IMPLEMENTACIÓN DE UN SERVIDOR RADIUS PARA APOYAR LA SEGURIDAD EN UNA RED DE TELECOMUNICACIONES.

CAROLYN STEPHANY JIMENEZ REYES
2063216

MONOGRAFIA PARA OPTAR POR EL TITULO DE INGENIERA ELECTRONICA.

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERIA ELECTRONICA
BOGOTA
2012

IMPLEMENTACIÓN DE UN SERVIDOR RADIUS PARA APOYAR LA SEGURIDAD EN UNA RED DE TELECOMUNICACIONES.

CAROLYN STEPHANY JIMENEZ REYES
2063216

MONOGRAFIA PARA OPTAR POR EL TITULO DE INGENIERA ELECTRONICA.

DIRECTOR
INGENIERO ALVARO ESCOBAR
Docente Facultad Ingeniería Electrónica, Universidad Santo Tomás

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERIA ELECTRÓNICA
BOGOTA
2012

RECTOR GENERAL
Padre Carlos Mario Alzate Montes, O.P.

VICERRECTOR ACADÉMICO
Padre Eduardo Gonzáles Gil, O.P.

VICERRECTOR ADMINISTRATIVO-FINANCIERO
Padre Luis Francisco Sastoque Poveda, O.P.

DECANO DIVISIÓN DE INGENIERÍAS
Padre Pedro José Díaz Camacho, O.P.

DECANO FACULTAD DE INGENIERÍA ELECTRÓNICA
Ingeniera Adriana Cecilia Páez Pino

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Tutor

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 05 julio 2012

AGRADECIMIENTOS

A Dios por darme la oportunidad de culminar esta etapa de mi vida con éxito.

A mi mamá quien me ha impulsado a ser mejor día a día, con sus consejos y su apoyo, me ha entregado fortaleza que en tantas ocasiones he necesitado, convirtiéndose en la persona más importante de mi vida y a la que le debo todo lo que soy.

A mi papá, aunque ya no se encuentre entre nosotros me enseño a no rendirme y luchar por mis sueños, ya que la perseverancia es la clave del éxito, me demostró que todo en la vida fortalece y forja un mejor carácter.

A mis hermanos, por su apoyo incondicional que me impulsa a mejorar con el paso de los días, sin sus consejos y su simple presencia en mi vida no estaría apunto de lograr una de mis metas mas preciadas.

A mis amigos quienes siempre me han brindado una palabra de aliento, han señalado mis errores y celebrado mis triunfos, convirtiéndose en una parte muy importante de mi vida.

A los docentes quienes con su paciencia y dedicación me han ayudado a forjarme como una profesional, segura y competente.

CONTENIDO

LISTA DE FIGURAS

ANEXOS

GLOSARIO

AUTENTICACIÓN: es el proceso de verificar si la identidad de una persona o una máquina es efectivamente la que declara. Busca establecer una relación de confianza entre los interlocutores. [1]

AUTORIZACIÓN: Es el proceso que se usa para realizar la verificación de la integridad de los datos transmitidos, especialmente mensajes.[5]

CHAP: siglas en ingles para (Challenge Handshake Authentication Protocol), Es un método de autentificación remota o inalámbrica, A diferencia de PAP, que sólo autentica una vez, CHAP realiza comprobaciones periódicas para asegurarse de que el nodo remoto todavía posee un valor de contraseña válido. [13]

DALORADIUS: Es básicamente una aplicación avanzada de administración de Radius web, usado para realizar la gestión de puntos de acceso y las implementaciones de proveedor de internet para fines generales.

EAP: Esta versión es basada en el intercambio de una contraseña (pre-shared key). No realiza la actualización dinámica de las claves WEP y por esta razón no es más segura que la norma anterior. La identificación se efectúa en sentido único (solo el usuario de identifica en el P.A) por lo que es susceptible de ser atacada mediante el método "man in the middle". [3]

ENCRIPTACIÓN: codificación la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red. Es por medio de la encriptación informática como se codifican los datos. Solamente a través de un software de descodificación que conoce el autor de estos documentos encriptados es como se puede volver a decodificar la información. [4]

FREERADIUS: servidor que hace uso del protocolo RADIUS para funciones de autentificación, es uno de los servidores más populares y versátiles de este protocolo. [1]

KERBEROS: Es un servicio de autentificación que se desarrollado en el proyecto athena en el MIT. Fue diseñado para abordar el abordar el problema que plantea el hecho de que en un entorno abierto distribuido, los usuarios de las estaciones de trabajo quieran acceder a servicios de servidores distribuidos por toda la red. [5]

MD5: Conocido como el algoritmo de resumen del mensaje, es un algoritmo usado para encriptar mensajes, es decir, encripta el password tecleado por el usuario y es imposible que partiendo desde la cadena encriptada se vuelva a la contraseña origen. Por esto mismo no hay problema de que alguien pueda acceder al campo encriptado de la base de datos. [6]

MySQL: Es un sistema de administración de bases de datos relacionales rápido solido y flexible. Es ideal para crear bases de datos con acceso desde paginas web dinámicas. [7]

NAS: Un Network Access Server es un sistema que proporciona acceso a la red. En algunos casos también se conoce como Remote Access Server (RAS) o Terminal Server. En general, NAS es un elemento que controla el acceso a un recurso protegido. [1]

PAP: siglas en ingles para (Password Authentication Protocol), es un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet, PAP sólo realiza el proceso de autenticación una sola vez. [13]

PHPMYADMIN: Es una herramienta libre escrita en PHP con la intención de manejar la administración de MySQL a través de páginas web, utilizando Internet. [8]

OPENLDAP: Es una implementación de código abierto de LDAP desarrollada por OPENLDAP Project, es multiplataforma existiendo versiones para Linux, Windows, BSD, HP-UX, Solaris, Mac OS X.[9]

RADIUS: Este es un protocolo AAA (Autenticación, Autorización y Administración) para aplicaciones como acceso a redes o movilidad IP. [1]

REGISTRO (accounting): Se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio. [1]

SAMBA: servidor capaz de compartir archivos, compartir impresoras y controlar el acceso a determinados recursos de red con igual o mayor eficiencia que los servidores basados en sistemas operativos de Microsoft. Pero, en este caso, el sistema operativo utilizado es el Linux.[10]

SLAPD: siglas para Stand-alone LDAP Daemon, es el demonio encargado de gestionar las peticiones de directorio OpenLDAP. [11]

SLURPD: siglas para Stand-alone LDAP update replication daemon, es el otro demonio encargado de gestionar las peticiones de directorio OpenLDAP. [11]

SQL: Acrónimo de (Structured Query Language) o lenguaje estructurado de consulta ha sido el que ha tenido mayor desarrollo y difusión, es hoy el lenguaje estándar para trabajar con bases de datos relacionales. [12]

ABSTRACT

With the advancement of technology in the world of telecommunications and the great influence that globalization has had on humanity, the information has become a very precious element that must be carefully kept, is for this reason that the implementation of elements that provide safety is so important, at this document will be possible find a short summary about network security, in addition the detailed explanation of the operation and implementation of a RADIUS server, to make an alternative proposal on a corporative network.

Keywords: AAA, NAS, Radius Server.

RESUMEN

Gracias al avance de la tecnología en el mundo de las telecomunicaciones y a la gran influencia que la globalización ha ejercido en la humanidad, la información se ha convertido en un elemento muy preciado que debe ser resguardado con mucho cuidado, es por esta razón que la implementación de elementos que brinden seguridad es tan importante, en este documento será posible encontrar un breve resumen acerca de seguridad en redes, además de la explicación detallada del funcionamiento e implementación de un servidor Radius, para realizar una propuesta alternativa en una red corporativa.

Palabras claves: AAA, NAS, Radius Server.

1. INTRODUCCIÓN

Con el paso del tiempo se ha observado como la humanidad ha ideado diferentes formas de comunicarse, sin embargo, con las diferentes amenazas a las que la información se encuentra expuesta, las alternativas ofrecidas para garantizar la seguridad de la información han sido numerosas.

Para evitar que la información de principal importancia en cualquier entidad, y las principales transacciones en una red de telecomunicaciones, sean manipuladas o usadas para fines fraudulentos, es vital importancia planear estrategias que permitan brindar seguridad a la red, haciendo uso de equipos, códigos, entre otros; convirtiéndose de cierta forma en una necesidad básica en esta época de expansión de las tecnologías, que en muchas ocasiones se encuentran basadas en Internet.

Es por esta razón que la implementación de nuevas estrategias que brinden seguridad a una red, ya sea corporativa o privada, se hace necesaria hoy en día, ya que si es posible controlar el acceso a estas, será posible también resguardar un poco más la seguridad de dicha red de telecomunicaciones, evitando el uso inescrupuloso de la información, beneficiando no solo a una empresa sino a la comunidad en general, ofreciendo un ambiente más confiable a los clientes y empleados de la compañía, que es el principal objetivo de este proyecto.

Es aquí donde el concepto de servidor de autenticación toma fuerza, ya que este elemento ofrece alternativas de protección en el acceso a una red de telecomunicaciones, a pesar de la existencia de muchas alternativas que cumplen esta función, un servidor Radius cuenta con las condiciones necesarias para cumplir este objetivo, y esta es la razón de ser de este proyecto implementar un servidor con estas características a fin de brindar nuevas alternativas de acceso a una red corporativa.

2. JUSTIFICACIÓN

Existen muchas formas de alcanzar la seguridad en una red, algunas de estas se complementan ya que muchos de los procedimientos existentes para este objetivo no abarcan todas las posibles amenazas a las que las redes se enfrentan hoy en día, un método muy usado en este ámbito es la implementación de servidores de autentificación, que permiten a la red constatar y dar acceso a esta solo a usuarios permitidos, por esta razón el objetivo principal de este proyecto es realizar la implementación de un servidor Radius que permita generar una nueva alternativa de seguridad para una red corporativa determinada.

Con la innovación y el avance del mundo globalizado, la seguridad en la información se ha convertido en uno de los principales preocupantes de la humanidad, ya que este elemento representa el tesoro mas grande de una persona u empresa, es por esta razón que es de vital importancia evitar que esta caiga en manos equivocadas, creando nuevas estrategias de protección y haciendo uso de cada uno de los elementos existentes para lograr dicho fin.

Es en este apartado donde las diferentes formas y alternativas ofrecidas por la tecnología para salvaguardar este elemento juegan un papel muy importante, una de las alternativas más usadas en el mundo de las redes de comunicaciones es el uso de servidores de autenticación, debido a que permiten acceso a la información y a los equipos de una empresa solo a personal autorizando, evitando de esta manera la manipulación y la malversación de cada uno de los elementos de esta.

3. PLANTEAMIENTO DEL PROBLEMA

A medida que el mundo va avanzando y con el su desarrollo tecnológico, se presentan nuevos inconvenientes para poder resguardar uno de los elementos más importantes en esta época, la información, por esta razón es preciso determinar cuáles son las alternativas que se ofrecen en la seguridad de las redes de Telecomunicaciones, y aun más importante ¿Cómo es posible brindar acceso seguro a una red corporativa de telecomunicaciones haciendo uso de un Servidor Radius?

En cualquier compañía o industria, los negocios se realizan o hacen uso en algún momento de una red de telecomunicaciones que puede estar expuesta a diferentes tipos de amenazas, es por este motivo que la implementación de un sistema de control de acceso a estas redes es tan importante, de esta manera podemos establecer diversas estrategias para alcanzar este objetivo, como la implementación de diversos equipos, servidores virtuales, entre otras, que brinden a las personas y/o compañías la posibilidad de mantener un control de acceso a su red de telecomunicaciones logrando que el uso de esta herramienta no caiga en manos equivocadas.

El servidor Radius ofrece la oportunidad de realizar un control de acceso a dicha red de telecomunicaciones, para que solo personal autorizado pueda hacer uso de cualquier información, y de utilizar algunas aplicaciones solo disponibles para usuarios de estas, brindando así una nueva alternativa para asegurar el uso de una red, resguardando así la información básica y de gran importancia.

En Colombia los registros de uso de este tipo de servidores de autenticación son muchos, debido al uso de este sistema para generar seguridad en la red, se encuentran caso tales como la red de Telefónica, Claro y algunas empresas mayoristas que evitan el acceso a sus redes y a sus equipos por medio de este método.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Ofrecer una nueva alternativa de seguridad en el acceso de la red corporativa de la empresa Orange Business Services por medio de la implementación de un servidor de autenticación Radius.

4.2 OBJETIVOS ESPECIFICOS

- Analizar la arquitectura y los componentes de un Servidor Radius.
- Controlar el acceso a la red corporativa de la empresa.
- Presentar una alternativa segura y confiable para garantizar la seguridad en el acceso a una red corporativa.

5. DISEÑO METODOLOGICO

5.1 TIPO DE PROYECTO.

Proyecto Investigacion-accion: Es una modalidad de trabajo que genera conocimiento, que produce cambios y que, en última instancia, es compatible con los otros tipos de proyecto, una Intervención, una evaluación y una investigación pueden desarrollarse bajo una modalidad clásica o convencional y también bajo la modalidad de la investigación-acción, para este caso se hace un proyecto investigación acción, ya que para realizar la implementación del servidor radius se realiza una investigación acerca de cada uno de los componentes de este tipo de servidor de autenticación para de esta forma logar una buena implementación del mismo.

5.2 TIPO DE ESTUDIO.

Se toma como base el estudio exploratorio, realizando una amplia documentación acerca de cada uno de los componentes y factores que contribuyen en la implementación de un servidor de autentificación Radius.

5.3 PERIODO Y LUGAR DE DESARROLLO.

Este proyecto se realizara durante el transcurso del primer periodo del 2012 en la empresa Orange Business Services.

5.4 UNIVERSO Y MUESTRA.

Para la realización de este proyecto se tomara en cuenta la red corporativa de la empresa Orange Business, a fin de crear una nueva alternativa de autentificación para el acceso a la misma.

5.5 MÉTODO.

El método empleado para este proyecto será el teórico practico, ya que este método permite profundizar en el conocimiento de las regularidades y cualidades esenciales de los fenómenos, de esta manera es posible realizar una investigación ardua para lograr implementar un servidor capaz de realizar la autentificación para lograr el acceso a una red de le telecomunicaciones.

6. ORANGE BUSINESS SERIVCES

Orange Business Services ha estado en Colombia desde 1994, y tienen presencia en ocho ciudades de nuestro país tales como son Bogotá, Barranquilla, Bucaramanga, Cali, Cartagena, Medellín, Pereira y San Andrés cubriendo un amplio porcentaje del país.

Esta empresa ofrece el conjunto de datos e IP más completo, realizando integración de sistemas y soluciones de infraestructura de gestión que permiten los procesos de negocios de los diferentes clientes que esta tiene.

Cuenta con experiencia certificada en la prestación de servicios de integración de las necesidades de comunicación complejas, en las que incluyen los servicios de instalación, configuración, adquisición y mantenimiento, ofreciendo de esta manera una solución completa de extremo a extremo para sus clientes.

Entre los convenios que se comparten se encuentra una de las principales con Cisco Systems, permitiéndoles ofrecer soluciones tecnológicas lideres para nuestro clientes, también encontramos acuerdos de asociaciones con otras empresas líderes en tecnología como Nortel, Avaya y Packeteer.

Son miembros del NAP Colombia, siendo uno de los portadores de tráfico de Internet más importantes en el país, cuenta con clientes en diferentes sectores de la economía como son: Finanzas, Industria, Telecomunicaciones, Gobierno y educación.

Entre sus clientes más importantes se destacan la ETB, la Súper intendencia de Notariado y Registro, Carvajal, Banco de Crédito y el Fondo Nacional del Ahorro. También apoyan a grandes compañías multinacionales como lo son Glaxo, Bimbo, Carrefour, Adidas, PWC, y la mayor parte del tráfico de las aerolíneas.

Esta compañía tiene acceso directo a la Red troncal de libre tránsito que significa que los saltos de menor importancia a la red troncal de Internet pública, proporcionando la velocidad, los tiempos de respuesta y calidad de servicio a nuestros clientes. Cuentan con la certificación ISO9001 desde el año 2004 [1]

[1] Tomado de: http://www.orange-business.com/en/mnc2/footer/local/office_colombia/colombia/

6.1 Actividades de la Empresa

Entre las actividades y servicios que ofrece la compañía Orange Business Services se puede encontrar:

* Soluciones de comunicaciones Integrales, con excelente efectividad y seguridad, diseñadas acorde a las necesidades de los clientes, combinando tecnologías fijas, móviles, datos, de voz y servicios multimedia.
* Administración de aplicaciones empresariales mejorando el funcionamiento con diferentes herramientas para optimizar el ancho de banda, priorizar el tráfico y acelerar transferencias de información, además de la creación y administración del Virtual Private Network (VPN), a bajo costo y gran funcionalidad. Soporta la mayoría de tipos de PBX incluyendo análogas, digitales o basadas en IP, sin necesidad de cambiar el equipo conectado, dejando espacio para la migración de tecnologías.
* Soluciones escalables que abarcan una completa Gama de servicios de red relacionados, para ofrecer visibilidad punto a punto y administración de redes LAN y WAN.
* Soluciones para áreas remotas donde la infraestructura terrestre no está completamente desarrollada, haciendo uso de comunicaciones satelitales dejando servicios seguros y confiables.

6.2 Actividades a realizar por el pasante

Una de las principales actividades que desempeña un estudiante que se encuentra realizando su práctica en Orange Business es ofrecer soporte en el área de operaciones de la compañía, concertándose de igual manera en la parte logística, administrativa y técnica, entre estos procedimientos se encuentra la recepción, almacenamiento, entrega de equipos a diferentes clientes, además de la verificación del correcto funcionamiento de los equipos que son regresados en calidad de garantía.

