



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

**SEGURIDAD EN EL SISTEMA
DE NOMBRES DE DOMINIO**

TESIS PROFESIONAL

MARIELA LETICIA MARTÍNEZ HERNÁNDEZ



MÉXICO, D.F.

2004



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

**SEGURIDAD EN EL SISTEMA
DE NOMBRES DE DOMINIO**

TESIS PROFESIONAL QUE PARA
OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

MARIELA LETICIA MARTÍNEZ HERNÁNDEZ

ASESOR:

DR. RICARDO RIVERA SOLER



MÉXICO, D.F.

2004

DEDICATORIAS

Este trabajo está dedicado a mi familia, que tanto quiero y admiro...

A mi padre:

Por siempre darme valor y ánimos para seguir adelante y confiar en que puedo alcanzar cualquier meta que me proponga. Por que gracias a ti he aprendido que asumir un compromiso es suficiente razón para cumplirlo. Sé que somos lo más importante para ti, de la misma manera en que tú lo eres para nosotras... gracias por todos los años que hemos estado juntos y por todos los recuerdos que llevaré siempre conmigo, orgullosa de tenerte como el mejor de los padres y el mejor de los amigos.

A mi madre:

Por que en todo momento has estado a mi lado, dándome el mejor ejemplo de una mujer siempre trabajadora y siempre dedicada a su familia, enseñándome que la derrota no existe y que ante cualquier adversidad hay que levantarse y seguir adelante. Gracias por siempre escucharme y ser el sentido de mi vida... eres la mujer más admirable, la madre más paciente y amorosa, la compañía siempre agradable y la amiga más sincera. A Dios siempre estaré agradecida por haberme escogido para ser tu hija.

A mi hermana, Anyanzi:

Por que hemos sido y siempre seremos incondicionalmente amigas, sabemos lo que podemos lograr y compartimos los anhelos de cada una, siempre escuchándonos y siempre alentándonos mutuamente. Siempre serás mi hermanita querida, y espero poder ser para ti el apoyo que necesites. Te quiero mucho nena.

- Marie -

AGRADECIMIENTOS

A DIOS

Por darme una vida siempre llena de tantas bendiciones, y por dejarme alcanzar esta meta tan anhelada.

A la U.N.A.M

Por darme las bases necesarias para cumplir uno de mis más grandes anhelos, ser una profesionista. Con orgullo siempre llevaré el honor de ser universitaria.

A el Dr. Rivera

A quien además de agradecerle todo el tiempo, dedicación y apoyo que me brindó para poder realizar este trabajo, agradezco sus valiosos sentimientos que siempre dan confianza para poder hablar en momentos tristes y difíciles.

Dr. Rivera: gracias a usted se ha reconciliado una amistad que tal vez de otra forma no hubiera sido posible... gracias por escucharme y gracias por ser amigo.

A mis amigos

Con quienes he compartido mi vida, en diferentes épocas y con diferentes formas de pensar, pero siempre con la misma sinceridad y amistad incondicional.

A mis amigos de la infancia:

Diego, José Daniel, Ada Elizabeth y Nancy Cahuich.

A mis amigos de la preparatoria:

Gaby, Xuxa, Lupita, Claudia, Rosario, Arturo y Octavio.

Y especialmente gracias a Ana María y Arturo por ser mis mejores amigos y por todo lo que hemos compartido a lo largo de tantos años. Que siempre seamos los hermanos que hemos sido hasta ahora.

A el NICunam

No existe una mejor manera de comenzar a experimentar el sabor de la vida laboral, que en un lugar como el Centro de Información de RedUNAM, donde se aprende y se aporta, donde se conoce el valor del trabajo en equipo y se obtiene la satisfacción de regresar a la Universidad un poco de todo lo que nos brinda. Gracias a DGSCA por darme la oportunidad de conocer a grandes personas y amigos: Ivette, Sarai, Sandy, Lulú, Alfredo, Hans, JAMM, Genny, Luis, Paul, Gonzalo y Ale.

ÍNDICE

INTRODUCCIÓN	1
1 MARCO PROBLEMÁTICO	3
1.1 ANTECEDENTES	4
1.2 IDENTIFICACIÓN DE PROBLEMA	5
1.3 DEMARCACIÓN DEL FENÓMENO	6
1.4 CONOCIMIENTO EMPÍRICO EN EL MEDIO	6
1.4.1 Personas a entrevistar	7
1.4.2 Preguntas	7
1.4.3 Aplicación del cuestionario	9
1.4.4 Conclusión de cada pregunta	9
1.4.5 Conclusión general	10
1.5 OPINIONES PROFESIONALES	10
1.5.1 Personas a entrevistar	11
1.5.2 Preguntas	11
1.5.3 Aplicación del cuestionario	13
1.5.4 Conclusión de cada pregunta	13
1.5.5 Conclusión general	14
1.6 HIPÓTESIS PRELIMINAR	14
1.7 OBJETIVOS	15
2 MARCO TEÓRICO	16
2.1 LIBROS	17
2.1.1 Lecturas de estudio	17
2.1.2 Lectura rápida	21
2.2 TESIS	24
2.3 INTERNET	27
2.4 REVISTAS ELECTRÓNICAS	36
2.5 DIPLOMADO	41
3 MARCO CONCEPTUAL	47
3.1 ANTECEDENTES	48
3.1.1 Historia de la Internet	48
3.1.2 Historia del Sistema de Nombres de Dominio	49
3.1.3 Definiciones	51
3.1.3.1 Definiciones etimológicas	51
3.1.3.2 Definiciones de diccionario	52
3.1.3.3 Definiciones de autores	52
3.1.3.4 Definición propia	53
3.1.3.5 Sinónimos	54
3.1.3.6 Antónimos	54
3.2 MONOGRAFÍA	55
3.3 CLASIFICACIONES	57
3.3.1 Amenazas a la seguridad	57
3.3.2 Ataques y tipos de ataques	59
3.3.3 Servicios de seguridad	61

3.3.4 Atacantes	62
3.3.5 Amenazas y ataques famosos en Internet	63
3.3.6 Ataques más comunes en Internet	64
3.4 EL SISTEMA DE NOMBRES DE DOMINIO	65
3.4.1 El espacio de nombres de dominio	65
3.4.2 Servidores de nombres y los registros de origen	71
3.4.3 El cliente o "resolver"	83
3.4.4 Ataques al DNS	88
3.4.5 Implementaciones del DNS	99
3.4.6 Configuración de un DNS	99
3.4.6.1 Configuración básica	100
3.4.6.1.1 Archivo de configuración named.conf	100
3.4.6.1.2 Archivos de la base de datos	102
3.4.6.2 Configuración avanzada	105
3.4.6.2.1 Listas de direcciones y listas de control de acceso ("Address Match Lists y ACL's")	105
3.4.6.2.2 Notificación DNS ("DNS Notify")	106
3.4.6.2.3 Actualización dinámica de DNS ("DNS Dynamic Update")	108
3.4.6.2.4 Transferencias de zonas	109
3.4.6.2.5 Recursos limitados	111
3.4.6.2.6 Intervalos de mantenimiento	112
3.4.6.2.7 Servidores de nombres promotores ("Forwarders")	113
3.4.6.2.8 Servidores de nombres no recursivos	113
3.4.6.2.9 Servidores de nombres delegados ("Name servers delegated")	114
3.4.6.2.10 Servidores de nombres que resuelven ("Name servers resolving")	114
3.4.6.3 Medidas de seguridad en un DNS	115
3.4.6.3.1 Ocultar versión de BIND	115
3.4.6.3.2 Restricción de peticiones	116
3.4.6.3.3 Restricción de transferencias de zonas	116
3.4.6.3.4 Correr BIND como usuario no-root o no privilegiado	117
3.4.6.3.5 Dos servidores de nombres ("Split function name servers")	118
3.4.6.3.6 Aplicar parches de BIND	121
3.4.6.3.7 Aplicar parches de sistema operativo	121
3.4.7 Criptografía en el DNS	121
3.4.7.1 DNSSEC	122
3.4.7.2 TSIG ("Transaction Signatures")	124
3.5 TENDENCIAS	124
4 MARCO METODOLÓGICO	134
4.1 VARIABLES	135
4.2 VARIABLES DE CONTROL	135
4.3 HIPÓTESIS DEFINITIVA	135

4.4	DEFINICIÓN DEL UNIVERSO	136
4.5	DETERMINACIÓN DE LA MUESTRA	136
4.6	COSTO DE LA INVESTIGACIÓN	136
4.7	CONSTRUCCIÓN DEL CUESTIONARIO	137
4.8	CUESTIONARIO PILOTO	143
4.9	CUESTIONARIO DEFINITIVO	143
4.10	REALIZACIÓN DE LA INVESTIGACIÓN	143
4.11	TRATAMIENTO SISTEMATIZADO DE LA INFORMACIÓN	159
4.12	CONCLUSIONES POR RESPUESTA	187
4.13	CONCLUSIONES GENERALES	189
4.14	APROBACIÓN O DESAPROBACIÓN DE LA HIPÓTESIS	190
5	MARCO INSTRUMENTAL	192
5.1	PROPUESTAS DE ACCIÓN	193
5.2	PLAN Y PROGRAMA DE TRABAJO	193
	ANEXOS	194
	ANEXO 1 – CUESTIONARIO APLICADO EN EL MARCO PROBLEMÁTICO	195
	ANEXO 2 – MODELO OSI, TCP/IP Y DIRECCIONAMIENTO IP	204
	ANEXO 3 – ISO 3166	214
	ANEXO 4 – CUESTIONARIO APLICADO EN EL MARCO METODOLÓGICO	221
	GLOSARIO	271
	BIBLIOGRAFÍA Y REFERENCIAS	279

INTRODUCCIÓN

La Dirección General de Servicios de Cómputo Académico de la Universidad Nacional Autónoma de México, cuenta con una Dirección de Telecomunicaciones cuyo objetivo es el apoyar a las funciones universitarias a través de una robusta y moderna infraestructura de cómputo y telecomunicaciones, que le permite la comunicación de voz, datos y videoconferencia con el fin de integrar a la comunidad universitaria al mundo de Internet.

Dentro de la Dirección de Telecomunicaciones, existe un departamento encargado de la operación y mantenimiento de la red de datos universitaria, conocido como Departamento de Operación de la Red, el cual está formado por tres áreas:

- ◆ Centro de Operación de la Red
- ◆ Centro de Información de RedUNAM
- ◆ Centro de Asistencia Técnica

En 1997 ingresé como becaria al Centro de Información de RedUNAM, el cual se encarga, entre otras funciones, de la administración de los servidores de nombres de RedUNAM.

Tres años de trabajo en el Centro de Información de RedUNAM, me dieron la oportunidad de aprender todo lo relacionado a la administración y operación del *DNS* y de darme cuenta de la necesidad de difundir la importancia que desempeña el Sistema de Nombres de Dominio en Internet. Es así como decidí realizar una investigación que estuviera relacionada con la seguridad del *DNS* y presentarlo como trabajo de tesis para poder obtener el título de licenciado en informática.

Este trabajo se divide en 5 capítulos:

1.- Marco problemático. En este primer capítulo se presenta de manera general, los antecedentes que llevan a la realización de este trabajo de investigación, así como la identificación y demarcación de la problemática que se plantea. Se realiza un cuestionario que pretende demostrar la coincidencia de opinión de otras personas acerca del problema y se presenta una hipótesis preliminar.

2.- Marco teórico. Es el resumen del estudio de obras afines al tema, así como una serie de lecturas relacionadas. Estas lecturas son de 5 fuentes: libros, revistas, otras tesis, páginas de Internet y un seminario de seguridad informática.

3.- Marco conceptual. Se desarrolla el tema del Sistema de Nombres de Dominio, de tal manera que se pueda entender todo lo relacionado con la problemática planteada. Este capítulo presenta de manera más profunda los

antecedentes de tema y las clasificaciones de ataques tanto a Internet como al Sistema de Nombres de Dominio, así como la explicación de la manera que funciona el DNS y algunas tendencias que sigue la administración de dominios.

4.- Marco metodológico. Se realizan algunos ajustes a la hipótesis planteada en el marco problemático, para presentarse la hipótesis definitiva del trabajo. Se determina el entorno y los escenarios en donde se da el problema de la seguridad en DNS y se realiza un cuestionario que es aplicado a administradores de servidores de nombres. Finalmente se presentan los resultados de la aplicación del cuestionario y las conclusiones del trabajo que llevará a la aprobación o desaprobación de la hipótesis.

5.- Marco instrumental. Se da un plan de actividades a realizar como resultado del trabajo. Se hace un plan y un programa para cumplir con las actividades propuestas.

6.- Anexos. Se incluyen algunos apartados que complementan el trabajo.

7.- Glosario. Apartado que contiene algunas definiciones y conceptos utilizados en el trabajo.

8.- Bibliografía y referencias. Lista las obras consultadas para la realización del trabajo.

CAPÍTULO 1

MARCO PROBLEMÁTICO

1 MARCO PROBLEMÁTICO

1.1 ANTECEDENTES

Actualmente, la *Internet* conecta millones de computadoras, ofreciendo un gran número de servicios y haciendo posible el intercambio de información y comunicación entre usuarios de todo el mundo.

Internet surgió a finales de la década de los 60's bajo el nombre de *ARPAnet*, e inicialmente fue un proyecto del Departamento de Defensa de los Estados Unidos, que unía unos cuantos cientos de *hosts* con el fin de compartir recursos e información entre algunos centros de investigación. Algunos años después se adoptó *TCP/IP* como el conjunto de protocolos bajo el cual trabajaría la *ARPAnet*.

IP (Internet Protocol) es uno de los protocolos que forman parte de *TCP/IP*. De acuerdo con este protocolo, cada computadora que sea conectada a Internet, debe contar con una dirección que la identifique de manera única. Esta dirección, conocida como *dirección IP*, está formada de 4 números separados por puntos, por ejemplo, 132.248.204.69. Un usuario que intenta utilizar los recursos de una computadora remota a través de la red, deberá hacerlo por medio de esa dirección IP.

Para la mayoría de los seres humanos es más fácil recordar nombres que recordar números; es por esto, que a lo largo de la historia de la Internet, se han buscado mecanismos mediante los cuales se puedan asociar nombres fáciles de recordar para los usuarios con las direcciones IP de las computadoras.

En un principio, cuando la red era conocida como *ARPAnet* y estaba formada por un número pequeño de computadoras conectadas, la relación de nombres y direcciones de los equipos se llevaba en un archivo llamado *HOSTS.TXT*, que tenía el formato de la tabla */etc/hosts* del sistema operativo *UNIX*. Este archivo se encontraba en una máquina conocida como *SRI-NIC* perteneciente al Centro de Información de Red ("Network Information Center") del Instituto de Investigaciones de Stanford ("Stanford Research Institute").

Cada vez que un administrador de red de *ARPAnet* deseaba dar de alta el nombre de una máquina o hacer algún cambio a un nombre ya registrado, enviaba un correo electrónico a los administradores de *SRI-NIC* solicitando los movimientos necesarios.

Debido a las constantes altas y cambios de nombres y direcciones de las computadoras, los administradores de red debían obtener vía *FTP* el archivo *HOSTS.TXT* una o dos veces por semana, eliminarle los campos que no le servían al sistema operativo *UNIX* y reemplazar el */etc/hosts* anterior con este

archivo. Esto con el fin de mantener lo más actualizado posible la relación de nombres y direcciones de los equipos conectados a la ARPAnet, lo cual no era difícil por el reducido número de computadoras que formaban la red.

Cuando ARPAnet comenzó a crecer, el mecanismo del HOSTS.TXT se volvió obsoleto, ya que cada nueva máquina que se conectaba a la red representaba no solamente una nueva línea en el archivo, sino una actualización necesaria para todos los demás equipos.

La máquina SRI-NIC comenzó a presentar graves problemas de tráfico debido al elevado número de conexiones FTP que se hacían para actualizar el archivo. Asimismo, la carga del procesador cada vez era mayor, hasta el punto de volverse intolerable.

Fue entonces cuando los gobernantes de la red, decidieron que eran necesarios la investigación y desarrollo de un sistema que resolviera los problemas del mecanismo anterior. De esta manera, en 1984, Paul Mockapetris propuso el Sistema de Nombres de Dominio ("Domain Name System" o "DNS").

El *DNS* es una base de datos distribuida, que trabaja bajo la *arquitectura cliente/servidor*, donde el programa cliente es llamado "*resolver*" y el programa servidor se conoce como "*name server*" o servidor de nombres. La base de datos del DNS contiene la relación de los nombres de las máquinas en Internet, con sus respectivas direcciones IP.

Gran parte de la disponibilidad de los servicios de Internet (tales como el correo electrónico, el acceso a las *páginas web*, la transferencia de archivos, etc.), depende del buen funcionamiento de los servidores de nombres, ya que para acceder a un servicio primero debe hacerse una consulta a un servidor de nombres.

Durante 3 años de trabajo en el Centro de Información de RedUNAM (*NICunam*), tuve la oportunidad de administrar los servidores de nombres de la red de datos de la Universidad, y de darme cuenta de que debido a la importancia que tiene el DNS en Internet, ha sido blanco de diferentes tipos de ataques de seguridad, con el fin de afectar los servicios que de él dependen.

En el presente trabajo de tesis, pretendo analizar la seguridad del sistema de nombres de dominio, incluyendo los tipos de ataques que reciben los servidores de nombres. También intento que esta tesis sea, en español, una buena referencia de seguridad en DNS para los administradores de servidores de nombres.

1.2 IDENTIFICACIÓN DEL PROBLEMA

En los últimos años, el uso de Internet como medio de comunicación ha ido en incremento por la gran cantidad de servicios que brinda, los cuales van desde

el correo electrónico y transferencias de archivos, hasta complejos sistemas distribuidos que pueden ser considerados de misión crítica para muchas organizaciones.

La seguridad en los sistemas basados en Internet ha ido cobrando mayor importancia debido a la cantidad y al tipo de información que estos manejan. Existen personas conocidas como *hackers*, dedicadas a corromper la seguridad de los sistemas, con el fin de alterar, eliminar o interceptar información de manera maliciosa.

Los servidores de nombres contienen la información de los servicios que están disponibles en Internet, proporcionando las direcciones IP de las computadoras que contienen dichos servicios, y los hackers han encontrado que atacando un servidor de nombres puede lograr sus objetivos sin atacar directamente a la máquina que contiene el servicio que les interesa. Al atacar un servidor de nombres, un hacker puede lograr, entre otras cosas, interceptar el servicio de correo electrónico de una organización, puede desviar la ruta de una página web hacia sus páginas, o bien, puede interrumpir algún servicio.

Los servicios en Internet deben estar disponibles en cualquier momento y con información confiable para los millones de usuarios que la utilizan actualmente. Es por esto que la seguridad en el Sistema de Nombres de Dominio se ha convertido en un problema que preocupa a miles de administradores de red en todo el mundo.

1.3 DEMARCACIÓN DEL FENÓMENO

El problema de seguridad en los servidores de nombres, se presenta en cualquier organización que tenga o utilice sistemas basados en Internet. Sin embargo, esta investigación se enfocará a la seguridad en los servidores de nombres de las empresas y organizaciones de la Ciudad de México y Monterrey.

1.4 CONOCIMIENTO EMPÍRICO EN EL MEDIO

El conocimiento empírico es la opinión de personas calificadas, acerca del problema. Estas personas tienen conocimientos prácticos o teóricos del tema a desarrollar y no son necesariamente profesionistas al respecto.

1.4.1 Personas a entrevistar

NOMBRE	EXPERIENCIA EN EL TEMA
Genny Marisol León Leal (NICunam)	Forma parte del equipo del Centro de Información de RedUNAM, administrando los servidores de nombres de la red de datos de la Universidad.
Ivette De Luna Bonilla (Ericsson)	Actualmente trabaja en Ericsson, y tiene experiencia en la administración de servidores de nombres.
Yazzmín Castillo Martínez (INAH)	Administra la red y servidores DNS del Instituto Nacional de Antropología e Historia.

1.4.2 Preguntas

1.- ¿Qué implementaciones del Sistema de Nombres de Dominio conoce?.

Razón de la pregunta:

Determinar si está familiarizado con el Sistema de Nombres de Dominio.

Pregunta esperada:

BIND y/o DNS de Windows NT.

2.- ¿Considera que el buen funcionamiento de los servidores de nombres es un factor importante para garantizar la disponibilidad de los servicios que proporciona Internet?. Si, no, ¿por qué?.

Razón de la pregunta:

Saber la importancia de los servidores de nombres en Internet.

Respuesta esperada:

La disponibilidad de los servicios en Internet que son accedidos por nombre, dependen del correcto funcionamiento de los servidores de nombres.

3.- ¿Qué tipos de ataques de seguridad en contra de un servidor de nombres conoce?.

Razón de la pregunta:

Saber qué ataques de seguridad a un servidor de nombres son conocidos.

Respuesta esperada:

Modificación de registros, saturación, negación de servicio.

4.- ¿Desde su punto de vista, que consecuencias traería un ataque exitoso a la seguridad de un servidor de nombres?.

Razón de la pregunta:

Determinar si conoce las consecuencias de no contar con un servidor de nombres seguro.

Respuesta esperada:

Intercepción de correo electrónico, falsificación de páginas web, negación o interrupción de servicios.

5.- ¿Qué medidas de seguridad deben implementarse en un servidor de nombres?.

Razón de la pregunta:

Determinar si son conocidas las medidas de seguridad que deben aplicarse en los servidores de nombres.

Respuesta esperada:

Variada (Versión de la implementación, restricción de consultas, restricción de transferencias, configuración especial, etc.).

6.- De las anteriores medidas de seguridad, ¿cuáles ha implementado en servidores de nombres administrados por usted?.

Razón de la pregunta:

Conocer, si como administrador de servidores de nombres, ha implementado las medidas de seguridad recomendadas.

Respuesta esperada:

Si, todas.

7.- ¿Conoce sitios web dedicados o relacionados a la seguridad en los servidores de nombres? ¿Cuáles?.

Razón de la pregunta:

Saber que tanta difusión tiene la seguridad en DNS

Respuesta esperada:

Varios

8.- ¿Conoce libros dedicados o relacionados a la seguridad en los servidores de nombres? ¿Cuáles?.

Razón de la pregunta:

Saber que tanta difusión tiene la seguridad en DNS

Respuesta esperada:

DNS & BIND y Windows on NT.

1.4.3 Aplicación del cuestionario

Las respuestas obtenidas de las personas empíricas entrevistadas, se presentan en el anexo 1 de este trabajo.

1.4.4 Conclusión de cada pregunta

Pregunta 1

De las tres personas entrevistadas, dos respondieron conocer dos implementaciones del Sistema de Nombres de Dominio (DNS BIND y DNS de Windows NT) y la tercer persona contestó equivocadamente confundiendo las implementaciones del DNS con los tipos de servidores de nombres que pueden configurarse.

Pregunta 2

El buen funcionamiento de los servidores de nombres, es un factor importante para garantizar la disponibilidad de los servicios que se ofrecen en Internet, ya que el acceso a estos servicios es, en general, a través de nombres y no de sus direcciones IP.

Pregunta 3

Los tipos de ataques que conocen las personas entrevistadas, corresponden más a los realizados a computadoras con sistema operativo UNIX que al servicio de DNS en particular.

Pregunta 4

Un ataque exitoso a la seguridad de un servidor de nombres traería como consecuencia daños como el borrado o la alteración de la información que proporcionan, afectando de manera parcial e incluso total los servicios que dependen de dicha información.

Pregunta 5

Se deben implementar medidas de seguridad tanto en el servidor de nombres que alberga el DNS, como en el servidor de nombres mismo. Las medidas de seguridad en el servidor que alberga el servicio pueden ser control de acceso, autenticación y métodos de cifrado e integridad de datos, y las que deben aplicarse al servidor de nombres son el manejo de listas de acceso para restringir las consultas y transferencias realizadas.

Pregunta 6

De acuerdo a las respuestas dadas podemos concluir que las medidas de seguridad que se recomiendan aplicar a un servidor de nombres no se aplican en su totalidad.

Pregunta 7

Los sitios en Internet dedicados a la seguridad en los servidores de nombres, son poco conocidos.

Pregunta 8

En general, las personas entrevistadas sólo conocen el libro "DNS and BIND" de Paul Albitz & Cricket Liu en su versión para UNIX y para Windows NT.

1.4.5 Conclusión general

De acuerdo a las respuestas dadas por las personas entrevistadas, se puede concluir que los administradores de servidores de nombres conocen la importancia que tiene el DNS para el buen funcionamiento de Internet y los servicios que proporciona, y están concientes de las consecuencias que trae consigo un ataque exitoso a la seguridad de un servidor de nombres. Sin embargo, entre las personas empíricas en este tema, son pocos conocidos los tipos de ataques que se pueden realizar al DNS y la manera de llevarlos a cabo, y a pesar de que conocen algunas medidas de seguridad para evitarlos, no las implementan en su totalidad.

1.5 OPINIONES PROFESIONALES

Consiste en conocer la opinión de personas profesionales en el tema para conocer su punto de vista acerca del problema.

1.5.1 Personas a entrevistar

NOMBRE	EXPERIENCIA EN EL TEMA
Jorge Alberto Martínez Melo (NICunam)	Coordinador del Centro de Información de RedUNAM, administra los servidores de nombres de la red de datos de la Universidad.
Francisco Arias (NIC-México)	Forma parte del equipo de trabajo de <i>NIC-México</i> .
Gunnar Wolf (UNAM)	Experto en seguridad en cómputo, administra la red del campus Iztacala de la UNAM.

1.5.2 Preguntas

1.- ¿Qué implementaciones del Sistema de Nombres de Dominio conoce?.

Razón de la pregunta:

Determinar si está familiarizado con el Sistema de Nombres de Dominio.

Pregunta esperada:

BIND y/o DNS de Windows NT.

2.- ¿Considera que el buen funcionamiento de los servidores de nombres es un factor importante para garantizar la disponibilidad de los servicios que proporciona Internet?. Si, no, ¿por qué?.

Razón de la pregunta:

Saber la importancia de los servidores de nombres en Internet.

Respuesta esperada:

La disponibilidad de los servicios en Internet que son accedidos por nombre, dependen del correcto funcionamiento de los servidores de nombres.

3.- ¿Qué tipos de ataques de seguridad en contra de un servidor de nombres conoce?.

Razón de la pregunta:

Saber qué ataques de seguridad a un servidor de nombres son conocidos.

Respuesta esperada:

Modificación de registros, saturación, negación de servicio.

4.- ¿Desde su punto de vista, qué consecuencias traería un ataque exitoso a la seguridad de un servidor de nombres?.

Razón de la pregunta:

Determinar si conoce las consecuencias de no contar con un servidor de nombres seguro.

Respuesta esperada:

Intercepción de correo electrónico, falsificación de páginas web, negación o interrupción de servicios.

5.- ¿Qué medidas de seguridad deben implementarse en un servidor de nombres?.

Razón de la pregunta:

Determinar si son conocidas las medidas de seguridad que deben aplicarse en los servidores de nombres.

Respuesta esperada:

Variada (Versión de la implementación, restricción de consultas, restricción de transferencias, configuración especial, etc.).

6.- De las anteriores medidas de seguridad, ¿cuáles ha implementado en servidores de nombres administrados por usted?.

Razón de la pregunta:

Conocer, si como administrador de servidores de nombres, ha implementado las medidas de seguridad recomendadas.

Respuesta esperada:

Si, todas.

7.- ¿Conoce sitios web dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?.

Razón de la pregunta:

Saber que tanta difusión tiene la seguridad en DNS.

Respuesta esperada:

Varios

8.- ¿Conoce libros dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?.

Razón de la pregunta:

Saber que tanta difusión tienen la seguridad en DNS.

Respuesta esperada:

DNS & BIND y Windows on NT.

1.5.3 Aplicación del cuestionario

Las respuestas obtenidas de las personas profesionales entrevistadas, se presentan en el anexo 1 de este trabajo.

1.5.4 Conclusión de cada pregunta

Pregunta 1

Las implementaciones del Sistema de Nombres de Dominio conocidas entre las personas profesionales en el tema que fueron entrevistadas son: DNS BIND, DNS para Windows NT, DBJDNS y TinyDNS.

Pregunta 2

El buen funcionamiento de los servidores de nombres, es un factor importante para garantizar la disponibilidad de los servicios que se ofrecen en Internet, ya que el acceso a estos servicios es, en general, a través de nombres y no de sus direcciones IP.

Pregunta 3

Las personas entrevistadas conocen algunos ataques realizados al DNS. Los ataques que mencionan son: *envenenamiento de caché*, *negación de servicio*, *buffer overflows* por errores en el código del servidor, *information leakage* por mala configuración en el servidor y *DNS spoofing*.

Pregunta 4

Un ataque exitoso a la seguridad de un servidor de nombres, traería diferentes consecuencias dependiendo de la ubicación dentro del espacio de nombres de dominio del DNS atacado, las cuales podrían ir desde interrupciones de

servicio, hasta el comprometer la seguridad de toda la red en la que se encuentra.

Pregunta 5

Las personas entrevistadas conocen tanto medidas de seguridad recomendables para el servidor que alberga el servidor de nombres, como las configuraciones necesarias para implementar seguridad en un DNS.

Pregunta 6

Los profesionales en el tema aplican todas las medidas de seguridad recomendadas para un servidor de nombres.

Pregunta 7

Los sitios en Internet dedicados a la seguridad en los servidores de nombres, son poco conocidos.

1.5.5 Conclusión general

De acuerdo a las respuestas dadas por las personas entrevistadas, se puede concluir que los administradores de servidores de nombres profesionales, conocen la importancia que tiene el DNS para el buen funcionamiento de Internet y los servicios que proporciona, y están concientes de las consecuencias que trae consigo un ataque exitoso a la seguridad de un servidor de nombres, conocen los tipos de ataques que se pueden realizar al DNS, la manera de llevarlos a cabo y algunas medidas de seguridad para evitarlos.

1.6 HIPÓTESIS PRELIMINAR

Un servidor de nombres sin medidas de seguridad puede ocasionar:

- ◆ Desvío del tráfico de un dominio.
- ◆ Falsificación de páginas web.
- ◆ Robo de correo electrónico.
- ◆ Robo de información acerca de una red.
- ◆ Desviaciones de servicios.
- ◆ Negaciones de servicios.
- ◆ Desconfianza en la información que proporciona.
- ◆ Distorsión en el espacio de nombres de dominio.

Un servidor de nombres con medidas de seguridad:

- ◆ Garantiza la integridad del espacio de nombres de dominio.
- ◆ Asegura que la información que proporciona es confiable.
- ◆ Evita falsificaciones de páginas web.
- ◆ Evita la interceptación de correo electrónico.
- ◆ Evita desviaciones de servicios.
- ◆ Evita negaciones de servicios.
- ◆ Contribuye a la seguridad en Internet.

Aplicar medidas de seguridad en los servidores de nombres garantiza la integridad del espacio de nombres de dominio y contribuye a la seguridad de los servicios en Internet, asegurando que la información que proporcionan es confiable y evitando falsificaciones de páginas web, interceptaciones de correo electrónico, desviaciones y negaciones de servicios.

1.7 OBJETIVOS

Particulares:

- ◆ Concluir con mis estudios de licenciatura.
- ◆ Cumplir con los requisitos establecidos en el Reglamento General de Exámenes de la Universidad Nacional Autónoma de México (Artículos 18, 19, 20, 21 y 27) y en el Nuevo Reglamento de Exámenes Profesionales de la Facultad de Contaduría y Administración, aprobado el 29 de abril de 1999 (Artículos 7 y 44 al 56), para obtener el título de Licenciado en Informática.
- ◆ Ser experta en el tema.
- ◆ Comenzar un camino hacia la especialización en la seguridad de redes.

Generales:

- ◆ Brindar una investigación útil para muchas organizaciones e individuos interesados en el tema.
- ◆ Aportar un documento que sirva de referencia, para la comunidad universitaria de la Facultad de Contaduría y Administración.
- ◆ Aportar un documento que sirva de referencia y apoyo a los integrantes del Centro de Información de RedUNAM.

CAPÍTULO 2

MARCO TEÓRICO

2 MARCO TEÓRICO

2.1 LIBROS

2.1.1 Lectura de estudio

Lectura profunda de toda o casi toda una obra.

Título	DNS and BIND
Autor	Albitz, Paul
Editorial	O'Reilly
Edición - Reimpresión	3ra. Edición
ISBN	1-56592-512-2
Colocación en biblioteca	QA76.76D57 A53 1998
Capítulo 1 "Background"	En este primer capítulo, el autor presenta la historia de Internet y del Sistema de Nombres de Dominio ("Domain Name System"). También se hace una similitud de la organización del Sistema de Nombres de Dominio, con la estructura de archivos que tiene el sistema operativo UNIX; esto con el fin de dar una introducción a la manera en que funciona el DNS.
Capítulo 2 "How Does DNS work?"	Explica que el DNS es una base de datos distribuida, que trabaja bajo la arquitectura cliente/servidor. Consta de tres partes, las cuales son: <ul style="list-style-type: none"> ♦ El espacio de nombres de dominio.- Es la forma en la que está organizada y distribuida la base de datos que contiene la información acerca de todos los dominios de Internet. ♦ Los servidores de nombres.- Son los programas encargados de dar la información acerca de una parte del espacio de nombres de dominio total. ♦ Los resolvers.- Son los programas clientes que se encargan de obtener información, a través de los servidores de nombres, acerca de alguna parte del espacio de nombres de dominio. Se dan otros conceptos que son necesarios para entender el funcionamiento del DNS, tales como: dominio, nombre de dominio, zona, registros origen, dominios de nivel superior, delegación de zonas, resolución y tipos de resolución.

<p>Capítulo 3</p> <p>"Where Do I Start"</p>	<p>Se da información acerca de donde obtener el software para instalar un servidor de nombres. También se dan los pasos a seguir para registrar un dominio y verificar que esté en funcionamiento a través de la herramienta conocida como <i>WHOIS</i>.</p>
<p>Capítulo 4</p> <p>"Setting Up BIND"</p>	<p>Se dice como configurar un servidor de nombres, ya sea de tipo primario o secundario y se explican los registros que conforman su base de datos y la manera correcta de utilizarlos. Existen varios tipos de registros, pero los más utilizados son:</p> <ul style="list-style-type: none"> ◆ NS (Name Server).- Indica cuál es el servidor de nombres para un dominio. ◆ A (Address).- Indica cuál es la dirección IP asociada a un nombre de dominio. ◆ CNAME (Canonical Name).- Sirve para asociar alias a un registro address. ◆ MX (Mail Exchanger).- Indica el nombre de la máquina que atenderá el correo electrónico para un dominio. ◆ PTR (Pointer).- Se utiliza para indicar el nombre asociado a una dirección IP. <p>Se explica la diferencia entre los tipos de servidores de nombres y la manera de probar su funcionamiento a través de una herramienta conocida como <i>nslookup</i>.</p>
<p>Capítulo 5</p> <p>"DNS and Electronic Mail"</p>	<p>Es un capítulo muy breve que habla de la manera en que funciona el correo electrónico en Internet a través del DNS. Explica el registro MX, el cual se da de alta para indicar la manera en que será entregado el correo electrónico para un determinado dominio.</p>
<p>Capítulo 6</p> <p>"Configuring Hosts"</p>	<p>Se explica como configurar los programas clientes o resolvers para que puedan consultar a sus respectivos servidores de nombres. Se dan opciones de configuración de resolvers para diferentes plataformas, como SunOS, Solaris, HP-UX, AIX, Digital, IRIX, Open Server, Linux, Windows 95 y Windows NT.</p>

<p>Capítulo 7</p> <p>"Maintaining BIND"</p>	<p>En este capítulo se tratan aspectos relacionados con el mantenimiento técnico de un servidor de nombres. Se dice como verificar que esté corriendo el programa servidor del DNS, como reiniciarlo, como actualizar la base de datos que contiene agregándole o eliminándole registros y como configurar el servidor de nombres para que genere bitácoras de su funcionamiento. También explica los mensajes normales que genera el DNS en un ambiente UNIX y la manera en que se deben interpretar las estadísticas que genera.</p>
<p>Capítulo 8</p> <p>"Growing Your Domain"</p>	<p>Da recomendaciones para planear el crecimiento de un servidor de nombres, incluyendo las cantidad de recursos que debe de consumir en una máquina, así como las consideraciones que se deben tener para asegurar el servicio de DNS en caso de un desastre.</p>
<p>Capítulo 9</p> <p>"Parenting"</p>	<p>Se tratan aspectos técnicos de la delegación de subdominios, tales como la configuración necesaria en los servidores de nombres, la delegación de dominios in-addr.arpa, y como solicitar la delegación de un dominio.</p>
<p>Capítulo 10</p> <p>"Advanced Features and Security"</p>	<p>En este capítulo se explican características avanzadas que pueden configurarse en un servidor de nombres, por ejemplo, listas de control de acceso, especificación del puerto por el cual responderá nuestro servidor, entre otras. También se tratan aspectos importantes de seguridad, como la restricción de consultas a los DNS, la prevención de transferencias de zonas no autorizadas y la configuración de dos servidores de nombres en una misma computadora. Este capítulo es de suma importancia para el presente trabajo, ya que da las recomendaciones mínimas de configuración para tener un servidor de nombres seguro.</p>
<p>Capítulo 11</p> <p>"nslookup"</p>	<p>Nslookup es una herramienta que se utiliza para consultar la información disponible en el Sistema de Nombres de Dominio. En este capítulo se explica la forma de utilizarla para obtener la información requerida acerca de un dominio, mostrando las posibles respuestas que genera y su interpretación.</p>

<p>Capítulo 12</p> <p>"Reading BIND Debugging Output"</p>	<p>Al instalarse, un servidor de nombres puede ser compilado con la opción de <i>"debug"</i>, lo que va a permitir obtener bitácoras de la manera en que el servidor de nombres esté operando. Se tienen 5 niveles de debug, de acuerdo a la información que se desee obtener por el administrador. Este capítulo explica las bases para poder interpretar toda esa información que se arroja en bitácoras por el debug del servidor de nombres. También explica el algoritmo que se sigue en el proceso de resolución.</p>
<p>Capítulo 13</p> <p>"Troubleshooting DNS and BIND"</p>	<p>Describe los problemas más comunes referentes al DNS, la manera de identificarlos y corregirlos con algunas de las herramientas más utilizadas por los administradores de red, como <i>nslookup</i>, <i>ping</i> y <i>traceroute</i>. Presenta los escenarios de errores posibles en los que se puede encontrar un administrador de DNS, como son, olvidar incrementar el número serial de una zona, no recargar la base de datos, que el servidor secundario no se esté comunicando con su respectivo primario, errores de sintaxis en los archivos de la base de datos, pérdida de la conectividad de la red, la incorrecta delegación de una zona o la negación de un servicio.</p>
<p>Capítulo 14</p> <p>"Programming with the resolver and name server library routines"</p>	<p>El último capítulo describe la manera de utilizar las librerías que acompañan a la distribución de BIND para hacer programas en C y en perl que pudieran ser útiles a los administradores de DNS en la solución y depuración de problemas relacionados con el servidor de nombres. Contiene algunos códigos de ejemplo.</p>
<p>Apéndices</p>	<p>El libro incluye una sección de apéndices donde se puede encontrar información acerca de:</p> <ul style="list-style-type: none"> ◆ Formato de los mensajes de DNS y los registros de origen. ◆ Manual de compilación e instalación en una <i>SUN</i>. ◆ Lista de los dominios de nivel superior. ◆ Formas de registro de dominios.

Título	DNS on Windows NT
Autor	Albitz, Paul
Editorial	O'Reilly
Edición - Reimpresión	1ra. Edición
ISBN	1-56592-511-4
Colocación en biblioteca	QA76.76D57 A54
Resumen general	Este libro contiene los mismos capítulos que "DNS and BIND" y está escrito por el mismo autor, con la diferencia de que se enfoca a configuraciones del Sistema de Nombres de Dominio sobre la implementación para Windows NT.

2.1.2 Lectura rápida

Lectura de algunos capítulos de una obra.

Título	Building Internet Firewalls
Autor	Zwicky, E., Cooper, S., Chapman, B.
Editorial	O'Reilly
Edición - Reimpresión	2ª. Edición
ISBN	1-56592-871-7
Colocación en biblioteca	TK5105.875I57 C43 2000
Capítulo 1 "Why Internet Firewalls"	En este libro se dan los conceptos necesarios para poder implementar un <i>firewall</i> en una organización. En el primer capítulo se da una introducción a los riesgos que se toman al estar conectados a Internet explicando de manera general los tipos de ataques a los que está expuesta la información y servicios de una organización. Se explica el concepto de firewall y la utilidad que puede tener en el esquema de seguridad de una red.
Capítulo 2 "Internet Services"	Hace un resumen de los servicios que ofrece Internet, como son el correo electrónico, la transferencia de archivos, el servicio de nombres de dominio, noticias, conferencias, bases de datos, acceso remoto, etc. Se explican brevemente los problemas de seguridad más comunes asociados a estos servicios.
Capítulo 4 "Packets and	Explica la estructura de la pila de protocolos TCP/IP y los pasos que se siguen en la comunicación entre dos componentes de una red IP. Los tres protocolos

Protocolos"	que pueden estudiarse en este capítulo son TCP, UDP e ICMP así como algunos ataques comunes en Internet dirigidos a estos protocolos.
Capítulo 20 "Naming and Directory Services"	En este capítulo se tratan los diferentes servicios de nombres disponibles para diferentes ambientes de trabajo en red. La mayor parte del capítulo se dedica a la explicación, aunque de manera general, del Sistema de Nombres de Dominio, por ser el servicio de nombres más utilizado en Internet. También se explican otros servicios de nombres como <i>NIS</i> y <i>WINS</i> , así como algunos servicios de directorio como <i>LDAP</i> y <i>Windows Browser</i> . En la explicación de cada uno de estos servicios se incluyen las recomendaciones para su configuración en redes protegidas por firewalls.

Título	Internet Firewalls and Network Security
Autor	Siyan, K. ; Hare, Ch.
Editorial	Prentice Hall
Edición - Reimpresión	1ª edición
ISBN	1562054376
Colocación en biblioteca	TK5105.875 I57 H37
Capítulo 1 "Network Security"	Da una introducción, explicando los riesgos que se corren actualmente en el uso de Internet. Explica por que es importante proteger la información y contra quien, y discuten algunos modelos de seguridad. También da una introducción a los firewalls, que son, como funcionan y su utilidad.
Capítulo 2 "Internet Services"	Hace un resumen de los servicios más demandados en Internet y los problemas de seguridad más frecuentes en cada uno de ellos.
Capítulo 3 "Security Strategies"	En este capítulo el autor hace notar la importancia de establecer políticas de seguridad computacional en una organización y de estar investigando constantemente los nuevos mecanismos de seguridad.

Título	Practical UNIX & Internet Security
Autor	Garfinkel, S.; Spafford, G.
Editorial	O'Reilly
Edición - Reimpresión	2ª edición.
ISBN	0131089293
Colocación en biblioteca	QA76.76063 G37
Capítulo 1 "Introduction"	El primer capítulo es un resumen de la historia del sistema operativo UNIX, y una introducción a la seguridad en Internet. Se explican los términos técnicos que se van a emplear en el resto de la lectura.
Capítulo 2 "Policies and Guidelines"	Explica la importancia de establecer políticas que garanticen la seguridad en las organizaciones, de los sistemas conectados a Internet. Da una guía de como establecer estas políticas, así como su planeación, análisis de riesgos y análisis de costo-beneficio.
Capítulo 3 "Users and Passwords"	Este capítulo es una introducción a la seguridad en una computadora con sistema operativo UNIX. Explica la finalidad de los passwords, que es lo que hace que un password se considere seguro o inseguro, y los algoritmos de cifrado de passwords que el sistema operativo utiliza. También habla de la responsabilidad de ser usuario administrador de un sistema y tener acceso total a toda la información de una máquina.
Capítulo 4 "The UNIX filesystem"	Se explica ampliamente la forma en que están organizados los archivos en un sistema operativo UNIX, los tipos de archivos que puede contener, la forma de establecer permisos a los usuarios y las facilidades de restringir directorios.
Capítulo 5 "Cryptography"	En este capítulo se explican los principios básicos de la criptografía, su utilidad en la seguridad de información y explica algunos esquemas criptográficos utilizados en los servicios de Internet, como son PGP, para proteger el correo electrónico.

2.2 TESIS

Título	Sistema de Nombres de Dominio en REDUNAM
Autor	Peñaloza Pérez, Sarai Jezabel
Carrera / escuela	Tesis Licenciatura (Ingeniero en Computación)-UNAM, Escuela Nacional de Estudios Profesionales Aragón
Lugar / Fecha	México, 2000
Colocación en biblioteca	001-41132-P1-2000
Capítulo 1 "Conceptos generales"	Se presentan algunos conceptos del mundo de Internet, su historia, la importancia que ha tenido en México, así como el uso de las direcciones IP y de los nombres de dominio. También se aborda el tema de la suite de protocolos TCP/IP para entender formato que tienen las direcciones IP.
Capítulo 2 "El Sistema de Nombres de Dominio"	Se describe lo que es en sí el Sistema de Nombres de Dominio, su historia, como se encuentra organizado el espacio de nombres de dominio, los dominios en general y los servidores de nombres, como se lleva a cabo el mapeo de nombres a direcciones IP, así como también la configuración de cada uno de los archivos de la bases de datos. Se da una breve explicación de lo que es BIND.
Capítulo 3 "Herramientas de búsqueda"	Se describe el manejo de dos herramientas importantes para llevar a cabo consultas en los servidores de nombres, tanto locales como remotos: nslookup y DIG.
Capítulo 4 "El Sistema de Nombres de Dominio (DNS) en RedUNAM"	Capítulo dedicado a explicar la manera en que trabaja el Centro de Información de RedUNAM, incluyendo la manera en que está organizado el dominio unam.mx, y distribuido para todas las facultades, escuelas e institutos de la Universidad. Explica que en RedUNAM se cuenta con 4 servidores de nombres distribuidos de acuerdo a la topología de red y con un servidor de nombres secundario para el dominio mx. Describe también las políticas a seguir para el registro de dominios internos y externos en la UNAM, así como para la asignación de direcciones IP en la red de la Universidad Nacional Autónoma de México.
"Conclusiones"	La autora presenta algunas conclusiones a su trabajo de tesis. Cabe mencionar que en este trabajo no se presentan aspectos de seguridad en DNS,

	únicamente aspectos básicos de la administración de los servidores de nombres en la red de datos de la universidad.
--	---

Título	Análisis de riesgos en centros de cómputo (Taxonomía propuesta de ataques a computadoras y a redes de computadoras)
Autor	López Guerrero, Victor.
Carrera / escuela	Licenciatura en Informática / Facultad de Contaduría y Administración – UNAM
Lugar / Fecha	México, 2001
Colocación en biblioteca	001-00623-L1-2001
Capítulo 1 "Marco problemático"	El primer capítulo es una introducción a todo el trabajo de tesis desarrollado por el autor. Describe la importancia de realizar un análisis de los riesgos que afectan la información que se maneja en un centro de cómputo y la problemática de no contar con organismos que regulen la materia de seguridad informática en nuestro país. Se resume la arquitectura de seguridad del modelo OSI y los cinco servicios de seguridad definidos en ella. En esta etapa del trabajo, el autor aplica un cuestionario a diversas personas expertas en seguridad informática con el fin de obtener diferentes puntos de vista acerca de la necesidad de realizar un análisis de riesgos en centros de cómputo.
Capítulo 2 "Marco teórico"	Es el resumen de la bibliografía consultada por el autor como apoyo para la realización de su investigación. Presenta libros, tesis, periódicos, direcciones de Internet, y asistencias a seminarios, congresos y mesas redondas acerca del tema.
Capítulo 3 "Marco conceptual"	Comienza por definir formalmente el término "seguridad en cómputo", tomando como punto de partida las preguntas "¿Qué recursos se intentan proteger?" y "Contra que deben ser defendidos los sistemas de cómputo?". La definición de seguridad que finalmente adopta para su investigación es "la seguridad en cómputo es prevenir que los atacantes logren sus objetivos a través de accesos no autorizados o usos no autorizados de computadoras y redes". Posteriormente el autor desarrolla una taxonomía propia de ataques a computadoras y redes de

	<p>computadoras, compuesta por 5 bloques que representan la simplificación de una ruta que un atacante debe tomar para poder realizar sus objetivos. Los 5 bloques que explica detalladamente son:</p> <ul style="list-style-type: none"> ◆ Atacantes y sus objetivos ◆ Herramientas ◆ Accesos ◆ Resultados ◆ Objetivos
<p>Capítulo 4</p> <p>"Marco metodológico"</p>	<p>En este capítulo el autor realiza la investigación que finalmente comprueba su hipótesis. Desarrolla un cuestionario que aplica a expertos en seguridad de cómputo y presenta el análisis de los resultados obtenidos.</p>
<p>Capítulo 5</p> <p>"Marco instrumental"</p>	<p>En el capítulo final, se presenta algunos planes de trabajo del autor para poder difundir los resultados y el desarrollo de su trabajo de tesis.</p>

Título	Sistema de Automatización del DNS (Domain Name System)
Autor	Aguilar Álvarez, Armando Antonio
Carrera / escuela	Tesis Licenciatura (Ingeniero en Computación)-UNAM, Facultad de Ingeniería
Lugar / Fecha	México, 1996
Colocación en biblioteca	001-01132-A12-1996-1
<p>Capítulo 1</p> <p>"Antecedentes"</p>	<p>Se presentan los fundamentos y antecedentes del DNS , es decir, la historia, los conceptos básicos de los servidores de nombres y sintaxis de los tipos de registros que se manejan. El objetivo del autor es desarrollar un sistema que permita la administración vía web de los servidores de nombres.</p>
<p>Capítulo 2</p> <p>"Metodología"</p>	<p>El autor explica la metodología de desarrollo de sistemas que utilizará para llevar a cabo su proyecto de tesis. En este capítulo se desglosa la técnica utilizada para realizar el sistema basado propiamente en el concepto de ingeniería de software.</p>
<p>Capítulo 3</p> <p>"Análisis y Diseño del SADNS"</p>	<p>Se realiza el análisis y diseño del SADNS (Sistema de Automatización del DNS). Se presentan los pasos a seguir de acuerdo a la metodología establecida previamente.</p>

Capítulo 4 "Desarrollo del sistema"	Se describe el desarrollo del sistema. Se revisa la utilización de los recursos para llevar a cabo el sistema así como las herramientas y lenguajes de programación utilizados para desarrollar el sistema. En este capítulo se presenta finalmente el sistema obtenido, que es un sistema de administración vía web de los servidores de nombres de DGSCA en la UNAM. Este sistema solo fue parte del proyecto de tesis ya que no se puso en operación real.
Capítulo 5 "Conclusiones"	El autor presenta las conclusiones a su trabajo de tesis.

