SEGURIDAD EN REDES

Análisis y evaluación de la Seguridad proporcionada por DNSSEC en Redes de Información IPv6 en un escenario de pruebas controlado

D. K. Terán Arévalo, D. V. Fernández García, y F. J. Terán Cuarán.

Resumen— El presente artículo se basa en el Análisis y evaluación de la seguridad proporcionada por DNSSEC en redes de información IPv6 en un escenario de pruebas controlado. Para el desarrollo de esta investigación, se implementó un escenario de pruebas controlado para el despliegue de DNSSEC en redes IPv6 en diferentes Ss. Os. (Windows, Linux), con equipos del Departamento de Telecomunicaciones de la Universidad del Cauca (Routers Cisco 2801, Routers software Quagga, Switches Catalyst 2960- S y Pcs). Además, se adaptó una metodología para el análisis de la seguridad proporcionada por DNSSEC en Redes IPv6 en el escenario de pruebas seleccionado, con base en el estudio de las metodologías de evaluación de la seguridad: ISSAF, OSSTMM y PTES, y se evaluó las vulnerabilidades de seguridad de DNSSEC en redes IPv6, con base en el Sistema de puntuación de vulnerabilidad común (CVSS, *Common Vulnerability Scoring System*), mediante diferentes PoC (Pruebas de Concepto), sobre escenarios distintos con diferentes requisitos de seguridad con el fin de determinar en qué casos DNSSEC fue o no fue vulnerable, es decir si DNSSEC proporcionó o no sus funciones de seguridad tales como *autenticación del origen y autenticación e integridad de los datos de DNS*.

Índice de Términos— DNSSEC, DNS, IPv6.

I. INTRODUCCIÓN

El sistema de Nombres de Dominio (DNS, Domain Name System) [1], resuelve un Nombre de Dominio en una dirección IP, por ejemplo el Nombre Dominio *www.google.com* en la dirección IPv6 [2]: *2001:4860:4860::8888*, posibilitando que internet sea más fácil de usar, sin que los usuarios tengan la necesidad de aprender, memorizar y recordar las direcciones IP/IPv6 de cada uno de los Dominios a los que se comunican. Pero aquí, hay un grave problema, todo este proceso es inseguro, ya que en la vida real, un usuario que se conecta desde una terminal y realiza una consulta a un Nombre de Dominio, no sabe quién le envió la respuesta verdadera, y tampoco sabe si los datos fueron modificados por un atacante durante el tránsito, redireccionando a la víctima a un sitio web falso, permitiendo robar de esta manera su información confidencial. Todo esto hace que el DNS sea un protocolo inseguro, debido a que no contempla ningún soporte de seguridad, para garantizar: Autenticación del origen, Autenticación e Integridad de los datos de DNS,

Confidencialidad de la información y Disponibilidad del servicio [3].

Por esta razón la IETF propuso el Sistema de Nombres de Dominio con Extensiones de Seguridad (DNSSEC, Domain Name System Security Extensions) [4, 5, 6], como un conjunto de extensiones que aumentan la seguridad del protocolo DNS, al proveer un mecanismo para la Autenticación del origen e Integridad de los datos DNS, y Denegación de existencia autenticada, mediante el uso de la firma digital de los datos DNS, nuevos registros de recursos y una Infraestructura de Clave Pública (PKI), para la construcción de una “Cadena de Confianza”. Sin embargo, no proporciona la confidencialidad de la información ni disponibilidad del servicio.

En ese sentido, en el presente artículo se presenta el proceso que se llevó a cabo, para Analizar y Evaluar la Seguridad Proporcionada por DNSSEC en Redes de Información IPv6 en un escenario de pruebas controlado, así como los aportes y conclusiones obtenidos como resultado de la investigación.

II. ESCENARIO DE PRUEBAS CONTROLADO

Para determinar el escenario de pruebas controlado, primero se llevó a cabo un estudio detallado sobre el funcionamiento de los Servicios de Internet DNS, DNSSEC y Web en Redes IPv6, y los componentes principales dentro de la infraestructura DNS: Servidores DNS autoritarios, Servidor DNS Caché y Clientes y los componentes DNSSEC:

Servidores autoritarios DNSSEC, Servidor DNS Caché Validador y Cliente Validador, y las funciones que cumplen en el proceso de validación para garantizar la autenticidad e integridad de los datos DNS de una respuesta [7].