El proceso de entrega de equipos se realiza de dos formas diferentes, una de ellas es la entrega directa a clientes, en la cual luego de constatar los seriales y datos del equipo se genera un acta de salida y entrega de equipos por medio de la plataforma de la compañía CAMALEON[2], para después llevar los equipos a su destino corroborando con el cliente que sea el equipo que se pidió y que esté en

[2] Camaleón es una plataforma que ofrece una base de datos, de los equipos que han ingresado y que han salido de la compañía (Orange Business Services), en esta plataforma se puede encontrar la ubicación del equipo en bodega, fecha de ingreso, fecha de salida, generación de actas de entrada y salida, cliente final del equipo y forma en la que se entrega el equipo, es decir si se entrega en calidad de reventa, activo fijo (CPE), repuesto o custodia.

condiciones de ser usado, para esto se llevan dos copias del acta de salida para ser diligenciadas por el cliente y el practicante, para así dejar un soporte de la entrega satisfactoria del equipo.

La segunda forma de entrega es entregar el activo a los técnicos de la empresa que se encargan de la instalación de los mismos, en este proceso al igual que en el anterior se genera un acta de salida con copia para que esta sea diligenciada por el técnico de la compañía y el cliente final, como este equipó es activo de la empresa se etiqueta con un código OBS, por medio del cual se realiza un control del mismo.

En la parte de recepción de equipos es de suma importancia verificar que estos equipos al momento de su llegada a la empresa contengan los documentos principales de compra y envió (guía aérea, orden de compra) así como comprobar que los datos en los documentos coincidan con los registrados en el equipo, para esto se confirman los seriales registrados en la factura de compra o en la guía aérea, con los que se encuentran detallados en la caja del equipo y en el mismo equipo, una copia de estos documentos debe ser entregada al Ingeniero de Operaciones que se encarga del manejo de equipos, otra debe ser entregada a la coordinadora de logística y comercio exterior de la compañía, para que esta pueda continuar con los procesos tributarios, otra copia de los documentos debe ser entregada en recepción para fines administrativos, por ultimo otra copia debe ser anexada en el registro personal del pasante, de este manera sea más sencillo identificar los equipos a la hora de entregarlos al cliente final. Adicionalmente es responsabilidad del estudiante en práctica escanear la orden de compra del equipo y enviarla por correo electrónico al administrador de la plataforma CAMALEON.

Después de pasadas dos horas, cuando la orden de compra se encuentre registrada en la plataforma, es necesario que el pasante ingrese lo seriales de todas las partes del equipo, y los accesorios que este tenga, tomando en cuenta que algunos de estos elementos no cuentan con un serial definido se remplaza con un N/A, de esta manera se indica en la plataforma la a ubicación exacta del equipo y sus componentes en la bodega de la compañía, para finalizar este proceso se genera un acta de entrada por medio de esta plataforma, para corroborar que este equipo se encuentra ingresado en la empresa, y almacenado en bodega, vale la pena aclarar que si el equipo no se encuentra registrado tampoco será posible realizar una orden de salida del mismo, es por esta razón que este proceso es tan importante.

Otra de las responsabilidades del estudiante en práctica en la compañía, es realizar el soporte físico de equipos activos fijos de la compañía, que han regresado a la empresa como RMA, es decir por garantía debido a fallas en su l

funcionamiento o por daño, el objetivo es verificar si efectivamente el equipo presenta daños o se encuentra defectuoso, después de comprobar el estado del equipo si este se presenta en realidad fallas debe ser enviado como garantía al fabricante, para esto se debe empacar correctamente, generar una nueva acta de salida por RMA o garantía y enviarlo a la sede del fabricante, la reposición del equipo debe llegar en menos de dos semanas, y es labor del practicante recibir nuevamente el equipo y registrar su ingreso normalmente.

Adicionalmente se aplicaron labores de aprendizaje y repaso técnico, realizando prácticas de laboratorio, reforzando los conocimientos del estudiante para plantear soluciones a diferentes proyectos presentados, para lograr este objetivo el practicante cuenta con el espacio, equipos y personal que genera un apoyo fundamental en prácticas relacionadas con routing, switching, y telefonía, logrando un desarrollo academice importante durante el transcurso de la practica empresarial.

Por último forma parte de la practica realizar un proyecto que presente mejoras en el desempeño de las actividades de la compañía, en esta ocasión se decidió optar por un proyecto que brindara una nueva alternativa de seguridad en el acceso a la red corporativa de la compañía, para la realización de este proyecto se recurrió a la investigación de los pro y los contra del uso de un servidor de autenticación, así como también a plantear el diseño del mismo, haciendo uso de los recursos ofrecidos por la compañía.

7. IMPLICACIONES DE LA SEGURIDAD EN REDES PARA LA SOCIEDAD.

Desde el inicio de los tiempos el hombre ha ideado diferentes maneras para comunicarse entre si, bien sea por el simple hecho de mantener relaciones interpersonales, como también para forjar lazos comerciales, pero siempre con el mismo objetivo darle a entender a otras personas que necesidades y que deseos tenia.

Los mecanismos de comunicación utilizados por la humanidad, se observan desde la prehistoria por medio de diferentes hallazgos pictográficos, uso de símbolos y gráficos que ejemplifican las formas de comunicación primitivas, estableciendo de igual manera las primeras formas de intercambio de información en la historia.

Conforme paso el tiempo, las necesidades básicas de la humanidad fueron aumentando, el uso de diferentes métodos de comunicación se fue presentando, partiendo de los egipcios quienes hacían uso de jeroglíficos en sus construcciones monumentales, contando de cierta manera su historia, plasmando su legado, conservando la información por el resto de los tiempos.

Los romanos hacían uso de la encriptación, escribiendo el mensaje con 3 letras del abecedario adelante es decir si la letra correcta para el mensaje era la B se escribía la E, los mensajes romanos nunca pudieron ser des encriptados por el enemigo.

Los métodos para mantener la seguridad de la informacion reaparecieron en la Europa medieval, partiendo de Carlomagno quien hizo uso de la sustitución de letras por símbolos desconocidos, también se hizo uso de este método para evitar los conflictos y malos entendidos entre el papado y las ciudades estado en Italia.

A principios del siglo XX, fue contemplada la posibilidad de resguardar la informacion no solo para fines bélicos sino también hacer uso de estas estrategias en ámbitos empresariales, siendo un tema de amplia discusión entre los teóricos, quienes concluyeron que este tema era tan importante para una empresa como el ámbito productivo, financiero o comercial.

En la actualidad la necesidad de resguardar la informacion, sigue siendo igual de importante como fue en la antigüedad, no solo para evitar conflictos bélicos, si no también para evitar que el uso de informacion financiera en una compañía y/o país caiga en manos de la competencia o en manos equivocadas, es por esta razón que no solo la encripción de mensajes es suficiente, también se hace uso de diferentes estrategias y servicios que evitan la simple manipulación de la informacion sin autorización previa.

Para nadie es un secreto que en el mundo empresarial el uso de redes de telecomunicaciones y de sistemas es de vital importancia para su funcionamiento, independientemente de la actividad económica que estas desempeñen, haciendo uso de esta tecnología para almacenar su informacion, bien sea de procesos de producción, datos administrativos, contabilidad, entre otros, confiando cada uno de estos datos a la red interna de la empresa, haciendo uso de ordenadores, servidores, servicios de internet entre otros.

El amplio uso de las tecnologías de las telecomunicaciones en el mundo, es sin lugar a dudas, uno de las principales razones por las que es de vital importancia reguardar la seguridad en las redes, en Colombia cada día se hace mas común el uso de estas tecnologías desde pequeñas empresas compuestas por no mas de 15 trabajadores hasta grandes Multinacionales

El mal uso de la información puede traer consigo diversas consecuencias, situaciones de crisis que pueden atentar contra la sostenibilidad operativa, económica de una empresa, poniendo en riesgo no solo información de carácter económico, sino también información personal, cuentas, extractos y claves bancarias, información sobre propiedades y otros bienes que en manos equivocadas puede generar fraudes.

Este tipo de situaciones deben ser prevenidas de raíz, evitando que personas no autorizadas accedan a la información almacenada en la red corporativa de la empresa, así como también evitar la edición de esta, es así como se crean diferentes alternativas útiles en el mundo empresarial, la encriptación de archivos, programas que eviten la infiltración de virus y agentes adversos, o simples servidores de autenticación que evitan a toda costa el acceso a personal no autorizado a la red, beneficiando de esta manera no solo a la empresa y a sus empleados sino también beneficiando a los clientes de la empresa, y al publico en general, basándose de esta manera en el principio de privacidad, ofreciendo un ambiente más confiable a todos las personas implicadas en la empresa, siendo este uno de los principales objetivos de este proyecto.

8. SEGURIDAD EN REDES

Para la protección de la información es necesario establecer diversas estrategias, como la implementación de algunos equipos, servidores virtuales, entre otros; por esta razón uno de los principales objetivos de este proyecto es lograr la implementación de un servidor Radius que consiga brindar seguridad a una red evitando así que la información que es de vital importancia para una organización caiga en manos equivocadas, sin embargo para realizar un correcto planteamiento de este proyecto, es necesario tener en claro el concepto de seguridad en redes, los ataques a los que estas se encuentran expuestas y las alternativas existentes para contrarrestarlos, por esta razón se hace un breve resumen acerca de cada uno de estos ítems.

8.1 SEGURIDAD DE LA INFORMACIÓN.

Es importante conocer que la seguridad de la información en un determinado ámbito laboral se puede clasificar de la siguiente manera:

* Seguridad de computadores.
* Seguridad de red.

Para garantizar la seguridad en un computador existen diferentes elementos ampliamente usados sin embrago uno de los elementos más usados es el firewall por medio del cual se evita el ingreso de agentes externos al equipo, además del uso de antivirus y anti espías que evitan que este tipo de agentes dañinos acedad a la información almacenada en el equipo.

En una red de telecomunicaciones el hacer uso de este tipo de elementos, en los equipos que la componen, no garantiza de ninguna manera que en el intermedio no existan agentes que violen la privacidad de la red, es por esta razón que una de las principales estrategias para resguardar la información de la red es la implementación de sistemas de autenticación inicial de esta manera se evita el acceso de agentes remotos no autorizados a los equipos conectados a la red y a la red en general.

Sin embargo el tema a tratar en este documento es netamente la seguridad en redes.

8.2 ASPECTOS DE LA SEGURIDAD DE LAS REDES DE TELECOMUNICACIONES

La seguridad de las redes de comunicaciones se puede organizar en tres ítems de suma importancia, sin embargo en este apartado solo vale la pena considerar los servicios de seguridad:

* Servicios de seguridad. Un adecuado plan de seguridad de redes debe comprender los elementos que conforman una arquitectura de servicios de seguridad tales como son:

  Autentificación: Es el proceso de verificar la identidad de los usuarios antes de dejarlos ingresar al sistema.

  Control de acceso: Su función es proteger contra accesos no autorizados a cualquier recurso.

  No repudiación: Es el proceso con el que se obtiene una prueba irrefutable de la identidad del emisor, así como de la integridad de los datos recibidos y/o enviados.

8.3 ATAQUES A LA SEGURIDAD

Entre los tipos de ataques a las redes de comunicaciones se encuentran:

Interrupción: se presenta cuando se pierde una parte del sistema o este no está disponible o simplemente no puede usarse. Es decir cuando se presenta la destrucción física de un equipo, el borrado de una aplicación o de un archivo de datos, una falla del sistema operativo.

Intercepción: Se habla de intercepción cuando una persona no autorizada logra acceder al sistema. Puede ser una persona o un programa cualquiera, en casos como la reproducción ilícita de archivos o de la intercepción de cables para sacar los datos de una red. Como no se pierden datos es muy difícil detectar este tipo de ataques.

Modificación: Se presenta cuando alguien no autorizado accede a la información del sistema y la modifica. Dicha persona puede cambiar valores en una base de datos o llegar a alterar un programa para que realice operaciones adicionales.

Fabricación: Se presenta cuando alguien no autorizado crea y añade objetos a un sistema de cómputo, insertando registros a una base de datos existente o añadiendo transacciones a un sistema de comunicación de redes[3].

8.4 CONTROL DE ACCESO

Generalmente, los esfuerzos en materia de seguridad están enfocados en prevenir intrusiones entre la red privada e Internet, por ejemplo, con un firewall, que se encuentra diseñado para bloquear el acceso no autorizado y que permite al mismo tiempo realizar comunicaciones autorizadas. La seguridad de las estaciones de trabajo se limita seguido a un sólo antivirus. Este enfoque considera que todos los problemas de seguridad se originan en el exterior, y por lo tanto, se recurre a asegurar el perímetro externo, mientras se les permite a los usuarios internos el fácil acceso a los recursos de red.[4]

Una de las principales amenazas para una red es la intromisión y el acceso de personas inescrupulosas a la misma, es por este motivo que en el mercado global existen diferentes alternativas solucionar este inconveniente, entre las cuales se encuentra la implementación de servidores de autenticación, el uso de equipo que prevengan la intromisión, sin embargo la implementación de estos equipos adquisición es muy costosa.

A continuación es posible encontrar una descripción detallada de algunos métodos para garantizar la seguridad en una red, partiendo de los equipos ASA de Cisco especializados en este tema, y los diferentes servidores de autenticación más utilizados en la industria.

8.4.1 Equipos ASA de Cisco**.**

Cisco ASA es una nueva línea de dispositivos de Cisco Systems que integra un sistema que se encuentra diseñado para bloquear el acceso no autorizado, permitiendo simultáneamente comunicaciones autorizadas, enfocándose en la seguridad para comunicaciones unificadas (Voz y Video), enlaces de VPN SSL y IPsec, brindando servicios de prevención de intrusos y servicios de seguridad en contenidos, todo en un flexible y modular producto.

En el caso de Cisco ASA los modelos existentes corresponden a la serie 55xx.

---

[3] ALCOCER, Carlos. Redes de computadoras, En: Seguridad de redes de Computadoras, capitulo 24

[4] Tomado de: http://freenac.net/es/solutions/lanaccesscontrol

Hay cuatro versiones Enterprise: Firewall, IPS, Anti-x y VPNs; y una versión Business para empresas medianas y pequeñas. Un total de 5 modelos.

Todos los ASA operan con el software ASA versión 7.2.2 con una interfaz más cercana al Cisco IOS que PIX OS.

Estos dispositivos incluyen servicios de prevención de intrusiones (IPS) y concentrado de VPNs. Es por esto que Cisco Systems indica que un ASA realizar por sí solo las tareas que hasta ahora requerían 3 dispositivos separados: un firewall PIX, un VPN (como el VPN 3000) y un IPS como el Cisco IPS 4000. [5]

Figura 1 Equipo ASA de Cisco Systems

Fuente: Cisco Systems Catalog. [6]

8.4.2 Servidores de autenticación.

Un servidor de autenticación es un dispositivo que controla quién puede acceder a una red de telecomunicaciones y quien no. Los objetivos son la autorización de autenticación, la privacidad y no repudio

Autorización: Es la encargada de determinar qué objetos o datos de un usuario puede tener acceso a la red, si estos existieran.

Privacidad: se encarga de mantener la información se divulgue a personas no autorizadas.

---

[5] tomado de Fuente: medio virtual: http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html

[6] tomado de: medio virtual http://librosnetworking.blogspot.com.br/2007/02/cisco-pix-cisco-asa.html

No repudio: Por lo general es un requisito legal y se refiere al hecho de que el servidor de autenticación puede registrar todos los accesos a la red junto con los datos de identificación, de manera que un usuario no puede repudiar o negar el hecho de que él o ella ha tenido o modificado el datos en cuestión.

Después de determinar que el mejor camino para brindar seguridad, en el acceso a una red corporativa es la implementación de un servidor de autenticación, es necesario conocer qué tipo de servidor se va implementar, por este motivo se hace un estudio de cada una de las opciones disponibles, A continuación se encuentra un breve resumen con las principales características de algunos servidores de autenticación.

Algunos Servidores de Autenticación**.** Los Servidores de autenticación se presentan de muchas formas diferentes. Este software de control de autenticación puede encontrase en un servidor de acceso a la red, una pieza de router o de otro tipo de hardware para controlar el acceso a esta, o algún otro punto de acceso de red. Independientemente del tipo de máquina que aloja el software de autenticación, el término servidor de autenticación sigue siendo generalmente utilizado para referirse a la combinación de hardware y software que cumple la función de autenticación. [7]

Además de las variaciones en el hardware, hay un número de diferentes tipos de algoritmos lógicos que pueden ser utilizados por un servidor de autenticación. El más simple de estos algoritmos de autenticación es generalmente considerado como el uso de contraseñas. En una aplicación sencilla, el servidor de autenticación sólo puede almacenar una lista de nombres de usuario válido y la contraseña correspondiente, y autenticar todos los usuarios que intentan conectarse a la red de acuerdo a esta lista.

* Kerberos. Kerberos es un protocolo de autenticación de red que le permite a un computador o a un equipo de telecomunicaciones, demostrar su identidad a otro a través de una red poco segura mediante un intercambio de mensajes encriptados.

  Una vez verificada la identidad, Kerberos proporciona a las dos equipos llaves de encriptación para una sesión de comunicación segura. Este servidor de autenticación fue desarrollado en el Instituto Tecnológico de Massachusetts (MIT) en la década de los '80s. Le pusieron el nombre del perro guardián de tres cabezas en la mitología griega que vigilaba las puertas del Hades (infierno).

[7] tomado de Fuente: medio virtual: http://lular.es/a/Internet/2010/08/Que-es-un-servidor-de-autenticacion.html

El nombre es apropiado pues Kerberos es un proceso de tres vías, que depende de un servicio de terceros llamado Key Distribution Center (KDC, o Centro de Distribución de Llaves) para verificar la identidad de una equipo por otro y para establecer llaves de encriptación para permitir una conexión segura entre las dos.

Kerberos funciona porque cada equipo comparte un secreto con el KDC, que consta de dos componentes: un servidor de autenticación Kerberos y un servidor otorgador de tiquetes. Si un KDC no conoce el servidor destino solicitado, remite la transacción de autenticación a otro KDC que sí lo conoce.