2.3 INTERNET

TÍTULO	URL
Internet Software Consortium	http://www.isc.org/products/BIND/
Internet International Ad Hoc Committee	http://www.iahc.org/
DNS Resources Directory	http://www.dns.net/dnsrd/
Centro de Información México NIC-México	http://www.nic.mx
Centro de Información de RedUNAM	http://www.nic.unam.mx
Acme Byte & Wire	http://www.acmebw.com/
Domain Name System Security	http://www.toad.com/~dnssec/
The Domain Name System Security Working Group	http://www.ietf.cnri.reston.va.us/proceedings/94dec/charters/dnssec-charter.html
PGP Security Research	http://www.pgp.com/research/nailabs/network-security/domain-name.asp
Domain Name System Security	http://compsec101.antibozo.net/papers/dnssec/dnssec.html
DNS Security	http://www.sans.org/infosecFAQ/firewall/DNS_sec.htm
DNS and DNS Security	http://www.laportestyle.org/talks/dns/index_files/v3_document.htm
Security Extensions in DNS	http://www.bovine.net/~jlawson/hmc/dns/security.html
DNS Security	http://www.cs.utk.edu/~nicholso/dns_security.html
DJBDNS	http://www.djbdns
DNSSEC - Securing the Domain Name System	http://www.dnssec.net/

Internet Software Consortium - BIND - Netscape 4

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop <http://www.isc.org/products/BIND/> Search Print

Home My Netscape! Net2Phone Download Customize...

INTERNET SOFTWARE CONSORTIUM

ISC BIND

BIND (Berkeley Internet Name Domain) is an implementation of the Domain Name System (DNS) protocols and provides an openly redistributable reference implementation of the major components of the Domain Name System, including:

- a Domain Name System server (named)
- a Domain Name System resolver library
- tools for verifying the proper operation of the DNS server

The BIND DNS Server is used on the vast majority of name serving machines on the Internet, providing a robust and stable architecture on top of which an organization's naming architecture can be built. The resolver library included in the BIND distribution provides the standard APIs for translation between domain names and Internet addresses and is intended to be linked with applications requiring name service.

Document: Done

Business Tech Fun Interact

IAHC Home - Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop <http://www.iahc.org/> Search Print

Home My Netscape! Net2Phone Download Customize...

The IAHC was dissolved on May 1, 1997
Please refer to: <http://www.gtld-mou.org>

IAHC

INTERNET INTERNATIONAL AD HOC COMMITTEE

ISOC IANA IAB FNC ITU INTA WIPO

What is the IAHC?

The IAHC is a coalition of participants from the broad Internet community, working to satisfy the requirement for enhancements to the Internet's global Domain Name System (DNS). Organizations naming members to the committee include:

- Internet Society (ISOC)

Quick Site Reference

- [IAHC Charter](#)
- [Press Releases](#)
- [Documents released by the IAHC](#)
- [Mailing Lists](#)
- [Public Information Resources](#)

Document: Done

Business Tech Fun Interact

DNS Resources Directory [DNSRD] - Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://www.dns.net/dnsrd/ Search Print

Home My Netscape! Net2Phone Download Customize...

DNSRD Books Documents Servers Tools Training About

DNS Resources Directory

About the DNS

The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses, and to control Internet email delivery. Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.

A selection of [overview documents](#) explains DNS from a high-level perspective, while the [RFC documents](#) are the official standards.

Contents

General

- [What is DNS?](#)
- [DNS books](#)
- [Where to find DNS training](#)
- [About DNSRD](#)

Reference material

- [Online documents](#)
- [FAQ](#)
- [Ask Mr. DNS at Acme Byte & Wire](#)
- [Newsgroups](#)
- [Mailing lists](#)

Document: Done

Business Tech Fun Interact

Bienvenido a los Servicios de NIC-México - Netscape 6

Archivo Editar Ver Buscar Marcadores Areas Ayuda

http://www.nic.mx/nic/ingles/nic_inicio

Inicio Netscape.es Buscar Shop Marcadores Net2Phone

nic.MX Comité Consultivo de **NIC-México**

nic.MX revisa la Política de Resolución de Disputas (UDRP)

Búsquedas	Noticias NIC
<p>Disponibilidad de Dominios Si deseas consultar la disponibilidad de un dominio puedes hacerlo aquí.</p> <p>Nombres de Dominio Contactos Para registrar un dominio debes de registrarte primero como contacto, aquí puedes registrarte y obtener tu NIC-ID (Identificador de Contacto).</p> <p>Organizaciones Para registrar un dominio debes de asociar tu dominio a una organización, aquí puedes registrar tu organización y obtener tu ORG-ID.</p> <p>Dominios Registra de nuevos dominios, políticas y otros servicios relacionados con los nombres de dominio.</p> <p>Pago de Dominios Cada 28 días de febrero. Aquí puedes realizar el pago de tu dominio, consultar el status de tu intención de pago y revisar tu estado de cuenta. Contacta al Departamento de Pagos</p>	<p>WHOWIS Búsqueda en base de datos WHOIS</p> <p>Otros Servicios</p> <p>Estadísticas Información sobre dominios, hosts y otros datos de Internet en México.</p> <p>Cursos de DNS Cursos de capacitación sobre DNS.</p> <p>IP Solicitud de direcciones IP y dominio inverso.</p> <p>ISP's (Proveedores de Servicios de Internet) Base de datos de ISP's mexicanas.</p> <p>FTP Anónimo Servicio de FTP Anónimo.</p> <p>NIC's Latinos Información de otros NIC's en Latinoamérica.</p>

Horario de Atención Telefónica
Lunes a Viernes de 9:30 a.m. a 1:00 p.m. y de 3:00 p.m. a 6:00 p.m.
Tel: +52(0)181367-6346
Correo: nic@nic.mx

Documento: Terminado

CENTRO DE INFORMACIÓN DE REDUNAM - NIDunam - Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://www.nic.unam.mx/ Search Print

Home My Netscape! Net2Phone Download Customize...



INFO. NICUNAM | BÚSQUEDA | NOTICIAS | FAQ | MAPA SITIO | HERRAMIENTAS | PERSONAL | LOGIN

El Centro de Información de RedUNAM (NICunam) se encarga de proporcionar servicios de: Asignación de Direcciones IP, Asignación de Dominios y Servicio de Nombres a las dependencias e instituciones conectadas a RedUNAM.

- ¿QUE ES REDUNAM? •
- POLITICAS DE SERVICIOS DE REDUNAM •
- FORMAS DE REGISTRO •
- ESTADISTICAS •
- INTERNET •

Tel. 5622 8110

Document: Done


Business Tech Fun Interact

Acme Byte & Wire - Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://www.acmebw.com/ Search Print

Home My Netscape! Net2Phone Download Customize...



BYTE & WIRE

Search


Ask Mr. DNS Q&A Archive

Resources

Ask Mr. DNS

About us

Acme Byte & Wire acquired by the Network Solutions Registry



On June 7, 2000, Acme Byte & Wire was acquired by Network Solutions, Inc. As a result, we are no longer accepting consulting engagements nor teaching our DNS and BIND training classes.

Mr. DNS is alive and well and we expect him to live through the transition, though he might not be able to answer as many questions. You can still access the [Ask Mr. DNS archive](#) on this web site. You can also still access our [papers and presentations](#).

For more information about our acquisition, please see the [Network Solutions press release](#). If you still want to get a hold of us, drop us a line at info@acmebw.com.

Document: Done

Business Tech Fun Interact

Domain Name System Security - Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://www.toad.com/~dnssec/ Search Print

Home My Netscape! Net2Phone Download Customize

Domain Name System Security

DNS Security (or DNSSEC) applies cryptography to the Domain Name System to authenticate the information served. This site is about the process of integrating DNS Security with the existing DNS infrastructure.

- [Protocol Development](#)
- [Software Integration](#)
- [Generating Keys](#)
- [Signing Your Zone](#)
- [Exchanging Keys with Sub- and Super-Zones](#)
- [How keying info gets used](#)
- [Government controls \(or the lack thereof\)](#)
- [Downloading an early prototype of the software](#)
- [RSA info about the "DNSsafe" software appearing soon in production releases](#)
- [ISC info about the "DNSsafe" software appearing soon in production releases](#)
- [Downloading production BIND DNS software \(which does not implement DNS Security yet\)](#)
- [Dec 23, 1997 Strong Crypto Code Published Online for Authentication](#)
- [Background information for Dec 23, 1997 press release](#)

UPDATES - March 1999

Document Done

Business Tech Fun Interact

DNS Security [dnssec] Charter - Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://www.ietf.cnri.reston.va.us/proceedings/94dec/ Search Print

Home My Netscape! Net2Phone Download Customize

DNS Security (dnssec) Charter

NOTE: This charter is accurate as of the 31st IETF Meeting in San Jose. It may now be out-of-date. (Consider this a "snapshot" of the working group from that meeting.) Up-to-date charters for all active working groups can be found elsewhere in this Web server.

Chair(s)

- James Galvin <galvin@ns.com>

Security Area Director(s):

- Jeffrey Schaller <js@mit.edu>

Mailing List Information

- General Discussion: dns-security@ns.com
- To Subscribe: dns-security-request@ns.com
- Archive: [ftp.isc.com/pub/dns-security](http://ftp.isc.org/pub/dns-security)

Document Done

Business Tech Fun Interact

PGP Security - Research - NAI Labs - Netscape

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://www.pgp.com/research/nailabs/network-secu Search Print

Home My Netscape Net2Phone Download Customize

Buy Download Home

PGP SECURITY

A Network Associates Business

PRODUCTS INDUSTRIES SERVICES SUPPORT COVERT LABS NAI LABS PARTNERS

NAI Labs

- Network Security
- Cryptographic Technologies
- Security Infrastructure
- Secure Execution Environments
- Adaptive Network Defense
- Distributed Systems Security
- IA Architecture, Modeling, and Management
- Security Privilege Management Solutions
- Internal Research & Development
- Finished Projects
- Open Source Software
- Documents
- News
- Security Research Alliance

Network Security
Domain Name System (DNS) Security

TISLabs at Network Associates is developing with ISC an implementation of DNS Security in BIND version 9 (Berkeley Internet Name Domain). Work is also being done to push the standards through the IETF and update them when necessary. This work is funded by the Department of Defense's Information Systems Agency (DISA), and was announced in August, 1998.

A short paper describing Secure DNS provides a high-level description of the extensions. Several prototype implementations have been released. All future releases will be made by the [Internet Software Consortium](#).

We have made a number of presentations that explain DNSSEC and its use, "DNSSEC: How to with BIND-9", "Introduction to DNSSEC", "DNS Security Extensions, Presentation to the 19th NANOG". NAI Labs in Holland maintains a good collection of links to [DNSSEC resources](#).

Simple Network Management Protocol

- Advisory Team Charter
- Interim Report
- Slides
- Elements of Procedure

Active Networks

- Secure Active Network Protocols
- Qui CAIRN Network Participation
- New Cryptographic Techniques for Active Networks

Domain Name System (DNS) Security

Routing Security

- Internet Infrastructure Protection project (IIP)

Document Done

Business Tech Fun Interact

Domain Name System (DNS) Security - Netscape

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://compsec101.antibozo.net/papers/dnssec/dns-9 Search Print

Home My Netscape Net2Phone Download Customize

By Diane Dawdowicz
© 1999 Diane Dawdowicz

1. Abstract

The Domain Name System (DNS) is vital to the Internet, providing a mechanism for resolving host names into Internet Protocol (IP) addresses. Insecure underlying protocols and lack of authentication and integrity checking of the information within the DNS threaten the proper functionality of the DNS. The Internet Engineering Task Force (IETF) is working on DNS security extensions to increase security within the DNS, known as DNSSEC. These security issues and solutions are presented in this paper.

2. Introduction

The DNS plays a critical role in supporting the Internet infrastructure by providing a distributed and fairly robust mechanism that resolves Internet host names into IP addresses and IP addresses back into host names. The DNS also supports other Internet directory-like lookup capabilities to retrieve information pertaining to DNS Name Servers, Canonical Names, Mail Exchangers, etc. Unfortunately many security weaknesses surround IP and the protocols carried by IP. The DNS is not immune to these security weaknesses. The accuracy of the information contained within the DNS is vital to many aspects of IP based communications.

The threats that surround the DNS are due in part to the lack of authenticity and integrity checking of the data held within the DNS and in part to other protocols that use host names as an access control mechanism. In response to this, the IETF formed

Document Done

Business Tech Fun Interact

DNS Security - Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://www.sans.org/infosecFAQ/firewall/DNS_sec.h Search Print

Home My Netscape! Net2Phone Download Customize...

SANS Information Security Reading Room

SANS Parliament Hill
Ottawa, Canada, August 8-18

DNS Security
Jeff Holland
July 23, 2000

This paper will address security issues involved with the DNS client/server architecture within a UNIX environment. Suggestions on securing DNS by preventing unauthorized zone transfers will also be discussed.

Background

The name service DNS (Domain Name Service) is a distributed database that allows for the translation of domain names into IP addresses. Inverse queries that map IP addresses to domain names are also possible, but are not entirely accurate [1]. To determine IP address to host-name mappings, consult the IN-ADDR.ARPA domain, which was created for this very purpose [1].

DNS has a hierarchical inverted tree structure, with a root node and seven immediate subdomain nodes below the root [2]. These subdomain nodes, which are domains themselves, are the top-level domains and are controlled by InterNIC (Internet Network Information Center) [3]. For example, given the small sample name space below, the "army" subdomain is a child domain of the parent domain "mil" which in turn is a

Document Done

Business Tech Fun Interact

DNS and DNS Security - Netscape 6

File Edit View Search Go Bookmarks Tasks Help

Back Forward Reload Stop http://www.laportestyle.org/talks/dns/index_files/v3 Search Print

Home My Netscape! Net2Phone Download Customize...

DNS Security

Topics

Topics (cont.)

DNS History

DNS History (cont.)

DNS Hierarchy

DNS Hierarchy (cont.)

Root Level Delegations

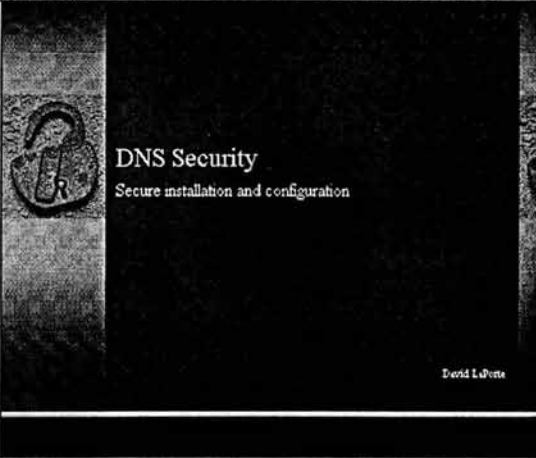
Zones vs. Subdomains

Delegation

Authoritative vs. Non-authoritative

Name Server Types

Common Record Types



David LuPota

Document Done

Business Tech Fun Interact

Security Extensions in DNS - Netscape 6

Archivo Editar Ver Buscar Marcadores Imprimir Ayuda

http://www.bovine.net/~jason/pw/1dnsecurity.html

Inicio | Netscape.es | Buscar | Shop | Marcadores | Net2Phone

Security Extensions in DNS

There have been a number of security extensions proposed for possible implementation by DNS servers and many of these ideas are documented in RFC 2065. The primary concerns addressed by the proposed security extensions are to allow the DNS infrastructure to have a method of verifying the integrity of the record being served, in addition to verifying the actual identity of servers claiming to be authoritative DNS servers. A second feature of the security extensions is to allow DNS to be used as a central distribution method for public keys.

Data Origin Authentication and Integrity

Authentication is provided by associating with resource records in the DNS cryptographically generated digital signatures. Commonly, there will be a single private key that signs for an entire zone. If a security aware resolver reliably learns the public key of the zone, it can verify, for signed data read from that zone, that it was properly authorized and is reasonably current. The expected implementation is for the zone private key to be kept off-line and used to re-sign all of the records in the zone periodically.

A resolver can learn the public key of a zone either by reading it from DNS or by having it statically configured. To reliably learn the public key by reading it from DNS, the key itself must be signed. Thus, to provide a reasonable degree of security, the resolver must be configured with at least the public key of one zone that it can use to authenticate signatures. From there, it can securely read the public keys of other zones, if the intervening zones in the DNS tree are secure and their signed keys accessible.

If signatures are always separately retrieved and verified when retrieving the information they authenticate, there will be more trips to the server and performance will suffer. To avoid this, security aware servers mitigate that degradation by always attempting to send the signature(s) needed.

Signature (SIG) record

The SIG or "signature" resource record (RR) is the fundamental way that data is authenticated in the secure Domain Name System (DNS). As such it is the heart of the security provided. The SIG RR, unobtrusively authenticates other RRs of a particular type, class, and name and binds them to a time interval and the signer's domain name. This is done using cryptographic techniques and the signer's private key. The signer is frequently the owner of the zone from which the RR originated.

The syntax of a SIG resource record (signature) includes the type of the RR(s) being signed, the name of the signer, the time at which the signature was created, the time it expires (when it is no longer to be believed), its original time to live (which may be longer than its current time to live but cannot be shorter), the cryptographic algorithm in use, and the actual signature. The shorter of the "original TTL" and the "current TTL" (determined by comparing the current absolute time to the "expiration time") is the value that is actually used by the downstream DNS client/server when deciding how long to cache the signature.

Document: Terminado

DNS Security - Netscape 6

Archivo Editar Ver Buscar Marcadores Imprimir Ayuda

http://www.cs.utk.edu/~nicholas/dns_security.html

Inicio | Netscape.es | Buscar | Shop | Marcadores | Net2Phone

DNS Security

Christopher Nicholson

CS594 - Computer and Network Security

December 14, 2000

Abstract

The DNS (the Domain Name System) is the sine qua non of the Internet. Yet it is inherently insecure. In the beginning this was hardly a concern, but, over time, changes in the jobs that globally-connected computers are expected to perform have made security more and more important. Security features have been continually added to the standard implementations of the system, but the ad hoc and distributed nature of the system stands in the way of making such changes generally effective. What follows is an examination of the development of the DNS and the attention paid to the security within the system by various bodies during this development, and speculation as to why problems have arisen and how they might be resolved.

1. Introduction

Earlier this year encryption software company RSA had one of its webpages, <http://www.rsa.com>, hacked and defaced. What was significant about this attack was that the server on which the page was kept was not broken into, but, rather, a higher-level DNS nameserver had its pointer to the www.rsa.com page redirected to another page. The page to which it pointed contained, by accounts, an apparently rambling and nonsensical message, but many believe that the real message of the hack was to demonstrate that the DNS is vulnerable to this sort of attack. This point was further reinforced by the fact that the site attacked was owned by one of the leading encryption companies [RGHT]. Had proposed DNS security measures been taken, such as use of the encryption software of the attacked company [RFC 2535], then this attack would likely have not been possible. The Domain Name System is a distributed directory that serves to make possible translation to and from numerical Internet Protocol (IP) addresses. Presently virtually the entire Internet relies on the DNS to effect the delivery of e-mail and to enable one's web

Document: Terminado

jdjbdns - Welcome - Netscape 6

Archivo Editar Ver Buzón Marcadores Areas Ayuda

http://www.djbdns.org

Inicio Netscape.es Buzón Shop Marcadores NetPhone

jdjbdns home page

[Marrors Argentina Australia 1 Australia 2 Ireland Korea Turkey]

Sie suchen eine deutschsprachige Seite zu djbdns? Or a Japanese one? Or a Turkish one?

Introduction

jdjbdns is a replacement for BIND. It is secure, reliable, small, fast, etc etc etc. Just like all of Dan Bernstein's tools, Dan has his own page for [jdjbdns](#). We've got this one so we can distribute our enhancements to djbdns.

Switching to djbdns because of BIND's bugs, or simple misfeatures like the format of the zone files? Dan has a web page for people [switching from bind](#).

Dan has a [mailing list](#) for djbdns. Fred Lindberg has a [web-accessible archive](#). There's also a [searchable archive](#). Please read the [FAQ's](#) page about djbdns before asking for help.

Felix von Leitner has a [FAQ](#). Luis Toro Tejero has translated the djbdns documentation into [Spanish](#).

The Open Root Server Confederation has a page on [configuring djbdns](#) to work with their list of top-level domains.

Testimonials: lycos. Any others?

Dns-cache is a recursive resolver, intended to be listed in `/etc/resolv.conf`'s "nameserver" entry. It makes DNS queries via UDP and TCP as needed. It imposes restrictions on what it will return, that's why it was written. It will only provide data obtained from authoritative servers. These servers are found via a chain of delegations from authoritative servers starting from the configured `-d` in roots. That's part of its security model. If it were to do anything less, it would be subject to the same cache-poisoning style attacks that work on the current insecure DNS servers.

Tinydns does authoritative nameserving via UDP only, it does not do recursive nameserving, nor does it answer TCP queries (axfrdns does that). The only hosts that should ask tinydns for a host are recursive nameservers, such as those found in `/etc/resolv.conf`, like djbdns or bind. Tinydns should never be listed in `/etc/resolv.conf`. Tinydns interoperates properly with every authoritative and recursive nameserver I know of, and supporting all the standards needed to do so.

Zone transfers are only supported over TCP. The zone transfer server is named axfrdns, and the client is named axfr-get. Both of these use Dan Bernstein's `ucspi-tcp` helpers. Why separate programs? To limit security incursions, and because many sites do not need zone transfers. As BIND has shown, excessive functionality is a

Documentos Terminado

DnsSEC - Securing the Domain Name System - Netscape

File Edit View Go Bookmarks Tools Window Help

http://www.dnssec.net/

Mail Home Radio Netscape Search Bookmarks 404 Not Found

DnsSEC - Securing the Domain Name System

Dnssec.net

Securing the Domain Name System

Securing the Domain Name System with DNSSEC	Intrusion Detection Systems, Honey Pots & Incident Response	The Border Gateway Protocol Advanced Routing Resources	Wardriving & Wireless (802.11) Networking Security	Internet Security Books Educate Yourself
DNSSEC.NET	HONEYPOTS.NET	BGP4.AS	WARDRIVE.NET	SECURITYBOOKS.ORG

- DNSSEC - what is it?
- Projects - Courses - Workshops
- Software - Tools - Practical Docs
- News - Mailing Lists
- Books - Articles - Presentations - Howtos
- RFC's and IETF Drafts
- Site suggestions
- About this Website

DNSSEC, what is it?

A short background on DNS, the Domain Name System

The **Domain Name System**, or DNS, is one of the core techniques used on the Internet today. DNS is a vital Internet protocol that maintains a database of **easy-to-remember domain names (hostnames)** and their corresponding numerical IP addresses.

For example: When visiting a website, let's say `www.cnn.com`, your browser asks (makes a query to) the local DNS server to look up the IP address of `www.cnn.com`, which happens to be `64.236.24.12`. At this moment, your web browser knows which computer to contact to retrieve the information from the CNN website. Further information retrieval takes place using the HTTP protocol.

Of course, the complete story is a little more sophisticated than this. But this is basically what DNS does.

In this article - [How Domain Name Servers Work](#) - you can have a closer look at the DNS system, so you can understand how it works and appreciate its amazing capabilities. Another document which describes DNS extensively can be found [here](#).

DNSSEC - Security Extensions for DNS

DNSSEC (short for "DNS Security Extensions") is a technique for securing the Domain Name System. It is a set of extensions to DNS, which provide end-to-end authenticity and integrity and was designed to protect the Internet from certain attacks. There are several distinct classes of threats to the DNS, most of which are DNS-related instances of more general problems, but a few of which are specific to peculiarities of the DNS protocol.

The Internet Engineering Task Force (IETF) - which is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture - has written a nice document which describes these threats, and the goal of DNSSEC.

For more information on what exactly is at stake, be sure to also read the following documents: [DNS Security Update \(ICANN\)](#) and [DNS Security: Present and Future \(IUI Labs\)](#). Many other insightful documents, presentations and FAQ's related to DNSSEC can be found on this page in section [Books](#), [Articles](#), [Presentations](#), [Howtos](#).

Frequently asked questions (and answers!) about DNSSEC can be found in [Homemum's DNSSEC FAQ](#).

Document: Dns (2.134 sec)

2.4 REVISTAS ELECTRÓNICAS

COMPUTERWORLD (<http://www.computerworld.com>)

Artículo	"Internet security hole called most serious yet"
URL	http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57056,00.html
Autor	Dan Verton
Fecha	29 de enero de 2001
Resumen	El mismo día en que se publicó este artículo, el organismo CERT anunció una serie de vulnerabilidades en BIND, que al ser explotadas por hackers pueden permitir el acceso y control del tráfico de web, correo electrónico y ftp de los dominios que el servidor de nombres atacado administre. Este artículo trata de forma muy general el anuncio del CERT al respecto y alienta a los administradores de DNS a actualizar lo antes posible la versión de BIND.

Artículo	"Survey: 25% of Fortune 1,000 has bad DNS"
URL	http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57075,00.html
Autor	Joris Evers
Fecha	29 de enero de 2001
Resumen	Trata acerca de un ataque de seguridad exitoso de tipo <i>DoS</i> en contra de la empresa Microsoft. Según el reportaje, este ataque impidió que los sitios de web de tal empresa pudieran ser accedidos. El ataque fue posible debido a una mala configuración y ubicación de los servidores DNS de Microsoft. Según cifras presentadas en este artículo, el 25% de las empresas que forman la base de datos "Fortune 1,000" y el 38% de 5,000 sitios tomados al azar en el dominio comercial .com, presentan malas configuraciones en su DNS, lo que los hace vulnerables a ataques de este tipo.

Artículo	"Stuck in a BIND"
URL	http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57547,00.html
Autor	Deborah Radcliff
Fecha	12 de febrero de 2001
Resumen	<p>En este artículo la autora critica varios aspectos del software BIND, como son:</p> <ul style="list-style-type: none"> • El control total que tiene ISC sobre BIND. • Las múltiples vulnerabilidades que se han encontrado en su código desde la versión 4 hasta la actualmente utilizada. • Como repercuten estas fallas en la seguridad de toda la Internet. <p>Cita a Ian Poynter, presidente de Jerboa Inc., diciendo de "BIND es el punto de falla más grande de toda la infraestructura de la Internet" y menciona algunas recomendaciones muy generales de seguridad para un servidor de nombres.</p>

Artículo	"Study: Many still lax in securing DNS"
URL	http://www.computerworld.com/storyba/0,4125,NAV47_STO58302,00.html
Autor	Joris Evers
Fecha	02 de marzo de 2001
Resumen	<p>El artículo menciona algunos de los resultados obtenidos en un estudio realizado por dos consultorías en DNS, después del anuncio por parte del organismo CERT a finales de enero del 2001 de que existían varios <i>bugs</i> de seguridad en varias de las versiones del software BIND. En ese estudio se probaron 1000 sitios de Internet escogidos de forma aleatoria, y de acuerdo con los resultados, un día después del anuncio de seguridad, el 33.3% de esos sitios utilizaba una versión de BIND vulnerable. Otro estudio similar se aplicó a los dominios nacionales de Alemania (.de), Suiza (.ch) y al dominio comercial del Reino Unido (com.uk), obteniendo que el 15.29% de los servidores de DNS en Alemania, el 11.54% en Suiza y el 9.87% de los dominios comerciales de UK utilizaban versiones vulnerables.</p>

Artículo	"Security to trump other matters at ICANN meeting"
URL	http://www.computerworld.com/storyba/0,4125,NAV47_STO65474,00.html
Autor	Sam Costello
Fecha	8 de noviembre de 2001
Resumen	Después de los sucesos del pasado 11 de septiembre del 2001, numerosas organizaciones en Internet comenzaron a enfocarse fuertemente a aspectos de seguridad informática ante posibles ataques a sus sistemas. Stuart M. Lynn afirma que en la reunión mensual del ICANN, se tratarían asuntos de seguridad en el DNS, y que la decisión de esta temática no estaba influenciada por la alarma de posibles ataques o por algún otro suceso. También dijo que el ICANN no se enfocaría a la seguridad de Internet, sino solo a la seguridad del DNS, que es un aspecto en lo que si tienen injerencia.

Artículo	"Q&A: ICANN's Lynn talks about DNS debate, Internet security"
URL	http://www.computerworld.com/storyba/0,4125,NAV47_STO65622,00.html
Autor	Patrick thibodeau
Fecha	12 de noviembre de 2001
Resumen	En este artículo se presenta una entrevista hecha a Stuart Lynn, quien es el actual presidente de ICANN. Se le cuestiona acerca de la seguridad en el Sistema de Nombres de Dominio y del alcance de las responsabilidades que tienen en cuanto a la seguridad del DNS y de todo Internet.

Artículo	"Web Addressing System Vulnerable"
URL	http://www.computerworld.com/itresources/rcstory/0,4167,STO65868_KEY73,00.html
Autor	Patrick Thibodeau
Fecha	19 de noviembre de 2001
Resumen	Se resume una conferencia que se llevó a cabo por ICANN para discutir la seguridad en el Sistema de Nombres de Dominio. De acuerdo con el artículo, en la conferencia el ICANN reconoció las fallas existentes en BIND, el software que el 80% de los servidores de nombres en Internet utilizan y gracias al cual es posible la comunicación por nombres. También menciona la importancia que tienen los 13 servidores de nombres raíz, los cuales están

	físicamente distribuidos alrededor del mundo.
--	---

Artículo	"Q&A with ICANN's security chairman, Stephen Crocker"
URL	http://www.computerworld.com/itresources/rcstory/0,4167,STO68514_KEY73,00.html
Autor	Patrick Thibodeau
Fecha	22 de febrero de 2002
Resumen	Como consecuencia de los numerosos incidentes de seguridad que se presentaron en el DNS durante el año 2001, el ICANN formó un comité de seguridad encabezado por Stephen Crocker, quien contribuyó en el desarrollo de los protocolos para la Arpanet, la red original que se convirtió en las bases de lo que actualmente es Internet. Este artículo presenta una entrevista realizada a Stephen Crocker respecto a la seguridad del sistema de nombres de dominio y de algunas de las funciones que debe realizar este comité.

Artículo	"CERT warns of BIND problem; Sun patches Solaris flaws"
URL	http://www.computerworld.com/securitytopics/security/story/0,10801,71715,00.html
Autor	Joris Evers & Sam Costello
Fecha	05 de junio de 2002
Resumen	Este artículo anuncia una vulnerabilidad de algunas versiones de BIND que están instaladas sobre el sistema operativo Solaris. Esta vulnerabilidad afecta a las versiones anteriores a la 9.2.1 y permite a los atacantes enviar ciertos tipos de paquetes al servidor de nombres y tomar el control del DNS. Al lograr este ataque, se puede dar de baja el servicio dejando fuera de Internet a los dominios que atiende el servidor de nombres víctima.

Artículo	"Net backbone withstands major attack"
URL	http://www.computerworld.com/securitytopics/security/story/0,10801,75324,00.html
Autor	Matt Berger & Nancy Weil
Fecha	23 de octubre de 2002
Resumen	Se narra un ataque distribuido de negación de servicio llevado a cabo unos días antes de la publicación de este artículo. El ataque

	<p>tuvo como objetivo los servidores de nombres de la zona raíz, conocidos como "root servers" y tuvo éxito en 8 de ellos, los cuales dejaron de dar servicio a Internet alrededor de 6 horas. Los root servers son los servidores de nombres más importantes de Internet, ya que son los principales nodos de los que se desprende todo el árbol que constituye el espacio de nombres de dominio. De acuerdo con el artículo, las organizaciones administradoras de los root server, como son "The NASA Ames Research Center", "The U.S. Army Research Lab", "The Internet Corporation for Assigned Names and Numbers" y "The Internet Software Consortium", no admitieron el éxito del ataque, sin embargo, miles de usuarios dejaron de recibir correo y de tener acceso a muchas páginas web.</p>
--	---

Artículo	"Q&A: Internet pioneer Stephen Crocker on this week's DDOS attack"
URL	http://www.computerworld.com/securitytopics/security/story/0,10801,75350,00.html
Autor	Patrick Thibodeau
Fecha	24 de octubre de 2002
Resumen	<p>En este artículo se presenta una entrevista realizada a Stephen Crocker, quien fue uno de los desarrolladores de los protocolos de Arpanet, la red que se convirtió en la base de la actual Internet. El tema de esta entrevista es el DDoS (Ataque de Negación de Servicio Distribuido), llevado a cabo en contra de los root servers. De acuerdo con la entrevista, Stephen Crocker considera que el ataque no puede considerarse como un ataque sofisticado, ya que se basó en el envío de paquetes ICMP de tamaño anormal y en una cantidad que inundó los servidores, ocasionando la saturación de sus recursos y dejando fuera el servicio de nombres. Asegura que los servidores de nombres de la zona raíz son administrados por personal altamente calificado que se preocupa y trabaja por la seguridad de los servidores. Las recomendaciones que hace para mejorar la seguridad de todo el servicio de nombres en Internet son: trabajar en el fortalecimiento de los protocolos en los que se basa en DNS, imponer disciplina entre los ISP's para exigir autenticación de los hosts que se conectan a Internet, continuar con el desarrollo de DNSSEC y finalmente, la actualización de las versiones de BIND en los servidores de nombres, ya que la mayoría trabajan con una versión obsoleta. La seguridad en el sistema de nombres de dominio es tan importante, que el ICANN ha formado un comité que se dedicará a este tema.</p>

2.5 DIPLOMADO

Diplomado "Seguridad Informática"

Impartido por el CEM-Polanco, UNAM.

Duración: 200 horas (12 módulos)

Fecha: Abril - Septiembre de 2002

<p>Módulo 1</p> <p><i>"Problemática y definición de la seguridad informática"</i></p>	<p>El primer módulo del diplomado es una introducción a la problemática existente entorno a la seguridad informática. Se da una reseña de los puntos más importantes en la historia de la computación así como un resumen de los incidentes de seguridad informática que más han trascendido en los últimos años. Se ven los conceptos de seguridad informática elementales, necesarios para entender los diferentes módulos que conforman el diplomado, como son definiciones de seguridad informática y los servicios de seguridad que debe ofrecer cualquier sistema de cómputo.</p>
<p>Módulo 2</p> <p><i>"Criptología"</i></p>	<p>La criptología es la ciencia de ocultar la información y se divide en dos áreas, la criptografía cuya función es transformar la información a una forma no legible basándose en una llave o secreto, y el criptoanálisis que se encarga de descubrir la información sin conocimiento de la llave o secreto que fue utilizado para cifrarla. La criptología es una parte fundamental cuando se habla de seguridad informática, ya que hoy en día es utilizada como herramienta para ofrecer los servicios de confidencialidad, autenticación, integridad y no repudio. En este módulo se trata el tema de la criptografía, distintas maneras de clasificarla, sus componentes, algoritmos y algunos ataques que pueden realizarse por medio del criptoanálisis.</p>

Módulo 3 "Aplicaciones criptográficas"	En el tercer módulo se explican diferentes protocolos que se basan en la criptografía y que se implementan para ofrecer servicios de seguridad. Algunos de las aplicaciones más importantes de la criptografía hoy en día, son las firmas y certificados digitales, que son utilizados por miles de organizaciones en el mundo como parte de sus esquemas de seguridad.
Módulo 4 "Políticas y normatividad"	La implementación de un esquema de seguridad en cualquier organización no debe contemplar únicamente la instalación de dispositivos dedicados a filtrar tráfico de red o software de monitoreo. La seguridad comienza por establecer la misión de seguridad que se tiene en la organización así como los objetivos y mecanismos que se desean alcanzar con la implementación de seguridad. Para ello es necesario el análisis y redacción de las políticas de seguridad que se establecerán en la organización. Este módulo da las bases para poder llevar a cabo la definición de las políticas, misión, objetivos y mecanismos de seguridad óptimos.
Módulo 5 "Control de acceso"	En el módulo 5 se tratan los conceptos del control de acceso como herramienta para la seguridad de los activos informáticos que se desean proteger. Primeramente se ve un poco de historia de la aplicación del control de acceso y su aplicación actual a ámbitos informáticos. Entre los diferentes mecanismos actuales de control de acceso que se tratan en este módulo están los sistemas basados en la biometría, tarjetas inteligentes y algunos modelos formales e informales.

<p>Módulo 6</p> <p>"Detección de intrusos"</p>	<p>En el módulo "detección de intrusos" se trata de manera general los 5 métodos existentes para la detección de intrusos en una red, los cuáles son: 1) Análisis de bitácoras, 2) Monitoreo y análisis de la actividad de los usuarios, 3) Reconocimiento de ataques conocidos, 4) Monitoreo de tráfico en la red, 5) Verificación de la integridad de los archivos críticos de un sistema y 6) Auditoria de la configuración del sistema y sus vulnerabilidades.</p> <p>Además se da una visión de las herramientas existentes que pueden ayudar en la detección de intrusos.</p>
<p>Módulo 7</p> <p>"Código malicioso"</p>	<p>Durante los primeros años de la historia de la computación, el círculo de especialistas en cómputo era muy pequeño y cerrado, además de que los recursos computacionales eran sumamente valiosos. Un programador tenía asignado determinado tiempo de CPU en las pocas computadoras que existían, y por lo regular, este tiempo asignado para la compilación de sus programas era muy limitado. Los programadores entonces no podían darse el lujo de programar código que no fuera destinado a su trabajo. El avance de la tecnología, así como el abaratamiento de recursos de cómputo, facilitó el surgimiento de programadores dedicados a la creación de código para fines maliciosos. En este capítulo se da la historia de la aparición de los programas conocidos como código malicioso, así como sus categorías, las cuales son:</p> <ul style="list-style-type: none"> ◆ Virus ◆ Ataques de penetración ◆ Ataques de negación de servicios ◆ Programas de espionaje ◆ Caballos de troya ◆ Bombas de tiempo

	De estas, se pone mayor énfasis en el grupo "virus", por ser el que mayores pérdidas económicas ha generado a miles de organizaciones.
<p>Módulo 8</p> <p>"Seguridad en sistemas operativos"</p>	Este módulo comienza con algunas definiciones de lo que se conoce como sistema operativo y las funciones que lleva a cabo. Posteriormente se estudian las características que debe cumplir un sistema operativo para cubrir los diferentes niveles de seguridad que define el <i>TCSEC</i> , conocido como libro naranja. También se dan algunos aspectos de seguridad en los sistemas operativos Linux/Unix y Windows.
<p>Módulo 9</p> <p>"Herramientas y protocolos"</p>	El objetivo de este módulo es conocer algunas de las principales herramientas de seguridad utilizadas y recomendadas hoy en día, y relacionar su funcionamiento con los conceptos de seguridad vistos a lo largo del diplomado. Las herramientas de seguridad vistas son, en primer lugar, sniffers de red, los cuales pueden ser utilizados por intrusos como una forma de obtener información confidencial en una red, pero también pueden ser utilizados por administradores para analizar comportamientos normales y anormales del tráfico de una red y poder detectar intrusiones. PGP es una herramienta que está basada en criptografía y es una de las mejores opciones existentes para cifrar información que se intercambia a través del correo electrónico y otras formas en Internet. También se estudia snort, como herramienta de detección de intrusos. Adicionalmente se explican los conceptos básicos de <i>VPN's</i> y los protocolos en que se basan. Finalmente se da una explicación de <i>SET</i> como protocolo para comercio electrónico.

<p>Módulo 10</p> <p><i>"Seguridad en redes"</i></p>	<p>En este módulo se comienza con los repases de los conceptos básicos que se deben de tener claros para un análisis de la seguridad de una red, como son el modelo de referencia OSI, la suite de protocolos TCP/IP, los diferentes tipos de ataques a los que es vulnerable cualquier red sin protección y los servicios de seguridad que debe ofrecer. Posteriormente se analizan algunos aspectos de la seguridad en los protocolos IP, es decir, en tcp y udp y se explica de manera general la problemática de seguridad que existe en Internet. Finalmente se analizan y prueban algunas herramientas de seguridad para redes, como son ssh, ssl, kerberos, nessus y adicionalmente se estudian los principales tipos de firewalls y su funcionamiento.</p>
<p>Módulo 11</p> <p><i>"Seguridad en bases de datos"</i></p>	<p>Actualmente los servidores de bases de datos, constituyen prácticamente una plataforma para los sistemas de cualquier empresa. Sin embargo, la seguridad en las bases de datos es un área poco desarrollada y conocida. En este módulo, se cubren algunos temas que sirven como base para el análisis e implementación de seguridad en las bases de datos. Se comienza con conceptos de bases de datos relacionales así como los amenazas de seguridad y requerimientos de protección de los datos. También se dan conceptos de integridad, control de acceso a los datos y los principales tipos de ataques que afectan a los sistemas de bases de datos. Finalmente se dan algunas prácticas de seguridad recomendadas en esta área y las características de seguridad de algunos sistemas de bases de datos comerciales.</p>

<p>Módulo 12</p> <p>"Buenas prácticas y tendencias futuras"</p>	<p>En el módulo final, se dan temas divididos en dos principales categorías, las cuales son: buenas prácticas de seguridad y tendencias futuras. Como buenas prácticas se dan recomendaciones de seguridad física para los centros de cómputo, administración de software, control de configuraciones de los equipos principales, recuperación de información en caso de desastres y el manejo de incidentes de seguridad. En la parte de tendencias futuras se analiza el funcionamiento de AES como protocolo criptográfico que ha reemplazado al tradicional DES y las curvas elípticas como alternativa para el cifrado de información. También se dan de manera general conceptos de <i>esteganografía</i> y su utilización en la seguridad de la información.</p>
--	---

CAPÍTULO 3

MARCO CONCEPTUAL

3 MARCO CONCEPTUAL

3.1 ANTECEDENTES

3.1.1 Historia de la Internet

La Internet es un mecanismo de difusión de información y un importante medio de colaboración entre individuos sin importar su ubicación geográfica. Es importante conocer los orígenes de esta gran red mundial, ya que ha venido a revolucionar el mundo de las computadoras y de las comunicaciones, representando un claro ejemplo de los beneficios que trae la inversión en investigación y desarrollo de infraestructura de la información.

En 1969, la Agencia de Investigación de Proyectos Avanzados del Departamento de la Defensa de los Estados Unidos, *DARPA* ("Defense Advanced Research Projects Agency") comenzó un proyecto de investigación y desarrollo de una red de computadoras que pudiera ser utilizada por importantes centros de investigación con el fin de compartir recursos e información. Esta red fue llamada ARPAnet, y tuvo tanto éxito que las organizaciones que estaban conectadas a ella comenzaron a utilizarla como medio de comunicación y para la transferencia diaria de su información.

"En 1975, la ARPAnet se convirtió de una red de experimental a una red operacional y la responsabilidad de administrar la red fue dada a la Agencia de Comunicaciones de la Defensa, *DCA* ("Defense Communications Agency")."¹

A principio de los años 80's, se desarrolló la suite de *protocolos* TCP/IP que fue adoptada como el estándar de red para las computadoras conectadas a ARPAnet. Los costos de conexión de redes comenzaron a disminuir, lo que permitió que más organizaciones se pudieran conectar a la red. "La red creció de unas cuantas computadoras a una red de decenas de miles de ellas. La ARPAnet original se convirtió en el backbone de una confederación de redes locales y regionales basadas en TCP/IP, llamada la Internet."²

En 1983, la ARPAnet fue dividida en dos partes, por un lado una red llamada *MILNET* perteneciente a la Defensa y por otro una ARPAnet más pequeña. A estas dos redes se les comenzó a conocer con el término "Internet". Cinco años más tarde, DARPA decidió terminar el proyecto y comenzó a dismantelar la ARPAnet, la cual fue reemplazada por la red *NFSNET* de la Fundación de Ciencias Nacional ("National Science Foundation") como el *backbone* de la Internet.

¹ Referencia 3, página 2.

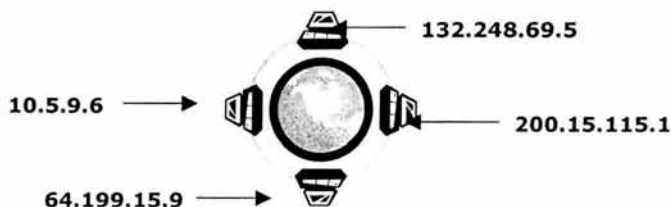
² Referencia 1, página 1.

Recientemente, en 1995, se hizo la transición de utilizar la NFSNET como el backbone de la Internet a utilizar múltiples backbones comerciales de empresas como *MCI* y *Sprint*.

Actualmente, la Internet conecta millones de computadoras haciendo posible el intercambio de información y comunicación entre usuarios de todo el mundo.

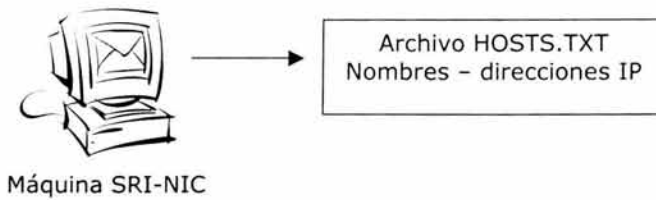
3.1.2 Historia del Sistema de Nombres de Dominio

Internet es una red basada en el conjunto de protocolos TCP/IP, el cual incluye un protocolo llamado IP, que lleva a cabo las funciones de direccionamiento y ruteo de paquetes de la red. De acuerdo al protocolo IP cada computadora que esté conectada a la red, debe contar con una dirección que la identifique de manera única. Esta dirección se conoce como dirección IP y está formada de 32 bits que se agrupan en octetos separados por puntos y representados en forma decimal. Un usuario que intenta utilizar los recursos de una computadora remota a través de la red deberá hacerlo por medio de esa dirección.



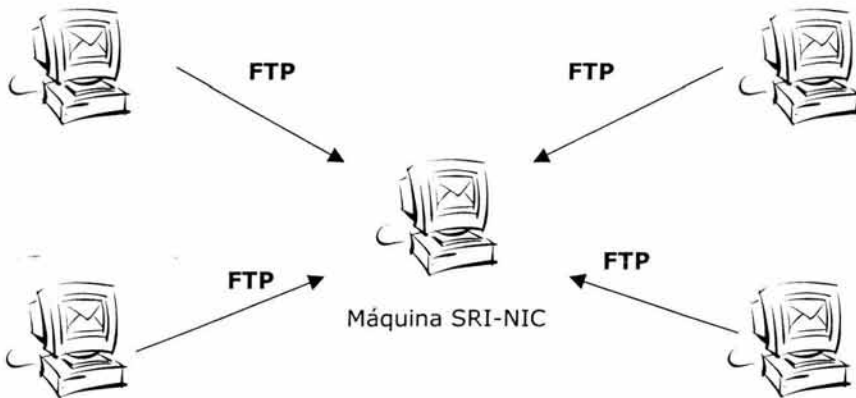
Para la mayoría de los seres humanos es más fácil recordar nombres que recordar números, por lo que, a lo largo de la historia de la Internet, se han asociado nombres fáciles de recordar para los usuarios con las direcciones IP de las computadoras. De esta manera, debe existir en alguna parte de la red, la relación completa de las direcciones disponibles con sus respectivos nombres. En el anexo 2 de este trabajo se puede consultar una explicación más detallada de TCP/IP y la manera en que funciona el direccionamiento IP.

En un principio, cuando la red era conocida como ARPANet y estaba formada por un número pequeño de computadoras conectadas, la relación de nombres y direcciones de los equipos se llevaba en un archivo llamado HOSTS.TXT, que tenía el formato de la tabla /etc/hosts del sistema operativo UNIX. Este archivo se encontraba en una máquina conocida como SRI-NIC perteneciente al Centro de Información de Red ("Network Information Center") del Instituto de Investigaciones de Stanford ("Stanford Research Institute").



Cada vez que un administrador de red de ARPAnet deseaba dar de alta el nombre de una máquina o hacer algún cambio a un nombre ya registrado, enviaba un correo electrónico a los administradores de SRI-NIC solicitando los movimientos necesarios.

Debido a las constantes altas y cambios de nombres y direcciones de las computadoras, los administradores de red debían obtener vía FTP el archivo HOSTS.TXT una o dos veces por semana, eliminarle los campos que no le servían al sistema operativo UNIX y reemplazar el /etc/hosts anterior con este archivo. Esto con el fin de mantener lo más actualizado posible la relación de nombres y direcciones de los equipos conectados a la ARPAnet, lo cual no era difícil por el reducido número de computadoras que formaban la red.



Cuando ARPAnet comenzó a crecer, el mecanismo del HOSTS.TXT se volvió obsoleto, ya que cada nueva máquina que se conectaba a la red representaba no solamente una nueva línea en el archivo, sino una actualización necesaria para todos los demás equipos.

La máquina SRI-NIC comenzó a presentar graves problemas de tráfico debido al elevado número de conexiones FTP que se hacían para actualizar el archivo. Asimismo la carga del procesador cada vez era mayor, hasta el punto de volverse intolerable.

El NIC podía asignar las direcciones a las máquinas de tal manera que fueran únicas y no se presentaran problemas de repetición que ocasionaran conflictos

a los usuarios y equipos. Pero el NIC no tenía control sobre los nombres que se daban de alta en el HOSTS.TXT, por lo que cada vez había más casos en los que dos máquinas tenían registrado el mismo nombre.

Al tiempo que la mayoría de los equipos ya habían actualizado el /etc/hosts de sus equipos con el último HOSTS.TXT, surgía un nuevo equipo que dar de alta y por lo tanto la necesidad de una nueva actualización.

“El problema esencial fue que el mecanismo del HOSTS.TXT no escaló bien. Irónicamente, el éxito de la ARPAnet como experimento, condujo al fracaso y obsolescencia del HOSTS.TXT”³

Fue entonces cuando los gobernantes de la red, decidieron que eran necesarios la investigación y desarrollo de un sistema que resolviera los problemas del mecanismo anterior. Plantearon las características que debía tener el nuevo sistema, por ejemplo, un espacio de nombres jerárquico para evitar la duplicidad de nombres, se tenía que descentralizar la administración de los datos para evitar el cuello de botella y tráfico en una sola máquina y se debía garantizar la disponibilidad de los datos por toda la red.

Entre los diversos trabajos presentados, se seleccionó el sistema planteado por Paul Mockapetris, quien en 1984 liberó los RFC’s 882 y 883 que describen el Sistema de Nombres de Dominio (“Domain Name System” o “DNS”). Estos RFC’s han sido reemplazados por los RFC’s 1034 y 1035 y complementados con muchos más que describen los problemas de seguridad del DNS, cuestiones administrativas, mecanismos para actualizaciones dinámicas, etc. Desde entonces, se ha utilizado el DNS como sistema de mapeo de nombres a direcciones IP en Internet.

3.1.3 Definiciones

3.1.3.1 Definiciones etimológicas

TÉRMINO	DEL LATÍN	DEFINICIÓN
Seguridad	Securitas - ātis	Calidad de seguro.
Sistema	Systēma	Conjunto de principios enlazados entre sí.
Nombre	Nōmen	Palabra que se da a algo.
Dominio	Dominium	Poder.

³ Referencia 1, página 3.

3.1.3.2 Definiciones de diccionario

TÉRMINO	DEFINICIÓN
Seguridad	Calidad de seguro Fianza u obligación de indemnidad a favor de uno, regularmente en materia de interés. Se aplica también a ciertos mecanismos que aseguran algún buen funcionamiento, precaviendo que éste falle, se frustre o se violente.
Sistema	Conjunto de reglas o principios sobre una materia enlazados entre sí. Conjunto de cosas que ordenadamente relacionados entre sí contribuyen a determinado objeto.
Nombre	Palabra que se apropia o se da a los objetos y a sus calidades para hacerlos conocer y distinguirlos de otros. Título de una cosa por el cual es conocida.
Dominio	Poder que uno tiene de usar y disponer libremente de lo suyo. Tierra o estado que un soberano o una república tiene bajo su dominación. Conjunto determinado de ideas, materias o conocimientos. Ámbito real o imaginario de una actividad.

3.1.3.3 Definiciones de autores

"The Domain Name System (DNS) provides the basis for converting the names of machines into IP addresses and back again and provides pointers to other resources such as mail handlers and system aliases."

"El Sistema de Nombres de Dominio (DNS) provee las bases para convertir los nombres de máquinas en direcciones IP y viceversa, y provee apuntadores a otros recursos tales como los manejadores de correo y sistemas alias".

