.5. Sistemas de Integración

PacketFence utiliza muchos componentes en una infraestructura. Por tanto se requiere los siguientes:

- Base de Datos del Servidor (MySQL): PacketFence registra los usuarios al igual que los administradores en su base datos, esto hace referencia a la autenticación e integridad de datos de los usuarios como condición previa para el acceso a la red. Como se identifica en la figura 1-5, se registrar el usuario administrador con su respectiva contraseña, Y en la figura 2-5 se demuestra el registro de los usuarios clientes.

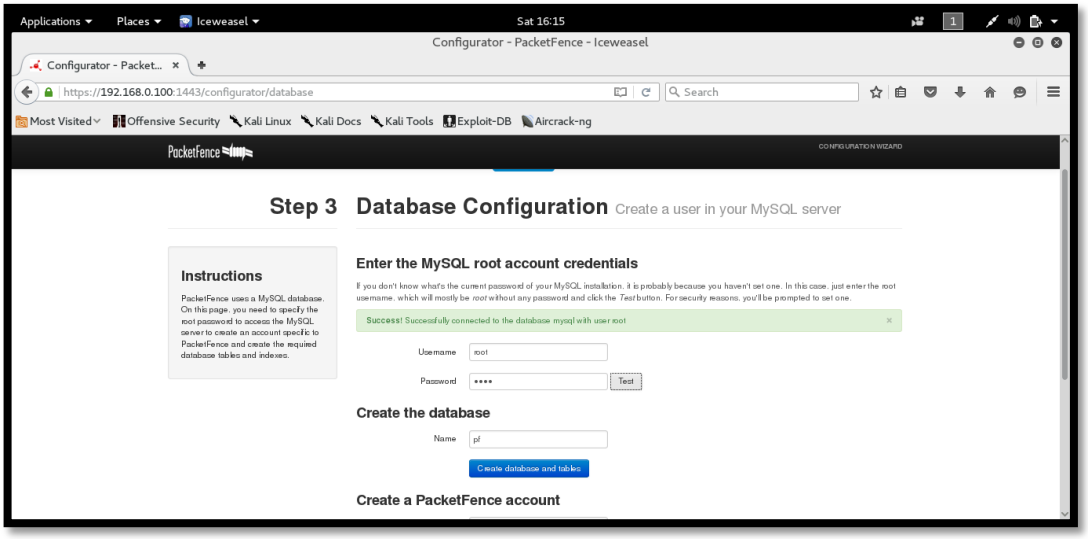

Figura 1-5: Configuración del Administrador

Realizado por: Julio Flores

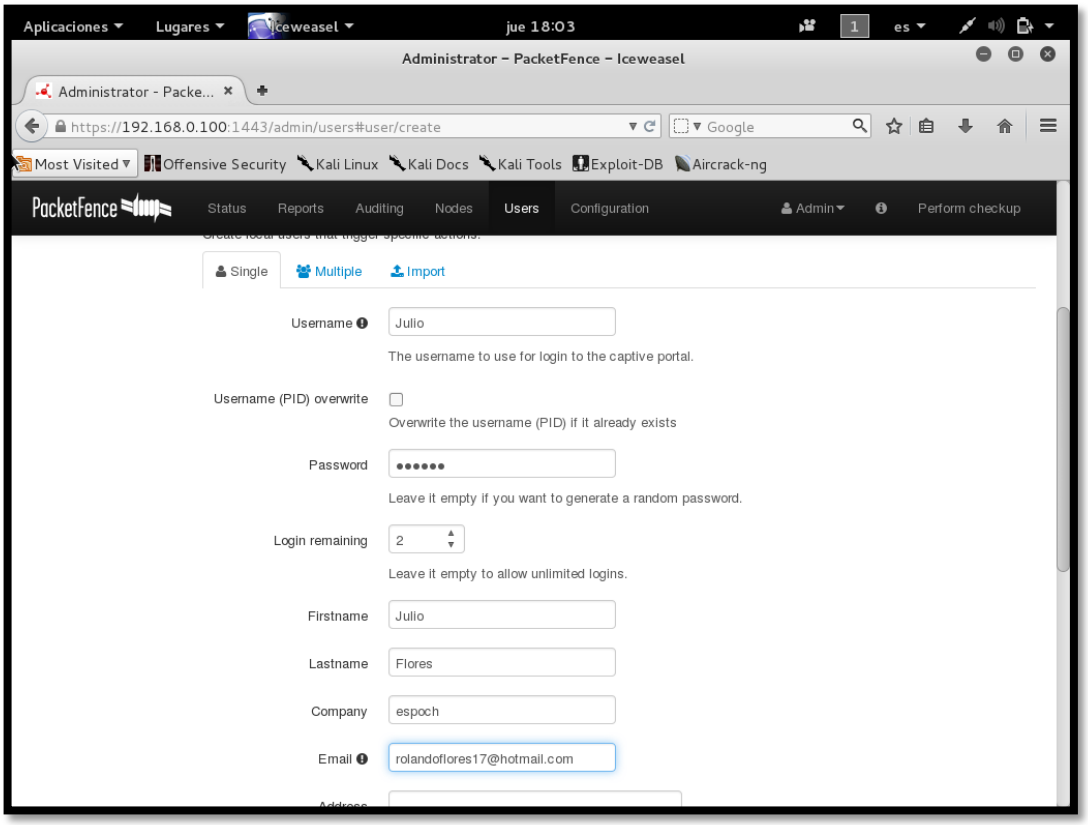

Figura 2-5: Configuración de Usuarios

Realizado por: Julio Flores

- Servidor Web (Apache): PacketFence utilizará el dominio y el nombre de su host para crear la URL para redirigir dispositivos en el portal cautivo. Si tiene un certificado HTTP puede utilizar el nombre de host y nombre de dominio para validar la conexión en el portal cautivo,

en cualquiera de los dos casos a esto lo denominamos disponibilidad. Como se muestra en la figura 3-5

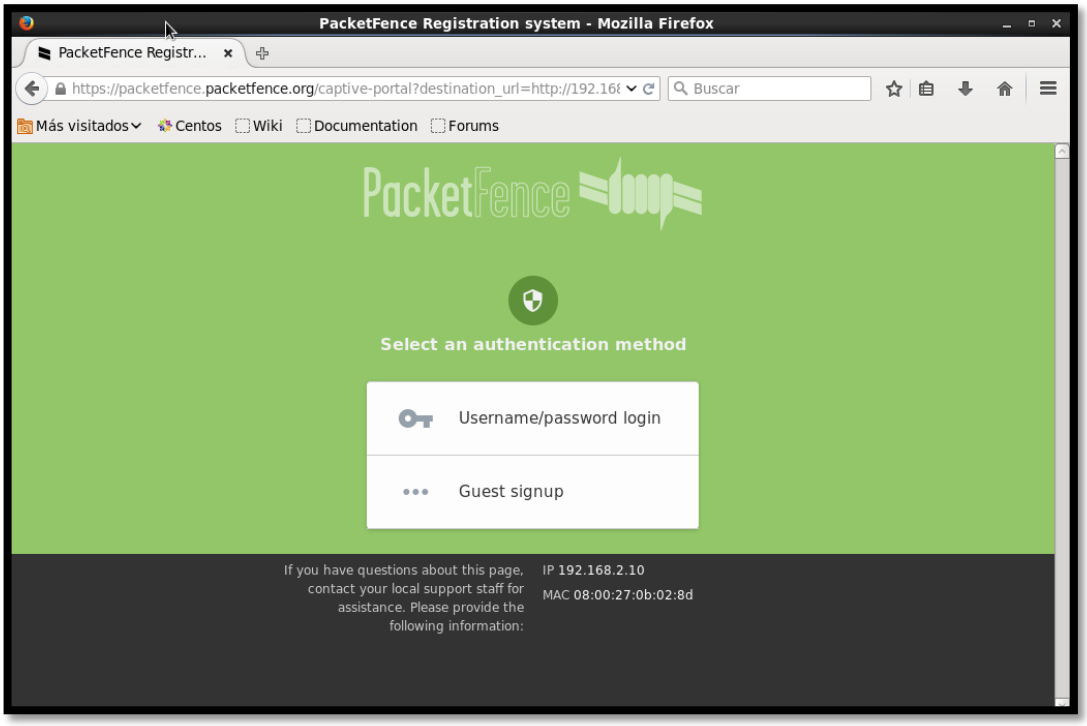

Figura 3-5: Portal Cautivo para el acceso de usuario

Realizado por: Julio Flores

- Servidor DHCP (ISC DHCP): PacketFence proporciona el servicio DHCP, este se hará cargo de la repartición de direccionamiento IP en nuestra red. Como se muestra en la presente figura 4-5.

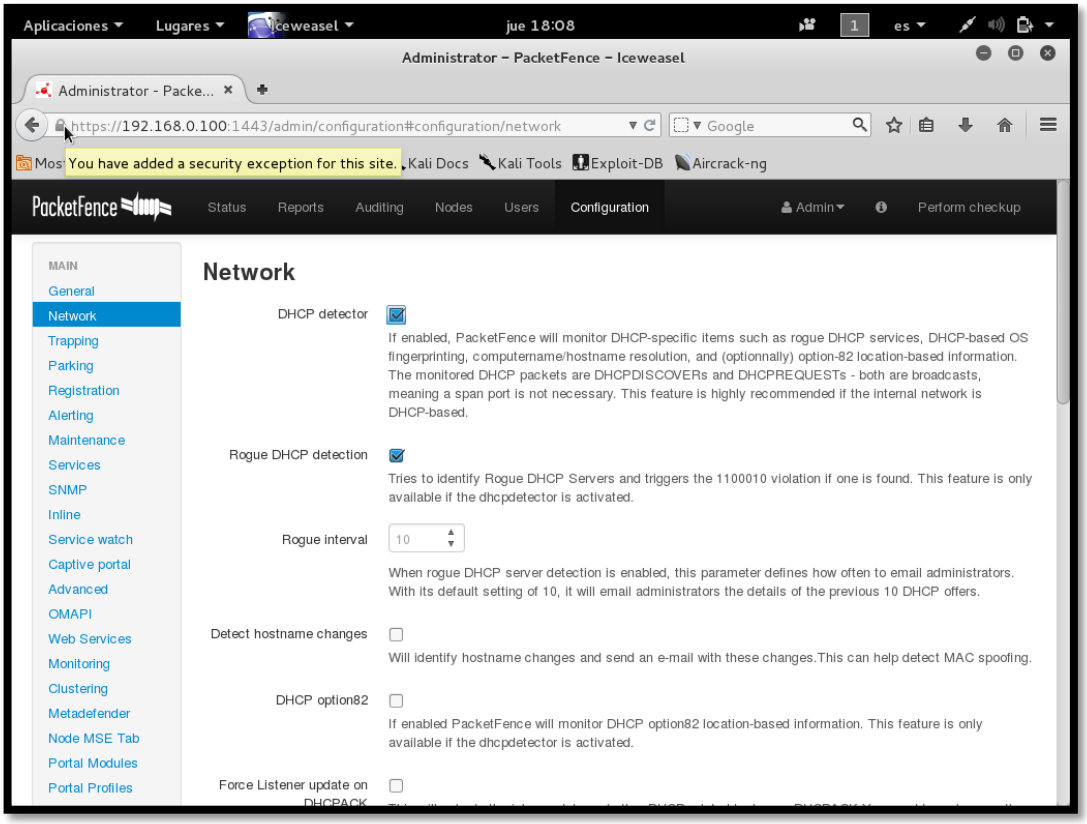

Figura 4-5: Activación Servidor DHCP

Realizado por: Julio Flores

- Servidor DNS (BIND): PacketFence ofrece el servicio de DNS, para la versión en línea, podemos proporcionar el DNS de la red corporativa. Como se presenta en la presente figura 5-5.

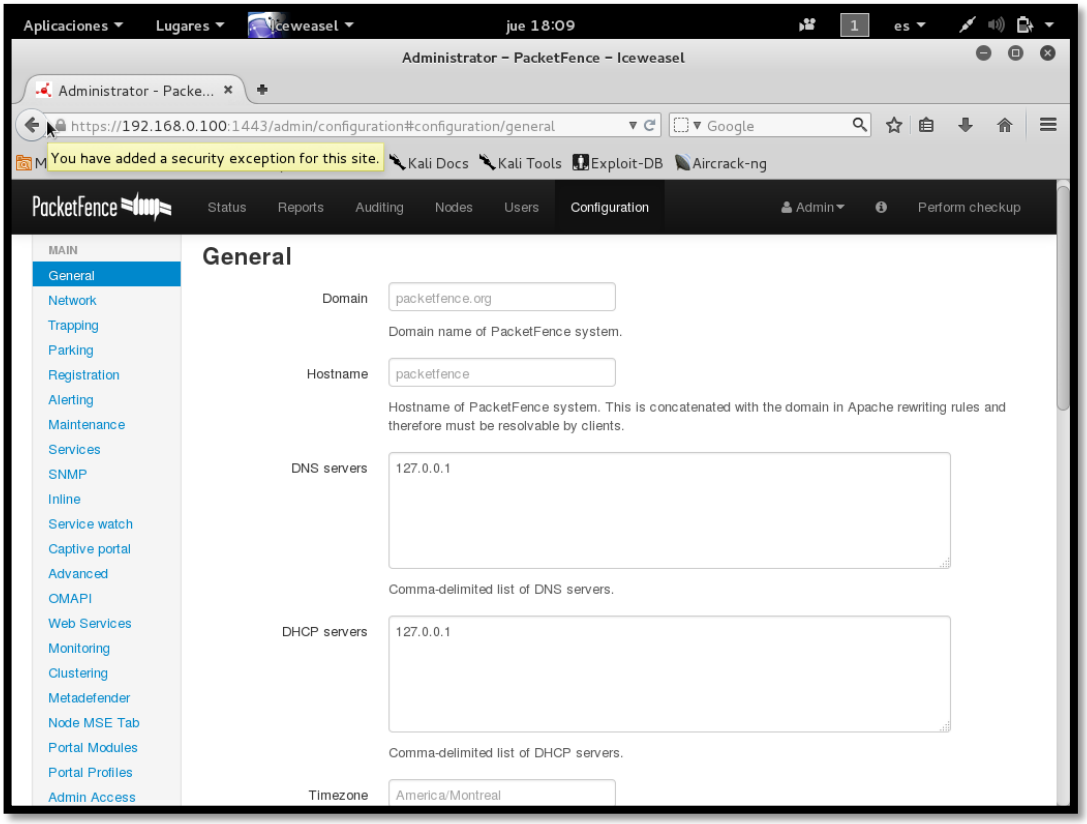

Figura 5-5: Activación Servidor DNS

Realizado por: Julio Flores

Todos los componentes mencionados se ejecutan en un mismo servidor

5.6. Políticas de Uso.

PacketFence trabaja de manera simultánea con un componente de registro llamado “portal cautivo”, la herramienta almacena los usuarios que previamente son registrados y automáticamente gestiona el acceso de autenticación y uso de la red. La principal política de uso es que los usuarios no pueden habilitar el acceso a la red sin primero haber sido registrado en el portal cautivo.

PacketFence presenta las siguientes políticas de control de acceso:

- Control de quién accede a la red y restricción del número de recursos. En la siguiente figura 6-5 se presenta los dispositivos registrados en la red.