Mediante el intercambio de una serie de mensajes encriptados, denominados "tiquetes", con el cliente, el KDC genera nuevas llaves de encriptación para cada etapa del proceso de autenticación. Puede verificar con éxito una computadora para otra sin comprometer las llaves secretas de ninguna de las dos y sin requerir que cualquier computadora almacene llaves para cada computadora con la cual eventualmente podría conectarse. Los tiquetes sirven únicamente para una computadora específica que se conecta a otra computadora específica durante un determinado lapso de tiempo.

Después de emitido el tiquete, el cliente puede usarlo para tener acceso al servidor destino las veces que quiera hasta que expire el tiquete. Ni el cliente ni nadie fisgoneando en la red puede leer o modificar un tiquete sin invalidarlo**.**[8]

* OpenLDAP**.** OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP.

  La aplicación de servidor LDAP proporciona funcionalidad de Servicios de Directorio a ordenadores Windows de una forma muy similar a los servicios de Microsoft Active Directory. Tales servicios incluyen gestionar las identidades y las relaciones entre los ordenadores, usuarios y grupos de ordenadores o usuarios que participan en la red, y proporcionan una forma consistente de describir, localizar y gestionar esos recursos. La implementación de libre distribución disponible en su sistema de libre se llama OpenLDAP. Los demonios de servidor responsables de gestionar las peticiones de directorio OpenLDAP, y la propagación de datos de directorio entre un servidor LDAP y otro Linux, son SLADP y SLURPD.

  OpenLDAP puede usarse junto con SAMBA para proporcionar servicios de Archivo, Impresión y Directorio prácticamente de la misma forma que un

[8] tomado de Fuente: medio virtual: http://sistemas_operativos.galeon.com/kerberos.htm

Controlador de Dominio de Windows, si se compila SAMBA con soporte LDAP

OpenLDAP no tiene nada que envidiarle al Microsoft Active Directory, las herramientas están ahí, sólo hay que saberlas implementar y administrar, lo que sería su único costo (tiempo y paciencia). [9]

* Servidor Proxy. Un servidor proxy es un servidor o un equipo que intercepta las peticiones y de una red interna y una red externa, como la Internet. Los servidores proxy a veces actúan como servidores de autenticación, además de un número de otras funciones que pueden cumplir. Hay muchas opciones diferentes que pueden ser utilizados para implementar los servidores de autenticación, incluyendo hardware, sistema operativo, y los requisitos de paquete de software. Como tal, suele ser importante para una organización a analizar a fondo los requisitos de seguridad antes de implementar un servidor de autenticación en el entorno de red. [10]

* Radius. RADIUS (Remote Authentication Dial-In User Server) es un protocolo que permite gestionar la "autenticación, autorización y registro" de usuarios remotos sobre un determinado recurso. La tupla "autenticación, autorización y registro" es más conocida como AAA, al ser éste su acrónimo de su denominación original inglesa "Authentication, Authorization, and Accounting" [11]

  RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie Port Master de sus Servidores de Acceso a la Red (NAS), más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes). RADIUS es extensible; la mayoría de fabricantes de software y hardware RADIUS implementan sus propios dialectos. [12]

  Muchos ISP requieren que se ingrese un nombre de usuario y contraseña para conectarse a la red. Antes de que el acceso a la red sea concedido, los datos de acceso son pasados por un dispositivo NAS (Network Access Server) sobre un protocolo de capa de enlace, luego hacia un servidor RADIUS sobre un

---

[9] tomado de Fuente: medio virtual: http://sistemas_operativos.galeon.com/kerberos.htm
[10] tomado de Fuente: medio virtual: http://windows.microsoft.com/es-ES/windows-vista/What-is-a-proxy-server
[11] tomado de: medio virtual http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf
[12] tomado de Fuente: medio virtual http://isabelchancayauri.blogspot.com/2010_08_01_archive.html

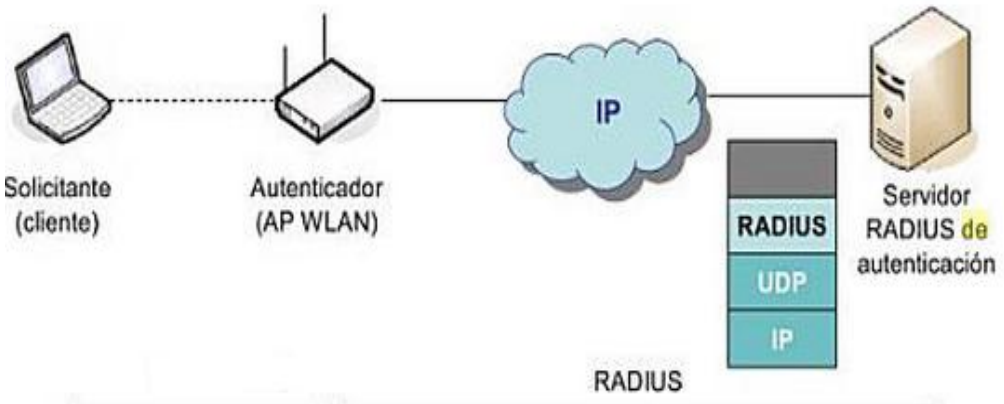
protocolo RADIUS.

El servidor RADIUS chequea que esa información sea correcta usando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptada, el servidor autorizará el acceso al sistema del ISP y seleccionará una dirección IP, parámetros L2TP, etc.

RADIUS también es comúnmente usado por el NAS para notificar eventos como:
* El inicio de sesión del usuario.
* El final de sesión del usuario.
* El volumen de datos transferidos durante la sesión.
* El total de paquetes transferidos durante la sesión.
* La razón para la terminación de la sesión [13]

Existen muchos modelos de aplicación de un servidor Radius en una red una de estas es la presentada en la Figura 2.

Figura 2 modelo de implementación de un servidor Radius



Fuente: Fundamentos y Aplicaciones de seguridad en redes WLAN: De la teoría a la práctica, Izaskun Pellejero, Fernando Andreu, Amaia Lesta [14]

8.4.3 Análisis de cada alternativa.

La autorización concede derecho a un usuario para acceder a un recurso. El control de acceso es el medio de hacer cumplir esas autorizaciones. En general, se puede afirmar que el control de acceso es el método empleado para prevenir el

[13] Tomado de: http://www.alegsa.com.ar/Dic/radius.php
[14] Tomado de: Fundamentos y Aplicaciones de seguridad en redes WLAN: De la teoría a la práctica, Izaskun Pellejero

uso no autorizado de los recursos.

Existen dos métodos para prevenir los accesos no autorizados:

* Filtro de las solicitudes de acceso: Verifica los derechos de un usuario respecto a un recurso, cuando el usuario intenta acceder a éste.
* Separación: Evita cualquier intento de acceso por parte de los usuarios no autorizados [15]

En el momento de determinar que alternativa de seguridad de acceso será implementada y por qué, es necesario no solo conocer el funcionamiento de cada una si no que también determinar cuales son sus ventajas y sus desventajas, es por esta razón que a continuación se analizaran cada una de ellas.

8.4.3.1 Servidor Kerberos.

* Ventajas de Kerberos*.* Elimina la transmisión de contraseñas encriptadas en la red, lo que permite eliminar eficazmente las amenazas de los husmeadores en la red, así el uso de rastreadores también llamados analizadores de paquetes, no tiene ninguna utilidad*.*

* Desventajas de Kerberos. A pesar de sus grandes ventajas Kerberos presenta muchas dificultades para su implementación entre ellas:

  Puede ser complicado enviar las contraseñas de los usuarios de una base de datos UNIX estándar, ya que desafortunadamente no existe ningún mecanismo automatizado para realizar este proceso, lo que complica un poco el diseño del servidor, además Kerberos supone que a pesar que cada usuario es confiables este usa una red o un equipo que no lo es, por lo que si alguien más tiene acceso al único equipo que envía los comprobantes utilizados para la autenticación, todo el sistema corre riesgo.[16]

8.4.3.2 Servidor OpenLDAP**.**

Ventajas del servidor OpenLDAP. La ventaja principal de usar este tipo de servidor es la compilación de cierto tipo de información en el interior de una empresa. Por ejemplo, todas las diferentes listas de usuarios en el interior de una empresa pueden ser unidas en un solo directorio LDAP. Este directorio, puede ser

[15] tomado de: http://biblioteca.pucp.edu.pe/docs/elibros_pucp/alcocer_carlos/24_Alcocer_2000_Redes_Cap_24.pdf

[16] Tomado de: http://docs.fedoraproject.org/es-ES/Fedora//html/Security_Guide/sect-Security_Guide-Kerberos.html

consultado desde cualquier aplicación LDAP-enabled a la que le sirva la información y también podrá ser utilizado por los usuarios que necesiten información sobre él.

Otras ventajas de OpenLDAP es que es sencillo de implementar además de la coherencia de sus API. Lo cual significa que el número de aplicaciones y de gateways que disfruta LDAP puede crecer en el futuro.

Desventajas del servidor OpenLDAP. El lado negativo es que si se desea utilizar OpenLDAP, debe usar un cliente LDAP-enabled o pasar a través de un gateway LDAP, y aunque se presume que la presencia de LDAP aumentara en el futuro por ahora, no existen muchas aplicaciones de las que disfrutar. Además, OpenLDAP soporta solo algunos controles en el acceso, y no todos los aspectos de la seguridad incluidos en otras alternativas.[17]

8.4.3.3 Servidor Proxy.

Ventajas del Servidor Proxy.

* Control. S e pueden limitar los derechos de los usuarios permitiendo solo al proxy realizar el trabajo real.
* Velocidad. Cuando más de 2 usuarios quieren acceder a la misma informacion o recurso, el proxy guarda la respuesta, lo que le permite entregarla directamente cuando sea solicitada nuevamente, logrando terminar su labor más rápido.
* Filtrado. El proxy se negará a dar respuesta a algunas peticiones si este detecta que están prohibidas.

Desventajas del Servidor Proxy

* Abuso. Puede realizar labores que no le corresponden, por lo que es muy difícil que determine quien puede acceder a sus servicios y quien no.
* Carga. Un proxy hace el trabajo de una gran cantidad de usuarios.
* Intromisión. Debido a que es un paso más entre el origen y destino, muchos usuarios no desean hacer uso de este, sobretodo por su función de guardar copia de los datos generando de cierta manera inseguridad en el usuario.
* Incoherencia. Puede cometer algunas equivocaciones si hace el uso del almacenamiento de datos, entregando datos antiguamente guardados y no actualizados. [18]

[17] Tomado de: ftp://archive.download.redhat.com/pub/redhat/linux/7.0/en/doc/RH-DOCS/rhl-rg-es-7.0/s1-ldap-procon.html
[18] Tomado de: http://era-tecnologica.blogspot.com.br/2009/07/ventajas-y-desventajas-del-servidor.html

8.4.3.4 Servidor Radius.

Ventajas del Servidor Radius.

Al implementar el servidor RADIUS, sus clientes solo deben implementar comunicación con este sin necesidad de hacer uso directamente de otras alternativas AAA tales como son Kerberos, CHAP, LDAP entre otros.

Nunca transmite las contraseñas directamente por la red, en su comunicación con NAS, ni siquiera al usar PAP, sino que usa algoritmos para ocultar las contraseñas como MD5.

Desventajas del Servidor Radius.

Como MD5 no es considerado como un sistema de protección de credenciales muy seguro, se aconseja hacer uso de otros sistemas adicionales para protección y cifrar el tráfico de RADIUS, como puede ser túneles de IPsec. [19]

Después de analizar cada una de estas opciones a profundidad, se decidió hacer la implementación de un servidor Radius, ya que es la forma más confiable, económica y sencilla en cuanto operación para el usuario, de brindar seguridad en su red de telecomunicaciones.

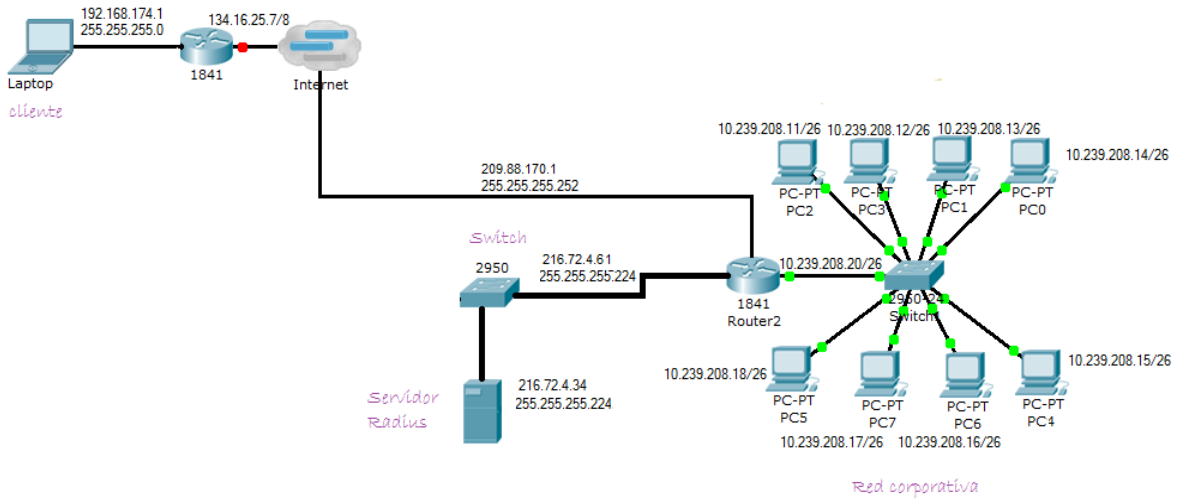
[19] Tomado de: http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

9. CONFIGURACION SERVIDOR RADIUS

Para la realización de este proyecto se planteo un esquema desarrollo comprendido de la configuración del servidor Radius virtualizado en un servidor de la compañía, usando de igual forma un Switch que servirá de punto de acceso a la red, y un equipo que actué como cliente para las pruebas finales.

En la figura 3 es posible apreciar el esquema de diseño de este proyecto.

Figura 3 Esquema de implementación del servidor Radius



Fuente: Autor

Para la configuración del punto de acceso se uso un switch cisco Catalyst 2950 de 48 puertos tal como se muestra en la figura 3 configurado para este fin, haciendo uso de una interfaz de Vlan para poder configurar la dirección IP de este punto de acceso, se asigna esta IP a la interfaz para poder administrar este dispositivo por medio de telnet.

A pesar de las diferentes alternativas que se ofrecen hoy para la instalación de un servidor de autenticación basado en el protocolo Radius, el FreeRadius Server se presenta como la alternativa mas viable y segura para esta labor, ya que es altamente flexible y configurable lo que lo hace el mas usado en la actualidad.

Para la configuración del este servidor se hizo uso del software Freeradius Server 2.1.12, este es un paquete de software de código abierto y libre distribución que implementa diversos elementos relacionados con RADIUS, tales como una

biblioteca BSD para clientes, módulos para soporte en apache, entre otros.

9.1 FREERADIUS SERVER

El servidor de FreeRadius es modular, para facilitar su extensión, siendo de igual manera muy escalable, entre sus principales ventajas encontramos:

- Puede acceder y almacenar la Información haciendo uso de diferentes bases de datos, entre ellas: LDAP, SQL.
- Soporta diversas variedades de clientes Radius entre ellos ChilliSpot, JRadius, mod_auth_radius, pam_auth_radius, Pyrad, extensiones php de RADIUS
- Se puede ejecutar en múltiples sistemas operativos tales como Linux (Debian, Ubuntu, Suse, Mandriva, Fedora Core), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin.[20]

9.2 CONFIGURACIÓN DEL SERVIDOR

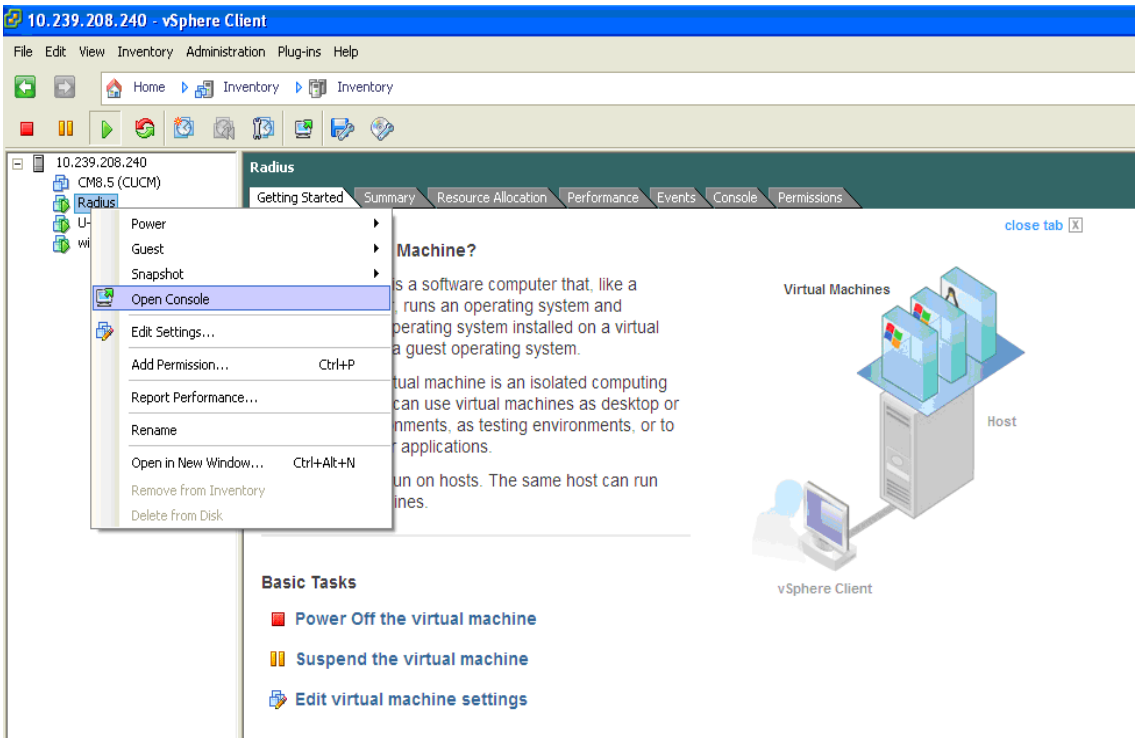
Para la configuración del servidor se decidió hacer uso del software Freeradius sobre Ubuntu 11.04 (ver anexo 1 para especificaciones), para que desde aquí sea posible realizar la autentificación a un punto de acceso definido configurado para que sea cliente de este servidor.