Nicholas Trio

revista electronica OTI "OnTheInternet" septiembre/octubre 1996

nrt@watson.ibm.com

<http://www.isoc.org/oti/printversions/0996prtrio.html>

"En Internet, la comunicación entre los equipos y los humanos se facilita por el hecho de que los primeros tienen asignado un nombre, de esta forma, recordamos más fácil el nombre de una máquina ya que podemos asociar este a la organización o lugar en el que se encuentra, sin tener que memorizar la

dirección de IP del equipo. Este concepto se conoce como Sistema de Nombres de Dominio"

Oscar Robles - NIC México
revista electrónica VISION - segunda edición, mayo 1998
orobles@nic.mx
<http://vision.mty.itesm.mx/visionvirtual/>

"The Domain Name System (DNS) is predominately used to translate a structured textual identifier into a protocol-specific value. It uses the structure embedded within a hierarchical identifier space to create a distributed database, where every node within the database corresponds to a node within the name structure. The most prevalent role of the DNS is to store a set of name to address translations, allowing a domain name to be translated to an IP address."

"El Sistema de Nombres de Dominio (DNS) es predominantemente utilizado para traducir un identificador textual estructurado en un valor de protocolo específico. Utiliza la estructura dentro de un espacio jerárquico de identificadores para crear una base de datos distribuida, donde cada nodo dentro de la base de datos corresponde a un nodo dentro de la estructura de nombres. La función más prevalente del DNS es almacenar un conjunto de traducciones de nombres a direcciones IP."

G.Huston - IAB
RFC 3172 - Septiembre 2001

"El Sistema de Nombres por Dominio (DNS, Domain Name System) es una forma alternativa de identificar a una máquina conectada a Internet. La dirección IP resulta difícil de memorizar, siendo su uso más adecuado para los ordenadores. El sistema de nombres por dominio es el utilizado normalmente por las personas para referirse a un ordenador en la red, ya que además puede proporcionar una idea del propósito o la localización del mismo."

Roberto Gordo Sáenz
<http://www.geocities.com/SiliconValley/Bay/8259/parte4.html>

3.1.3.4 Definición propia

"El DNS (Domain Name System) es el sistema que permite asociar nombres a direcciones IP, mediante una base de datos distribuida y jerárquica, y que facilita el acceso a los diferentes servicios que ofrece Internet"

3.1.3.5 Sinónimos

TÉRMINO	SINÓNIMOS
Seguridad	Certeza, certidumbre, confianza, evidencia, confirmación, convicción, convencimiento, fe, protección, defensa, amparo.
Sistema	Método, régimen, técnica, procedimiento, gobierno, medio, vía, rumbo, plan, práctica, uso, costumbre, estilo, modo, suerte, tenor, modalidad, norma, regla, fórmula, ordenanza.
Nombre	Apodo, mote, alias, seudónimo, sobrenombre, calificativo, dictado, designación, denominación, título, epígrafe, tratamiento, apelativo, apellido, patronímico, sustantivo.
Dominio	Feudo, posesión, pertenencia, territorio, colonia, hacienda, reino, mandato, propiedad, terreno, campo, tierra.








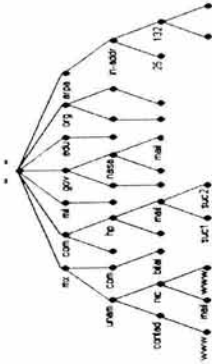


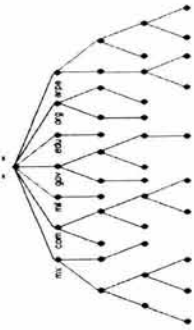
3.1.3.6 Antónimos

TÉRMINO	ANTÓNIMOS
Seguridad	Incertidumbre, debilidad, duda, desconfianza, sospecha, alarma.
Sistema	Desorganización.
Nombre	Anónimo, desconocimiento.
Dominio	Esclavitud, subordinación

3.2 MONOGRAFÍA - SEGURIDAD EN DNS

<p>Internet.- Es la red de computadoras más grande en el mundo. Permite compartir información, recursos computacionales y comunicación entre usuarios de todo el mundo.</p>	<p>Servicios en Internet.- Internet ofrece diversos servicios, los más utilizados son:</p> <ul style="list-style-type: none"> ◆ Web.- Consulta de información. ◆ E-mail.- Comunicación entre usuarios. ◆ FTP.- Transferencia de archivos. ◆ NEWS.- Difusión de noticias. 	<p>Dirección IP.- Es el conjunto de 4 números separados por puntos que sirven para identificar de manera única a las computadoras conectadas a Internet. No deben repetirse. Ejemplo, 200.15.115.130</p>
<p>Nombre de dominio.- Es el nombre que se utiliza para hacer referencia a una máquina o servicio dentro de Internet. Se usa como sinónimo de las direcciones IP de las máquinas. Ejemplo, www.nic.unam.mx.</p>	<p>DNS (Sistema de Nombres de Dominio).- Es una base de datos distribuida que contiene la información acerca de los dominios en Internet. Consta de 3 componentes principales: El espacio de nombres de dominio, los servidores de nombres y los resolvers.</p>	<p>Servidor de Nombres.- Es un componente del sistema de nombres de dominio. Es un programa que da información acerca de ciertos dominios en Internet.</p>
<p>Espacio de nombres de dominio.- Es la base de datos distribuida en la que está contenida toda la información acerca de los nombres de dominio en Internet. Tiene una estructura jerárquica y arborescente, donde el primer nivel se conoce como dominio raíz.</p>	<p>Resolver.- es un componente del Sistema de Nombres de Dominio que interactúa entre los programas de los usuarios y los servidores de nombres. Sus funciones son:</p> <ul style="list-style-type: none"> ◆ Hacer a los servidores de nombres la pregunta que le ha pasado algún programa de usuario. ◆ Interpretar las respuestas enviadas por el servidor de nombres. ◆ Pasar la respuesta a los programas de usuario que solicitaron la información. 	<p>Dominio de nivel superior.- Son los dominios que se encuentran en el nivel 1 dentro de la estructura de nombres de dominio. Inicialmente eran:</p> <ul style="list-style-type: none"> ◆ Com.- Organizaciones comerciales. ◆ Edu.- Instituciones educativas. ◆ Gov.- Instituciones de gobierno. ◆ Mil.- Instituciones militares. ◆ Net.- Organizaciones y Proveedores de Servicios de Internet. ◆ Org.- Organizaciones no lucrativas ◆ Int.- Instituciones internacionales <p>Se ha agregado un dominio de nivel superior para cada país y algunos otros de uso general. Ej, mx, ca, info.</p>

MONOGRAFÍA - SEGURIDAD EN DNS

		 <p>200.15.115.130</p>  <p>200.15.115.131</p>
 <p>www.nic.unam.mx =</p> <p>200.15.115.131</p>	<p>www.unam.mx www.banamex.com</p>  <p>www.nasa.gov www.semarnat.gob.mx</p>	<p>¿Quién es www.unam.mx?</p> <p>38 15 115 200 1 N A C</p>  <p>DNS</p>
<p>Espacio de Nombres de Dominio</p> 	<p>Servidor de Nombres</p>  <p>Resolver</p>  <p>Programas de usuario</p>	<p>Dominios de Nivel Superior</p> 

3.3 CLASIFICACIONES

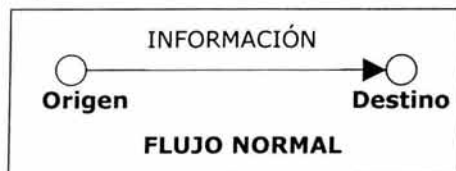
Actualmente, Internet es uno de los medios de comunicación más utilizados en todo el mundo. Millones de personas consultan diariamente la información que se publica a través de las miles de páginas web existentes y hacen uso de los múltiples servicios que se ofrecen, como son, el correo electrónico, la transferencia de archivos, transacciones bancarias, comercio electrónico, etc. Sin embargo, Internet no puede considerarse una red segura, ya que nadie puede garantizar que la información o servicios que se consultan son plenamente confiables.

Inicialmente, Arpanet no fue diseñada pensando en la seguridad de la información que en ella se almacenara o transmitiera. La comunidad que tenía acceso a la red, estaba formada principalmente por investigadores con un alto grado de conocimientos en computación, y dada la ausencia de carreras profesionales en el área de cómputo, era difícil que cualquier persona mal intencionada cubriera el perfil necesario para hacer uso de los recursos de la red. "El gremio de los especialistas en computación era bastante pequeño y esto propiciaba un control interno de los especialistas: cualquiera que tuviera una conducta inapropiada, era rápidamente denunciado ante sus colegas y veía cerradas las puertas de la mayoría de los empleos en una sanción social automática"⁴. La posibilidad de cometer un delito informático era prácticamente nula.

En los últimos años, el uso de la computadora personal se ha vuelto más popular, el costo del hardware ha disminuido considerablemente y para tener acceso a Internet ya no es necesario ser experto en computación. Prácticamente cualquier persona con acceso a la gran red, puede lograr irrumpir en el sistema de alguna organización y tener a su disposición información que pueda considerarse confidencial.

3.3.1 Amenazas a la seguridad

En el proceso normal de comunicación, existen 3 componentes principales: el emisor, el receptor y el medio por el cuál se lleva a cabo dicha comunicación. De igual manera, en el intercambio electrónico de información, existe un flujo normal de datos que va desde un origen a un destino y que puede representarse de la siguiente manera:



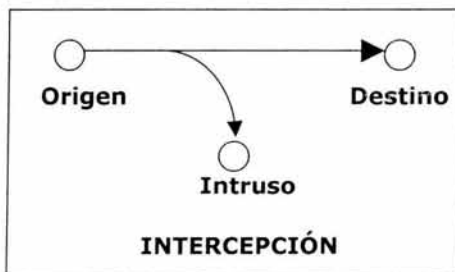
⁴ Referencia 11, página 3.

Cuando se lleva a cabo un ataque a la seguridad de la información, se corrompe este flujo normal que debería seguir el intercambio de datos. De acuerdo a la manera en que este flujo es alterado, podemos clasificar las amenazas a la seguridad de un sistema de cómputo en 4 categorías:

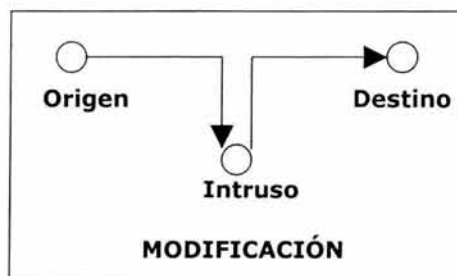
Interrupción.- Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de administración de archivos.



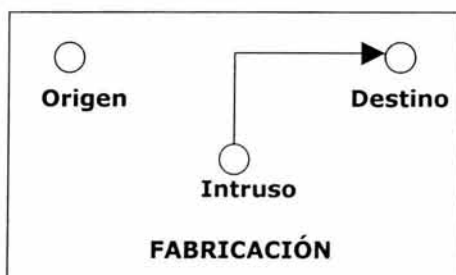
Intercepción.- Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora. Ejemplos de este ataque son la intervención de una línea de comunicación para obtener los datos que circulan por la red (intercepción de datos), o bien la lectura de los encabezados de paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación (intercepción de identidad).



Modificación.- Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.



Fabricación.- Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes en una red o añadir registros a un archivo.



3.3.2 Ataques y tipos de ataques

Un ataque a la seguridad es cualquier acción que compromete la seguridad de la información, de una persona u organización. Existen diversos tipos de ataques, los cuales podemos clasificar de una manera muy general, de acuerdo al objetivo que persiguen, en ataques pasivos y ataques activos.

Ataques pasivos

El atacante no altera la comunicación, únicamente la escucha o monitorea, para obtener información que está siendo transmitida (Intercepción). Ataques de este tipo son:

- ♦ **Revelación del contenido de mensajes.-** Se obtiene el contenido de los mensajes transmitidos. Por ejemplo, una conversación telefónica, correos electrónicos, transferencias de archivos con información sensible o confidencial.
- ♦ **Análisis de tráfico.-** Aún cuando existe una manera de cifrar el contenido de los mensajes, se pueden obtener datos acerca de la naturaleza de la información analizando los patrones de los

mensajes, como pueden ser: determinar la ubicación e identidad de los hosts que se están comunicando u observar la frecuencia y tamaño de los mensajes que se están intercambiando.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos (Interrupción, modificación y fabricación). Ataques de este tipo son:

- ◆ **Suplantación de identidad.-** El intruso se hace pasar por una identidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, capturar y repetir secuencias de mensajes que han sido autenticados, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la identidad que posee esos privilegios.
- ◆ **Repetición.-** Involucra la captura pasiva de unidades de datos y su posterior retransmisión para producir un efecto no deseado, como por ejemplo, ingresar repetidas veces en una cuenta dada.
- ◆ **Modificación de mensajes.-** Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".
- ◆ **Negación del servicio.-** Impide o inhibe el uso normal o la administración de recursos informáticos y de comunicaciones. Ejemplos de estos ataques pueden ser paralizar temporalmente el servicio de un servidor de correo, web, ftp, DNS, etc.

Existen muchos ataques informáticos que pueden clasificarse desde diferentes puntos de vista. Dos ataques que nos interesan son los que se realizan a los algoritmos y a los protocolos.

Podemos decir que un **algoritmo** es una serie de pasos, finitos y ordenados con el objetivo de resolver un problema, y un **protocolo** es la forma de utilizar los algoritmos para implementar servicios de seguridad.

De esta manera los ataques a los algoritmos atacan las debilidades del algoritmo mismo. Estos ataques se llevan a cabo regularmente por criptoanálisis y son difíciles de realizar ya que se necesita un alto grado de conocimientos de técnicas matemáticas.

Los ataques a los protocolos, explotan la forma en que son utilizados los algoritmos, es decir, las implementaciones. La mayoría de los ataques

existentes están incluidos dentro de esta categoría, y entre ellos se incluyen los ataques al DNS.

3.3.3 Servicios de seguridad

Un servicio de seguridad es una función que debe de cumplir un sistema de información para salvaguardar los datos que maneja. De acuerdo a la arquitectura de seguridad OSI, existen 5 clases de servicios de seguridad:

Confidencialidad.- Servicio que consiste en que la información sea accedida únicamente por las entidades autorizadas. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

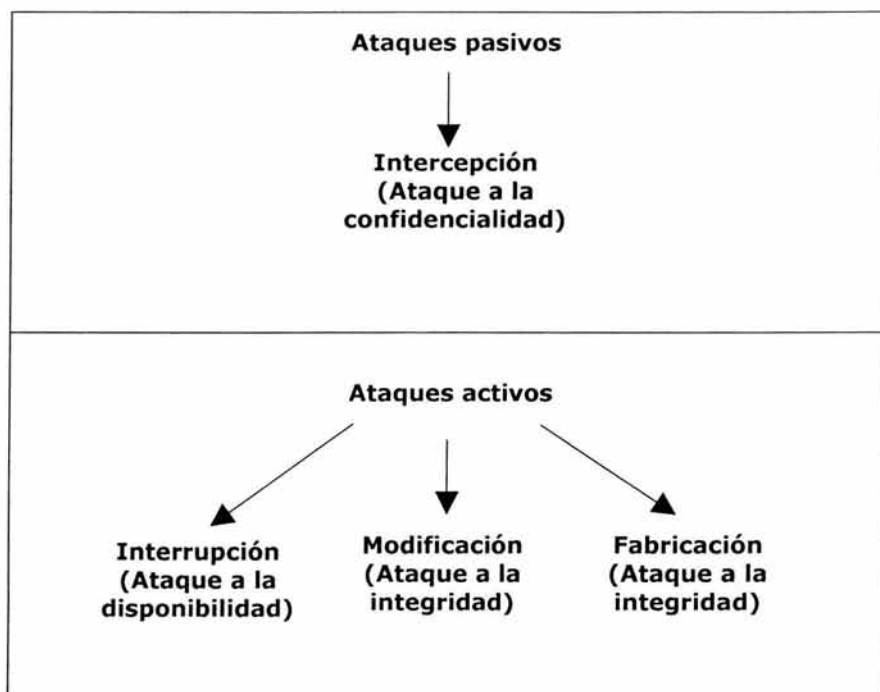
Integridad.- Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y repetición de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas.

Autenticación.- Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: **de entidad**, que asegura la identidad de las entidades participantes en la comunicación, y **de origen** de información, que asegura que una unidad de información proviene de cierta entidad.

No Repudio.- Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

Control de Acceso.- Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

De esta manera, la clasificación de ataques, de acuerdo a la amenaza que representan y el servicio de seguridad que afectan, puede resumirse en el siguiente cuadro:



3.3.4 Atacantes

El tipo de personas que realizan los ataques informáticos, así como los objetivos que buscan, son diversos. Víctor López Guerrero, en su tesis "Análisis de riesgos en centros de cómputo", nos propone la siguiente clasificación de los tipos de atacantes y los objetivos que estos persiguen.

Atacantes:

- Hackers
- Espías
- Terroristas
- Jinetes corporativos
- Criminales profesionales
- Vándalos

Objetivos que persiguen los atacantes al irrumpir en un sistema:

- Reto, status
- Objetivos políticos
- Objetivos financieros
- Daño

3.3.5 Amenazas y ataques famosos en Internet

Sin duda, los ataques a los servicios y sistemas conectados a Internet han tenido su mayor auge en los últimos años. Esto se debe al rápido crecimiento que ha tenido la gran red en la última década. A continuación se presenta una cronología resumida de los ataques a seguridad y hechos que han tenido mayor trascendencia en la historia de Internet.

1969

- ♦ Internet comienza como ARPANET. Los protocolos de aquella red, fueron diseñados para proporcionar flexibilidad en el servicio, no seguridad. Los usuarios, que en su mayoría eran investigadores, necesitaban compartir su información de una manera fácil y tener acceso a la red sin restricciones.

1971

- ♦ Se unen más computadoras de gobierno y de universidades a la ARPANET, la cual se convierte en una importante herramienta de intercambio de información para la investigación. Los usuarios comienzan a jugarse bromas entre sí a través de la red, tales como mensajes obscenos, y otras violaciones de seguridad que se consideraban menores.

1987

- ♦ Robo a banco. Gerente regional obtiene 25 millones de dólares.
- ♦ Ataque a la transmisión satelital (HBO) por *uplink*.
- ♦ Club del caos. Club de Alemania del este. Anunciaban penetración exitosa a computadora de la NASA.
- ♦ Clif Stoll y la KGB. *Crackers* de Alemania del Este intentan penetrar 450 computadoras, en 30 tienen éxito. Su objetivo era obtener información para vender a la KGB.

1988

- ♦ Aerolínea importante descubre que su sistema de reservación y boletaje ha sido penetrado. Se hacen reservaciones ficticias. Se utilizan boletos ilegales.
- ♦ Gusano en Internet. Se registra el primer incidente de seguridad automatizado en la red, conocido como "The Morris Worm". Un estudiante de la Universidad de Cornell, Robert Morris, escribió un programa que se conectaría a una máquina remota y se autoreplicaría para acceder a otras máquinas. Como resultado, el 10% de las computadoras conectadas a la ARPANET quedaron fuera de servicio.
- ♦ Virus Viernes 13. Borra disco duro de computadoras financieras, administrativas y de investigación. Origen en la universidad hebrea de Jerusalén.

- ♦ Virus Flambe. Infecta computadora de firma consultora, altera el barrido (scan rate) de monitores IBM y provoca que estallen en llamas.
- ♦ Sistema de posicionamiento satelital. Niño de 14 años con una computadora Apple irrumpe en sistema de la fuerza aérea de USA.

1990

- ♦ Operación Desert Storm / Desert Shield. 40 intentos conocidos (6 con éxito confirmado).

1995

- ♦ Sistemas de control de tráfico aéreo. El tráfico aéreo se retrasa por varias horas.
- ♦ Macro Virus Word. Virus prevalentes actuales.

1997

- ♦ Caballo de Troya ActiveX. Transfiere fondos de cuentas bancarias a la del hacker.

3.3.6 Ataques más comunes en Internet

En Internet existe un centro dedicado a la atención de reportes de seguridad. Este centro es conocido como CERT/CC, y de acuerdo a sus estadísticas de reportes, los ataques más comunes en Internet son:

Prueba.- Se caracteriza por intentos de lograr acceso a un sistema o de encontrar información acerca del sistema. Un ejemplo es un intento de acceso a una cuenta que no es utilizada. Las pruebas son seguidas de eventos de seguridad más serios, pero regularmente son el resultado de la curiosidad o de la confusión.

Escaneo.- Un escaneo o barrido es simplemente un gran número de pruebas realizadas utilizando una herramienta automática. Algunas veces los escaneos son el resultado de una mala configuración pero la mayoría de las veces son un preludio de un ataque dirigido a sistemas en los cuales los intrusos han encontrado una vulnerabilidad.

Comprometer cuentas.- Una cuenta es comprometida cuando es utilizada por una persona diferente a su dueño. Puede ocasionar pérdida y/o robo de información, así como robo de servicios.

Comprometer cuentas de administración.- La cuenta comprometida es aquella con privilegios de administración sobre el sistema. Es el caso de los sistemas UNIX, la cuenta de administración es conocida como root y tiene

privilegios ilimitados, por lo cual, un ataque exitoso a esta cuenta podría ocasionar serios daños al sistema.

Olfateo de paquetes ("Paquet Sniffer").- Un olfateador de paquetes es un programa que captura datos de los paquetes de información mientras son transmitidos a través de la red. La información capturada puede incluir nombres de usuarios, passwords, información confidencial, números de tarjetas bancarias, etc.

Negación de servicio.- El objetivo de un ataque de negación de servicio no es obtener acceso a un sistema, sino evitar que los usuarios legítimos lo hagan. Para lograr esto, los atacantes envían una gran cantidad de peticiones de algún servicio a la máquina atacada, consumiendo así gran parte de sus recursos y ocasionando que otros servicios no puedan ser atendidos.

Explotación de relaciones de confianza.- Las computadoras conectadas a red, regularmente tienen relaciones de confianza unas con otras. El uso no autorizado de esa relación de confianza ocasiona un problema de seguridad que puede resultar en un ataque.

Ataques a la infraestructura de Internet.- Son poco comunes, pero involucrar componentes clave de la infraestructura de Internet, por ejemplo, los servidores de nombres.

Para este trabajo nos interesa conocer los ataques que se llevan a cabo a los servidores de nombres, ya que tal y como el mismo CERT lo menciona, este servicio es una parte importante para el funcionamiento de Internet.

3.4 EL SISTEMA DE NOMBRES DE DOMINIO

El Sistema de Nombres de Dominio, es una base de datos distribuida, que trabaja bajo la arquitectura cliente/servidor y que contiene la información acerca de los dominios en Internet. Consta de 3 componentes principales:

- ◆ **El espacio de nombres de dominio,**
- ◆ **los servidores de nombres y**
- ◆ **los clientes o "resolvers".**

3.4.1 El Espacio de Nombres de Dominio.

Toda la información acerca de los nombres en Internet, se encuentra en una base de datos distribuida y jerárquica, a la que se le conoce con el nombre de "espacio de nombres de dominio". Esta base de datos tiene una estructura con forma de árbol invertido, en donde cada hoja del árbol o nodo representa un nombre de dominio o bien el nombre de una computadora bajo un dominio. De cada uno de los nodos que forman el árbol puede desprenderse cualquier

número de nodos que al ser dependientes del primero recibirán el nombre de "nodos hijos". Al nodo que les da origen se le da el nombre de "nodo padre". "La profundidad del árbol está limitada a 127 niveles"⁵.

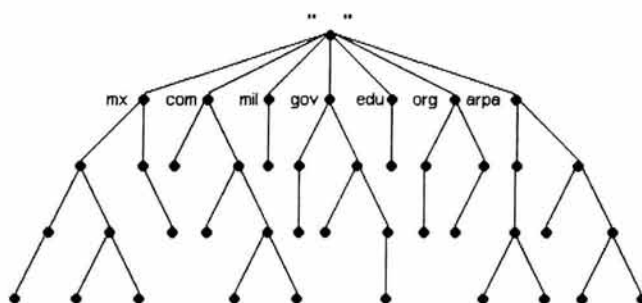


Figura 1.- El Espacio de Nombres de Dominio.

Al nodo que se encuentra en la parte más alta del espacio de nombres de dominio y el cual le da origen a todos los demás nodos, se le conoce con el nombre de "dominio raíz".

"Cada nodo en el árbol tiene una etiqueta de texto (sin puntos) que puede ser de hasta 63 caracteres de longitud"⁶. La etiqueta vacía (" ") está reservada como nombre para el dominio raíz, pero todos los demás nodos pueden tener cualquier nombre siempre y cuando este no se repita entre dos nodos que se encuentran en el mismo nivel y que dependan del mismo nodo padre. Esta última regla permite que los nombres sean únicos en todo el espacio de nombres y no ocasionen conflictos de repetición.

A cada uno de los nodos del árbol se le da un nombre de dominio como identificador. "El nombre de dominio completo de cualquier nodo en el árbol es la secuencia de etiquetas en la ruta que va desde ese nodo hasta la raíz"⁷. Cada una de las etiquetas que forman el nombre de dominio deberá estar separada con un punto (".") y deberá colocarse a la izquierda el nombre del nodo al que estemos haciendo referencia y a la derecha el nombre del nodo más cercano al dominio raíz o bien el dominio raíz. La longitud total de un nombre de dominio está limitada a 255 caracteres.

⁵ Referencia 1, página 12.

⁶ Referencia 1, página 12.

⁷ Referencia 1, página 12.

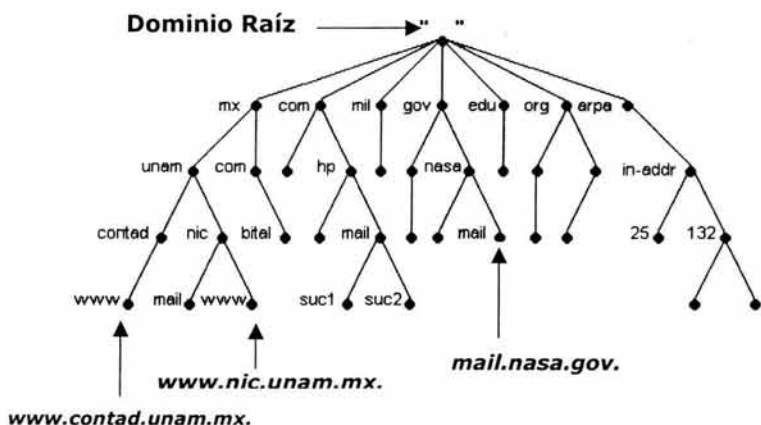


Figura 2.- Nombres de dominio.

En la figura anterior se puede ver que existen dos nodos llamados "www" en el mismo nivel, pero al no depender del mismo nodo padre, no ocasionan conflictos de repetición de nombres, ya que uno se llama *www.contad.unam.mx* y el otro *www.nic.unam.mx*.

Se puede dividir los nombres de dominio en dos tipos: nombres de dominio absolutos y nombres de dominio relativos.

Cuando en un nombre de dominio se pone un punto al final, se le está incluyendo la etiqueta vacía del dominio raíz, por lo cual se dice que es un nombre de dominio absoluto o bien un Nombre de Dominio Completamente Calificado, FQDN ("Fully Qualified Domain Name"). "Un nombre de dominio absoluto es escrito relativo a la raíz y especifica sin ambigüedades la ubicación de un nodo en la jerarquía"⁸.



⁸ Referencia 1, página 12.

Si no se incluye el punto al final del nombre de dominio se dice que es un nombre relativo y deberá ser completado con el dominio en el que se está trabajando. Por ejemplo, si un usuario que esté trabajando con un software que tenga configurado el dominio nic.unam.mx, hace referencia al nombre "deimos" sin incluirle el punto al final, el software interpretará que deberá agregarle el dominio nic.unam.mx para completarlo y dejarlo como nombre absoluto.



Un dominio es una parte del espacio de nombres de dominio total que comienza en cualquier nodo e incluye todos y cada uno de sus nodos hijos. "El nombre de dominio de un dominio es el mismo que el nombre de dominio del nodo que se encuentra en la cima del dominio"⁹. Por ejemplo, el dominio mx comienza en el nodo con el nombre de dominio mx e incluye todos los nodos que de él se derivan, tal y como se muestra en la siguiente figura:

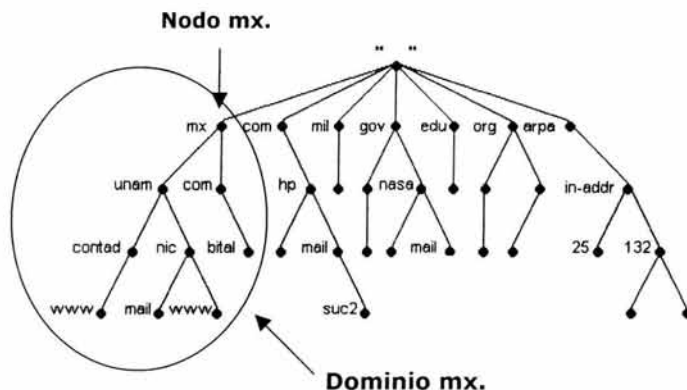


Figura 3.- Dominio mx y nodo mx.

"Un dominio es un subdominio de otro dominio si está contenido dentro de ese otro dominio"¹⁰. De esta manera y tomando en cuenta la figura anterior, unam.mx y com.mx son subdominios del dominio mx. A su vez,

⁹ Referencia 1, página 13.

¹⁰ Referencia 6, página 8.

contad.unam.mx y nic.unam.mx son subdominios del dominio unam.mx y bital.com.mx es un subdominio de com.mx.

Pero los nodos del espacio de nombres de dominio no sólo representan dominios y subdominios, también representan la información que realmente le interesa a los usuarios. "Los nombres de dominio en las hojas del árbol generalmente representan hosts individuales y estos pueden apuntar a direcciones de red, información de hardware e información de ruteo de correo"¹¹

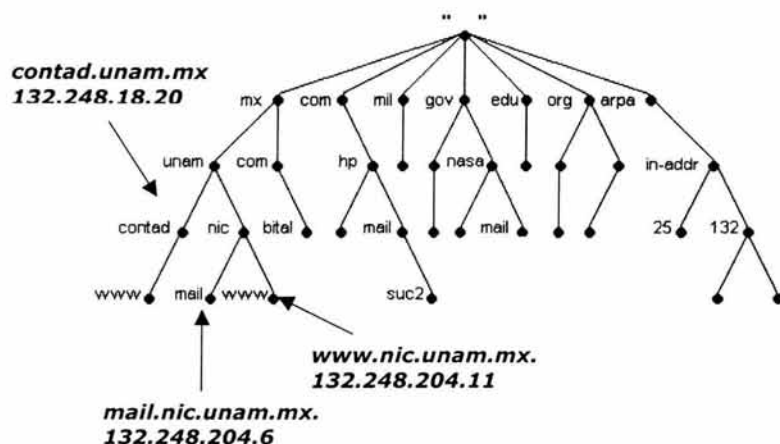


Figura 4.- Nombres de hosts asociados a direcciones IP

En esta figura el nodo con el nombre de dominio contad.unam.mx, representa el inicio del dominio contad.unam.mx, pero a su vez indica que existe un equipo de cómputo con el mismo nombre y con la dirección IP 132.248.18.20. El nodo www.nic.unam.mx representa el nombre de otro equipo de cómputo apuntando a la dirección IP 132.248.204.11.

Otra manera de hacer referencia a los dominios, además de su nombre, es por su nivel. El nodo del espacio de nombres de dominio que representa el dominio raíz está en el nivel 0 por ser el nodo más alto. Todos los dominios que se derivan directamente del dominio raíz están en el nivel 1 y son conocidos como Dominios de Nivel Superior o TLD ("Top Level Domains"). Los dominios que se derivan de alguno de nivel superior se encuentran en el nivel 2 y así sucesivamente.

¹¹ Referencia 1, página 15.

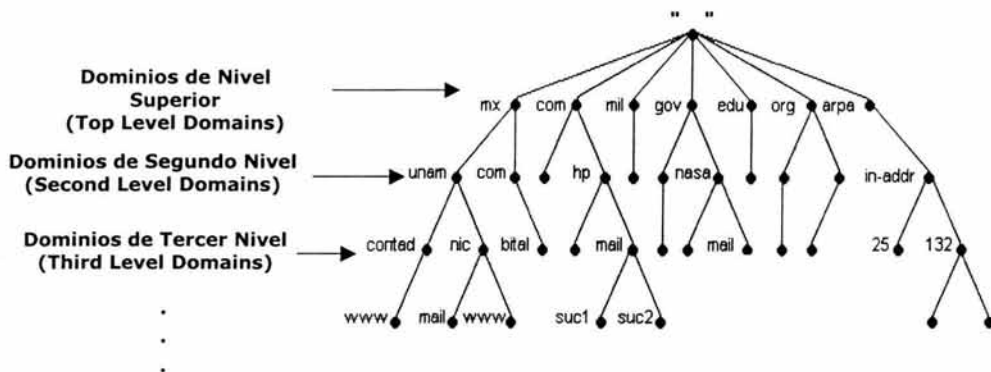


Figura 5.- Niveles de Dominios.

En el espacio de nombres de dominio que actualmente se utiliza en Internet, se han asignado nombres especiales a los Dominios de Nivel Superior como una forma de organización de acuerdo al uso que se les vaya a dar a los dominios.

Cuando comenzó el uso del Sistema de Nombres de Dominio, sólo existían siete Dominios de Nivel Superior, los cuales eran:

- Com** Destinado a organizaciones comerciales (Ejemplo: hp.com para Hewlett Packard).
- Edu** Utilizado por instituciones de educación superior (Ejemplo: berkeley.edu para la Universidad de Berkeley).
- Gov** Para instituciones gubernamentales (Ejemplo: nasa.gov para la NASA).
- Mil** Organizaciones militares (Ejemplo: army.mil para las Fuerzas Armadas).
- Net** Para instituciones que tengan que ver con la organización de Internet así como para Proveedores de Servicios de Internet (ISP's). (Ejemplo: nfs.net).
- Org** Destinado para organizaciones no lucrativas (Ejemplo: eff.org).
- Int** Reservado para instituciones internacionales (Ejemplo: nato.int).

Al incrementarse el uso de Internet alrededor del mundo, se agregaron otros Dominios de Nivel Superior, uno para cada país de acuerdo a un estándar internacional llamado ISO 3166, el cual establece abreviaturas de dos letras para los nombres de todos los países. El estándar ISO 3166 es incluido en el anexo 3 del presente trabajo.

3.4.2 Servidores de nombres y los registros de origen

Como ya se ha mencionado, el Sistema de Nombres de Dominio trabaja bajo la arquitectura cliente/servidor, en donde la parte del servidor la realizan los programas conocidos como "servidores de nombres" o "name servers".

"Los servidores de nombres generalmente tienen información completa acerca de alguna parte del espacio de nombres de dominio, llamada zona, la cual cargan de un archivo o de otro servidor de nombres"¹².

Uno de los principales objetivos del diseño del Sistema de Nombres de Dominio, era la descentralización de la administración de los nombres. Esto se logra dividiendo el espacio de nombres de dominio en zonas y delegándolas a diversas organizaciones para que se hagan cargo de su administración y mantenimiento.

No es lo mismo hablar de un dominio que de una zona. Un **dominio** es un conjunto de nodos que terminan con el mismo nombre de dominio y una **zona** es un área dentro de un dominio cuya autoridad, administración y mantenimiento ha sido delegados a una organización. "Una zona define el contenido de una sección contigua del espacio de nombres de dominio, generalmente limitado por límites administrativos"¹³.

Actualmente, la zona que se encuentra en la parte superior del espacio de nombres de dominio se conoce como "zona raíz" y se encuentra bajo la administración de IANA ("Internet Assigned Number Authority"), la cual ha ido delegando el mantenimiento de algunos de los dominios de nivel superior que forman la zona raíz. "La Internet Assigned Numbers Authority (IANA) es responsable de toda la coordinación y administración del Sistema de Nombres de Dominio (DNS), y especialmente la delegación de porciones del espacio de nombres llamados dominio de nivel superior"¹⁴

La zona raíz esta dividida en 5 categorías de Dominios de Nivel Superior:

1) Dominios mundiales, mantenidos por InterNIC:

- ◆ COM
- ◆ NET
- ◆ ORG

¹² Referencia 1, página 21.

¹³ Referencia 9, página 1.

¹⁴ Referencia 3, página 3.

2) Dominios de estado especial:

- ◆ EDU
- ◆ INT

3) Dominios reservados para Estados Unidos:

- ◆ GOV
- ◆ MIL

4) Dominios para países basados en el ISO 3166

- ◆ FR, MX, CA, BR, etc.

5) Dominio inverso

- ◆ IN-ADDR.ARPA

Los dominios COM, NET, ORG y EDU son mantenidos por InterNIC, organización dedicada al registro de dominios. IANA mantiene la autoridad sobre los dominios INT e IN-ADDR.ARPA.

Los dominios GOV y MIL están a cargo del gobierno y el ejército de Estados Unidos respectivamente.

Adicionalmente, en noviembre del 2000, después de largas discusiones en la comunidad de Internet, el ICANN aprobó la creación de 8 nuevos dominios de nivel superior. Estos nuevos TLD's fueron creados para dar de alta dominios de acuerdo al giro o propósito de las organizaciones y son:

.aero	Industria de aero-transporte.
.biz	Empresas (Business).
.coop	Asociaciones cooperativas.
.info	Para todos los usuarios.
.museum	Museos.
.name	Individuos.
.pro	Profesiones
.tv	Cadenas televisoras.

De estos dominios solo .biz, .info y .name se encuentran actualmente disponibles para registros.

En el caso de los dominios de nivel superior basados en el ISO 3166, han sido delegados a una organización en particular dentro de cada país.

El dominio mx, correspondiente a México, ha sido delegado a NIC-México ("Network Information Center - México"), organización cuyas funciones son "el proveer los servicios de registro y asignación de recursos de Internet para

México, tales como nombres de dominio bajo el nTLD o direcciones de IP, así como el mantenimiento de las bases de datos respectivas a cada recurso¹⁵.

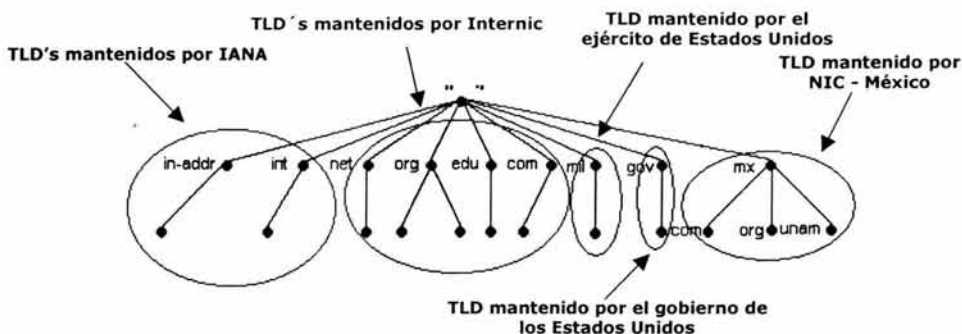


Figura 6.- La zona raíz

Si una organización que está a cargo de una zona lo considera necesario, puede tomar zonas más pequeñas y delegarlas a su vez a otras entidades, por ejemplo, NIC-México delegó la administración de la zona unam.mx al Centro de Información de RedUNAM.

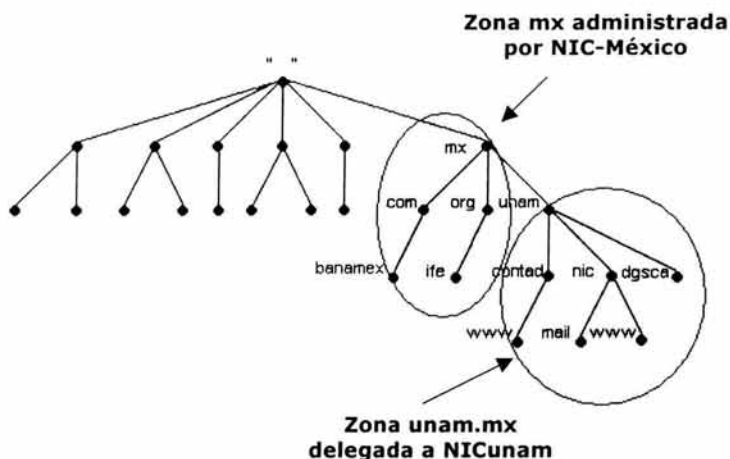


Figura 7.- Delegación de Zonas

¹⁵ Referencia 12.

Cada organización debe tener sus propios servidores de nombres en los que se encontrará toda la información acerca de las zonas que le han sido delegadas. "Una zona contiene los nombres de dominio que el dominio con el mismo nombre dominio contiene, excepto para los nombres de dominio en los subdominios delegados"¹⁶, por lo tanto, los servidores de nombres de NIC-México contienen la información de toda la zona mx, excepto de la zona unam.mx, la cual está contenida en los servidores de nombres de RedUNAM.

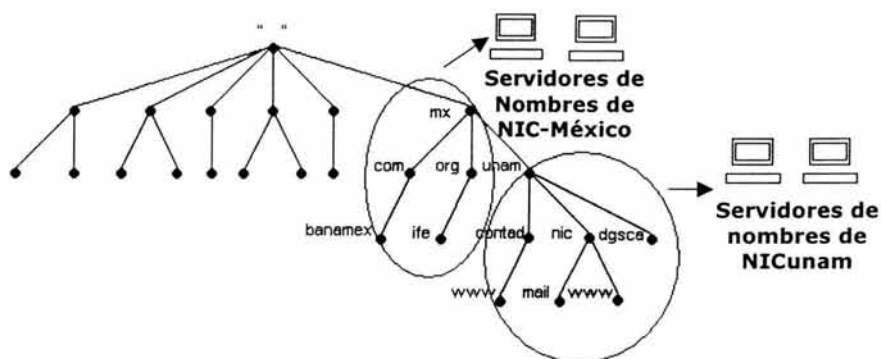


Figura 8.- Servidores de Nombres por Zona.

Una organización puede tener delegadas varias zonas del espacio de nombres de dominio sin que estas se encuentren necesariamente juntas o cerca en el árbol.

Cuando un servidor de nombres contiene la información de una zona se dice que es "autorizado" o "autoritario" para dicha zona. De esta manera, los servidores de nombres de NIC-México son autorizados para la zona mx, excepto para la zona unam.mx, ya que los servidores de nombres autorizados para esta son los del Centro de Información de RedUNAM.

Los servidores de nombres tienen configurado un archivo por cada una de las zonas o dominios para los cuales son autorizados. Estos archivos se conocen con el nombre de "archivos de la base de datos" o "db files" ("Data base files") y es en estos donde se guarda toda la información existente sobre la zona o dominio.

Existen dos tipos de servidores de nombres: primarios y secundarios.

¹⁶ Referencia 1, página 22.

Los servidores de nombres **primarios** o **“maestros”** obtienen la información acerca de las zonas para las cuales son autorizados a partir de archivos que se encuentran en la misma máquina. Los archivos de configuración de zonas en un servidor de nombres primario son creados y modificados manualmente por el administrador.

Los servidores de nombres **secundarios** o **“esclavos”** también tienen archivos con la información acerca de las zonas o dominios para los cuales son autorizados, pero estos no se crean ni modifican por el administrador, sino son copiados del servidor primario de estas zonas o dominios. Al proceso de copiar el archivo de la base de datos de una zona desde un servidor de nombres primario a uno secundario se le conoce como **“transferencia de zona”**.

Una zona puede estar configurada únicamente en su servidor de nombres primario, pero puede, y de hecho es muy recomendable, estar configurado también en uno secundario. “Los servidores de nombres esclavos son importantes por que es buena idea configurar más de un servidor de nombres para una zona dada”¹⁷. Esto ayuda a repartir la carga de trabajo entre ambos servidores de nombres y a asegurar que en caso de que uno falle estará el otro disponible para seguir dando información acerca de la zona.

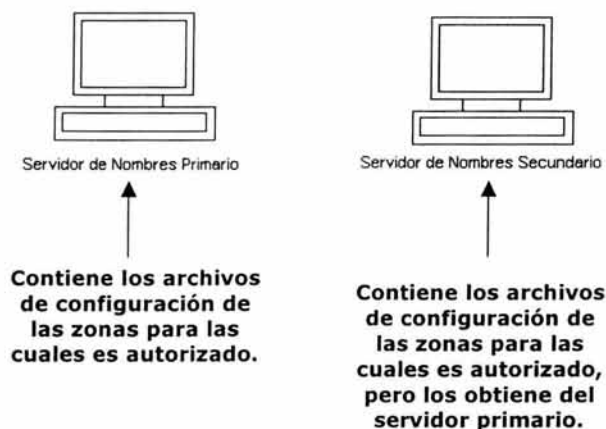


Figura 9.- Servidores de nombres primarios y secundarios.

Los archivos de configuración que contienen los servidores de nombres para cada una de las zonas para las cuales son autorizados, son archivos de tipo

¹⁷ Referencia 1, página 25.

texto y están formados de registros que tienen un formato especial. A los registros se les llama "Registros de Origen" o "RR's" ("Resource Records"). "Los registros de origen describen todas las computadoras en la zona y marcan cualquier delegación de subdominios"¹⁸.

Existen varios tipos de registros de origen que definen los diferentes tipos de información que un servidor de nombres puede dar acerca de una zona. Un registro de origen especifica la dirección IP que tiene asignado un nombre de dominio, la forma en que una máquina recibe correo electrónico, información acerca del software y hardware de un equipo, etc.

El formato general de los registros de origen está formado de 5 campos, separados por espacios en blanco.

< nombre > < ttl > < clase > < tipo > < datos >

Este número de campos puede variar según el tipo de registro de origen en cuestión.

< nombre >

El primer campo especifica el nombre de dominio al que se va a aplicar el registro. Cuando este campo se deja en blanco hace referencia al mismo nombre de dominio del registro anterior en el archivo de configuración. Los nombres de dominio utilizados en este campo pueden ser tanto absolutos como relativos. Si se utilizan nombres de dominio relativos se les agregará al final el nombre de la zona o dominio al cual pertenece el archivo de configuración.

Cualquier caracter de 8 bits es permitido en el Sistema de Nombres de Dominio, sin embargo, algunas otras aplicaciones o protocolos tienen restricciones en cuanto a los caracteres que permiten. "Debido a las restricciones de otros protocolos, solamente los siguientes caracteres son recomendados para usar en un nombre de máquina (además del punto separador):

A - Z, a - z, 0 - 9, guión seguido y guión bajo"¹⁹.

< ttl >

El TTL ("Time To Live") es el tiempo de vida en segundos de la información que está definiendo el registro, es decir, es el tiempo que un cliente de DNS podrá guardar en su memoria la información acerca de este registro antes de desecharla y tener que volver a preguntarle al servidor de nombres.

¹⁸ Referencia 1, página 26.

¹⁹ Referencia 9, página 4.

El tiempo de vida para cada registro lo decide cada administrador considerando que tan frecuentemente cambiará la información de una zona. Si se define un tiempo de vida muy bajo, el servidor de nombres tendrá mucha carga de trabajo ya que los clientes de DNS guardarán la información del registro por muy poco tiempo y preguntarán constantemente al servidor de nombres acerca del registro. Si se define un tiempo de vida muy alto, la carga del servidor de nombres disminuirá, pero al hacer alguna modificación en la información que contiene el registro, no será distribuida entre los clientes de DNS hasta que estos desechen la información anterior y pregunten nuevamente al servidor de nombres; como consecuencia, los clientes de DNS podrían estar contestando con información que ya no sea válida. "Todos los registros de origen con el mismo nombre, clase y tipo deben tener el mismo valor TTL"²⁰.

< clase >

El diseño del Sistema de Nombres de Dominio permite manejar información útil bajo cualquier grupo de protocolos. "El campo clase es utilizado para identificar el grupo de protocolos dentro del cual está cada RR"²¹.

La clase más utilizada en este campo es "**IN**" que se refiere al grupo de protocolos utilizadas en Internet, es decir, TCP/IP.

Otras clases existentes pero raramente utilizadas son:

Hesiod.- Para los protocolos de la red Hesiod del Instituto Tecnológico de Massachusset (MIT).

CHAOS.- Para los protocolos de *CHAOSNET*.

"Un archivo de zona debe contener solamente RR's de la misma clase"²².

< tipo >

Existen una gran variedad de tipos de registros de origen, que como ya se había dicho, definen los diferentes tipos de información que puede dar un servidor de nombres acerca de una zona para la cual es autorizado. A continuación se describen los tipos de registros de origen de uso más común y un ejemplo de ellos.

²⁰ Referencia 9, página 4.

²¹ Referencia 9, página 4.

²² Referencia 9, página 5.

SOA ("Start Of Authority")

Este registro indica los datos de la autoridad para el dominio o zona en cuestión, por lo que cada dominio deberá incluir al menos un registro de este tipo en su archivo de configuración. Incluye información como el nombre de la zona, el correo electrónico del administrador responsable, la versión del archivo y el tiempo de vida de los registros.

```
<Nombre> <TTL> <Clase> SOA <Origen> <Persona> (
                                     <serial>
                                     <refresco>
                                     <reintento>
                                     <expiración>
                                     <mínimo>
                                     )
```

- Nombre** Es el nombre de la zona o dominio.
- Origen** Es el nombre del servidor de nombres primario para la zona.
- Persona** Es la dirección de correo electrónico del administrador responsable de la zona. Debido a que el carácter "@" es un carácter especial en los registros de origen, es sustituido por un punto "." .
- Serial** Es un número consecutivo que indica la versión del archivo de la zona. Cada vez que algún registro cambia, este número debe ser incrementado al menos en uno.
- Refresco** Indica cada cuantos segundos un servidor de nombres secundario tiene que ir a preguntar al primario si es necesaria una transferencia de zona debido a alguna actualización de algún registro. El servidor de nombres secundario toma el número serial que tiene en el archivo de una zona y lo compara con el que tiene el primario, si el serial ha incrementado en el servidor de nombres primario, indica que es necesaria la transferencia de zona. "Un buen valor aquí podría ser una hora (3600)"²³.
- Reintento** Es la cantidad de segundos que debe dejar pasar un servidor de nombres secundario, después de un intento fallido, para contactar al primario. "Un buen valor aquí podría ser 10 minutos (600)"²⁴.
- Expiración** Después de un intento del servidor secundario por contactar al

²³ Referencia 9, página 6.

²⁴ Referencia 9, página 6.

primario sin éxito, empieza a contar el tiempo de expiración. Este tiempo indica la cantidad de segundos que deberá dejar pasar el servidor secundario para dejar de tratar de contactar al primario. Después de transcurridos la cantidad de segundos especificados aquí, el servidor de nombres secundario ya no contestará de manera autoritativa o autorizada para la zona. El tiempo de expiración debe ser mucho mayor al tiempo de reintento.

Mínimo Es el tiempo mínimo que será asignado como "Tiempo de Vida" para los demás registros cuando no se les asigne uno en específico.

Ejemplo:

```
@      IN      SOA      dns1.unam.mx.  dns.unam.mx. (
                2000060801  ; Serial [yymddss]
                3600      ; Refresh [secs]
                1200      ; Retry [secs]
                604800    ; Expire [secs]
                86400 )   ; TTL [secs]
```

El carácter @ indica el nombre de dominio de la zona a la que pertenece el archivo de configuración y es válido en cualquier tipo de registro. Un punto y coma ";" indica el inicio de un comentario.