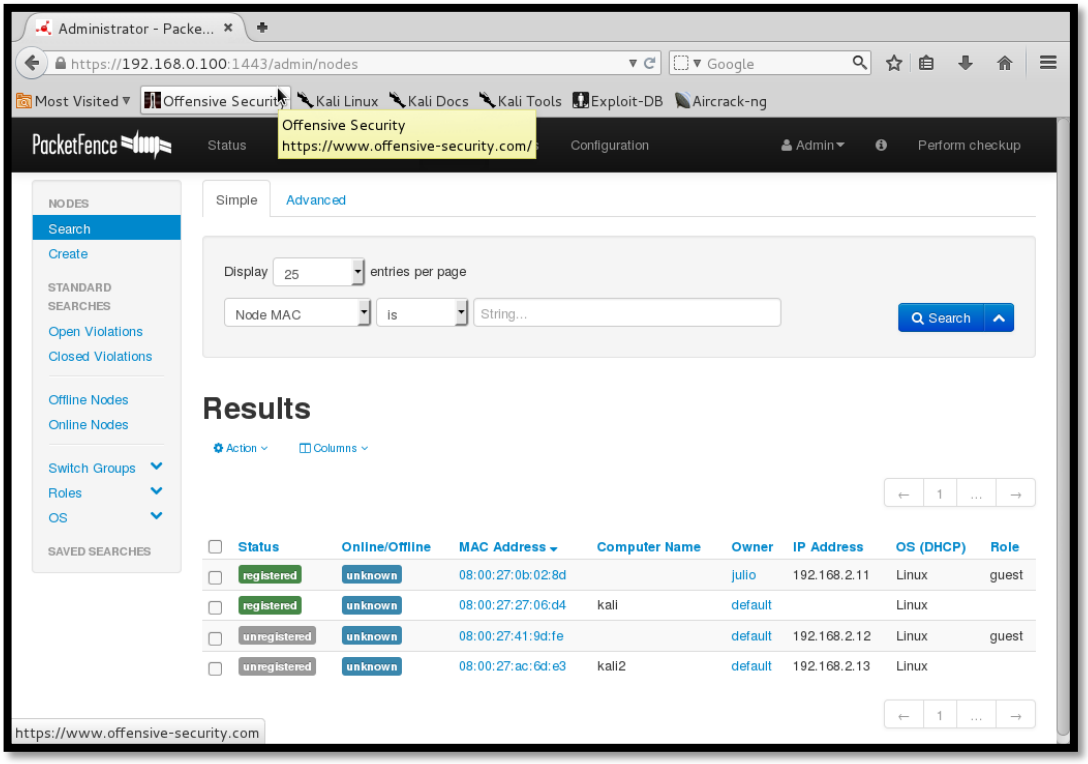

Figura 6-5: Control de Acceso a la Red

Realizado por: Julio Flores

- Restricción del acceso a información. En la figura 7-5 se configura las acciones que puede realizar el usuario registrado

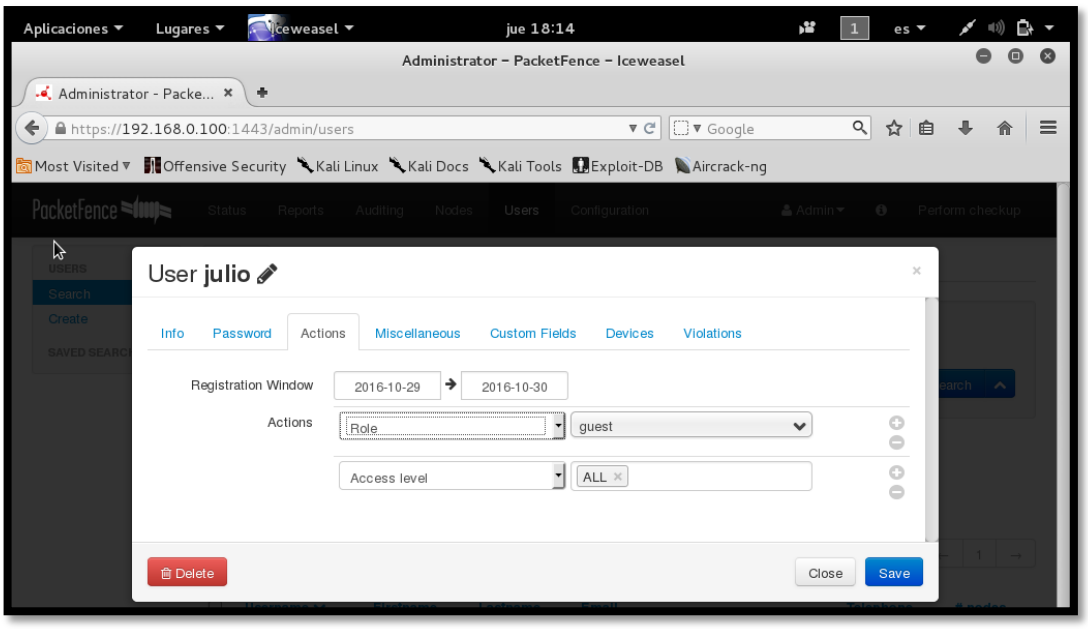

Figura 7-5: Restricción de Acceso a la Red

Realizado por: Julio Flores

- Control de los accesos en función del rol del usuario. En la figura 8-5 se muestra los accesos registrados de los usuarios así como también los usuarios que no se encuentran registrados.

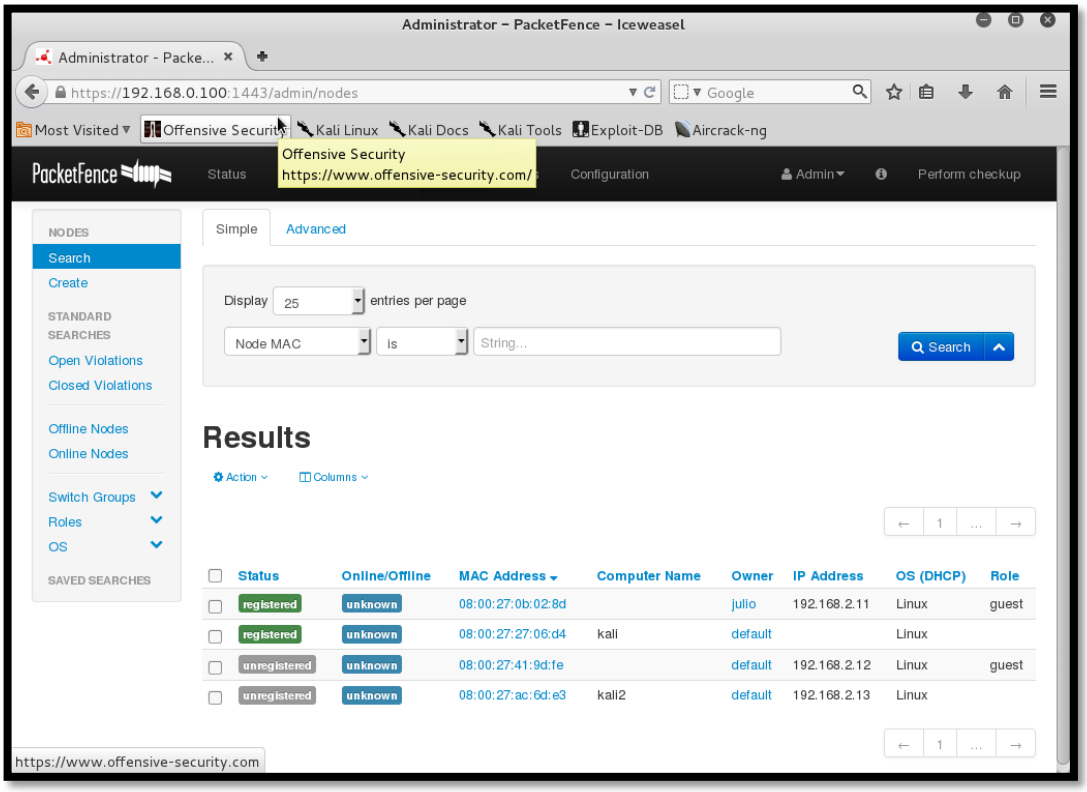

Figura 8-5: Acceso a la Red

Realizado por: Julio Flores

- Protección contra malware y virus, conocidos y desconocidos.

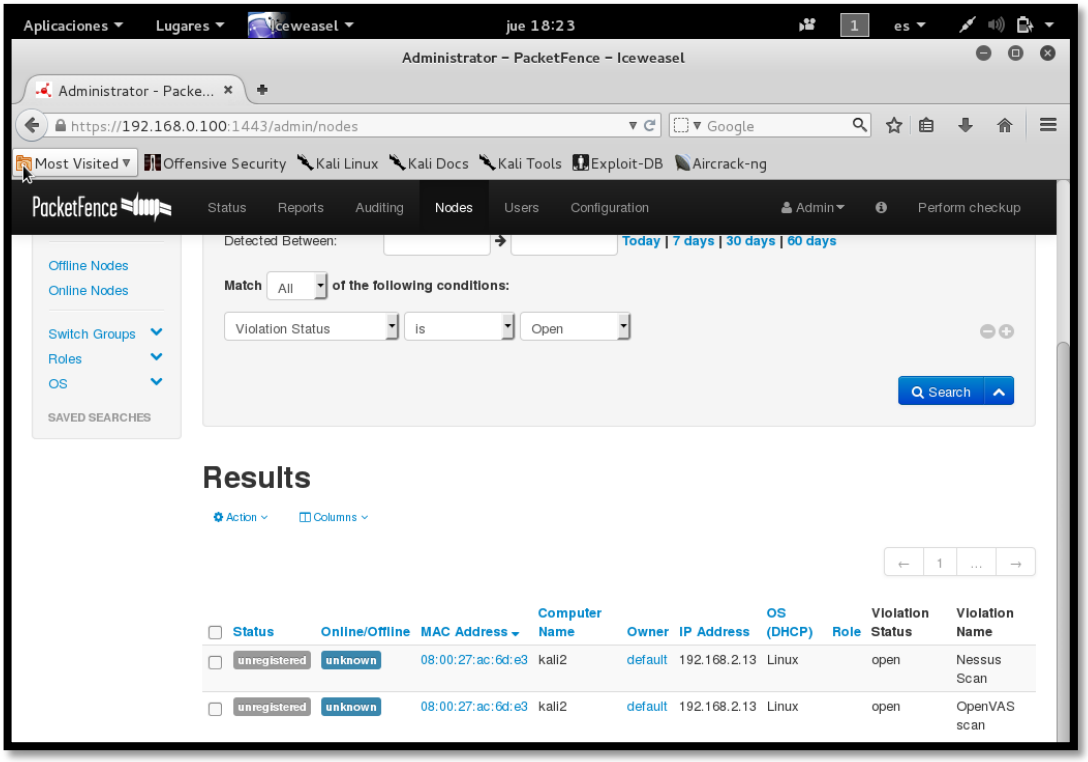

Figura 9-5: Acceso a la Red

Realizado por: Julio Flores

5.7. Aprendizaje del Usuario

En esta sección se indicara los pasos necesarios para instalar y configurar PacketFence, hay que indicar que la instalación de cada uno de los servicios es una tarea difícil y requiere de mucho tiempo. En la instalación se utilizaron los paquetes RPM (Package Manager), descubriendo que si cualquiera de los servicios que se instalan en un directorio diferente de lo que está escrito en los archivos de PacketFence, generara problema. Por lo que se sugiere utilizar la versión PacketFence ZEN (Zero Nac), que es una imagen de CentOS en el que vienen pre-instalados los componentes necesarios.

5.7.1. Instalación de PacketFence

La última versión de PacketFence (versión 6.3.0), la misma que ha sido liberada el 05/10/2016. Esta versión es estable y se puede utilizar en un entorno de red. Por lo que nos ubicaremos en la página web oficial de PacketFence, https://packetfence.org/ de aquí nos ubicaremos en el pestaña descargar o Down load y procederemos a descargar la imagen ISO de PacketFence ZEN como se muestra en la figura 10-5

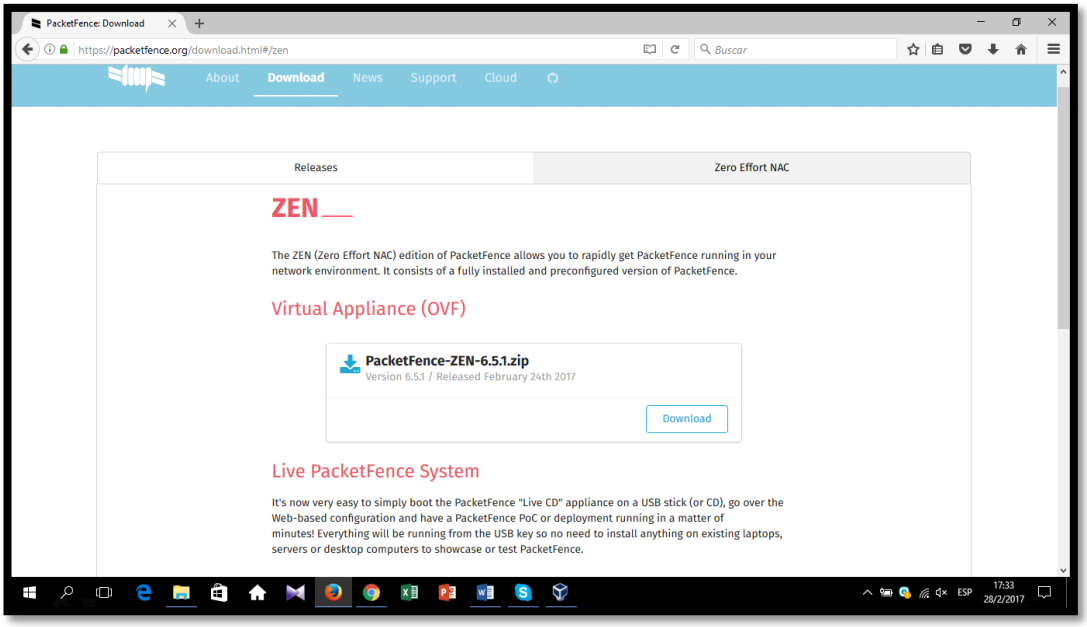

Figura 10-5: Pagina Web de descarga de PacketFence

Realizado por: Julio Flores

5.7.1.1. Configuración.

En este apartado, se revisará el proceso de configuración de PacketFence. Esta herramienta utiliza MySQL, Apache, Servidor DHCP, Servidor DNS, los servicios se ejecutan en el mismo servidor en el PacketFence.

El primer paso después de instalar PackectFence, es la configuración de PacketFence, que nos proporciona una útil y detallada configuración web. Para acceder a la aplicación de configuración solo se tendrá que acceder a la siguiente url: https//Direccion Ip PacketFence:1443/configurator, desde allí, el proceso de configuración se describe a continuación:

Paso 1, figura 11 - 5.
Se selecciona, la aplicación en línea para la creación del portal cautivo

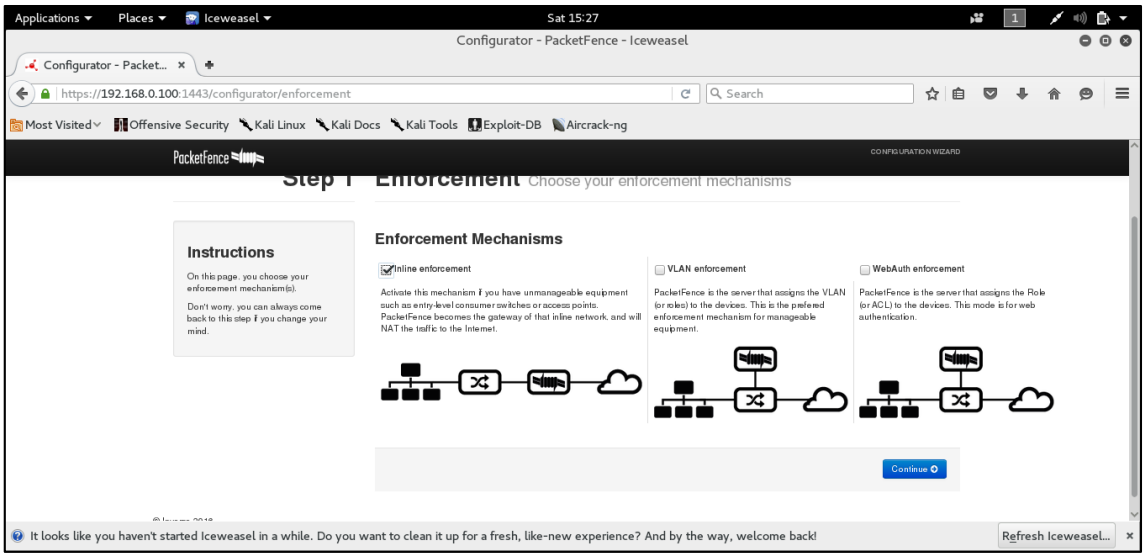

Figura 11-5: Escenario de configuración de PacketFence

Realizado por: Julio Flores

Paso 2, figura 12-5, figura 13-5 y figura 14-5.

Configuración de la red, en este punto indicaremos las interfaces por las que el servidor PacketFence recibirá las peticiones y en las cuales se aplican las diferentes técnicas de funcionamiento.

