UN ENFOQUE PARA LA IDENTIFICACIÓN Y EL ANÁLISIS FORENSE DE ATAQUES DNS

ARTÍCULO ORIGINAL

SOUSA, Robson Everton[1], VALE, Samyr[2]

SOUSA, Robson Everton. VALE, Samyr. **Un enfoque para la identificación y el análisis forense de ataques DNS.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Año 08, Ed. 07, Vol. 01, pp. 24-44. Julio de 2023. ISSN: 2448-0959, Enlace de acceso: https://www.nucleodoconhecimento.com.br/ciencias-de-la-computacion/analisis-forense, DOI: 10.32749/nucleodoconhecimento.com.br/ciencias-de-la-computacion/analisis-forense

RESUMEN

Los servidores de resolución de nombres de dominio (DNS) desempeñan una función clave en el establecimiento del acceso a las páginas web. Debido a su importancia, son constantes objetivos de ciberataques, que tienen como objetivo borrar o reemplazar algunos de sus registros, causando enormes pérdidas para los usuarios, empresas e instituciones en todo el mundo. En Brasil, para prevenir tales ataques, se establece una disposición legal que tipifica penalmente la invasión de dispositivos informáticos conectados a la *World Wide Web*, lo que incluye ataques al servicio de DNS. Sin embargo, la identificación de ciberataques es difícil, ya que depende de la correcta aplicación de medios de protección, monitoreo de servicios de red y extracción e interpretación de datos que permitan la identificación de factores criminales. El presente trabajo propone un enfoque forense computacional para detectar automáticamente la ocurrencia de un ataque de envenenamiento de la memoria caché de DNS, subsumiendo los elementos que constituyen el ataque al dispositivo legal, identificando así la comisión de un delito.

Palabras clave: Informática forense, Delitos informáticos, Redes de computadoras.

1. INTRODUCCIÓN

Los servidores de resolución de nombres de dominio (DNS) son una de las infraestructuras más importantes de Internet que mapean las conexiones entre el nombre de dominio (URL) y la dirección de protocolo de Internet (IP) (Wang, Zang y

Lan, 2018). A pesar de su gran importancia, tiene deficiencias debido a que se pasaron por alto algunos problemas de seguridad durante su creación.

Los ataques DNS son bastante recurrentes; el 92% de las redes analizadas están sujetas a al menos un tipo de envenenamiento de la caché de DNS (Alharbi *et al.*, 2019). Esto fue corroborado al evaluar el 97% de los resolutores que operan de manera abierta, el 74% de las redes corporativas a través de servidores de correo electrónico y el 68% de los proveedores de servicios de Internet (ISP) medidos a través de anuncios en red.

Aunque las herramientas de seguridad y protección de redes, como los sistemas de detección de intrusiones (IDS), monitorean la actividad y el tráfico de la red, incluyendo posibles ataques, estos registros se almacenan en archivos de registro internos y se actualizan constantemente de manera dinámica. Típicamente, los datos generados allí permanecen sin procesar, actuando solo como información de ocurrencia de eventos para los administradores de red. A menudo, cuando se detectan ataques repetidos, los registros de actividades de piratería se pierden invariablemente entre el gran volumen de información generada por estas herramientas. La razón de esto es que no están destinados a realizar análisis forenses, sino solo a proteger el tráfico de datos.

El enfoque propuesto tiene como objetivo identificar las características de un delito de intrusión en dispositivos informáticos, en particular los ataques a servidores DNS, y reconocer la intrusión para hacer cumplir las leyes penales apropiadas.

Una vez hecho esto, el enfoque propone registrar pruebas de la ocurrencia de un ataque en un documento de experto cualificado. Luego, estos datos pueden ser analizados e interpretados para determinar si el tráfico de datos en un servidor DNS es una actividad estándar o una intrusión intentada. Con este fin, se analizan los desastres de red notificados por el IDS para identificar a su atacante, la técnica de invasión utilizada, su dirección IP de origen y destino, la hora de la ocurrencia del ataque, los servicios informáticos afectados y el alcance del daño causado.