NS ("Name Server")

Este tipo de registro sirve para indicar el nombre de los servidores de nombres tanto primarios como secundarios para la zona. Su formato es:

<dominio>	<TTL>	<Clase>	NS	<Servidor>
------------------------	--------------------	----------------------	-----------	-------------------------

En el campo dominio se indica el nombre de la zona o dominio al cual pertenece el archivo de configuración y en el campo de servidor, el nombre de la máquina que proporcionará el servicio, es decir, el nombre del servidor de nombres de la zona.

Ejemplo:

```
nic.unam.mx.      IN      NS      dns1.unam.mx.
nic.unam.mx.      IN      NS      dns2.unam.mx.
nic.unam.mx.      IN      NS      dns3.unam.mx.
nic.unam.mx.      IN      NS      dns4.unam.mx.
```

A ("Address")

Es uno de los registros más importantes ya que sirven para apuntar el nombre de una máquina a su correspondiente dirección IP. Su formato es:

<nombre>	<TTL>	<Clase>	A	<Dirección IP>
-----------------------	--------------------	----------------------	----------	-----------------------------

En el campo de nombre, se especifica el nombre con el que se conocerá la máquina y en el campo de dirección su respectiva dirección IP.

Ejemplo:

deimos	IN	A	132.248.204.6
argos	IN	A	132.248.204.11

CNAME ("Canonical NAME")

Este tipo de registro es utilizado para declarar alias para el nombre que ya tiene una dirección IP. De esta manera se puede hacer referencia a una misma máquina a través de dos o más nombres diferentes. Su formato es:

<Alias>	<TTL>	<Clase>	CNAME	<Nombre>
----------------------	--------------------	----------------------	--------------	-----------------------

El campo alias corresponde al nombre adicional que se le dará a la máquina y el campo nombre corresponde al nombre que ya tiene asignado el equipo.

Ejemplo:

ftp	IN	CNAME	argos
www	IN	CNAME	argos

HINFO ("Host Info")

A través de este registro se puede declarar información acerca del hardware y software de una máquina. Su formato es:

<Nombre>	<TTL>	<Clase>	HINFO	<Hardware>	<Software>
-----------------------	--------------------	----------------------	--------------	-------------------------	-------------------------

En el primer campo se especifica el nombre del equipo en cuestión. Los dos últimos campos corresponden al hardware y software separados por un espacio en blanco.

Ejemplo:

deimos	IN	HINFO	Ultra10-Sun UNIX
argos	IN	HINFO	Sparc4-Sun UNIX

WKS ("Well Known Services")

Se utiliza para listar los servicios que proporciona una máquina en particular. "El registro WKS lista que servicios están disponibles en cierta dirección utilizando ciertos protocolos"²⁵. Su formato es:

<Nombre> <TTL> <Clase> WKS <Dirección><Protocolo><Servicios>

El primer campo corresponde al nombre del equipo que proporciona los servicios. En el campo de dirección se especifica la dirección IP, a continuación el protocolo bajo el cual corren los servicios, que puede ser TCP o UDP y por último se listan los servicios.

Ejemplo:

deimos	IN	WKS	132.248.204.6	TCP	telnet ftp smtp
--------	----	-----	---------------	-----	-----------------

MX ("Mail Exchanger")

Este es otro de los tipos de registro más común ya que define la manera en que se recibe el correo electrónico y el nombre de la máquina que lo atenderá. El formato de este registro es el siguiente:

<Nombre><TTL> <Clase> MX <Preferencia> <Servidor>
--

En el campo nombre se define el nombre con el que se recibirá el correo, es decir, es la parte de una dirección de correo electrónico que se encuentra a la

²⁵ Referencia 9, página 7.

derecha del carácter arroba "@". Por ejemplo, para las direcciones con el formato usuario@nic.unam.mx, el nombre del mail exchanger sería "nic.unam.mx". La preferencia se utiliza en caso de que se tengan declarados dos mail exchangers con el mismo nombre, en donde se tiene que especificar que máquina tiene mayor prioridad para atender ese correo. Entre menor sea el número que indique la preferencia mayor será su prioridad. En el último campo se escribe el nombre de la máquina que tendrá el servidor de correo que atenderá ese mail exchanger.

Ejemplo:

nic.unam.mx. IN MX 1 deimos.nic.unam.mx.

Los servidores de nombres reciben las solicitudes de información acerca de los registros de una zona en forma de peticiones ("**queries**").

Al recibir una petición, un servidor de nombres puede contestar de tres maneras:

- ♦ Responder en base a la información contenida en su base de datos, en caso de ser servidor de nombres autorizado para la zona consultada.
- ♦ Responder con la relación de quienes son los servidores de nombres autorizados para la zona consultada.
- ♦ Responder con mensajes de error en caso de que la información no exista.

Tanto las peticiones al servidor de nombres, como las respuestas que este genera, son transportadas en un mensaje formado de cinco secciones:

Encabezado (<i>Header</i>)
Pregunta (<i>Question</i>)
Respuesta (<i>Answer</i>)
Autoridad (<i>Authority</i>)
Adicional (<i>Additional</i>)

"El encabezado incluye campos que especifican cuales de las siguientes secciones están presentes y también especifica si el mensaje es una petición, o

una respuesta, o una petición estándar²⁶, etc. Esta sección es obligatoria para todos los mensajes.

La segunda sección, llamada "pregunta", contiene campos que describen la información que se quiere obtener de un servidor de nombres. Estos campos son: el tipo de registro (QTYPE), la clase (QCLASS) y el nombre de dominio (QNAME).

La siguiente sección contiene los registros de origen que directamente contestan la pregunta hecha al servidor de nombres.

En caso de que se haya preguntado a un servidor de nombres no autorizado para la zona de la cual se quiere obtener información, la siguiente sección contendrá los registros de origen que indican que servidores de nombres si son autorizados.

La última sección contiene registros de origen que pueden ser útiles a las demás secciones sin ser precisamente registros que correspondan a la respuesta buscada.

El Sistema de Nombres de Dominio maneja mensajes que son transportados tanto en forma de datagramas UDP como en conexiones TCP, ambos casos a través del puerto 53.

Los datagramas UDP son utilizados para las peticiones, mientras que las conexiones TCP son utilizadas para las transferencias de zona, las cuales necesitan estar libres de errores de transmisión para completarse.

3.4.3 El cliente o "resolver"

Dentro de la arquitectura cliente/servidor bajo la cual trabaja el Sistema de Nombres de Dominio, los "resolvers" son los programas que llevan a cabo la parte del cliente. "Los resolvers son programas que funcionan como interfase entre los programas de usuario y los servidores de nombres"²⁷. Los programas de usuario, tales como telnet, ftp, http y otros, hacen preguntas a los resolvers acerca de un nombre de dominio en forma de llamadas al sistema o subrutinas y este se encarga de obtener la respuesta con el servidor de nombres que tiene configurado.

Los resolvers son programas poco inteligentes, por lo que sus únicas funciones son:

- ♦ Hacer a los servidores de nombres la pregunta que le ha pasado algún programa de usuario.

²⁶ Referencia 7, página 25.

²⁷ Referencia 6, página 29.

- ♦ Interpretar las respuestas enviadas por el servidor de nombres. Estas respuestas pueden ser registros de origen o errores.
- ♦ Pasar la respuesta a los programas de usuario que solicitaron la información.

“Una muy importante meta del resolver es eliminar el retraso de red y la carga en los servidores de nombres originada por la mayoría de las preguntas contestándolas con su memoria caché de resultados previos”²⁸. El tiempo que los resolvers guardarán la información consultada en un servidor de nombres, será el tiempo de vida (TTL) especificado en cada registro de origen.

El proceso que se lleva a cabo al ir a consultar un servidor de nombres para obtener información acerca de un dominio se llama **“proceso de resolución de nombres”** o simplemente resolución.

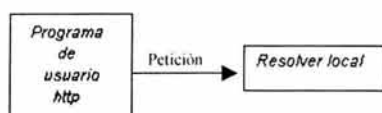
Cuando un programa de usuario necesita información de un nombre de dominio hace una consulta al resolver. El resolver revisa su memoria caché para ver si tiene información al respecto. En caso de no conocer nada del nombre de dominio va y hace una consulta al servidor de nombres que tiene configurado. El servidor de nombres busca en los archivos de su base de datos y en caso de no encontrar nada, debido a no ser autorizado para el nombre de dominio consultado, comienza una búsqueda por todo el espacio de nombres de dominio comenzando por los servidores de nombres de la zona raíz, hasta encontrar a los servidores de nombres autorizados del nombre de dominio y conseguir la información o bien un error. Una vez que el servidor de nombres que comenzó la búsqueda tiene la respuesta la regresa al resolver y este a su vez al programa de usuario que la solicitó.

Los servidores de nombres de la zona raíz son conocidos como **“Root Servers”** y contienen la información acerca de que servidores de nombres son autorizados para cada uno de los dominios de nivel superior. “Dada una consulta acerca de cualquier nombre de dominio, los root servers pueden al menos proveer los nombres y direcciones de los servidores de nombres que están autorizados para el dominio de nivel de superior en el que está el nombre de dominio”²⁹

Un ejemplo del proceso que se siguen para conocer la información acerca de un nombre de dominio podría ser un usuario que trate de acceder a la página www.nic.unam.mx desde una maquina en el dominio yahoo.com. El programa de usuario http le enviará una petición a su resolver local para saber cuál es la dirección IP de la máquina con el nombre www.nic.unam.mx.

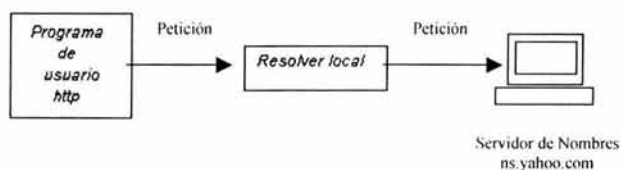
²⁸ Referencia 6, página 29.

²⁹ Referencia 1, página 27.



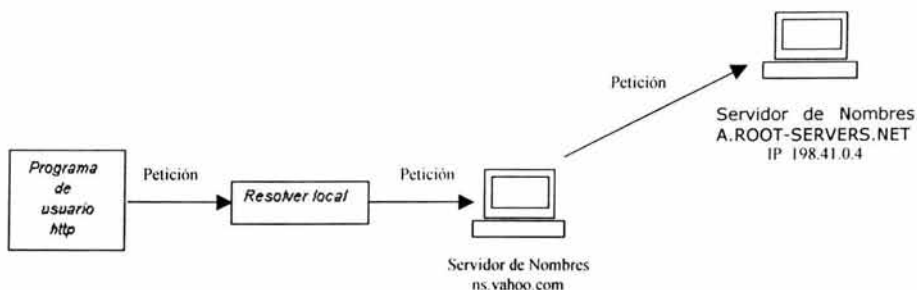
Petición = "¿Qué dirección IP tiene el nombre `www.nic.unam.mx` ?"

El resolver local interpretará la pregunta y la pasará al servidor de nombres que tenga configurado.

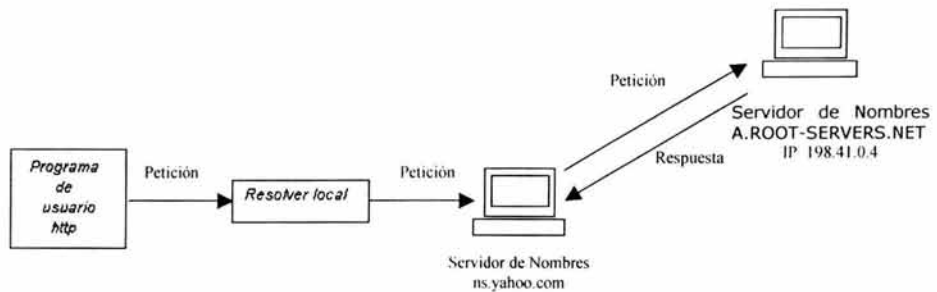


El servidor de nombres `ns.yahoo.com` buscará en su base de datos para ver si es autorizado para el nombre de dominio `www.nic.unam.mx`. Al no encontrar información entonces comenzará una búsqueda por el espacio de nombres de dominio para tratar de encontrar a los servidores de nombres autorizados para el nombre de dominio en cuestión.

La búsqueda comenzará enviando una petición a cualquiera de los servidores de nombres de la zona raíz.

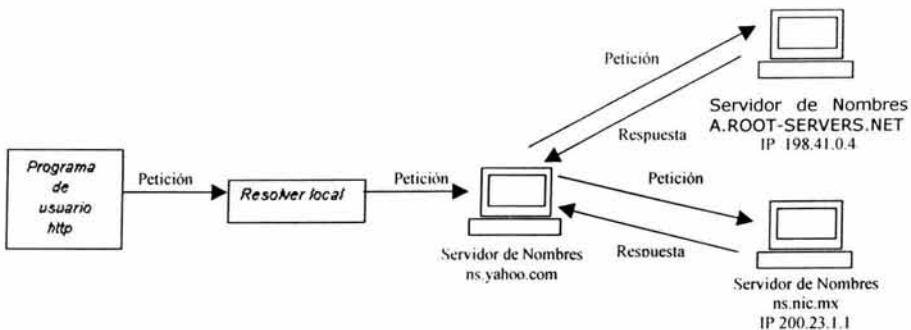


El servidor de nombres de la zona raíz recibe la petición, pero al no tener información autorizada del nombre de dominio `www.nic.unam.mx` le responde al servidor `ns.yahoo.com` con la mejor información que conoce al respecto. Los servidores de nombres de la zona raíz tienen la relación de los nombres y direcciones IP de cada uno de los dominios de nivel superior, por lo cual, `A.ROOT-SERVERS.NET` conoce el nombre y la dirección IP de los servidores de nombres autorizados para el dominio `mx`, y es esta la información que le regresa a `ns.yahoo.com`.



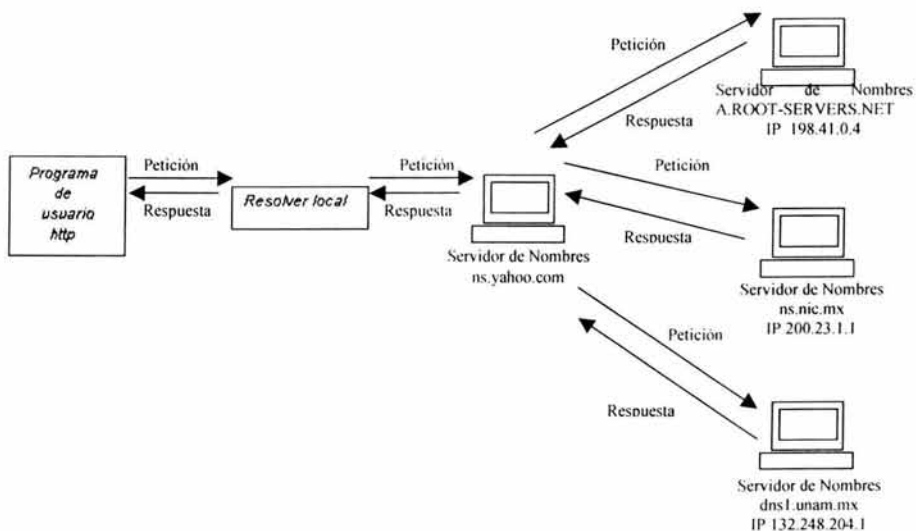
Respuesta de A.ROOT-SERVERS.NET = "Servidor autorizado para la zona mx es ns.nic.mx con dirección IP 200.23.1.1"

Una vez que el servidor de nombres `ns.yahoo.com` conoce quién es el servidor de nombres autorizado para la zona `mx`, le envía una petición acerca de la información que desea saber. El servidor de nombres `ns.nic.mx` no tiene información autorizada acerca del nombre de dominio `www.nic.unam.mx`, pero sí tiene la relación de quienes son los servidores de nombres autorizados para la zona `unam.mx`, por lo que le responde a `ns.yahoo.com` con el nombre y dirección IP correspondientes.



Respuesta de ns.nic.mx = "Servidor autorizados para la zona unam.mx es dns1.unam.mx con dirección IP 132.248.204.1"

Ahora que ns.yahoo.com conoce la dirección IP y nombre del servidor de nombres autorizado para la zona unam.mx, le envía la petición correspondiente para tratar de obtener la dirección IP de www.nic.unam.mx. Entonces el servidor de nombres de la zona unam.mx encuentra que es autorizado para el dominio nic.unam.mx y busca en su correspondiente archivo de configuración información acerca de algún registro www que indique su dirección IP. Al encontrar la información se la envía a ns.yahoo.com y este a su vez al resolver que le hizo la consulta. El resolver interpretará la respuesta y se la enviará al programa de usuario.



Respuesta de dns1.unam.mx = "www.nic.unam.mx apunta a la dirección IP 132.248.204.11"

Existen dos tipos de resolución: **recursiva** e **iterativa**.

La **resolución recursiva** consiste en ir a preguntar a los servidores de nombres que sean necesarios hasta encontrar la información autorizada que se está buscando o bien un error.

En la resolución recursiva "un resolver envía una petición recursiva a un servidor de nombres, de información acerca de un nombre de dominio en

particular. El servidor de nombres consultado es entonces obligado a responder con los datos solicitados o con un error indicando que el tipo de datos solicitado no existe o que el nombre de dominio especificado no existe³⁰.

En el ejemplo anterior, la resolución recursiva la llevó a cabo el servidor ns.yahoo.com al buscar la información solicitada por el resolver en el espacio de nombres de dominio.

Por otro lado, en una **resolución iterativa**, "un servidor de nombres simplemente da la mejor respuesta que conoce"³¹. En el ejemplo, las peticiones enviadas de ns.yahoo.com hacia los servidores A.ROOT-SERVERS.NET, ns.nic.mx y dns1.unam.mx fueron iterativas, por lo cual se limitaron a contestar con la mejor información al respecto que tenían en ese momento.

Una de las ventajas de la resolución iterativa es que permite que los servidores de nombres raíz se dediquen a contestar solamente con la información acerca de las nombres y direcciones IP de los servidores de nombres autorizados para cada uno de los dominios de nivel superior, evitando así que se saturen tratando de averiguar por su cuenta la información autorizada que les están solicitando otros servidores de nombres.

3.4.4 Ataques al DNS

Una vez explicado el funcionamiento del Sistema de Nombres de Dominio, veremos los diferentes tipos de ataques que se pueden llevar a cabo en contra de este servicio.

Existen dos razones por las que un servidor de nombres puede ser atacado exitosamente:

- ◆ **Por vulnerabilidades en el código de la implementación del DNS.**
- ◆ **Por configuración errónea.**

Por vulnerabilidades en el código de la implementación del DNS.

ATAQUE	CONSECUENCIA
Client flooding	Información falsa aceptada por el cliente.
DNS buffer overflow	Acceso al servidor con privilegios de root.
DNS caché poisoning	Envenenamiento del caché con información falsa.

³⁰ Referencia 1, página 29.

³¹ Referencia 1, página 30.

DNS spoofing attack	Suplantación de un servidor de nombres válido.
DoS attack	Negaciones de servicio.
Dynamic update vulnerabilities	Alteración de los registros DNS y acceso como root.

Por configuración errónea.

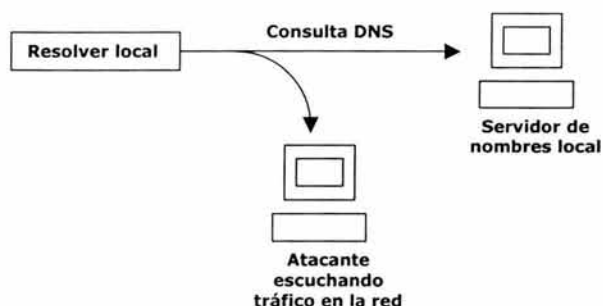
ATAQUE	CONSECUENCIA
Implementación y versión de servidor de nombres visible	Expone vulnerabilidades de la implementación.
Transferencias de zonas no autorizadas	Permite obtener la información de la red y los hosts que la componen.
Peticiones permitidas a todo mundo	Sobrecarga del DNS.
Correr BIND como usuario root	En caso de ser atacado con éxito el atacante obtiene privilegios de root.

A continuación se explica en que consiste cada uno de estos ataques.

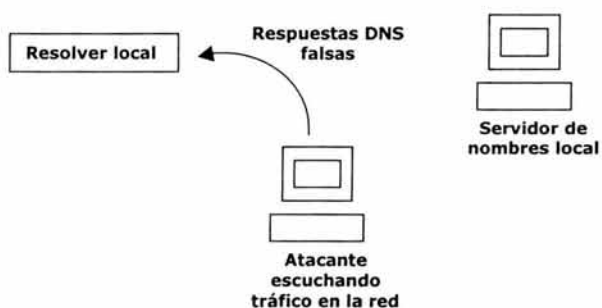
Inundación del cliente ("Client flooding").- En este ataque suponemos que el atacante es capaz de escuchar el tráfico de una red, por lo que sabe en que momento el cliente envía una consulta a algún servidor de nombres. La inundación del cliente ocurre cuando este envía una consulta a un servidor de nombres, pero recibe y acepta cientos de respuestas DNS del atacante. El éxito de este ataque se basa en la falta de autenticación de dichas respuestas. El ataque se realiza para aparentar que las respuestas son originarias del servidor de nombres esperado, pero sin una fuerte autenticación, el cliente no tiene la capacidad de verificar el origen de tales respuestas. Este ataque suele utilizarse en lugar de un DNS spoofing para lograr que un host suplante una aplicación y el cliente acceda a un servicio falso o bien para negarle el servicio.

El ataque se lleva a cabo de la siguiente manera:

1.- El cliente envía una consulta a un servidor de nombres. El atacante está escuchando el tráfico en la red del cliente e intercepta los paquetes de consulta del cliente hacia el DNS.



2.- El atacante suplanta al servidor de nombres tomando los identificadores válidos de las consultas DNS y regresa ciento de respuestas al cliente.



3.- El cliente acepta estos paquetes como válidos. Debido a la cantidad de paquetes recibidos y aceptados, el cliente se satura, ocasionando una negación de servicio para el cliente o bien, accede a servicios falsos controlados por el atacante.

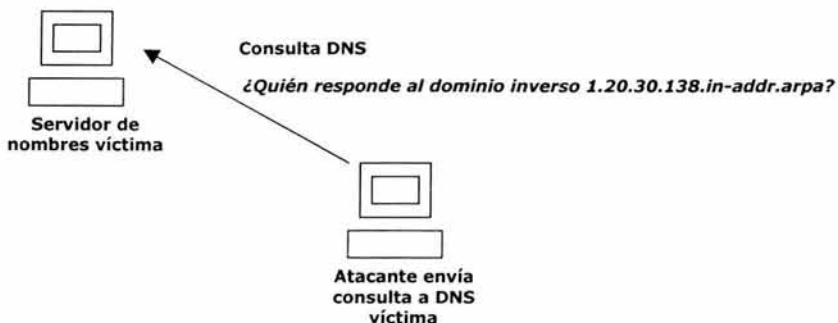
Sobrecarga de buffer del DNS ("DNS Buffer Overflow").- Los ataques buffer overflow no son exclusivos del DNS ya que existen muchos otros servicios que son vulnerables. Este tipo de ataque ocurre cuando un programa acepta más datos provenientes de un origen externo, de los que puede almacenar en la memoria que tiene asignada en el sistema. Los datos extra o sobrantes sobrecargan la memoria donde están almacenadas múltiples operaciones válidas que el sistema operativo debe llevar a cabo y por lo tanto las instrucciones que sobrescriban la memoria se ejecutan como válidas. Una vez que ocurre esto, el atacante puede lograr acceso como usuario privilegiado y tomar control no sólo del servicio DNS sino de todo el sistema.

Este tipo de ataque, es el más común para un DNS. La mayoría de las vulnerabilidades que se anuncian para DNS, realizan un buffer overflow en la implementación BIND, que es la más utilizada en Internet.

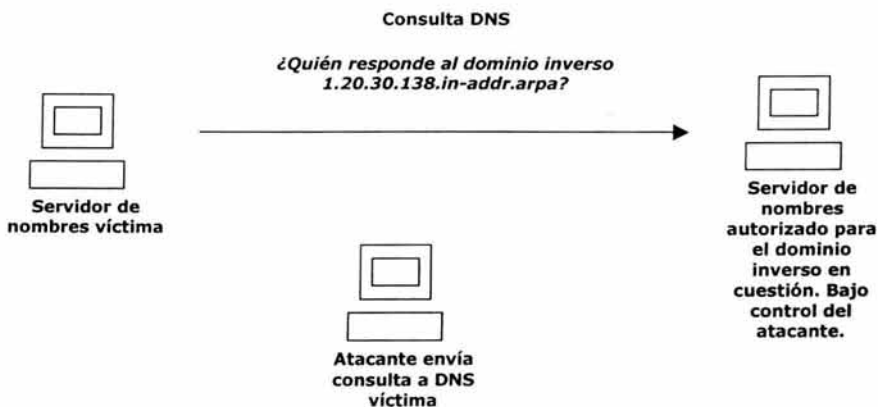
Envenenamiento de caché (“Cache poisoning”).- Se introduce falsa información en el caché de los servidores de nombres.

El ataque consiste en lo siguiente:

1.- El atacante envía consultas al servidor de nombres víctima pidiendo la resolución inversa de una dirección IP.



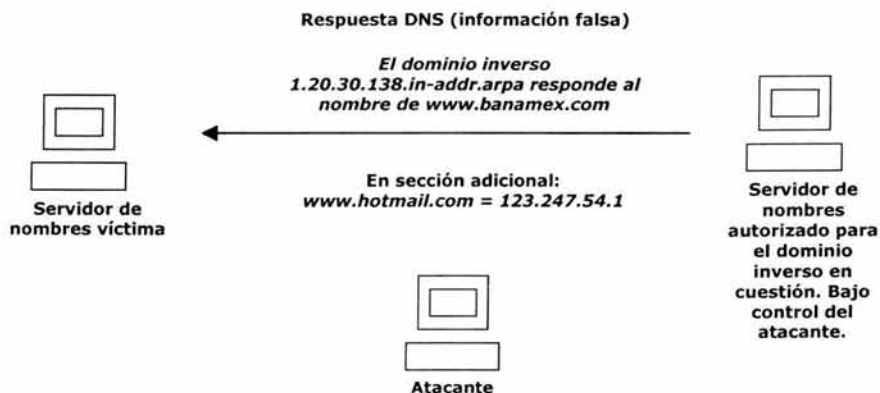
2.- El servidor de nombres víctima, que acepta resolución recursiva, busca el servidor autorizado para el dominio inverso en cuestión y le envía las peticiones correspondientes.



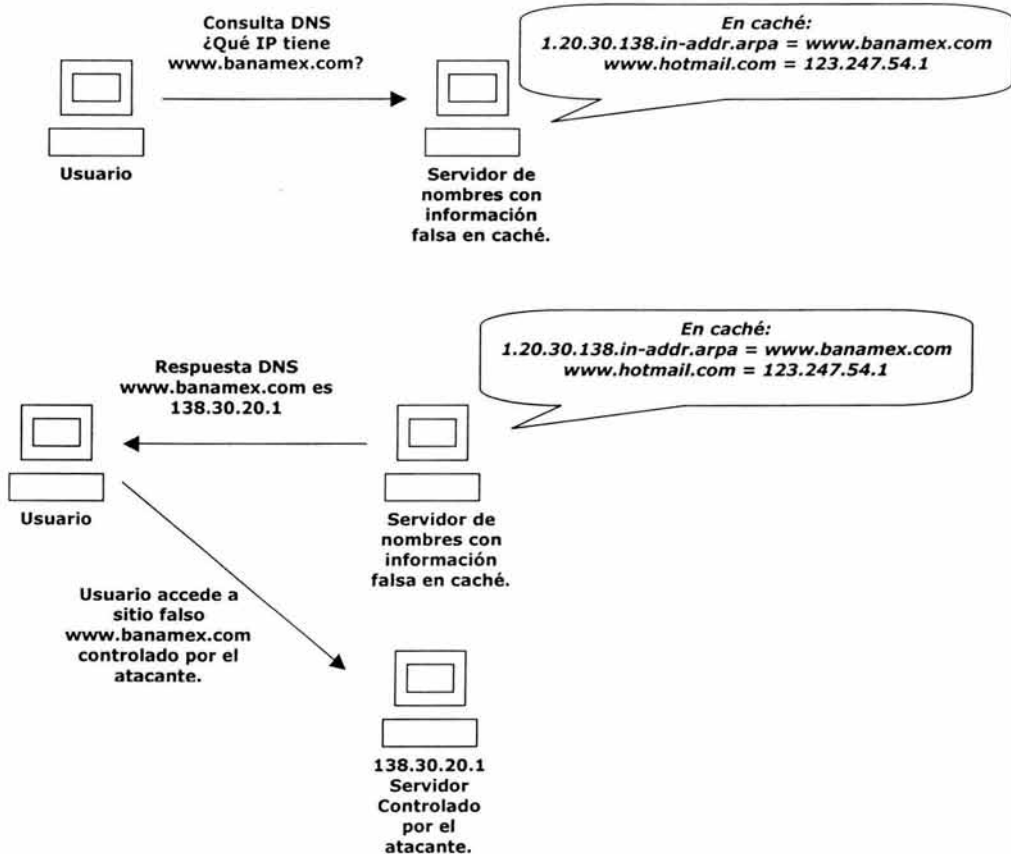
3.- El atacante tiene control total sobre el DNS autorizado para el dominio inverso en cuestión y manipula los paquetes que serán enviados al servidor de nombres víctima.



4.- Se envían los paquetes con información falsa hacia el servidor de nombres víctima. Este guardará en su caché la información falsa. Los paquetes DNS contienen una sección de información adicional, que el atacante puede aprovechar para agregar más información falsa que el DNS víctima aprenderá.



5.- Los resolvers que utilicen el DNS víctima como servidor de nombres, utilizarán sin saberlo, la falsa información que guardó en memoria caché.

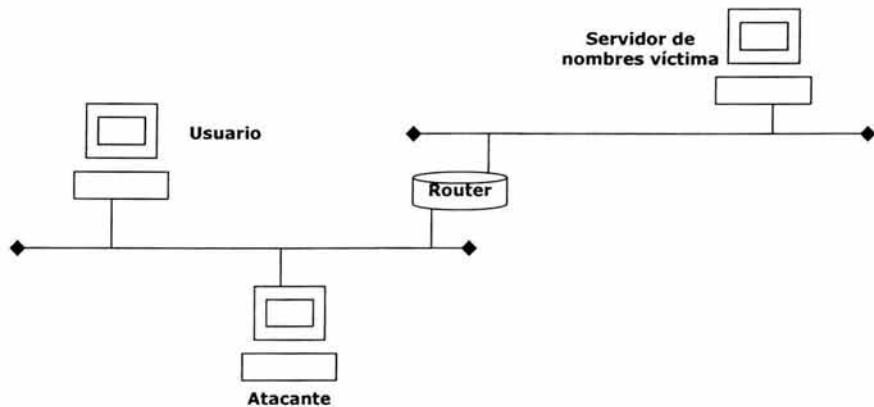


Un atacante que logra introducir información falsa en el caché de un servidor de nombres, puede suplantar páginas y servicios de Internet fácilmente. Por ejemplo, puede suplantar un sitio de correo gratuito y capturar todas las contraseñas de los usuarios que intenten entrar al servicio falso, o bien, número de cuentas bancarias con sus respectivas contraseñas que posteriormente puede utilizar para ingresar a los sitios reales. El atacante también puede ocasionar un Denial of Service Attack al direccionar el nombre de un sitio válido hacia una dirección IP inexistente.

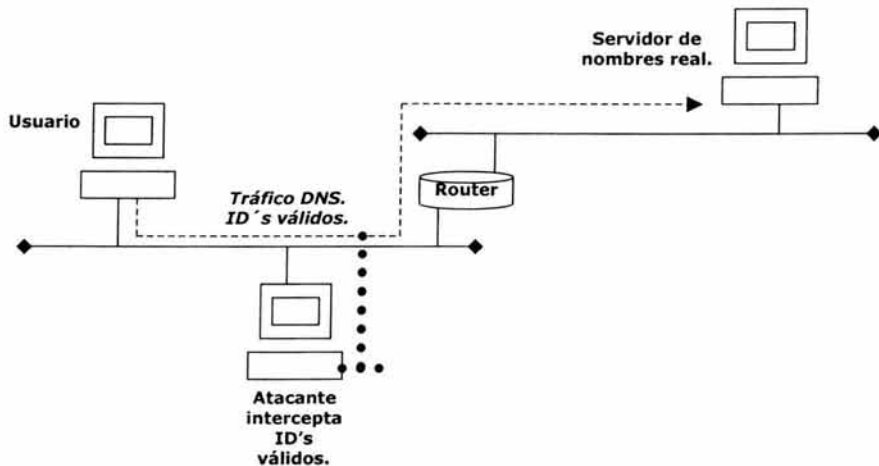
Suplantación de DNS ("DNS spoofing").- Se basa en el robo de ID de paquetes DNS autorizados para enviar información falsa como respuesta a un servidor de nombres. A diferencia del ataque por envenenamiento de caché, este ataque suplanta servidores de nombres válidos.

El ataque se lleva a cabo de la siguiente manera:

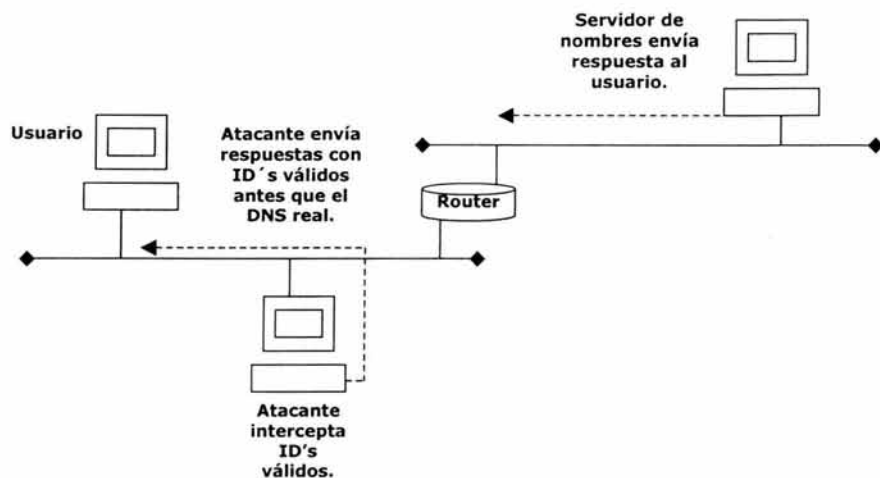
1.- La máquina del atacante debe estar en la misma red que el DNS víctima, para poder enviar las supuestas respuestas de manera más rápida que el DNS real.



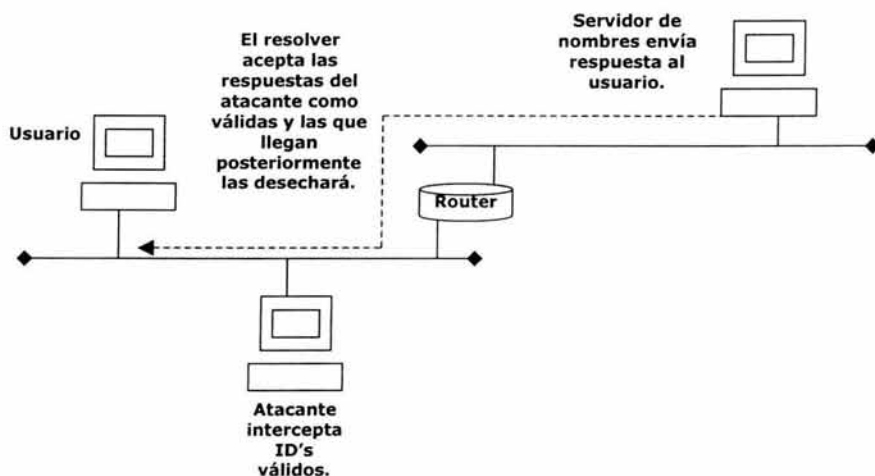
2.- El atacante captura el tráfico de red y se entera del ID de los paquetes DNS que el servidor de nombres atacado envía fuera de su red.



3.- El ID correcto es utilizado por el atacante para enviarle supuestas respuestas que la víctima tomará como válidas al reconocer el ID.



4.- Al llegar la respuesta de los DNS reales, la víctima los rechazará al tomarlos como paquetes duplicados.



La suplantación de servidores de nombres es otra manera para el atacante de manipular la información de DNS y desviar o bien negar los servicios de Internet a su conveniencia.

Negación de servicio DNS (“DNS Denial of Service” o “DNS DoS”).- Los ataques de negación de servicio utilizando las vulnerabilidades del Sistema de Nombres de Dominio, pueden llevarse a cabo de distintas maneras. Una de ellas es aprovechando las respuestas negativas que genera como respuesta un servidor de nombres, por ejemplo, si se envía una respuesta a una petición indicando que el nombre de dominio consultado no existe, resulta una negación de servicio para el cliente que desea consultar dicho nombre de dominio. Otra manera de negación de servicio se lleva a cabo si un servidor de nombres comprometido envía una respuesta que redirecciona al cliente a un servidor diferente, el cual no contiene el servicio deseado. Existe otro DoS asociado a los servidores de nombres e involucra también el envenenamiento de caché del DNS al insertar un registro CNAME que apunta a si mismo, por ejemplo:

```
tienda.org      IN      CNAME    tienda.org
```

Si un atacante logra insertar este registro en el caché del DNS víctima, puede provocar la caída del servidor de nombres con tan sólo solicitar una transferencia de zona para tienda.org. Esto debido a que el nombre de dominio con el registro CNAME está apuntando a si mismo, lo que ocasiona que el servidor de nombres entre en un ciclo de consultas infinito y se sature hasta agotar los recursos del servidor de nombres.

Ataque mediante actualizaciones dinámicas (“Dynamic update exploit”).- El DNS Dynamic Updates es una modificación al RFC 1035 que permite actualizaciones dinámicas de los registros contenidos en un DNS. La forma de restringir o permitir actualizaciones dinámicas en un DNS es en base a las direcciones IP desde las cuales se pretende hacer la modificación. Sin embargo, si un atacante logra suplantar una dirección IP permitida, el atacante puede realizar las modificaciones sobre los registros que desee. De esta manera, un atacante puede crear, eliminar y modificar registros dentro del dominio comprometido.

Otra manera de explotar esta vulnerabilidad, es enviando una gran cantidad de paquetes similares. Después de varios paquetes de dynamic update recibidos en el host víctima, se producirá un *Segmentation Fault*, lo que llevará a un ataque de negación de servicio.

Versión de BIND visible.- A través de herramientas de consulta de servidores de nombres, tales como nslookup o dig, es posible obtener la versión de BIND que se está utilizando. Esto puede considerarse peligroso para la seguridad de toda nuestra red, ya que al exponer esta información estamos prácticamente ayudando a un atacante a encontrar fácilmente las vulnerabilidades a las que está expuesto nuestro servidor de nombres.

Para conocer la versión de un servidor de nombres:

```
% nslookup -query=txt -class=chaos version.bind [IP del NS]
```

o bien

```
% dig [@servidor] txt chaos version.bind
```

Ejemplo:

```
% nslookup -query=txt -class=chaos version.bind 132.245.5.6
Server: ns.midominio.mx
Address: 132.245.5.6
```

```
VERSION.BIND text = "8.2.2-P7"
```

Esto no es propiamente un ataque, sino una falla que permite dar información acerca de nuestro servidor de nombres, y el dar este tipo de información puede resultar riesgoso. En el ejemplo anterior, saber que se está trabajando con la versión 8.2.2-P7, es información valiosa para un atacante, ya que solamente tiene que averiguar las vulnerabilidades de esta versión para poder planear un ataque.

Transferencias de zonas no autorizadas.- De acuerdo a lo que se describió previamente en este capítulo, una transferencia de zona es el proceso de copiar el archivo de configuración de una zona desde un servidor de nombres primario a uno secundario. A través de una transferencia de zona, un servidor de nombres obtiene toda la información referente a un dominio. Este proceso debería ser permitido únicamente para los servidores de nombres secundarios autorizados del dominio en cuestión. Sin embargo, una configuración errónea en el servidor de nombres puede permitir a cualquier servidor de nombres impostor realizar una transferencia de toda una zona o dominio.

Una transferencia de zona no autorizada resulta peligrosa ya que, como en el caso anterior (revelación de la versión de BIND), estamos regalando información acerca de nuestra red. Por lo regular, en todas las organizaciones se nombran a los servidores de acuerdo a las aplicaciones y servicios que contienen, por ejemplo, al servidor de web se le asigna el nombre `www.midominio.com` y al servidor de bases de datos es común que se le dé nombres como `db.midominio.com` u `oracle.midominio.com`. Al obtener la base de datos de un dominio, podemos conocer todos los nombres que están asignados a los diferentes servidores que tenemos en nuestra organización, y con esto es fácilmente reconocer qué servicios corren en qué máquinas. Es este caso también estamos facilitando el trabajo del atacante, ya que sólo le resta elegir los servidores que tienen aplicaciones con vulnerabilidades conocidas y enfocarse en tratar de explotar dichas fallas. Las transferencias de zona también pueden realizarse con `nslookup` o `dig`, mediante el comando "`ls -t any zona o dominio`".

Por ejemplo,

```
xcaret[marie]% nslookup
Default Server: dns.semarnat.gob.mx
Address: 10.1.1.25
```

```
> ls -t any semarnat.gob.mx
```

```
[dns.semarnat.gob.mx]
$ORIGIN semarnat.gob.mx.
@ 1H IN SOA dns.semarnat.gob.mx root.semarnat.gob.mx (
    2003063000; serial
    1H ; refresh
    1H ; retry
    1W ; expiry
    1H ) ; minimum

    1H IN NS telecom.semarnat.gob.mx.
    1H IN MX 5 telecom.semarnat.gob.mx.
telecom 1H IN A 10.1.2.34
oracle 1H IN A 10.1.2.37
routercisco 1H IN A 10.1.1.1
proxysj 1H IN A 10.1.1.4
www 1H IN CNAME oracle
```

Es este ejemplo, solo se muestran unos cuantos nombres de aplicaciones, pero suficientes para saber que en el servidor 10.1.2.37 corre un servidor de web y un servidor de oracle, que la máquina con ip 10.1.1.4 tiene un proxy, que la ip 10.1.1.1 se trata de un ruteador cisco, y que el servidor telecom con ip 10.1.2.34 es el servidor de correo de la institución además de ser el servidor de nombres. Con esta información, un atacante puede concentrarse en ahora buscar una vulnerabilidad del servidor de correo o de nombres del dominio semarnat.gob.mx y si logra explotarla, puede tener acceso a este servidor, que por lo que se ve, se trata de un servidor de misión crítica. En caso de un ataque de negación de servicio contra el servidor telecom, se dejaría sin servicio de nombres a la institución y sin servicio de correo, con lo que prácticamente se deja fuera de Internet a toda la organización.

Peticiones (“queries”) permitidas a todo mundo.- De acuerdo con lo que se explicó previamente en este capítulo, existen dos tipos de resolución de nombres: resolución recursiva y resolución iterativa. Un servidor de nombres sólo debe de permitir resolución recursiva para aquellos clientes dentro de su red ó grupo de subredes de la organización. Esto con el fin de entregarles la información solicitada o bien el error correspondiente. Para todos los demás clientes externos, sólo debe de permitir resolución iterativa, es decir, entregar sólo la mejor respuesta que conozca y no gastar recursos en ir a buscar la información solicitada en todo el espacio de nombres de dominio, o bien, restringir completamente cualquier consulta que provenga del exterior. Si un servidor de nombres acepta peticiones de cualquier cliente, esto se puede

convertir en un serio hueco de seguridad, y un atacante puede aprovecharlo para saturar los recursos del DNS con consultas innecesarias.

Correr BIND como usuario root.- Correr una aplicación o servicio, bajo los privilegios del superusuario, resulta riesgoso para cualquier sistema. Este no es un caso exclusivamente de un servidor de nombres, sino de cualquier otro servicio que corra bajo el sistema operativo UNIX, por ejemplo, sendmail. Si un atacante logra con éxito aprovechar la vulnerabilidad del servicio, y toma el control de este, también puede tomar el control de todo el servidor, ya que estaría adoptando los privilegios de root con los que corre el servicio.

3.4.5 Implementaciones del DNS

BIND (Berkeley Internet Name Domain) es una implementación de los protocolos que conforman el Sistema de Nombres de Dominio y fue programado originalmente en la Universidad de California en Berkeley. A partir de la versión 4.9.3 es mantenido y distribuido por el ISC (Internet Software Consortium). Las versiones 4.X han sido sustituidas por las versiones 8.X, debido a numerosos problemas de seguridad encontrados. Actualmente las versiones 8.X se consideran las más estables, a pesar de que también se les han encontrado numerosos huecos de seguridad. Existe ya una versión 9.X que ya ha sido liberada pero que aún se encuentra en etapa de prueba, por lo que su uso no es muy común.

Existe otra implementación de Sistema de Nombres de Dominio para plataformas windows, conocida como **DNS de Microsoft**. Esta implementación es utilizada comúnmente donde se utilizan redes windows y no existen servidores UNIX donde se pueda instalar BIND. Las versiones de esta implementación también tienen huecos de seguridad que han sido utilizados incluso para llevar a cabo ataques exitosos al sitio oficial de la empresa Microsoft.

DJBDNS es otra implementación del Sistema de Nombres de Dominio que prácticamente es desconocida. Sin embargo, de acuerdo a la página web de donde se puede obtener la distribución ([http:// www.djbdns.org](http://www.djbdns.org)), DJBDNS es un excelente reemplazo de BIND, basado en un modelo de operación seguro y rápido. En esta misma página se puede encontrar un apartado donde se ofrecen \$500 dólares a la persona que encuentre un hueco de seguridad en este software, como garantía de que la distribución es totalmente confiable.

3.4.6 Configuración de un DNS

La configuración de un servidor de nombres, varía dependiendo de la implementación sobre la que se esté trabajando. Sin embargo, para este trabajo nos basaremos en la configuración específica de BIND en sus versiones 8.X.

3.4.6.1 Configuración básica

La configuración básica de un servidor de nombres en BIND, consiste en la creación de los siguientes archivos:

- ◆ **Archivo de configuración named.conf.**
- ◆ **Archivos de la base de datos.**

3.4.6.1.1 Archivo de configuración named.conf

El archivo named.conf es el archivo que va a contener la configuración principal del servidor de nombres. En este archivo se especifican varios parámetros bajo los cuáles va a correr el servidor de nombres y los dominios para los cuáles va a ser autorizado. A continuación se presenta un ejemplo de la configuración básica de este archivo:

```
# SERVIDOR PRIMARIO

options {
    directory "/etc/named";
};

zone "." {
    type hint;
    file "root.cache";
};

zone "127.in-addr.arpa" {
    type master;
    file "named.127";
};

zone "semarnap.gob.mx" {
    type master;
    file "named.semarnap.gob.mx";
};
```

En este ejemplo, podemos ver la configuración necesaria para crear un servidor de nombres primario para el dominio semarnap.gob.mx. En el primer párrafo hay una sección llamada "options" en donde podemos cambiar los parámetros bajo los cuales trabajará nuestro dns, por ejemplo, la ruta del directorio en donde se encontrarán los archivos de configuración de cada zona, a qué direcciones IP's o redes se les va a dar autorización para hacer transferencias de zona o consultas directamente a nuestro servidor, sobre qué puerto TCP va a correr el DNS, etc. En este ejemplo, solamente le estamos especificando en qué directorio deberá buscar los archivos de configuración de cada dominio para el cual será autorizado (/etc/named).

Después de la sección de opciones se especifican los dominios para los cuales nuestro servidor de nombres será autorizado. Cada uno de los dominios se da de alta con un párrafo que comienza con la palabra "zone" seguido del nombre absoluto (FQDN) del dominio:

```
zone "semarnap.gob.mx" {
    type master;
    file "named.semarnap.gob.mx";
};
```

Mediante estas líneas estamos dando de alta el dominio "semarnap.gob.mx", para el cual seremos servidor de nombres primario ("master") y cuyo archivo de configuración se llamará "named.semarnap.gob.mx".

En caso de que seamos servidor de nombres secundario para un dominio, las líneas de configuración varían un poco y quedarían como sigue:

```
zone "ine.gob.mx" {
    type slave;
    file "named.ine.gob.mx";
    masters {
        10.65.1.45;
    };
};
```

En este caso estamos especificando que somos servidor de nombres secundario ("slave") para el dominio ine.gob.mx y que su archivo de configuración se llamará named.ine.gob.mx. Éste último archivo no lo tendremos que crear nosotros, sino que el propio servidor de nombres tendrá que obtenerlo vía una "transferencia de zona" del servidor de nombres primario correspondiente. Para esto, tenemos que especificarle en la opción "masters" la dirección IP del servidor de nombres primario autorizado del dominio en cuestión.

Un servidor de nombres puede ser al mismo tiempo, primario para uno o más dominios y secundario para otros.

Las zonas "." y "127.in-addr.arpa" son zonas especiales que deben configurarse en todo servidor de nombres.

Durante el proceso de resolución de nombres, se consulta el archivo named.conf para determinar para qué dominios nuestro servidor de nombres es autorizado. Cuando se realiza una consulta para un dominio que no se encuentra en nuestra base de datos, debe darse una referencia de en qué otros servidores de nombres podemos encontrar la respuesta. Esta es la función de la zona ".", ya que en esta zona especificamos los nombres y las direcciones de los servidores de nombres raíz (root servers) a los cuales se deberá consultar para completar el proceso de resolución. El archivo

correspondiente a esta zona se puede obtener vía FTP del sitio FTP.RS.INTERNIC.NET y deberá colocarse también en el directorio de la base de datos de nuestro servidor sin olvidar nombrarlo tal y como lo especificamos en la declaración de la zona “.”.

La zona "127.in-addr.arpa" sirve para resolver la dirección ip 127.0.0.1, la cual es utilizada por todas las redes y por todos los hosts para direccionar tráfico a ellos mismos. La dirección 127.0.0.1 se conoce como dirección de loopback.

3.4.6.1.2 Archivos de la base de datos

Los archivos de configuración van a contener los registros de origen (“Resource Records” o “RR’s”) para cada dominio y el nombre de estos archivos deberá ser el establecido en el archivo named.conf para cada dominio. Por ejemplo, si en el named.conf tenemos la siguiente configuración:

```
zone "semarnap.gob.mx" {
    type master;
    file "named.semarnap.gob.mx";
};
```

entonces el nombre del archivo de la base de datos correspondiente al dominio semarnap.gob.mx deberá ser named.semarnap.gob.mx y deberá estar ubicado en el directorio establecido mediante la sentencia “directory” del named.conf.

El archivo de configuración de un dominio deberá contener al menos el registro SOA y un registro NS. Por lo que un ejemplo para el dominio semarnap.gob.mx puede ser:

```

; RR SOA Start of Authority
;-----
;
@ IN SOA telecom.semarnap.gob.mx. root.semarnap.gob.mx. (
                                2002092400 ; numero de serie
                                3600 ; refresh
                                3600 ; retry
                                604800 ; expire
                                3600 ) ; TTL
; RR NS Name Servers
;-----
;
IN NS telecom.semarnat.gob.mx.
```

En estos archivos todos los comentarios se marcan con un punto y coma (;) al principio.

