ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

MAESTRÁA EN SEGURIDAD INFORMÁTICA APLICADA

“IMPLEMENTACIÓN DE UN RADIUS SERVER COMO MÉTODO DE AUTENTICACIÓN PARA TRABAJADORES CON ACCESO INALÁMBRICO DE UNA EMPRESA STARTUP UTILIZANDO RASPBERRY COMO PLATAFORMA PARA HARDWARE”

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

JOFRE JAVIER HARO BULGARIN

GUAYAQUIL – ECUADOR

2016

AGRADECIMIENTO

A Dios por darme apoyo cada día.

DEDICATORIA

Dedico el presente trabajo mi abuela Maria por su apoyo incondicional.

TRIBUNAL DE SUSTENTACIÓN

RESUMEN

En el Capítulo 1 se presenta visión general de la situación actual de la empresa startup situada en la ciudad de Guayaquil en cuanto a la falta de un esquema de autenticación para sus trabajadores para accesar los recursos informáticos de la empresa y la solución propuesta.

En el Capítulo 2 se revisará la metodología del desarrollo de la solución del sistema de autenticación analizando la plataforma y metodología de autenticación seleccionada, de igual manera el software como aplicativo como mejor opcion para aplicarse y las pruebas respectivas.

En el Capítulo 3 se analizará los resultados de las pruebas de lo recopilados en el capítulo 1 como análisis comparativo para confirmar las mejoras en el método de autenticación de esta empresa.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad se tiene plena conciencia de los procesos de seguridad informáticos relacionados con los recursos informáticos y en especial con el contenido que estos poseen y que son de gran valor para las empresas del cual depende su funcionamiento y continuad del negocio. [1]

La ISO/IEC 17799:2005 fue creada con el objetivo de poder llevar un mejor control de los recursos informáticos de una organización no importan la naturaleza del negocio que esta esté prestando a la sociedad. En este standard se da claramente reglas de cómo preservar la información asi como la confidencialidad, la fiabilidad, autenticidad, fiabilidad el no repudio. [1]

La sociedad en general debe proteger su información tanto personal como empresarial la cual puede ser usada para beneficios ajenos y como resultados afectara la continuidad del negocio afectando o no solo servicios privados sin o también servicios gubernamentales que podría acarrear problemas como la falta de servicios de importancia fundamental para la generación de ingreso a los estados. [1]

El trabajo que presento detalla la situación actual de una empresa que inicia sus actividades con bajo presupuesto y que maneja información valiosa para su funcionamiento la misma está al alcance de sus empleados de manera continua, pero con un sistema de autenticación básico el cual hace notar la vulnerabilidad que esta empresa posee para manejar su sistema de información.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

Una empresa dedicada a la venta de insumos textiles domiciliada en la ciudad de Guayaquil ha iniciado sus operaciones la misma posee un presupuesto reducido y en especial lo asignado para su sistema de información, sus actividades las inicio en agosto del 2016 iniciando con un reducido personal de ventas el cual tiene contacto directo con el cliente final el cual se clasifica al por mayor y al por mejor.

Esta empresa tiene desarrollado un método de autenticación básico para que los trabajadores accedan a los recursos informáticos y accedan vía inalámbrica para distintas tareas entre ellas revisión, control y venta de su inventario los cuales se basan en insumos textiles de alta calidad y un valor elevado lo cual hace que la empresa

tenga un método de autenticación considerable en función de proteger sus viene.

1.2. Descripción del problema

Debido al presupuesto limitado que tiene esta empresa startup la cual se dedica a la venta de materiales en la industria textil, decidió que su red de acceso seria solo tipo wireless. Esta empresa startup tiene una infraestructura básica y rudimentaria de Internet, con relación a la parte de autenticación de los trabajadores, estos acceden a la Internet de la empresa a través de tres access point los cuales poseen un único SSID. Los trabajadores en gran mayoría son asesores de ventas, personal administrativo y operativo.

Todo el personal de la empresa tiene equipos asignados para tener acceso directo a la base de datos del inventario que posee la empresa. En la figura 1.1 podemos observar la infraestructura de Internet que tiene la empresa. Esta empresa con poco tiempo en el mercado ha sufrido varias intrusiones de personas ajenas a la empresa debido que algún trabajador ha compartido las credenciales de acceso a la red wireless.