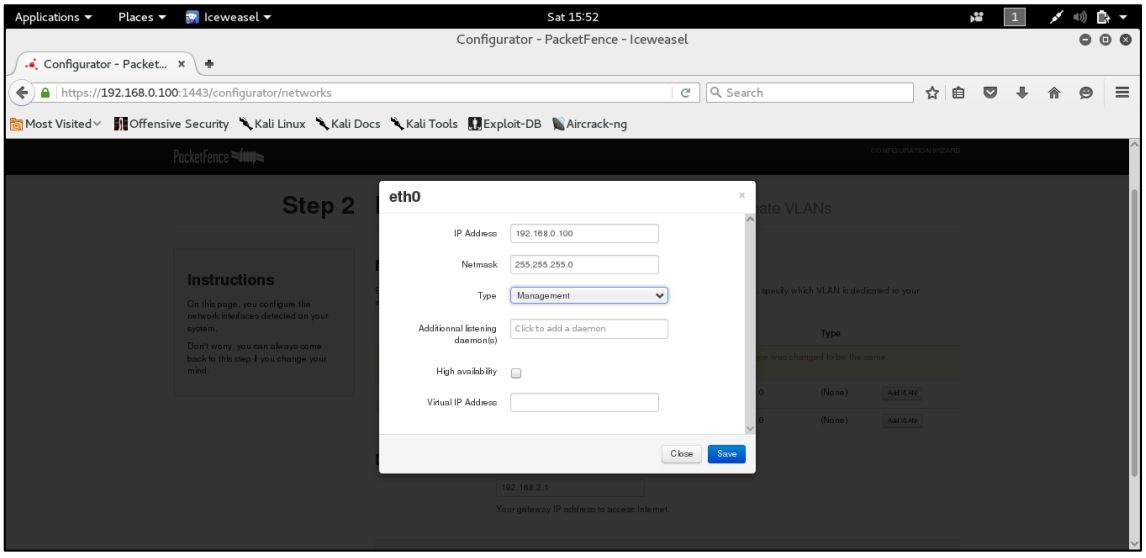

Figura 12-5: Escenario de configuración de Tarjetas de Red eth0

Realizado por: Julio Flores

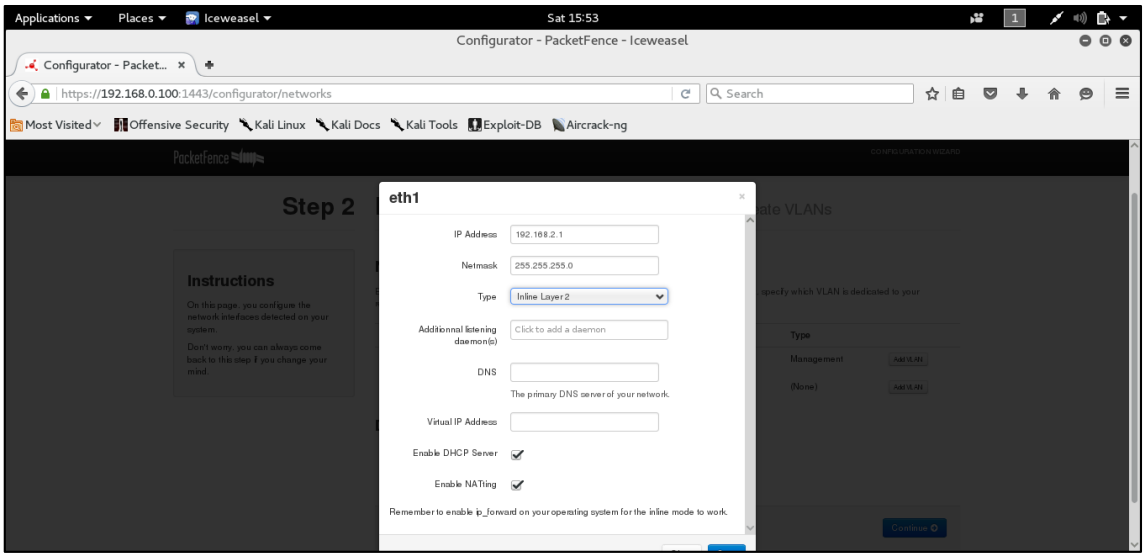

Figura 13-5: Escenario de configuración de Tarjetas de Red eth1

Realizado por: Julio Flores

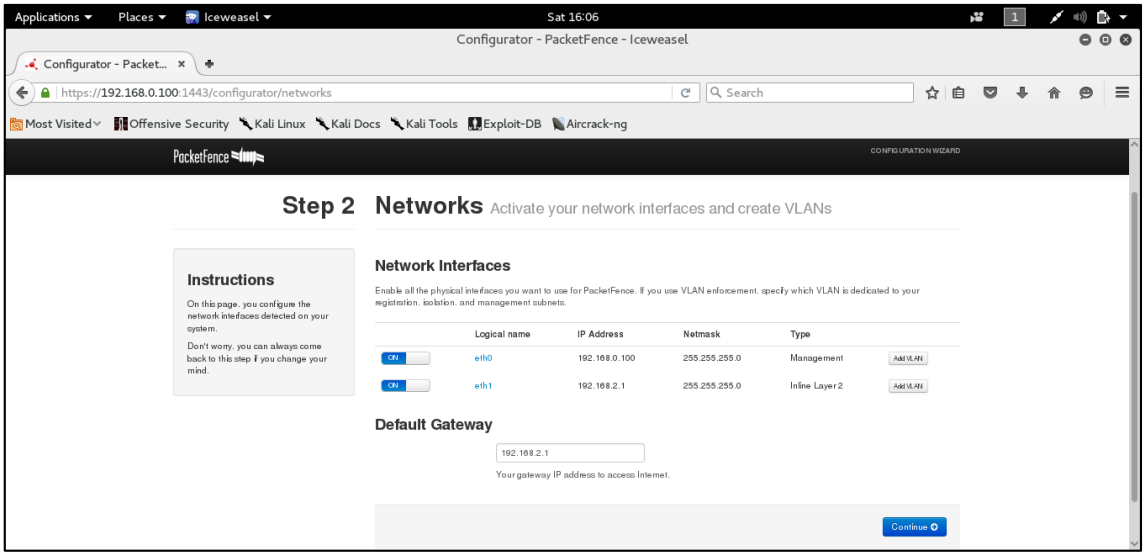

Figura 14-5: Escenario de configuración de Interfaces de Red

Realizado por: Julio Flores

Paso 3 figura 15-5, figura 16-5 y figura 17-5

Configuración de la base de datos, en este paso PacketFence creará la estructura correcta de tablas y referencias, además de la creación de un usuario para la administración de la base de datos con su respectiva contraseña.

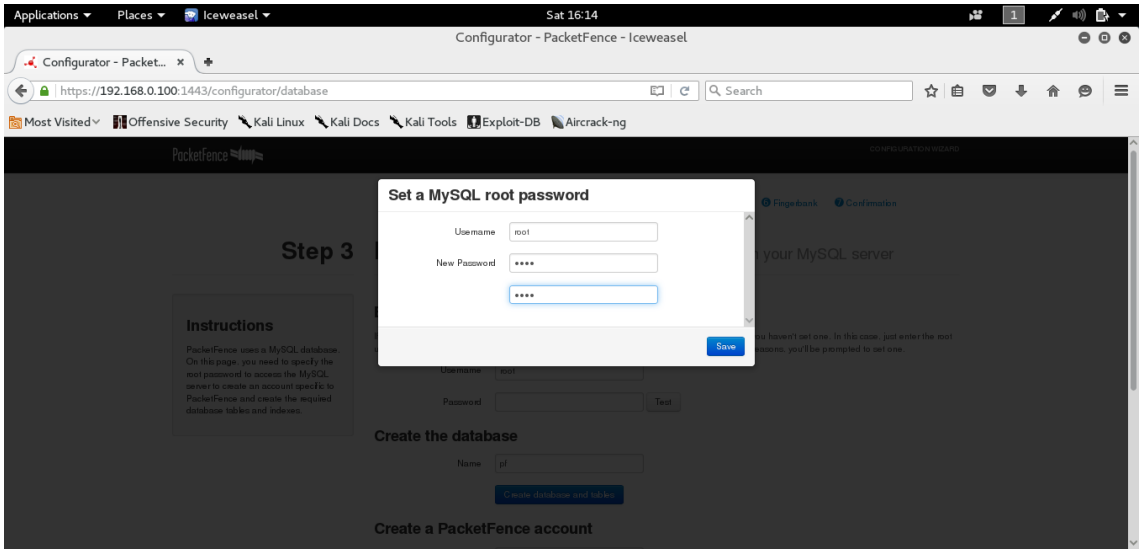

Figura 15-5: Escenario de configuración MySQL

Realizado por: Julio Flores

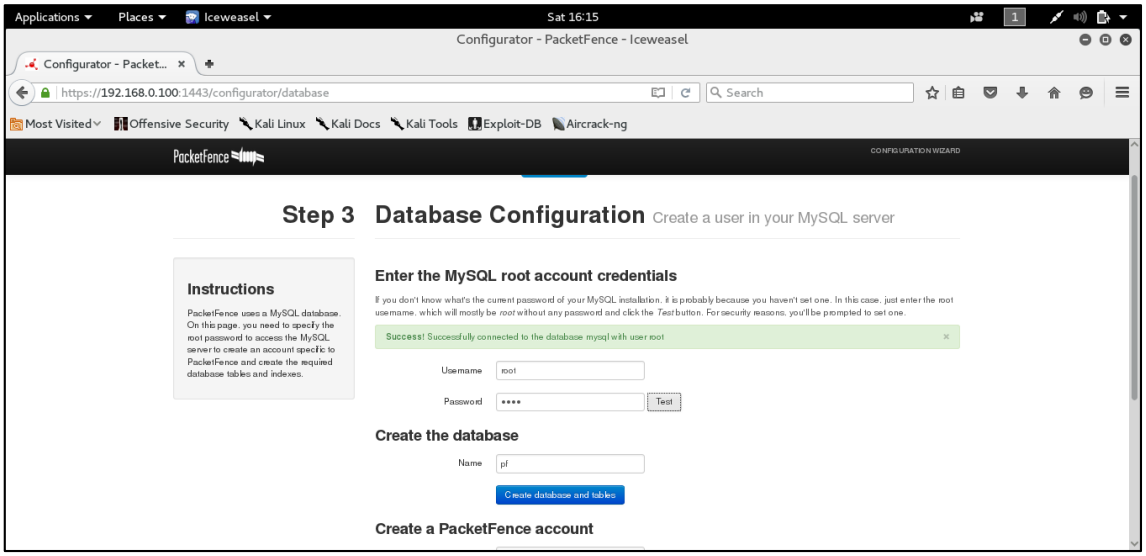

Figura 16-5: Escenario de configuración de MySQL cuenta de Administrador

Realizado por: Julio Flores

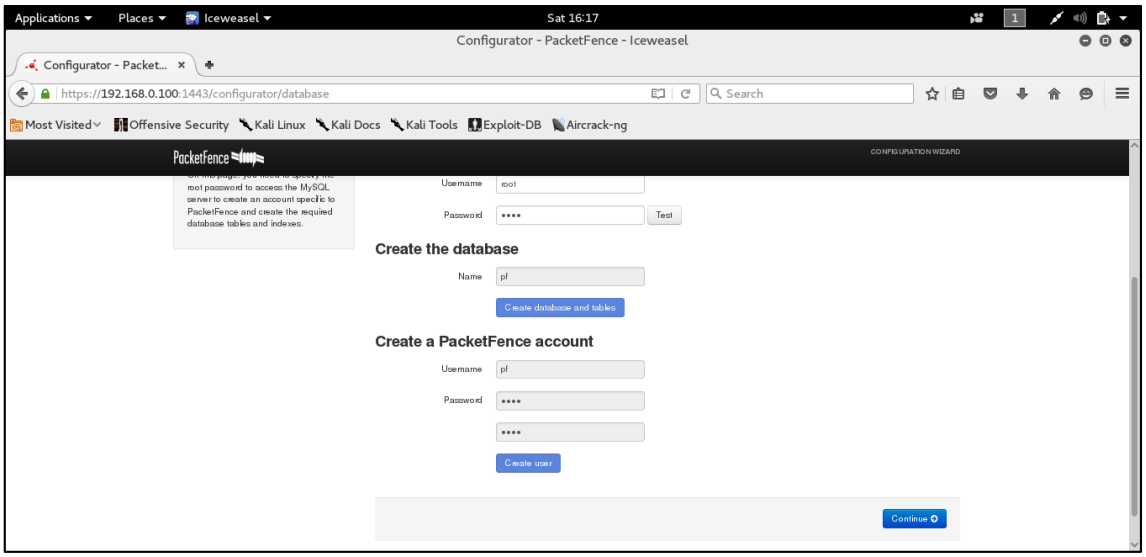

Figura 17-5: Escenario de configuración Base de Datos registro Clientes

Realizado por: Julio Flores

Paso 4, figura 18-5

Configuración general de PacketFence tales como el dominio donde estará integrado el sistema, nombre de máquina, definición servidor DHCP, correo de alerta.

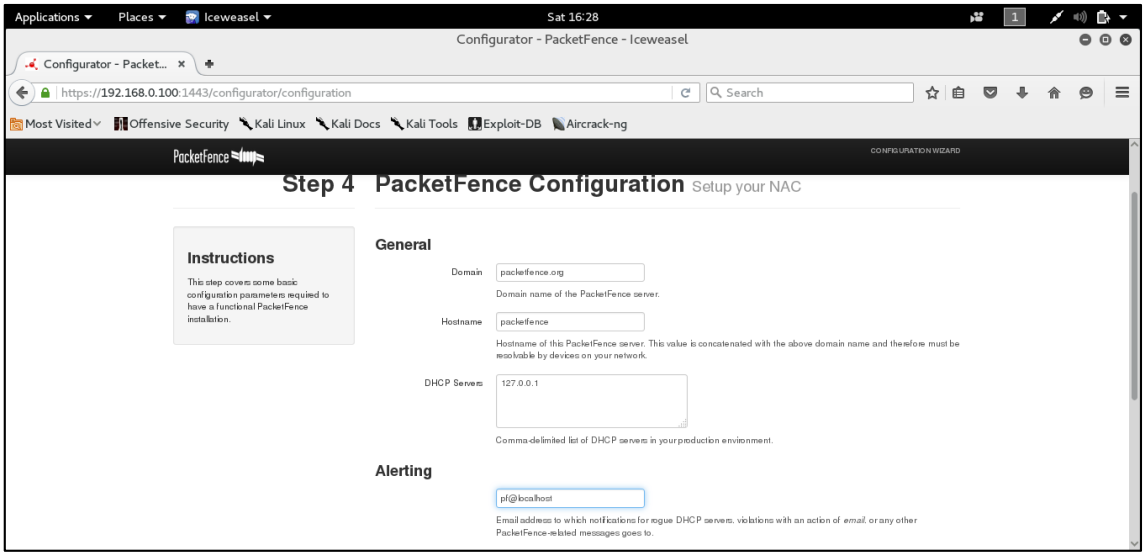

Figura 18-5: Escenario de configuración del Servidor DHCP

Realizado por: Julio Flores

Paso 5, figura 19-5.

Creación usuario administrador para acceder a la administración web de los servicios proporcionados por PacketFence.

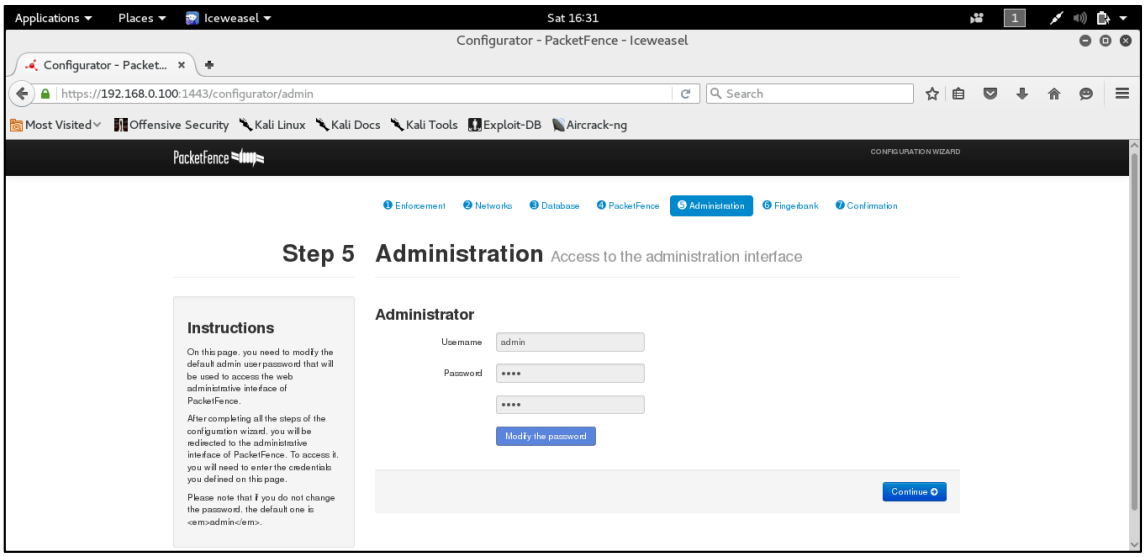

Figura 19-5: Escenario de configuración de Administrador

Realizado por: Julio Flores

Paso 6, figura 20-5, figura 21-5, figura 22-5 y figura 23-5 .