Con el archivo `named.conf` y el archivo `named.semarnap.gob.mx` mostrados, nuestro servidor de nombres ya debe de responder como servidor primario del dominio `semarnap.gob.mx`. Posteriormente podemos dar de alta los registros necesarios para nuestro dominio, debajo del registro SOA y del o los registros NS.

Los archivos de las zonas `."` y `"127.in-addr.arpa."` también deben incluirse en la base de datos de nuestro servidor.

A continuación se presenta un ejemplo de un archivo que contiene el listado de servidores de nombres raíz a consultar, es decir, el formato de un archivo de configuración para la zona `."`.

```

;   This file holds the information on root name servers needed to
;   initialize cache of Internet domain name servers
;   (e.g. reference this file in the "cache . <file>"
;   configuration file of BIND domain name servers).
;
;   This file is made available by InterNIC registration services
;   under anonymous FTP as
;   file           /domain/named.root
;   on server      FTP.RS.INTERNIC.NET
;   last update:   Aug 22, 1997
;   related version of root zone: 1997082200
;
;
; formerly NS.INTERNIC.NET
;
.           3600000 IN NS   A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000  A   198.41.0.4
;
; formerly NS1.ISI.EDU
;
.           3600000   NS   B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000  A   128.9.0.107
;
; formerly C.PSI.NET
;
.           3600000   NS   C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000  A   192.33.4.12
;
; formerly TERP.UMD.EDU
;
.           3600000   NS   D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000  A   128.8.10.90
;
; formerly NS.NASA.GOV
;

```

```

.           3600000   NS   E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000   A   192.203.230.10
;
; formerly NS.ISC.ORG
;
.           3600000   NS   F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET. 3600000   A   192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.           3600000   NS   G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET. 3600000   A   192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.           3600000   NS   H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET. 3600000   A   128.63.2.53
;
; formerly NIC.NORDU.NET
;
.           3600000   NS   I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET. 3600000   A   192.36.148.17
;
; temporarily housed at NSI (InterNIC)
;
.           3600000   NS   J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET. 3600000   A   198.41.0.10
;
; housed in LINX, operated by RIPE NCC
;
.           3600000   NS   K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET. 3600000   A   193.0.14.129
;
; temporarily housed at ISI (IANA)
;
.           3600000   NS   L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET. 3600000   A   198.32.64.12
;
; housed in Japan, operated by WIDE
;
.           3600000   NS   M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET. 3600000   A   202.12.27.33
; End of File

```

La zona "127.in-addr.arpa" también debe seguir el formato que se utiliza para cualquier otra zona. A continuación se presenta un ejemplo:

```

;
; RR SOA Start Of Authority
;-----
;
@ IN SOA telecom.semarnap.gob.mx. root.semarnap.gob.mx.
(
                2000062700      ; serial number
                7200           ; refresh
                3600           ; retry
                6044800        ; expire
                86400 )        ; TTL
;
; RR NS Name Servers
;-----
;
IN NS telecom.semarnap.gob.mx.
;
; RR A Address-to Name Mapping
;-----
;
1 IN PTR localhost

```

Como se puede observar, en este archivo existe un solo registro además del SOA y del NS. Este registro es de tipo PTR y será el que resuelva la dirección 127.0.0.1 apuntando al nombre "localhost".

3.4.6.2 Configuración avanzada

Como podemos ver, configurar un servidor de nombres no es un proceso complicado, pero es precisamente por la relativa facilidad con la que se echa a andar un DNS, que los administradores no le dedican tiempo y esfuerzo a las cuestiones de seguridad que pueden afectar el servicio. Una vez funcionando el servidor, se olvidan incluso de darle mantenimiento, provocando que un descuido en la configuración pueda ser aprovechado para llevar a cabo un ataque de seguridad exitoso.

A continuación se presentan aspectos de configuración avanzada en BIND que pueden ayudarnos en la seguridad de nuestro servidor de nombres.

3.4.6.2.1 Listas de direcciones y listas de control de acceso ("Address Match Lists y ACL's")

Las "Address Match Lists" y las listas de control de acceso ("Access Control List") son utilizadas en la configuración de ciertas características del DNS.

Las **Address Match Lists** son listas de términos que especifican una o más direcciones IP. Los elementos en esta lista pueden ser:

- ◆ Direcciones IP individuales.
- ◆ Prefijos de direcciones IP.

Configuración:

Red / bits de la máscara

Ejemplo: 15/8 (Red 15.0.0.0 con máscara 255.0.0.0)

Una **lista de control de acceso** debe de estar previamente declarada con una sentencia "acl", la cual tiene la siguiente estructura:

Configuración:

```
acl "nombre" {
    {address_match list; } ;
};
```

Ejemplo:

```
acl "RED-INTERNA" {
    {132.245/24; } ;
};
```

A cada lista de acceso se le asocia un nombre para identificar a todos los elementos que contiene.

Existen cuatro listas de control de acceso predefinidas:

None	Ninguna dirección IP.
Any	Todas las direcciones IP.
Localhost	Cualquiera de las direcciones IP del host local.
Localnets	Cualquiera de las redes en las que el host local tiene una interface de red.

3.4.6.2 Notificación DNS ("DNS Notify")

La notificación DNS ("DNS Notify") es la facilidad que permite a los servidores de nombres primarios avisar a sus secundarios cuando ha ocurrido una modificación en los registros de origen de sus zonas.

Una **petición de notificación** ("Notify Request"), es la notificación enviada por el servidor de nombres primario hacia el secundario cuando ha ocurrido un cambio en alguna zona. Una **respuesta a notificación** ("Notify Response") es

la respuesta que envía el servidor de nombres secundario hacia el primario una vez que ha recibido una petición de notificación.

El servidor de nombres secundario procede tal y como si el tiempo de refresco hubiera expirado: le pide al servidor de nombres primario el registro SOA de la zona para comparar los números seriales, y si el del servidor primario es mayor se realiza la transferencia de zona.

La razón de la verificación del SOA es evitar un "Denial of Service Attack" hacia el servidor de nombres primario.

BIND Versión 4 y algunas otras implementaciones como el DNS Server de Microsoft's Windows NT, no soportan DNS Notify, por lo que al recibir una petición NOTIFY responderán con el error NOTIMP ("Not Implemented").

En BIND 8 la notificación DNS está habilitado por omisión, pero se puede deshabilitar.

Configuración global para desactivar la notificación DNS:

```
options {
    notify no;
};
```

Para una zona en particular:

```
zone "midominio.mx" {
    type master;
    file "db.midominio.mx";
    notify no;
};
```

Para crear una lista de servidores de nombres a los que se les debe enviar una petición de notificación además de aquellos especificados en los registros NS:

```
zone "red.midominio.mx" {
    type master;
    file "db.red.midominio.mx";
    notify yes;
    also-notify { 132.245.10.8 }
};
```

3.4.6.2.3 Actualización dinámica de DNS (“DNS Dynamic Update”)

La actualización dinámica de DNS (“DNS Dynamic Update”) es una facilidad que permite agregar o eliminar registros de origen a una zona existente para la cual nuestro servidor de nombres está autorizado.

La actualización dinámica permite:

- ◆ Agregar o eliminar registros de origen.
- ◆ Eliminar RRsets (grupos de registros de origen con el mismo nombre de dominio, clase y tipo).
- ◆ Eliminar todos los registros asociados con un nombre dado.

La sintaxis para realizar una actualización dinámica es:

```
% update delete nombre_de_dominio [type] [rdata]
```

Elimina el nombre de dominio especificado o, si se especifica el tipo, elimina el RRset especificado o, si se especifica el rdata, elimina el registro que coincida con el nombre de dominio, tipo y rdata.

```
% update add nombre_de_dominio ttl [clase] type rdata
```

Agrega el registro especificado para la zona. El ttl debe ser incluido además del tipo y del campo rdata, pero la clase es opcional y toma por omisión el valor IN.

Ejemplo 1:

```
% nsupdate
> update add www.midominio.com 333 in a 192.168.1.5
>
```

Ejemplo 2:

```
% nsupdate
> update add midominio.com. in mx 10 mail.midominio.com.
> update add midominio.com. in mx 15 mail2.midominio.com.
>
```

Por omisión, BIND 8 no permite las actualizaciones dinámicas.

Para poder utilizar las actualizaciones dinámicas se debe agregar la sentencia allow-update en la declaración de la zona en la que se desea habilitar.


```
zone "midominio.com" {
    type master;
    file "db.midominio.com";
    allow-update { 192.168.1.5}
};
```

3.4.6.2.4 Transferencias de zonas

BIND permite configurar varios parámetros que nos van a permitir controlar las transferencias de zonas que son realizadas hacia nuestro servidor de nombres.

Para limitar el número de transferencias de zona iniciadas por un servidor de nombres externo, se puede configurar el parámetro "transfers-per-ns" de la siguiente manera:

Globalmente:

```
options {
    transfers-per-ns 2;
};
```

Por Servidor:

```
server 192.167.1.6 {
    transfers 2;
}
```

Por omisión, el número de transferencias simultáneas que permite un servidor de nombres es de 2 por cada servidor externo.

Si existen varios servidores de nombres secundarios que pueden iniciar una transferencia de zona en nuestro servidor primario, podemos limitar el número total de transferencias iniciadas, con el fin de evitar que se consuman los recursos de nuestro servidor atendiendo dichas transferencias.

```
options {
    transfers-in 10;
};
```

Asimismo, podemos limitar la duración de una transferencia de zona configurando el parámetro "max-transfer-time-in", tal y como se muestra a continuación:

Globalmente:

```
options {  
    max-transfer-time-in 180;  
};
```

Por zona:

```
options {  
    max-transfer-time-in 60;  
};  
  
zone "midominio.com" {  
    type master;  
    file "db.midominio.com";  
    max-transfer-time-in 180  
};
```

Una transferencia de zona está compuesta de varios mensajes DNS enviados sobre una conexión TCP. Cada mensaje contiene un solo registro.

BIND 8 puede manejar un formato para la transferencias de zonas llamado "many-answers", en el cual se colocan tantos registros de origen como sea posible en cada mensaje DNS.

El resultado es que las transferencias de zona consuman menos ancho de banda y menos tiempo CPU, lo que las hace más eficientes.

La configuración del parámetro "many-answers" es el siguiente:

Globalmente:

```
options {  
    transfer-format many-answers;  
};
```

Por servidor:

```
server 192.168.1.4 {  
    transfer-format one-answer;  
};
```

3.4.6.2.5 Recursos limitados

Si en la máquina que contiene el servidor de nombres, corren otras aplicaciones, o bien, sabemos de antemano que no dispone de muchos recursos, podemos configurar el DNS de tal manera que limitemos esos recursos que utilizará para poder funcionar.

A continuación se listan los recursos que pueden limitarse, así como la configuración necesaria para limitarlos :

El límite del tamaño del segmento de datos que utilizará el DNS,

```
options {
    datasize size;
};
```

dónde "size" es un valor entero en bytes.

El límite del tamaño del stack o pila de memoria a utilizar por el DNS,

```
options {
    stacksize size;
};
```

Las opciones `datasize` y `stacksize` sólo pueden utilizarse si el sistema operativo lo permite.

El límite del tamaño de los archivos core que se generen en caso de error o falla del servicio,

```
options {
    coresize size;
};
```

El límite de archivos que el DNS puede tener abiertos,

```
options {
    files number;
};
```

Se debe de tener cuidado en no limitar demasiado los recursos para nuestro servidor de nombres, ya que podemos provocar una percepción de bajo rendimiento del servicio ante los usuarios. Como pocos son los usuarios que

saben de la existencia de los servidores de nombres, pueden asumir que la lentitud del servicio es el acceso a Internet.

3.4.6.2.6 Intervalos de mantenimiento

En BIND se cuenta con tres características configurables que pueden tomarse como propias del DNS, ya que las utiliza para el mantenimiento del servidor de nombres. Estas características son:

Cleaning Interval

Este intervalo se refiere a cada cuantos minutos, el servidor de nombres vaciará la información acerca de los nombres de dominio consultados y aprendidos que ha almacenado en memoria caché. Esta opción se configura de la siguiente manera:

```
options {
    cleaning-interval 120;
};
```

Hay que considerar que el proceso de vaciado de la memoria caché utiliza tiempo CPU y en servidores lentos o muy saturados no se recomienda que se realice cada hora. Para desactivar este proceso se puede establecer un valor de 0.

Interface Interval

Por omisión, BIND está disponible a través de todas las interfaces de red de una computadora. BIND es un software lo suficientemente inteligente como para darse cuenta cuando una tarjeta de red en el servidor donde está corriendo, se cae o se levanta. Para hacer esto, verifica el estado de las tarjetas de red del servidor cada 60 minutos. Sin embargo, esta verificación se puede deshabilitar mediante la siguiente configuración:

```
options {
    interface-interval 0;
};
```

Al deshabilitar la opción de verificar el estado de las interfaces del servidor se reduce trabajo innecesario que lleva a cabo el DNS.

Statistics Interval

Este intervalo se refiere a cada cuantos minutos el servidor de nombres vaciará las estadísticas del servicio a los archivos destinados para este fin. Se configura de la siguiente manera.

```
options {
    statistics-interval 60;
};
```

Para desactivar la generación del archivo de estadísticas se establece un valor de 0 para este intervalo.

3.4.6.2.7 Servidores de nombres promotores ("Forwarders")

La finalidad de los servidores de nombres promotores ("forwarders") es retener en memoria caché el mayor número de peticiones y sus respectivas respuestas hechas hacia afuera de la red.

El modo de operación de un servidor de nombres primario o secundario al utilizar un servidor promotor es el siguiente:

1.- Si la información solicitada por el resolver se encuentra en la base de datos de información autorizada o en caché, se le contesta con esta información.

2.- Si la información no se encuentra, el servidor de nombres enviará la petición al servidor promotor y esperará un período de tiempo pequeño por la respuesta antes de contactar el mismo a los servidores de nombres externos.

Las peticiones hechas a un servidor de nombres promotor son recursivas. La manera de declarar en el archivo de configuración de un servidor de nombres, la dirección o direcciones IP de los servidores que fungirán como promotores, es la siguiente:

```
options {
    forwarders { 192.168.1.8; 192.168.1.9; };
};
```

3.4.6.2.8 Servidores de nombres no recursivos

En algunas ocasiones, no se desea que los servidores de nombres formen una base de datos de información no autorizada.

Este es el caso de los servidores de nombres raíz, que están tan ocupados que no deben gastar tiempo ni recursos tratando de contestar las peticiones recursivas que reciban.

La característica en los servidores de nombres de almacenar una base de datos de información no autorizada se conoce como "fetch-glue" y para deshabilitarla se debe realizar la siguiente configuración:

```
options {
    recursion no;
    fetch-glue no;
};
```

Si se tiene un servidor de nombres no recursivo no debe listarse en el archivo resolv.conf de alguna máquina con UNIX, ni utilizarse como servidor de nombres promotor, ya que de lo contrario, la o las máquinas que utilicen este servidor como servidor de nombres, no podrán encontrar ningún nombre de dominio ajeno a los que tenga declarado como autorizados.

3.4.6.2.9 Servidores de nombres delegados ("Name servers delegated")

Podemos decir que los servidores de nombres delegados ("Name servers delegated") son autorizados para nuestras zonas pero responden las peticiones que reciben de otros servidores de nombres de Internet de manera no recursiva. De esta manera, sólo pueden dar información que tengan en su base de datos, es decir, únicamente darán información acerca de los dominios para los que es o está autorizado.

Las medidas de seguridad que se recomiendan para un servidor de nombres delegado son:

- 1.- Asegurarse de que no reciba peticiones recursivas (no deben ser utilizados como servidores promotores ni tampoco debe haber ningún resolver utilizándolos)
- 2.- Desactivar la recursión. Esto elimina un rango grande de probabilidades de ataque. El ataque de tipo spoofing más común es inducir a un servidor de nombres a hacer peticiones hacia servidores de nombres controlados por el atacante.
- 3.- Restringir las transferencias de zona.
- 4.- Desactivar el "glue fetching".

3.4.6.2.10 Servidores de nombres que resuelven ("Name servers resolving")

Los servidores de nombres "resolving" son los que están configurados para responder de manera recursiva a resolvers o para servir como promotores, por lo que no pueden rechazar peticiones recursivas.

No se les puede aplicar las mismas medidas de seguridad que a los servidores delegados, pero sí podemos restringir las peticiones que reciban para que

respondan sólo los que provengan de nuestros resolvers. Esta restricción se configura de la siguiente manera:

```
options {
    allow-query {132.248/16: };
};
```

3.4.6.3 Medidas de seguridad en un DNS

3.4.6.3.1 Ocultar versión de BIND

El tener instalada y corriendo la última versión de BIND es una forma de proteger nuestros servidores de nombres en contra de los ataques y vulnerabilidades conocidos. No obstante, algunas personas dedicadas a la administración de DNS opinan que ésta es una medida de *seguridad por oscuridad* (Security by obscurity), pero lo cierto es que si un atacante conoce la versión de nuestro servidor de nombres y conoce las vulnerabilidades de dicha versión, puede fácilmente aprovecharlas para atacar nuestro sistema.

La última versión de BIND de la serie 8.X es la 8.4.4, liberada en enero del 2004 y la última versión de BIND de la serie 9.X es la 9.2.3 liberada en octubre del 2003.

Para conocer la versión de un servidor de nombres:

```
% nslookup -query=txt -class=chaos version.bind [IP del NS]
```

o bien

```
% dig [@servidor] txt chaos version.bind
```

Ejemplo:

```
% nslookup -query=txt -class=chaos version.bind 132.245.5.6
```

```
Server: ns.midominio.mx
```

```
Address: 132.245.5.6
```

```
VERSION.BIND text = "8.2.2-P7"
```

Para evitar dar a conocer la versión que corre nuestro BIND, debemos configurar la siguiente opción en el archivo `named.conf` del servidor de nombres:

```
options {
    version "Go away!";
};
```

en donde "Go away" puede ser cualquier texto de nuestra elección.

3.4.6.3.2 Restricción de peticiones

BIND 8 permite crear listas de direcciones IP, las cuales hemos explicado previamente y podemos utilizar para restringir las peticiones hechas a nuestro servidor de nombres. Estas listas puede aplicar a una zona en particular o bien a todas las zonas declaradas en el `named.conf`.

Para restringir todas las peticiones:

```
options {
    allow-query { adres_match_list; };
};
```

Ejemplo:

```
options {
    allow-query { 192.168.5/24; 132.246.3/24; };
};
```

Para restringir las peticiones para una zona en particular:

```
zone "midominio.com" {
    type slave;
    file "midominio.com";
    masters { 192.168.1.5; };
    allow-query {"RED-UNAM"; };
};
```

3.4.6.3.3 Restricción de transferencias de zonas

Por cuestiones de seguridad que también hemos explicado en la sección de ataques al DNS, debemos asegurarnos que los servidores que estén realizando transferencias de nuestras zonas sean realmente nuestros servidores secundarios.

Si algún usuario hace una petición a nuestro servidor, está solicitando información sobre algo que ya conoce, por ejemplo, está solicitando la dirección IP de un nombre de dominio que le interese. Pero si el usuario puede hacer una transferencia de zona completa, está obteniendo toda la información de una zona, con lo cual probablemente se este enterando de qué servicios tenemos en nuestra red y exactamente en qué direcciones IP.

La sentencia `allow-transfer` de BIND 8 permite aplicar listas de acceso a las transferencias de zona. `allow-transfer` se puede declarar en la sección de opciones de nuestro `named.conf` o bien en la declaración de alguna zona en particular.

En el servidor primario:

```
zone "unam.mx" {
    type master;
    file "named.unam.mx";
    allow-transfer {132.241.101.2; 132.241.6.25 };
};
```

En el servidor secundario:

```
zone "unam.mx" {
    type slave;
    file "named.unam.mx";
    master { 132.241.2.12; };
    allow-transfer {none; };
};
```

De forma global:

```
options {
    allow-transfer { 132.248/24; };
};
```

3.4.6.3.4 Correr BIND como usuario no-root o no privilegiado.

Normalmente el demonio named, que es el proceso que debe de estar permanentemente activo en un servidor UNIX para que funcione nuestro DNS, es ejecutado por el usuario root. Pero esto puede representar un peligro para nuestro sistema, ya que si un hacker encuentra alguna vulnerabilidad en el servidor de nombres a través de la cual pueda escribir o leer archivos en el sistema, podría tener acceso al sistema de archivos como usuario root.

A partir de BIND 8.1.2 se incluyen nuevas opciones que permiten cambiar el usuario y grupo bajo el cual corre el demonio named. De esta manera, el demonio named se ejecuta con los permisos mínimos necesarios para poder funcionar sin necesidad de hacerlo como root. Si alguien llegara a entrar al sistema mediante el servidor de nombres al menos no tendrá privilegios de superusuario.

También se incluye una opción, conocida como "DNS enjaulado" que permite cambiar el directorio raíz del servidor de nombres, de tal manera que el directorio root del servidor de nombres sea desde su punto de vista algún subdirectorio del sistema de archivos. Si algún atacante entra al sistema quedará encerrado en este directorio junto con el servidor de nombres.

Estas opciones se especifican en la línea de comandos:

-u cambia el usuario

Ej. % named -u bin

-g cambia el grupo

Ej. % named -g other

-t cambia el directorio raíz del servidor de nombres.

Ej. % named -t /export/home/named

Se recomienda crear un usuario y un grupo especial para correr el servidor de nombres, por ejemplo, named.

Debe tomarse en cuenta que al cambiar el usuario y grupo del servidor de nombres se deben cambiar también el usuario y grupo de los archivos de la base de datos y de los archivos de bitácoras en caso de utilizarse.

Además se debe poner el archivo named.pid en algún directorio con permisos de escritura para el usuario y grupos especificados:

```
options {
    pid-file "/var/named/named.pid";
};
```

Si se opta por cambiar el directorio raíz del servidor de nombres debemos asegurarnos de incluir todos los archivos que el named utiliza y tomar en cuenta que nuestro servidor no podrá enviar mensajes al *syslog* de nuestro sistema.

Al cambiar el directorio raíz se debe verificar que en el nuevo directorio se incluirán los siguientes archivos para el correcto funcionamiento del DNS:

- ◆ named-xfer
- ◆ librerías
- ◆ /dev/null

3.4.6.3.5 Dos servidores de nombres. ("Split function name servers.")

¿Que pasa si sólo tenemos un servidor de nombres para anunciar nuestras zonas y para atender a nuestros resolvers y no podemos afrontar el gasto de comprar otro servidor?.

Existen dos soluciones para este caso:

1) Configurar el mismo servidor de nombres para responder a servidores externos anunciando nuestras zonas y al mismo tiempo responder a los resolvers de nuestra red permitiéndoles peticiones recursivas. Esto no evita que los servidores de nombres externos nos envíen peticiones recursivas, pero nuestro servidor de nombres no las responderá por no provenir de resolvers de nuestra red.

La configuración necesaria para esta opción es la siguiente:

```
options {
    allow-query { 132.248/16; };
};

zone "unam.mx" {
    type master;
    file "named.unam.mx";
    allow-query { any; };
    allow-transfer { 132.248.10.2; 132.248.64.250; };
};

zone "248.132.in-addr.arpa" {
    type master;
    file "named.132.248";
    allow-query { any; };
    allow-transfer { 132.248.10.2; 132.248.64.250; };
};
```

2) Correr dos procesos named en el mismo host. Uno de estos procesos será configurado como "delegated" y el otro como "resolving".

Dado que no tenemos forma de configurar los servidores remotos y resolvers para que consulten nuestros servidores de nombres en puertos diferentes, debemos configurar ambos named en el puerto 53 (el puerto por omisión de named) pero en direcciones IP diferentes.

Se pueden tener dos tarjetas de red en nuestro host y configurarle una dirección IP a cada una de estas interfaces. Si no se cuenta con una segunda tarjeta de red se pueden configurar alias de IP o IP's virtuales sobre la única tarjeta que tengamos (si el sistema operativo lo permite).

Si no se cuenta con un sistema operativo que permita crear IP's virtuales, todavía tenemos una última opción utilizando la dirección de loopback (127.0.0.1) como segunda dirección IP. Al configurar un servidor de nombres sobre la dirección de loopback solo el resolver de nuestro host local podrá enviarle peticiones.

La configuración para el servidor "delegated" es la siguiente:

```
options {
    directory "/usr/local/named";
    recursion no;
    listen-on { 132.248.204.2; };
    pid-file "delegated.pid";
};

zone "unam.mx" {
    type master;
    file "named.unam.mx";
    allow-query { any; };
    allow-transfer { 132.248.10.2; 132.248.64.250; };
};

zone "248.132.in-addr.arpa" {
    type master;
    file "named.132.248";
    allow-query { any; };
    allow-transfer { 132.248.10.2; 132.248.64.250; };
};

zone "." {
    type hint;
    file "db.cache";
};
```

La configuración para el servidor "delegating" es:

```
options {
    directory "/usr/local/named1";
    listen-on { 127.0.0.1; };
    pid-file "resolving.pid";
};

zone "." {
    type hint;
    file "db.cache";
};
```

La sentencia listen-on también nos sirve para especificar o modificar el puerto por el que correrá nuestro servidor de nombres:

```
options {
    listen-on port <n> { address_match_list };
};
```

Para poder utilizar el servidor "resolving" que esta corriendo en la dirección de loopback también debemos darlo de alta en nuestro resolv.conf

```
nameserver 127.0.0.1
```

3.4.6.3.6 Aplicar parches de BIND

BIND es una implementación de DNS al que constantemente se le van encontrando vulnerabilidades en el código que son aprovechadas por los hackers. Es importante tener actualizada la versión de BIND que se está utilizando para disminuir la probabilidad de un ataque exitoso derivado de la explotación de una vulnerabilidad conocida. El sitio oficial de dónde se pueden obtener los parches y últimas versiones oficiales de BIND es <http://www.isc.org>

3.4.6.3.7 Aplicar parches de sistema operativo.

Prácticamente todos los días aparecen anuncios de nuevas vulnerabilidades en los diferentes sistemas operativos que existen, por lo que es importante para un administrador de DNS tener actualizados los parches del sistema operativo donde tenga instalado su servidor de nombres, ya que no tiene caso preocuparse solamente por los parches de la implementación si la seguridad del sistema operativo está descuidada. En los sitios oficiales de cada sistema operativo se pueden encontrar los parches necesarios.

3.4.7 Criptografía en el DNS

Tal y como ya se había mencionado anteriormente, la Internet no fue diseñada para ser una red segura. Los medios de transmisión y los protocolos de comunicación que utiliza hacen posible que se pueda conocer la información que se está transmitiendo, mediante programas conocidos como *sniffers*. Este método de interceptación de información es muy utilizado actualmente por los hackers para intervenir diversos servicios, entre ellos, el DNS.

La criptografía, "es el estudio de técnicas matemáticas relacionadas a aspectos de seguridad de la información, tales como confidencialidad, integridad de datos, autenticación de entidad y autenticación de origen de datos"³². La criptografía aplica diversas técnicas matemáticas para cifrar información basándose en un secreto conocido como "llave", de tal manera que la información sólo pueda conocerse si se conoce dicho secreto.

Los servicios que proporciona la criptografía son:

³² Referencia 4, página 4.

Cifrado.- Es la transformación de datos legibles a una forma ilegible, con el fin de garantizar su confidencialidad.

Descifrado.- Transforma los datos ilegibles a su forma original.

Autenticación.- Asegurar que una persona, proceso, computadora, sistema o hardware sea quien dice ser.

Firmas digitales.- Una firma digital es el equivalente a una firma autógrafa.

De acuerdo al número de llaves que se utilizan para cifrar la información, podemos clasificar los sistemas criptográficos en tres tipos:

Criptografía simétrica.- También conocida como criptografía convencional, clásica o de llave secreta. Utiliza una misma llave para cifrar y para descifrar.

Criptografía asimétrica.- También conocida como criptografía de llave pública. Utiliza una llave para cifrar y una distinta para descifrar.

Funciones hash.- No utilizan ninguna llave. Una función hash "es una función matemática que acepta como entrada un conjunto de datos y genera como salida un resultado de longitud fija"³³

Actualmente existen dos protocolos basados en criptografía cuyo objetivo es agregar seguridad al DNS: **DNSSEC** y **TSIG**.

Ambos protocolos proveen autenticación del origen de los datos y verificación de la integridad para el DNS, lo cual se lleva a cabo mediante firmas digitales. La diferencia entre estos protocolos es el tipo de criptografía que utilizan para crear las firmas, ya que DNSSEC utiliza criptografía de llave pública, mientras que TSIG utiliza criptografía de llave secreta.

3.4.7.1 DNSSEC

Este protocolo se describe en el RFC 2535. **DNSSEC** provee tres servicios distintos:

- ♦ Autenticación del origen de los datos e integridad de los datos.
- ♦ Distribución de llaves.
- ♦ Seguridad de transacciones.

DNSSEC no provee confidencialidad de las peticiones o respuestas del DNS, ya que este servicio se deja a otros protocolos de seguridad como *IPSEC*.

³³ Referencia 10, página 10.

Autenticación del origen de datos e integridad de los datos

La autenticidad se provee por firmas digitales generadas criptográficamente y que son asociadas a grupos de RR's.

Distribución de llaves

Se define un nuevo registro llamado "KEY" destinado a asociar llaves a nombres de dominio. Esto permite utilizar el DNS como un mecanismo de distribución de llaves públicas para el DNS mismo y para otros protocolos.

Seguridad de transacciones

Asegura a un resolver que al menos está obteniendo respuestas del servidor que pretende y que la respuesta corresponde a la petición enviada.

La manera en que trabaja DNSSEC es la siguiente:

- ◆ Cada zona tiene su propia llave pública y privada.
- ◆ La llave privada es utilizada para firmar grupos de registros en la zona, es decir, conjuntos de registros con el mismo dueño, clase y tipo.
- ◆ La firma digital para los grupos de registros se añade a la zona en forma de un nuevo registro llamado "SIG".
- ◆ La llave pública de la zona se almacena en otro registro conocido como registro "KEY".

Para verificar las firmas digitales del DNS:

Un servidor de nombres o resolver que solicita un registro en una zona firmada, obtendrá una respuesta que incluye el registro SIG que corresponde a los registros consultados.

El servidor de nombres o resolver puede entonces obtener el registro KEY de la zona y verificarlo.

Una vez que el servidor de nombres o resolver ha verificado el registro KEY, puede descifrar la firma digital en el registro SIG para obtener un valor hash, recalcularlo y compararlos.

Con esta verificación se prueba que los registros que se obtuvieron realmente provienen de la zona correcta y que los datos no han sido modificados desde que fueron firmados.

Ataques contra los que protege DNSSEC:

- ◆ Intercepción y/o modificación de paquetes
- ◆ Caché poisoning

Este protocolo involucra cifrado asimétrico, es decir, utiliza dos llaves diferentes para cifrar y para descifrar, lo que lo hace computacionalmente caro ya que se requiere de más recursos para realizar su función. También se requiere de espacio en el DNS para almacenar las llaves y la certificación por parte de la zona padre dentro del espacio de nombres de dominio.

3.4.7.2 TSIG (“Transaction Signatures”)

TSIG está definido mediante el *Internet Draft* “draft-ietf-dnsbind-tsig-11.txt” y es un mecanismo para agregar seguridad al Sistema de Nombres de Dominio mediante la autenticación de mensajes DNS, particularmente las transferencias de zona y actualizaciones automáticas. Proporciona servicios de autenticación e integridad.

TSIG se vale de funciones hash y llaves para firmar:

- ◆ Consultas
- ◆ Respuestas
- ◆ Transferencias de zona
- ◆ Actualizaciones dinámicas

TSIG funciona a través de un registro que nunca aparece en los archivos de la base de datos del DNS. Esta llave debe de ser conocida por el servidor y el DNS o resolver con el cual va a intercambiar transacciones.

En comparación con DNSSEC, este protocolo sólo requiere de una función hash, lo que representa un ahorro de recursos para el proceso de firmado de zonas.

3.5 TENDENCIAS

A continuación se presentan los resultados de algunos censos relacionados con el Sistema de Nombres de Dominio, realizados por NIC-México y por el ISC. Algunos de estos datos cambian constantemente, por lo que se trata de presentar la información más reciente al momento de la investigación.

Cantidad de nombres de dominio registrados bajo .mx (3 de junio de 2004)

.com.mx	80,261
.gob.mx	2,213
.net.mx	539
.edu.mx	2,298
.org.mx	3,227
.mx	172
TOTAL	88,710

Total mensual de nombres de dominio registrados bajo .mx

FECHA	.COM.MX	.GOB.MX	.NET.MX	.EDU.MX	.ORG.MX	.MX	TOTAL
31-May-2004	80,149	2,207	541	2,294	3,236	172	88,599
30-Abr-2004	79,367	2,184	537	2,254	3,214	172	87,728
31-Mar-2004	78,513	2,162	542	2,217	3,196	172	86,802
29-Feb-2004	77,090	2,123	549	2,161	3,156	172	85,251
31-Ene-2004	76,049	2,101	550	2,137	3,149	172	84,158
31-Dic-2003	74,885	2,074	557	2,114	3,148	172	82,950
30-Nov-2003	74,653	2,062	564	2,082	3,176	172	82,709
31-Oct-2003	74,073	2,015	570	2,047	3,185	172	82,062
30-Sep-2003	71,480	1,957	573	2,002	3,176	172	79,360
31-Ago-2003	70,644	1,936	584	1,966	3,171	172	78,473
31-Jul-2003	69,834	1,899	588	1,939	3,176	172	77,608
30-Jun-2003	70,525	1,875	595	1,904	3,183	172	78,254
31-May-2003	70,443	1,845	603	1,857	3,195	172	78,115
30-Abr-2003	69,075	1,800	603	1,825	3,129	172	76,604
31-Mar-2003	68,602	1,761	607	1,798	3,111	172	76,051
28-Feb-2003	68,471	1,724	615	1,762	3,144	172	75,888
31-Ene-2003	67,706	1,709	620	1,722	3,111	172	75,040
31-Dic-2002	66,545	1,687	621	1,692	3,085	172	73,802

30-Nov-2002	66,657	1,666	630	1,660	3,109	172	73,894
31-Oct-2002	66,301	1,642	634	1,627	3,125	177	73,506
30-Sep-2002	65,479	1,611	628	1,578	3,070	177	72,543
31-Ago-2002	65,217	1,576	639	1,528	3,034	177	72,171
31-Jul-2002	64,752	1,540	643	1,509	2,969	177	71,590
30-Jun-2002	64,374	1,517	649	1,474	2,949	177	71,140
31-May-2002	64,143	1,488	646	1,435	2,952	177	70,841
30-Abr-2002	63,715	1,456	651	1,400	2,931	177	70,330
31-Mar-2002	63,418	1,418	653	1,361	2,905	177	69,932
28-Feb-2002	63,431	1,392	657	1,324	2,871	177	69,852
31-Ene-2002	62,626	1,367	656	1,280	2,799	177	68,905
31-Dic-2001	61,496	1,278	662	1,245	2,759	177	67,617
30-Nov-2001	62,041	1,250	673	1,224	2,772	177	68,137
31-Oct-2001	63,445	1,224	699	1,197	2,842	177	69,584
30-Sep-2001	65,244	1,192	744	1,154	2,939	177	71,450
31-Ago-2001	70,227	1,169	818	1,113	3,162	177	76,666
31-Jul-2001	69,274	1,142	815	1,069	3,107	177	75,584
30-Jun-2001	67,515	1,111	810	1,043	2,995	177	73,651
31-May-2001	65,625	1,082	805	1,010	2,909	177	71,608
30-Abr-2001	63,322	1,047	789	967	2,774	177	69,076
31-Mar-2001	62,509	1,022	791	945	2,726	177	68,170
28-Feb-2001	60,523	990	783	914	2,627	177	66,014
31-Ene-2001	58,830	965	782	885	2,524	177	64,163
31-Dic-2000	56,769	935	761	855	2,399	177	61,896
30-Nov-2000	55,118	919	754	836	2,337	177	60,141
31-Oct-2000	53,138	889	749	808	2,238	177	57,999
30-Sep-2000	50,723	864	743	780	2,136	177	55,423
31-Ago-2000	48,394	848	730	748	2,045	177	52,942
31-Jul-2000	45,560	832	720	720	1,938	177	49,947

30-Jun-2000	42,987	802	716	696	1,827	177	47,205
31-May-2000	40,250	582	709	678	1,732	177	44,128
30-Abr-2000	37,272	560	702	654	1,594	177	40,959
31-Mar-2000	34,446	547	695	636	1,480	177	37,981
29-Feb-2000	30,843	529	687	603	1,370	177	34,209
31-Ene-2000	27,520	523	662	584	1,282	177	30,748
31-Dic-1999	25,026	510	639	557	1,221	177	28,130
30-Nov-1999	23,692	492	634	544	1,179	177	26,718
31-Oct-1999	21,608	475	596	530	1,093	177	24,479
30-Sep-1999	21,059	459	575	512	1,072	177	23,854
31-Ago-1999	19,411	447	544	494	1,009	177	22,082
31-Jul-1999	17,522	424	515	482	948	177	20,068
30-Jun-1999	16,698	404	511	471	940	177	19,201
31-May-1999	15,421	392	498	449	851	177	17,788
30-Abr-1999	14,332	383	477	433	799	178	16,602
31-Mar-1999	13,379	377	458	423	753	187	15,577
28-Feb-1999	12,312	367	440	398	695	189	14,401
31-Ene-1999	11,356	358	421	377	654	189	13,355
31-Dic-1998	10,661	350	395	359	622	189	12,576
30-Nov-1998	10,505	346	398	344	615	189	12,397
31-Oct-1998	9,964	336	384	333	589	189	11,795
30-Sep-1998	9,135	322	355	301	557	189	10,859
31-Ago-1998	8,634	302	332	293	511	189	10,261
31-Jul-1998	7,976	290	306	277	487	189	9,525
30-Jun-1998	7,428	284	296	254	469	189	8,920
31-May-1998	7,082	262	272	243	448	189	8,496
30-Abr-1998	6,574	247	246	226	417	188	7,898
31-Mar-1998	5,972	230	222	211	360	188	7,183
28-Feb-1998	6,837	218	285	195	429	188	8,152

31-Ene-1998	6,402	212	272	180	408	188	7,662
31-Dic-1997	6,043	201	262	168	389	188	7,251
30-Nov-1997	5,736	179	254	160	367	188	6,884
31-Oct-1997	5,428	160	240	147	343	186	6,504
30-Sep-1997	5,028	151	234	126	322	191	6,052
31-Ago-1997	4,730	143	225	108	298	191	5,695
31-Jul-1997	4,374	137	216	97	283	197	5,304
30-Jun-1997	4,025	128	208	83	269	198	4,911
31-May-1997	3,680	121	198	73	245	198	4,515
30-Abr-1997	3,341	109	187	55	224	197	4,113
31-Mar-1997	3,085	100	178	39	207	195	3,804
28-Feb-1997	2,832	85	166	32	174	193	3,482
31-Ene-1997	2,556	81	154	19	164	188	3,162
31-Dic-1996	2,286	75	143	13	142	179	2,838
30-Nov-1996	2,005	68	129	6	134	176	2,518
31-Oct-1996	1,703	63	125	1	123	173	2,188
30-Sep-1996	1,412	48	114	0	104	162	1,840
31-Ago-1996	1,181	43	95	0	84	156	1,559
31-Jul-1996	996	37	84	0	69	144	1,330
30-Jun-1996	722	30	66	0	45	137	1,000
31-May-1996	593	27	56	0	36	129	841
30-Abr-1996	460	23	49	0	29	122	683
31-Mar-1996	372	18	39	0	23	115	567
29-Feb-1996	288	16	33	0	17	112	466
31-Ene-1996	234	13	29	0	16	104	396
31-Dic-1995	180	12	20	0	13	101	326
30-Nov-1995	153	11	16	0	9	99	288
31-Oct-1995	116	9	14	0	5	93	237
10-Oct-1995	100	9	14	0	5	83	211

31-Jul-1994	5	1	0	0	0	44	50
30-Jun-1994	5	0	0	0	0	40	45
05-Abr-1992	1	0	0	0	0	?	?
25-Sep-1991	0	0	0	0	0	1	1
28-Feb-1989	0	0	0	0	0	1	1

Crecimiento anual de nombres de dominio registrados bajo .mx

.COM.MX		
Año	Nombres de dominio registrados	Crecimiento (%)
1989	0	N/A
1991	0	N/A
1992	1	N/A
1994	5	400.00
1995	180	3,500.00
1996	2,286	1,170.00
1997	6,043	164.35
1998	10,661	76.42
1999	25,026	134.74
2000	56,769	126.84
2001	61,496	8.33
2002	66,545	8.21
2003	74,885	12.53

.GOB.MX		
Año	Nombres de dominio registrados	Crecimiento (%)
1989	0	N/A
1991	0	N/A
1992	0	N/A
1994	1	N/A
1995	12	1,100.00
1996	75	525.00
1997	201	168.00
1998	350	74.13
1999	510	45.71
2000	935	83.33
2001	1,278	36.68
2002	1,687	32.00
2003	2,074	22.94

.NET.MX		
Año	Nombres de dominio registrados	Crecimiento (%)
1989	0	N/A
1991	0	N/A
1992	0	N/A
1994	0	N/A
1995	20	N/A
1996	143	615.00
1997	262	83.22
1998	395	50.76
1999	639	61.77
2000	761	19.09

2001	662	-13.01
2002	621	-6.19
2003	557	-10.31

.EDU.MX		
Año	Nombres de dominio registrados	Crecimiento (%)
1989	0	N/A
1991	0	N/A
1992	0	N/A
1994	0	N/A
1995	0	N/A
1996	13	N/A
1997	168	1,192.31
1998	359	113.69
1999	557	55.15
2000	855	53.50
2001	1,245	45.61
2002	1,692	35.90
2003	2,114	24.94

.ORG.MX		
Año	Nombres de dominio registrados	Crecimiento (%)
1989	0	N/A
1991	0	N/A
1992	0	N/A
1994	0	N/A
1995	13	N/A

1996	142	992.31
1997	389	173.94
1998	622	59.90
1999	1,221	96.30
2000	2,399	96.48
2001	2,759	15.01
2002	3,085	11.82
2003	3,148	2.04

.MX		
Año	Nombres de dominio registrados	Crecimiento (%)
1989	1	N/A
1991	1	0.00
1992	?	N/A
1994	44	N/A
1995	101	129.55
1996	179	77.23
1997	188	5.03
1998	189	0.53
1999	177	-6.35
2000	177	0.00
2001	177	0.00
2002	172	-2.82
2003	172	0.00

Cantidad de hosts en México bajo el dominio .mx

Fecha	com.mx	edu.mx	.mx	gob.mx	org.mx	net.mx	Total mx
Febrero 1998	11,000	200	20,000	500	300	12,000	44,000
Agosto 1998	15,000	800	28,000	650	400	24,000	68,850
Febrero 1999	19,318	1,540	38,120	1,187	510	38,811	99,486
Agosto 1999	27,053	1,433	37,853	1,024	672	131,332	199,367
Febrero 2000	31,013	1,584	43,414	1,693	1,292	210,268	289,264
Agosto 2000	56,181	2,091	55,955	1,545	1,699	350,831	468,302
Febrero 2001	53,441	1,626	50,188	1,038	1,519	452,485	560,297
Agosto 2001	54,042	1,592	61,058	762	1,460	630,934	749,848
Febrero 2002	53,506	1,441	45,280	881	1,954	870,215	973,277

CAPÍTULO 4

MARCO METODOLÓGICO

4 MARCO METODOLÓGICO

4.1 VARIABLES

VARIABLE INDEPENDIENTE

Un servidor de nombres sin medidas de seguridad.

VARIABLE DEPENDIENTE

- ◆ Puede ocasionar la desviación de tráfico en una red.
- ◆ Puede ocasionar la desviación de servicios de Internet.
- ◆ Puede ocasionar la negación de servicios de Internet.
- ◆ Puede ocasionar la falsificación de páginas web.
- ◆ Puede ocasionar la interceptación de correo electrónico.
- ◆ Puede ocasionar el robo de información acerca de los servicios que proporciona una red.
- ◆ Afecta la seguridad de los servicios de Internet.
- ◆ Afecta la integridad del espacio de nombres de dominio.
- ◆ Afecta la imagen de las organizaciones.
- ◆ No contribuye a la confiabilidad de la información que contiene.

4.2 VARIABLES DE CONTROL

Para el presente trabajo de tesis, he considerado que las variables de control (intervinientes y distorsionantes), no aplican, ya que los factores que generalmente se utilizan para trabajar con dichas variables, no se adaptan al tema de "Seguridad en el Sistema de Nombres de Dominio".

4.3 HIPÓTESIS DEFINITIVA

"Un servidor de nombres sin medidas de seguridad, puede ocasionar la falsificación, desviación y negación de servicios en Internet, así como la interceptación y el robo de información acerca de los hosts y servicios que proporciona una red, afectando la seguridad de dichos servicios, la integridad del espacio de nombres de dominio y la imagen de las organizaciones"

4.4 DEFINICIÓN DEL UNIVERSO

El Sistema de Nombres de Dominio, es utilizado por todos los usuarios conectados a Internet, por lo que el problema de seguridad en el DNS que se plantea en este trabajo, bien podría presentarse en cualquier servidor de nombres de cualquier parte del mundo. De esta manera, el universo de estudio puede generalizarse y hacer participe a todo aquel que administre o haya administrado uno o más servidores de nombres.

4.5 DETERMINACIÓN DE LA MUESTRA

Este no es un estudio de prueba plena, por lo que no se intenta convencer a ninguna persona de que la presentación del problema en sus efectos son factores suficientes para someter a investigación la hipótesis de trabajo.

Dado que es imposible observar a todos los elementos que componen el universo de estudio, se debe seleccionar una muestra, que para efectos de este trabajo será no probabilística y de juicio.

La muestra se compondrá de organizaciones de diversa índole y la finalidad será comprobar si estas organizaciones cuentan con las medidas de seguridad necesarias en sus servidores de nombres y la opinión que tienen los administradores de DNS acerca de la seguridad en el Sistema de Nombres de Dominio.

La muestra se compone de las siguientes organizaciones:

- ◆ Benemérita Universidad Autónoma de Puebla
- ◆ Check Point Software Technologies México
- ◆ Ericsson
- ◆ INAH (Instituto Nacional de Antropología e Historia)
- ◆ NIC-México (Network Information Center – México)
- ◆ NICunam (Centro de Información de RedUNAM)
- ◆ Podernet S.A. de C.V.
- ◆ Secretaría de Hacienda y Crédito Público
- ◆ U.N.A.M. - Iztacala
- ◆ Universidad La Salle

4.6 COSTO DE LA INVESTIGACIÓN

A continuación se presenta un valor aproximado de los costos y gastos realizados durante el trabajo de investigación (Mayo del 2001 a Junio del 2004). Cabe señalar que se toman en cuenta 18 meses de trabajo efectivo.

RUBRO	SUBTOTAL	COSTO M.N.
Sueldo		
1 persona	172,800.00	172,800.00
Rentas		
Oficina	14,400.00	14,400.00
Equipo		
Mesa de cómputo	1,000.00	
Computadora	7,000.00	8,000.00
Papelería y artículos de oficina		
Discos	150.00	
Hojas	200.00	
Cuaderno y lapiceros	50.00	400.00
Gastos diversos		
Alimentos	2,160.00	
Pasajes	1,620.00	
Copias fotostáticas	600.00	
Teléfono	2,880.00	
Internet	2,880.00	
Libros	800.00	10,940.00
TOTAL		\$206,540.00

4.7 CONSTRUCCIÓN DEL CUESTIONARIO

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND
 DNS de Microsoft
 DJBDNS

Razón de la pregunta:

Determinar que implementaciones de DNS son las más conocidas.

Pregunta esperada:

BIND, DNS de Microsoft y DJBDNS.

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- BIND versión _____
 DNS de Microsoft versión _____
 DJBDNS versión _____

Razón de la pregunta:

Determinar que implementación y versión de DNS es la más utilizada y si los administradores de DNS suelen actualizar la versión a la más reciente.

Pregunta esperada:

BIND 8.2.X

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Razón de la pregunta:

Saber que factores influyen en la elección de la implementación de DNS para una organización.

Pregunta esperada:

Es la más conocida.

Existe más documentación de esa implementación.

No se ha probado alguna otra en mi organización.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Razón de la pregunta:

Conocer si existe conciencia entre los administradores de DNS acerca del papel que desempeña el DNS en el funcionamiento de Internet.

Pregunta esperada:

Muy importante debido a que el DNS permite la ubicación de los servicios de Internet por medio de nombres.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

() Muy importante _____

() Más o menos importante _____

() Poco importante _____

() No es importante _____

Razón de la pregunta:

Conocer la opinión de los administradores de DNS acerca de la importancia que tiene la implementación de seguridad en los servidores de nombres.

Pregunta esperada:

Muy importante...

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- () DNS spoofing attack
- () DNS buffer overflow
- () DNS Denial of Service attack
- () Client flooding
- () Dynamic updates vulnerabilities

Razón de la pregunta:

Saber que ataques son los más conocidos.

Pregunta esperada:

Todas.

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

() Si, porque _____

() No, porque _____

Razón de la pregunta:

Determinar si el entrevistado coincide en que la mayoría de los administradores de DNS no conocen a profundidad el funcionamiento de un servidor de nombres.

Pregunta esperada:

No, debido a falta de interés por parte de los administradores.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado.
- Split function name servers. Dos servidores de nombres.
- DNS enjaulado.
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo.
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra: _____

Razón de la pregunta:

Corroborar que la mayoría de los administradores de DNS no aplica medidas de seguridad en los servidores de nombres.

Pregunta esperada:

Todas.

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado.
- Split function name servers. Dos servidores de nombres.
- DNS enjaulado.
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo.

- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión

Razón de la pregunta:

Saber si los administradores de DNS entrevistados conocen la configuración necesaria para implementar las medidas de seguridad recomendadas para un servidor de nombres.

Pregunta esperada:

Todas.

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?

- Vulnerabilidades en el código de la implementación de DNS
 - Vulnerabilidades del sistema operativo
 - Mala administración del servidor que alberga el DNS
 - Mala configuración del servidor de nombres
 - Otra: (especifique) _____
-
-

Razón de la pregunta:

Comprobar que la mala administración del servidor que alberga el DNS y la mala configuración de los servidores de nombres son las principales causas de ataques exitosos a servidores de nombres.

Pregunta esperada:

Mala administración del servidor que alberga el DNS.
Mala configuración del servidor de nombres.

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?

- Negación del servicio
 - Robo de correo electrónico
 - Falsificación de páginas web
 - Obtener información acerca de los hosts de una red
 - Creación de registros
 - Desvío de transferencias de archivos
 - Obtener acceso como usuario root
 - Otro: (especifique) _____
-
-

Razón de la pregunta:

Determinar si son conocidos los objetivos por los cuales se atacan los servidores de nombres.

Pregunta esperada:

Todas.

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía, conoce?

- DNSSEC
- TSIG

Razón de la pregunta:

Determinar si son conocidos los protocolos basados en criptografía, como métodos para agregar seguridad al DNS.

Pregunta esperada:

Ambos

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?

- DNSSEC
- TSIG

Razón de la pregunta:

Determinar si son empleados estos protocolos en el DNS. Debido a la escasez de información respecto a estos protocolos, se espera que los entrevistados contesten que no aplican ninguno.

Pregunta esperada:

Ninguno.

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS? Explique

Si, por que _____

No, porque _____

Razón de la pregunta:

Conocer las razones por las cuales no se ha hecho popular el uso de protocolos criptográficos en el DNS.