El resto de este artículo se estructura de la siguiente manera. La Sección II describe el contexto tecnológico del estudio actual; la Sección III presenta trabajos relacionados en la literatura y sus deficiencias; la Sección IV trata el análisis forense utilizando herramientas de DNS; y finalmente, la Sección V presenta las conclusiones.

2. PANORAMA TECNOLÓGICO

Según Lencse (2020), el Sistema de Nombres de Dominio (DNS) es un recurso tecnológico importante capaz de soportar ampliamente la *World Wide Web*, siendo imperceptible cuando funciona correctamente. Sin embargo, cuando ocurre una falla, la desaceleración que afecta la calidad del servicio se vuelve rápidamente perceptible.

Según Naqash *et al.* (2012), la arquitectura del DNS no logró agregar los criterios de seguridad necesarios para bloquear la recepción de datos falsificados en la caché del servidor DNS. Hmood *et al.* (2015) y Steinho, Wiesmaier y Araújo (2006) mencionan que los delincuentes aprovechan esta vulnerabilidad al insertar información falsificada en la caché de los servidores DNS y cambiar los parámetros de referencia para hacerlo no disponible o redirigir su tráfico a páginas maliciosas. Estos parámetros pueden cambiar de recursivos a autoritativos durante el flujo de consultas.

2.1 TECHNIQUES AND ATTACKS ON DNS

Kim y Reeves (2020) describen los ataques a servidores DNS como actos de manipulación de datos, inundación, abuso del DNS y estructura de contraataque al servidor DNS. Esta clasificación permite analizarlos por áreas de acuerdo a los diferentes intereses de los atacantes. El presente trabajo tiene como objetivo analizar el envenenamiento de caché DNS, que, según Kim y Reeves (2020), cae bajo la modalidad de manipulación de datos.

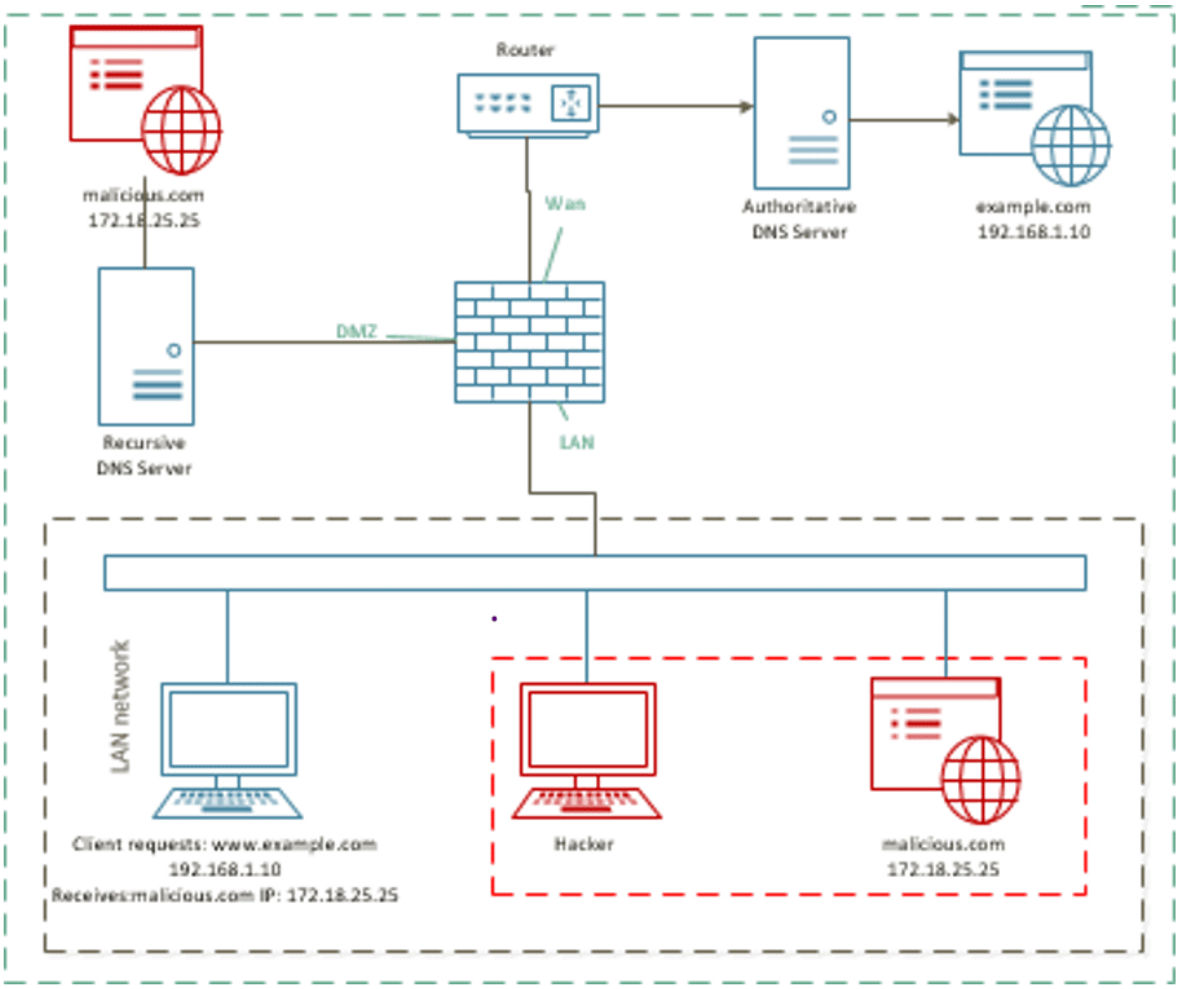
Zhang *et al.* (2021) y Kaminsky *et al.* (2008) mencionan que uno de los primeros envenenamientos de caché DNS fue descubierto por Kaminsky en 2008. A diferencia del envenenamiento de caché local, el envenenamiento de caché DNS se puede realizar de forma remota. Según Tripathi, Swarnkare y Hubballi (2018), el