Comprobar el estado de la NAC y arranque de los servicios

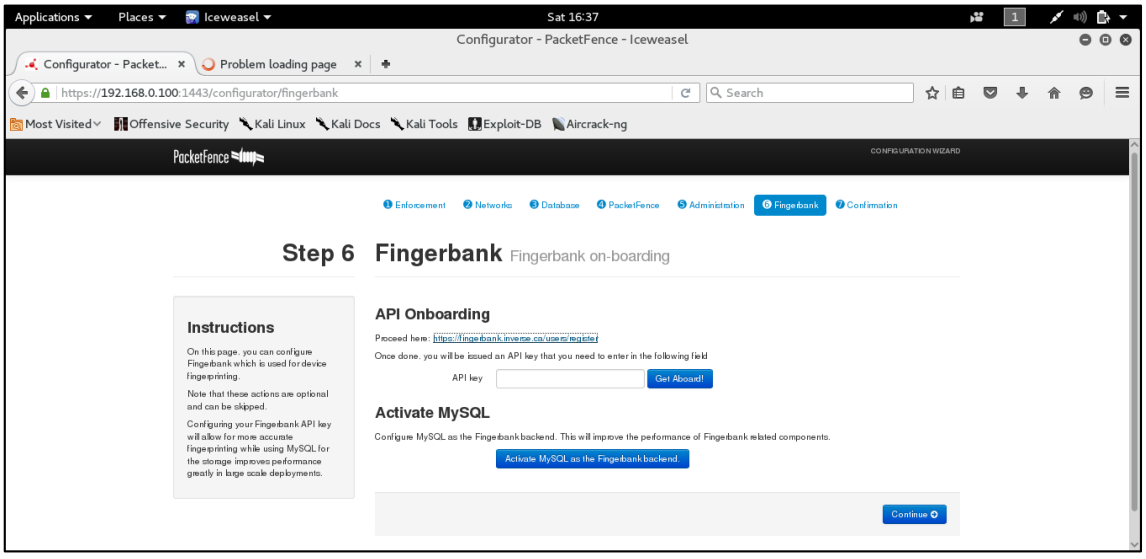

Figura 20-5: Escenario de configuración de Fingerbank

Realizado por: Julio Flores

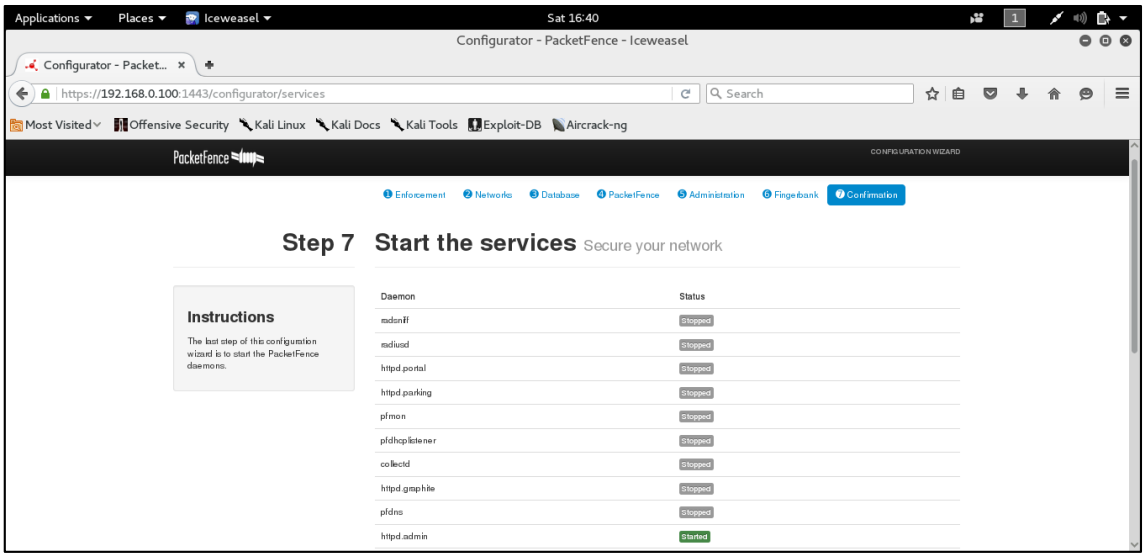

Figura 21-5: Inicio de Setvicios

Realizado por: Julio Flores

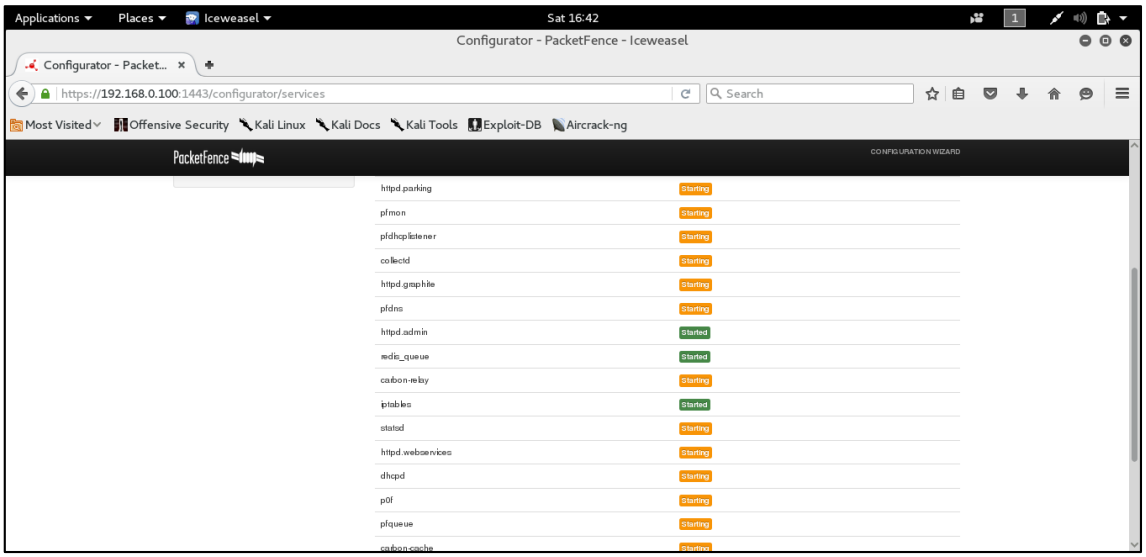

Figura 22-5: Activación de Servicios

Realizado por: Julio Flores

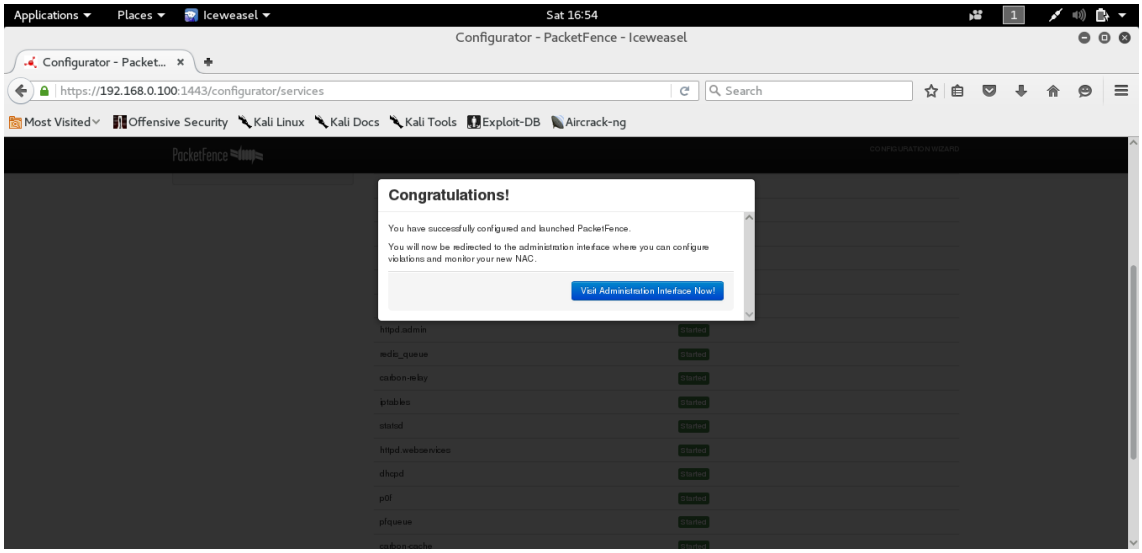

Figura 23-5: Ventana de Finalización de configuración

Realizado por: Julio Flores

5.7.1.2. Revisión de Opciones

Una vez configurado todos los pasos iniciales en nuestro servidor PacketFence podremos acceder desde la interfaz de web https//192.168.0.100:1443/configurator aquí se debe ingresar el usuario y la contraseña que se ingresó al momento de la configuración de nuestro servidor PacketFence como se muestra en la figura 24-5.

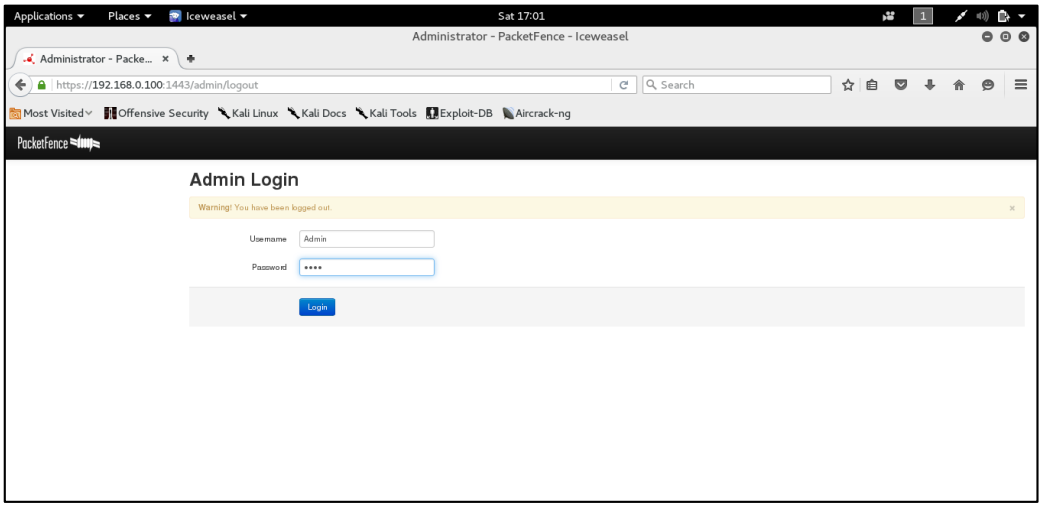

Figura 24-5: Ingreso del Usuario Administrador

Realizado por: Julio Flores

En la figura 25-5 se muestra la pestaña Usuario en la cual podemos observar los usuarios registrados, agregar usuario y buscar usuarios.

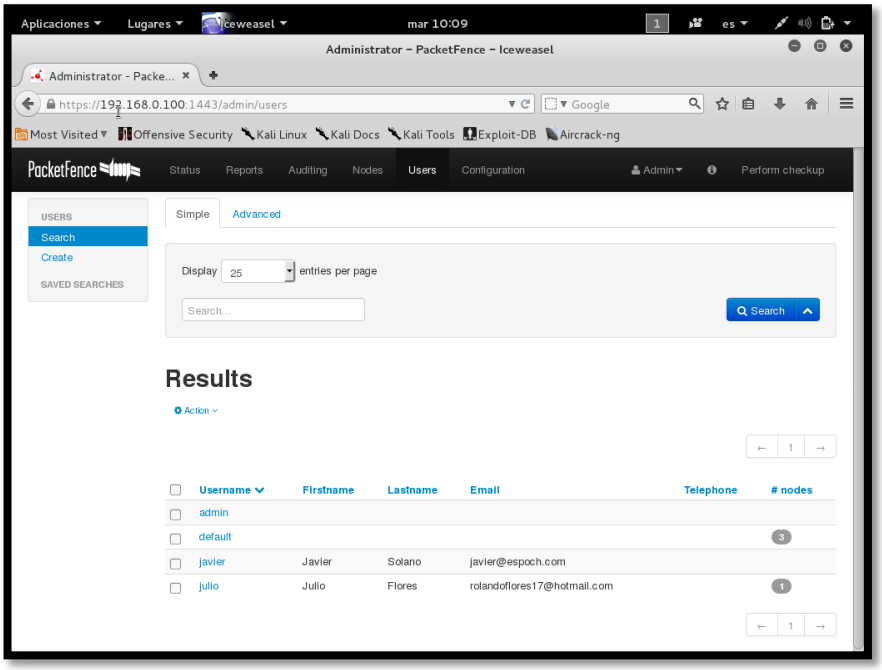

Figura 25-5: Escenario de configuración de Usuarios PacketFence

Realizado por: Julio Flores

En la siguiente opción NODO se visualiza la dirección MAC de la PC, el nombre del dispositivo conectado, la categoría, el estado (registrado, no registrado), la descripción del sistema operativo que se intenta conectar, aquí encontrará las opciones de ver, buscar adicionar e importar, se visualiza en la figura 26-5.

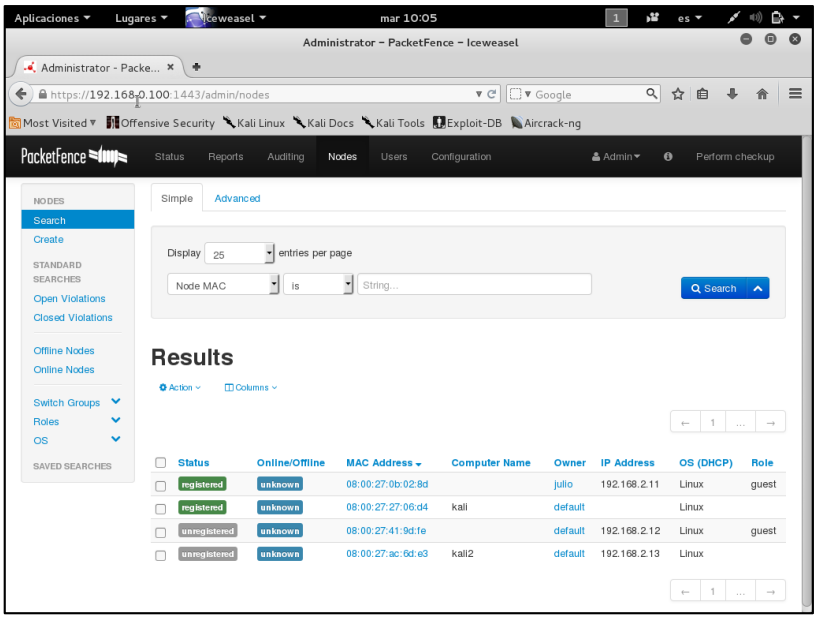

Figura 26-5: Escenario de configuración de Usuarios Registrados

Realizado por: Julio Flores

En la Pestaña NODO opción Open Violation se observa los intentos de acceso fallidos, o de usuarios que no han sido registrados, se registra la dirección MAC del dispositivo que intenta conectarse, así como el nombre del computador, la dirección IP y el sistema operativo del dispositivo se muestra en la figura 27-5.

