INTRODUCCIÓN

INTRODUCCIÓN

El presente trabajo contiene la información de cómo el conjunto de redes de computadoras interconectadas a lo largo de todo el mundo, contienen información muy valiosa, la cual se encuentra compartida para el acceso de todos los usuarios.

Pero para tener acceso a dicha información se necesita saber en donde se encuentra, para ello se consulta a un Servidor de Nombre de Dominio (DNS) que es una base de datos distribuida y delimitada que contiene la ubicación de un nombre de dominio que apunta a una IP homologa.

Es decir que para que exista una comunicación entre dos servidores es necesario que cada uno tengan su propia dirección IP y esta sea única e irrepetible, al principio esta conexión empezaron con 4 nodos, pero conforme al paso del tiempo se fue aumentando el número de nodos conectados y el número de direcciones IP por lo que resulto más complicado recordar dichas direcciones.

Esta consecuencia provocó que se creara un nuevo sistema llamado DNS (Sistema de Nombre de Dominio), con las características de un sistema jerárquico en niveles.

Pero por ser de consulta pública los servidores de nombre de dominio (DNS) no tienen la seguridad, esto ocasiona que entes ajenos a la información solicitada, generen vulnerabilidades las cuales desvíen la información que no corresponde a la IP, el no contar con las herramientas necesarias para la seguridad de los DNS traería como consecuencia el caos en la Internet, entre la suplantación de identidad, como denegación del propio servicio.

Este necesita de cierta seguridad para que al momento de realizar la consulta de un nombre o una IP sea la que realmente el usuario desea.

En la actualidad hablar de seguridad es de suma importancia, es por eso que con el uso de herramientas ayude a fortalecer un sistema, y por supuesto no podría faltara en un servidor de nombre de dominio que son los encargados de responder que zonas se encuentran a su cargo.

Cuando el usuario busca en específico una página con ayuda de algún explorador (Internet Explorer, Mozilla, etc.), éste se encarga de encontrar, lo que se solicita por medio del nombre de dominio, pero se puede encontrar con pérdida de información o suplantación de dicha información.

Con la siguiente investigación se pretende ver la funcionalidad de las **Extensiones de Seguridad en los Servidores de Nombre de Dominio (DNSSEC)** para los **Servidores de Nombre de Dominio (DNS)** de la Universidad Nacional Autónoma de México, por lo que se realizaran las pruebas correspondientes para comprobar la eficiencia de dicho protocolo.

DNSSEC brinda la seguridad mediante firmas digitalizadas para evitar la suplantación de identidad, es un protocolo que se está planeando implementar en los DNS de la Universidad Nacional Autónoma de México y estar a la vanguardia en este tipo de nueva tecnología que será de gran utilidad dada su importancia.

Reforzar la trasferencia de zonas de los DNS con la utilización de las llaves de encriptación proporcionando una mayor seguridad.
Garantizando los conjunto de subdominios que se encuentran bajo unam.mx revisando su autenticidad.

Asegurando al usuario que el dominio que están consultando se encuentra registrado en los DNS de RedUNAM y la IP se encuentra en el segmento otorgado por NIC-UNAM, reforzando la trasferencia de zonas de los DNS mediante llaves de encriptación y así evitar la suplantación de identidad y denegación de servicio.

En los antecedentes se verá todo lo referente al surgimiento y quiénes son los responsables del origen del medio de comunicación más importante de lo que hoy nos comunica con todo el mundo en poco tiempo, también del funcionamiento que realizan los Servidores de Nombre de Dominio para lograr dicha comunicación.

En el capítulo 1. Se describe todo lo referente a la ciencia, que se encarga de diseñar funciones o dispositivos capaces de generar el ocultamiento de información, que hoy en día se le conoce como criptografía, abarcando desde sus orígenes y también el estudio de los diferentes algoritmos existentes.

En el capítulo 2. Contiene todo lo referente a los problemas que contenían los Servidores de Nombre de Dominio, así como el surgimiento del grupo que su objetivo principal era proteger la información mediante el uso de firmas y éstas a su vez utiliza algoritmos vistos en el capítulo 1.

Capítulo 3. En este capítulo se habla del desarrollo de las extensiones que a lo largo de los años se han logrado implementar en los servidores de nombre de dominio logrando así una mayor seguridad a algunas vulnerabilidades anteriormente mencionadas en el capítulo 2 y revisar la implementación de RNDC, TESISG y DNSSEC.