En este caso por fines prácticos se realizo la implementación de una maquina virtual en la cual es posible encontrar instalado Ubuntu 11.04, para acceder a la maquina virtual sencillamente se hace uso el programa Vmware vSphere Client (Ver anexo 2*), en el cual simplemente debe colocar dirección IP, User name, y password.

Después de ingresar a la plataforma de Vmware se procede a ingresar a la maquina virtual, entrando a la consola tal como se muestra en la figura 4, para después hacer uso de esta en la configuración principal del servidor.

[20] Tomado de: http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

Figura 4 ingreso a la maquina virtual



Fuente: Autor

9.2.1 Instalación y configuración de freeradius Server.

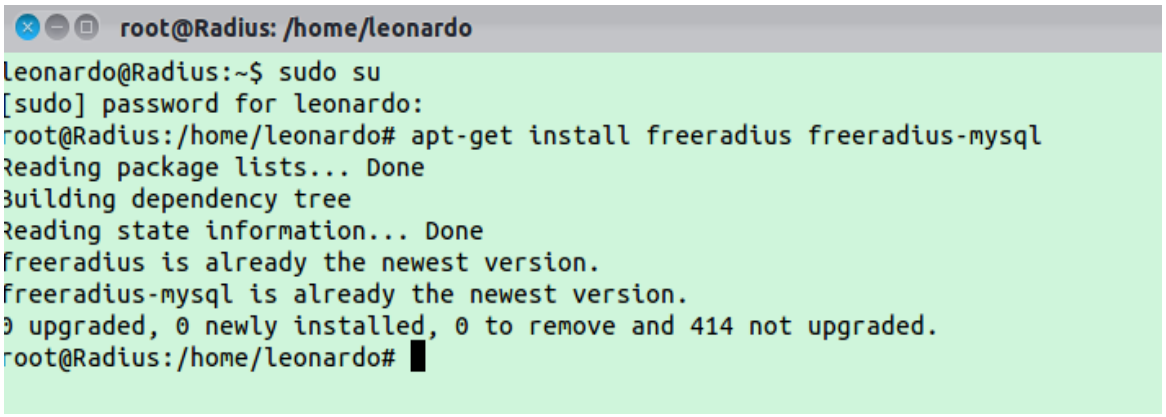
Como primera medida para la Configuración del servidor Radius, es necesario realizar la instalación de freeradius Server, vale la pena aclarar que la Configuración deberá ser realizada en su totalidad en el terminal de Ubuntu 11.04 en este caso.

Es necesario asegurar una conexión a Internet para poder descargar este software, desde modo se realiza el registro como usuario root usando el comando sudo su, se digita la contraseña y se procede a realizar la adquisición e instalación del freeradius Server:

root@Radius:/home/Leonardo# apt–get install freeradius freeradius-mysql

En la figura 5 se muestra la instalación de freeradius en Ubuntu 11.04

Figura 5 instalación de freeradius en Ubuntu



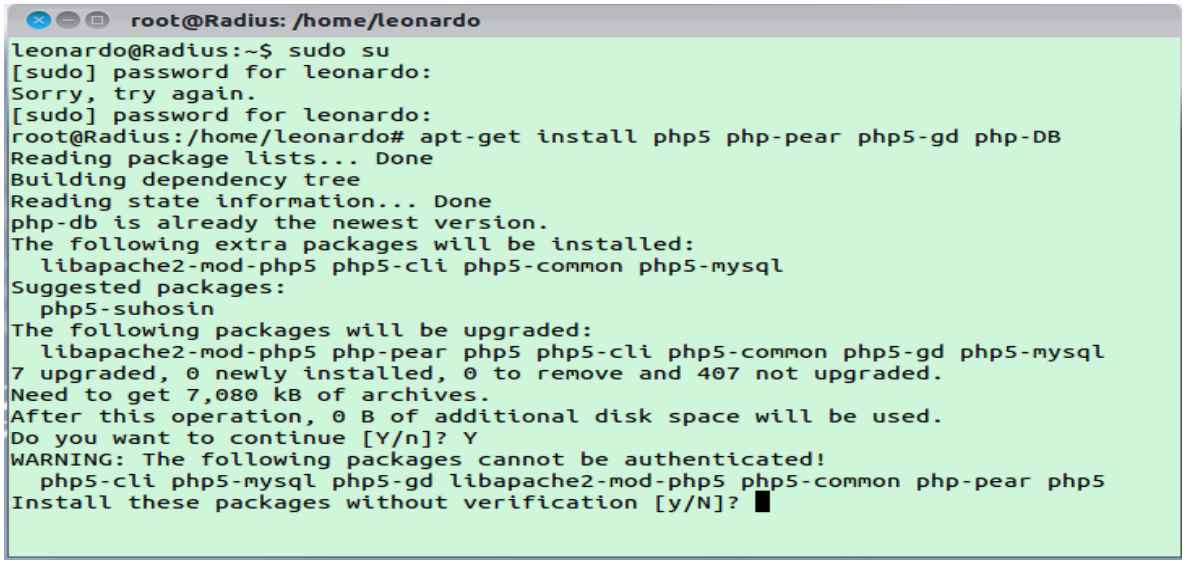
Fuente: Autor

Sin embargo para facilitar el manejo de los usuarios en el servidor se recurre al uso de SQL y todo su paquete:

root@Radius:/home/Leonardo# apt–get install mysql-client mysql-server
root@Radius:/home/Leonardo# apt–get install phpmyadmin
root@Radius:/home/Leonardo# apt–get install php5 php-pear php5-gd php-DB

La instalación de este paquete se desarrolla tal cual se muestra en la figura 6.

Figura 6 instalación del paquete SQL



Fuente: Autor

Para comprobar que el servidor apache esta funcionando de manera correcta. Es necesario abrir un explorador y digitar la dirección IP del sistema que se esta usando, si sale un anuncio con “it work’s” significa que hasta el momento la instalación es correcta.

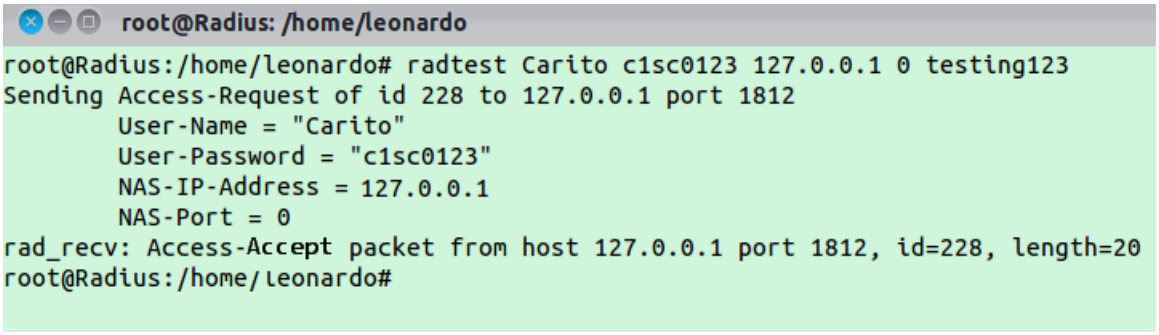
Para probar el servidor con el usuario del sistema se hace uso del comando radtest conformado así:

root@Radius:/home/Leonardo# radtest [Usuario] [contraseña] [dirección a testear] [puerto] [shared secret]

En esta oportunidad el usuario y la contraseña usados para esta prueba son los que serán configurados para el primer cliente del servidor, aquí lo principal es la contraseña compartida que viene configurada por default como testing123, de esta manera el comando queda expresado como sigue:

root@Radius:/home/Leonardo# radtest Carito C1sc0123 127.0.0.1 0 testing123
Si el sistema freeradius esta bien instalado el mensaje recibido será algo similar a rad_recv: Acces_Accept packet…. Tal como se muestra en la figura 7.

Figura 7 prueba de funcionamiento del sistema freeradius con el usuario del sistema



Fuente: Autor

Después de comprobar que el servidor esta funcionando de forma local se procede a realizar las configuraciones más importantes en los archivos.

9.2.1.1 Configuración del archivo eap.conf**.**

Como primera medida se accede al directorio /etc/freeradius/ y se edita el archivo eap.conf con el comando nano:

root@Radius:/home/Leonardo# cd /etc/freeradius/

root@Radius: /etc/freeradius# nano eap.conf

Una vez en este archivo se busca la línea que dice default_esp_type = nds y se le cambia el valor por peap decir quedaría default_esp_type = peap.

En la línea que dice Private-key-password = whatever, se modifica y se cambia su valor por el de la contraseña compartida que será la misma contraseña que en el punto de acceso en este caso es “c1sc0123” así pues la línea quedaría escrita como Private-key-password = c1sc0123.

Después de modificar cada archivo se guarda con ctrl+O, y se sale de este con ctrl+X.

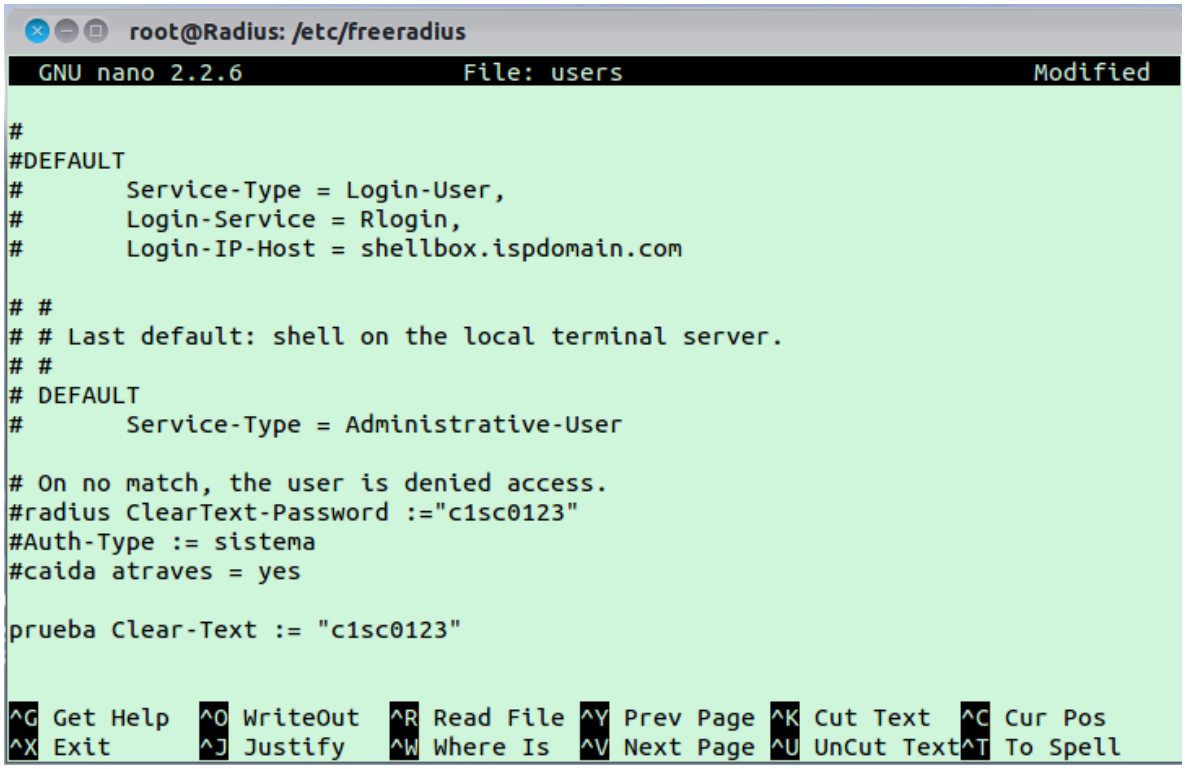
Figura 8 Edición del archivo eap.conf

Fuente: Autor

9.2.1.2 Configuración del archivo radiusd.conf. El segundo paso de configuración es manteniéndose dentro del mismo directorio /etc/freeradius/ se edita el archivo radiusd.conf, y se descomenta la línea que dice $ INCLUDED sql.conf, se guarda y se sale.

9.2.1.3 Configuración del archivo users**.** Permaneciendo en el mismo directorio se accede al archivo users, aquí se va a realizar el primer paso como tal para autenticar, al final del archivo se escribe la línea prueba Clear-text := “c1sc0123” es decir es aquí donde se coloca la contraseña que será usada por el primer usuario de este servidor, nuevamente ctl+O para guardar y ctrl.+X para salir.

Figura 9 Edición del archivo users



Fuente: Autor

9.2.1.4 Configuración del archivo clients.conf. En el archivo clients.conf que se encuentra en el directorio /etc/freeradius, con el comando nano, se agregan las direcciones IP del punto de acceso en el que va a trabajar el servidor radius, junto con la contraseña compartida, que será la misma que se configurar en el punto de acceso.

Client 216.72.4.61{

Secret = testing 123
Shortname = radius
}

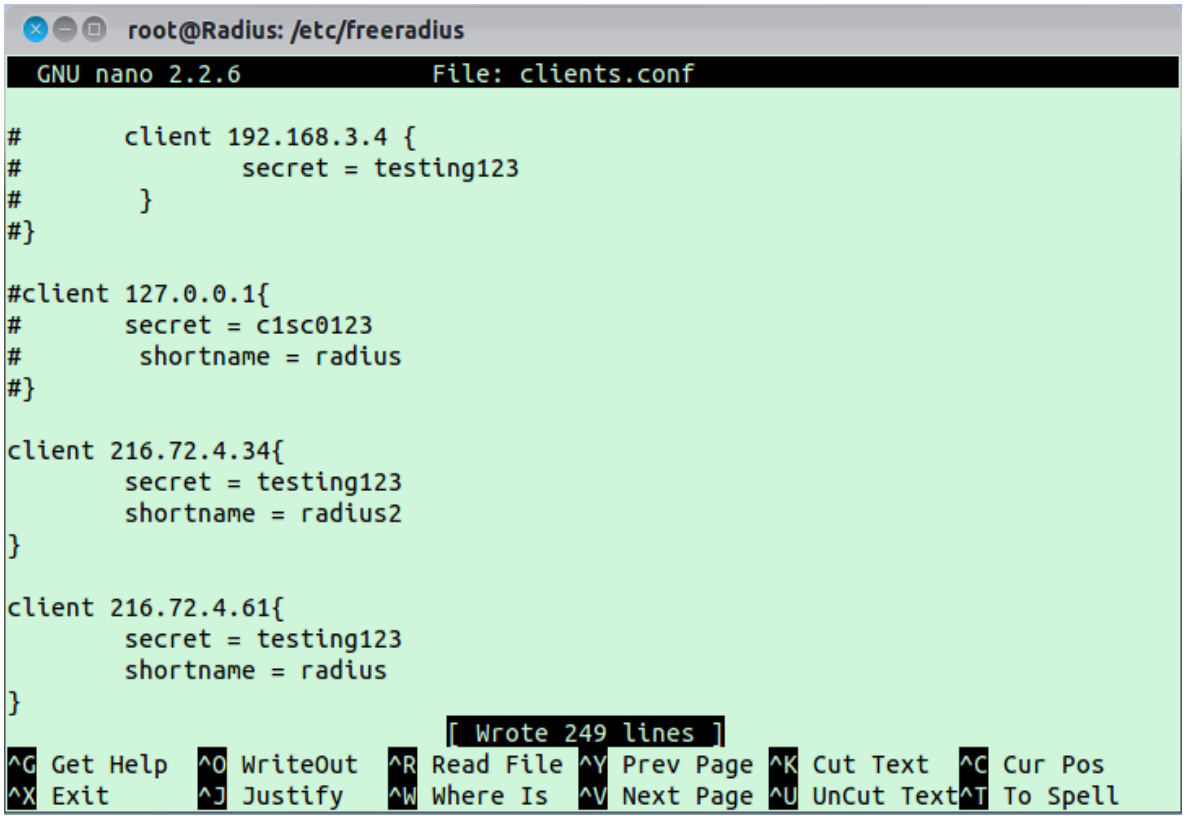
Sin embargo para evitar posibles inconvenientes en el funcionamiento del sistema de autentificación, se procede a agregar también la dirección IP asignada a este equipo de configuración, con la misma contraseña compartida, no se debe cambiar el nombre asignado al cliente.