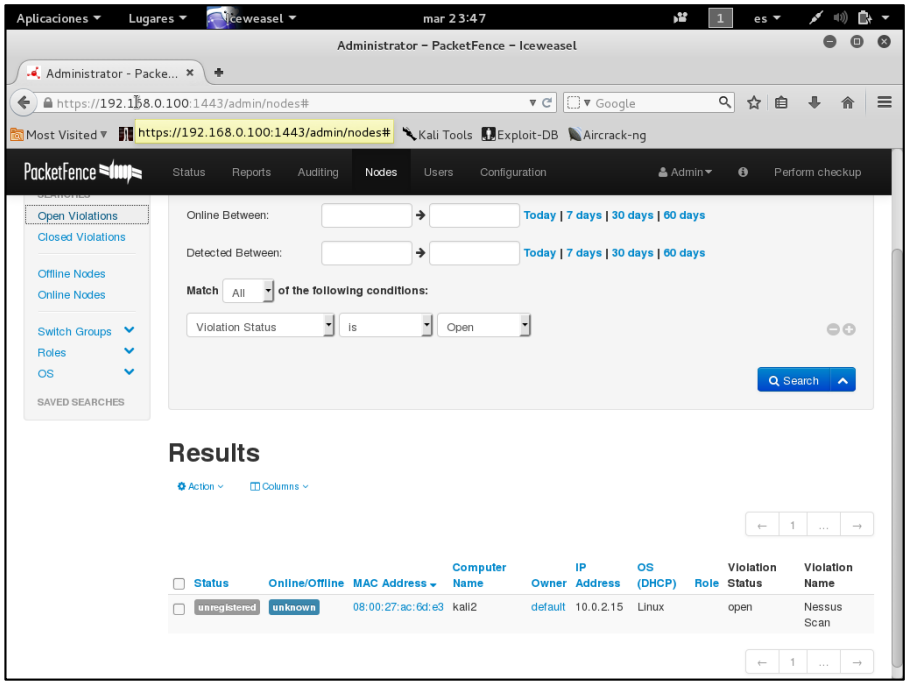

Figura 27-5: Reporte de Violaciones de Acceso

Realizado por: Julio Flores

5.8. Costos Asociados

La implementación de la Tecnología NAC beneficiará a todas las áreas, ya que estas estarán conectadas entre sí para agilizar los procesos, esto permitirá a la institución la optimización de sus procesos y el fácil acceso a la información y el mejor resguardo, permitiendo brindar un mejor servicio.

A continuación se detalla los costos que la institución debería realizar para la implementación de la tecnología NAC.

PRODUCTO	CANTIDAD	COSTOS
Servidor	1	$ 4.000
Licencia PacketFence	1	$ 0.000
TOTAL		$ 4.000

CONCLUSIONES

- El estudio determinó que en la actualidad las redes corporativas se ven en la necesidad de implementar soluciones de acceso a la red NAC para brindar alternativas de seguridad y prevenir ataques externos e internos. El análisis realizado durante el desarrollo documental y bibliográfico de la investigación, determinó que la herramienta PacketFence, debido a sus características es la mejor alternativa ya que integra diferentes herramientas de escaneo de vulnerabilidades en la red para brindar seguridad externa e interna en redes corporativas.
- La aplicación de la encuesta a los administradores de la red corporativa de la Escuela Superior Politécnica de Chimborazo, determinó que esta red no cuenta con herramientas NAC para el control de acceso ya que los esfuerzos están en la mayoría enfocados a la actualización de antivirus en los equipos de la institución.
- Para el levantamiento de la simulación de la red corporativa se tomó como referencia un nodo de red como se muestra en la figura de simulación, se utilizó el software GNS3 junto con la herramienta NAC PacketFence, misma que cumplió con los estándares de seguridad propuestas como son la autenticación, Integridad y disponibilidad mediante la creación de un portal cautivo que realizó tareas de autenticación de usuarios y dispositivos de red en un 98% de efectividad en cuanto a la integridad de datos 99% y disponibilidad de servicios 99% de efectividad.
- El estudio permitió la creación de una guía de implementación de la solución NAC para redes corporativas, con el software libre PacketFence proporciona funciones de registro, detección de actividades de la red, aislamiento de los dispositivos problemáticos.
- En respuesta a la hipótesis de investigación y en base a los resultados obtenidos en el escenario simulado, se puede indicar que la implementación de la solución NAC (PacketFence) propuesta en el estudio se constituirá el grado de efectividad del 98.67% para la seguridad externa e interna de las redes corporativas que opten por esta solución de seguridad informática, de acuerda a las pruebas realizadas en esta investigación.

RECOMENDACIONES

- La adecuada determinación de una solución de seguridad informática que pueda solucionar los problemas de una empresa o institución, muchas de las veces depende de costos que su implementación ocasione, en ese sentido, soluciones de proveedores como Microsoft y Cisco tienen altos costos para proveer soluciones de control de acceso a la red NAC, por lo cual se recomienda la aplicación de soluciones de Código Abierto o Software Libre como PacketFence.
- PacketFence es una herramienta de código abierto, es una distribución de Linux basada en CentOS, por lo que se recomienda, sea instalada ya sea en CentOS o en RedHat, ya que la instalación en otras distribuciones tiene su grado de dificultad.
- La solución NAC debe ejecutar todos los componentes y dependencias necesarias para su buen funcionamiento, además de recordar que PacketFence se integra también con redes inalámbricas a través del módulo FreeRADIUS, esto permite asegurar sus redes inalámbricas.
- PacketFence que es una herramienta de código abierto y de constantes cambios por lo cual es necesario contar con la más reciente actualización para su implementación, ya que en las pruebas realizadas cada vez existen cambios mejorando su funcionamiento.
- PacketFence, es una tecnología apropiada para la implementación por lo cual es necesaria realizar un proceso de socialización y capacitación en administradores de laboratorios y centros de cómputo para su adecuada y transparente implementación, sin descuidar la capacitación estudiantil, ya que en la encuesta aplicada se determinó su desconocimiento.

BIBLIOGRAFÍA

Microsoft. (2005) *Arquitectura de protección de acceso a la Red*. Recuperado el 10 de 08 de 2015. http://www.microsoft.com/en-us/download/details.aspx?id=8415

Wikispaces . (2006). *Administración y Seguridad en Redes*. Recuperado el 12 de 04 de 2015, de Seguridad: http://yoalo.wikispaces.com/4.4+Control+de+acceso+criptogr%C3%A1fico

Mindtools. (2009) *Control de Acceso a la Red*. Recuperado el 21 de 03 de 2015, de NAC´s : http://www.mindtools.com/CXCtour/PDCA.php

University of Maryland Introducción a las Normas ISO (2012). Recuperado el 22 de 06 de 2015, http://trace.wisc.edu/docs/taacmtg_sep96/iso.htm

NTSI 27002, I. (2007). *Norma Técnica de Seguridad de la Información.* Bogotá.

Aguirre, J. (2006). *Seguridad Informática y Criptografía Versión 4.1.* Madrid: Departamento de Publicaciones de la Universidad Politécnica de Madrid.

Bello, C. (2002). *Manual de Seguridad en Redes.* Buenos Aires: Arcert.

Carracedo Gallardo, J. (2004). *Seguridad en Redes Telemáticas.* Madrid: McGraw -Hill.

Carracedo, J. (2004). *Seguridad en Redes Telemáticas.* Madrid: McGraw-Hill / Interamericana.

CISCO ESPAÑA. (2006). *Cisco Netwok Admision Control and Protection.* Indianapolis: Cisco Press.

Knipp, E., & Brian, B. (2002). *Cisco Netwok Security.* California: Syngress.

Nakhjir, M., & Nakhjiri, N. (2002). *AAA and Netwok Security for mobile Access: Radius, Diameter, EAP, PKI and IP Mobility.* California: Syngress.

Opensource. (2012). *Free Nac Solutions for LAN.* New York: Prentice Hall.

Solutions, D. o. (2012). *Packetfence Solutions.* Boston: Opensource.

ANEXOS

Anexo A Encuesta aplicada a los encargados de los laboratorios y centros de cómputo de la ESPOCH

ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

ESCUELA DE POSGRADO

MAESTRIA EN INTERCONECTIVIDAD DE REDES

OBJETIVO: Determinar el grado de conocimiento de Seguridad Informática.

CUESTIONARIO

1. ¿Qué concepto daría Ud. acerca de la seguridad informática?

   …….
   …….

2. ¿Qué tipo de amenazas a la red según su criterio tienen mayor afectación?.

   Internas ( ) Externas ( )

3. ¿Cuál es la afectación más importante en seguridad informática?

   Seguridad física ( ) Seguridad lógica ( )

4. Los ataques lógicos a los que más expuestos están son:

- Controles de acceso ( )
- Identificación ( )
- Roles ( )

- Transacciones ( )
- Limitación a los servicios ( )
- Control de acceso interno ( )

5. ¿Administra algún tipo de políticas externas e internas de seguridad informática?.

SI ( ) NO ( )

6. ¿Qué tipo de políticas?

……..

……..

7. ¿En dónde se enfocan sus esfuerzos de seguridad?

- Configuración de firewalls ( )
- Actualización de antivirus ( )
- Control de credenciales y usuarios ( )

8. ¿Conoce Ud. que son las NAC?

SI ( ) NO ( )

9. ¿Podría Ud. indicarnos que ventajas ofrece las NAC?

1. Seguridad lógica ( )
2. Seguridad física ( )
3. Controla acceso a la red ( )
4. Controla acceso a recursos de red ( )

10. ¿Qué tipo de políticas de seguridad recomendaría Ud. para la institución?

- Software con licencia (Cisco, Microsoft) ( )
- Software libre (Open Source). ( )

Gracias por su colaboración

Anexo B: Análisis y procesamiento de las encuestas

Encuesta realizada sobre seguridad Informática para el control de acceso a la red Para conocer el criterio de los encargados de los diferentes centros de cómputo y laboratorios de la facultad se procedió a la recolección de datos a través de la encuesta planteada mediante la tabulación de datos, así también para la gráfica de los cuadros estadísticos a través del programa Microsoft Excel para de una forma gráfica - visual conocer el criterio de los encuestados.

1. **¿Qué concepto daría Ud. acerca de la seguridad informática?**

La tabla 1; recaba información sobre el grado de conocimiento de los encargados de laboratorio sobre la seguridad informática.

Tabla 1: Conceptualización Seguridad Informática

VARIABLE	VALOR	PORCENTAJE
Control de riesgo de acceso de datos	4	11%
Proteger información	5	14%
Garantizar seguridad información	4	11%
Políticas, normas de seguridad	4	11%
Seguridad en los sistemas	4	11%
Vulnerabilidad en software y sistemas operativos	4	11%
Protección infraestructura	4	11%
Aplicación de protocolos	4	11%
Integridad en los datos	3	9%
Total	**36**	**100%**

Realizado por: Julio Flores

Análisis e interpretación.

El gráfico 1, aplicado a los encargados de laboratorio manifestaron conceptos variados acerca de los que consideran seguridad informática, con un 14% el porcentaje más alto manifestaron que la seguridad informática cuida y protege la información en un 14%, los demás conceptos mantienen un porcentaje del 11%.

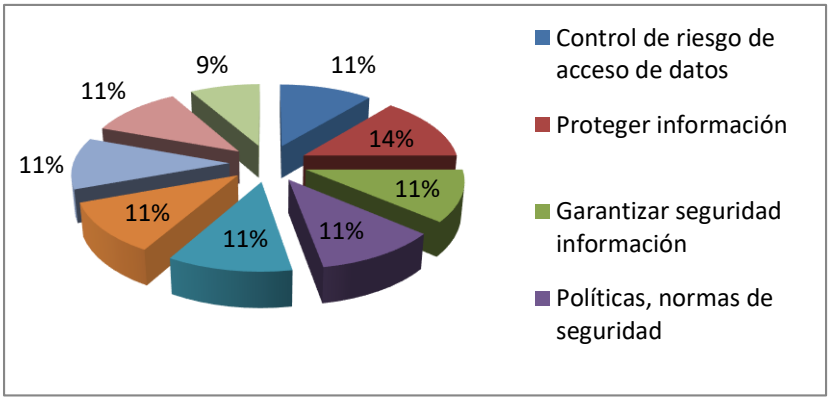

Gráfico 1: Conceptualización Seguridad Informática

Realizado por: Julio Flores

2. ¿Qué tipo de amenazas a la red según su criterio tienen mayor afectación?.

La tabla 2 recaba información sobre las frecuentes amenazas que se encuentran en una red corporativa.

Tabla 2: Amenazas de mayor afectación

VARIABLE	VALOR	PORCENTAJE
Amenazas Internas	29	81%
Amenazas Externas	7	19%
TOTAL	**36**	**100%**

Análisis e interpretación.

La gráfica 2, aplicada a los encargados de laboratorio expresaron que las amenazas internas con un 81% son las que mayor afectación que perjudican la seguridad informática, mientras que un 19% consideran que las amenazas externas son las que menor afectación tienen para la seguridad en el ámbito informático.

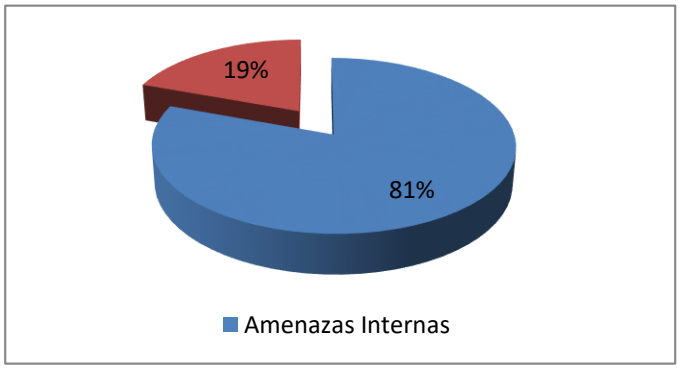

Gráfico 2: Amenazas de mayor afectación

Realizado por: Julio Flores

3. ¿Cuál es la afectación más importante en seguridad informática?

La tabla 3; muestra información de las seguridades informáticas que se ponen en marcha para detectar posibles infiltraciones y ataques a la red.

Tabla 3: Afectación de la seguridad informática

Variable	Valor	Porcentaje
Seguridad Física	2	6%
Seguridad Lógica	34	94%
Total	36	100%

Análisis e interpretación.

En el grafico 3, Los encargados de laboratorio manifiestan que en un 94% afecta a la seguridad lógica es la mayor afectación debido a que los ataques que se realizan son por los usuarios de la red, ya que el control de la seguridad física es muy bajo con un 6% de afectación.

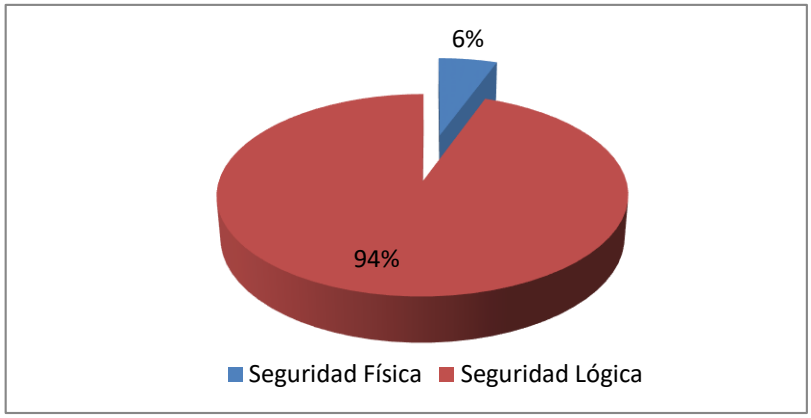

Gráfico 3: Afectación de la seguridad informática

Realizado por: Julio Flores

4. Los ataques lógicos a los que más expuestos están son:

La tabla 4; muestra información de los ataques lógicos más comunes en una red corporativa.

Tabla 4: Ataques lógicos

Variable	Valor	Porcentaje
Controles de acceso	24	30%
Identificación	10	12%
Roles	8	10%
Transacciones	15	18%
Limitación a los servicios	12	15%
Control de acceso interno	12	15%

Análisis e Interpretación

El gráfico 4, indica los ataques lógicos que más están expuestos los laboratorios de la ESPOCH están en el orden de 30% en el control de acceso, un 10% de roles, un 15% la limitación de servicios, problemas de identificación con un 12% , en transacciones se manejan un 18% y un control, de acceso interno con un 15%.