Como primera medida ha decidido que solo los equipos asignados a la nómina de los trabajadores deberían accesar a la red de la empresa, pero esta medida lo ha logrado de manera parcial debido que no tiene personal técnico que tenga conocimiento de accesar las MAC ADDRESS en los access point y los mismo tienen limitación en la cantidad de estas que puedan ser ingresadas.

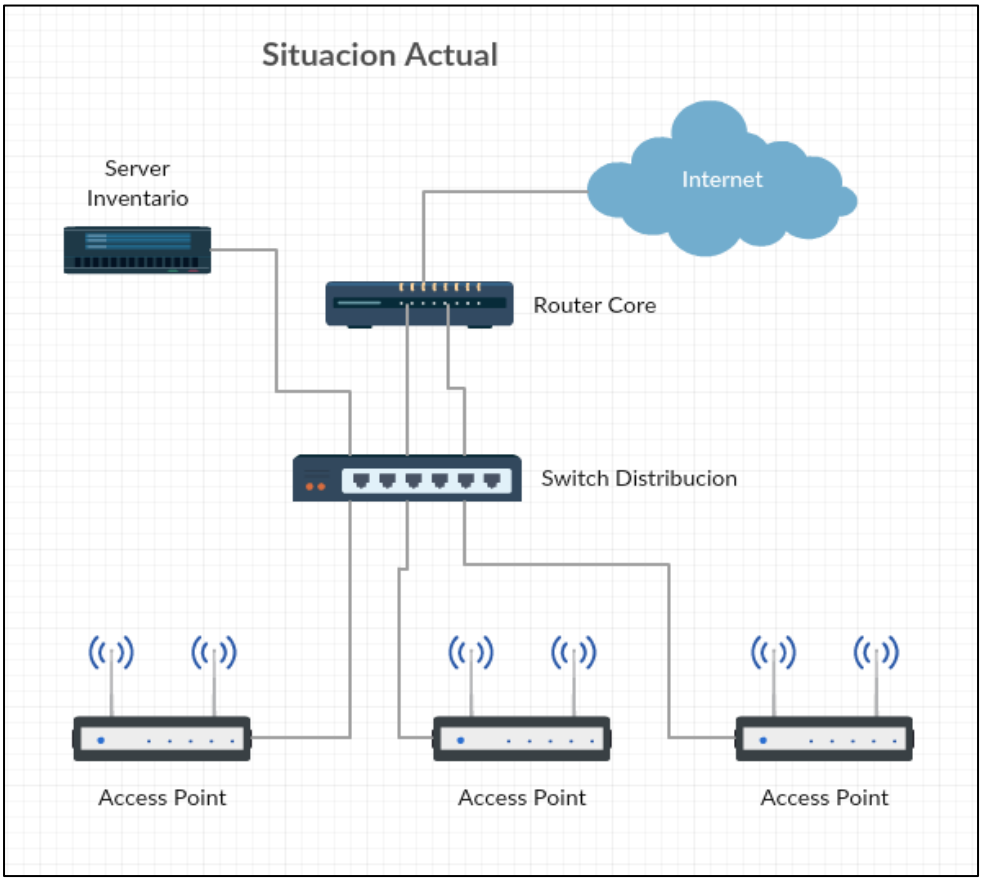

Figura 1.1 Situación actual de la empresa

La empresa tiene proyectado un considerable crecimiento, pero teme que sufra de alguna intrusión a su red y puedan sufrir pérdidas que puedan afectar de manera considerable su funcionamiento además

ha observado que los trabajadores usan la red de la empresa parra access a Internet en sus momentos de descanso lo cual esta congestionando la comunicación con sus proveedores y demás.

En conclusión, esta empresa startup requiere llevar una auditoria en línea de los trabajadores que están accediendo a su Internet a través de la red de acceso wireless: cantidad de usuarios registrados, restringir por MAC ADDRESS, asignación de ancho de banda como registro, asignar a cada empleado única credencial, usuarios bloqueados por razones varias, usuarios dados de baja, disponibilidad de ancho de banda según la cantidad de usuarios registrados, asignación de ancho de banda ocupado según usuario registrados, respaldo del sistema de autenticación.

La empresa tiene limitado su presupuesto para implementar este sistema de autenticación para lo cual pide se proponga un sistema el cual se acople al dimensionamiento de su cantidad de trabajadores dejando un cuarenta por ciento de capacidad para incrementar su nómina con una plataforma económica y rentable.