envenenamiento de caché local es más fácil de implementar que el envenenamiento de caché DNS, ya que el atacante solo necesita estar presente en el mismo segmento de red para enviar identificadores falsos (Figura 1). Si coincide con el original, puede envenenar la caché del servidor DNS local y realizar un mapeo incorrecto.

Según Hussain *et al.* (2016), el envenenamiento de caché DNS también se puede llevar a cabo a través del spoofing de DNS, donde se falsifica el origen de un paquete de mensajes DNS. Esta técnica es ventajosa para los atacantes, ya que cambia los campos de origen y destino de la dirección IP (Liska y Stowe, 2016).

De acuerdo con Tripathi, Swarnkare y Hubballi (2018), este método permite que los campos de los paquetes IP se llenen con una dirección que no coincide con la IP real, lo que puede llevar a los usuarios a realizar conexiones inseguras (Figura 1).

Figura 1. Envenenamiento de un servidor DNS recursivo mediante la técnica de envenenamiento de caché DNS



Fuente: Autor (2023).

Wang (2014), Kim y Reeves (2020) y Zhang *et al.* (2021) han investigado el envenenamiento de caché DNS utilizando la técnica Kaminsky. Los autores enfatizan que a pesar de que la implementación de este ataque es más costosa, es bastante perjudicial y afecta sustancialmente a un servidor DNS autoritario que presta servicios a diversas redes. Este tipo de ataque ha atraído considerable atención entre los investigadores debido a sus graves impactos y consecuencias.

2.2 SISTEMA DE DETECCIÓN DE INTRUSOS

Según lo informado por Eskandari *et al.* (2020), los sistemas de detección de intrusos (IDS) monitorean y analizan eficazmente el tráfico de la red o del host. Este análisis se realiza utilizando firmas o basado en un modelo de comportamiento.

Vazão (2021) informó que cuando se detectan violaciones de reglas, se guardan en un archivo de evidencia. Estos registros se conocen como registros *("logs")* y proporcionan información relevante necesaria para identificar la hora del ataque, los servicios violados, la identidad del atacante y el daño causado. Estos registros están disponibles en formato de texto y son indispensables para identificar intrusiones en la infraestructura de la red y determinar si el delito ocurrió o no.