Pregunta esperada:

Se espera que la respuesta predominante sea que no es popular el uso de estos protocolos debido a la complejidad en la configuración necesaria en los servidores de nombres y a la falta de documentación al respecto.

4.8 CUESTIONARIO PILOTO

Antes de aplicar el cuestionario de manera definitiva, se aplicó a dos personas en forma de prueba, con el fin de verificar que el cuestionario elaborado sea comprensible.

El formato del cuestionario piloto se encuentra en el anexo 4 de este trabajo.

Las personas entrevistadas fueron:

1) Paul Conde Medina

S.H.C.P.

Desarrollo de Aplicaciones (ex-integrante del Centro de Información de RedUNAM)

2) Erick González Hernández

D.G.S.C.A

Centro de Información de RedUNAM

En base a las respuestas obtenidas en la aplicación del cuestionario en forma piloto y a los comentarios que hicieron los entrevistados de manera personal, se hicieron los siguientes ajustes leves al cuestionario:

- ◆ En la pregunta número 6 se agregó la opción de respuesta "otro".
- ◆ En la pregunta número 9 se agregó la opción de respuesta "ninguna".
- ◆ En la pregunta 12 y 13 se agregó la opción de respuesta "ninguno".

4.9 CUESTIONARIO DEFINITIVO

El formato del cuestionario definitivo se encuentra en el anexo 4 de este trabajo.

4.10 REALIZACIÓN DE LA INVESTIGACIÓN.

El cuestionario definitivo se aplicó a las siguientes personas:

Francisco Arias

FA_1
NIC-México
Administración de servidores de nombres

Yazzmín Castillo Martínez

YCM_2
Instituto Nacional de Antropología e Historia
Administración de red

Paul Conde Medina

PCM_3
S.H.C.P.
Desarrollador de aplicaciones

Ivette De Luna Bonilla

ILB_4
Ericsson
Área de equipos de datos

José Enrique Díaz Jolly

JDJ_5
Podernet S.A. de C.V.
Gerente de sistemas

Mario Farias

MF_6
Universidad La Salle
Administración de red

Erick González Hernández

EGH_7
D.G.S.C.A.
Integrante del Centro de Información de RedUNAM

Martín Humberto Hoz Salvador

MHS_8
Check Point Software Technologies México
Experto en seguridad

Genny León Leal

GLL_9
D.G.S.C.A.
Integrante del Centro de Información de RedUNAM

Jorge Alberto Martínez Melo

JMM_10

D.G.S.C.A.

Coordinador del Centro de Información de RedUNAM

Sergio Moreno Reyes

SMR_11

D.G.S.C.A.

Integrante del Centro de Información de RedUNAM

Ricardo Santos Quintero

RSQ_12

Benemérita Universidad Autónoma de Puebla

Administración de servidores de nombres

Gunnar Wolf

GW_13

U.N.A.M. Iztacala

Seguridad y administración de servidores

Las respuestas de las personas entrevistadas se encuentran en el anexo 4 de este trabajo.

A continuación se presenta el resumen de las respuestas proporcionadas por las personas a quienes se les aplicó el cuestionario.

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- a) BIND
- b) DNS de Microsoft
- c) DJBDNS

	a	b	c
FA_1	X		
YCM_2	X		
PCM_3	X		
ILB_4	X		
JDJ_5	X		X
MF_6	X	X	
EGH_7	X		
MHS_8	X	X	
GLL_9	X	X	
JMM_10	X	X	
SMR_11	X		

RSQ_12	X	X	
GW_13	X		

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- a) BIND
- b) DNS de Microsoft
- c) DJBDNS

	a	b	c
FA_1	8.2.5		
YCM_2	8.2.2-P5		
PCM_3	8.2.X		
ILB_4		X	
JDJ_5	8.3.1		1.0.5
MF_6	9.1.3		
EGH_7	8.4.X		
MHS_8	Meta IP DNS*		
GLL_9	8		
JMM_10	8.3 y 9.2		
SMR_11	8.2.3		
RSQ_12	8.3.1	X	
GW_13	4		

* Meta IP DNS de Check Point es una variante propietaria de BIND 8.

3.- ¿Por qué razón utiliza esa implementación de DNS?.

	Respuesta
FA_1	Es la más estable, funcional y segura.
YCM_2	Hasta el momento es la única que he manejado y me es sencilla de entender y manejar.
PCM_3	Por el tipo de recursos disponibles en la organización.
ILB_4	Por estándar, todo se trabaja bajo plataforma windows.
JDJ_5	BIND porque es la implementación más completa y concretamente 8.3.1 es en este momento la más segura y estable. Además cumple con todos los protocolos establecidos. No utilizo la 9x porque aún está en desarrollo y no cumple con todos los protocolos o algunos aún no han sido debidamente implementados o están en desarrollo en IETF. DJBDNS lo utilizamos solamente en cachés que se utilizan como

	DNS/resolver para distintas redes.
MF_6	Es la más estable y con menos problemas de seguridad.
EGH_7	Porque es libre y es de las más probadas.
MHS_8	Porque es la que fabrica la compañía.
GLL_9	Porque la última versión todavía no está por aprobarse y esta es la que ha estado en práctica y ha funcionado relativamente bien.
JMM_10	La versión 8.3 es considerada la más estable para poner en producción. La versión 9.2 la empleo para probar IPv6.
SMR_11	Porque la plataforma UNIX es más segura, confiable, estable y poderosa. Además, BIND se ha consolidado como una aplicación muy estable, capaz de soportar alta demanda de peticiones de DNS y cuenta con soporte, FAQ's, y lista para resolver dudas, comentarios y sugerencias.
RSQ_12	Utilizamos la versión 8 de BIND dado que es la más estable y probada para ambientes de producción en sistemas 24x7. En un futuro próximo tenemos planeado utilizar la versión 9 y aprovechar características como DNSSEC, TSIG y soporte de IPv6. Asimismo estamos concientes que BIND sobre UNIX es la mejor opción en términos de seguridad y disponibilidad para DNS servers sin embargo, el uso de DNS de Microsoft nos es requerido para el funcionamiento óptimo de MS Active Directory. Actualmente estamos haciendo pruebas con Active Directory y BIND 8/9 para relevar el uso de MS-DNS.
GW_13	Por ser código auditado - El equipo de desarrollo de OpenBSD incluye BIND versión 4 pues ha comprobado exhaustivamente su seguridad, cosa que nadie ha hecho con versiones posteriores de este programa. Y claro, elegí usar BIND por ser libre.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

	Respuesta
FA_1	Tiene una importancia muy alta puesto que el DNS es quien provee el mapeo de nombres a IP's.
YCM_2	Muchísima, diría que es un servicio primordial para todos

	<p>aquellos que usamos los servicios de Internet, debido a que un DNS nos proporciona la traducción de direcciones IP a nombre y viceversa nos facilita el trabajo de obtener información en forma rápida.</p>
PCM_3	<p>Es una materia delicada lo que respecta al DNS, pues es aquí donde es posible encontrar todos los dominios, nombres, hosts disponibles en Internet.</p>
ILB_4	<p>Alta, pues sin ese servicio no funcionarían varias aplicaciones.</p>
JDJ_5	<p>Son fundamentales pues sin ellos Internet no sería lo que es hoy en día. No es lo mismo aprenderse la dirección:puerto de un recurso que un nombre.</p>
MF_6	<p>Muy importante, ya que es el servicio medular de la Internet, sin él sería imposible navegar por la Internet, debido a que la mayoría de los usuarios no conocen las direcciones IP's de los servidores.</p>
EGH_7	<p>Su importancia es muy alta. Facilita el acceso a sitios web por nombre. El sistema jerarquizado permite que los DNS administren su espacio respectivo del Sistema de Nombres de Dominio facilitando la administración y actualización de las zonas. Brinda información de direcciones IP con sus respectivos dominios. Esto ayuda a realizar tareas de troubleshooting.</p>
MHS_8	<p>Bastante. Simplemente sin nombres no podríamos vivir.</p>
GLL_9	<p>Una importancia del 100% ya que sin este no hay un buen funcionamiento en Internet, no existe un orden de las cosas y por medio de DNS existe una adecuada administración de los dominios y resoluciones inversas.</p>
JMM_10	<p>Básicamente es el mecanismo que hace posible el acercamiento de la red con cualquier tipo de usuario y de manera más clara y optima para usuarios no especializados. Técnicamente, el DNS es un medio para validar y autenticar servicios y conexiones.</p>
SMR_11	<p>Es vital, puesto que sin los DNS, la Internet no sería la misma, ya que en el caso de las direcciones IP, tendríamos que aprendernos todas y cada una de ellas para decidir a cual acceder, además de eso, los DNS trabajan de manera transparente para el usuario, el cual quizá no sabe que existen, pero cuando se genera una falla, son los primeros en detectarlo y sobrevienen los problemas. Un DNS, es demasiado importante para la Internet, pues sin</p>

	ellos, sería prácticamente imposible que cualquier usuario común y corriente pudiera comunicarse con el resto del mundo, pues es mucho más sencillo conocer una dirección por su nombre que por su IP, y para ipv6, pues la situación es peor.
RSQ_12	Tiene un nivel de importancia de primer orden. Dado que en Internet y en caso particular dentro de nuestras intranets con el paso del tiempo se crean y liberan nuevos servicios de los cuales algunos de ellos están ligados directamente como servicio a un registro en nuestras zonas de DNS.
GW_13	La resolución de nombres es vital para prácticamente todos los aspectos del uso de Internet.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

FA_1	Muy importante	Por ser el servicio de mapeo de nombres a IP's.
YCM_2	Muy importante	Es un servicio que siempre debe estar disponible los 365 días del año por su gran importancia, sin este servicio no podríamos acceder a los servicios en forma rápida y tendríamos que averiguar el nombre asignado a tal dirección IP.
PCM_3	Muy importante	Para evitar problemas relacionados con relay y spam, que al fin y al cabo, consumen recursos de nuestra organización.
ILB_4	Muy importante	Implicaría costos a la empresa.
JDJ_5	Muy importante	Porque al ser una de las piedras fundamentales de la red, si un DNS es contaminado por información que no es correcta, se puede volver un caos. Por otro lado, puede hacerse pública información que no debe ser pública, por ejemplo, los nombres de una red interna.
MF_6	Muy importante	Es uno de los servicios medulares de la Internet.
EGH_7	Muy importante	Se deja a toda la zona de la que es responsable ese DNS deshabilitada de Internet y por consecuencia a sus clientes y no se podría tener acceso a información y servicios valiosos dentro de la zona del DNS.

MHS_8	Muy importante	Un DNS mal configurado puede ser un boquete demasiado grande. Desde bugs en la implementación del servicio que permitan ejecutar código arbitrario a un atacante, pasando por envenenamientos y falsificación de nombres, hasta llegar a negaciones de servicio y pérdida de negocio.
GLL_9	Muy importante	Si algo ocurre con el servidor de nombres provocaría un gran descontrol ante las zonas y nombres de dominio, también se expondría su adecuado funcionamiento y se harían redireccionamientos hacia otros nombres de dominios falsos, también se podría comprometer todo el servidor de nombres provocando negación del servicio, falsificar datos, violar la integridad de los datos o hacerse pasar por una entidad falsa.
JMM_10	Muy importante	Es muy importante dado que es un servicio crítico que asegura el correcto orden y funcionamiento de la red.
SMR_11	Muy importante	La seguridad es uno de los aspectos más importantes para cualquier servidor, sea web, correo, BD o DNS. En el caso de DNS es muy importante, ya que al igual que cualquier equipo conectado a Internet, es susceptible de ser atacado, y es por ello que debemos tener herramientas que sirvan de apoyo para detectar y evitar cualquier posible ataque, ya que si se compromete el servicio, miles de usuarios se verían afectados por el servicio de DNS.
RSQ_12	Muy importante	Una de las razones es por que contiene información sobre los hosts de una red.
GW_13	Muy importante	En todo servidor es muy importante

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- a) DNS spoofing attack
- b) DNS buffer overflow
- c) DNS Denial of Service attack

- d) Client flooding
 e) Dynamic updates vulnerabilities
 f) Otro (especifique):

	a	b	c	d	e	f
FA_1	X	X	X		X	Configuración insegura.
YCM_2			X			
PCM_3						Ninguno
ILB_4						Ninguno
JDJ_5	X	X	X	X	X	Cache Polution, Fake Resolving
MF_6		X	X		X	
EGH_7	X		X			
MHS_8	X	X	X	X	X	DNS cache poisoning
GLL_9		X	X			
JMM_10	X	X		X	X	
SMR_11	X	X				
RSQ_12	X	X	X	X	X	Transferencia no autorizada de zonas
GW_13	X	X	X	X	X	

7.- Considera usted, que en general los administradores de DNS, concocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

		Respuesta
FA_1	No	No los conocen por que en la mayoría de los casos que conozco no se le da importancia al DNS debido a la relativa sencillez con que se pone a funcionar.
YCM_2	No	Depende, para aquellos administradores que sólo manejan un servidor DNS se les podría facilitar conocer a detalle este tipo de ataques, para aquellos que manejamos de todo es mucho más difícil, te dedicamos a instalarlo, configurarlo y listo, es más difícil dedicarle más tiempo, eso en caso de que se presente un ataque y entonces si tengas necesariamente que entender el problema y resolverlo.
PCM_3	No	No todos los administradores de DNS saben la

		responsabilidad que tienen en sus manos, hay algunos que ni siquiera saben lo que es un "ataque".
ILB_4	No	Porque pueden implementar los sistemas de seguridad más comunes y sentirse seguros.
JDJ_5	No	En general no están capacitados, muchos con trabajos conocen los rudimentos de la operación de DNS. La prueba es la cantidad de MX que resuelven a CNAMES etc.
MF_6	No	La mayoría de los administradores, por lo menos en México, están muy acostumbrados a utilizar el DNS de Microsoft, por lo que no tienen un conocimiento profundo del servicio DNS, su importancia y mucho menos las vulnerabilidades que tienen. Dependen mucho de los parches del fabricante.
EGH_7	No	Pienso que casi siempre hasta que uno (en general) hasta que se ve envuelto en un problema de seguridad es cuando se preocupa por conocer los tipos de ataque o como prevenirlos.
MHS_8	No	Porque si no, no tendríamos tantos problemas con casos famosos y no tantos, en los que el DNS fue el problema.
GLL_9	No	Lamentablemente hoy en día estos temas no son muy conocidos por los administradores, solo se dedican a tener buen funcionamiento en sus sistemas o dan prioridad a otros aspectos dejando su seguridad a un lado; con esto dan una menor importancia a este aspecto sin saber que al atacar el mismo pueden llegar a perder todo el control del servidor. Existe desconocimiento por parte de los administradores debido a que son poco difundidos estos temas y el poco material que existe se encuentra en el idioma inglés, otro aspecto lamentable es que muchos administradores ni siquiera saben como configurar el DNS o lo que es peor ni siquiera conocen su funcionamiento.
JMM_10	No	Por lo menos en México, apenas se esta fomentando e inculcando la seguridad en la red. Tal vez se demore un poco de tiempo en que esta preocupación llega a cada uno de los servicio de Internet.
SMR_11	No	En muchas ocasiones, el administrador no sabe ni siquiera lo que es un servidor, y creo que cuando

		conocen algo de administración de servidores, se enfoca a servicios como correo, web o bases de datos, pero en el caso de DNS, es muy difícil que alguien se interese en conocer a detalle todo lo que implica, quizá porque aparentemente no brinda un servicio "palpable" a los usuarios, sino más bien es invisible para ellos, y quizá están más preocupados por sus aplicaciones de mayor prioridad que por la de un DNS.
RSQ_12	No	Es un problema de cultura que radica en la creencia de que los servidores de DNS son cajas que una vez instalados y operando estarán bien mientras resuelvan páginas y correos.
GW_13	No	La seguridad no es importante para mucha gente

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- a) Ocultar versión de BIND
- b) Restricción de queries
- c) Restricción de transferencias de zonas
- d) Correr BIND como usuario no-root o no privilegiado
- e) Split function name servers. Dos servidores de nombres
- f) DNS enjaulado
- g) Aplicación de parches de BIND
- h) Aplicación de parches de sistema operativo
- i) DNSSEC
- j) TSIG
- k) Restricción de actualizaciones automáticas
- l) Desactivación de recursión
- m) Ninguna
- n) Otra (especifique):

	a	b	c	d	e	f	g	h	i	j	k	l	m	n
FA_1	X		X											
YCM_2			X	X			X	X						
PCM_3	X	X	X				X	X	X		X			
ILB_4	X	X	X			X	X							
JDJ_5														X*
MF_6			X				X	X						
EGH_7			X	X			X	X	X		X			
MHS_8			X				X	X			X			X**
GLL_9	X	X	X	X			X	X						

JMM_10						X	X					X		
SMR_11	X		X	X	X		X							
RSQ_12						X								
GW_13														X***

* Respuesta de JDJ_5: En general son pocos los que las utilizan. Algunas son complejas de implementar, como por ejemplo DNSSEC a veces es complejo de implementar. Algunas protecciones son desde el punto de vista de la administración de servidores (por ejemplo, parches) otras son de diseño del servicio como la restricción de queries y de queries recursivos.

** Respuesta de MHS_8: Poner firewalls para proteger el equipos.

*** Respuesta de GW_13: El ocultar la versión de BIND se me hace un ejemplo de seguridad por obscuridad, o lo que es lo mismo, de falta de seguridad. No sugiero usarlo.

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra (especifique):

	a	b	c	d	e	f	g	h	i	j	k	l	m	n
FA_1	X	X	X	X	X	X	X	X	X	X	X	X		
YCM_2		X	X	X				X						
PCM_3	X	X	X				X	X	X		X			
ILB_4		X	X					X						
JDJ_5	X	X	X	X	X	?	X	X	X	X	X	X		
MF_6	X	X	X	X	X	X	X	X	X		X	X		
EGH_7				X			X	X						
MHS_8	X	X	X	X	X	X	X	X	X	X	X			
GLL_9	X	X		X			X	X						
JMM_10	X	X	X	X	X	X	X	X	X	X	X	X		

SMR_11	X		X	X			X	X			X	X		
RSQ_12	X	X	X	X		X	X	X	X	X	X	X		
GW_13		X	X	X		X	X	X				X		

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- a) Vulnerabilidades en el código de la implementación de DNS
 b) Vulnerabilidades del sistema operativo
 c) Mala administración del servidor que alberga el DNS
 d) Mala configuración del servidor de nombres
 e) Otra (especifique):

	a	b	c	d	e
FA_1			X	X	
YCM_2	X			X	
PCM_3	X	X	X	X	
ILB_4		X	X	X	
JDJ_5	X	X	X	X	
MF_6	X	X	X		
EGH_7			X	X	
MHS_8	X				
GLL_9			X		
JMM_10			X		
SMR_11	X		X	X	
RSQ_12			X		
GW_13				X	

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- a) Negación del servicio
 b) Robo de correo electrónico
 c) Falsificación de páginas web
 d) Obtener información acerca de los hosts de una red
 e) Creación de registros
 f) Desvío de transferencias de archivos
 g) Obtener acceso como usuario root
 h) Otro: (especifique)

	a	b	c	d	e	f	g	h
FA_1	X				X		X	
YCM_2			X	X		X	X	
PCM_3	X			X			X	

ILB_4			X	X	X	X	X	
JDJ_5			X	X	X	X	X	
MF_6	X			X			X	
EGH_7	X	X			X			
MHS_8	X		X		X			X*
GLL_9	X		X	X	X		X	
JMM_10		X	X	X		X		
SMR_11	X		X	X		X	X	
RSQ_12			X				X	
GW_13	X		X	X			X	

* Respuesta de MHS_8: Mala imagen para competidores.

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- a) DNSSEC
b) TSIG
c) Ninguno

	a	b	c
FA_1	X	X	
YCM_2	X		X
PCM_3			
ILB_4			X
JDJ_5	X	X	
MF_6	X	X	
EGH_7	X		
MHS_8		X	X
GLL_9	X		
JMM_10	X	X	
SMR_11	X		
RSQ_12	X	X	
GW_13	X	x	

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- a) DNSSEC
b) TSIG
c) Ninguno

	a	b	c
FA_1			X
YCM_2			X

PCM_3	X		
ILB_4			X
JDJ_5		X	
MF_6 *	X		
EGH_7			X
MHS_8			
GLL_9	X		X**
JMM_10			X
SMR_11			X
RSQ_12			X
GW_13			X

* Adicionalmente, levanto una VPN con IPSec entre los servidores donde esta el master y el slave.

** Respuesta de MHS_8: Yo no administro el DNS, aunque se que se utiliza TSIG internamente.

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS? Explique.

		Respuesta
FA_1	No	No está terminada la especificación (protocolo).
YCM_2	Si	He escuchado y leído sobre DNSSEC, y considerado que es muy popular en la red, es necesario estar documentado y conocer este tipo de recursos para agregar seguridad a nuestros servidores.
PCM_3		DNSSEC esta disponible en la versión 9 y no todos tienen el equipo suficiente para instalarlo.
ILB_4		No tengo conocimiento al respecto.
JDJ_5	No	No es fácil su implementación particularmente DNSSEC y es poco frecuente que un administrador de DNS se tome la molestia de analizar quien o quienes deben tener acceso a su DNS y de que forma. Por ejemplo la restricción de transferencias, de queries y de queries recursivos.
MF_6	No	Primero porque no estamos acostumbrados a tener una cultura de seguridad informática, por lo que no le damos importancia. Segundo, por lo mismo que se utilizan esquemas de criptografía el tráfico que se genera aumenta y generalmente los enlaces que se tienen son de baja capacidad. Y tercero, el más importante, no se

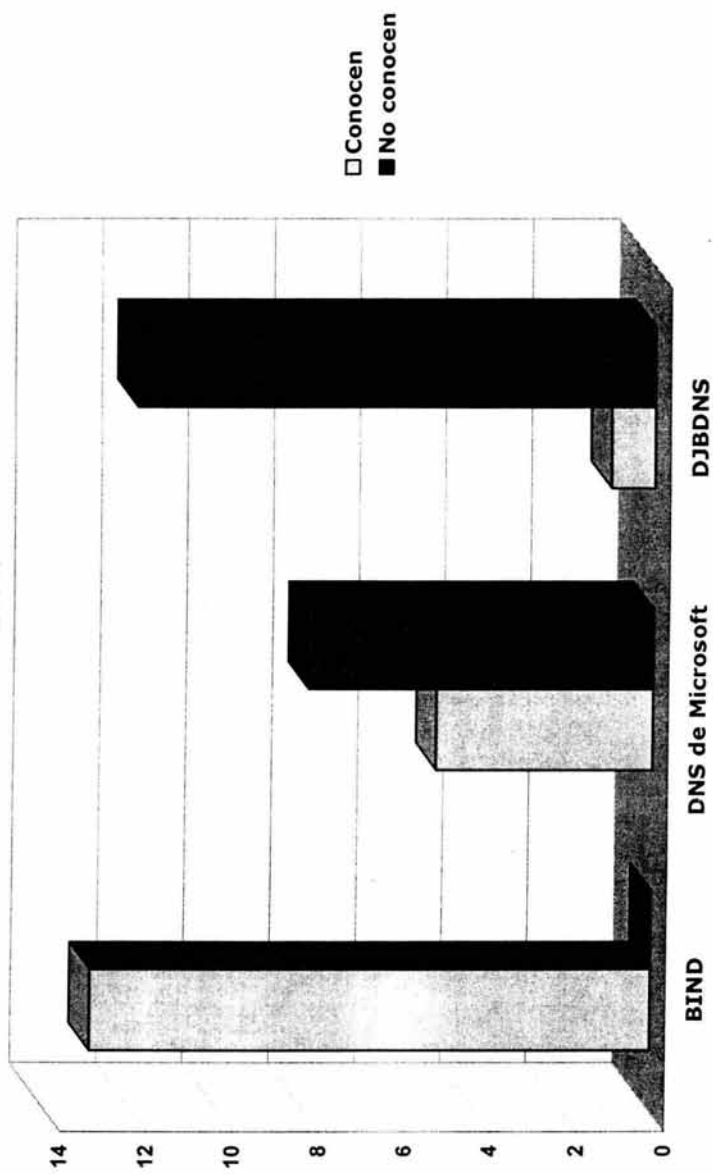
		ha dado a conocer en forma masiva los problemas de la seguridad y el como evitarlos.
EGH_7	No	Porque solo en ISP's muy grandes se preocupan por estas cuestiones.
MHS_8	No	En decenas de implementaciones de DNS que he visto, solo en un par de ellas he visto TSIG activado.
GLL_9	No	DNSSEC no consigue una buena difusión porque estos protocolos suelen ser más costosos en términos de recursos.
JMM_10	No	Realmente firmar las zonas degrada un poco la velocidad de transferencia de zonas y si se implementa en servidores que tienen muchas zonas y/o muy pesadas, pues esto resulta no muy óptimo.
SMR_11	No	No porque en muchas ocasiones no se cuenta con noticias, foros o noticias de las nuevas mejoras, herramientas o manuales de configuración y administración de DNS, además de que en muchas ocasiones implantar alguna herramienta suele ser costoso si no se conoce a detalle, pues puede provocar cambios en el servicio o en el peor de los casos, exponer el servicio a un ataque más fuerte.
RSQ_12		Creo que aún es un "add on" en fase experimental, si bien ya ha sido liberado su implementación pone en duda la estabilidad e interoperabilidad con clientes (otros servidores o clientes como tales) que no soporten el uso de DNSSEC y TSIG).
GW_13	No	Por su falta de compatibilidad con versiones anteriores, por la poca conciencia de seguridad en la gente.

4.11 TRATAMIENTO SISTEMATIZADO DE LA INFORMACIÓN

Pregunta No. 1

¿Qué implementación de DNS conoce y ha configurado?

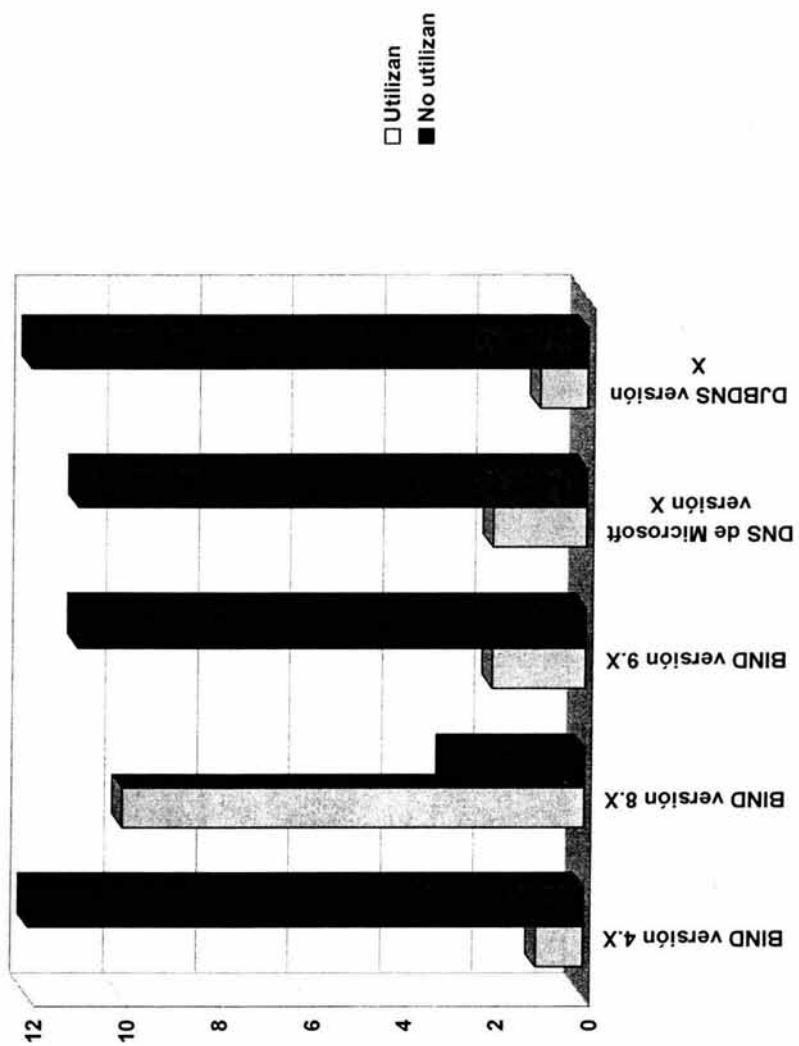
Respuesta	Conocen (de 13)		No conocen (de 13)	
BIND	13	100%	0	0%
DNS de Microsoft	5	38.5%	8	61.5%
DJBDNS	1	7.7%	12	92.3%



Pregunta No. 2

¿Qué implementación y versión de DNS utiliza en su organización?

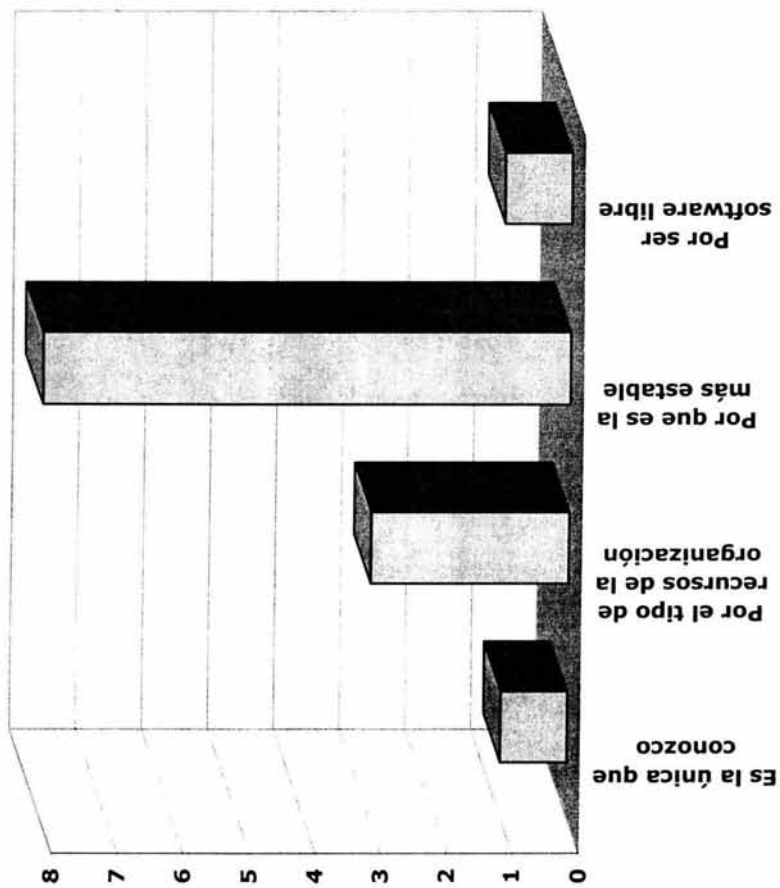
Respuesta	Utilizan (de 13)	No utilizan (de 13)
BIND		
Versión 4.X.....	1	12
Versión 8.X.....	10	3
Versión 9.X.....	2	11
DNS de Microsoft		
Versión X.....	2	11
DJBDNS		
Versión X.....	1	12



Pregunta No.3

¿Por qué razón utiliza esa implementación de DNS?

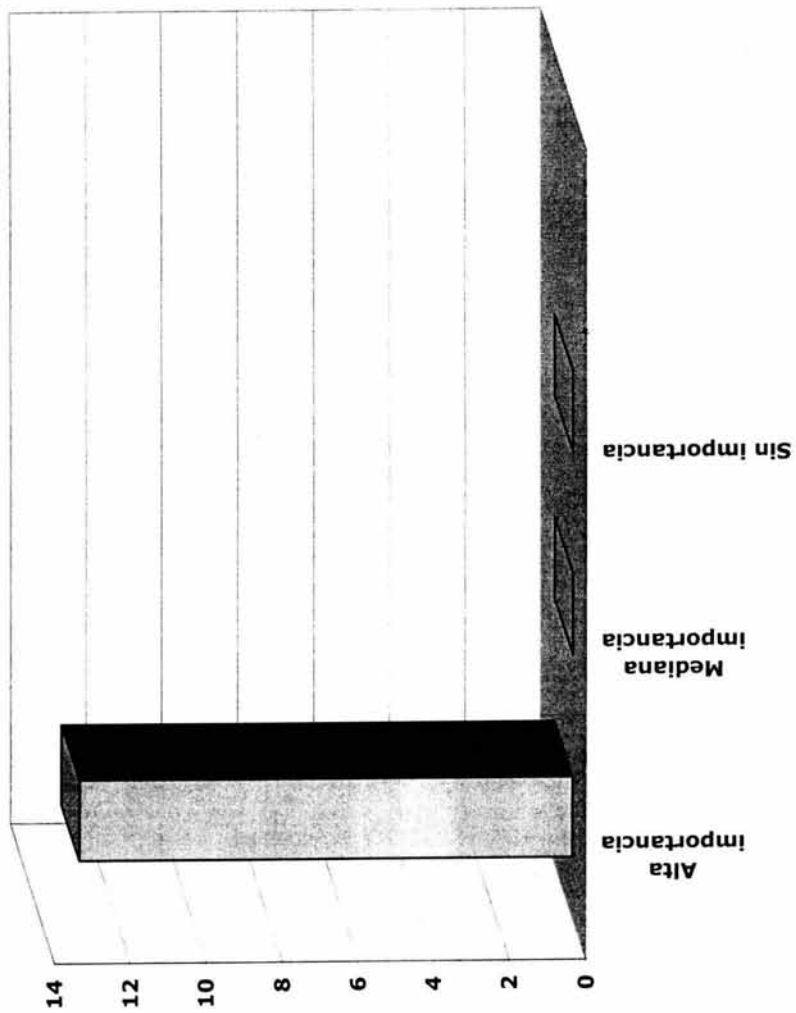
Respuesta	Cantidad	Porcentaje (%)
Es la única que conozco.....	1	8
Por el tipo de recursos de la organización.....	3	23
Por que es la más estable.....	8	61
Por ser software libre.....	1	8



Pregunta No. 4

¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?

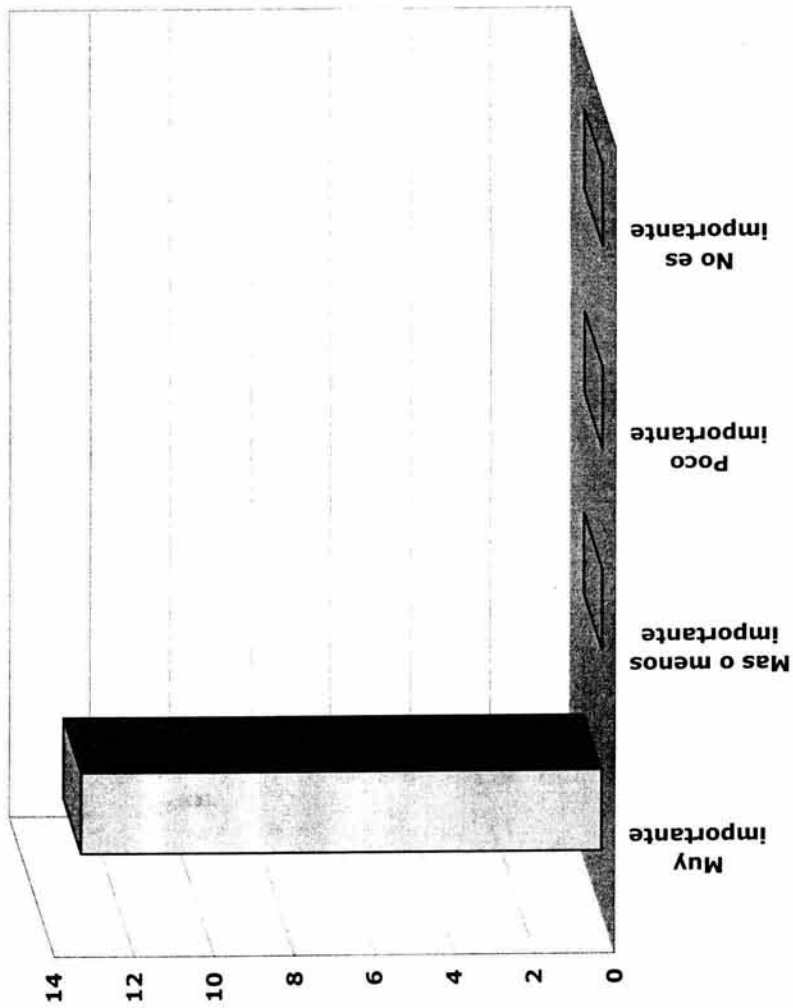
Respuesta	Cantidad	Porcentaje (%)
Alta importancia.....	13	100
Mediana importancia.....	0	0
Sin importancia.....	0	0



Pregunta No. 5

¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?

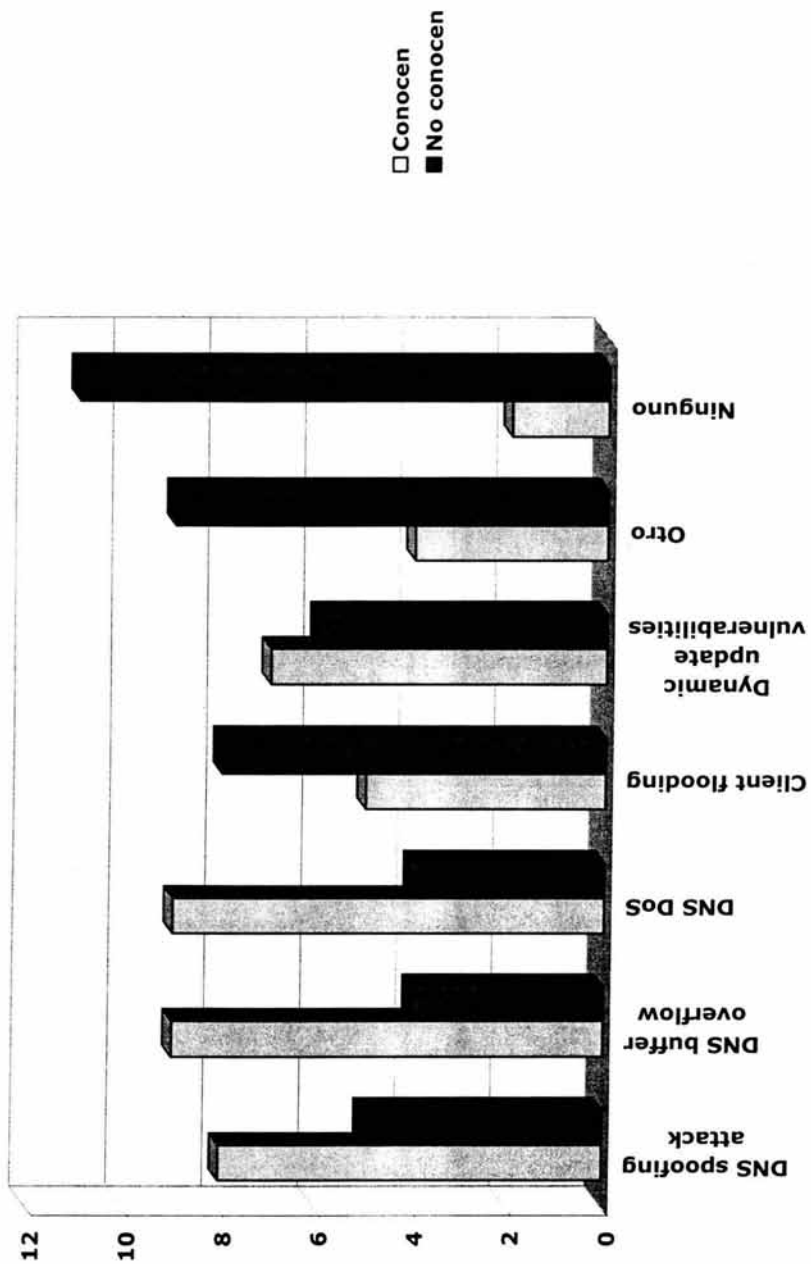
Respuesta	Cantidad	Porcentaje (%)
Muy importante.....	13	100
Más o menos importante.....	0	0
Poco importante.....	0	0
No es importante.....	0	0



Pregunta No. 6

De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuales conozca la manera de llevarlos a cabo y como prevenirlos.

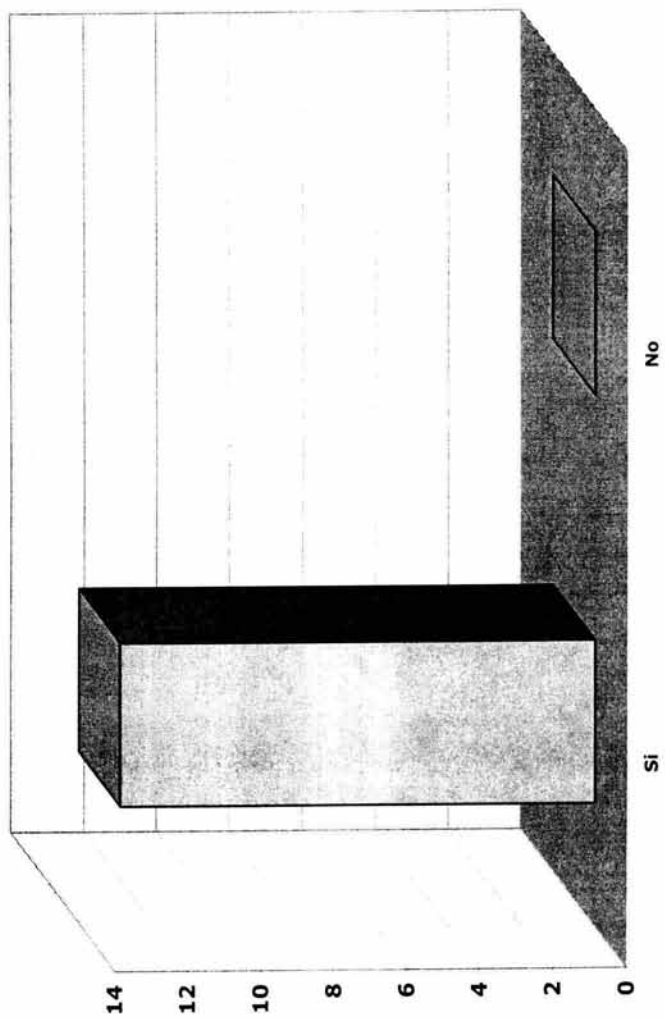
Respuesta	Conocen (De 13)	No conocen (De 13)
DNS spoofing attack.....	8 61.5%	5 38.5%
DNS buffer overflow.....	9 69.2%	4 30.8%
DNS DoS.....	9 69.2%	4 30.8%
Client flooding.....	5 38.5%	8 61.5%
Dynamic update vulnerabilities.....	7 53.8%	6 46.2%
Otro.....	4 30.8%	9 69.2%
Ninguno.....	2 15.4%	11 84.6%



Pregunta No. 7

¿Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?

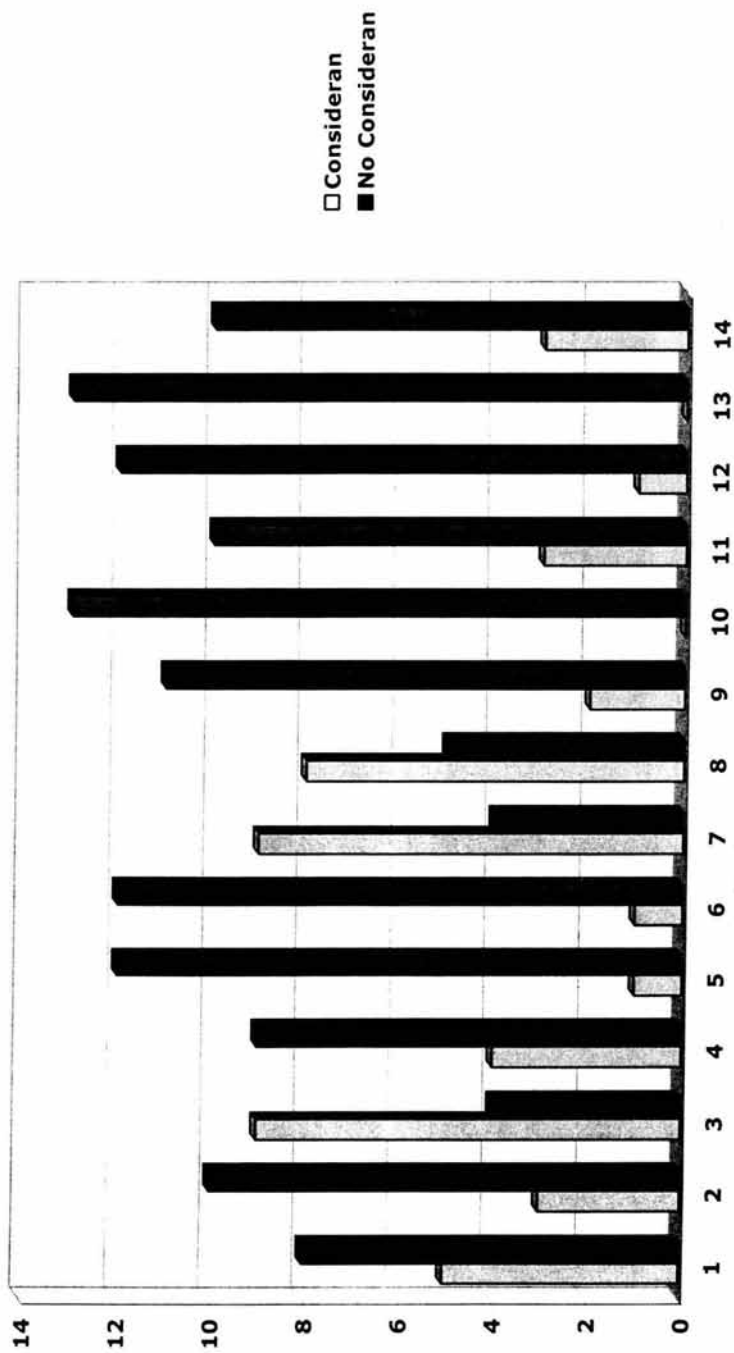
Respuesta	Cantidad	Porcentaje (%)
Si.....	13	100
No.....	0	0



Pregunta No. 8

De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?

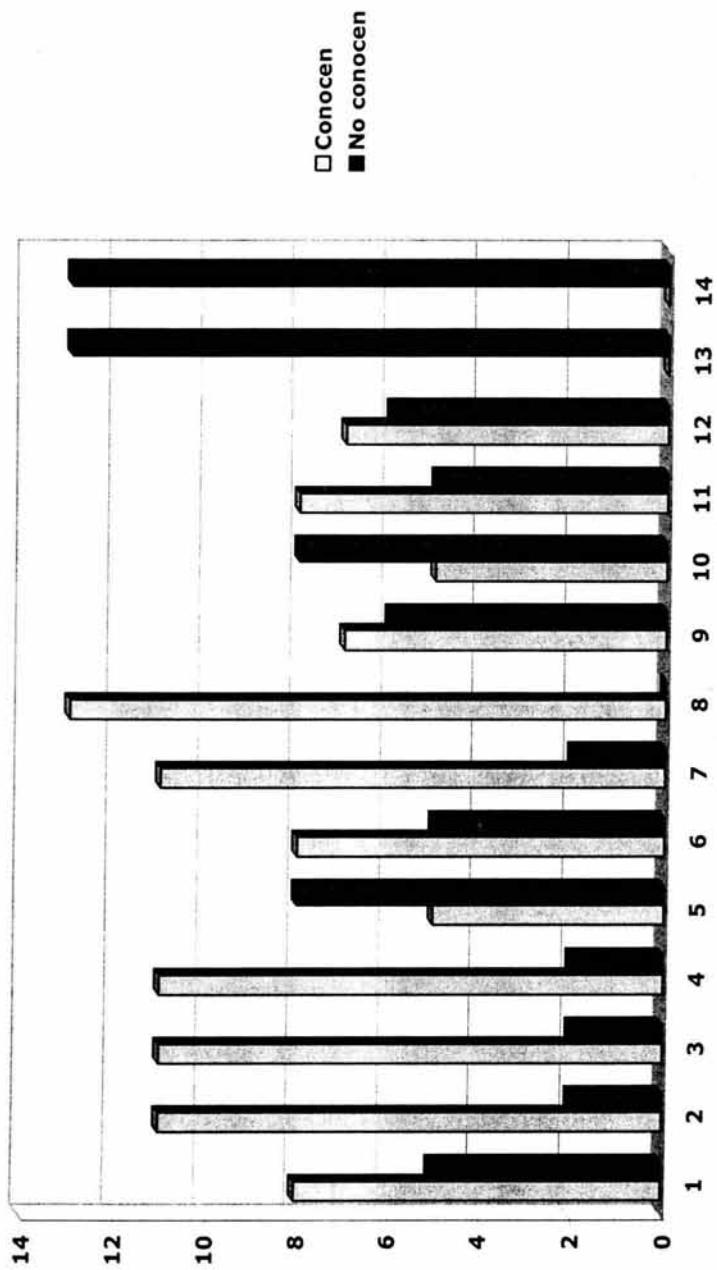
No. De respuesta en gráfica	Respuesta	Consideran (De 13)		No consideran (De 13)	
1	Ocultar versión de BIND.....	5	38.5%	8	61.5%
2	Restricción de queries.....	3	23%	10	77%
3	Restricción de transferencias de zonas.....	9	69.2%	4	30.8%
4	Correr BIND como usuario no-root o no privilegiado.....	4	30.8%	9	69.2%
5	Split function name servers. Dos servidores de nombres.....	1	7.7%	12	92.3%
6	DNS enjaulado.....	1	7.7%	12	92.3%
7	Aplicación de parches de BIND.....	9	69.2%	4	30.8%
8	Aplicación de parches de sistema operativo.....	8	61.5%	5	38.5%
9	DNSSEC.....	2	15.4%	11	84.6%
10	TSIG.....	0	0%	13	100%
11	Restricción de actualizaciones automáticas.....	3	23%	10	77%
12	Desactivación de recursión.....	1	7.7%	12	92.3%
13	Ninguna.....	0	0%	13	100%
14	Otra.....	3	23%	10	77%



Pregunta No. 9

De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

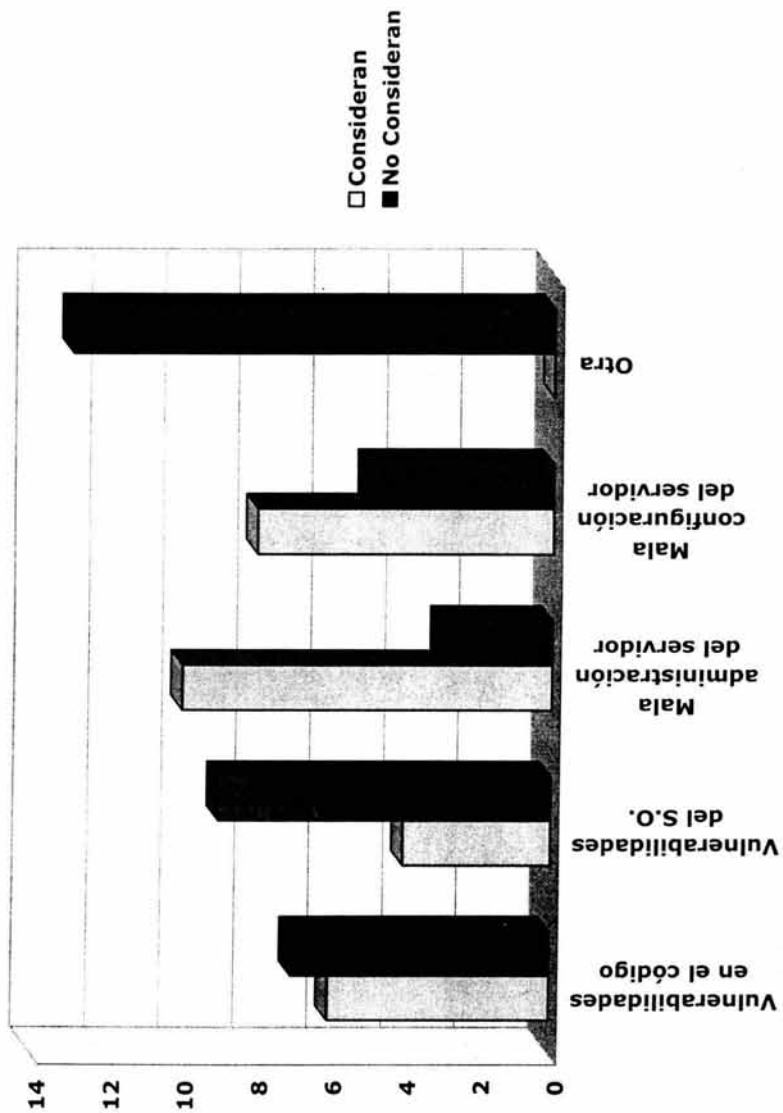
No. de respuesta en gráfica	Respuesta	Conocen (De 13)		No conocen (De 13)	
1	Ocultar versión de BIND	8	61.5%	5	38.5%
2	Restricción de queries	11	84.6%	2	15.4%
3	Restricción de transferencias de zonas	11	84.6%	2	15.4%
4	Correr BIND como usuario no-root o no privilegiado	11	84.6%	2	15.4%
5	Split function name servers. Dos servidores de nombres	5	38.5%	8	61.5%
6	DNS enjaulado	8	61.5%	5	38.5%
7	Aplicación de parches de BIND	11	84.6%	2	15.4%
8	Aplicación de parches de sistema operativo	13	100%	0	0%
9	DNSSEC	7	53.8%	6	46.2%
10	TSIG	5	38.5%	8	61.5%
11	Restricción de actualizaciones automáticas	8	61.5%	5	38.5%
12	Desactivación de recursión	7	53.8%	6	46.2%
13	Ninguna	0	0%	13	100%
14	Otra	0	0%	13	100%



Pregunta No. 10

¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?