Client 216.72.4.34{

Secret = testing 123
Shortname = radius2
}

De esta manera el archivo clients.conf debe quedar como se muestra en la figura 10

Figura 10 Edición del archivo clients.conf



Fuente: Autor

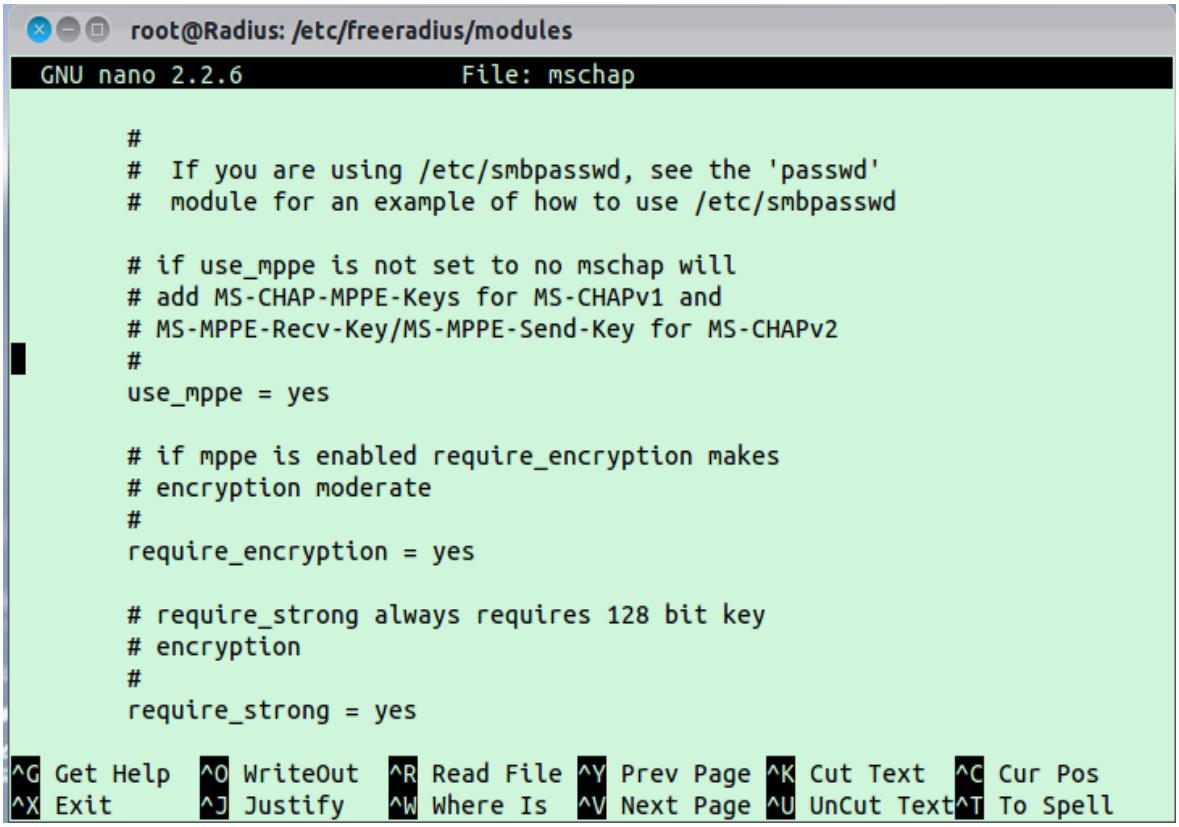
9.2.1.5 Configuración del archivo mschap**.** Para que sea posible una autentificación correcta por medio de freeradius es necesario realizar unas pequeñas modificaciones en el archivo mschap que se encuentra en el directorio etc/freeradius/modules en las siguientes líneas es necesario cambiar el valor por

yes.

Use-mppe = no
Require-encryptation = yes
Require strong = yes
Whit-ntdomain-hack = no

En la figura 11 es posible apreciar la presentación del archive mschap.

Figura 11 Archivo mschap



Fuente: Autor

9.2.2 Paquete SQL.

Antes de iniciar con una de las configuraciones principales de este proyecto es necesario identificar que es y para que sirve este paquete.

9.2.2.1 MySQL**.** MySQL es un sistema de gestión de bases de datos relacional, licenciado bajo la GPL de la GNU. Su diseño multihilo le permite soportar una gran

carga de forma muy eficiente. MySQL fue creada por la empresa sueca MySQL AB, que mantiene el copyright del código fuente del servidor SQL, así como también de la marca.

Aunque MySQL es software libre, MySQL AB distribuye una versión comercial de MySQL, que no se diferencia de la versión libre más que en el soporte técnico que se ofrece, y la posibilidad de integrar este gestor en un software propietario, ya que de no ser así, se vulneraría la licencia GPL.

Este gestor de bases de datos es, probablemente, el gestor más usado en el mundo del software libre, debido a su gran rapidez y facilidad de uso. Esta gran aceptación es debida, en parte, a que existen infinidad de librerías y otras herramientas que permiten su uso a través de gran cantidad de lenguajes de programación, además de su fácil instalación y configuración

* Características de MySQL

  Entre las principales características de este administrador de bases de datos es posible apreciar:

- ✓ El aprovechamiento de la potencia de sistemas multiprocesador, gracias a su implementación multihilo.
- ✓ Tiene gran capacidad para soportar cantidades importantes de tipos de datos para las columnas.
- ✓ Presenta características que le permiten una gran portabilidad entre sistemas.
- ✓ Permite usar hasta 32 índices por tabla.
- ✓ Manteniene un muy buen nivel de seguridad en los datos, al realizar procesos de gestión de usuarios y passwords. [21]

9.2.2.2 PHPmyadmin**.** Es un programa de libre distribución en PHP. Es una herramienta muy completa que permite acceder a todas las funciones típicas de la base de datos MySQL a través de una interfaz Web muy intuitiva.

Además proporciona una gran variedad de herramientas que facilita mucho la administración de bases de datos.
La aplicación en si no es más que un conjunto de archivos escritos en PHP que se pueden copiar en un directorio de cualquier servidor Web, de modo que, cuando se acceda a esos archivos, muestra unas páginas donde se puede encontrar las bases de datos a las que se tienen acceso en un servidor de bases de datos determinado.

---

[21] Tomado de: http://www.danielpecos.com/docs/mysql_postgres/x57.html

Esta herramienta permite crear tablas, examinarlas, filtrar y buscar registros, insertar y actualizar datos en las tablas existentes, ver y gestionar los registros de las tablas, permitiendo su edición y su eliminación, borrar tablas, ver las sentencias necesarias para incluirlas en desarrollos PHP, etc., incluso podemos ejecutar sentencias SQL y hacer backups de la base de datos.

La página de inicio del programa ofrece la posibilidad de ver un demo online, aunque nos avisan de que el servidor donde se aloja puede estar caído.

PHPmyadmin es un proyecto escrito en PHP, por lo que se hace necesario colocar los archivos en un servidor Web que permita programación de páginas PHP Además, se debe acceder a la herramienta a través de la dirección del servidor Web.

Por ejemplo en este caso la carpeta phpMyAdmin se encuentra ubicada en "/srv/www/htdocs", la cual es la carpeta de publicación del servidor web Apache 2 que se encuentra instalado en el servidor.[22]

Después de tener conocimiento sobre estos aspectos se procede a la configuración de este paquete, teniendo en cuenta que es muy útil para la administración de los usuarios clientes en el servidor.

Para la configuración de varios usuarios como es el caso, es muy útil el uso de una base de datos es por esta razón que se realizo la instalación del paquete SQL, junto con el administrador de dicha base de datos: phpMyadmin, por esta razón ahora es necesario realizar la configuración de dichas herramientas.

Para esto primero se accede al directorio SQL/MySQL con el siguiente comando:

root@Radius: /etc/freeradius/# cd sql/mysql
root@Radius: /etc/freeradius/ cd sql/mysql#

Ya estando dentro de este directorio se procede a hacer la creación de la base de datos la cual fue nombrada como Radius, de esta manera se accede a mysql para la posterior creación de la base de datos:

root@Radius: /etc/freeradius/ cd sql/mysql# mysql –u root –p

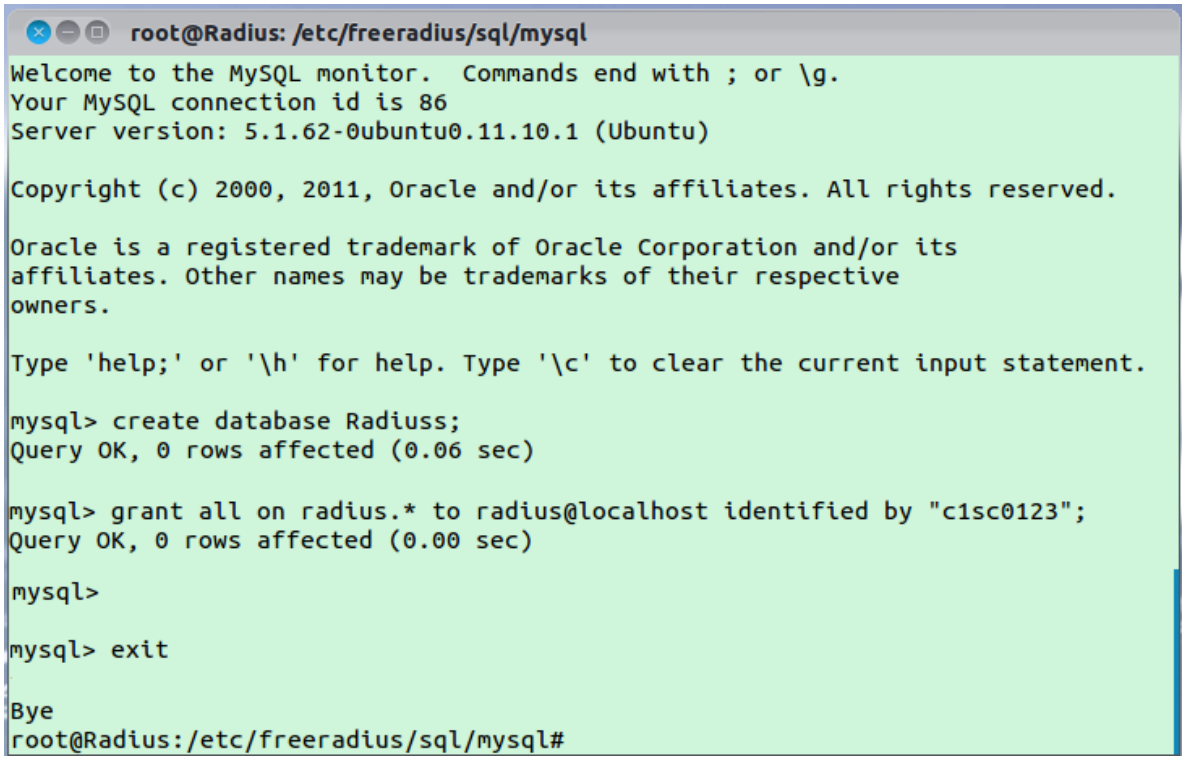
Se coloca la contraseña que se ingreso al momento de la instalación y una vez dentro de este editor, se procede a la creación de la base de datos haciendo uso de los siguientes comandos:

[22] Tomado de: http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

mysql> create database Radius;
mysql> grant all on Radius. to radius@localhost identified by “c1sc0123”;*

En la figura 12 se presenta el procedimiento y la respuesta a este proceso.

Figura 12 Creación de la base de datos en MySQL



Fuente: Autor

9.2.3 Configuración de los servicios

9.2.3.1 Configuración de los permisos. Después de crear la base de datos en mysql se procede a agregarle las tablas, es decir agregar las sentencias sql que son indispensables para la autenticación de los usuarios y que se encuentran en el archivo schema.sql, para esto se usa el comando:

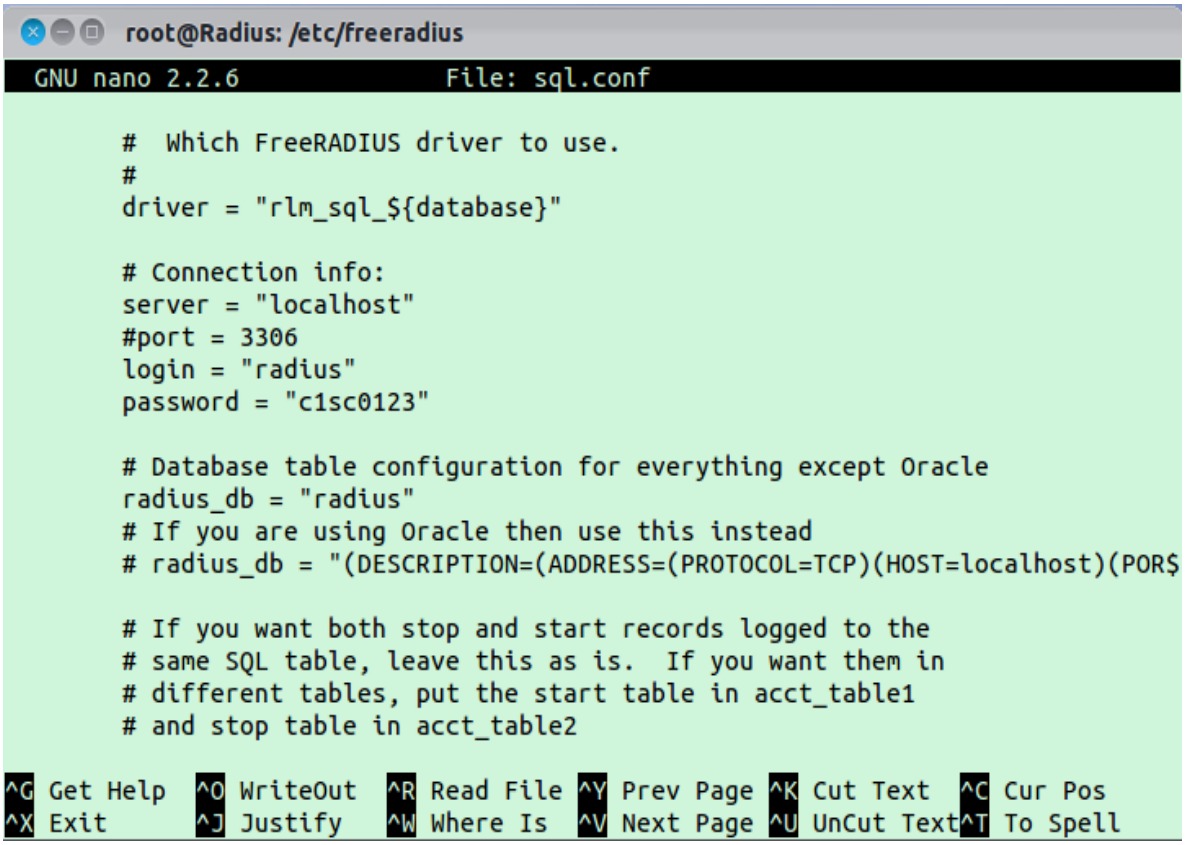
root@Radius: /etc/freeradius/ cd sql/mysql# mysql –u root –p < schema.sql

Se ingresa la contraseña y si no se muestra ningún error quiere decir que estas

sentencias fueron agregadas correctamente.

9.2.3.2 Habilitación de los usuarios**.** Para habilitar la autentificación de usuarios se edita el archivo sql.conf, que se encuentra localizado en el directorio /etc/freeradius, aquí se cambia el valor de la contraseña por “c1sc0123” como se muestra en la figura 13.

Figura 13 habilitación de la autentificación de usuarios



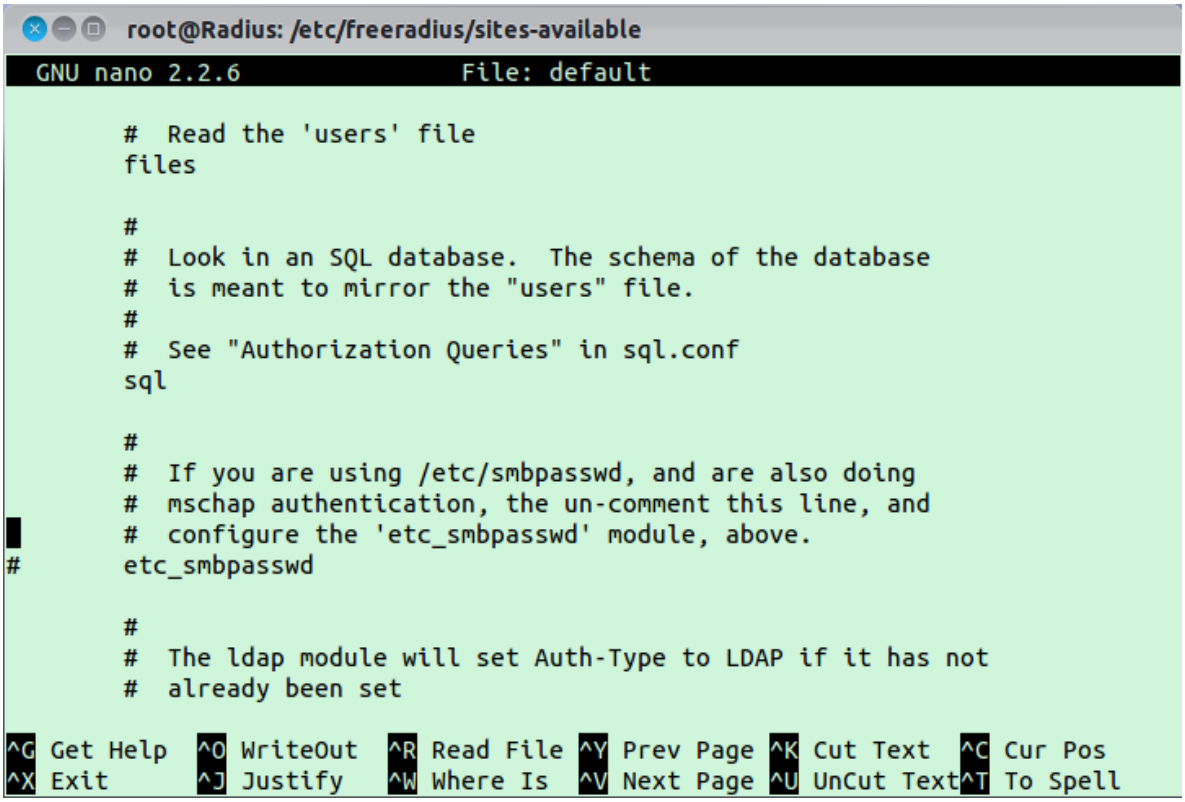
Fuente: Autor

9.2.3.3 Edición del archivo Default. Después de realizar este procedimiento se edita el archivo default que se encuentra dentro del directorio etc/freeradius/sites-available descomentando las líneas que contengan sql es de suma importancia descomentar las líneas en la sección de accounting y la sección de authorize.

root@Radius: /etc/freeradius/# cd sites-avaible
root@Radius: /etc/freeradius/sites-avaible# nano Default

En la figura 14 se posible apreciar el resultado de la edición de este archivo.