Con base en esto se determinaron los componentes principales que formarían parte y cumplirían un rol específico para su implementación en redes IPv6 en el escenario de pruebas controlado.

La topología de red del escenario de pruebas controlado en redes IPv6 que se definió para lograr el propósito del proyecto, está conformada por una red interna y una red externa. La red interna, está constituida por la implementación de la delegación segura DNSSEC para los dominios y subdominios internos de la organización Bancodk, y la red externa, conformada por la implementación de la cadena de

Dalia. K Terán Arévalo, daliateran@unicauca.edu.co, Diana. V. Fernández García, dianvf@unicauca.edu.co y Francisco. J Terán Cuarán, fteran@unicauca.edu.co; Universidad del Cauca, Popayán, Colombia.

confianza DNSSEC, en todos los servidores autoritarios involucrados en los niveles de la jerarquía DNS.

La configuración e implementación de la cadena de confianza DNSSEC se divide en 2 estados: el primero, cuando todos los niveles de la jerarquía DNS se encuentran firmados con DNSSEC, a excepción del dominio networks.com y el segundo cuando la cadena de confianza está rota, es decir que el dominio de nivel superior gTLD.COM, no se encuentra firmado con DNSSEC.

La implementación del escenario de pruebas, se llevó a cabo con equipos del Departamento de Telecomunicaciones de la Universidad del Cauca tales como:

Routers cisco 2801, routers software quagga, switches catalyst 2960-s y pcs y se utilizó el protocolo estándar de enrutamiento BGP para redes IPv6 [8].

Para permitir la conectividad de todos los componentes involucrados en el escenario, definiendo 6 sistemas autónomos, para especificar las redes IPv6 del escenario en formato hexadecimal, como se aprecia en la Figura 1.

Figura 1. Escenario de pruebas controlado DNSSEC en IPv6.
Fuente: Los autores.

III. METODOLOGÍAS DE EVALUACIÓN DE LA SEGURIDAD

Para adaptar una metodología para el análisis y evaluación de la seguridad proporcionada por DNSSEC en redes IPv6 en el escenario de pruebas controlado, se realizó un estudio, análisis detallado y comparación de los aspectos y características más importantes de las metodologías de evaluación de la seguridad: ISSAF 2.1 [9], OSSTMM 3.0 [10] y PTES 1.1 [11], las cuales tienen en común que el tipo de licencia con el que se han creado permite su utilización de forma libre, es decir sin costo, cuyo resultado fue la definición de la Metodología Adaptada.

Figura 2. Metodologías de evaluación de seguridad.
Fuente: Tomada de [8].

En la Tabla I, se observa la comparación general de los aspectos más relevantes incluidos en cada una de las metodologías, las marcas de verificación de color verde representan los aspectos que tienen en común todas las metodologías, y las marcas de verificación rojas los que no.

TABLA I
COMPARACIÓN GENERAL DE LAS METODOLOGÍAS
DE EVALUACIÓN DE LA SEGURIDAD

ASPECTOS	ISSAF	OSSTMM	PTES
Acreditación
Alcance
Introducción a conceptos
Gestión del compromiso
Gestión de proyecto
Entornos de aplicabilidad
Metodología de penetración
Guía técnica
Métricas
Informes
Recomendaciones
Usabilidad y uso

IV. DEFINICIÓN DE LA METODOLOGÍA ADAPTADA PARA EL ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD PROPORCIONADA POR DNSSEC

A partir del análisis comparativo de los aspectos más relevantes incluidos en cada una de las metodologías mencionadas anteriormente, se determinaron los aspectos y características más importantes que sirvieron como base para la definición de la Metodología Adaptada, resaltando las características generales que se querían obtener de manera que se adapte a las necesidades del Proyecto para el análisis y evaluación de la seguridad proporcionada por DNSSEC en redes IPv6 en un escenario de pruebas controlado, siendo comprensible, detallada y de fácil aplicabilidad en este contexto.

A. Alcance

El alcance de la Metodología Adaptada se compone de: la definición del test de intrusión, los objetivos, el ambiente o entorno donde se realizarán las pruebas, y la metodología de penetración con su correspondiente guía técnica, métricas y estructura para la entrega de resultados.

B. Entorno de Aplicabilidad

El entorno de aplicabilidad de la Metodología es la seguridad de los sistemas y redes de información, desde la perspectiva de la evaluación de la seguridad proporcionada por la extensión de seguridad del protocolo DNSSEC.