3. TRABAJOS RELACIONADOS

Newton y Beliche (2020) propusieron un enfoque forense para la detección y análisis de ataques de denegación de servicio (DoS) con el fin de establecer la ocurrencia de un delito de interrupción del servicio informático según lo establecido en la Ley n. 12.737/2012. Este enfoque se centró en el delito de perturbación, excluyendo el análisis del delito de invasión, que es el tema de este artículo. Vazão (2021) comparó cuatro soluciones de gestión de información y eventos de seguridad que presentaban un marco de registro centralizado de aplicaciones y equipos de red para identificar vulnerabilidades. Estos registros se utilizaron como entrada para medidas de reparación y contención de amenazas. A pesar de esta iniciativa, la investigación no consideró hechos relacionados con la legislación sobre delitos informáticos.

Este artículo propone un enfoque forense para capturar la evidencia de los ataques contra los servidores DNS a través de herramientas de monitoreo y protección de redes. En primer lugar, los datos de ataque recopilados se almacenan en una base de datos de registro de intrusiones; luego, los hechos se consideran a la norma, y finalmente se genera un informe forense como evidencia legal de la ocurrencia de un delito.

4. ENFOQUE FORENSE PARA ATAQUES DNS - FORDNS

El enfoque propuesto analiza las reclamaciones de la red informadas por el IDS para identificar al atacante, la técnica de intrusión, las direcciones IP de origen y destino, la hora, los servicios de red afectados (servidores) y el daño causado. Luego, estos datos se analizan para identificar actividades delictivas contra el servidor DNS a la luz de la legislación brasileña (Artículo 154-A del Código Penal). Este proceso genera un informe que puede ayudar a las autoridades a identificar al atacante, los hechos, las víctimas, las circunstancias y las consecuencias, y determinar los procedimientos legales apropiados.

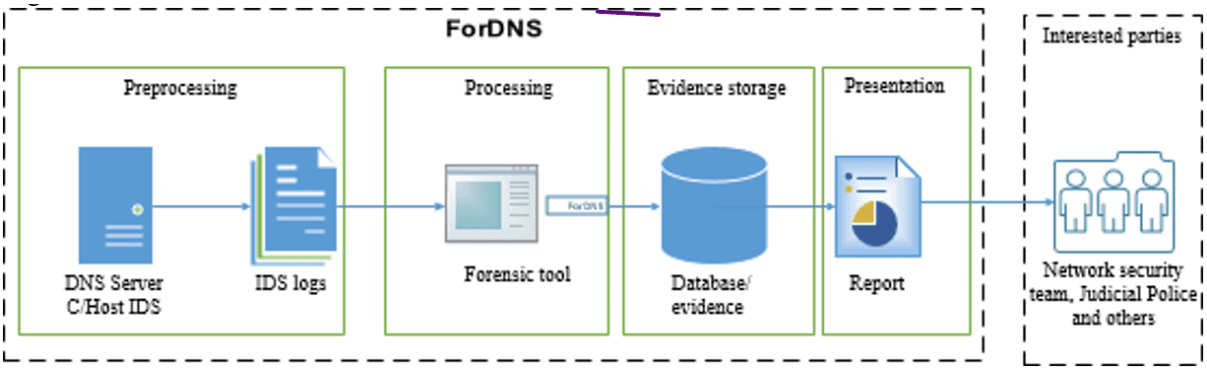
4.1 PROCESO

Las Figuras 2 y 3 ilustran el análisis forense de un servidor DNS utilizando el enfoque propuesto. Esta herramienta recopila datos de infracción que corroboran los delitos informáticos, ya que la mayoría de ellos no se investigan debido a la falta de pruebas o a la volatilidad de los datos registrados en el archivo de registro.

Esta herramienta es parte de una arquitectura informática que automatiza el análisis de ataques a servidores DNS. En la mayoría de los casos, estos ataques son identificados manualmente por profesionales de seguridad de la información, que primero localizan la vulnerabilidad (si aún está en el archivo de registro del IDS), extraen los datos y los envían a quienes pueden determinar si se ha cometido un delito.

El IDS Suricata puede monitorear el servidor DNS en modo HIDS, es decir, monitorea un servidor (anfitrión) que proporciona servicios DNS. Para identificar correctamente una actividad maliciosa, los dispositivos de seguridad en las redes informáticas, como el cortafuegos y el IDS, deben aplicarse y configurarse correctamente.