1.3. Solución Propuesta

Tomando en cuenta que la empresa no tiene un sistema de autenticación que proteja su sistema de información se recomienda Implementar un sistema de autenticación capaz de proveer el servicio a los trabajadores que acceden vía wireless en los access point. La empresa tiene una nómina de cuarenta empleados los cuales deberán ser migrados al sistema de autenticación propuesto.

Se propone implementar el sistema de autenticación usando el modelo AAA (Authentication, Authorization and Accounting). Este modelo de autenticación tiene muchos años en funcionamiento el mismo ha sido usado ampliamente demostrado su capacidad para ser aplicados en sistemas de autenticación, este modelo este modelo AAA la primera etapa de autenticación es como su nombre lo indica, el usuario deberá demostrar quién es proporcionando su clave respetiva cuando el server lo requiera, es decir este paso es uno de los pilares para los sistemas de autenticación para poder acceder a la red que esta requiriendo. En el paso de autenticación hay diferente modelo como el normal, distribuido y roaming, dependiendo donde este el usuario haciendo este requerimiento.

En el paso de autorización se revisa los privilegios que tiene estos usuarios, pero tomando como referencia quien es, en este paso se le proporcionara los privilegios específicos que él solicita lo cuales ya fueron cargados en la base de datos donde ha sido creado el usuario. Cabe indicar que estas autorizaciones también se basan en las restricciones que tendrá este usuario según como ha sido creado en la base de datos por la organización y esto lo podrá limitar a los niveles de acceso que tendrá. Algo muy importante que realiza esta fase también es controlar los accesos simultáneos que podría intentar realizar el usuario. Los permisos a los cuales se les da a un usuario están dados en función de lo que permite los diferentes departamentos de una organización y no de lo que usuario desea accesar. Por ejemplo, para controlar los servicios que el usuario tendrá accesos podrian basarse en el rango de IP que se le pueda asignar y también parámetros de QoS.

El otro paso es la contabilización como parte del modelo AAA, esta fue creada para llevar estadística de consumo de recursos en la red por los usuarios que han podido validad su identidad. Las los ISP, organización y pequeñas pymes es de mucha importancia debido que esto les puede servir para llevar estadísticas y poder asi dimensionar su red informática de mejor maneja en caso que sea

necesario. El modelo AAA permite llevar la contabilización en tiempo real en caso que alguna organicen lo requiera todo dependiendo como sea configurada.

El protocolo RadiusServer que usa este modelo AAA es de código abierto lo cual garantiza ser de mucha ayuda a empresa de baja escala para ser implementada en su organización, según se muestra en la figura 1.2 sobre este Radius Server estará corriendo FreeRadius, daloRadius, MySQL, PHP y Apache. [3]