Figura 14 configuración del archivo default



Fuente: Autor

9.2.4 Creación de usuarios en la base de datos**.**

Una ves configurados cada uno de los parámetros importantes para SQL, es el momento de crear los usuarios en la base de datos, de esta manera se recurre a un programa que fue instalado al comienzo del proceso, el PHPmyadmin. Que será el programa encargado de administrar esta base de datos.

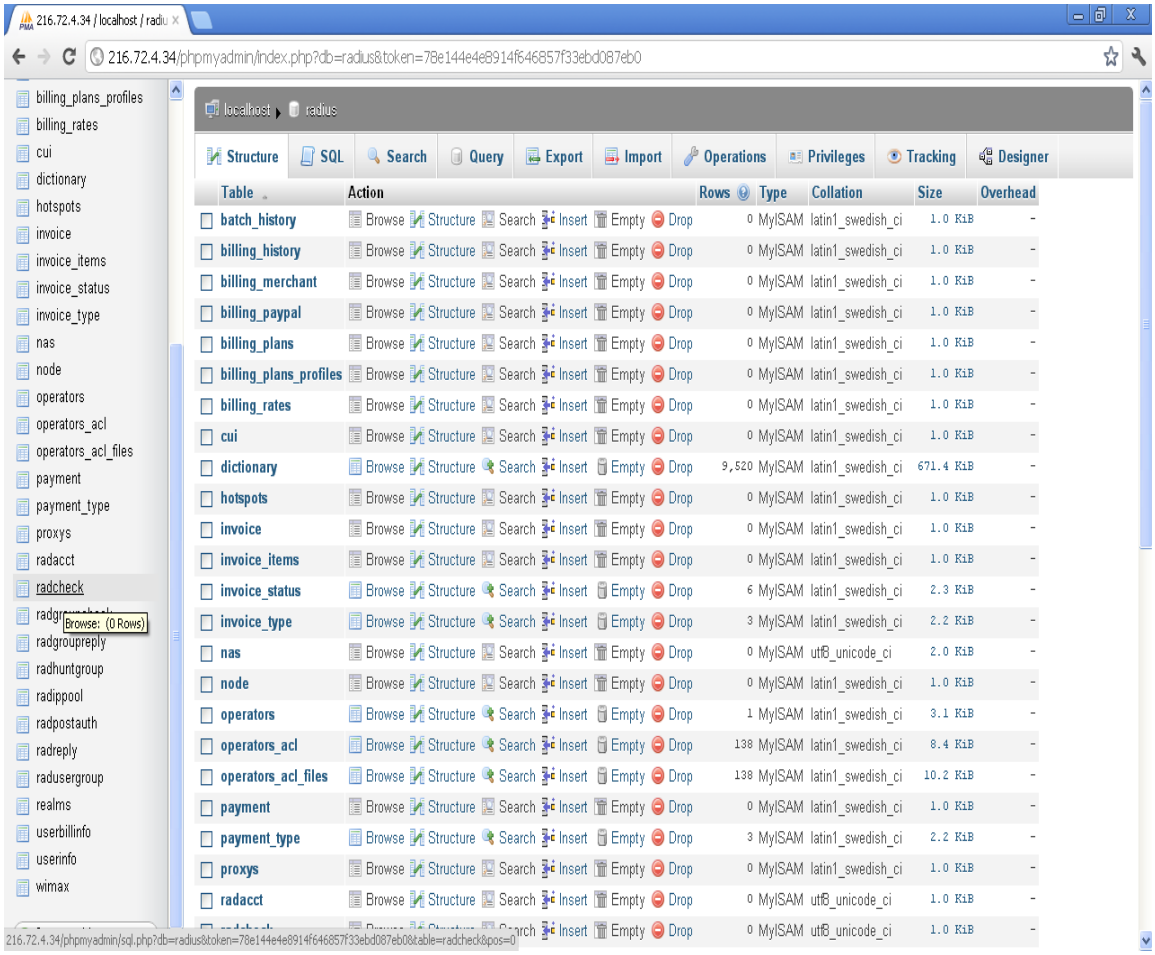
De esta manera se abre un explorador y se digita la dirección IP localhost/phpmyadmin, en este caso en particular seria:

http//:216.72.4.34/phpmyadmin

Se debe desplegar una ventana en la cual se solicita colocar un usuario y contraseña, el usuario es root y la contraseña es la misma que se configuro en el momento de la instalación, después de ingresar a esta cuenta, se accede a la base de datos Radius, para luego ingresar a la tabla radcheck, que es la tabla

encargada de almacenar los usuarios.

Figura 15 configuración de phpMyAdmin

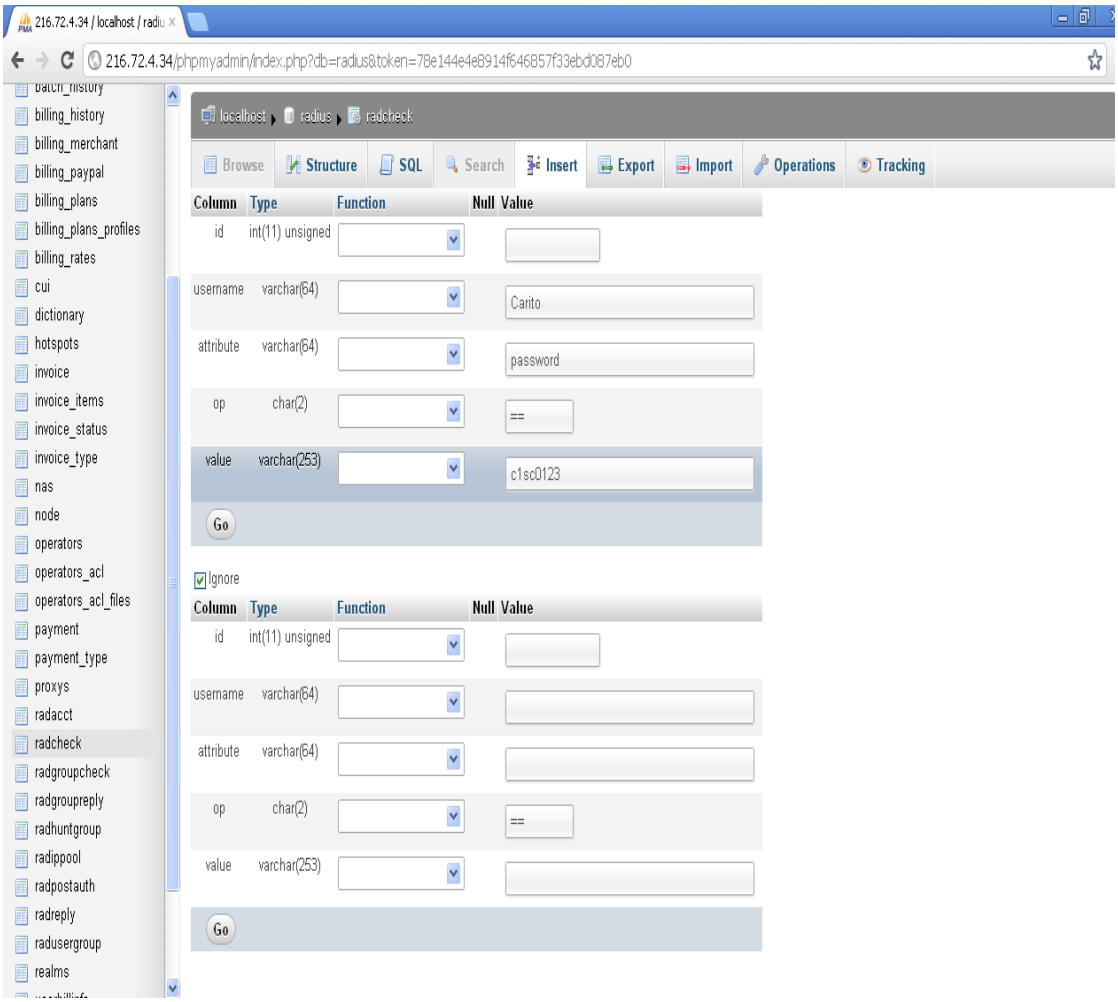


Fuente: Autor

Dentro de esta tabla simplemente se recurre a la pestaña insertar y se agrega el nombre de usuario que se va a configurar para acceder al servidor y la contraseña que se va a usar para la autentificación.

Se debe presentar una ventana como la que se representa en la figura 16.

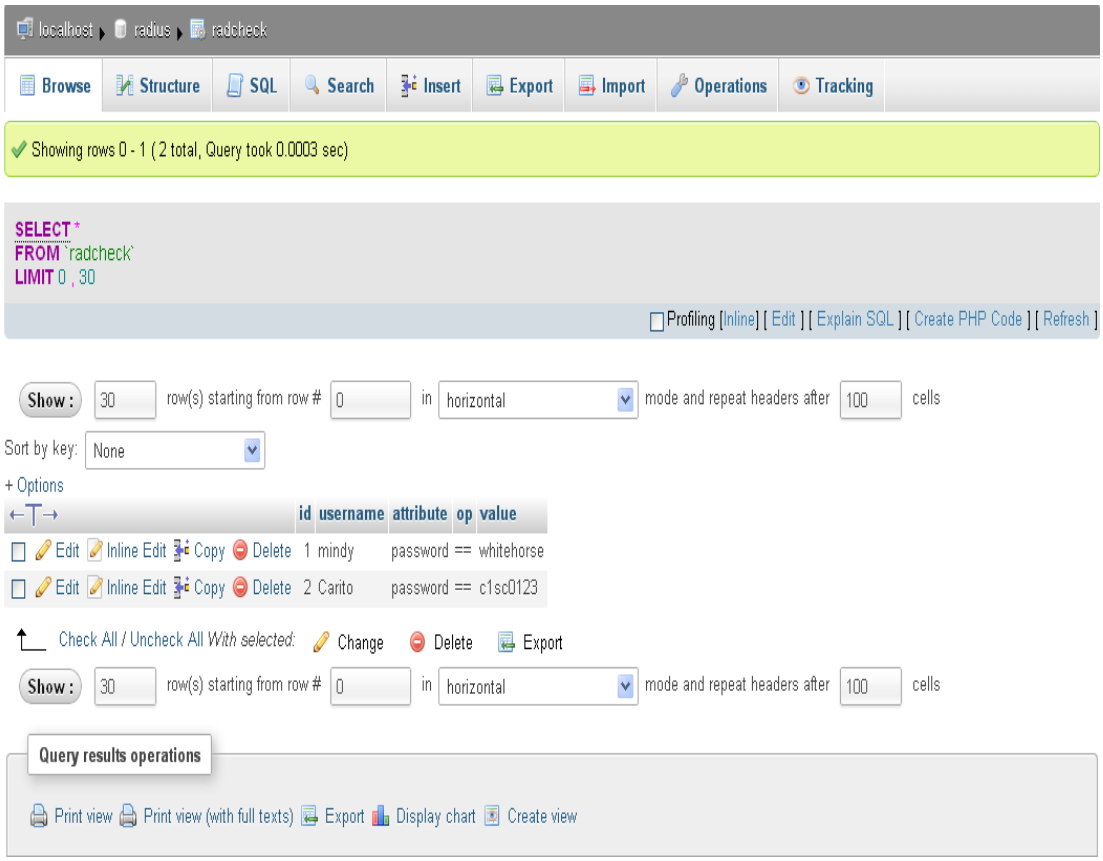
Figura 16 Creación de los usuarios por medio de phpMyAdmin



Fuente: Autor

Para observar los usuarios almacenados en la tabla solo es necesario entrar en la pestaña examinar y allí se desplegaran los datos de los usuarios es decir (nombre de usuario y la contraseña).

Figura 17 Almacenamiento de usuarios en phpMyAdmin



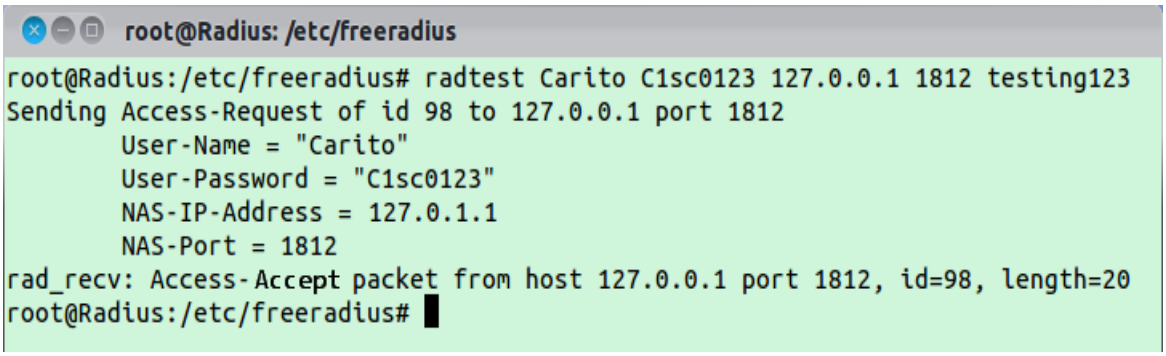
Fuente: Autor

9.2.5 Pruebas iniciales.

De esta manera ya se encuentra instalado freeradius con mysql, por esta razón es momento de realizar una nueva prueba con radtest para determinar si el software esta funcionando correctamente o no, en esta oportunidad se coloca el puerto1812 que es el puerto usado por Radius para realizar sus labores de autentificación.

root@Radius:/home/Leonardo# radtest Carito C1sc0123 127.0.0.1 1812 testing123

Figura 18 resultado de la segunda prueba provisional del servidor.



Fuente: Autor

9.2.6 Instalación y configuración de DaloRadius.

Para realizar la gestión en los puntos de acceso se hace uso del software Daloradius, que no es más que una aplicación avanzada de gestión de Radius, esta interfaz Web permite configurar y administrar de una manera más practica y eficaz el servidor Radius.

Como primera medida se procede a acceder al link:

http://sourceforge.net/projects/daloradius/files

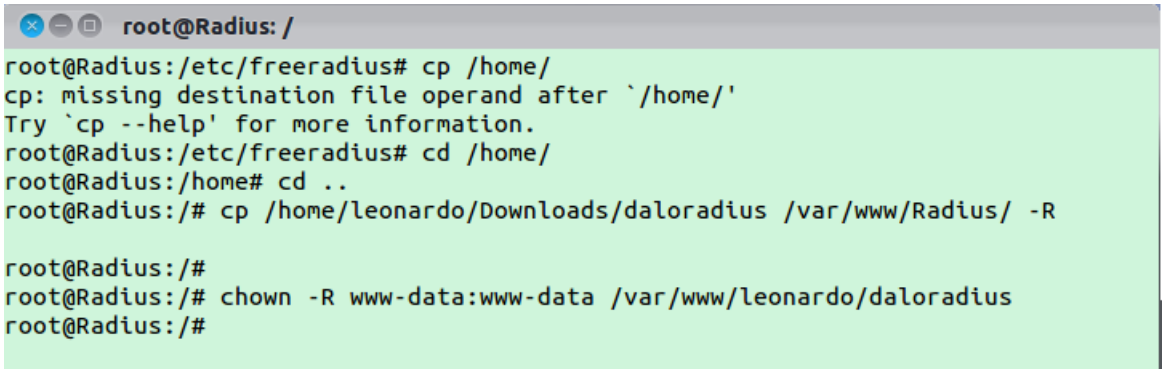
Del cual se descargara el software Daloradius, este queda guardado en descargas, se descomprime el paquete y se nombra Daloradius, en el terminal de Ubuntu se realiza una copia de este programa, se cambia su propietario y los permisos haciendo uso de los siguientes comandos:

Copia

root@Radius: / # cp /home/Leonardo/Downloads/Daloradius /var/www/Radius/ - R
Permisos

root@Radius: / # chown –R www-data:www-data /var/www/Radius/ - R

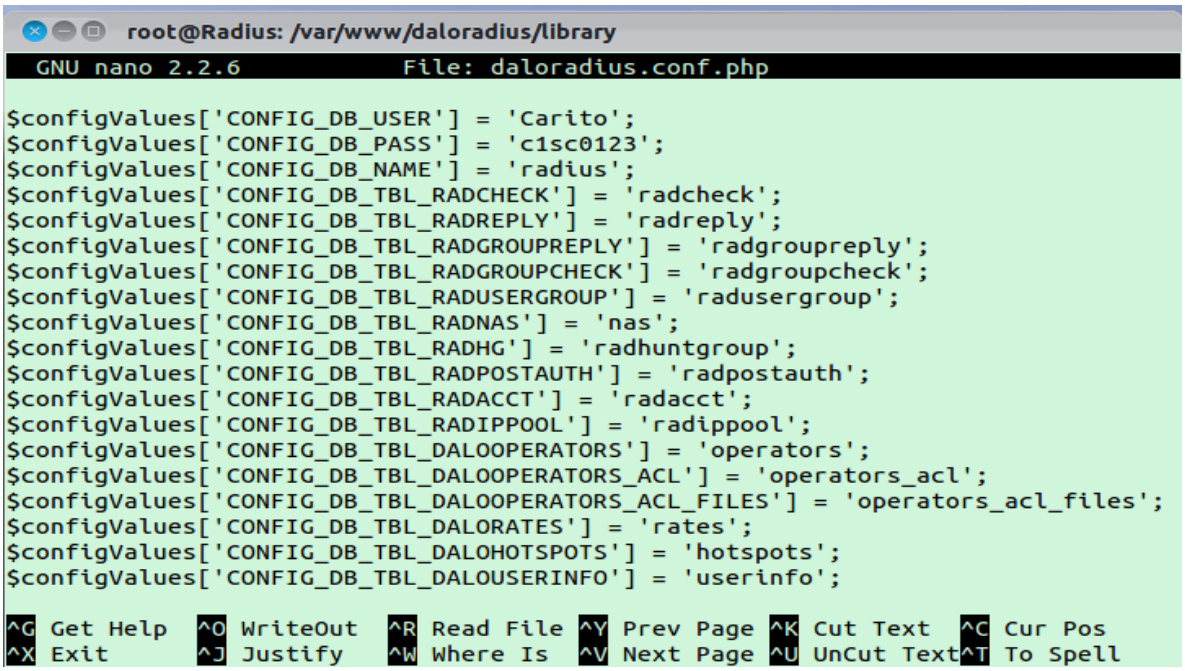
Figura 19 configuración inicial Daloradius.