Figura 2. FORDNS



Fuente: Autor (2023).

En el enfoque propuesto, una detección de intrusión desencadena una alerta del IDS. Luego, el administrador de red inicia la herramienta forense desarrollada para examinar los registros del IDS. La herramienta escanea el archivo de registro; si encuentra referencias a ataques al servidor DNS, captura la evidencia principal y la almacena en una base de datos. Esta base de datos genera un informe que se puede utilizar para un análisis posterior y actuar como prueba del delito. Esto es posible debido a la forma en que el IDS pone sus datos a disposición, permitiendo que los datos contenidos en el registro sean leídos y capturados.

La Figura 2 muestra el flujo de trabajo del enfoque propuesto. El IDS ejecuta las etapas de preprocesamiento del tráfico de red y procesamiento de los registros del IDS y almacena la evidencia criminal. Luego, se extrae y analiza el informe que contiene la información principal de los delitos según los tipos delictivos.

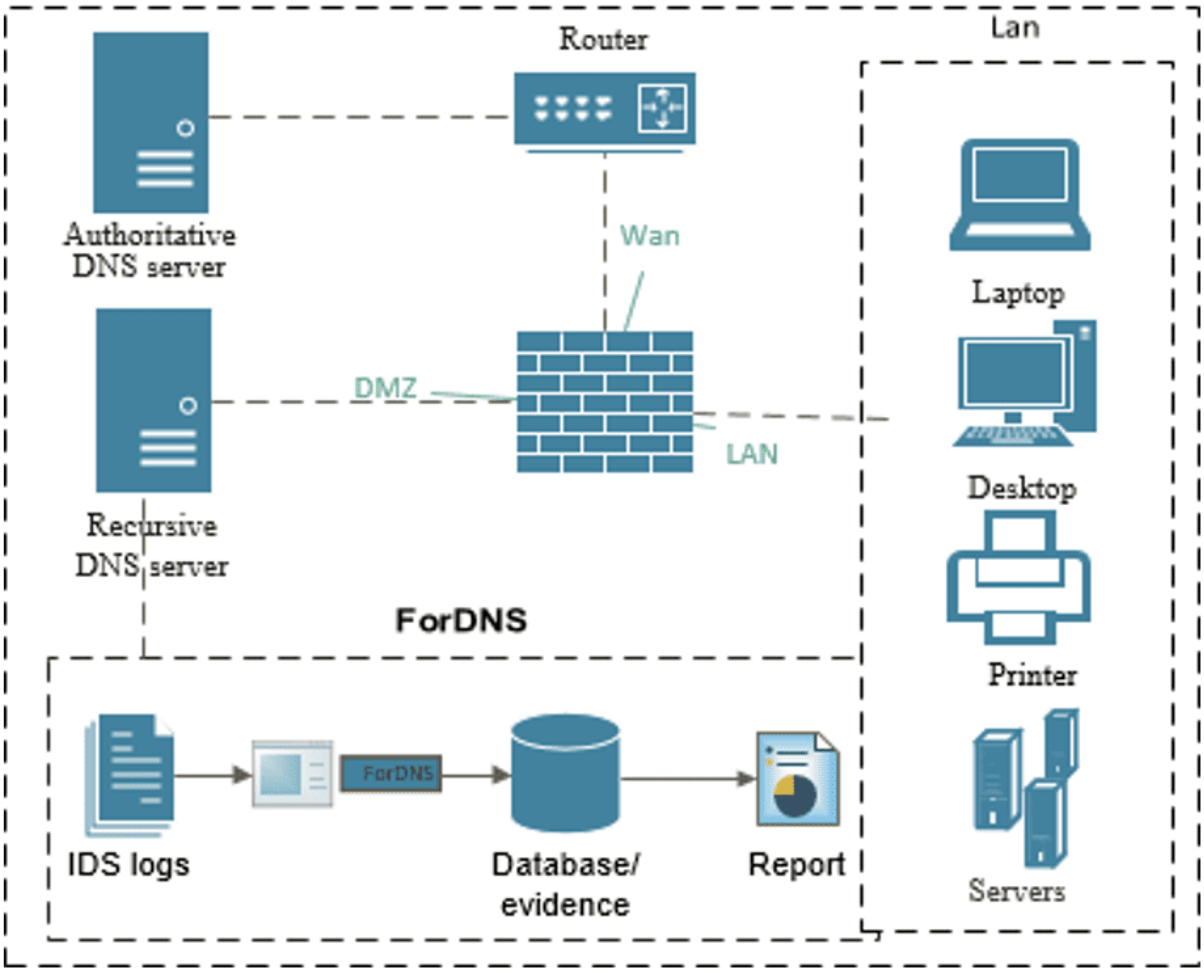
4.2 ARQUITETURA FORDNS

Por lo general, la arquitectura de una red corporativa consta de los siguientes elementos: un enrutador que interconecta la red WAN (externa), es decir, la *World Wide Web*, donde se encuentran ubicados el servidor DNS autorizado y otros servicios de Internet; la red LAN, que es la red interna de la empresa donde se encuentran los hosts de usuarios que demandan servicios de Internet y otros servicios de red privada; el *Firewall,* que es una herramienta de seguridad de red; y la DMZ (Zona

Desmilitarizada), una área que comparte servicios de red disponibles para acceso público o privado.