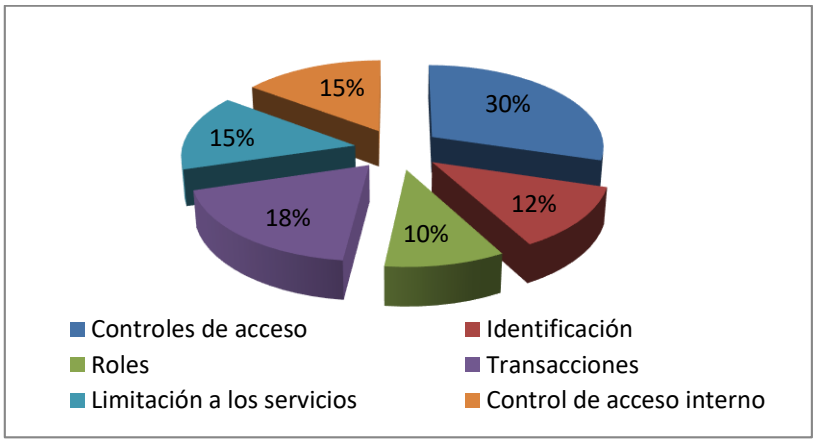

Gráfico 4-1 Ataques lógicos

Realizado por: Julio Flores

5. ¿Administra algún tipo de políticas externas e internas se seguridad informática?.

La tabla 5; muestra información si existe o no seguridad en la red corporativa.

Tabla 5: Administración de políticas de seguridad

Variable	Valor	Porcentaje
SI	16	44%
NO	20	56%
Total	**36**	**100%**

Análisis e interpretación

En el gráfico 5, Los administradores de red se visualiza que no tienen políticas de red con un alto porcentaje en un 56%, mientras que en un 44% de los administradores de red si tiene políticas de seguridad en especial los encargados de las facultades de informática y electrónica.

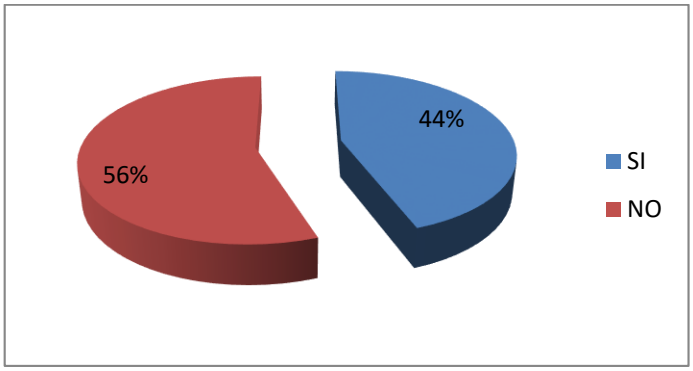

Gráfico 5: Administración de políticas de seguridad
Realizado por: Julio Flores

6. ¿Qué tipo de políticas?

La tabla 6; muestra información de las políticas de seguridad

Tabla 6: Administración de políticas de seguridad

VARIABLE	VALOR	PORCENTAJE
Https	4	11%
Control de acceso	20	56 %
Encriptación información	4	11%
Actualización de antivirus	4	11%
Firewall	4	11%
Total	36	100%

Análisis e interpretación

En la gráfica 6 se puede identificar que el más alto porcentaje de usuarios en un 56% consideran que el control de acceso a la red debe ser una de las prioridades de las políticas de seguridad en las redes internas, con un 11% en iguales porcentajes de las seguridades de https, encriptación de la información, actualización de antivirus y firewall.

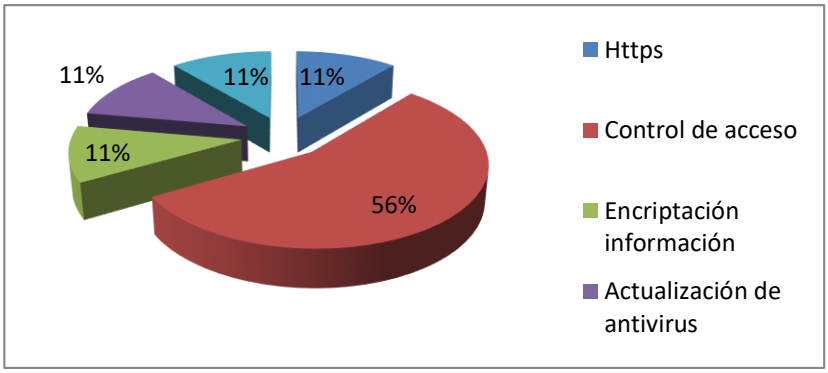

Gráfico 6: Administración de políticas de seguridad

Realizado por: Julio Flores

7. ¿En dónde se enfocan sus esfuerzos de seguridad?

La tabla 7; describe las acciones realizadas de los administradores de la red.

Tabla 7: Esfuerzos de seguridad

VARIABLE	VALOR	PORCENTAJE
Configuración de firewalls	18	36%
Actualización de antivirus	21	42%
Control de credenciales y usuarios	11	22%

Análisis e interpretación

La grafica 7, describe la configuración de firewalls en un porcentaje del 36% son las actividades que como esfuerzos de seguridad realizan los encargados de laboratorios de las facultades de la ESPOCH, mientras que en un alto porcentaje un 42% de los encuestados manifiestan que en un 42% realiza la actualización de software y un pequeño porcentaje realiza actividades de control de credenciales y de usuarios.

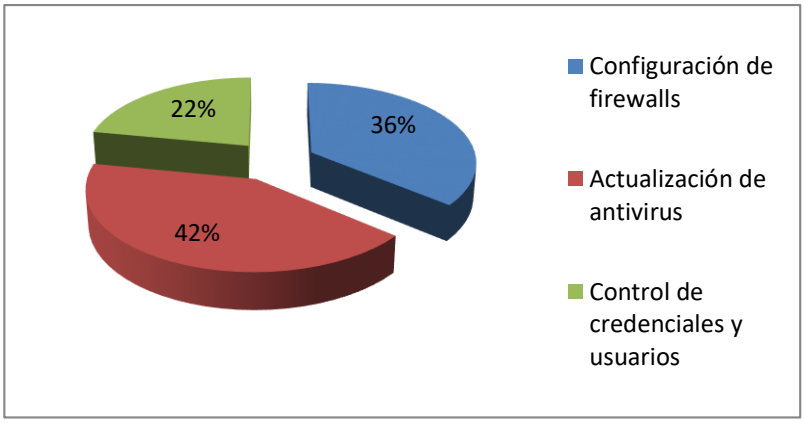

Gráfico 7: Esfuerzos de seguridad

8. ¿Conoce Ud. que son las NAC?

La tabla 8; identifica el conocimiento sobre las tecnologías NAC.

Tabla 8: Conocimiento de las NAC´s

VARIABLE	VALOR	PORCENTAJE
SI	10	28%
NO	26	72%
TOTAL	**36**	**100%**

Análisis e interpretación

La grafica 8, identifica el grado de conocimiento de las políticas de las NAC tan solo está en un porcentaje del 28%, el desconocimiento en un 72% por lo cual se vuelve necesario e imprescindible capacitaciones que permitan el desarrollo, aplicación e implementación de políticas de seguridad que permitan un mejor control de amenazas tanto internas como externas.

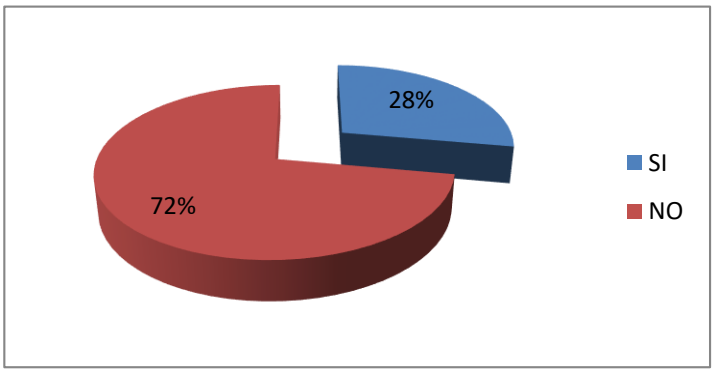

Gráfico 8: Grado de conocimiento de las NAC´s

9. ¿Podría Ud. indicarnos que ventajas ofrece las NAC?

La tabla 9; identifica las ventaja de utilizar una tecnología NAC

Tabla 9: Ventajas de uso de tecnologías las NAC's

VARIABLE	VALOR	PORCENTAJE
Seguridad Lógica	2	6%
Seguridad Física	0	0%
Control de acceso a la red	14	39%
Controla recursos de acceso a la red	3	8%
No contesta	17	47%
Total	36	100%

Análisis e interpretación

La gráfica 9, de los administradores de red al consultarlos acerca de las ventajas que ofrecen las NAC´s en su gran mayoría no contestaron en un 47% lo que refleja el desconocimiento de las políticas NAC´s, un 39% manifiesta que son seguridades implementadas para el control de accesos a la red, un 8% manifiesta que son controles de acceso de recursos de red, y un 6% manifiesta que se refiere a la seguridad lógica dentro de la infraestructura de red.

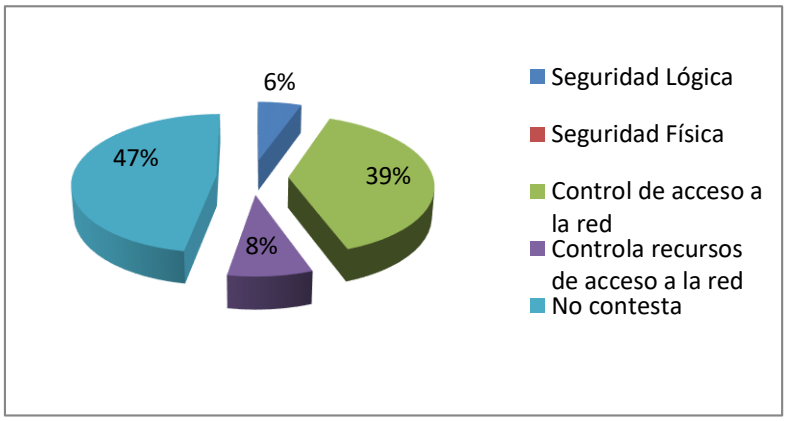

Gráfico 9: Ventajas del uso de las NACs

10. ¿Qué tipo de políticas de seguridad recomendaría Ud. para la institución?

La tabla 10; políticas de seguridad recomendadas en una red corporativa

Tabla 10: Recomendación de seguridad en una red corporativa

Variable	Valor	Porcentaje
Software con licencia (Cisco, Microsoft)	15	42%
Software libre (Open Source)	17	47%
No responde	4	11%
Total	**36**	**100%**

Realizado por: Julio Flores

Análisis e interpretación

La mayoría de encuestados manifestaron su inclinación a utilizar productos de Software libre, en un 47% paquetes de como PacketFence puede ser una alternativa viable para precautelar la seguridad de la red, mientras que en un 42% un porcentaje relativamente alto manifestó su deseo de ocupar productos con licencia a pesar del costo que involucra y un 11% se abstuvo de contestar ya que no ha implementados o desconoce de aplicaciones para el control de acceso en la red. Como se puede visualizar en la gráfica 10.

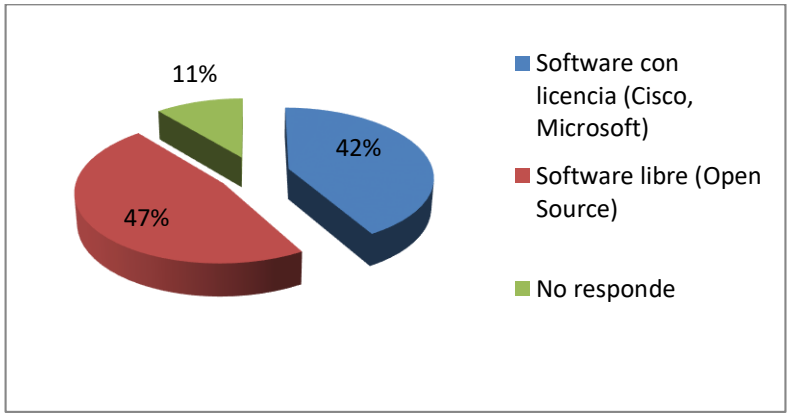

Gráfico 10-4: Recomendación de seguridad

Anexo C. PRUEBAS, ATAQUES

Ataque de Denegación de servicios.

La figura 1, indica el procedimiento a seguir para realizar el ataque con Kali Linux al servidor PacketFence empleando la herramienta Metaexploit.

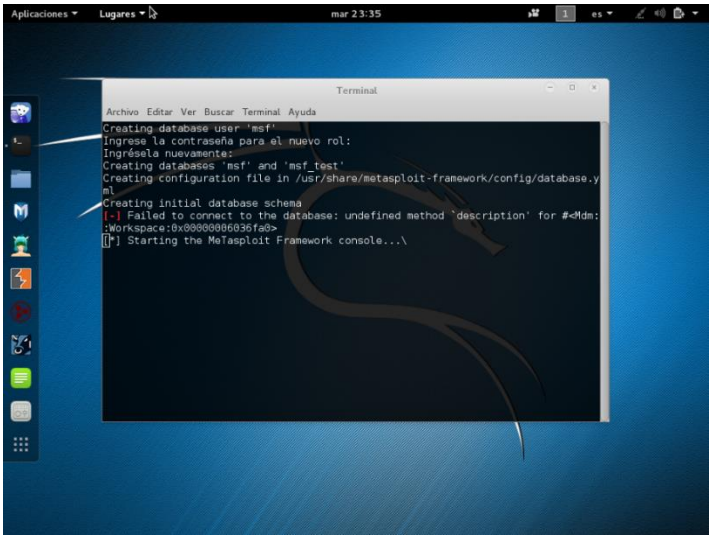

Figura 1: Escenario de Ataque con Kali Linux

Realizado por: Julio Flores

En esta sección ingresamos el comando set RHOST y la dirección de nuestro servidor PacketFence que es 192.168.0.100 figura 2-4.

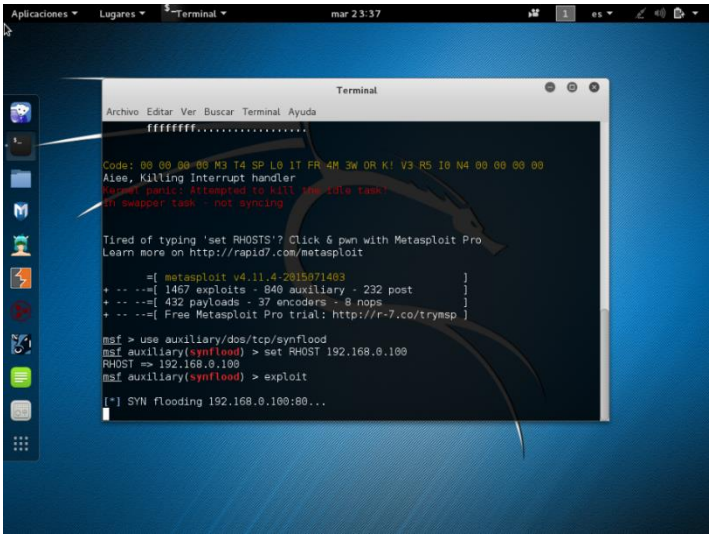

Figura 2: Escenario de Ataque con Kali Linux

Realizado por: Julio Flores

Figura 3, verificamos en nuestro servidor PacketFence que reporte nos brinda con respecto a nuestro ataque

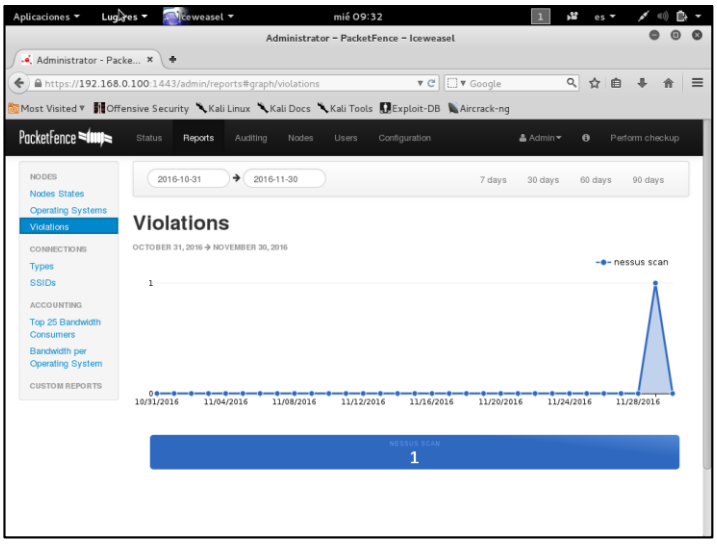

Figura 3: Escenario de Reporte de Violación

Realizado por: Julio Flores

Luego nos dirigimos a la opción nodos de nuestro servidor PacketFence y se verifica que el nodo atacante Kali Linux 2 se encuentra no registrado dando como resultado que no se puede conectar figura 4-4.