Fuente: Autor

Se ingresa al directorio cd /var/www/daloradius/library, con el comando ls se puede observar todos los archivos presentes en este directorio, en el archivo daloradius.conf.php se encuentra la información mas importante para el acceso a este software, así que se edita el nombre de usuario, la contraseña y la base de datos como se presenta en la figura 20.

Figura 20 configuración del acceso a Daloradius.



Fuente: Autor

Para relacionar la base de datos con daloradius se accede al directorio /var/www/daloradius/ y con la línea *cd contrib/db/* se accede al archivo db en el cual se realizara este procedimiento de la siguiente manera:

root@Radius: /var/www/daloradius/contrib/db # MySQL –u root –p radius < mysql-daloradius.sql

Si pide la contraseña y no enseña ningún error quiere decir que el procedimiento culmino con éxito.

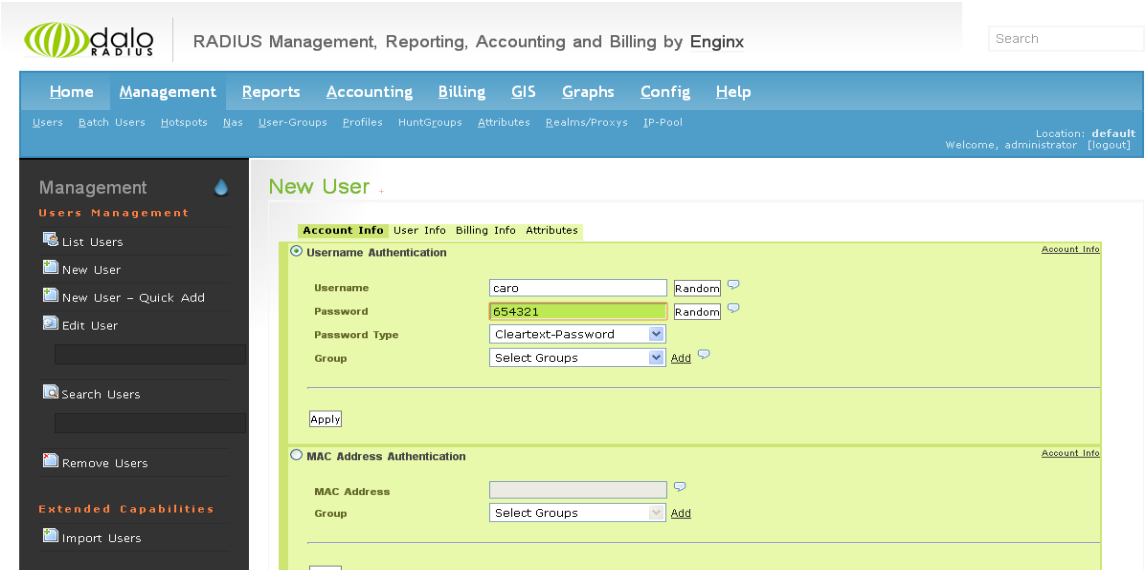
Teniendo configurado el daloradius completamente, se accede a este para empezar a añadir los puntos de acceso del mismo y de esta manera empezar a realizar la autenticación, para esto en un explorador se coloca:

http://216.72.4.34/daloradius

Se debe presentar una ventana en la que se solicita usuario y contraseña, el usuario es administrador y la contraseña es radius, esta puede ser modificada si se quiere en daloradius.conf.php

Una vez habiendo accedido a daloradius se procede a agregar la información de los puntos de acceso en este programa, en la pestaña Management, se ingresa a la opción New user y se coloca el nombre con el que se va a acceder y la contraseña configurada, se guarda.

Figura 21 creación de usuarios en Daloradius



Fuente: Autor

En la opción NAS creamos una nueva y se nombra con la dirección IP del punto de acceso a usar en este caso 216.72.4.61, con esta última configuración se tiene la configuración parcial del servidor radius, sin embargo es necesario realizar la configuración del punto de acceso.

9.3 CONFIGURACIÓN DEL PUNTO DE ACCESO

Para la configuración del punto de acceso se uso un switch cisco Catalyst 2950 de 48 puertos configurado para este fin, la dirección de este cliente es la 216.72.4.61, la configuración es sencilla basta con seguir los siguientes pasos:

Se entra en el modo configuración del switch, y una ves aquí se inicia la configuración:

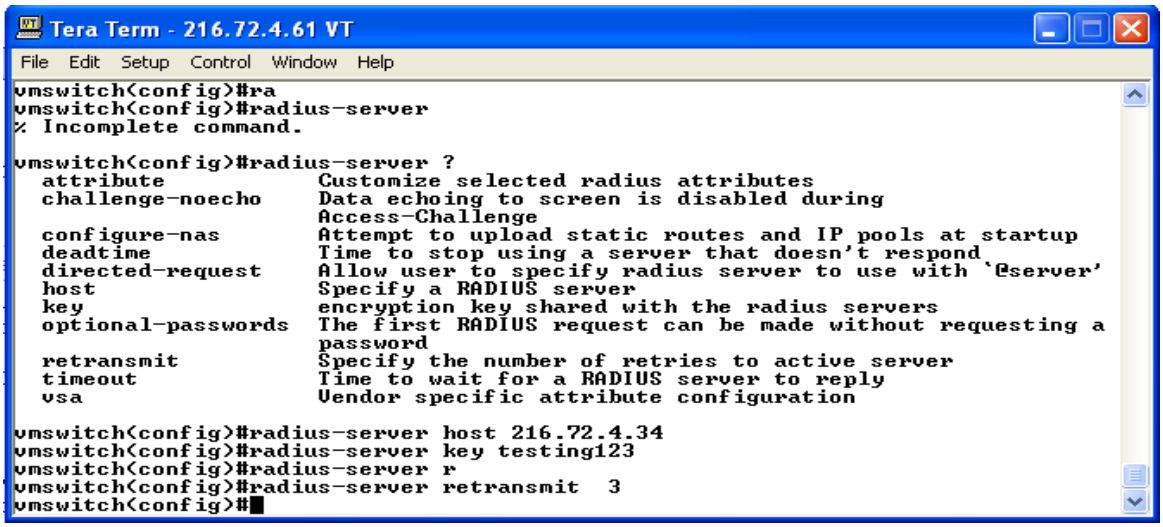
Vmswitch#config terminal
Vmswitch<config># radius-server host 216.72.4.34

Con este comando se le esta indicando al switch que trabaje con el protocolo Radius, y que además de esto permita a la dirección 216.72.4.34 que sea la que administre este servicio, ahora es necesario configurar la clave compartida que fue configurada de igual manera en el servidor freeRadius, para realizar esta configuración se hace uso del siguiente comando:

Vmswitch<config># radius-server key testing123
Vmswitch<config># radius-server retransmit 3

La última línea se configura para determinar cuantos intentos de trasmisión se realizaran antes de rechazar totalmente el acceso al sistema si el *usuario* y/o la contraseña se encuentran errados, en la figura 22 se encuentra la configuración realizada a este equipo para el desarrollo del proyecto.

Figura 22 Configuración del punto de acceso



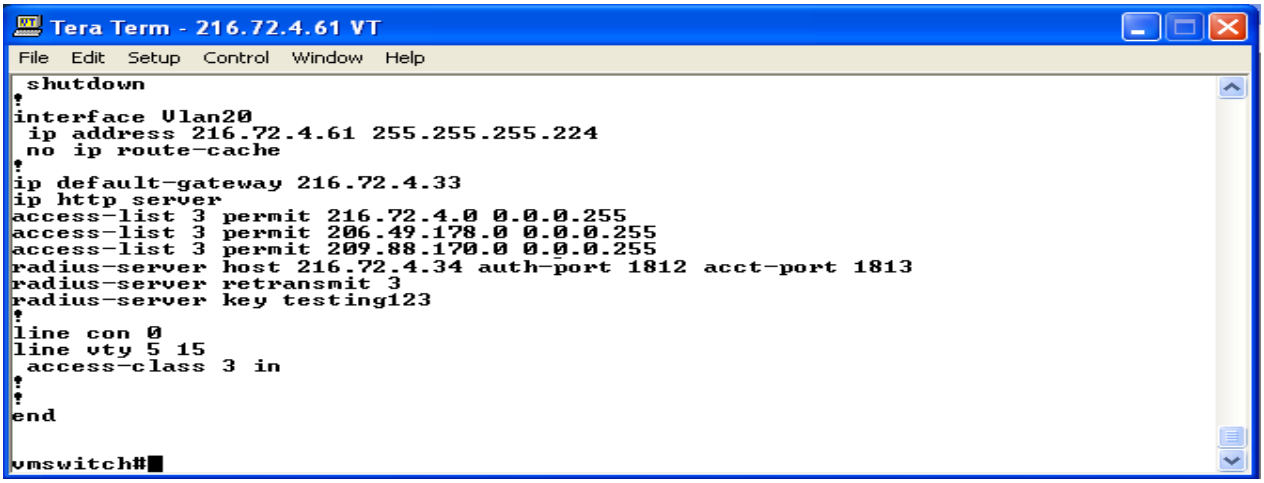
Fuente: Autor

Para asegurarse que el servicio de Radius se encuentra activo y que fue configurado correctamente en el switch que se usara como punto de acceso, se realiza un show run en el mismo donde se presentaran cada una de las configuraciones realizadas en el mismo

Vmswitch#show run

En la figura 23 es posible apreciar los resultados entregados por el switch.

Figura 23 Configuraciones realizadas en el punto de acceso (switch)



Fuente: Autor

9.4 CONFIGURACIÓN DEL SUPLICANTE

Una vez realizada la configuración del punto de acceso es necesario realizar la configuración del suplicante, que es la entidad que es autenticada por el servidor es decir, es el encargado de iniciar y terminar intercambios de autenticación, este es uno de los puntos principales del proyecto ya que la autenticación solo inicia cuando se realiza la conexión del suplicante al autenticado, para esto se hace uso del software Odyssey Client para Windows XP

9.4.1 Odyssey**.**

Es una solución de seguridad 802.1X extremo a extremo, que permite a los usuarios concertarse a la red de una forma segura, puede ser fácil y ampliamente desplegada por medio de una red de trabajo corporativa.

Es por esta razón que Odyssey es considerada como una solución completa para redes, asegurando la autenticación del cliente, así como la conexión a la misma; Odyssey cuenta con 2 grandes componentes:

Odyssey Client: se comunica con Odyssey Server o con un servidor basado en 802.1x para establecer una conexión segura.

Odyssey Server: Es un servidor Radius basado en protocolos de autenticación como MD5 y/o EAP.

9.4.2 Características de Odyssey

- Odyssey Client se ejecuta bajo Windows XP, 98, CE.
- Administración de certificados basada en el servidor (no se requiere certificado del lado del cliente excepto al hacer uso de EAP-TLS)
- Trabaja con cualquier hardware basado en 802.1X.
- Generación de llave dinámica para una seguridad superior.[23]

9.4.3 Configuración de Odyssey Client.

Después de descargar y de instalar el software Odyssey Client, se procede a dar inicio al Client manager que es el que permite configurar un cliente EAP, después se desactiva el cliente en la opción settings y luego en disable Odyssey.

---

[23] Tomado de: catarina.udlap.mx/u_dl_a/...d.../capitulo3.pdf

Como segunda medida se accede a profiles en donde se hace la configuración de cada uno de los perfiles del usuario, en la opción que dice Add se accede a la pestaña User info, es aquí donde se debe colocar el nombre de usuario que se ha venido configurando para este primer caso se usa el usuario Carito, el usuario Caro este ultimo se realiza de la misma manera que el anterior, es indispensable activar las opciones que dicen Permit login using Password y prompt password.

Ahora en la Authentication se debe eliminar todos los protocolos de autenticación presente en esta, ahora se selecciona la opción add, se elige la opción EAP/MD5, se sale.

En la opción Networks se realiza la configuración de las redes para las que se encuentra configurado el cliente EAP, aquí es preciso seleccionar la opción any y configurarla en propiedades.

Una ves dentro de propiedades se activan las casillas autentícate using Carito y connect to any available network, el mismo procedimiento se realiza para el otro usuario.

En la opción adpters se comprueba que el adaptador de red del equipo este en la lista, luego en la opción conection se elije este adaptador en el menú adapter, se activa la opción connect using profiles Carito, lo mismo se hace para el otro usuario.

9.5 PRUEBAS DE AUTENTICACIÓN.

Una vez realizadas todas configuraciones necesarias para el correcto funcionamiento del servidor, se procede a realizar las pruebas de login con el mismo, en este caso se realiza como primera medida una prueba de accesso haciendo uso de Telnet, si el servidor funciona correctamente debe pedir contraseña y usuario.

9.5.1 Lanzamiento del demonio**.**

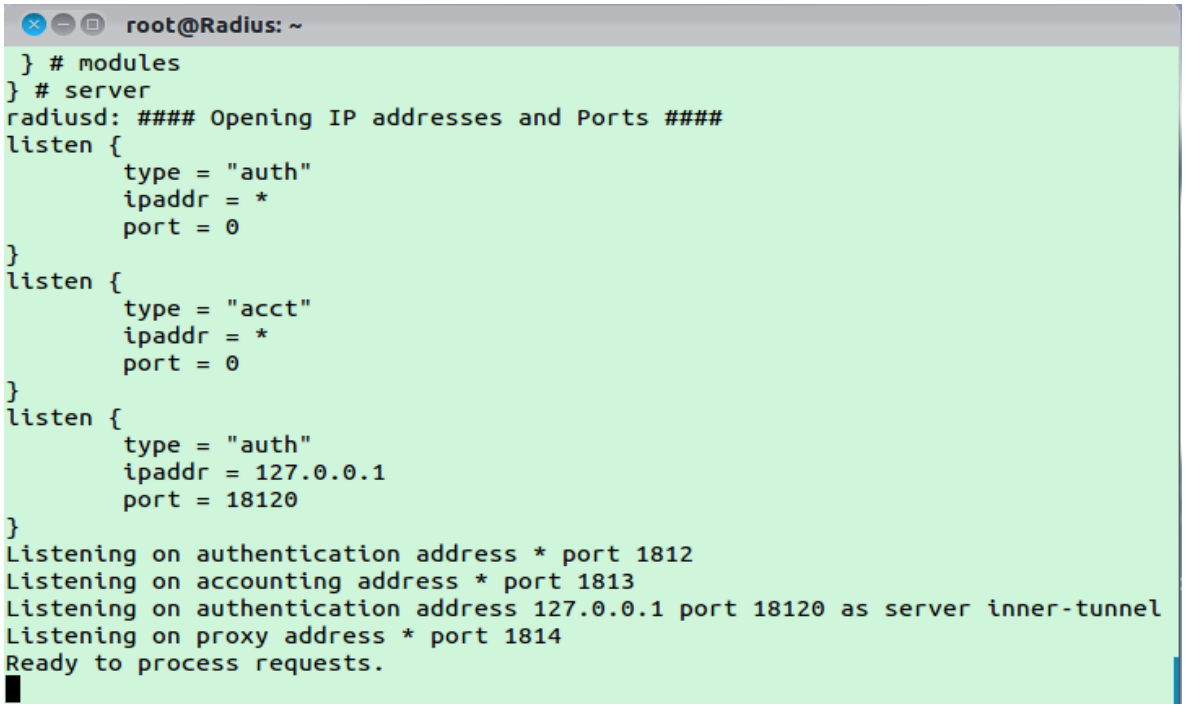
Aunque la Configuración del servidor ha sido realizada en su totalidad, aun falta el procedimiento más importante, lanzar el demonio del programa, es decir poner a funcionar al servidor, Para realizar este procedimiento es necesario ingresar al modo root, haciendo uso del comando sudo su, con el siguiente comando, se corre el demonio.

root@Radius:/home/Leonardo#freeradius –X

Por medio de este procedimiento se logra poner en funcionamiento el servidor de autenticación ya configurado, garantizando su correcto funcionamiento, vale la pena aclarar que si se encuentra algún error en las ultimas partes de Configuración, al realizar este procedimiento se mostrara en que archivo existe alguna inconsistencia, ya sea un error de sintaxis o la ejecución de un comando inexistente.

En la figura 24 es posible apreciar como se realizo el procedimiento para el lanzamiento del demonio.

Figura 24 Lanzamiento del Demonio.



Fuente: Autor

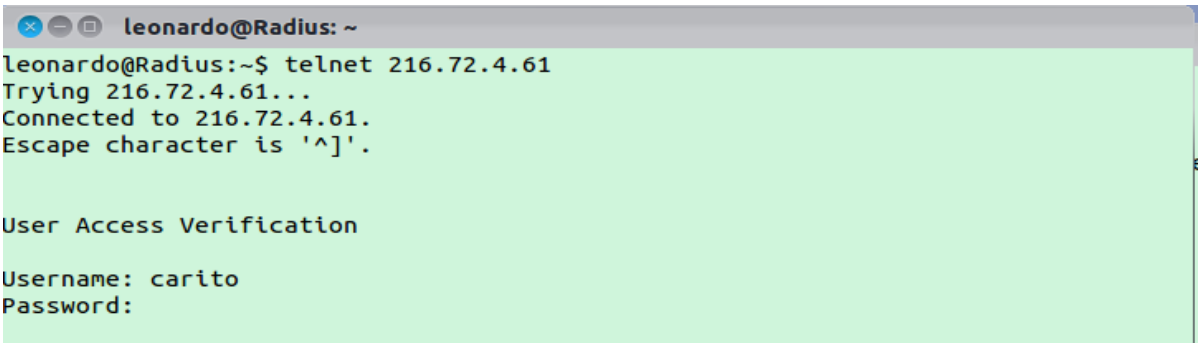
9.5.2 Pruebas iniciales**.**

Una vez comprobado que la Configuración no presenta falencia alguna, se realiza la primera prueba de autenticación haciendo uso de Telnet, con la dirección configurada para el punto de acceso, para este caso la dirección es 216.72.4.61, una vez aquí esta debe exigir un usuario y una contraseña.