La arquitectura del enfoque desarrollado *ForDNS* comprende un *software* que lee y analiza los registros del IDS. La información extraída de estos registros se almacena en una base de datos cuyo propósito principal es generar informes forenses, que pueden servir como evidencia del ataque.

Figura 3. Arquitectura



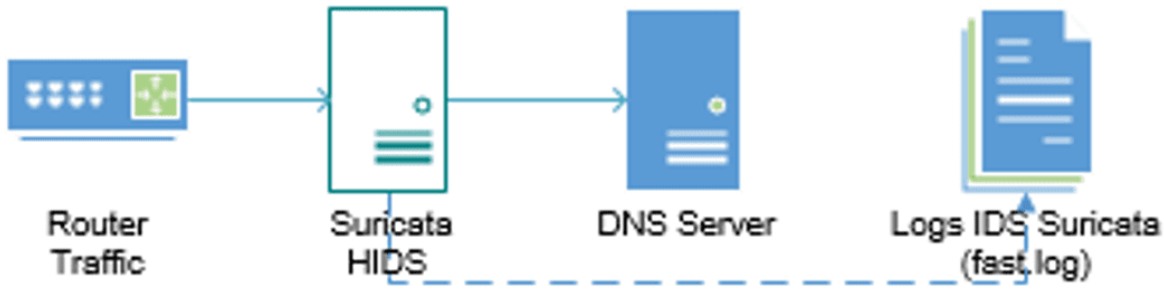
Fuente: Autor (2023).

RC: 149501
Disponible: https://www.nucleodoconhecimento.com.br/ciencias-de-la-computacion/analisis-forense

4.3 PREPROCESAMIENTO DEL TRÁFICO DE RED POR EL IDS SURICATA

Como se muestra en la Figura 4, el preprocesamiento es la primera fase de la investigación donde se generará la fuente de datos. El archivo de registro (llamado *fast.log*) del IDS Suricata (OISF, 2023) registra todos los incidentes que ocurren mientras se monitorean los paquetes de red.

Figura 4. Preprocesamiento



Fuente: Autor (2023).

El IDS recibe el tráfico de la red, analiza los paquetes según las firmas registradas y, en caso de coincidencia entre las reglas y los paquetes procesados, registra el incidente en el archivo de registro (*fast.log*) y alerta al equipo de monitoreo (Eldow *et al.,* 2016). Estos registros contienen la información necesaria para identificar datos importantes, incluyendo mensajes, flujo de red, referencias, números de identificación, clasificación y tipo. La Figura 5 describe cada una de las reglas.

Figura 5. Información de las reglas

Information managed in each rule	
Msg	Alerts issued by the Suricata IDS
Flow	Contains guidelines on what should be analysed within the traffic
Content	These are rule references. Registered rules usually have a link to identify their source. When the rule is drafted by the network manager, he can describe it
Sid	Rule identification ID, i.e. the identification number
Ver	Rule version
Classtype	Main information and rule classification

Fuente: Autor (2023).