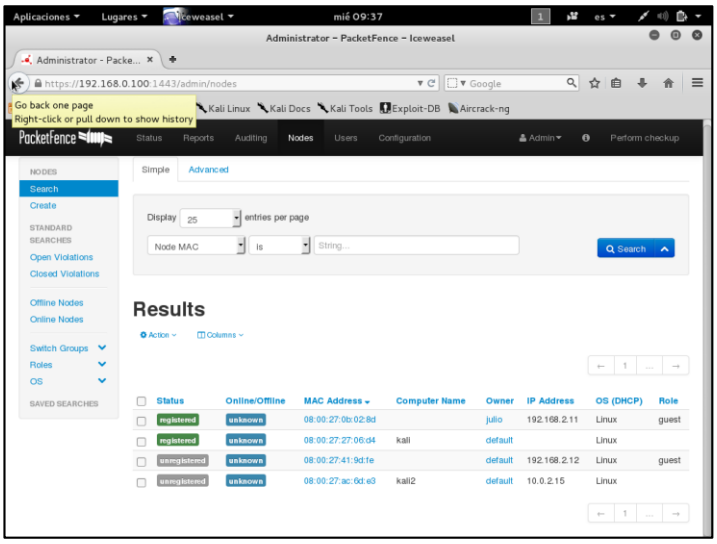

Figura 4: Escenario de Reporte de Violación

Realizado por: Julio Flores

Anexo D: Guía de Instalación PacketFence.

PACKETFENCE

PacketFence es una solución NAC basada en código abierto y gratuito. Esta solución nos ofrece un conjunto de características como por ejemplo un cautivo en donde los usuarios se autentificaran para su debido registro, una gestión centralizada tanto dispositivos inalámbricos como por cable, asilamiento de dispositivos de capa 2, integración con escáner de vulnerabilidades y detección de intrusos.

Además PacketFence esta preparado y diseñado para brindar servicio tanto a redes pequeñas como grandes redes donde se encuentran instalados dispositivos y puntos de acceso a la red.

CARACTERÍSTICAS PRINCIPALES DE PACKETFENCE

- Sitio web cautivo para autenticación y registro de dispositivos que solicitan el acceso a la red.
- Detección de actividades de la red anormales
- Exploraciones preventivas de vulnerabilidades
- Aislamiento de los dispositivos problemáticos
- Servicio de DHCP
- Listado de potenciales BYOD
- Control de acceso basado en roles
- Integración con escáneres de vulnerabilidades diferentes y soluciones de detección de intrusos
- Ancho de banda controlada para cada dispositivo
- Soporte 802.1x con FreeRadius includo
- Gestión centralizada de las redes tanto cableada como inalámbrica.
- Integración con el sistema para la detección de intrusos SNORT y NESSUS.
- Soporte VLAN y aislamiento de redes.
- Autenticación, PacketFence tiene soporte para: Microsoft Active Directory, Novell eDirectory, OpenLDAP, Cisco ACS, RADIUS (FreeRADIUS, Radiator, etc.) y local user file).

Estándares soportados:

- 802.1X
- SNMP (Simple Network Management Protocol)

- BRIDGE-MIB, Q-BRIDGE-MIB, IF-MIB, IEEE8021-PAE-MIB
- RADIUS
- Netflow / IPFIX
- WISPR (Wireless ISP Roaming)

REQUISITOS MÍNIMOS DE HARDWARE

- Intel o AMD CPU 3GHz
- 4 GB de RAM
- 100 GB de espacio libre en el disco
- 1 tarjeta de red
- 1 tarjeta de red para alta disponibilidad (opcional)
- 1 tarjeta de red para alta detección de intrusos (opcional)

REQUISITOS MINIMOS DEL S.O.

PacketFence soporta tanto una arquitectura de i386 como de x86_64 en los siguientes S.O.

- Red Hat Enterprise Linux 6.
- CentOS 6.x
- Debian 7.0
- Ubuntu 12.04 LTS

SERVICIOS DEL SISTEMA

Para un correcto funcionamiento de PacketFence los siguientes servicios deben estar ejecutándose correctamente:

- Servicio del Servidor Web (httpd)
- Servicio DHCP (dhcpd)
- Servicio RADIUS (radiusd)
- Servicio Snort/Suricata IDS (snort/suricata)
- Firewall (iptables)

El primer paso después de instalar PackectFence, es la configuración de PacketFence, que nos proporciona una útil y detallada configuración web. Para acceder a la aplicación de configuración solo se tendrá que acceder a la siguiente url: https//Direccion Ip PacketFence:1443/configurator, desde allí, el proceso de configuración se describe a continuación:

Paso 1, figura 1

Se selecciona, la aplicación en línea para la creación del portal cautivo

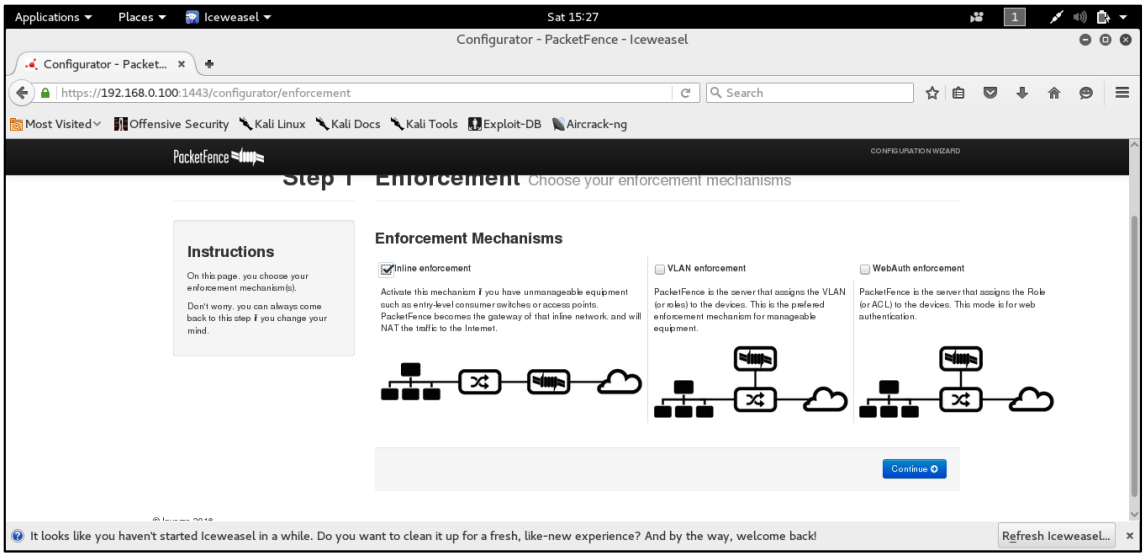

Figura 1: Escenario de configuración de PacketFence

Realizado por: Julio Flores

Paso 2, figura 2, figura 3 y figura 4.

Configuración de la red, en este punto indicaremos las interfaces por las que el servidor PacketFence recibirá las peticiones y en las cuales se aplican las diferentes técnicas de funcionamiento.

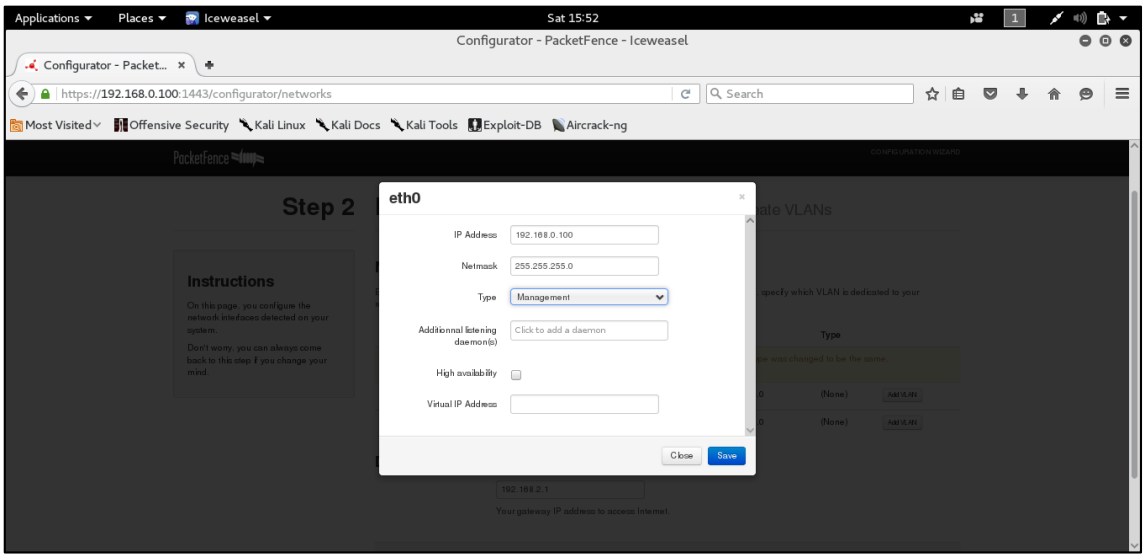

Figura 2: Escenario de configuración de PacketFence

Realizado por: Julio Flores

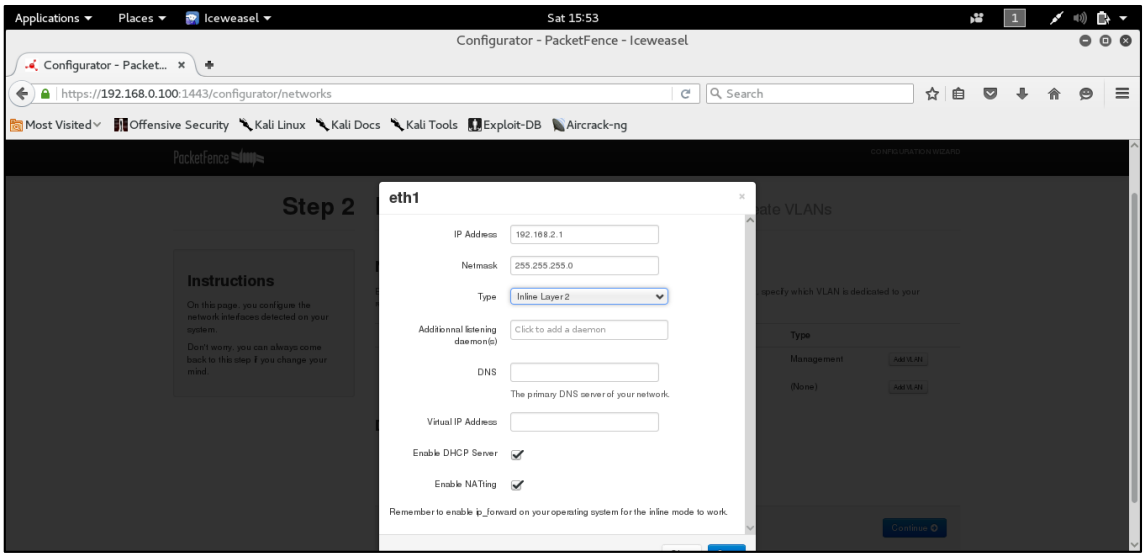

Figura 3: Escenario de configuración de PacketFence

Realizado por: Julio Flores

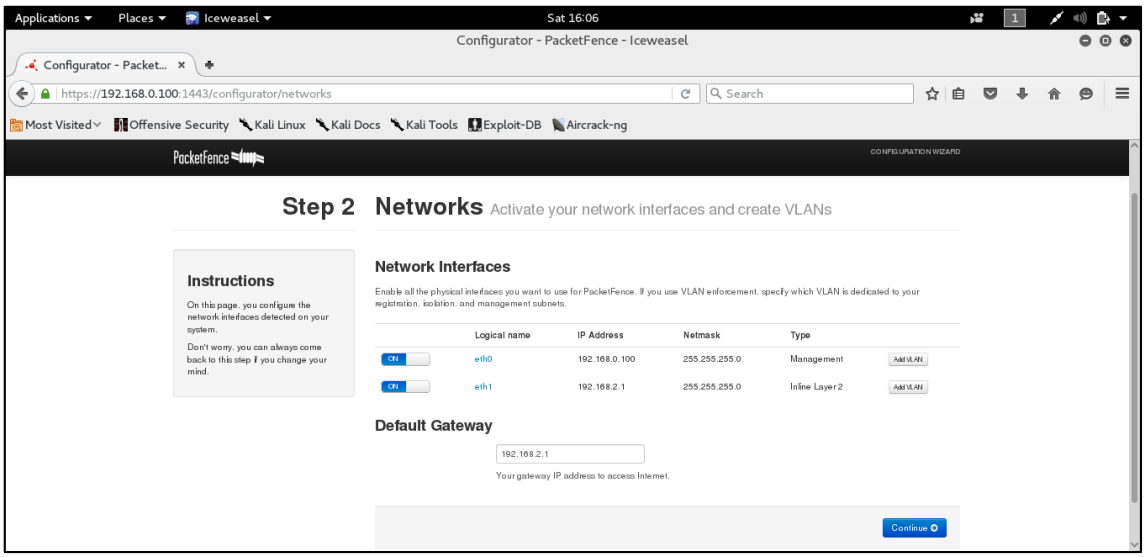

Figura 4: Escenario de configuración de PacketFence

Realizado por: Julio Flores

Paso 3 figura 5, figura 6 y figura 7

Configuración de la base de datos, en este paso PacketFence creará la estructura correcta de tablas y referencias, además de la creación de un usuario para la administración de la base de datos con su respectiva contraseña.