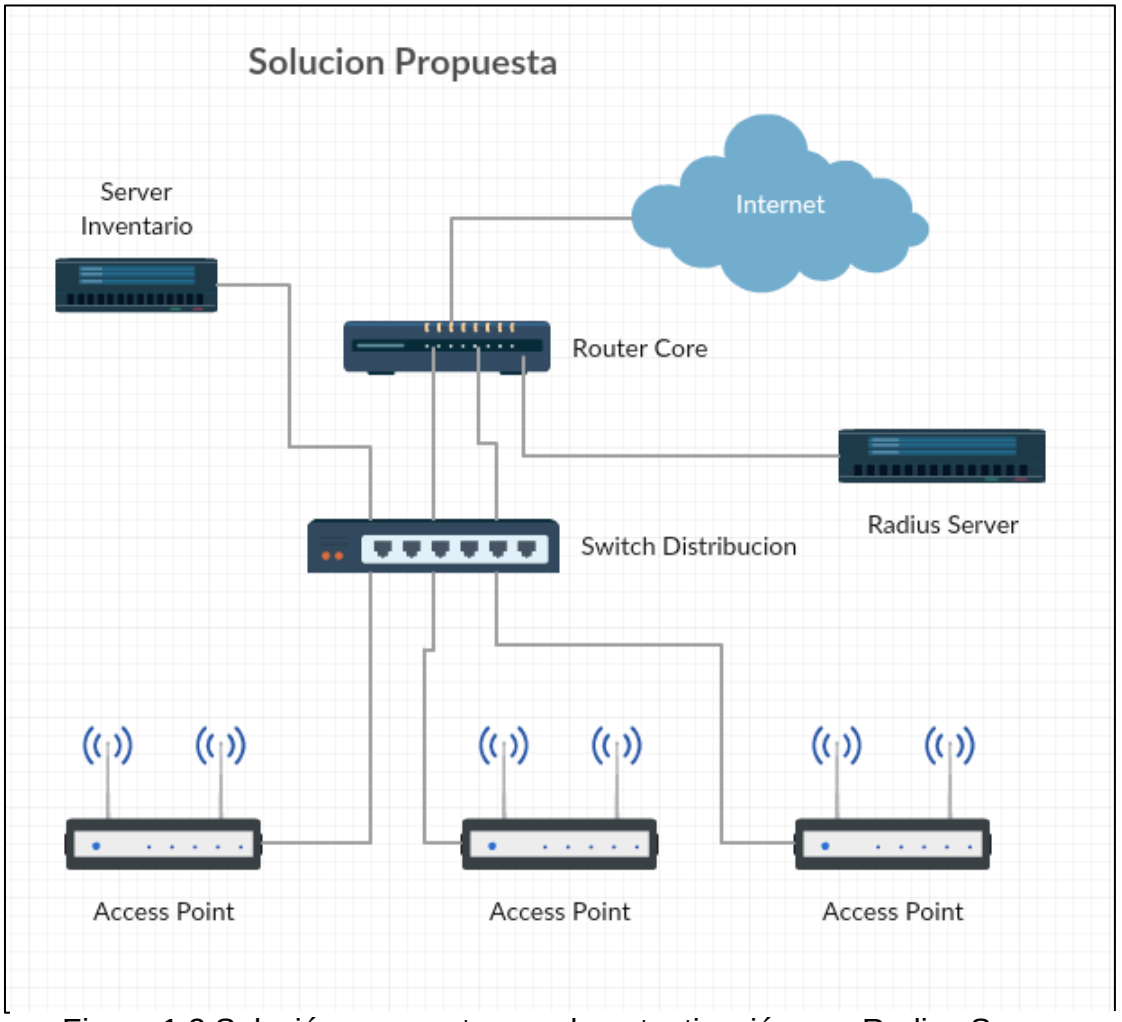

Figura 1.2 Solución propuesta para la autenticación con Radius Server

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. Modelo y protocolo de autenticación

El protocolo de aplicación Radius Server funciona sobre UDP a diferencia del protocolo Diameter que trabaja sobre TCP. La diferencia entre estos dos protocolos de autenticación es el control de congestión que posee Diameter lo cual es una de las debilidades de Radius Server. A continuación, se muestra el esquema de cómo trabaja Radius Server método de autenticación elegido como solución para esta empresa.

En la figura 2.1 se puede observar un flujo básico de cómo trabaja Radius Server, la interacción con el cliente en este caso con los usuarios finales será de vital importancia que esté funcionando en toda su capacidad para brindar un óptimo servicio.

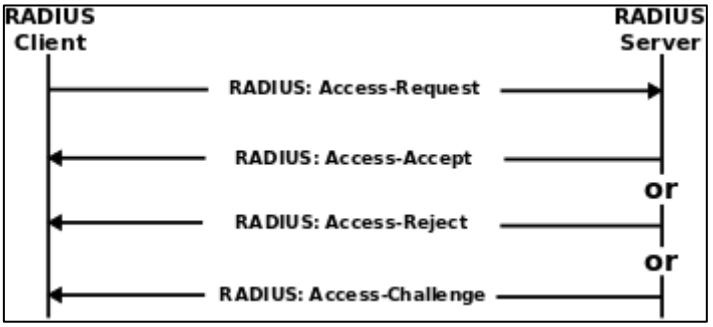

Figura 2.1 Flujo de comunicación del protocolo Radius Server [2]

El cliente Radius realiza un requerimiento al Radius Server para poder autenticarse y acceder a los servicios informáticos, pero antes deben pasar alguna prueba de confianza el cliente, para la solución propuesta al cliente se creará un usuario para cada empleado el mismo que será de absoluta responsabilidad de este.

