CONCLUSIONES

En todo sistema informático es de vital importancia proteger cada uno de sus componentes, como son: hardware, software, datos, memoria y usuarios. Cualquiera de estos es vulnerable y proclive a ataques. Para mejorar la seguridad de un sistema de información se puede hacer uso de los servicios de seguridad cuya meta es evitar los ataques a sus componentes, evitando así la interrupción, intercepción, modificación y generación de contenido diferente al que el usuario original pretende enviar. Si se cumplen estos servicios de seguridad se considera que los datos están protegidos. Los servicios son: confidencialidad, integridad, disponibilidad, no repudio, control de acceso, autenticación.

El control de acceso se refiere al dispositivo que controla el acceso a un medio de información, tal como un monitor por el cual se verifica si es posible el acceso o no. Este acceso requiere una verificación, en este caso, una autenticación por la cual se compruebe que la persona que requiere el acceso tiene la autorización para realizarlo. El servicio de autenticación asegura que la comunicación proviene de una fuente autentica y mantiene ese aspecto durante todo el proceso de comunicación. En general, el proceso utiliza algo que se tiene, algo que se sabe, algo que se es, y que poseen las fuentes que originan la comunicación.

Por otro lado, las vulnerabilidades de un servidor o servicio de autenticación son los agujeros o bugs de seguridad, documentados o no, que ayudan a los hackers a encontrar las puertas traseras de acceso a un sistema.

A medida que se van divulgando y se van haciendo conocidas, todas ellas se van solucionando por parte de los programadores que crean los programas; pero el principal problema consiste en que los administradores y los usuarios suelen ser mucho más lentos actualizando sus sistemas

Este trabajo aporta un estudio del servicio de la autenticación, donde se ofrece a un administrador de red la posibilidad de aplicar una política de seguridad uniforme en todos los dispositivos de red, basándose en la Autenticación, Autorización y Auditoría, conocida como AAA. Este tipo de política tiene dos ventajas: provee a un administrador

de red la capacidad de centralizar toda la información contable, y crea un nivel de acceso que pueden aplicarse uniformemente a través de la red. Los protocolos más utilizados asociados a la AAA son Kerberos, Remote Authentication Dial-In User Service (RADIUS) y Lightweight Directory Access Protocol (LDAP).

Esta política maneja conceptos claros respecto a lo que es la autenticación, definiéndole como el proceso en el que se identifica un usuario en un dispositivo. La autorización es lo que determina el nivel de acceso a los que un usuario tiene acceso. Ambos son registrados por la auditoría, que permite tener un control sobre cada uno de los usos que se le han dado a un dispositivo.

En este trabajo se han realizado implementaciones prácticas para observar el funcionamiento la autenticación en diferentes servidores implementados bajo plataformas en Windows y Unix, donde se observa que este servicio de seguridad proporciona una gran seguridad dentro del sistema informático, ya que al implementar este servicio en una red de datos se puede llevar una eficaz administración en la creación y asignación de perfiles para los usuarios que tienen acceso al sistema, controlando con esto la identidad y autorizar el acceso a los distintos recursos que conforman la red de datos.

Analizando las implementaciones realizadas de los servidores de autenticación que emplean los protocolos Kerberos, Radius y LDAP bajo las plataformas en Windows y Unix, se pueden comparar sus características y elegir la mejor opción de acuerdo a la necesidad del usuario en base a su complejidad de instalación, administración y optimización de recursos.

Para el rubro de “complejidad de instalación” se considera como el más adecuado al servidor de autenticación bajo la plataforma en Windows con los protocolos Kerberos, Radius y LDAP, esto porque la instalación de Windows Server soporta cualquiera de los tres protocolos mencionados, sólo basta con elegir el tipo de protocolo que se desea implementar y continuar aplicando las políticas deseadas. Esto para el administrador significa de gran utilidad ya que permite realizar una instalación con baja complejidad y sin necesidad de conocer conceptos de programación.

Se considera al servidor de autenticación Fedora Directory Server bajo el protocolo LDAP como la mejor opción para la administración de la red de datos, esto porque analizando su interfaz de usuarios resulta bastante amigable diseñar el árbol para la asignación de perfiles, así como realizar la autorización de los distintos recursos de la red de datos.

Los servidores de autenticación bajo la plataforma Unix se consideran como los más ideales para la optimización de recursos en el servidor donde se instale la aplicación, esto porque es menor el consumo de memoria RAM por la poca utilización de gráficos, además se necesita menor cantidad de disco duro para instalar un Sistema Operativo UNIX, que al instalar un servidor bajo plataforma Windows.

En el caso de los servidores de autenticación tratados en este trabajo de tesis, con los años de vida que tienen cada uno de ellos, se han encontrado gran cantidad de fallos de seguridad y vulnerabilidades en los métodos de encriptación utilizados y en sus módulos de funcionalidades. Por supuesto que si se mantienen dichos servidores actualizados y al día, con los últimos componentes, es muy difícil que esto suceda. Y esta es la primera y primordial tarea para la implementación de un servidor de autenticación: mantenerse informado y actualizado.

Finalmente, hay que recordar que la seguridad integral de un sistema la decide el componente de seguridad más débil que incorpore. Un método avanzado de autenticación debe ser el único permitido para el acceso; activar métodos avanzados de seguridad y dejar los más débiles también activados, reduce la seguridad total al más débil.

.