C. Metodología de Penetración

La metodología de penetración de la Metodología Adaptada, está fundamentada en los procedimientos de las metodologías de penetración de PTES e ISSAF.

D. Guía Técnica

La guía técnica de la Metodología Adaptada, se basa en el modelo propuesto por la metodología de penetración de ISSAF, al especificar las herramientas y como se pueden utilizar para la ejecución de las pruebas de cada una de las fases.

E. Métricas

Este trabajo, no cubre el parámetro de métrica como la mayoría de las metodologías estudiadas, mediante el análisis y evaluación del riesgo, sino que se enfoca en el análisis y evaluación de las vulnerabilidades por medio del Sistema Común de Puntuación de Vulnerabilidades (CVSS, Common Vulnerability Scoring System), el cual es un estándar de la industria para evaluar la gravedad de las vulnerabilidades de seguridad informática del sistema.

F. Informes

Los informes de la Metodología Adaptada incluyen los criterios básicos contenidos en los informes de pruebas de penetración de las metodologías de OSSTMM, ISSAF y PTES, con el fin de fortalecer y complementar dichos criterios propuestos.

G. Recomendaciones

Se establecen recomendaciones sobre cómo se deben llevar a cabo cada una de las fases de la Metodología adaptada para analizar y evaluar la seguridad proporcionada por DNSSEC en un escenario de pruebas controlado en redes IPv6, con base en las recomendaciones que proponen las metodologías ISSAF, OSSTMM y PTES.

H. Meticulosidad

El nivel de meticulosidad de la Metodología Adaptada, tiene en cuenta la minuciosidad y exactitud que aportan la metodología ISSAF para el manejo detallado de la guía técnica para la realización de cada una de las pruebas, haciendo uso de herramientas actualizadas como el manejo exhaustivo de OSSTMM para el manejo de la métrica, en nuestro caso orientada a llevar a cabo un correcto análisis de la evaluación de la seguridad teniendo en cuenta el estándar CVSS. De igual forma teniendo en cuenta los criterios contenidos en los reportes y los lineamientos de acción de todas las metodologías estudiadas.

I. Usabilidad y uso

El nivel de usabilidad de la Metodología Adaptada es alto, como resultado a la meticulosidad en la descripción de la planeación, la prueba técnica de penetración, la evaluación de los resultados obtenidos mediante el CVSS y la presentación de informes.

V. FASES DE LA METODOLOGÍA ADAPTADA

Con base en el análisis de las metodologías anteriores, se determinó que la Metodología Adaptada para analizar y

evaluar la seguridad de DNSSEC en Redes de Información IPv6 está conformada por las siguientes cuatro Fases principales, como se observa en la Figura 3:

Figura 3. Fases de la Metodología Adaptada.
Fuente: Los autores.

VI. METODOLOGÍA ADAPTADA PARA ANALIZAR Y EVALUAR LA SEGURIDAD DE DNSSEC EN REDES DE INFORMACIÓN IPV6

A. Fase 1: Planeación

En esta fase, se describen los objetivos, el tipo de test de intrusión, el diagrama de red del ambiente de prueba, el alcance y el plan de pruebas definido que se llevará a cabo en el escenario real de pruebas controlado, como se muestra a continuación:

- 1) **Objetivo:** analizar y evaluar la seguridad proporcionada por DNSSEC en redes de información IPv6 en el escenario real de pruebas controlado.
- 2) **Tipo de test de intrusión:** Caja Gris.
- 3) **Alcance:** Pruebas en las redes interna y externa del escenario con determinados requisitos de seguridad.
- 4) **Diagrama de red:** es el escenario de pruebas controlado, mostrado en la Figura 1.
- 5) **Plan de pruebas:** El plan de pruebas de seguridad se divide en dos tipos de pruebas, el plan de pruebas de recolección de información y el plan pruebas de identificación y explotación de vulnerabilidades, indicando con una X las pruebas que se realizaron en cada escenario, como se muestra en las Tabla II y III.