2.2. Servidor de aplicaciones de autenticación

La limitante del cliente era el presupuesto destinado para esta solución se optó por un Raspberry modelo 2 B el cual tiene un costo muy asequible para este tipo de empresa, en el cual está instalado Debian(Raspbian) esta distribución de Linux es proporcionada por la empresa que crea los módulos de Raspberry. En la figura 2.2 podemos observar más detalles acerca de la version de Debian

usada por esta plataforma.

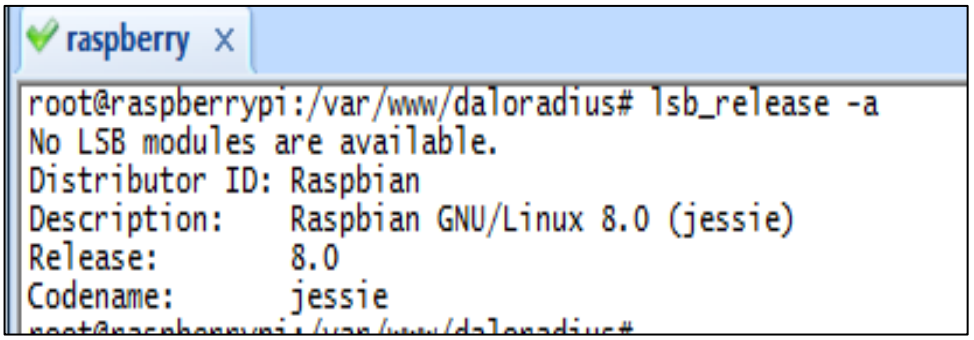

Figura 2.2 Distribución de Linux usada en plataforma Raspberry Pi

Este Raspberry requiere de una alimentación de 5V y 1A DC tipo mini USB, tiene cuatro puertos USB 2.0 capaces de porprocionar acceso a dispositivos externos como memorias para expansión y demás, tiene un puerto ethernet el cual proporcionar conectividad LAN, en el procesador de este Raspberry. El procesador brinda la solución de wifi y bluetooth de manera integrada, para esta solución no la utilizaremos debido que su alto procesamiento interferirá con el rendimiento para el óptimo funcionamiento del Radius Server, este Raspberry posee un mini slot para integrar una memory stick hasta 64 GB de capacidad, para esta solución se adquirió una memoria de 32 GB en el cual estará aojada el sistema operativo la base de datos

MySQL, y los demás servicios, en la figura 2.3 se pude observar la calidad que tiene el Raspberry y la usada donde ya está instalado todos los servicios con la base de datos creada con MySQL. [4]

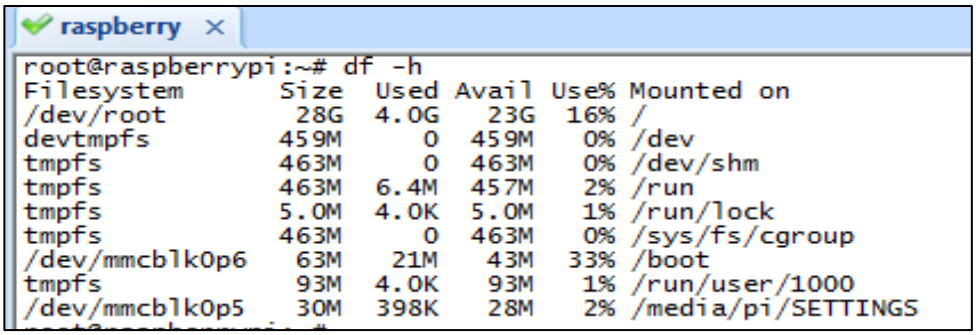

Figura 2.3 Capacidad y distribución en Raspberry con Raspbian

2.3. Desarróllo de Radius Server como plataforma de autenticación

Como paso previo para iniciar la instalación del Radius Server se procedió con la instalación del sistema operativo Raspbian 8.0 el cual está alojado en una memoria con capacidad de 32 GB, ahora se procederá con la instalación según se va indicando paso a paso, instalaremos y configuraremos un server Apache, MySQL y PHP con lo cual tendremos un LAMP Server.

Primero procedemos con la update de las librerías del Raspbian el cual servirá para descargar los diferentes servicios que usara Radius Server, la figura 2.4 nos muestra el update que sufre Raspbian antes de instalar los diferentes servicios.