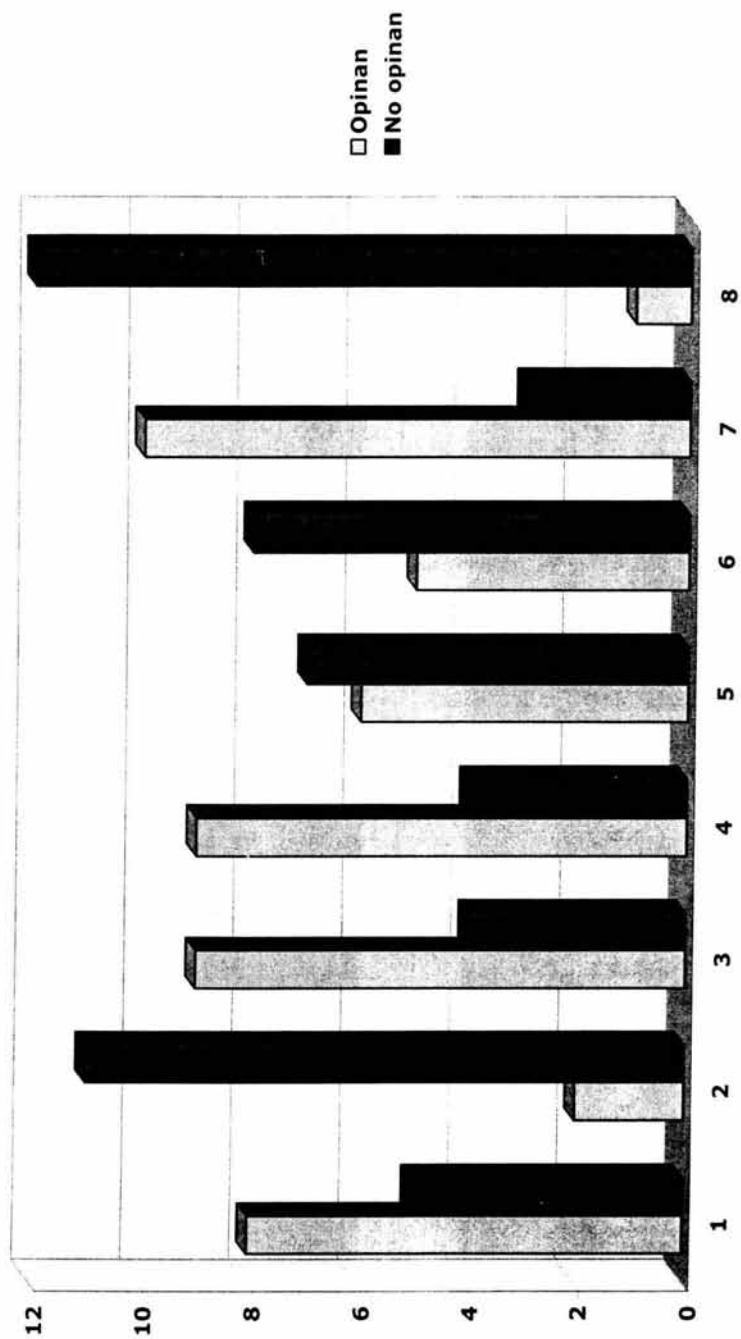
Respuesta	Consideran (De 13)	No consideran (De 13)
Vulnerabilidades en el código de la implementación de DNS.....	6 46.2%	7 53.8%
Vulnerabilidades del sistema operativo.....	4 30.8%	9 69.2%
Mal administración del servidor que alberga el DNS.....	10 77%	3 23%
Mal configuración del servidor de nombres.....	8 61.5%	5 38.5%
Otra.....	0 0%	13 100%



Pregunta No. 11

Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

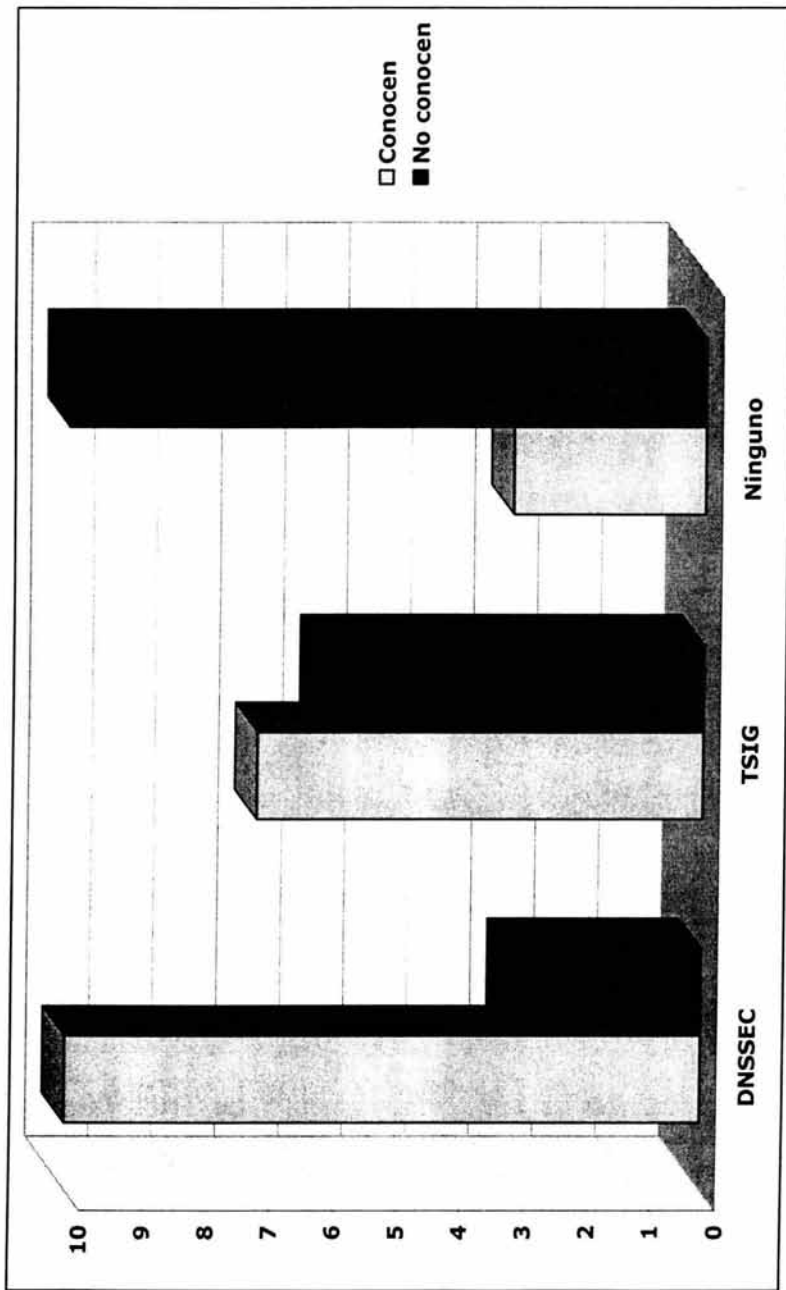
No. de respuesta en gráfica	Respuesta	Opinan (De 13)		No opinan (De 13)	
1	Negación del servicio.....	8	61.5%	5	38.5%
2	Robo de correo electrónico.....	2	15.4%	11	84.6%
3	Falsificación de páginas web.....	9	69.2%	4	30.8%
4	Obtener información acerca de los hosts de una red.....	9	69.2%	4	30.8%
5	Creación de registros.....	6	46.2%	7	53.8%
6	Desvío de transferencias de archivos	5	38.5%	8	61.5%
7	Obtener acceso como usuario root...	10	77%	3	23%
8	Otro.....	1	7.7%	12	92.3%



Pregunta No. 12

¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

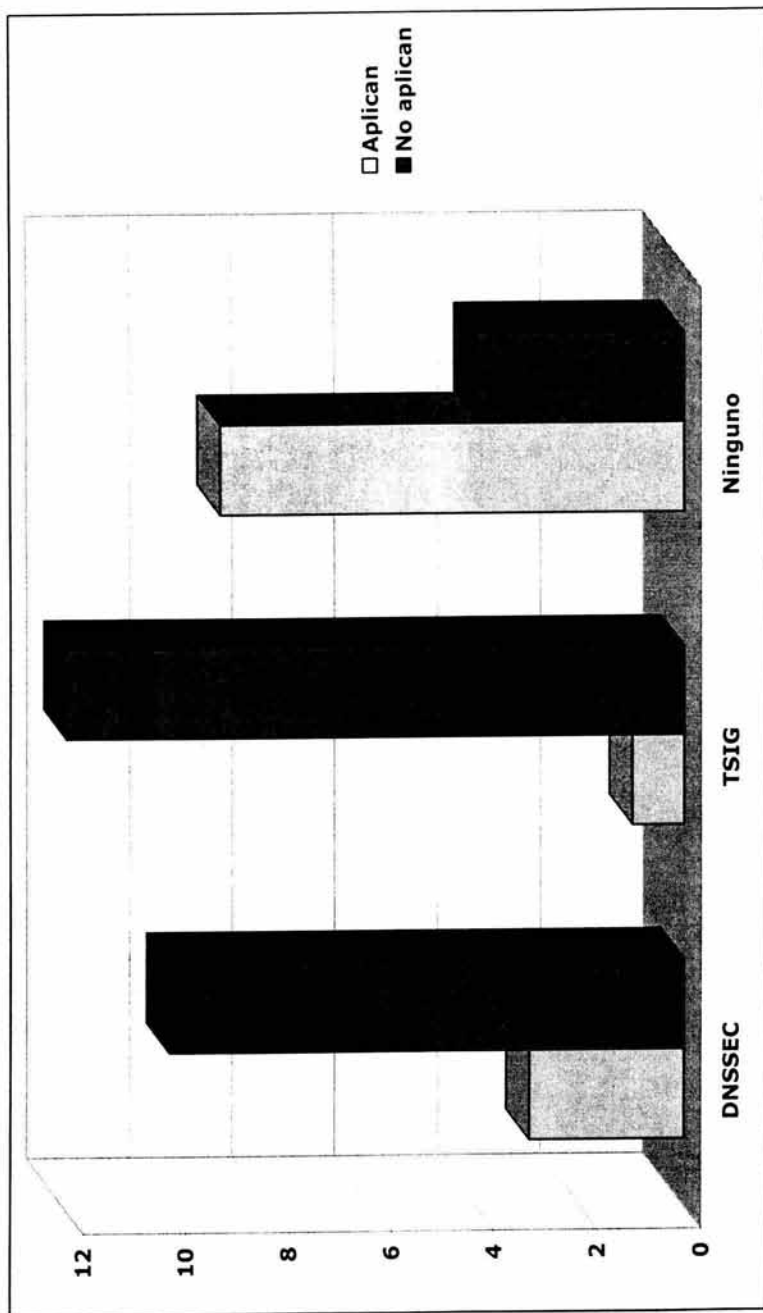
Respuesta	Conocen (De 13)	No conocen (De 13)
DNSSEC.....	10 77%	3 23%
TSIG.....	7 53.8%	6 46.2%
Ninguno.....	3 23%	10 77%



Pregunta No. 13

¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?

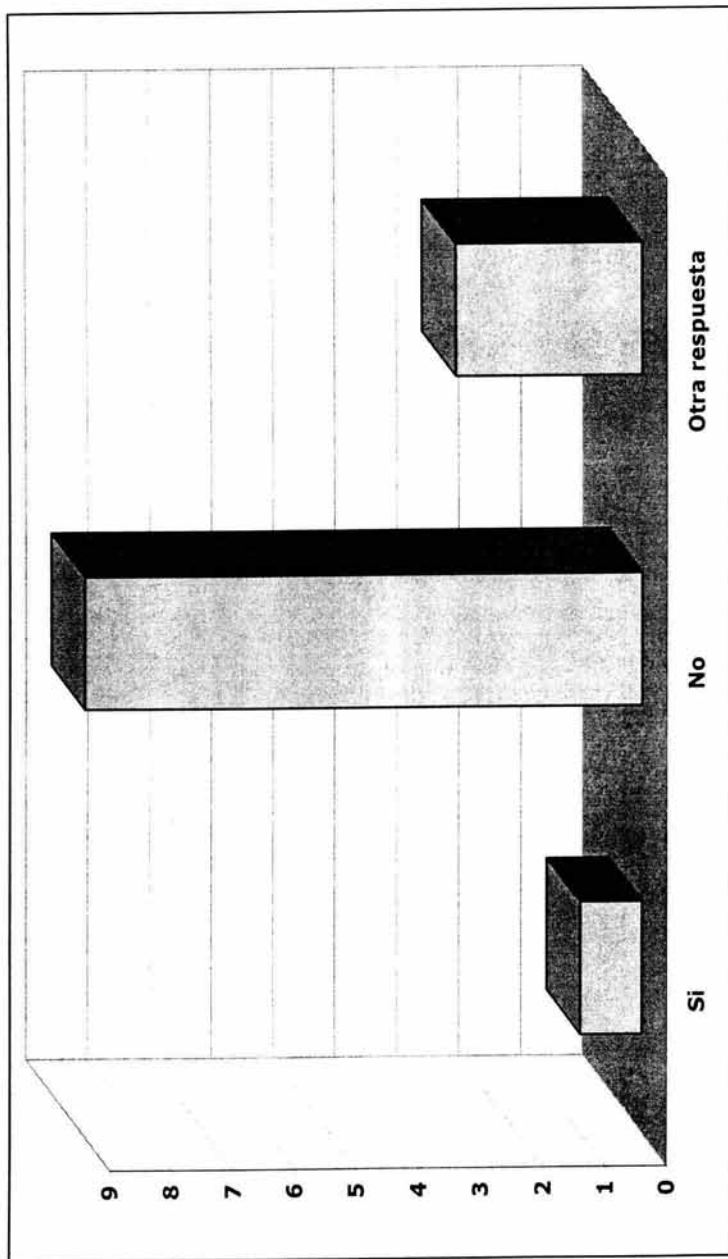
Respuesta	Aplican (De 13)	No aplican (De 13)
DNSSEC.....	3 23%	10 77%
TSIG.....	1 7.7%	12 92.3%
Ninguno.....	9 69.2%	4 30.8%



Pregunta No.14

¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?
Explique.

Respuesta	Cantidad	Porcentaje (%)
Si.....	1	7.7%
No.....	9	69.2%
Otra respuesta.....	3	23%



4.12 CONCLUSIONES POR RESPUESTA

1.- La implementación BIND es conocida por el 100% de los entrevistados. El software de DNS de Microsoft es conocida por el 38.5% y DJDNS solamente por el 7.7%.

La implementación de DNS más conocida es BIND.

2.- El 77% de los entrevistados utilizan la implementación BIND en su versión 8.X. Las versiones 9.X y 4.X de esta implementación sólo son utilizadas por el 15.4% y 7.7% respectivamente. El DNS de Microsoft en cualquiera de sus versiones sólo es utilizado por el 15.4% de los administradores de DNS y el DJBDNS únicamente por el 7.7%.

La implementación de DNS más utilizada por los administradores de servidores de nombres es BIND en su versión 8.X.

3.- El 61% de los administradores de servidores de nombres utilizan BIND en su versión 8.X debido a que consideran que es la versión más estable. El 8% utilizan esta versión por tratarse de software libre o bien por ser la única implementación que conocen. El 23% utiliza otras implementaciones de acuerdo al tipo de recursos con los que cuenta la organización.

La implementación BIND en su versión 8.X es la más utilizada por ser la más estable.

4.- El 100% de los entrevistados consideran que el DNS tiene una alta importancia para el buen funcionamiento de Internet.

El DNS tiene una alta importancia para el buen funcionamiento de Internet.

5.- El 100% de los entrevistados considera muy importante implementar seguridad en los servidores de nombres.

Es de suma importancia implementar seguridad en los servidores de nombres.

6.- Los ataques a servidores de nombres más conocidos, para los cuales los administradores conocen la manera de llevarlos a cabo y la forma de prevenirlos, son el DNS buffer overflow y el DNS DoS. Estos dos ataques son conocidos por el 69.2% de los entrevistados. Otro ataque bastante conocido

por los administradores de DNS es el DNS spoofing attack (61.5%). Un importante 15.4% de los administradores entrevistados no conoce ninguno de los ataques a DNS existentes.

Los ataques a DNS no son bien conocidos por todos los administradores de los servidores de nombres.

Entre los administradores de servidores de nombres que conocen ataques a DNS, los más conocidos son el DNS buffer overflow, el DNS DoS y el DNS spoofing attack.

7.- El 100% de los entrevistados consideran que en general los administradores de DNS no conocen los ataques que se pueden llevar a cabo en contra de la seguridad de los servidores de nombres, ni sus consecuencias, ni la manera de prevenirlos.

El 100% de los entrevistados consideran que en general no existe conocimiento por parte de los administradores de DNS acerca de los ataques a DNS existentes, sus consecuencias ni la manera de prevenirlos.

8.- El 69.2% de los administradores de DNS consideran que las medidas de seguridad que realmente son utilizadas son la restricción de transferencias de zona y la aplicación de parches de BIND, seguidas de la aplicación de parches de sistema operativo con un 61.5%.

Las medidas de seguridad que los administradores de DNS consideran que realmente son utilizadas son la restricción de transferencias de zona, la aplicación de parches de BIND y la aplicación de parches de sistema operativo.

9.- Las medidas de seguridad que los administradores de DNS principalmente conocen y para las cuales conocen la configuración necesaria son la aplicación de parches de sistema operativo, la restricción de queries, la restricción de transferencia de zonas, correr BIND como usuario no privilegiado y la aplicación de parches de BIND.

Son pocas las medidas de seguridad que son realmente utilizadas para proteger servidores de nombres.

10.- El 77% de los entrevistados opinan que la causa principal de los ataques exitosos a la seguridad de los servidores de nombres es la mala administración de los servidores que albergan el DNS.

La causa principal de los ataques exitosos a la seguridad de los servidores de nombres es la mala administración de los servidores que albergan el DNS.

11.- De acuerdo con el 69.2% de los administradores entrevistados, el objetivo principal que se busca al atacar un servidor de nombres es obtener acceso como usuario privilegiado, seguido de la falsificación de páginas web y la obtención de información acerca de los hosts existentes en una red.

El objetivo principal que se busca al atacar un servidor de nombres es obtener acceso como usuario privilegiado.

12.- El 77% de los administradores conocen DNSSEC, mientras el 53.8% conoce TSIG. El 23% no conoce ninguno de estos protocolos de seguridad para DNS.

El protocolo basado en criptografía más conocido para añadir seguridad a un DNS es DNSSEC.

13.- El 69.2% de los administradores no aplican ninguno de los protocolos basados en criptografía y firmas digitales para añadir seguridad a los servidores de nombres. Solamente el 23% aplica DNSSEC y un 7.7% utiliza TSIG.

La mayoría de los administradores de DNS no aplica ninguno de los protocolos basados en criptografía y firmas digitales para añadir seguridad a los servidores de nombres.

14.- La mayoría de los administradores coinciden en que no es popular el uso de protocolos basados en criptografía y firmas digitales para añadir seguridad a los servidores de nombres.

4.13 CONCLUSIONES GENERALES

Para las siguientes conclusiones se tomaron en cuenta las conclusiones a cada respuesta presentadas en el punto anterior, así como las respuestas abiertas proporcionadas en los cuestionarios aplicados y algunos puntos del marco conceptual.

- ♦ La implementación de DNS más conocida y utilizada entre los administradores de servidores de nombres es BIND en su versión 8.X

- ◆ Debido a que el DNS proporciona el servicio de mapeo de nombres a direcciones IP, es de vital importancia para el correcto funcionamiento de los servicios que se proporcionan en Internet, por lo que es necesario implementar medidas de seguridad que garanticen la autenticidad, integridad y confiabilidad de la información que proporcionan.
- ◆ Existen varios ataques que pueden realizarse a la seguridad de un DNS, sin embargo, no todos los administradores de servidores de nombres conocen en que consisten ni las medidas de seguridad existentes para prevenirlos.
- ◆ La mala administración de los servidores que albergan los DNS, la mala administración de los servidores de nombres mismos y las múltiples vulnerabilidades existentes en las implementaciones del servicio de nombres, son las causas principales de los ataques exitosos a la seguridad de los DNS, provocando:
 - El acceso no autorizado de intrusos con privilegios de root.
 - La falsificación de páginas web.
 - La obtención de información acerca de los hosts y servicios que proporciona una red.
 - La negación de servicio.
- ◆ Existen protocolos basados en criptografía y firmas digitales para añadir seguridad a la operación del Sistema de Nombres de Dominio, sin embargo, estos protocolos son pocos conocidos y utilizados por los administradores de servidores de nombres.

4.14 APROBACIÓN O DESAPROBACIÓN DE LA HIPÓTESIS

La hipótesis definitiva presentada en el punto 4.3 de este trabajo es:

"Un servidor de nombres sin medidas de seguridad, puede ocasionar la falsificación, desviación y negación de servicios en Internet, así como la interceptación y el robo de información acerca de los hosts y servicios que proporciona una red, afectando la seguridad de dichos servicios, la integridad del espacio de nombres de dominio y la imagen de las organizaciones" .

Basándose en los temas desarrollados en el marco conceptual y principalmente en las respuestas obtenidas al cuestionario aplicado en este marco metodológico podemos afirmar que:

Un servidor de nombres sin medidas de seguridad...

- ◆ si puede ocasionar la falsificación, desviación y negación de servicios en Internet.
- ◆ Si puede ocasionar la interceptación y el robo de información acerca de los hosts y servicios que proporciona una red.

Con esto se pone en riesgo la seguridad de los servicios que se encuentran disponibles a través de Internet así como la confiabilidad en el espacio de nombres de dominio.

La imagen de las organizaciones si se puede ver dañada al explotarse la falta de seguridad en el servidor de nombres que da información acerca de sus servicios

Por lo tanto, la hipótesis definitiva propuesta para presentar la presente tesis, es válida.

CAPÍTULO 5

MARCO INSTRUMENTAL

5.1 PROPUESTAS DE ACCIÓN

Con el fin de dar a conocer este trabajo, se proponen las siguientes acciones:

- A. Publicación del trabajo completo en Internet, a través de la página del Centro de Información de RedUNAM. ([http:// www.nic.unam.mx](http://www.nic.unam.mx))
- B. Impartir el taller de "Seguridad en DNS" como parte del diplomado de seguridad que da la UNAM a través del CEM-Polanco.
- C. Publicación de este trabajo de tesis adecuándolo a un libro.

5.2 PLAN Y PROGRAMA DE TRABAJO

- A. Publicación del trabajo completo en Internet.

Se le pedirá directamente al coordinador del Centro de Información de RedUNAM, la publicación del presente trabajo en la sección de "documentos" de su página web. La publicación será en formato PDF con el fin de que no pueda ser alterado su contenido.

- B. Impartir el taller de "Seguridad en DNS"

En el CEM-Polanco (UNAM) se imparte el diplomado "Seguridad informática", en el cuál participan como instructores distinguidos doctores y maestros en ciencias de la computación. Como parte complementaria al diplomado se han organizado una serie de talleres con el fin de aplicar los conocimientos teóricos adquiridos.

Anteriormente se propuso al comité académico del diplomado la creación de un taller de Seguridad en DNS y este fue aceptado. Se retomarán las pláticas con el comité para establecer las condiciones a cumplir para que este taller pueda impartirse en próximas fechas.

- C. Después de titulada y merecida la aprobación del contenido de esta tesis, realizaré la búsqueda del mejor medio para su publicación como libro.

ANEXOS

ANEXO 1

**CUESTIONARIO APLICADO EN EL MARCO
PROBLEMÁTICO**

CUESTIONARIO APLICADO A PERSONAS EMPÍRICAS

Nombre: Genny Marisol León Leal

Empresa o Institución: DGSCA-Operación de la red.

1.- ¿Qué implementaciones del Sistema de Nombres de Dominio (DNS) conoce?.

R = DNS para Windows NT y DNS para UNIX.

2.- ¿Considera que el buen funcionamiento de los servidores de nombres es un factor importante para garantizar la disponibilidad de los servicios que proporciona Internet?. Si, no, ¿por qué?.

R = Si, ya que sin un buen funcionamiento no se podría acceder por nombre no sólo a páginas web, sino también implica el no poder acceder a los hosts o servidores de correo. Esto traería grandes consecuencias ya que en Internet todas las páginas son accedidas por nombre, por lo tanto es de vital importancia tener un buen funcionamiento en los DNS.

3.- ¿Qué tipos de ataques a la seguridad de un servidor de nombres conoce?.

R = Negación del servicio, acceso a máquinas como root, suplantación de identidad.

4.- Desde su punto de vista, ¿qué consecuencias traería un ataque exitoso a la seguridad de un servidor de nombres?.

R = Podría ser borrada toda la base de datos del servidor de nombres dejándolo inhabilitado, crear nuevos dominios o incluso nuevos registros. Apuntar las direcciones IP a otros dominios que posiblemente podrían ser páginas pornográficas.

5.- Mencione las medidas de seguridad que deben implementarse en un servidor de nombres.

R = Autenticación, control de acceso, integridad de datos, cifrado de datos, confidencialidad.

6.- De las anteriores medidas de seguridad, ¿cuáles ha implementado en servidores de nombres administrados por usted?.

R = La autenticación, control de acceso, jaulas (aunque esta se encuentra en pruebas).

7.- ¿Conoce sitios web dedicados o relacionados a la seguridad en los servidores de nombres? ¿Cuáles?.

R = No conozco que exista algún sitio dedicado a la seguridad de los servidores de nombres.

8.- ¿Conoce libros dedicados o relacionados a la seguridad en los servidores de nombres? ¿Cuáles?

R = No, tengo entendido que sólo existen dos libros "DNS and BIND" y "DNS for Windows NT", pero ninguno dedicado exclusivamente a la seguridad de los servidores de nombres.

Nombre: Ivette De Luna Bonilla

Empresa o Institución: Ericsson

1.- ¿Qué implementaciones del Sistema de Nombres de Dominio (DNS) conoce?.

R = Dos, BIND y DNS como uno de los servicios que incluye Windows NT.

2.- ¿Considera que el buen funcionamiento de los servidores de nombres es un factor importante para garantizar la disponibilidad de los servicios que proporciona Internet?. Si, no, ¿por qué?.

R = Sí, pues el acceso a los servicios gira alrededor del servicio de nombres.

3.- ¿Qué tipos de ataques a la seguridad de un servidor de nombres conoce?.

R = Alteración o eliminación de registros de la base de datos de un servidor.

4.- Desde su punto de vista, ¿qué consecuencias traería un ataque exitoso a la seguridad de un servidor de nombres?.

R = Considerando la respuesta anterior, habría servicios de Internet inaccesibles o bien, falsos.

5.- Mencione las medidas de seguridad que deben implementarse en un servidor de nombres.

R = Restricción de acceso remoto, local, de consultas y de transferencias de la base de datos.

6.- De las anteriores medidas de seguridad, ¿cuáles ha implementado en servidores de nombres administrados por usted?.

R = Todas

7.- ¿Conoce sitios web dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?

R = www.isc.org, www.dns.net

8.- ¿Conoce libros dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?

R = DNS & BIND de O'Reilly

Nombre: Yazmin Castillo Martínez

Empresa o Institución: Instituto Nacional de Antropología e Historia

1.- ¿Qué implementaciones del Sistema de Nombres de Dominio (DNS) conoce?.

R = Conozco la implementación de un DNS primario y secundario.

2.- ¿Considera que el buen funcionamiento de los servidores de nombres es un factor importante para garantizar la disponibilidad de los servicios que proporciona Internet?. Si, no, ¿por qué?.

R = Así es, porque sin un servidor de nombres no podemos tener el servicio de Internet por lo menos a través de los nombres que se manejan en Internet, ya que al hacerlo tan sólo por IP sería ineficiente, lento e inseguro. Su buen funcionamiento nos llevaría a que el servicio sea rápido y seguro.

3.- ¿Qué tipos de ataques a la seguridad de un servidor de nombres conoce?.

R = Se de los llamados exploit que matan el proceso named y cuando manipulan la información del servidor como falsa a través del robo de los paquetes.

4.- Desde su punto de vista, ¿qué consecuencias traería un ataque exitoso a la seguridad de un servidor de nombres?.

R = Para comenzar información falsa, porque podría ser que los nombres de dominio apunten a direcciones incorrectas, esto propiciaría desconfianza por parte de los usuarios, descontentos.

5.- Mencione las medidas de seguridad que deben implementarse en un servidor de nombres.

R = Para empezar, la seguridad del propio servidor, utilizar encriptación (ssh, tcp-wrappers, etc), no utilizar más que los puertos necesarios y bloquear lo demás. Dentro del DNS manejar listas de acceso, ya sea para ejecutar queries, transferencias, etc).

6.- De las anteriores medidas de seguridad, ¿cuáles ha implementado en servidores de nombres administrados por usted?.

R = Estoy trabajando actualmente en la seguridad del servidor de nombres, pienso implementar las antes mencionadas.

7.- ¿Conoce sitios web dedicados o relacionados a la seguridad en los servidores de nombres? ¿Cuáles?

R = <http://www.hut.fi/~sasu/Tturvae/document/>
<http://www.toad.com/~dnssec/>
http://www.sans.org/infosecFAQ/firewall/DNS_sec.htm

8.- ¿Conoce libros dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?.

R = Libros: DNS and BIND de Paul Albitz & Cricket Liu

CUESTIONARIO APLICADO A PERSONAS PROFESIONALES

Nombre: Jorge Alberto Martínez Melo
Empresa o Institución: NICunam

1.- ¿Qué implementaciones del Sistema de Nombres de Dominio (DNS) conoce?.

R = BIND, Microsoft DNS Manager.

2.- ¿Considera que el buen funcionamiento de los servidores de nombres es un factor importante para garantizar la disponibilidad de los servicios que proporciona Internet?. Si, no, ¿por qué?.

R = Claro que si, en realidad creo que es algo tan esencial que mucha gente ni siquiera se entera de su existencia. Lo cierto es que simplifican la conexión entre usuarios de Internet. Ya más a profundidad podemos encontrar que muchas aplicaciones hacen validaciones para autenticar conexiones basándose en el DNS.

3.- ¿Qué tipos de ataques a la seguridad de un servidor de nombres conoce?.

R = Existen muchos y muy variados.

4.- Desde su punto de vista, ¿qué consecuencias traería un ataque exitoso a la seguridad de un servidor de nombres?.

R = Causaría problemas en cuanto a la ubicación de máquinas dentro de la red. De igual forma que existen ataques en específico para un DNS también el mismo DNS puede ayudar a un atacante a establecer estrategias dañinas.

5.- Mencione las medidas de seguridad que deben implementarse en un servidor de nombres.

R = Primero implementar las herramientas mínimas de seguridad a un servidor UNIX cualquiera. En cuanto a DNS hay varias cosas por hacer, por citar algunas se tiene que: hacer lista de acceso para transferencia de zonas y queries, restringir desplegar la versión de BIND, deshabilitar el *glue*, firmar zonas, hacer las transferencias cifradas, correr el proceso *named* en una jaula y bajo un usuario no privilegiado, etc, etc. De lo que siempre debemos preocuparnos es mantener actualizada la versión.

6.- De las anteriores medidas de seguridad, ¿cuáles ha implementado en servidores de nombres administrados por usted?.

R = Todas

7.- ¿Conoce sitios web dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?

R = www.isc.org
www.dns.net

8.- ¿Conoce libros dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?

R = DNS and BIND
Domain Name Handbook

Nombre: Francisco Arias Correa
Empresa o Institución: NIC-México

1.- ¿Qué implementaciones del Sistema de Nombres de Dominio (DNS) conoce?

R = BIND y Microsoft DNS.

2.- ¿Considera que el buen funcionamiento de los servidores de nombres es un factor importante para garantizar la disponibilidad de los servicios que proporciona Internet?. Si, no, ¿por qué?

R = Sí, por supuesto; si consideramos que la inmensa mayoría de los usuarios de Internet son personas que no te podrían acceder un sitio si no funcionan los nombres.

3.- ¿Qué tipos de ataques a la seguridad de un servidor de nombres conoce?

R = Negación de servicio; buffer overflows por bugs en el código del servidor; information leakage por mala configuración en el servidor (allow-transfer, allow-query, etc.) y DNS spoofing.

4.- Desde su punto de vista, ¿qué consecuencias traería un ataque exitoso a la seguridad de un servidor de nombres?

R = Depende del servidor y la información que se comprometa. Si se comprometiera la zona "root", por ejemplo, sería un caos en el Internet, si se compromete el DNS que da servicio a los clientes de un ISP, se puede generar un caos para los clientes del ISP nada más, y así sucesivamente.

5.- Mencione las medidas de seguridad que deben implementarse en un servidor de nombres.

R = Adecuada configuración para prevenir fugas de información (information leakage), mantenerse al tanto con los parches para el servidor de DNS, implementar (si es posible) el "DNS enjaulado".

6.- De las anteriores medidas de seguridad, ¿cuáles ha implementado en servidores de nombres administrados por usted?.

R = Todas.

7.- ¿Conoce sitios web dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?.

R = <http://www.isc.org/>
<http://www.acmebw.com/>
<http://www.dns.net/dnsrd/>

8.- ¿Conoce libros dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?.

R = DNS & BIND de Paul Albitz y CRIQUET Liu, 4 ed.

Nombre: Gunnar Wolf

**Empresa o Institución: FES Iztacala y Departamento de Seguridad en
Cómputo - DGSCA - UNAM**

1.- ¿Qué implementaciones del Sistema de Nombres de Dominio (DNS) conoce?.

R = BIND, DJBDNS, TinyDNS.

2.- ¿Considera que el buen funcionamiento de los servidores de nombres es un factor importante para garantizar la disponibilidad de los servicios que proporciona Internet?. Si, no, ¿por qué?.

R = Sí

3.- ¿Qué tipos de ataques a la seguridad de un servidor de nombres conoce?.

R = Envenenamiento de caché, suplantación, ataques al demonio (negación de servicio, desbordamientos de pila).

4.- Desde su punto de vista, ¿qué consecuencias traería un ataque exitoso a la seguridad de un servidor de nombres?.

R = Dependiendo del tipo de ataque, desde perder visibilidad del dominio temporalmente hasta una intrusión completa en los servidores.

5.- Mencione las medidas de seguridad que deben implementarse en un servidor de nombres.

R = chroot, configurar estrictamente acorde con la naturaleza del dominio, estar al día con actualizaciones, pruebas de penetración, etc.

6.- De las anteriores medidas de seguridad, ¿cuáles ha implementado en servidores de nombres administrados por usted?

R = Todas ellas en diferentes momentos.

7.- ¿Conoce sitios web dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?

No respondió.

8.- ¿Conoce libros dedicados o relacionados a la seguridad en los servidores de nombres?. ¿Cuáles?

No respondió.

ANEXO 2

MODELO OSI, TCP/IP Y DIRECCIONAMIENTO IP

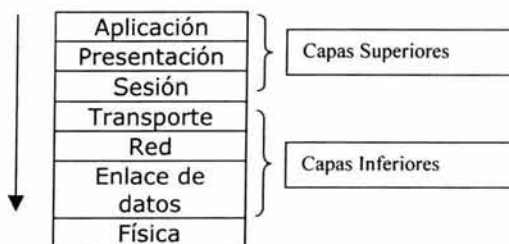
EL MODELO DE COMUNICACIONES DE DATOS OSI

OSI ("Open Systems Interconnect") es un modelo conceptual desarrollado por la Organización de Estándares Internacional, ISO ("International Standards Organization") en 1984 y es utilizado para describir la manera en que las computadoras intercambian información a través de una red. Está compuesto de siete capas, cada una de las cuales definen ciertas funciones que se tienen que llevar a cabo en la comunicación e intercambio de datos en la red.

Las funciones que se definen en cada una de las capas del modelo OSI, pueden llevarse a cabo por uno o varios protocolos.

Un protocolo es una regla formal de comportamiento, y en el contexto de conexión de redes, "un protocolo es un conjunto de reglas formales y convenciones que gobiernan la manera en que las computadoras intercambian información sobre un medio de red"³⁴

Las siete capas que conforman este modelo son:



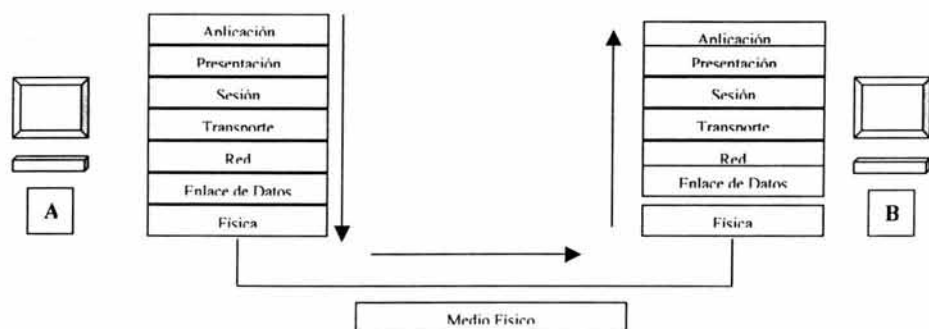
Estas capas están divididas en capas superiores y capas inferiores. Las capas superiores llevan a cabo funciones relacionadas con las aplicaciones y generalmente solo están implementadas en software. Las funciones de las capas inferiores tienen que ver con el transporte de datos y algunas están implementadas en software y otras en hardware.

Cada capa tiene interacción directa con tres más, la capa que se encuentra arriba de ella, la que se encuentra debajo y con su misma capa pero en el sistema remoto.

En la transmisión de información de un sistema a otro, los datos bajan por cada una de las capas del sistema local para llegar al medio físico a través de cual viajarán hasta llegar al sistema remoto, donde empezarán a subir hasta

³⁴ Referencia 13, página 4.

llegar a la capa correspondiente. Por ejemplo, si un software que se encuentra en la capa de aplicación de un sistema A necesita enviar información a la capa de aplicación de un sistema B, debe pasar la información a la capa de presentación, esta a su vez a la capa de sesión y así hasta llegar a la capa física la cual pondrá los datos en el medio físico. Al llegar la información al sistema B, la capa física tomará los datos y los pasará a la capa de enlace de datos y así sucesivamente hasta llegar a la capa de aplicación.



Al bajar los datos por cada una de las capas, se le va agregando cierta información de control que le será de utilidad a la misma capa pero en el sistema remoto. "La información de control generalmente toma una de dos formas: headers o trailers. Los headers son agregados al principio de los datos que son pasados hacia abajo por capas superiores. Los trailers son agregados al final de los datos que son pasados hacia abajo por capas superiores"³⁵.

Cuando una capa recibe el header, los datos y trailer de una capa superior, los toma todos como datos y les pega su propio header y trailer. Cuando una capa recibe información de una capa inferior, le quita sólo el header y trailer que le corresponden y pasa los datos restantes a la capa superior. De esta manera, los datos de una capa pueden contener varios headers, datos y trailers de capas superiores, lo cual se conoce como "encapsulación".

El manejar varias capas en el modelo OSI permite la creación o modificación de los protocolos que las forman sin necesidad de cambiar todo el modelo. Las características de cada una de las siete capas son:

³⁵ Referencia 13, página 6.

CAPA FÍSICA

La capa física define las especificaciones que deben tener los medios por los cuales estarán unidos los medios de comunicaciones. "Las especificaciones de la capa física definen características tales como niveles de voltaje, sincronización de cambios de voltaje, tasas de datos física, distancias máximas de transmisión y conectores físicos"³⁶. Algunos ejemplos de implementaciones en esta capa son los estándares de red Ethernet, Token Ring y FDDI.

CAPA DE ENLACE DE DATOS

Esta capa permite que la transmisión de datos en una red física sea confiable. Las especificaciones de esta capa "definen diferentes características de red y protocolos, incluyendo el direccionamiento físico, la topología de red, notificación de errores, secuencia de frames y control de flujo"³⁷. El direccionamiento físico se refiere a la manera en que están direccionados los dispositivos en esta capa y la topología de red a la forma en que están físicamente conectados. Las notificaciones de error sirven para alertar a los protocolos de capas superiores cuando ha ocurrido un error en la transmisión y la secuencia de frames ordena los paquetes de información cuando estos han sido transmitidos en desorden. Por último el control de flujo permite que los dispositivos no se sobre carguen recibiendo mas paquetes de información que los que puede procesar a la vez.

CAPA DE RED

Esta capa provee los servicios de ruteo de datos y otros relacionados. Estos servicios se llevan cabo por medio del direccionamiento lógico (no físico como en la capa de enlace de datos) de los dispositivos, es decir, existe un esquema de asignación de direcciones para cada uno de los dispositivos conectados a la red.

CAPA DE TRANSPORTE

La capa de transporte asegura que al dispositivo receptor le lleguen los datos exactamente como le fueron enviados. Las funciones de esta capa "típicamente incluyen control de flujo, multiplexaje, manejo de circuitos virtuales y chequeo de errores y recuperación de datos"³⁸.

³⁶ Referencia 13, página 7.

³⁷ Referencia 13, página 8.

³⁸ Referencia 13, página 9.

CAPA DE SESIÓN

Las aplicaciones al comunicarse de un sistema local a uno remoto, deben establecer sesiones de comunicación, las cuales consisten en peticiones y respuestas de servicio. El establecimiento, manejo y terminación de estas sesiones se llevan a cabo en la capa de sesión del modelo OSI.

CAPA DE PRESENTACIÓN

En esta capa se incluyen los formatos de caracteres, esquemas de compresión y de cifrado de datos que permiten que la información enviada por una computadora local pueda ser leída en la computadora remota. "La capa de presentación provee una variedad de funciones de codificación y conversión que son aplicadas a los datos de la capa de aplicación"³⁹.

CAPA DE APLICACIÓN

Es la capa en donde se encuentra el software con el que interactúa directamente el usuario y que incluyen funciones de comunicación a través de la red.

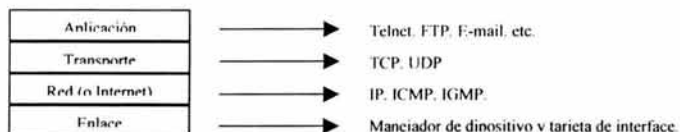
TCP/IP

TCP/IP ("Transmission Control Protocol / Internet Protocol") es un conjunto de protocolos utilizados para la comunicación de computadoras en Internet sin importar su plataforma o sistema operativo.

Generalmente los protocolos están agrupados en familias (también conocidas como suites o stacks). La familia de protocolos de TCP/IP está formada por protocolos como IP ("Internet Protocol"), ARP ("Address Resolution Protocol"), ICMP("Internet Control Message Protocol"), UDP ("User Datagram Protocol"), TCP("Transport Control Protocol"), RIP ("Routing Information Protocol"), DNS("Domain Name System"), etc.

Cada uno de estos protocolos lleva a cabo una o varias funciones especificadas en el modelo de comunicaciones OSI, aunque a diferencia de este, TCP/IP tiene cuatro capas.

³⁹ Referencia 13, página 10.



CAPA DE APLICACIÓN

En esta capa se manejan todos los detalles concernientes a las aplicaciones de uso común en Internet, tales como telnet para acceso a sistemas remotos, FTP para transferencia de archivos, SMTP para envío de correo electrónico, etc.

CAPA DE TRANSPORTE

La capa de transporte está formada por dos protocolos que permite el flujo de datos entre dos computadoras. Estos protocolos son conocidos como TCP ("Transmission Control Protocol") y UDP ("User Datagram Protocol").

TCP es un protocolo que proporciona un flujo de datos confiable ya que en el envío de paquetes, espera cierto tiempo para recibir un acuse de recibo por parte del equipo remoto para poder enviar los siguientes, y en caso de no recibir la notificación correspondiente los reenvía hasta asegurarse que han sido recibidos.

UDP por otro lado, solo envía los paquetes sin asegurarse de que han sido recibidos en el equipo remoto, por lo que cualquier confiabilidad deseada debe ser agregada por la capa de aplicación.

CAPA DE RED (O INTERNET)

Es la capa que se encarga del manejo de paquetes a través de la red. La forman protocolos como IP ("Internet Protocol"), ICMP ("Internet Control Message Control") e IGMP (Internet Group Management Protocol").

CAPA DE ENLACE

También es llamada capa de enlace de datos o capa de interface de red y normalmente incluye a la tarjeta de red y al manejador de esta interface que esta contenido en el sistema operativo

PROCOLO IP

IP (Internet Protocol) es un protocolo de la capa 3 de la suite de protocolo TCP/IP que contiene información acerca del direccionamiento e información de control que permite el enrutamiento de paquetes en Internet. Este protocolo es el principal de la capa de red y junto con TCP representa el corazón de los protocolos que hacen posible la comunicación de los miles de hosts conectados a Internet.

El protocolo de Internet, tiene dos funciones principales; la primera, es ofrecer la entrega de datagramas de manera óptima y la segunda es fragmentar y reensamblar dichos datagramas para poder soportar transmisiones de datos mayores a los MTU (Maximun Transmission Unit)

Un paquete IP está compuesto de varios campos que se describen a continuación:

- ◆ Versión.- Indica la versión de IP actualmente en uso.
- ◆ IHL.- Indica la longitud del encabezado del datagrama en conjuntos de 32 bits.
- ◆ Tipo de servicio.- Especifica cómo desea un protocolo de las capas superiores que se maneje el datagrama. Se asignan diferentes niveles de acuerdo a su importancia.
- ◆ Longitud total.- Especifica la longitud, en bytes, del paquete IP total, incluyendo los datos y el encabezado.
- ◆ Identificación.- Consta de un número entero que identifica el datagrama actual. Este campo se utiliza para ayudar a reconstruir los fragmentos del datagrama.
- ◆ Apuntadores.- Consta de un campo de 3 bits entre los cuales los 2 bits de menor orden (los menos significativos) controlan la función de fragmentación. El bit de menor orden especifica si se puede fragmentar el paquete. El bit de en medio especifica si el paquete es el último fragmento en una serie de paquetes fragmentados. El tercer bit, o bit de mayor orden, no se usa.
- ◆ Desplazamiento del fragmento.- Indica la posición de los datos del fragmento en relación con el comienzo de los datos en el datagrama original, lo cual permite que el proceso IP del destino reconstruya adecuadamente el datagrama original.
- ◆ Tiempo de vida.- Conserva un contador que disminuye gradualmente hasta llegar a cero, donde se elimina. Esto evita que los paquetes circulen en ciclo de manera indefinida.

- ◆ Protocolo.- Indica que protocolo de las capas superiores recibe los paquetes entrantes una vez terminado el procesamiento IP.
- ◆ Suma de verificación del encabezado.- Ayuda a asegurar la integridad del encabezado IP.
- ◆ Dirección origen.- Especifica el nodo emisor.
- ◆ Dirección destino.- Especifica el nodo receptor.
- ◆ Opciones.- Permite que el protocolo IP soporte varias opciones como la seguridad.
- ◆ Datos.- Contiene información de las capas superiores.

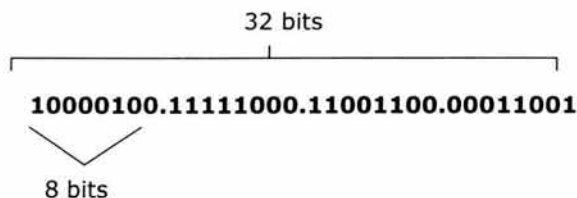
DIRECCIONAMIENTO IP

Dentro de las redes que trabajan con TCP/IP, debe existir un esquema que permita asignar un identificador único a cada host conectado a la red. De este esquema se encarga la capa de transporte a través del protocolo IP.

Como ya se mencionó anteriormente, el paquete IP está formado de varios campos, dos de los cuáles hacen referencia a direcciones numéricas conocidas como direcciones IP.

Una dirección IP es precisamente el identificar único que va a distinguir a cada una de las máquinas que se encuentran conectadas a la red TCP/IP y tiene una longitud de 32 bits.

“La dirección IP de 32 bits se agrupa en 8 bits a un mismo tiempo, separados por puntos y representados en formato decimal (conocidos como notación decimal de puntos).”⁴⁰



Cada uno de los octetos tiene un valor binario, que debe traducirse a su valor decimal para poder formar la dirección IP.

⁴⁰ Referencia 2, página 369.

10000100.11111000.11001100.00011001

10000100 = 132

11111000 = 248

11001100 = 204

00011001 = 25

Por lo tanto,

10000100.11111000.11001100.00011001 **(Notación binaria)**

es igual a

132.248.204.25 **(Notación decimal)**

Una dirección IP se divide en dos campos: el identificador de la red (NETid) y el identificador del host (HOSTid). Dependiendo de la longitud en bits de cada uno de estos identificadores, será la clase de red a la que pertenece la dirección IP.

Existen 5 clases de direcciones IP:

Clase A

NETid = 8 bits

HOSTid = 24 bits

El primer octeto debe comenzar con 0 (binario):

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

De esta manera, las posibles combinaciones en binario para el NETid van del 00000001 (1) al 011111110 (126). Por lo tanto, el rango de direcciones IP clase A es:

1.0.0.0 al 126.255.255.255

La red 127.0.0.0 no se toma en cuenta ya que está reservada para uso especial.