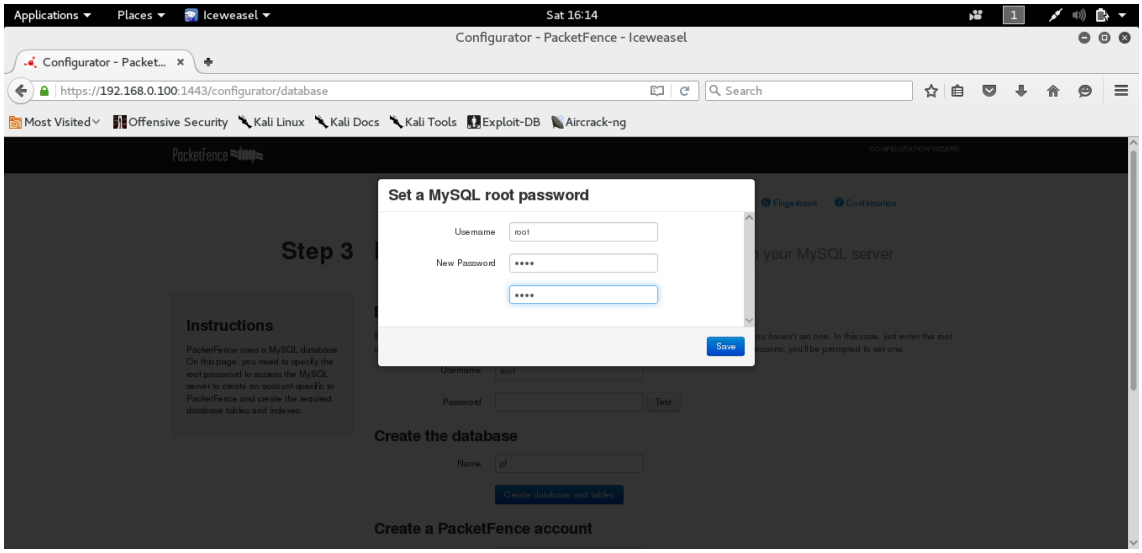

Figura 5: Escenario de configuración de PacketFence

Realizado por: Julio Flores

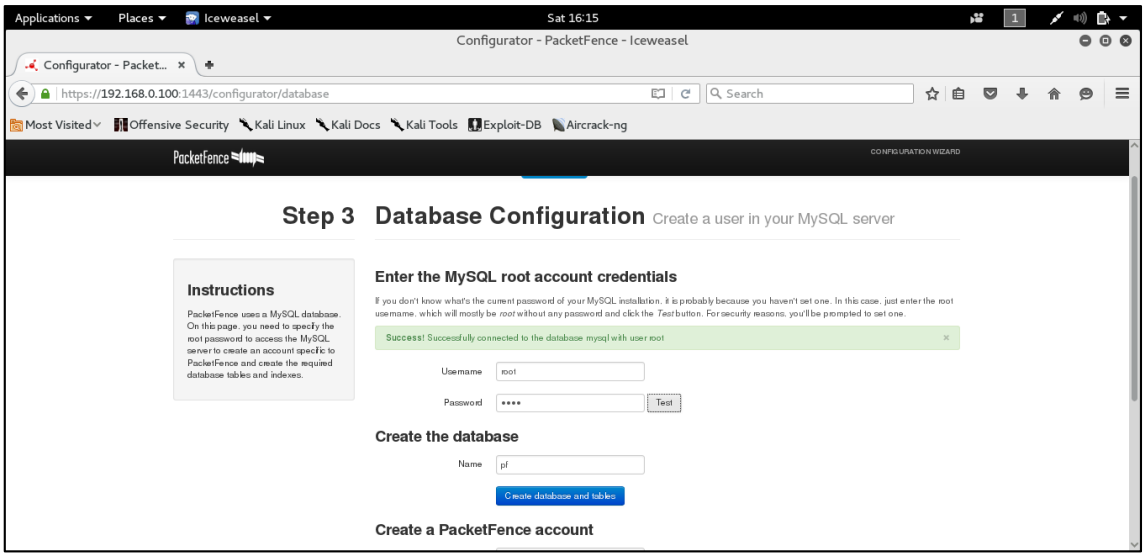

Figura 6: Escenario de configuración de PacketFence

Realizado por: Julio Flores

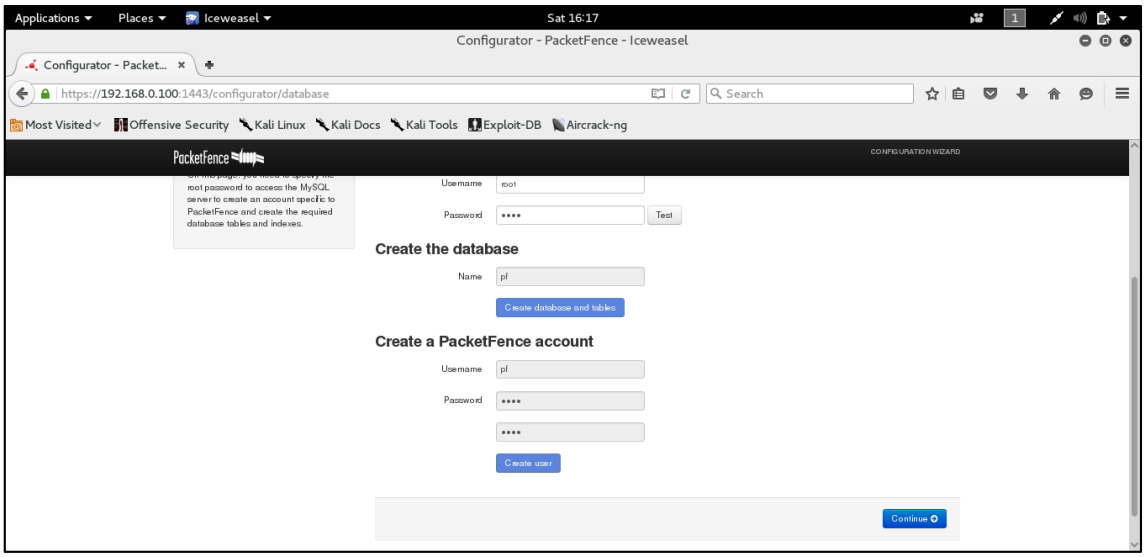

Figura 7: Escenario de configuración de PacketFence

Realizado por: Julio Flores

Paso 4, figura 8

Configuración general de PacketFence tales como el dominio donde estará integrado el sistema, nombre de máquina, definición servidor DHCP, correo de alerta.

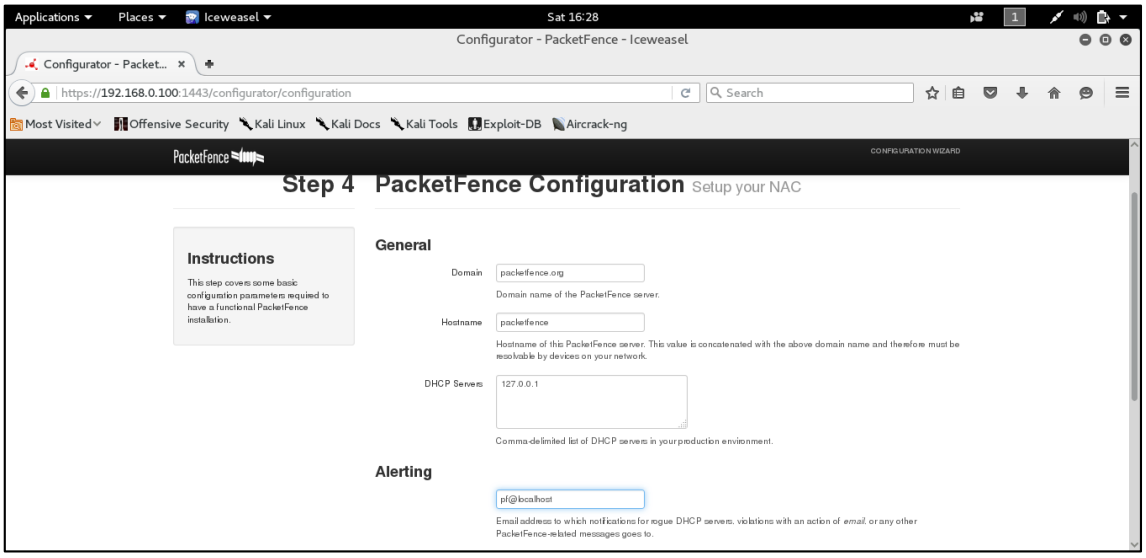

Figura 8: Escenario de configuración de PacketFence

Realizado por: Julio Flores

Paso 5, figura 9.

Creación usuario administrador para acceder a la administración web de los servicios proporcionados por PacketFence.

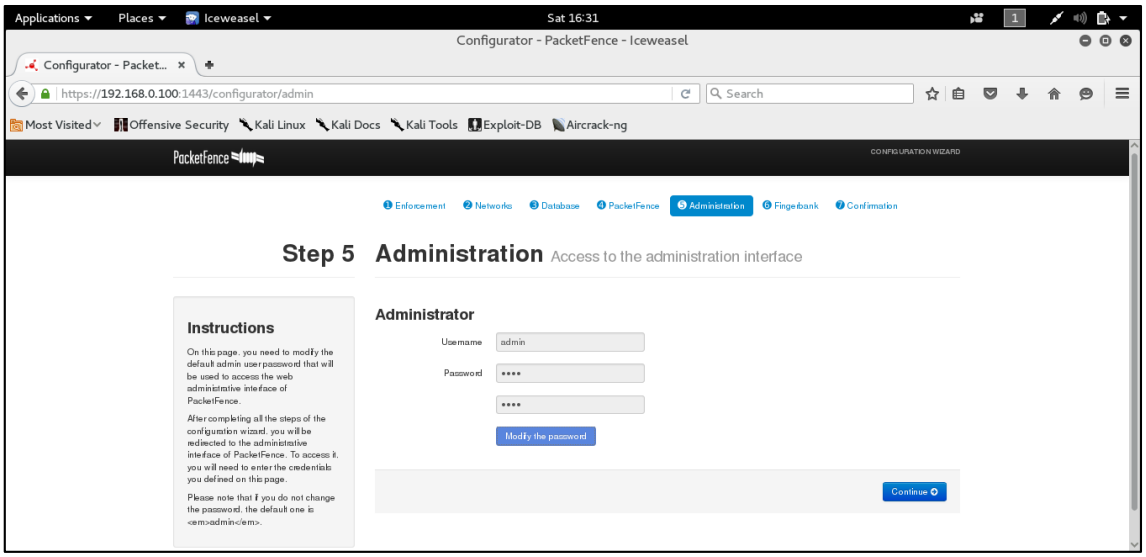

Figura 9: Escenario de configuración de PacketFence

Realizado por: Julio Flores

Paso 6, figura 10, figura 11, figura 12 y figura 13.

Comprobar el estado de la NAC y arranque de los servicios

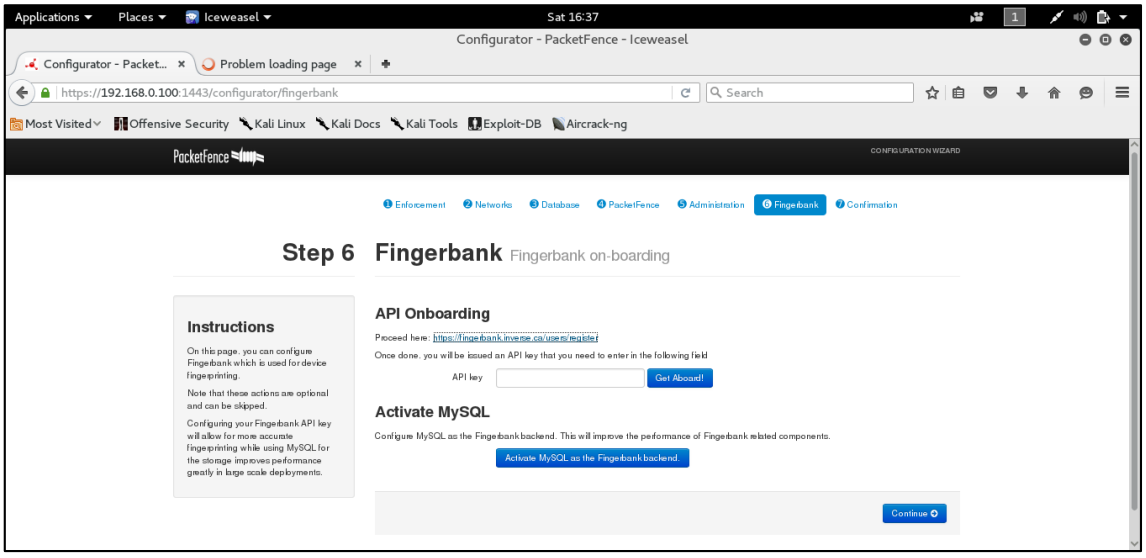

Figura 10: Escenario de configuración de PacketFence

Realizado por: Julio Flores

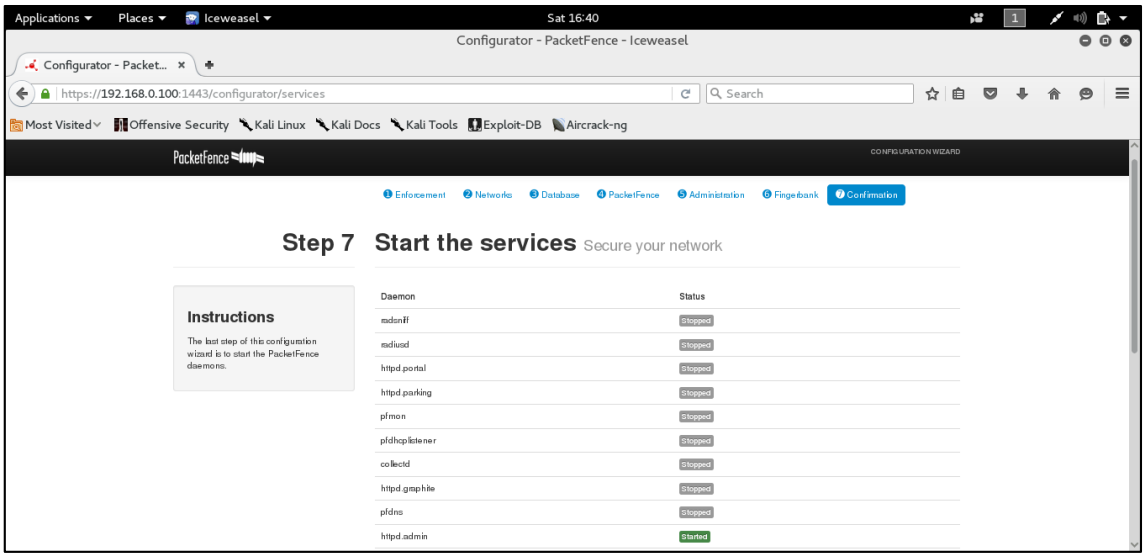

Figura 11: Escenario de configuración de PacketFence

Realizado por: Julio Flores

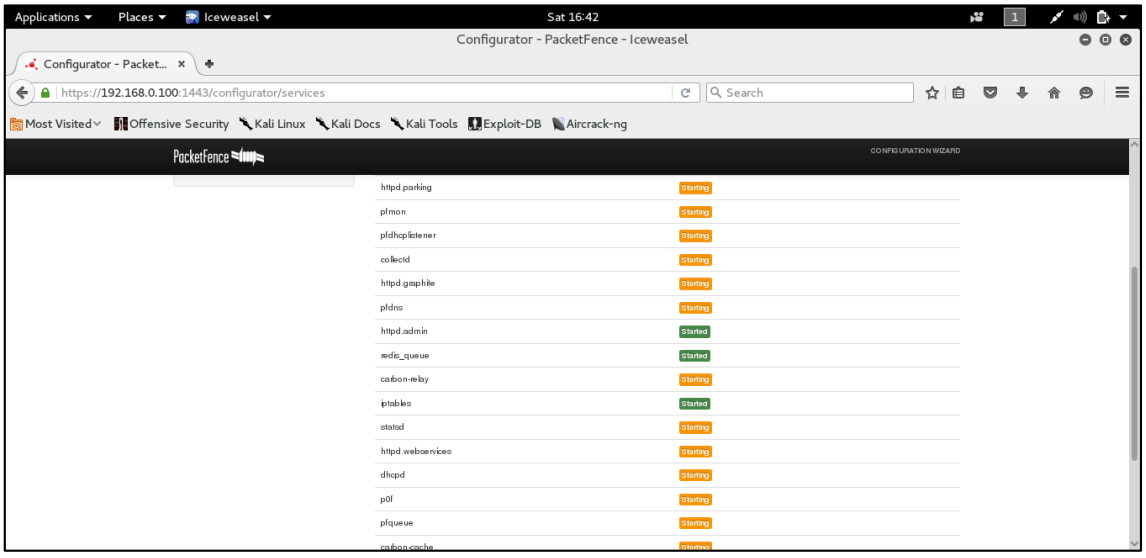

Figura 12: Escenario de configuración de PacketFence

Realizado por: Julio Flores

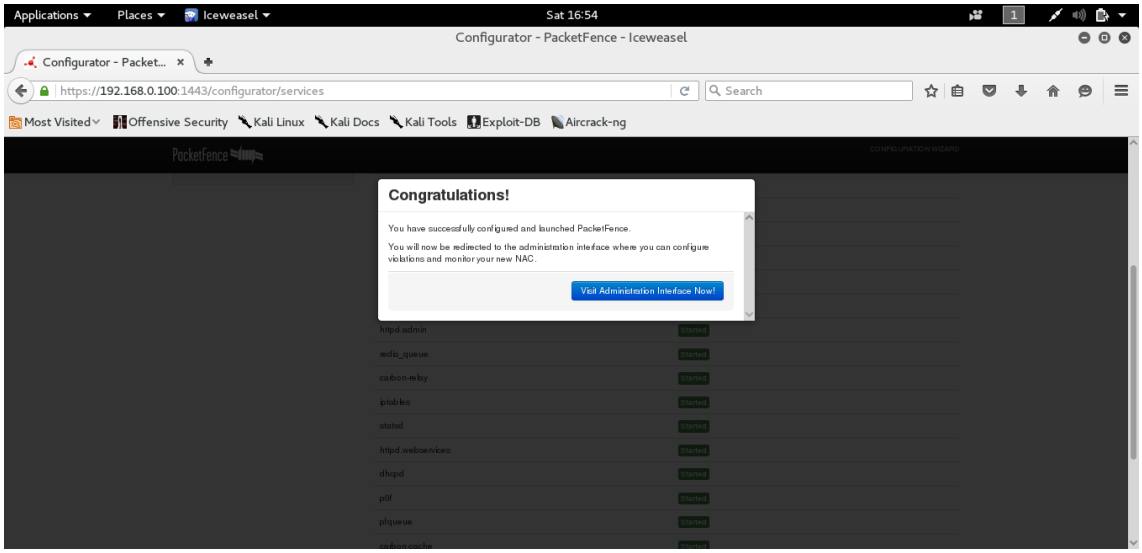

Figura 13: Escenario de configuración de PacketFence

Realizado por: Julio Flores