Figura 2.4 Update en librerías de Raspbian

Ahora se procede con la instalación de Apache con el siguiente comando: [7]

apt-get install apache2 apache2-doc apache2-utils

Figura 2.5 Instalación de Apache

En la figura 2.5 podemos observar el proceso de instalación de Apache. Después de este primero paso instalaremos PHP con los siguientes comandos

apt-get install libapache2-mod-php5 php5 php-pear php5-xcache

apt-get install php5-mysql [7]

En la figura 2.6 y 2.7 podemos observar las fases de instalación de PHP.

Figura 2.6 PHP fase 1

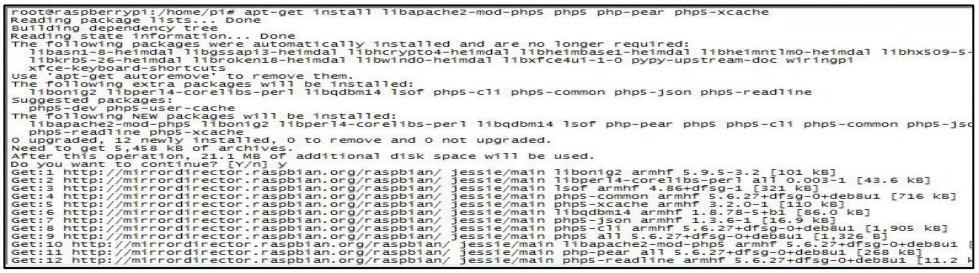

Figura 2.7 PHP fase 2

Como siguiente paso se procederá con la instalación de la base de datos MySQL con el siguiente comando

apt-get install mysql-server mysql-client [7]

En la figura 2.8 se puede observar el proceso de instalación de MySQL.

Figura 2.8 Instalación de MySQL

El siguiente paso es configurar el Raspberry como IP estática, pero el Router Ubiquiti modelo EdgeMax que posee el cliente nos provee la opcion de separar IP como estática y con chequeo de MAC ADDRESS lo cual se la mayor seguridad para separar una IP estática al Radius Server.

En la figura 2.9 se puede observar cómo se configura IP estática desde el Router lo cual no hace necesario configurar desde Radius Server.

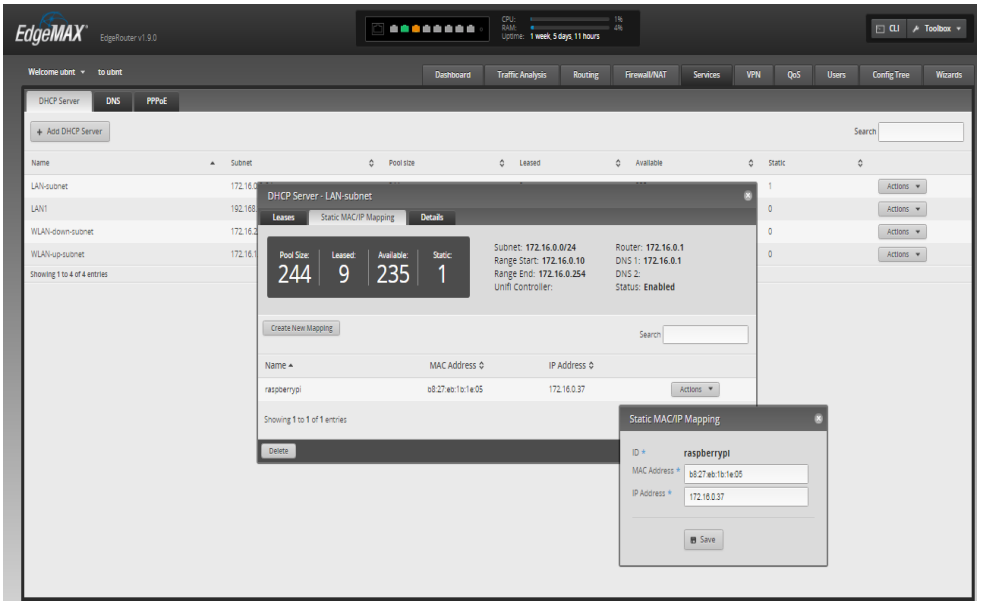

Figura 2.9 Configuracion de IP estática para Radius Server desde el Router

Ahora procederemos con la instalación de FreeRadius en cual actuara como un GUI en conjunto con daloRADIUS para la interacción del Administrador del Radius Server de manera amigable, los siguientes comandos son para la instalación de FreeRadius:

sudo su

apt-get install freeradius freeradius-mysql php5-gd php-db

Instalamos daloRADIUS:

cd /usr/src

wget

http://downloads.sourceforge.net/project/daloradius/daloradius/dalor

adius0.9-9/daloradius-0.9-9.tar.gz

tar xvfz daloradius-0.9-9.tar.gz -C /var/www

mv /var/www/daloradius-0.9-9/ /var/www/daloradius

cd /var/www/daloradius [7]