TABLA II
PLAN DE PRUEBAS DE RECOLECCIÓN DE INFORMACIÓN

	SISTEMA OPERATIVO	EJECUCIÓN DE LA PRUEBA	RED OBJETIVO	PoC	DNS	DNSSEC
RECOLECCIÓN DE INFORMACIÓN	Centos Debian Windows-Debian Windows-Centos	RED INTERNA	INTERNA	Descubrir host activos en segmento de red	X	X
				Encontrar Sistemas Operativos servicios y versiones	X	X
				Identificar relaciones IPv6 con servidores, dominios y subdominios	X	X
			EXTERNA	Identificar relaciones IPv6 con servidores, dominios y subdominios	X	X

TABLA III
PLAN DE PRUEBAS DE EXPLOTACIÓN DE VULNERABILIDADES IDENTIFICADAS

	SISTEMA OPERATIVO	EJECUCIÓN DE LA PRUEBA	SERVIDORES O DOMINIOS INTERNO/ EXTERNO OBJETIVO	POC	DNS	DNSSEC NSEC	DNSSEC NSEC3
IDENTIFICACIÓN Y EXPLOTACIÓN DE VULNERABILIDADES	Centos Debian Windows-Debian Windows-Centos	INTERNA	INTERNA	Transferencia de zona	X	X	X
				Enumeración de dominios por consultas incorrectas		X	X
				Denegación de servicio	X		X
				DNS Spoofing			X
		INTERNA	EXTERNA	Transferencia de zona	X	X	X
				Enumeración de dominios por consultas incorrectas		X	X
				Denegación de servicio	X		X
				DNS Spoofing			X

B. Fase2: Penetración

Esta fase se lleva a cabo las actividades de Recolección de información e Identificación y Explotación de Vulnerabilidades.

- 1) **Identificación de Vulnerabilidades:** Esta actividad se realizó con base en la documentación investigada donde se encontraron una serie de posibles vulnerabilidades del servicio DNS y DNSSEC relacionadas con:
 - El uso de *DNSSEC con RR NSEC*, que permite enumerar el contenido de una zona, a partir de la consulta de Nombres de Dominio que no existen. RFC 5551, RFC 7129 [13], [14].
 - El uso de *UDP como protocolo de transporte*, que posibilita IP spoofing. RFC3833 [12].

- El Resolver DNSSEC no puede verificar las respuestas que se originan en una zona sin firmar. RFC4033 [4].
- Un Cliente resolver que NO realiza validación. RFC4033 [4].

2) **Explotación de Vulnerabilidades:** Para verificar la existencia de vulnerabilidades en DNSSEC, se realizaron las siguientes PoC:

1. Transferencia de zona.
2. Enumeración de dominio por consultas incorrectas.
3. Denegación de Servicio.
4. Secuestro de URL por ataque Typosquatting.
5. DNS Spoofing.

C. Fase 3: Evaluación de vulnerabilidades

La evaluación de las vulnerabilidades de DNSSEC en redes IPv6, se realizó con base en el Sistema de Puntuación de Vulnerabilidad Común CVSS [15], que proporciona una forma de capturar las características principales de una vulnerabilidad y producir una puntuación numérica asociado a un valor de severidad, como se observa en la Tabla IV, y está compuesto por tres grupos principales de métricas: Base, Temporal y de Entorno, cada una con un conjunto de métricas como se observa en la Tabla V:

TABLA IV
 PUNTUACIÓN CVSS Y VALOR CUALITATIVO (SEVERIDAD)

Puntuación	Severidad
0	Nula
0.1-3.9	Baja
4.0-6.9	Media
7.0-8.9	Alta
9.0-10.0	Crítica

TABLA V
 FASE DE EVALUACIÓN DE VULNERABILIDADES

GRUPO METRICAS BASE	GRUPO METRICAS TEMPORAL	GRUPO METRICAS ENTORNO
Métricas de Explotabilidad <ul style="list-style-type: none"> • Vector de Ataque • Complejidad de Ataque • Requerimiento de Privilegios • Interacción de Usuarios Métricas de Impacto <ul style="list-style-type: none"> • Impacto de Confidencialidad • Impacto de Integridad 	<ul style="list-style-type: none"> • Madures del Código de Explotación • Nivel Remediación • Reporte de Confianza 	<ul style="list-style-type: none"> • Requisitos de Confidencialidad • Requisitos de Integridad • Requisitos de Disponibilidad

Se realizó el cálculo CVSS en cada Prueba de Concepto de las actividades de la Fase 2 de Penetración, determinando los valores de cada uno de los parámetros de las métricas Base, Temporal y Ambiental, hasta obtener el resultado final de la severidad de la vulnerabilidad [16]. A continuación se muestra un Ejemplo de los resultados obtenidos:

1) Evaluación de vulnerabilidad con la PoC DNS Spoofing Dominio Inexistente, Cadena de Confianza Firmada

En este ejemplo se realiza el cálculo de la severidad con la PoC de DNS Spoofing exitosa, cuando la cadena de confianza DNSSEC está Firmada y el MITM se realiza entre el Servidor Caché Validador Windows Server y la Gateway de la red CAFE cuando el Cliente No Validador consulta por el Dominio inexistente **coomunicate.com**, y el escenario está implementado sobre el sistema operativo Windows-Centos/Debian (Red interna-Red Externa).

