INTRODUCCIÓN

La transmisión y flujo de información en redes de datos ha crecido aceleradamente durante el último par de décadas, principalmente por la facilidad con que es posible acceder a un equipo de cómputo e implementarlo en la mayoría de los rubros de la vida diaria, afectando principalmente las formas de comercio y la economía en general, con lo cual las decisiones comerciales deben ser tomadas cada vez con mayor rapidez lo que implica que aquellas personas que las toman, tengan acceso inmediato a información exacta y segura.

Sin embargo, no sólo es necesario que la planeación de una red incluya los aspectos de funcionalidad y rapidez, que son visibles para el usuario, sino que adicionalmente debe contemplar todos los aspectos necesarios que permitan a la red mantener la robustez necesaria a fin de mantenerse óptima, segura, funcional y en permanente crecimiento.

El flujo de información es de suma importancia y ha conseguido un aumento considerable; por lo que no sólo la información personal de los usuarios de la red es transmitida, ya sea de sus cuentas bancarias, contraseñas, datos personales o simples conversaciones, también se transmiten datos de investigaciones y mercantiles de una empresa, al igual que todos los documentos laborales de las mismas; es decir, en esta época cualquier información es valiosa.

Considerando que la transmisión de información en una red de datos es el intercambio de datos entre dos dispositivos a través de algún medio de transmisión, la *seguridad de la información* tiene gran importancia para la realización de este trabajo, ya que la transmisión de datos debe cumplir una efectividad en el sistema de comunicación.

En este sentido, las comunicaciones en redes de datos no siempre son seguras. Para evitar este defecto se deben aplicar servicios que garanticen la *seguridad informática* del sistema, tales como la confidencialidad, autentificación, integridad, no repudio, control de acceso y disponibilidad.

En un sistema de transmisión de información, la *confidencialidad* es la capacidad de asegurar que sólo las personas autorizadas tienen acceso a ella, la *autenticación* o *autentificación*[1] es considerada como la forma de verificar la identidad entre los participantes de una comunicación, la *integridad* garantiza que la información no ha sido alterada o destruida en el lapso de transferencia, el *no repudio* ofrece la prevención tanto a emisores como a receptores de comprobar que su mensaje fue transmitido, el *control de acceso* en un sistema ofrece la opción de poder controlar qué usuario está autorizado para usar un recurso del sistema y la *disponibilidad* hace referencia a poder acceder a la información deseada cuando lo requiera y cuantas veces sea necesario por el usuario previamente autorizado.

Cabe mencionar que cada uno de estos servicios puede ser muy sencillo o extremadamente complejo, según el número de usuarios y niveles que garanticen la seguridad.

El presente trabajo de tesis, se enfocara en la *autenticación* de equipos de una misma red, centralizando el análisis en los protocolos que se utilizan para el reconocimiento entre las diferentes entidades, y se basará en el supuesto de que en su mayoría los equipos de las redes se encuentran interconectados por cable. De esta forma, se establecerán las características de los protocolos de autenticación con lo cual cada administrador de red puede decidir cuál será el más conveniente para el tipo de red que se pretende implementar. Este trabajo está conformado de cuatro capítulos que se encuentran debidamente relacionados.

En el capítulo uno denominado CONCEPTOS BÁSICOS se proporciona una serie de definiciones sobre la seguridad informática, redes de datos y criptografía, los cuales son explicados en términos simples con el propósito que lectores no familiarizados con estos conceptos comprendan lo abordado en este capítulo y queden claros conceptos claves para seguir con la explicación y aprendizaje de los protocolos de seguridad abordados en el siguiente capítulo.

[1] En este trabajo se referirán indistintamente los términos *autenticación* y *autentificación* como el mismo concepto.

En el capítulo dos de nombre PRINCIPALES PROTOCOLOS DE AUTENTICACIÓN se da un panorama de los distintos protocolos de autenticación que actualmente existen, donde se mencionan sus antecedentes, características de seguridad informática y en algunos casos se mencionan los servidores de autenticación que existen en el mercado. Se describirán esencialmente por tipo comercial o de código abierto sobre plataformas Windows y Unix, lo que dará un panorama para elegir las implementaciones de autenticación descritas en el capítulo siguiente.

En el capítulo tres llamado IMPLEMENTACIÓN DE SERVIDORES DE AUTENTICACIÓN se describen los pasos de instalación para el sistema operativo, instalación y configuración del servidor de autenticación y las distintas pruebas de conexión para los clientes dados de alta en el servidor, proporcionando muestras de administración en una red de datos y pruebas reales de la autenticación de un cliente con el servidor. Estas implementaciones dan paso al capítulo siguiente, donde se describen sus correspondientes análisis.

En el capítulo cuatro ANÁLISIS DE IMPLEMENTACIONES se da un análisis puntual de las implementaciones realizadas, donde se dará detalle de acuerdo a las siguientes características; administración del servidor implementado, optimización de recursos del servidor de acuerdo a las necesidades del sistema operativo y del servicio de autenticación instalado, así como eficiencia del protocolo de seguridad que emplea cada servidor de autenticación implementado.