Inicializamos la base de datos MySQL parqa FreeRADIUS con el siguiente procedimiento:

mysql -u root -p

CREATE DATABASE radiusdb ;

exit

mysql -u root -p radiusdb < /var/www/daloradius/contrib/db/fr2-mysql-

daloradius-and-freeradius.sql

mysql -u root -p

CREATE USER ‘radiususer’@’localhost’ ;

SET PASSWORD FOR ‘radiususer’@’localhost’ =

PASSWORD(‘radiuspass’) ;

GRANT ALL ON radiusdb.* to ‘radiususer’@’localhost’ ;

exit

Editamos en daloRADIUS var/www/daloradius/library/daloradius.conf.php lo cual permitirá que daloRADIUS sea integrado en la base de datos MySQL

$configValues[‘CONFIG_DB_USER’] = ‘radiususer’ ;

$configValues[‘CONFIG_DB_PASS’] = ‘radiuspass’ ;

$configValues[‘CONFIG_DB_NAME’] = ‘radiusdb’ ;

Configuramos en FreeRADIUS con la creación de usuario y password

Se requiere editar /etc/freeradius/users

client 172.16.0.0/24 {

secret = prueba123

shortname = oficina-principal

} [7]

2.4. Pruebas del sistema de autenticación con Radius Server

Ahora procedemos con varias pruebas para verificar el correcto funcionamiento de Radius Server, procedemos con detener y reiniciar el servicio FreeRadius:

service freeradius stop

service freeradius start

Con el siguiente comando simulamos un requerimiento y si esta todo correctamente configurado obtendremos como respuesta “Access-Accept”.

radtest “TEST” hello localhost 0 prueba123

Finalmente procedemos con la fase final de pruebas configurando FreeRADIUS en la base de datos MySQL, editamos en archivo de configuración /etc/freeradius/radiusd.conf removiendo “#” que esta como comentarios para podernos activar:

$INCLUDE sql.conf

$INCLUDE sql/mysql/counter.conf

Ahora editamos /etc/freeradius/sql.conf para que refleje lo siguiente:

server = “localhost”

login = “radiususer”

password = “radiuspass”

radius_db = “radiusdb”

Para finalizar debemos editar /etc/freeradius/sites-enabled/default retirando “#” los comentarios para poder activar

“authorize”

“accounting”

“session”

“post-auth” [7]

Finalmente procedemos con el reinicio del Raspberry para verificar su correcto funcionamiento:

reboot

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1. Análisis comparativo

Para realizar un análisis comparativo se procedió con la verificación después de la implementacion de este sistema de autenticación algunas variables que la empresa puede manejar como percepción de los medios de autenticación, manejo seguro según el estándar ISO 27001 el cual proporciona buenas método de aseguramiento de la información.

Antes esta empresa solo requería compartir la única clave de los access point a los empleados los cuales a su vez la usaban para accesar a los diferentes recursos informáticos de la empresa y no existía un control estricto de quien y a que recursos informativos cada empleado ingresaba.

Ahora la empresa maneja de maneja estricta los accesos y uso de los recursos informativos de cada empleado gracias al modelo AAAA, nótese que la empresa está en capacidad de llevar un auditoria en línea de cada empleado mientras estén autenticados en la red. Según se muestra en la figura 3.1 daloRADIUS es muy rico en la información del comportamiento de cada usuario

Figura 3.1 Interface gráfica daloRADIUS

3.2. Análisis de los resultados obtenidos

Notamos la mejoría en relacion al control de acceso que tiene la empresa de cada empleado en tiempo real y no solo compartiendo la única clave con todos ellos. Observamos una resistencia natural de los empleados para aceptar el nuevo método de autenticación, pero se procedió con la socialización del uso de este método el cual traerá muchos beneficios para la empresa y para todos los empleados debido que la empresa ya no tendrá comprometida la continuidad del negocio, ahora el control de acceso se dara a cada empleado según su rango y departamento que pertenezca.