Clase B

NETid = 16 bits

HOSTid = 16 bits

El primer octeto debe comenzar con 10 (binario):

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

De esta manera, las posibles combinaciones en binario para el NETid van del 10000000.00000001 (128.1) al 10111111.11111111 (191.255). Por lo tanto, el rango de direcciones IP clase B es:

128.1.0.0 al 191.255.255.255

Clase C

NETid = 24 bits

HOSTid = 8 bits

El primer octeto debe comenzar con 110 (binario):

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

De esta manera, las posibles combinaciones en binario para el NETid van del 11000000.00000000.00000000 (192.0.0) al 11011111.11111111.11111111 (223.255.255). Por lo tanto, el rango de direcciones IP clase C es:

192.0.0.0 al 223.255.255.255

Clase D y Clase E

La clase D son direcciones IP reservadas para aplicaciones de multicast y la clase E no está en uso.

ANEXO 3

ISO 3166-1

La siguiente tabla presenta los códigos de dos letras utilizados en los nombres de dominio de nivel superior. Estos códigos están basados en el estándar ISO 3166-1.

Código	País
ac	Ascension Island
ad	Andorra
ae	United Arab Emirates
af	Afghanistan
ag	Antigua and Barbuda
ai	Anguilla
al	Albania
am	Armenia
an	Netherlands Antilles
ao	Angola
aq	Antarctica
ar	Argentina
as	American Samoa
at	Austria
au	Australia
aw	Aruba
az	Azerbaijan
ba	Bosnia and Herzegovina
bb	Barbados
bd	Bangladesh
be	Belgium
bf	Burkina Faso
bg	Bulgaria
bh	Bahrain
bi	Burundi
bj	Benin
bm	Bermuda
bn	Brunei Darussalam
bo	Bolivia
br	Brazil
bs	Bahamas
bt	Bhutan
bv	Bouvet Island
bw	Botswana
by	Belarus
bz	Belize
ca	Canada
cc	Cocos (Keeling) Islands
cd	Congo, Democratic Republic of the

cf	Central African Republic
cg	Congo, Republic of
ch	Switzerland
ci	Cote d'Ivoire
ck	Cook Islands
cl	Chile
cm	Cameroon
cn	China
co	Colombia
cr	Costa Rica
cu	Cuba
cv	Cap Verde
cx	Christmas Island
cy	Cyprus
cz	Czech Republic
de	Germany
dj	Djibouti
dk	Denmark
dm	Dominica
do	Dominican Republic
dz	Algeria
ec	Ecuador
ee	Estonia
eg	Egypt
eh	Western Sahara
er	Eritrea
es	Spain
et	Ethiopia
fi	Finland
fj	Fiji
fk	Falkland Islands (Malvina)
fm	Micronesia, Federal State of
fo	Faroe Islands
fr	France
ga	Gabon
gd	Grenada
ge	Georgia
gf	French Guiana
gg	Guernsey
gh	Ghana
gi	Gibraltar
gl	Greenland
gm	Gambia
gn	Guinea

gp	Guadeloupe
gq	Equatorial Guinea
gr	Greece
gs	South Georgia and the South Sandwich Islands
gt	Guatemala
gu	Guam
gw	Guinea-Bissau
gy	Guyana
hk	Hong Kong
hm	Heard and McDonald Islands
hn	Honduras
hr	Croatia/Hrvatska
ht	Haiti
hu	Hungary
id	Indonesia
ie	Ireland
il	Israel
im	Isle of Man
in	India
io	British Indian Ocean Territory
iq	Iraq
ir	Iran (Islamic Republic of)
is	Iceland
it	Italy
je	Jersey
jm	Jamaica
jo	Jordan
jp	Japan
ke	Kenya
kg	Kyrgyzstan
kh	Cambodia
ki	Kiribati
km	Comoros
kn	Saint Kitts and Nevis
kp	Korea, Democratic People's Republic
kr	Korea, Republic of
kw	Kuwait
ky	Cayman Islands
kz	Kazakhstan
la	Lao People's Democratic Republic
lb	Lebanon
lc	Saint Lucia
li	Liechtenstein
lk	Sri Lanka

lr	Liberia
ls	Lesotho
lt	Lithuania
lu	Luxembourg
lv	Latvia
ly	Libyan Arab Jamahiriya
ma	Morocco
mc	Monaco
md	Moldova, Republic of
mg	Madagascar
mh	Marshall Islands
mk	Macedonia, Former Yugoslav Republic
ml	Mali
mm	Myanmar
mn	Mongolia
mo	Macau
mp	Northern Mariana Islands
mq	Martinique
mr	Mauritania
ms	Montserrat
mt	Malta
mu	Mauritius
mv	Maldives
mw	Malawi
mx	Mexico
my	Malaysia
mz	Mozambique
na	Namibia
nc	New Caledonia
ne	Niger
nf	Norfolk Island
ng	Nigeria
ni	Nicaragua
nl	Netherlands
no	Norway
np	Nepal
nr	Nauru
nu	Niue
nz	New Zealand
om	Oman
pa	Panama
pe	Peru
pf	French Polynesia
pg	Papua New Guinea

ph	Philippines
pk	Pakistan
pl	Poland
pm	St. Pierre and Miquelon
pn	Pitcairn Island
pr	Puerto Rico
ps	Palestinian Territories
pt	Portugal
pw	Palau
py	Paraguay
qa	Qatar
re	Reunion Island
ro	Romania
ru	Russian Federation
rw	Rwanda
sa	Saudi Arabia
sb	Solomon Islands
sc	Seychelles
sd	Sudan
se	Sweden
sg	Singapore
sh	St. Helena
si	Slovenia
sj	Svalbard and Jan Mayen Islands
sk	Slovak Republic
sl	Sierra Leone
sm	San Marino
sn	Senegal
so	Somalia
sr	Suriname
st	Sao Tome and Principe
sv	El Salvador
sy	Syrian Arab Republic
sz	Swaziland
tc	Turks and Caicos Islands
td	Chad
tf	French Southern Territories
tg	Togo
th	Thailand
tj	Tajikistan
tk	Tokelau
tm	Turkmenistan
tn	Tunisia
to	Tonga

tp	East Timor
tr	Turkey
tt	Trinidad and Tobago
tv	Tuvalu
tw	Taiwan
tz	Tanzania
ua	Ukraine
ug	Uganda
uk	United Kingdom
um	US Minor Outlying Islands
us	United States
uy	Uruguay
uz	Uzbekistan
va	Holy See (City Vatican State)
vc	Saint Vincent and the Grenadines
ve	Venezuela
vg	Virgin Islands (British)
vi	Virgin Islands (USA)
vn	Vietnam
vu	Vanuatu
wf	Wallis and Futuna Islands
ws	Western Samoa
ye	Yemen
yt	Mayotte
yu	Yugoslavia
za	South Africa
zm	Zambia
zw	Zimbabwe

ANEXO 4

**CUESTIONARIO APLICADO EN EL MARCO
METODOLÓGICO**

FORMATO DEL CUESTIONARIO (PILOTO)

Instrucciones: Favor de contestar las siguientes preguntas. En caso de que la pregunta no sea lo suficientemente clara, considere que es confusa o que debería cambiarse la redacción, favor de indicarlo. Gracias.

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- () BIND
 () DNS de Microsoft
 () DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- | | |
|----------------------|---------------|
| () BIND | versión _____ |
| () DNS de Microsoft | versión _____ |
| () DJBDNS | versión _____ |

3.- ¿Por qué razón utiliza esa implementación de DNS?.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

- () Muy importante _____

- () Mas o menos importante _____

- () Poco importante _____

() No es importante _____

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- () DNS spoofing attack
- () DNS buffer overflow
- () DNS Denial of Service attack
- () Client flooding
- () Dynamic updates vulnerabilities

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

() Si, porque _____

() No, porque _____

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- () Ocultar versión de BIND
- () Restricción de queries
- () Restricción de transferencias de zonas
- () Correr BIND como usuario no-root o no privilegiado.
- () Split function name servers. Dos servidores de nombres.
- () DNS enjaulado.
- () Aplicación de parches de BIND
- () Aplicación de parches de sistema operativo.
- () DNSSEC
- () TSIG
- () Restricción de actualizaciones automáticas
- () Desactivación de recursión
- () Ninguna
- () Otra: _____

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado.
- Split function name servers. Dos servidores de nombres.
- DNS enjaulado.
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo.
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
 - Vulnerabilidades del sistema operativo
 - Mala administración del servidor que alberga el DNS
 - Mala configuración del servidor de nombres
 - Otra: (especifique) _____
-
-

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
 - Robo de correo electrónico
 - Falsificación de páginas web
 - Obtener información acerca de los hosts de una red
 - Creación de registros
 - Desvío de transferencias de archivos
 - Obtener acceso como usuario root
 - Otro: (especifique) _____
-
-

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

Si, por que _____

No, porque _____

FORMATO DEL CUESTIONARIO (DEFINITIVO)

Nombre:

Empresa o institución:

Cargo:

El objetivo del presente cuestionario es, conocer la opinión de personas expertas en la administración de DNS, acerca de algunos aspectos de seguridad en el Sistema de Nombres de Dominio.

Instrucciones: Favor de contestar las siguientes preguntas. En caso de que la pregunta no sea lo suficientemente clara, o considere que la redacción es confusa, favor de indicarlo. Gracias.

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- () BIND
 () DNS de Microsoft
 () DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- () BIND versión _____
 () DNS de Microsoft versión _____
 () DJBDNS versión _____

3.- ¿Por qué razón utiliza esa implementación de DNS?.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

- () Muy importante _____
-

() Más o menos importante _____

() Poco importante _____

() No es importante _____

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- () DNS spoofing attack
- () DNS buffer overflow
- () DNS Denial of Service attack
- () Client flooding
- () Dynamic updates vulnerabilities
- () Otro

7.- Considera usted, que en general los administradores de DNS, concen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

() Si, porque _____

() No, porque _____

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- () Ocultar versión de BIND
- () Restricción de queries
- () Restricción de transferencias de zonas
- () Correr BIND como usuario no-root o no privilegiado.
- () Split function name servers. Dos servidores de nombres.
- () DNS enjaulado.
- () Aplicación de parches de BIND

-
- Aplicación de parches de sistema operativo.
 - DNSSEC
 - TSIG
 - Restricción de actualizaciones automáticas
 - Desactivación de recursión
 - Ninguna
 - Otra: _____

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado.
- Split function name servers. Dos servidores de nombres.
- DNS enjaulado.
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo.
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
 - Vulnerabilidades del sistema operativo
 - Mala administración del servidor que alberga el DNS
 - Mala configuración del servidor de nombres
 - Otra: (especifique) _____
-
-

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos

Obtener acceso como usuario root

Otro: (especifique) _____

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

DNSSEC

TSIG

Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

DNSSEC

TSIG

Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

Sí, por que _____

No, porque _____

RESPUESTAS OBTENIDAS AL CUESTIONARIO DEFINITIVO

Nombre: Francisco Javier Arias Correa

Empresa o institución: NIC - México

Cargo: Coordinador de Ingeniería

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND
- DNS de Microsoft
- DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- BIND versión: 8.2.5

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Es la más estable, funcional y segura.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Tiene una importancia muy alta puesto que el DNS es quien provee el mapeo de nombres a IP's.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?

- Muy importante, por que:

Por ser el servicio de mapeo de nombres a IP's.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- DNS spoofing attack
- DNS buffer overflow
- DNS Denial of Service attack
- Client flooding
- Dynamic updates vulnerabilities

Otro (especifique): Configuración insegura.

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

No, porque: No los conocen por que en la mayoría de los casos que conozco no se le da importancia al DNS debido a la relativa sencillez con que se pone a funcionar.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra (especifique):

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión

Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra (especifique):

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: No está terminada la especificación (protocolo).

Nombre: Yazmín Castillo Martínez

Empresa o institución: Instituto Nacional de Antropología e Historia

Cargo: Jefe de Departamento (Administración de red)

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND
- DNS de Microsoft
- DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- | | |
|---|-------------------|
| <input checked="" type="checkbox"/> BIND | versión: 8.2.2-P5 |
| <input type="checkbox"/> DNS de Microsoft | versión: |
| <input type="checkbox"/> DJBDNS | versión: |

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Hasta el momento es la única que he manejado y me es sencilla de entender y manejar.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Muchísima, diría que es un servicio primordial para todos aquellos que usamos los servicios de Internet, debido a que un DNS nos proporciona la traducción de direcciones IP a nombre y viceversa nos facilita el trabajo de obtener información en forma rápida.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

Muy importante, por que: Es un servicio que siempre debe estar disponible los 365 días del año por su gran importancia, sin este servicio no podríamos acceder a los servicios en forma rápida y tendríamos que averiguar el nombre asignado a tal dirección IP.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- DNS spoofing attack
- DNS buffer overflow

- (x) DNS Denial of Service attack
- () Client flooding
- () Dynamic updates vulnerabilities
- () Otro (especifique): Sobre el ataque DNS Denial of Service Attack conozco en forma teórica como provenirlo, debido a que no se me ha presentado algún ataque de esta naturaleza. Pero si es importante estar prevenido.

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

() No, porque: Aquí pondría que depende, para aquellos administradores que solo manejan un servidor DNS se les podría facilitar conocer a detalle este tipo de ataques, para aquellos que manejamos de todo es mucho mas difícil, te dedicas a instalarlo, configurarlo y listo, es mas difícil dedicarle más tiempo, eso en caso de que se presente un ataque y entonces si tengas necesariamente que entender el problema y resolverlo.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- () Ocultar versión de BIND
- () Restricción de queries
- (x) Restricción de transferencias de zonas
- (x) Correr BIND como usuario no-root o no privilegiado
- () Split function name servers. Dos servidores de nombres
- () DNS enjaulado
- (x) Aplicación de parches de BIND
- (x) Aplicación de parches de sistema operativo
- () DNSSEC
- () TSIG
- () Restricción de actualizaciones automáticas
- () Desactivación de recursión
- () Ninguna
- () Otra (especifique):

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- () Ocultar versión de BIND
- (x) Restricción de queries
- (x) Restricción de transferencias de zonas
- (x) Correr BIND como usuario no-root o no privilegiado

- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra (especifique):

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

Si, por que: He escuchado y leído sobre DNSSEC, y considerado que es muy popular en la Red, es necesario estar documentado y conocer este tipo de recursos para agregar Seguridad a nuestros servidores.

Nombre: Paul Conde Medina

Empresa o Institución: Secretaría de Hacienda y Crédito Público

Cargo: Desarrollador de aplicaciones

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND
- DNS de Microsoft
- DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- BIND versión 8.2.X
- DNS de Microsoft versión
- DJBDNS versión

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Por el tipo de recursos disponibles en la organización.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Es una materia delicada lo que respecta al DNS, pues es aquí donde es posible encontrar todos los dominios, nombres, hosts disponibles en Internet.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

Muy importante: Para evitar problemas relacionados con relay y spam, que al fin y al cabo, consumen recursos de nuestra organización.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- DNS spoofing attack
- DNS buffer overflow
- DNS Denial of Service attack
- Client flooding
- Dynamic updates vulnerabilities
- Otro

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

No, porque: no todos los administradores de DNS saben la responsabilidad que tienen en sus manos, hay algunos que ni siquiera saben lo que es un "ataque".

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado.
- Split function name servers. Dos servidores de nombres.
- DNS enjaulado.
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo.
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra:

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado.
- Split function name servers. Dos servidores de nombres.
- DNS enjaulado.
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo.
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra: (especifique)

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque DNSSEC esta disponible en la versión 9 y no todos tienen el equipo suficiente para instalarlo.

Nombre: Ivette De Luna Bonilla

Empresa o institución: Ericsson

Cargo: Área de datos y ex-integrante del Centro de Información de RedUNAM.

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- DNS de Microsoft

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Por estándar, todo se trabaja bajo plataforma Windows

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Alta, pues sin ese servicio no funcionarían varias aplicaciones

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

- Muy importante, por que: Porque implicaría costos a la empresa

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- DNS spoofing attack
- DNS buffer overflow
- DNS Denial of Service attack
- Client flooding
- Dynamic updates vulnerabilities
- Otro (especifique): Ninguno

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

No, porque: Porque pueden implementar los sistemas de seguridad mas comunes y sentirse seguros.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra:

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres

- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra: (especifique)

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: No tengo conocimiento al respecto.

Nombre: José Enrique Díaz Jolly

Institución o empresa: Podernet SA de CV

Cargo: Gerente de Sistemas

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- (x) BIND
- () DNS de Microsoft
- (x) DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- | | |
|------------|----------------|
| (x) BIND | versión: 8.3.1 |
| (x) DJBDNS | versión: 1.05 |

3.- ¿Por qué razón utiliza esa implementación de DNS?.

BIND porque es la implementación más completa y concretamente 8.3.1 es en este momento la más segura y estable. Además cumple con todos los protocolos establecidos. No utilizo la 9x porque aún está en desarrollo y no cumple con todos los protocolos o algunos aun no han sido debidamente implementados o están en desarrollo en IETF.

DJBDNS lo utilizamos solamente en caches que se utilizan como DNS/resolver para distintas redes.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Son fundamentales pues sin ellos Internet no sería lo que es hoy en día. No es lo mismo aprenderse la dirección:puerto de un recurso que un nombre

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?

(x) Muy importante, por que: Porque al ser una de las piedras fundamentales de la red, si un DNS es contaminado por información que no es correcta, se puede volver un caos. Por otro lado, puede hacerse publica información que no debe ser pública. E.G. Los nombres de una red interna.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- (x) DNS spoofing attack
- (x) DNS buffer overflow
- (x) DNS Denial of Service attack
- (x) Client flooding
- (x) Dynamic updates vulnerabilities
- (x) Otro (especifique): Cache Polution, Fake Resolving

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

(x) No, porque: En general no están capacitados, muchos con trabajos conocen los rudimentos de la operación de DNS. La prueba es la cantidad de MX que resuelven a CNAMEs etc.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- () Ocultar versión de BIND
- () Restricción de queries
- () Restricción de transferencias de zonas
- () Correr BIND como usuario no-root o no privilegiado
- () Split function name servers. Dos servidores de nombres
- () DNS enjaulado
- () Aplicación de parches de BIND
- () Aplicación de parches de sistema operativo
- () DNSSEC
- () TSIG
- () Restricción de actualizaciones automáticas
- () Desactivación de recursión
- () Ninguna

() Otra (especifique): En general son pocos los que lo utilizan. Algunas son complejas de implementar, como por ejemplo DNSSEC a veces es complejo de implementar, algunas protecciones son desde el punto de vista de la administración de servidores (i.e. Parches) otras son de diseño del servicio como la restricción de queries y de queries recursivos.

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split función name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra (especifique): Todas y en conjunto forman una bomba de tiempo.

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: no es fácil su implementación particularmente DNSSEC y es poco frecuente que un administrador de DNS se tome la molestia de analizar quien o quienes deben tener acceso a su DNS y de que forma. Por ejemplo la restricción de transferencias, de queries y de queries recursivos.

Nombre: Mario Farias-Elinos

Empresa o institución: Universidad La Salle

Cargo: Investigador, mis líneas son: Seguridad en cómputo, Procesamiento de imágenes, Computo distribuido y paralelo.

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND
- DNS de Microsoft
- DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- BIND versión: 9.1.3

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Es la más estable y con menos problemas de seguridad.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?

Muy importante, ya que es el servicio medular de la Internet, sin el sería imposible navegar por la Internet, debido a que la mayoría de los usuarios no conocen las direcciones IP's de los servidores.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?

(X) Muy importante, por que: es uno de los servicios medulares de la Internet.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- () DNS spoofing attack
- (X) DNS buffer overflow
- (X) DNS Denial of Service attack
- () Client flooding
- (X) Dynamic updates vulnerabilities
- () Otro (especifique):

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?

(X) No, porque: No, la mayoría de los administradores, por lo menos en México, están muy acostumbrados a utilizar el DNS de Microsoft, por lo que no tienen un conocimiento profundo del servicio DNS, su importancia y mucho menos las vulnerabilidades que tienen. Dependen mucho de los parches del fabricante.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?

- () Ocultar versión de BIND.
- () Restricción de queries
- (X) Restricción de transferencias de zonas
- () Correr BIND como usuario no-root o no privilegiado
- () Split function name servers. Dos servidores de nombres
- () DNS enjaulado

- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra (especifique):

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra (especifique):

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root

() Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- (X) DNSSEC
- (X) TSIG
- () Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- (X) DNSSEC
- () TSIG
- () Ninguno

Adicionalmente, levanto un VPN con IPSec entre los servidores donde esta el Master y el slave.

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: primero porque no estamos acostumbrados a tener una cultura de seguridad informática, por lo que no le damos importancia. Segundo, por lo mismo que se utilizan esquemas de criptografía el tráfico que se genera aumenta y generalmente los enlaces que se tienen son de baja capacidad. Y tercero, el más importante, no se ha dado a conocer en forma masiva los problemas de la seguridad y el como evitarlos.

Nombre: Erick González Hernández

Institución o empresa: NICunam

Cargo: Administrador de servidores de nombres

1.- ¿Qué implementación de DNS conoce y ha configurado?

- (x) BIND
- () DNS de Microsoft
- () DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?

(x) BIND versión: 8.4.x

3.- ¿Por qué razón utiliza esa implementación de DNS?

Porque es libre y es de las mas probadas

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?

Su importancia es muy alta. Facilita el acceso a sitios web por nombre. El sistema jerarquizado permite que los DNS administren su espacio respectivo del sistema de nombres de dominio facilitando la administración y actualización de las zonas. Brinda información de direcciones IP con sus respectivos dominios. Esto ayuda a realizar tareas de troubleshooting.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?

(x) Muy importante, por que: Se deja a toda la zona de la que es responsable ese DNS deshabilitada de Internet y por consecuencia a sus clientes y no se podría tener acceso a información y servicios valiosos dentro de la zona del DNS

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- (x) DNS spoofing attack
- () DNS buffer overflow
- (x) DNS Denial of Service attack
- () Client flooding
- () Dynamic updates vulnerabilities
- () Otro

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?

(x) No, porque: pienso que casi siempre hasta que uno (en general) hasta que se ve envuelto en un problema de seguridad es cuando se preocupa por conocer los tipos de ataque o como prevenirlos.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra:

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursion
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- (1) Mala administración del servidor que alberga el DNS
- (2) Mala configuración del servidor de nombres
- () Otra: (especifique)

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS? Explique

No, porque: porque solo en ISP's muy grandes se preocupan por estas cuestiones.

Nombre: Martín Humberto Hoz Salvador

Empresa o institución: Check Point Software Technologies México

Cargo: Security Engineer

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND
- DNS de Microsoft
- DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

(X) BIND versión: Meta IP DNS de Check Point, que es una variante propietaria de BIND 8.

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Porque es la que fabrica la compañía.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Bastante. Simplemente sin nombres no podríamos vivir.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

(X) Muy importante, por que: Un DNS mal configurado puede ser un boquete demasiado grande. Desde bugs en la implementación del servicio que permitan ejecutar código arbitrario a un atacante, pasando por envenenamientos y falsificación de nombres, hasta llegar a negaciones de Servicio y pérdida de negocio.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

(X) DNS spoofing attack

(X) DNS buffer overflow

(X) DNS Denial of Service attack

(X) Client flooding

(X) Dynamic updates vulnerabilities

() Otro (especifique): DNS cache poisoning (Diferente del spoofing, porque se envenena en caché, no se suplanta la identidad de un servidor de DNS.

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

(X) No, porque: Porque si no, no tendríamos tantos problemas con casos famosos y no tantos, en los que el DNS fue el problema.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra (especifique): Poner firewalls para proteger el equipos.

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra (especifique):

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique) Mala imagen para competidores.

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG
- Ninguno - Yo no administro el DNS, aunque se que se utiliza TSIG internamente.

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: En decenas de implementaciones de DNS que he visto, solo en un par de ellas he visto TSIG activado.

Nombre: Genny Marisol León Leal

Empresa o institución: DGSCA

Cargo: Administrador UNIX

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND
- DNS de Microsoft
- DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

(X) BIND versión: 8

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Porque la última versión todavía no esta por aprobarse y esta es la que ha estado en practica y ha funcionado relativamente bien.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Una importancia del 100% ya que sin este no hay un buen funcionamiento en Internet, no existe un orden de las cosas y por medio de DNS existe una adecuada administración de los dominios y resoluciones inversas.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

(X) Muy importante, por que: si algo ocurre con el servidor de nombres provocaría un gran descontrol ante las zonas y nombres de dominio, también se expondría su adecuado funcionamiento y se harían redireccionamientos hacia otros nombres de dominios falsos, también se podría comprometer todo el servidor de nombres provocando denegación del servicio, falsificar datos, violar la integridad de los datos o hacerse pasar por una entidad falsa.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- () DNS spoofing attack
- (X) DNS buffer overflow
- (X) DNS Denial of Service attack
- () Client flooding
- () Dynamic updates vulnerabilities
- () Otro (especifique): Configuración insegura.

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

(X) No, porque: lamentablemente hoy en día estos temas no son muy conocidos por los administradores, solo se dedican a tener buen funcionamiento en sus sistemas o dan prioridad a otros aspectos dejando su seguridad a un lado; con esto dan una menor importancia a este aspecto sin saber que al atacar el mismo pueden llegar a perder todo el control del servidor. Existe desconocimiento por parte de los administradores debido a que son poco difundidos estos temas y el poco material que existe se encuentra en el idioma inglés, otro aspecto lamentable es que muchos administradores ni siquiera saben como configurar el DNS o lo que es peor ni siquiera conocen su funcionamiento.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra (especifique):

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra (especifique):

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: DNSSEC no consigue una buena difusión porque estos protocolos suelen ser más costosos en términos de recursos.

Nombre: Jorge Alberto Martínez Melo
Empresa o institución: DGSCA - UNAM
Cargo: Coordinador de NICunam

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND
- DNS de Microsoft
- DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- BIND versión: 8.3 y 9.2

3.- ¿Por qué razón utiliza esa implementación de DNS?.

La versión 8.3 es considerada la más estable para poner en producción. La versión 9.2 la empleo para probar IPv6.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Básicamente es el mecanismo que hace posible el acercamiento de la red con cualquier tipo de usuario y de manera más clara y óptima para usuarios no especializados. Técnicamente, el DNS es un medio para validar y autenticar servicios y conexiones.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

Muy importante, por que: Es muy importante dado que es un servicio crítico que asegura el correcto orden y funcionamiento de la red.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- DNS spoofing attack
- DNS buffer overflow
- DNS Denial of Service attack
- Client flooding
- Dynamic updates vulnerabilities
- Otro (especifique):

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

(x) No, porque: Por lo menos en México, apenas se esta fomentando e inculcando la seguridad en la red. Tal vez se demore un poco de tiempo en que esta preocupación llega a cada uno de los servicio de Internet.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra (especifique):

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra (especifique):

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: No, realmente firmar las zonas degrada un poco la velocidad de transferencia de zonas y si se implementa en servidores que tienen muchas zonas y/o muy pesadas, pues esto resulta no muy óptimo.

Nombre: Sergio Moreno Reyes
Empresa o institución: DGSCA - UNAM
Cargo: Integrante del Centro de Información de RedUNAM

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- (X) BIND
- () DNS de Microsoft
- () DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- (x) BIND versión: 8.2.3

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Porque la plataforma UNIX es mas segura, confiable estable y poderosa. Además, BIND se ha consolidado como una aplicación muy estable, capaz de soportar alta demanda de peticiones de DNS y cuenta con soporte, FAQs, y lista para resolver dudas, comentarios y sugerencias.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Es vital, puesto que sin los DNS, la internet no sería la misma, ya que en el caso de las direcciones IP, tendríamos que aprendernos todas y cada una de ellas para decidir a cual acceder, además de eso, los DNS trabajan transparente para el usuario, el cual quizá no sabe que existen, pero cuando se genera una falla, son los primeros en detectarlo y sobrevienen lo problemas.

Un DNS, es demasiado importante para la Internet, pues sin ellos, sería prácticamente imposible que cualquier usuario común y corriente pudiera comunicarse con el resto del mundo, pues es mucho mas sencillo conocer una dirección por su nombre que por su ip, y para ipv6, pues la situación es peor.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

(x) Muy importante, por que: La seguridad es uno de los aspectos más importantes para cualquier servidor, sea web, correo, BD o DNS. En el caso de DNS es muy importante, ya que al igual que cualquier equipo conectado a Internet, es susceptible de ser atacado, y es por ello que debemos tener herramientas que sirvan de apoyo para detectar y evitar cualquier posible

ataque, ya que si se compromete el servicio, miles de usuarios se verían afectados por el servicio de DNS.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- DNS spoofing attack
- DNS buffer overflow
- DNS Denial of Service attack
- Client flooding
- Dynamic updates vulnerabilities

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?

No, porque: En muchas ocasiones, el Administrador no sabe ni siquiera lo que es un servidor, y creo que cuando conocen algo de administración de servidores, se enfoca a servicios como correo, web o bases de datos, pero en el caso de DNS, es muy difícil que alguien se interese en conocer a detalle todo lo que implica, quizá porque aparentemente no brinda un servicio "palpable" a los usuarios, sino mas bien es invisible para ellos, y quizá están mas preocupados por sus aplicaciones de mayor prioridad que por la de un DNS.

Es falta de cultura informática y ganas de conocer a detalle el funcionamiento de este servicio.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión

- Ninguna
- Otra (especifique):

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra: (especifique)

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- (x) DNSSEC (Lo conozco muy vagamente)
 () TSIG
 () Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?

- () DNSSEC
 () TSIG
 (x) Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: No porque en muchas ocasiones no se cuenta con noticias, foros o noticias de las nuevas mejoras, herramientas o manuales de configuración y administración de DNS, además de que en muchas ocasiones implantar alguna herramienta suele ser costoso si no se conoce a detalle, pues puede provocar cambios en el servicio o en el peor de los casos, exponer el servicio a un ataque mas fuerte.

Nombre: Ricardo Santos Quintero

Empresa o institución: Subdirección de Administración de Sistemas. Sistema de Información Universitaria. Benemérita Universidad Autónoma de Puebla

Cargo: Planeación, Desarrollo y Administración de Servicios de Internet

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- (x) BIND
 (x) DNS de Microsoft
 () DJBDNS

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- | | |
|----------------------|-------------------------------------|
| (x) BIND | versión: 8.3.1 |
| (x) DNS de Microsoft | versión: Windows 2K Advanced Server |

3.- ¿Por qué razón utiliza esa implementación de DNS?.

Utilizamos la versión 8 de BIND dado que es la más estable y probada para ambientes de producción en sistemas 24x7. En un futuro próximo tenemos

planeado utilizar la versión 9 y aprovechar características como DNSSEC, TSIG y soporte de IPv6. Asimismo estamos concientes que BIND sobre UNIX es la mejor opción en términos de seguridad y disponibilidad para DNS servers sin embargo, el uso de DNS de Microsoft nos es requerido para el funcionamiento optimo de MS Active Directory. Actualmente estamos haciendo pruebas con Active Directory y BIND 8/9 para relevar el uso de MS-DNS.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?.

Tiene un nivel de importancia de primer orden. Dado que en Internet y en caso particular dentro de nuestras intranets con el paso del tiempo se crean y liberan nuevos servicios de los cuales algunos de ellos están ligados directamente como servicio a un registro en nuestras zonas de DNS.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?.

(X) Muy importante, por que: Una de las razones es por que contiene información sobre los hosts de una red.

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- (X) DNS spoofing attack
- (X) DNS buffer overflow
- (X) DNS Denial of Service attack
- (X) Client flooding
- (X) Dynamic updates vulnerabilities
- (X) Otro (especifique): Transferencia no autorizada de zonas

7.- ¿Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

(X) No, porque: Es un problema de cultura que radica en la creencia de que los servidores de DNS son cajas que una vez instalados y operando estarán bien mientras resuelvan páginas y correos.

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna
- Otra (especifique):

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

- Ocultar versión de BIND
- Restricción de queries
- Restricción de transferencias de zonas
- Correr BIND como usuario no-root o no privilegiado
- Split function name servers. Dos servidores de nombres
- DNS enjaulado
- Aplicación de parches de BIND
- Aplicación de parches de sistema operativo
- DNSSEC
- TSIG
- Restricción de actualizaciones automáticas
- Desactivación de recursión
- Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

- Vulnerabilidades en el código de la implementación de DNS
- Vulnerabilidades del sistema operativo
- Mala administración del servidor que alberga el DNS
- Mala configuración del servidor de nombres
- Otra (especifique):

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio

- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS? Explique

No, porque: Creo que aun es un "add on" en fase experimental, si bien ya ha sido liberado su implementación pone en duda la estabilidad e interoperabilidad con clientes (otros servidores o clientes como tales) que no soporten el uso de DNSSEC y TSIG)

Nombre: Gunnar Wolf

Empresa o institución: UNAM-Iztacala

Cargo: Seguridad y administración de servidores

1.- ¿Qué implementación de DNS conoce y ha configurado?.

- BIND

2.- ¿Qué implementación y versión de DNS utiliza en su organización?.

- BIND versión: 4

3.- ¿Por qué razón utiliza esa implementación de DNS?

Por ser código auditado - El equipo de desarrollo de OpenBSD incluye BIND versión 4 pues ha comprobado exhaustivamente su seguridad, cosa que nadie ha hecho con versiones posteriores de este programa.

Y claro, elegí usar BIND por ser libre.

4.- ¿Qué importancia considera que tiene el DNS para el correcto funcionamiento de Internet y por qué?

La resolución de nombres es vital para prácticamente todos los aspectos del uso de Internet.

5.- ¿Qué tan importante considera que es implementar seguridad en los servidores de nombres y por qué?

- Muy importante, por que: En todo servidor es muy importante
 Mas o menos importante, por que:
 Poco importante, por que:
 No es importante, por que:

6.- De la siguiente lista de ataques a DNS por vulnerabilidades en el código de la implementación, marque aquellos para los cuáles conozca la manera de llevarlos a cabo y como prevenirlos.

- DNS spoofing attack
 DNS buffer overflow
 DNS Denial of Service attack
 Client flooding
 Dynamic updates vulnerabilities
 Otro (especifique):

7.- Considera usted, que en general los administradores de DNS, conocen a detalle los ataques que se pueden llevar a cabo en contra de la seguridad de un DNS, sus consecuencias, y la manera de prevenirlos?.

- No, porque: La seguridad no es importante para mucha gente

8.- De las siguientes medidas de seguridad para un DNS, ¿cuáles considera que son realmente utilizadas por los administradores de DNS?.

Ocultar versión de BIND

Este se me hace un ejemplo de seguridad por oscuridad, o lo que es lo mismo, de falta de seguridad. No sugiero usarlo.

Restricción de queries

Restricción de transferencias de zonas

Correr BIND como usuario no-root o no privilegiado

Split function name servers. Dos servidores de nombres

DNS enjaulado

Aplicación de parches de BIND

Aplicación de parches de sistema operativo

DNSSEC

TSIG

Restricción de actualizaciones automáticas

Desactivación de recursión

Ninguna

Otra (especifique): Esta pregunta no puede ser respondida, está mal formulada en mi opinión.

9.- De las anteriores medidas de seguridad, indique para cuáles conoce la configuración necesaria.

Ocultar versión de BIND

Restricción de queries

Restricción de transferencias de zonas

Correr BIND como usuario no-root o no privilegiado

Split function name servers. Dos servidores de nombres

DNS enjaulado

Aplicación de parches de BIND

Aplicación de parches de sistema operativo

DNSSEC

TSIG

Restricción de actualizaciones automáticas

Desactivación de recursión

Ninguna

10.- ¿Cuál considera que es la causa principal de ataques exitosos a la seguridad de un servidor de nombres?.

Vulnerabilidades en el código de la implementación de DNS

Vulnerabilidades del sistema operativo

Mala administración del servidor que alberga el DNS

Mala configuración del servidor de nombres

Otra (especifique):

11.- Desde su punto de vista, ¿cuáles son los objetivos más comunes que se persiguen al atacar un servidor de nombres?.

- Negación del servicio
- Robo de correo electrónico
- Falsificación de páginas web
- Obtener información acerca de los hosts de una red
- Creación de registros
- Desvío de transferencias de archivos
- Obtener acceso como usuario root
- Otro: (especifique)

12.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, conoce?.

- DNSSEC
- TSIG
- Ninguno

13.- ¿Cuál de los protocolos para añadir seguridad al DNS, basados en criptografía y firmas digitales, aplica en su servidor de nombres?.

- DNSSEC
- TSIG
- Ninguno

14.- ¿Desde su punto de vista, considera que es popular el uso de DNSSEC y TSIG para agregar seguridad al DNS?. Explique.

No, porque: Por su falta de compatibilidad con versiones anteriores, por la poca conciencia de seguridad en la gente.

GLOSARIO

- ♦ **/etc/hosts.-** Archivo del sistema operativo UNIX, que contiene una relación de nombres de máquinas con sus respectivas direcciones IP.
- ♦ **AES (Advanced Encryption Standar).-** Algoritmo criptográfico para el cifrado de información.
- ♦ **Archivo core.-** Archivo generado después de que un programa o proceso del sistema operativo UNIX falla de manera crítica.
- ♦ **ARPAnet.-** Es la red que precedió a la actual Internet. Comenzó en 1969 como un proyecto del Departamento de Defensa de los Estados Unidos y unía a algunos cientos de computadoras.
- ♦ **Arquitectura cliente/servidor.-** Arquitectura de sistemas en la que existe un programa servidor dedicado a brindar uno más servicios y un programa cliente a través del cual se tendrá acceso al programa servidor.
- ♦ **Backbone.-** Red central de alta velocidad que conecta a otras redes independientes que pueden ser de velocidad inferior.
- ♦ **BIND (Berkeley Internet Domain Name).-** Implementación del sistema de nombres de dominio, distribuido por el "Internet Software Consortium".
- ♦ **Broadcast.-** Es un paquete de datos que se envía a todos los nodos de una red.
- ♦ **Buffer overflow.-** Ataque intencional a sistemas de cómputo que consiste en la saturación de la memoria, con el fin de sobrescribir las instrucciones que están almacenadas como válidas para ejecutar código malicioso.
- ♦ **Bug.-** Vulnerabilidad o falla encontrada en algún software y que puede ser aprovechado para violar la seguridad de un sistema.
- ♦ **C.-** Lenguaje de programación estructurada.
- ♦ **Caché.-** Memoria de alta velocidad que tiene como uso principal el reducir la diferencia de tiempo de acceso que existe entre la memoria central y los dispositivos de memoria externa. La memoria caché aumenta la velocidad de muchas operaciones del microprocesador, almacenando el contenido de la memoria del sistema al que se ha tenido acceso más recientemente.
- ♦ **CERT (Computer Emergency Response Team).-** Centro dedicado a la atender reportes de problemas de seguridad en Internet.
- ♦ **CHAOSNET.-** Fue una de las primeras redes de área local desarrollada por el MIT en los años 70's.

- ◆ **Cliente.**- Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un archivo a un servidor es un cliente de este servidor.
- ◆ **Cracker.**- Tipo de atacante a los sistemas informáticos, que rompe los esquemas de protección de algún programa y los pone a libre disposición de quien desee usarlo.
- ◆ **DARPA (Defense Advanced Research Projects Agency).**- Es la organización de investigación y desarrollo central del departamento de defensa de Estados Unidos.
- ◆ **DCA (Defense Communications Agency).**- Agencia del gobierno de Estados Unidos responsable de la instalación de las redes de datos de la defensa.
- ◆ **DES (Data Encryption Standar).**- Algoritmo criptográfico para el cifrado de información.
- ◆ **DdoS (Distributed Denial of Service).**- Se trata de un ataque DoS dirigido a varios sistemas informáticos en un mismo lapso de tiempo.
- ◆ **Debug.**- Procedimiento para la detección, y en ocasiones solución de errores en un programa o proceso.
- ◆ **Demonio.**- Daemon. Programa que permanece en ejecución bajo el sistema operativo UNIX, y que realiza una tarea específica. Es transparente para el usuario.
- ◆ **DIG.**- Herramienta que emula un cliente de DNS y que permite hacer peticiones directas a servidores de nombres.
- ◆ **Dirección IP.**- Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.
- ◆ **DNS (Domain Name System).**- Es el sistema de nombres utilizado en Internet.
- ◆ **DNS (Domain Name Server).**- Servidor de nombres. Contiene la relación de nombres de computadoras con su respectiva dirección IP.
- ◆ **DNS de Windows NT.**- Implementación del sistema de nombres de dominio para sistema operativo Windows NT.
- ◆ **DNSSEC.**- Protocolo basado en criptografía utilizado para agregar seguridad al DNS.

- ◆ **DoS (Denial of Service).**- Ataque a sistemas informáticos que consiste en la negación del servicio que proporcionan.
- ◆ **Esteganografía.**- Es el arte de esconder información para transmitirla en formas que impidan conocer la existencia de los mensajes ocultos.
- ◆ **Firewall.**- Barrera de seguridad en una red formada por hardware y/o software capaz de permitir o negar el acceso de paquetes de información de acuerdo a políticas establecidas. Normalmente se encuentra entre una red corporativa y el acceso a Internet.
- ◆ **Fortune 1000.**- Es una base de datos con información de contactos de las 1000 compañías más grandes e importantes de Estados Unidos. Se vende a través de Internet en el URL <http://www.fortune.com>.
- ◆ **FTP (File Transfer Protocol).**- Es parte del conjunto de protocolos TCP/IP y es utilizado para transferir archivos a través de la red.
- ◆ **Glue.**- Característica del DNS que permite almacenar información extra acerca de un nombre de dominio consultado.
- ◆ **Hacker.**- Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y equipos de cómputo. Puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos.
- ◆ **Host.**- Es el nombre que recibe cualquier computadora conectada a una red.
- ◆ **HTTP (Hiper Text Transfer Protocol).**- Protocolo de Transferencia de Hipertextos Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.
- ◆ **IANA (Internet Assigned Number Agency).**- Organismo en Internet encargado de la asignación de direcciones IP.
- ◆ **ICANN (Internet Corporation for Assigned Names and Numbers).**- Organismo en Internet que regula la asignación de nombres de dominio y direcciones IP.
- ◆ **IETF (Internet Engineering Task Force).**- Grupo de operaciones de ingeniería de Internet.
- ◆ **Information leakage.**- Fuga provocada de información de un sistema.
- ◆ **Internet.**- (con i mayúscula). Es la red de computadoras más grande del mundo. Está basada en la suite de protocolos TCP/IP.

- ♦ **internet.**- (con i minúscula).- Término utilizado para hacer referencia a una red de computadoras privada. También se le conoce como Intranet.
- ♦ **Internet Draft.**- Documentos acerca de los trabajos e investigaciones realizadas por la IETF.
- ♦ **IP (Internet Protocol)** .- Protocolo de la capa de red en la suite de protocolos TCP/IP. Proporciona características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblado, y seguridad.
- ♦ **IPSEC (IP Security).**- Conjunto de estándares abiertos que proporcionan servicios de confidencialidad, integridad y autenticación de datos.
- ♦ **LDAP (Lightweight Directory Access Protocol).**- Protocolo que provee acceso para la administración y utilización de aplicaciones bajo el estándar X.500.
- ♦ **MCI.**- Proveedor de servicios de telecomunicaciones.
- ♦ **Memoria caché.**- Almacenamiento temporal.
- ♦ **MILNET.**- Red perteneciente al Departamento de Defensa de los Estados Unidos.
- ♦ **Multicast.**- Son paquetes individuales enviados a un subconjunto específico de direcciones de red.
- ♦ **Name server.**- Programa servidor del sistema de nombres de dominio.
- ♦ **Named.**- Proceso que corre en el sistema operativo UNIX encargado del funcionamiento de un servidor de nombres.
- ♦ **Negación de servicio.**- Ataque de negación de servicio. DoS.
- ♦ **NFSNET (National Science Foundation Network).**- Red que inicialmente fue utilizada como espina dorsal de la Internet.
- ♦ **NIC (Network Information Center).**- Centro de Información de la Red.
- ♦ **NIC-México.**- Centro de Información de Red en México, encargado del dominio mx.
- ♦ **NICunam (Centro de Información de RedUNAM).**- Área de la Subdirección de Telecomunicaciones de la Dirección General de Servicios de Cómputo Académico de la UNAM. Se encarga de la administración de los DNS de la red de datos de la UNAM.

- ♦ **NIS (Network Information Service).**- Protocolo desarrollado por Sun Microsystems que permite acceso remoto a archivos, especialmente bases de datos, en red.
- ♦ **Nslookup.**- Herramienta que emula un cliente de DNS y que permite hacer peticiones directas a servidores de nombres.
- ♦ **PING (Packet INternet Groper).**- Programa que utiliza el protocolo ICMP de TCP/IP para verificar la disponibilidad de algún dispositivo de la red.
- ♦ **Página web.**- Conjunto de información programada en algún lenguaje que puede ser accesible a través de http.
- ♦ **Perl.**- Lenguaje de programación estructurada.
- ♦ **PGP (Pretty Good Privacy).**- Aplicación basada en criptografía de llave pública para brindar seguridad en el intercambio de mensajes electrónicos.
- ♦ **Protocolo.**- Descripción formal de un conjunto de reglas y convenciones. En el ámbito de las telecomunicaciones rigen el modo de intercambiar información entre redes.
- ♦ **Resolver.**- Programa cliente del sistema de nombres de dominio.
- ♦ **RFC's (Requests For Comments).**- Documentos que contienen definiciones de protocolos y políticas dentro de Internet.
- ♦ **Segmentation Fault.**- Falla crítica en la operación normal de un programa o proceso.
- ♦ **Seguridad por oscuridad.**- Práctica de seguridad informática que consiste en esconder la información acerca del funcionamiento de un programa, proceso, protocolo o sistema. No se recomienda utilizarlo.
- ♦ **Sendmail.**- Programa utilizado para el envío de correo electrónico.
- ♦ **SET (Secure Electronic Transactions).**- Protocolo para brindar seguridad en las transacciones de comercio electrónico.
- ♦ **Syslog.**- Facilidad del sistema operativo que permite mostrar y registrar los mensajes o alertas generados por un programa o proceso.
- ♦ **Sprint.**- Proveedor de servicios de telecomunicaciones.
- ♦ **Spoofing.**- Suplantación maliciosa de un programa, sistema, proceso o servicio informático.

- ♦ **SRI-NIC.**- Computadora perteneciente al Centro de Información de Red del Instituto Tecnológico de Stanford en la cuál se albergaba el archivo con los nombres y direcciones IP que formaban la ARPAnet.
- ♦ **SUN.**- Marca de fabricante de equipos servidores que utilizan sistema operativo Solaris.
- ♦ **TCP (Transmission Control Protocol).**- Protocolo orientado a conexión que permite la transmisión de datos de manera confiable.
- ♦ **TCP/IP (Transmission Control Protocol / Internet Protocol).**- Conjunto de protocolos para conectar en red, computadoras de diferentes plataformas. Se le conoce como suite, pila, o snack de protocolos TCP/IP.
- ♦ **TCSEC (Trusted Computer System Evaluation Criteria).**- Estándar desarrollado por el gobierno de los Estados Unidos, que establece lineamientos de seguridad en cómputo. Se conoce como "libro naranja".
- ♦ **Traceroute.**- Programa que utiliza el protocolo ICMP de TCP/IP para verificar la ruta a través de los dispositivos de red que tiene que seguir un paquete de información para alcanzar cierto destino.
- ♦ **TSIG (Transaction Signatures).**- Protocolo basado en criptografía utilizado para agregar seguridad al DNS.
- ♦ **UDP (User Datagram Protocol).**- Protocolo no orientado a conexión que forma parte de la familia TCP/IP. Entrega paquetes o datagramas sin garantía de que hayan sido recibidos.
- ♦ **Unicast.**- Mensaje que se envía a un solo destino en la red.
- ♦ **UNIX.**- Sistema operativo multiusuario y multiproceso, creado en la década de los 60's por la Universidad de Berkeley en California.
- ♦ **Uplink.**- un enlace tierra-satélite o enlace ascendente.
- ♦ **URL (Uniform Resource Locator).**- Localizador Uniforme de Recursos. Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el World Wide Web. El URL está conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.sfp.gov.ar) más el puerto por el cuál se proporciona el servicio.
- ♦ **Windows Browser.**- Servidor de Windows que proporciona información acerca del entorno de red.
- ♦ **WINS (Windows Internet Name Service).**- Servicio de nombres para ambientes de red Windows. Mapea direcciones IP a nombres de NetBIOS.

- ♦ **VMS (Virtual Memory System).**- Versión de sistema operativo utilizado para computadoras DEC`s VAX.
- ♦ **VPN (Virtual Private Network).**- Enlace virtual privado que permite la transferencia de datos de manera segura a través de una red pública TCP/IP.
- ♦ **WHOIS.**- Herramienta que permite consultar la información administrativa relacionada con los nombres de dominio. Por ejemplo, los datos de los contactos o administradores de un dominio.

BIBLIOGRAFÍA Y REFERENCIAS

LIBROS

1. Albitz, P., Liu, C. DNS AND BIND. Editorial O'Reilly. Estados Unidos. 3ª edición. 1998. 482 pp.
2. Ford, M. TECNOLOGÍAS DE INTERCONECTIVIDAD DE REDES. Editorial Prentice-Hall Hispanoamericana. México. 1ª edición. 1998. 736 pp.
3. Hunt, C. TCP/IP, NETWORK ADMINISTRATION. Editorial O'Reilly. Estados Unidos. 2ª edición. 1998. 612 pp.
4. Menezes, A. HANDBOOK OF APPLIED CRYPTOGRAPHY. Editorial CRC Press. Estados Unidos. 1ª edición. 1997. 780 pp.
5. Stevens, W. TCP/IP ILUSTRATED. Editorial Addison-Wesley. Estados Unidos. 11ª impresión. 1998. 575 pp.

RFC's

6. Lottor, M. DOMAIN ADMINISTRATORS OPERATIONS GUIDE. RFC 1033. 1987.
7. Mockapetris, P. DOMAIN NAMES - CONCEPTS AND FACILITIES. RFC 1034. 1987.
8. Mockapetris, P. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION. RFC 1035. 1987.
9. Postel, J. DOMAIN NAME SYSTEM STRUCTURE AND DELEGATION. RFC 1591. 1994.

APUNTES

10. Hernández, L. MÓDULO 2 - CRIPTOLOGÍA. Diplomado "Seguridad Informática". UNAM. 2002.
11. Mallen, G. MÓDULO 7 - CÓDIGO MALICIOSO. Diplomado "Seguridad Informática". UNAM. 2002.

URL 's

12. Historia de NIC-México
http://www.nic.mx/nic/plsql/nic.nic_IniNic?X=0&Y=0
13. Internetworking Basics
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm

OTROS LIBROS (MARCO TEÓRICO)

14. Albitz, P., Liu, C. DNS ON WINDOWS NT. Editorial O'Reilly. Estados Unidos. 1ª edición. 1998. 329 pp.
15. Garfinkel, S., Spafford, G. PRACTICAL UNIX AND INTERNET SECURITY. Editorial O'Reilly. Estados Unidos. 2ª edición. 1996. 971 pp.
16. Siyan, K., Hare, Ch. INTERNET FIREWALLS AND NETWORK SECURITY. Editorial Prentice Hall. Estados Unidos. 1ª edición. 1995. 410 pp.
17. Zwicky, E., Cooper, S. BUILDING INTERNET FIREWALLS. Editorial O'Reilly. Estados Unidos. 2ª edición. 2000. 869 pp.