Para esta primera prueba se hace uso del usuario Carito y la contraseña C1sc0123, que fueron las primeras configuradas.

En la figura 25 es posible apreciar el funcionamiento del servidor de autenticación.

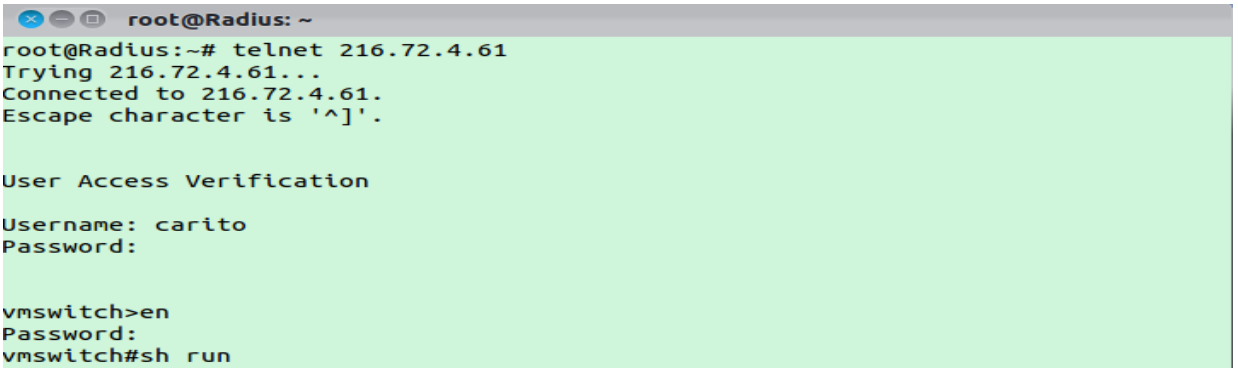
Figura 25 primera prueba del servidor.



Fuente: Autor

Una vez aquí solamente es necesario esperar que el servidor le consulte al punto de acceso si es permitida la conexión desde aquí y con esto dejara ingresar a la Configuración del switch.

Figura 26 primer acceso al switch por medio del servidor.

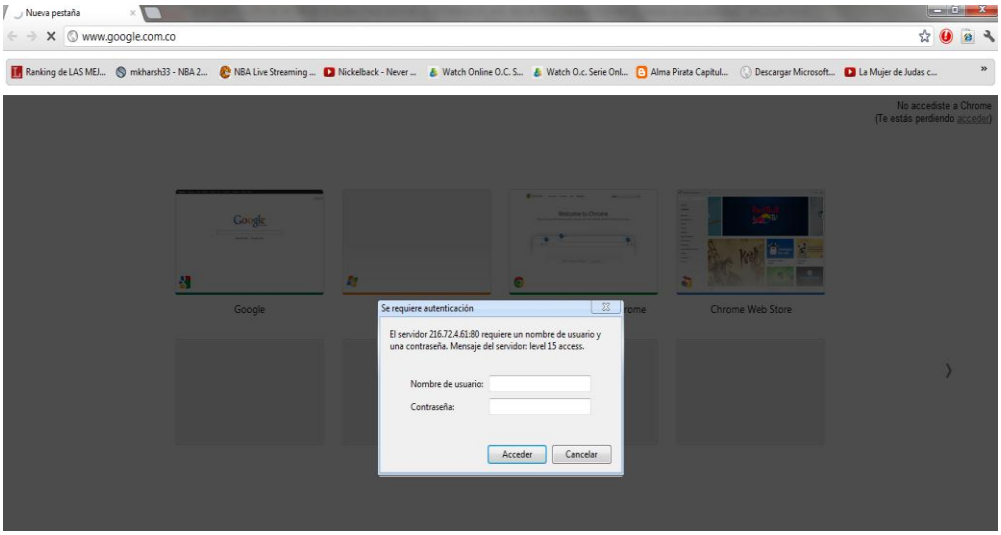


Fuente: Autor

9.5.3 Prueba final.

Después de comprobar satisfactoriamente que el servicio este bien instalado y permitir el acceso desde el servidor al switch, se procede a realizar la prueba final, intentar acceder a Internet haciendo uso de un explorador normal.

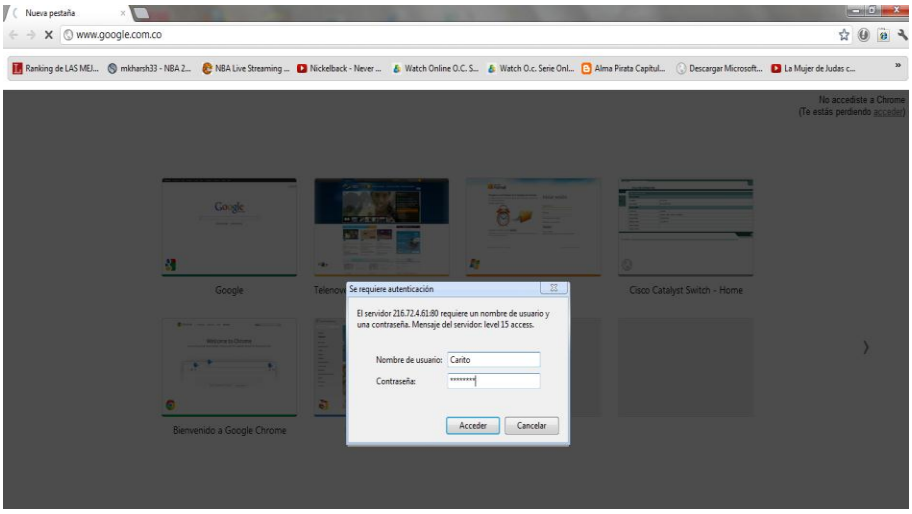
Figura 27 primer intento de acceso a internet después de configurar el servidor



Fuente: Autor

En este caso el explorador pide el ingreso de un nombre de usuario y de una contraseña, par permitir el acceso al servicio, para esto simplemente se hace uso de uno de los usuarios antes configurados con su respectiva contraseña, para este caso se usa el usuario Carito y la contraseña c1sc0123, si el servidor esta funcionando de manera correcta permitirá el acceso a internet a este usuario.

Figura 28 Uso del usuario configurado para el acceso a internet



Fuente: Autor

CONCLUSIONES

La seguridad en el acceso a una red corporativa juega un papel importante en la organización de una empresa, aunque existen múltiples alternativas para brindar este servicio, gracias a este proyecto ha sido posible determinar, que la alternativa mas viable para este caso es la implementación de un servidor Radius ya que este es un método seguro, confiable y económico, que presenta menores desventajas y características más acordes con las necesidades de la empresa.

Con el diseño de políticas de seguridad para aplicaciones comunes en redes empresariales, se logra mayor disponibilidad de acceso a más usuarios sin poner en riesgo la seguridad. Se limita el acceso a los recursos de red mientras se mantiene eficacia operacional, se provee diferentes clases de servicios a distintas clases de usuarios mejorando así la calidad de uso de la red.

De esta manera para presentar una alternativa en el esquema de seguridad de la compañía, se realizo la implementación de un servidor AAA FreeRadius, ya que este tiene la capacidad de acceder y almacenar la información de los usuarios haciendo uso de bases de datos, en este caso del paquete SQL, presentando también facilidades en su configuración por medio de Ubuntu, brindando así un servicio íntegro con facilidades para el usuario final, sin arriesgar la seguridad de la red de telecomunicaciones en ningún momento.

Para brindar seguridad a una red de telecomunicaciones existen diferentes alternativas, sin embargo una de las mas viables es la implementación del servidor de autentificación Radius, ya que brinda un gran apoyo a la seguridad de la red, siendo sencillo de implementar y manejar, evitando que personas no autorizadas tengan acceso a la informacion de la red, sin embargo si se desea obtener mejores resultados es recomendable el uso de un equipo ASA de Cisco ya que ofrece los mismos servicios con un margen de error menor, por este motivo la implementación de un servidor radius se recomienda para el uso de redes corporativas de pequeñas empresas, donde no es posible realizar una inversión tan alta.

Gracias a la implementación de este proyecto fue posible adquirir mayores conocimientos en las estrategias usadas para implementar la seguridad en una red de telecomunicaciones, así como también la posibilidad de hacer uso de bases de datos por medio del paquete SQL, logrando de esta manera una formación más sólida en el mundo de la seguridad informática.

Por medio de la practica empresarial en la compañía Orange Business Services fue posible no solo afianzar los conocimientos adquiridos durante el transcurso de

la formación académica en la facultad, si no que también fue posible conocer de cerca algunos de los elementos que componen el mundo de las telecomunicaciones, con el reconocimiento, la utilidad y la configuración de algunos equipos, alcanzando de esta manera una mejor formación académica en este campo de la ingeniería.

BIBLIOGRAFIA

ALCOCER, Carlos. Redes de computadoras, En: Seguridad de redes de Computadoras, capitulo 24. Libro electrónico, pie de imprenta Lima Infolink, 2000 Extraído el 21 de Febrero, 2012 de http://biblioteca.pucp.edu.pe/docs/elibros_pucp/alcocer_carlos/24_Alcocer_2000_Redes_Cap_24.pdf.

ALEGRE Ramos Maria del pilar, Sistemas Operativos en Red, Ediciones Paraninfo S.A, 1ra Edición, Extraído el 9 de Octubre, 2012, cap 9. pág. 224.

BERTOLIN Javier Areito, SEGURIDAD DE LA INFORMACION REDES, INFORMATICA Y: SISTEMAS DE INFORMACION, Learning Paraninfo S.A, 2008 Extraído el 9 de Octubre, 2012 capitulo 9, pag. 374.

CAPOTE, Olga Pons, Introducción a las bases de datos: El modelo relacional, Thomson Editores S.A, Extraído el 9 de Octubre, 2012, Cap 7 pág. 212.

Instalación y configuración de un Servidor Radius, Extraído el 21 de Febrero, 2012 de Medio virtual: http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

HASSELL Jonathan, Radius. Editorial: O'Reilly Media Inc., Primera edición, octubre 2002, págs.: 204.

HEURTE Oliver, PHP y MySQL Domine el desarrollo de un sitio Web dinámico e interactivo, Ediciones ENI, Extraído el 7 de Octubre, 2012, página 186.

Lorincz, J. Udovicic, G., Architecture of SQL databases for WLAN access control and accounting. Aritculo IEEE, En: Software, Telecommunications and Computer Networks, 2007. SoftCOM 2007. 15th International Conference on, 27-29 Sept. 2007, Pags 1 - 6

Orange Business Services, Extraído el 21 de febrero, 2012 de Medio virtual http://www.orange-business.com/en/mnc2/footer/local/office_colombia/colombia/

PEREZ, francisco Maciá, JORQUERA Marcos D, Administración de servicios de Internet: De la teoría a la práctica, Publicaciones de la Universidad de Alicante, año: 2008, Extraído el 9 de Octubre, 2012, pág. 303.

SERVIDORES RADIUS Extraído el 19 de febrero, 2012 de Medio virtual http://isabelchancayauri.blogspot.com/2010_08_01_archive.html

Shen-Ho Lin, Dept. of Electr. Eng., Chang Gung Univ., Taoyuan, Taiwan, Authentication Schemes Based on the EAP-SIM Mechanism in GSM-WLAN

Heterogeneous Mobile Networks, Aritculo IEEE, En: INC, IMS and IDC, 2009. NCM '09. Fifth International Joint. 25-27 Aug. 2009, Pags. 2089 – 2094.

STALLINGS William, Fundamentos de seguridad en redes: Aplicaciones y estándares. PEARSON EDUCACION S.A, Segunda Edición, 2004, Extraído el 1 de Octubre cap. 4. pág. 92.

REFERENCIAS

[1] medio virtual: prácticas de tecnología avanzadas, Extraído el 21 de Febrero, 2012 de http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf.

[2] medio virtual: Manual del servidor Radius, Extraído el 19 de Marzo, 2012 de http://www.scribd.com/doc/33983013/Manual-Servidor-Radius-Linux-Ubuntu

[3] ROYER Jean-Marc, Seguridad en la informática de empresa: Riesgos, amenazas, prevención y Soluciones, Extraído el 7 de Octubre, 2012, cap 2 pág. 112.

[4] BERTOLIN Javier Areito, SEGURIDAD DE LA INFORMACION REDES, INFORMATICA Y: SISTEMAS DE INFORMACION, capitulo 9, pág. 374.

[5] STALLINGS William, Fundamentos de seguridad en redes: Aplicaciones y estándares. cap 4. págs. 92, 393.

[6] COBO Ángel, PHP y MySQL: Tecnología para el desarrollo de aplicaciones web, Extraído el 29 de Octubre, 2012, pag 348.

[7] HEURTE Oliver, PHP y MySQL Domine el desarrollo de un sitio Web dinámico e interactivo, Extraído el 7 de Octubre, 2012, página 186

[8] medio virtual: Guía Ubuntu, Extraído el 8 de Marzo, 2012 de www.guia-ubuntu.org/index.php?title=PhpMyAdmin.

[9] PEREZ, francisco Maciá, JORQUERA Marcos D, Administración de servicios de Internet: De la teoría a la práctica, Extraído el 9 de Octubre, 2012, pág. 303.

[10] ALEGRE Ramos Maria del pilar, Sistemas Operativos en Red, Extraído el 9 de Octubre, 2012, cap 9. pág. 224.

[11] PALOMARES Ortega Miguel Ángel, Manual Práctico: Servicios de Redes de Área Local, Extraído el 29 de Octubre, 2012, pag 116.

[12] CAPOTE, Olga Pons, Introducción a las bases de datos: El modelo relacional, Extraído el 9 de Octubre, 2012, Cap 7 pág. 212.

[13] medio virtual: Cisco Redes, Extraído el 15 de Junio, 2012 http://www.ciscoredes.com/tutoriales/75-pap-y-chap.html

[14] medio virtual: Características de Ubuntu 11.04, Extraído el 10 de Junio, 2012 de: http://ubuntu-bo.com/index.php?option=com_content&view=article&id=29

[15] medio virtual: Vmware productos, Extraído el 15 de Junio, 2012 de: http://www.vmware.com/es/products/datacenter-virtualization/vsphere/mid-size-and-enterprise-business/features.html

ANEXO 1

UBUNTU 11.04

La versión 11.04 es una de las mas recientes versiones de este sistema operativo, y fue lanzada oficialmente en 28 de abril de 2011, con varias modificaciones en su interfaz visual, iniciando con la creación de la interfaz Unity.

Ubuntu 11.04 incluye tres sesiones de escritorio en la entrada de usuario de Ubuntu; la primera sesión es Ubuntu, utiliza Unity y exige la presencia de controladores para ambientes gráficos 3D, la segunda sesión es Ubuntu Clásico, que hace uso del mismo entorno que se utilizaba en versiones anteriores de Ubuntu, usando efectos de escritorio, la tercera sesión es Ubuntu Clásico es decir sin ningún tipo de efectos.

Su instalador permite actualizar el sistema operativo a Ubuntu 11.04 desde versiones anteriores, sin ningún inconveniente. En esta nueva versión se presentaron cambios en los menús de sistema por ejemplo el menú de sonido incluye las listas de reproducción de música del reproductor, utilizando como innovación el reproductor de música Banshee de manera predeterminada y añadiendo a su ves dos nuevos indicadores, el de conexión de red y el de hora y fecha.

Se agregó también una funcionalidad parecida a Aero Snap, permite que al momento de mover una ventana a la izquierda o derecha, ésta se ajusta a ese lado del escritorio, y si se mueve al borde superior se maximiza, de igual forma, esta versión incluye el núcleo Linux 2.6.38, que permite mejoras de rendimiento hasta 50%, también incluye soporte para más tarjetas gráficas con prestaciones 3D. [24]

Debido a sus características y su disponibilidad lo más recomendable es usar la versión servidor de Ubuntu es decir hacer uso de este sistema para la instauración y configuración del servidor Radius, principalmente por su paquete LAMP (Linux, Apache, MySQL y PHP), que es un beneficio muy importante para este caso.

[24] Tomado de: http://ubuntu-bo.com/index.php?option=com_content&view=article&id=29:ubuntu-1104&catid=11:natty-narwhal&Itemid=100006

ANEXO 2

Vmware vSphere Client

Esta es una de las plataformas de virtualización más completa y sólidas de este campo, permite transformar los centros de datos en una infraestructura en la cloud extraordinariamente simplificada y que posibilita la nueva generación de servicios de TI flexibles y fiables, proporcionando agilidad con un control sin precedentes y máxima eficacia, sin limitar la libertad de elección del cliente.

VMware vSphere incluye muchos componentes que transforman el hardware estándar del sector en un entorno compartido fiable con controles de nivel de servicio integrados para todas las aplicaciones. Estos componentes se dividen de la siguiente forma.

- Servicios de infraestructura: dichos componentes virtualizan de forma integral los recursos de servidores, almacenamiento y red, agrupándolos y asignándolos de manera precisa según demanda a las aplicaciones dependiendo que prioridad tengan.
- Servicios de aplicaciones: Estos componentes proporcionan controles de nivel de servicio para todas las aplicaciones que se ejecutan en su plataforma, independientemente del tipo de aplicación o sistema operativo.
- VMware vCenter Operations y VMware vCenter Server proporcionan la base para la gestión de la virtualización, esencial para administrar los servicios de infraestructura y de las aplicaciones, con máxima visibilidad de todos los aspectos de la infraestructura virtual, automatización de las tareas operativas cotidianas y escalabilidad para gestionar entornos de grandes centros de datos.[25]

[25] Tomado de: http://www.vmware.com/es/products/datacenter-virtualization/vsphere/mid-size-and-enterprise-business/features.html