Figura 4. PoC DNS Spoofing, Dominio Inexistente.
 Fuente: Los autores.

TABLA VI
 PUNTAJE BASE

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICAS BASE	Vector de ataque	AV	Adyacente	7.9
	Complejidad de ataque	AC	Alto	
	Privilegios requeridos	PR	Ninguno	
	Interacción de usuario	UI	Requerido	
	Alcance	S	Cambio	
	Confidencialidad	C	Alto	
	Integridad	I	Alto	
	Disponibilidad	D	Alto	

TABLA VII
 PUNTAJE TEMPORAL

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICA TEMPORAL	Explotar el vencimiento del Código	E	Alto	7.7
	Nivel de remediación	RL	solución Alternativa	
	Informe de confianza	RC	Confirmado	

TABLA VIII
PUNTAJE AMBIENTAL

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICAS AMBIENTALES	Requisito de Confidencialidad	CR	Bajo	7.7
	Requisito de Integridad	IR	Alto	
	Requisito de Disponibilidad	DR	Alto	

Una vez asignado los valores de cada uno de los parámetros de las métricas Base, Temporal y Ambiental para esta prueba de concepto, se determina que el valor cuantitativo de la vulnerabilidad está representado por el siguiente puntaje como se puede apreciar en la Figura 5:

Figura 5. Cálculo Puntaje general CVSS
Fuente: Los autores.

TABLA IX
PUNTUACIÓN CVSS DNS SPOOFING

Puntuación	Severidad
7.7	Alta

Como se obtiene una **Puntuación CVSS** de 7.7 esta corresponde a una **severidad asociada de Media**.

D. Fase 4: Reporte de auditoría

Se divide en 2 reportes:

- Reporte ejecutivo:** tiene como objetivo dar conocer de manera resumida los resultados obtenidos de las PoC, con su respectivo análisis, conclusiones y recomendaciones.
- Reporte técnico:** Se documentan todos los hallazgos de las PoC realizadas sobre el escenario real de pruebas controlado, con una descripción escrita, las herramientas utilizadas, la topología de red, el ambiente real de la prueba, las características de los equipos involucrados por prueba, capturas de pantalla como evidencia y algunas recomendaciones para tener en cuenta.

En las Tablas X, XI y XII, se muestra la clasificación de severidad, con las PoC exitosas en el escenario real de pruebas controlado DNSSEC en redes de información IPv6:

TABLA X
CLASIFICACIÓN DE SEVERIDAD, CON LAS PRUEBAS EXITOSAS DE LA ACTIVIDAD DE RECOLECCIÓN DE INFORMACIÓN

SISTEMA OPERATIVO	EJECUCIÓN DE LA PRUEBA	ESTADO DE LA CADENA DE CONFIANZA DNSSEC	PRUEBA	N° PoC exitosas	SEVERIDAD
Centos/Debian Windows-Debian Windows-Centos	Red Interna	Firmada	Encontrar hosts activos en el segmento de red	1	BAJA
			Encontrar Ss. Os, servicios y versiones	1	MEDIA
			Identificar Relaciones de Direcciones IPv6 con Servidores, Dominios y Subdominios	4	MEDIA
			Total de pruebas		6

TABLA XI
CLASIFICACIÓN DE SEVERIDAD, CON LAS PRUEBAS EXITOSAS DE LA ACTIVIDAD DE IDENTIFICACIÓN Y EXPLOTACIÓN DE VULNERABILIDADES

SISTEMA OPERATIVO	EJECUCIÓN DE LA PRUEBA	ESTADO DE LA CADENA DE CONFIANZA DNSSEC	PRUEBA	N° PoC EXITOSAS	SEVERIDAD
Centos	Red Interna	Firmada	Transferencia de Zona	2	BAJA
	Red Externa			4	BAJA
Centos/Debian Windows-Debian Windows-Centos	Red Interna	Firmada	Enumeración de Dominios por Consultas Incorrectas	2	BAJA
			Denegación de Servicio (DoS)	2	ALTA
			Total de pruebas	10	