El dueño de esta empresa comprendió después de ver los resultados con el nuevo método de autenticación los beneficios que ha obtenido cuando fue instalado Radius Server, siempre aplicando normas de seguridad, aunque eso implique inversiones desde cientos de dólares hasta millones siempre conlleva beneficios para el aseguramiento de los sistemas informáticos de las empresas.

CONCLUSIONES Y RECOMENDACIONES

1. Cuando finalice este trabajo y liego de haber implementado este sistema de autenticación en una empresa que inicio sus actividades como proveedor de insumos para textiles teniendo que mejorar la menar como sus empleados se deberían autenticar para acceder a los recursos informáticos, se concluye que:

2. Cuando se realizó el levantamiento de información acerca de cómo esta empresa tenía implementado el sistema de autenticación para sus empleados se concluye que esa extremadamente básica sin ningún tipo de cuidado al permitir que los empleados conocían la única clave de la red wireless para accesar a la red no garantizaba la seguridad de la red.
3. El incremento paulatino de los empleados que eran contratados por esta empresa hacia caóticos el control de acceso de cada uno

de estos a los recursos informáticos he incrementaba algún tipo de ataque informático a la red debido que el método de autenticación era conocido por todos y fácilmente podrian ser compartidos con personas ajenas a la empresa.

4. Se requería establecer de manera diaria el cambio de clave para que todos los empleados se puedan autenticar en la red asi como realizar actualización de enrutamiento debido a la congestión de la red LAN debido que la mayor parte de los empleados usaban de manera indebida la red para accesar a INTERNET para lo cual no fue creada la red de esta empresa.

5. La falta de socialización a los empleados por parte de la empresa permite que extraños a la empresa puedan tener acceso a los recursos informáticos en inicio como medio para accesar a INTERNET, pero este podría llevar a comprometer con el acceso a sus recueros informáticos que son de vital importancia para su funcionamiento.

6. Al finalizar este trabajo y luego de haber implementado un esquema de autenticación para una empresa proveedora de insumos textiles se recomienda que:

7. Se conversó con el dueño de esta empresa y se recomendó cuando tenga el presupuesto necesario fortalezca el sistema de autenticación con un segundo Radius Server como método de respaldo en caso que el primero falle, esto protegerá la continuidad del negocio de esta empresa.

8. Se puede seguir utilizando como base de datos MySQL el cual es instalado en el Raspberry hasta cuando se detecte una alta carga de CPU lo cual nos indicara que el cliente deberá una otro dispositivo donde deberá alojar esta base de datos, al momento de realizar esta implementacion no se logró un stress de la plataforma para confirmar la máxima transacciones que podría soportar esta plataforma.

9. Para poder garantizar la continuidad del negocio de esta empresa requiere de manera oportuna se integre un segundo Raspberry para poder tenerlo como respaldo, de igual manera esta empresa debido que su principal recurso es el manejo de su inventario se implemente de manera oportuna un respaldo de la base de datos de sus empleados en la parte de autenticación se aloje en otro lugar físico para garantizar en caso de afectación total de sitio esta plataforma de autenticación pueda ser restablecida en el menor tiempo usando esta respaldo remoto que fue recomendado.

10. Se realice socialización y capacitaciones de manera continua para los empleados pueden administrar sus credenciales de manera responsables y tener conocimiento de los riegos en casos de compartir esta información con otros empleados o extraños a la empresa.

BIBLIOGRAFÍA

[1] ISO/IEC 17799:2005, Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

[2] Protocolo AAA, https://es.wikipedia.org/wiki/Protocolo_AAA

[3] Modelo de flujo de Radius Server, https://en.wikipedia.org/wiki/RADIUS

[4] ISO/IEC 27001:2011 Tecnología de la Información – Técnica de seguridad – Sistema de Gestión de la Seguridad de la Información (SGSI).

[5] Raspberry Organización, https://www.raspberrypi.org

[6] Raspberry FreeRadius,

http://www.binaryheartbeat.net/2013/12/raspberry-pi-based-freeradius-server.html

[7] RADIUS Server,

https://www.globalknowledge.com/us-en/resources/resource-library/white-papers/building-installing-and-configuring-a-radius-server/