TABLA XII
CLASIFICACIÓN DE SEVERIDAD, CON LAS PRUEBAS EXITOSAS DE DNS SPOOFING

SISTEMA OPERATIVO	EJECUCIÓN DE LA PRUEBA	ESTADO DE LA CADENA DE CONFIANZA DNSSEC	ESTADO DEL DOMINIO	PRUEBA	N° PoC EXITOSAS	SEVERIDAD
Debian/Centos	Red Interna	Firmada	F-int / F-ext / NF / NF-I	DNS Spoofing	21	MEDIA
Windows-Centos Windows-Debian			F-int / F-ext	DNS Spoofing	3	MEDIA
			NF-I	DNS Spoofing	3	ALTA
Centos/Debian Windows-Debian Windows-Centos	Red Interna	Rota	F-int / NF / NF-I	DNS Spoofing	23	MEDIA
			F-ext	DNS Spoofing	6	ALTA
Debian	Red Externa	Firmada	F-ext / NF-I	DNS Spoofing	2	ALTA

VII. CONCLUSIONES

- Para analizar y evaluar la seguridad de los Servicios de Internet DNS, DNSSEC y Web en Redes IPv6, se requiere implementar toda la Jerarquía DNS y la Cadena de confianza DNSSEC, en un escenario de pruebas controlado
- La Metodología Adaptada para analizar y evaluar la seguridad de DNSSEC en Redes de Información IPv6 incluye las siguientes las Fases: Planeación, Penetración, Evaluación de Vulnerabilidades y Reporte de Auditoría.

- Implementar DNSSEC en Windows Server, es mucho más complejo que implementar DNSSEC en un una Distribución de Linux, se requiere mayor capacidad de recursos y procesamiento, para optimizar el servicio.

- Para la Recolección de Información y Explotación de las Vulnerabilidades relacionadas con la seguridad de DNSSEC en Redes IPv6, actualmente son muy pocas las herramientas existentes y disponibles.

Con base en la **clasificación de severidad**, con las PoC de DNS Spoofing, **se determinó que los peores escenarios en que DNSSEC NO proporciona sus funciones de seguridad:** autenticación del origen, y autenticación e integridad de los datos de DNS.

- Cuando la **cadena de confianza está firmada**, el peor escenario presenta una clasificación de **severidad Media**, cuando el proceso de **validación DNSSEC es realizado únicamente por el Servidor Caché o cuando se consulta por un dominio NO firmado**, debido que bajo este escenario, **el cliente que no realiza el proceso de validación es vulnerable a la suplantación de dominio** al aceptar la respuesta falsa del atacante.
- Cuando la **cadena de confianza está rota**, el peor escenario presenta una clasificación de **severidad Alta**, cuando **se consulta por un dominio firmado y el cliente como el servidor cache que realicen el proceso de validación DNSSEC no tienen almacenada el ancla de confianza del dominio**, de modo que no se puede realizar la validación de la respuesta.

Con base en las **PoC NO exitosas** de DNS Spoofing, **se determinó que los mejores escenarios en que DNSSEC PROPORCIONA sus funciones de seguridad:** autenticación del origen, y autenticación e integridad de los datos de DNS.

- Cuando la **cadena de confianza está firmada**, el mejor escenario se presenta cuando el **Cliente como el Servidor Caché con soporte de validación DNSSEC, tienen almacenada el ancla de confianza del servidor Raíz y/o del dominio interno de la organización**, de esta manera son capaces de validar las respuestas DNS y evitan la suplantación de identidad de un dominio y el envenenamiento de la memoria caché.
- Cuando la **cadena de confianza está rota**, el mejor escenario se presenta cuando el **Cliente como el Servidor Caché con soporte de validación DNSSEC, tienen almacenada el ancla de confianza de un dominio firmado con DNSSEC**.
- DNSSEC NO protege contra ATAQUES de:

1. Denegación de Servicio (DoS, Denial of Service).
2. Transferencia de zona.
3. MITM (Man in the Middle).

REFERENCIAS

- [1] R. Arends, " Internet Protocol, Version 6 (IPv6) Specification", IETF, RFC 2460, Diciembre 1998.
- [2] P. Mockapetris, "Domain Names - Implementation And Specification", IETF, RFC 1035, November 1987.R.
- [3] C. Gónzales, "Análisis de vulnerabilidades del DNS", Proyecto de Grado, Ingeniería de Sistemas Telemáticos, E.T.S.I. Telecomunicación (UPM), Madrid, 2015.
- [4] Arends, "DNS Security Introduction and Requirements", IETF, RFC 4033, Marzo 2005.
- [5] R. Arends, "Resource Records for the DNS Security Extensions", IETF, RFC 4034, Marzo 2005.
- [6] R. Arends, "Protocol Modifications for the DNS Security Extensions", IETF, RFC 4035, Marzo 2005.
- [7] T. E. Sánchez, "Extensiones de Seguridad para el Sistema de Nombres de Dominio", Trabajo de Grado, Facultad de informática, Universidad Nacional de la Plata, UNLP, Argentina, 2012.
- [8] Y. Rekhter, "IPv6 Address Specific BGP Extended Community Attribute", IETF, RFC 5701, Noviembre 2009.
- [9] Rathore and Oissg, "ISSAF-Information Systems Security Assessment Framework 0.2.1B," p. 845, 2006.
- [10] Herzog,Pete, "OSSTMM: The Open Source Security Testing Methodology Manual: v3", 2010.
- [11] Nickerson, D. Kennedy, and C. J. Reil, "The Penetration Testing Execution Standard," 2014, 2017.
- [12] Atkins, "Threat Analysis of the Domain Name System", IETF, RFC 3833, Agosto 2004.
- [13] R. Gellens, Ed, "Lemonade Notifications Architecture", IETF, RFC 5551, Agosto 2009.
- [14] R. Gieben, "Authenticated Denial of Existence in the DNS", IETF, RFC 7129, Febrero 2014.
- [15] T. Base and T. Base, "Common Vulnerability Scoring System v3. 0 Examples," no. July, pp. 1–38, 2016.
- [16] FIRST.org. (1989). Common Vulnerability Scoring System Version 3.0 Calculator [Online]. Available: <https://www.first.org/cvss/calculator/3.0>FIRST.org

Dalia Kelly Terán Arévalo Ingeniera en Electrónica y Telecomunicaciones de la Universidad del Cauca. Candidata a Magister en Seguridad Informática de UNIR “Universidad Internacional de la Rioja - España”. Áreas de interés: Seguridad en redes y sistemas de información, protocolos de routing en IPv4 e IPv6, Redes IPv4/IPv6 cableadas e inalámbricas.

Diana Victoria Fernández García Ingeniera en Electrónica y Telecomunicaciones de la Universidad del Cauca. Áreas de interés: lenguajes de programación C, Linux y MatLab. Experiencia en la configuración e instalación de servidores Windows, Linux y Centos.

Francisco Javier Terán Cuarán Magíster en Electrónica y Telecomunicaciones, Universidad del Cauca. Ingeniero en Electrónica, Universidad del Cauca. Pasantía Internacional en Redes y Servicios Telemáticos, Universidad de Chile. Gestor, Promotor y Coordinador del Programa de Especialización en Redes y Servicios Telemáticos de la Universidad del Cauca. Gestor y Promotor del Programa de Ingeniería de Sistemas de la Universidad del Cauca. Gestor, Promotor y Coordinador de la Red de Información de la Universidad del Cauca. Gestor y Promotor del Programa de Maestría en Telecomunicaciones de la Universidad del Cauca. Profesor Titular de Planta adscrito al Departamento de Telecomunicaciones de la FIET de la Universidad del Cauca. Profesor en pregrado y posgrado de la FIET. Decano de la Facultad de Ingeniería Electrónica y Telecomunicaciones (FIET) de la Universidad del Cauca. Jefe del Departamento de Telecomunicaciones de la FIET. Jefe de la División de Tecnologías de la Información y las Comunicaciones (TIC) de la Universidad del Cauca. Auditor interno de Sistemas de Gestión de Seguridad de la Información ISO 27001, Certificación de Bureau Veritas. Áreas de interés: Redes y Servicios IPv4. Enrutamiento IPv4/IPv6, Internetworking, Redes y Servicios IPv6, IPv4/IPv6 móvil, Seguridad en Redes y Sistemas de Información, SGSI Sistemas de Gestión de la Seguridad de la Información y Datacenters.