El análisis de los registros por la herramienta *ForDNS* busca palabras clave como el número de identificación (Sid) de la regla y el (Msg), que comprenden el mensaje que indica el tipo de ataque. La Figura 6 destaca estas palabras clave.

Figura 6. Reglas de detección de envenenamiento de caché DNS

```
root@lab-STI-NI-1401:/var/lib/suricata/rules# grep kaminsky suricata.rules
# alert udp any 53 -> $HOME_NET any (msg:"ET DNS Query Responses with 3 RR's set (50+ in 2 seconds)
tempt"; content: "|81 80 00 01 00 01 00 01|"; offset: 2; depth:8; threshold: type both, track by_src
rl,infosec20.blogspot.com/2008/07/kaminsky-dns-cache-poisoning-poc.html; reference:url,doc.emergingt
classtype:bad-unknown; sid:2008475; rev:4; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
# alert udp any 53 -> $HOME_NET any (msg:"ET DNS Query Responses with 3 RR's set (50+ in 2 seconds)
ttempt"; content: "|85 00 00 01 00 01 00 01|"; offset: 2; depth:8; threshold: type both, track by_sr
rl,infosec20.blogspot.com/2008/07/kaminsky-dns-cache-poisoning-poc.html; reference:url,doc.emergingt
classtype:bad-unknown; sid:2008447; rev:7; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

Fuente: Autor (2023).

Esta información servirá como base para analizar el hecho y su posible conexión con el delito de intrusión en un dispositivo informático conectado a una red de computadoras, de conformidad con el Art. 154-A del Código Penal Brasileño.

4.4 PROCESAMIENTO DE REGISTROS DE IDS CON LA HERRAMIENTA FORENSE

Como se muestra en las Figuras 7 y 8, la herramienta forense procesa la fuente de datos, es decir, el archivo *fast.log*, en búsqueda de palabras clave (SIDs) de las reglas responsables de identificar los ataques.

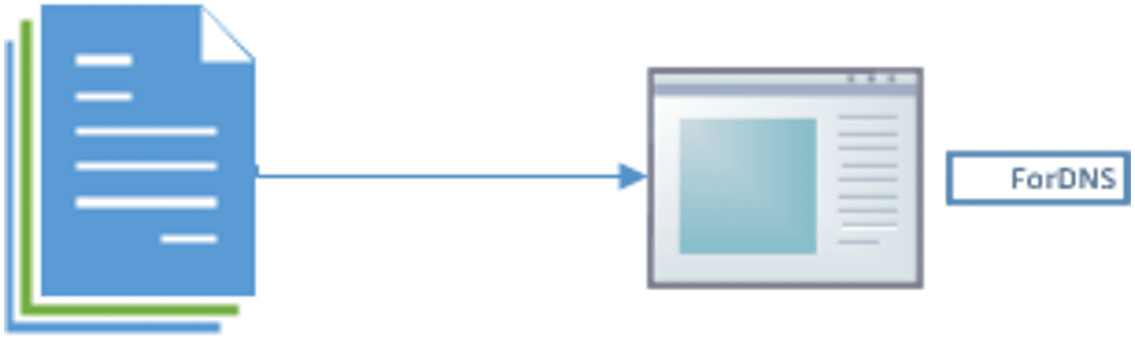
Figura 7. Registros de Meerkat IDS

```
07/11/2022-16:35:14.031606  [**] [1:2008446:9] ET DNS Excessive DNS Responses
with 1 or more RR's (100+ in 10 seconds) - possible Cache Poisoning Attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.71:53 ->
192.168.1.3:61880
```

Fuente: Autor (2023).

Si se detecta una intrusión, la herramienta recopila los siguientes datos: IP de origen, IP de destino, fecha/hora, origen y puertos, y la técnica utilizada para el ataque; estos datos se registran en una base de datos como evidencia de hackeo criminal para su posterior análisis. Finalmente, se genera un informe que contiene los elementos que constituyen el delito.

Figura 8. Procesamiento de evidencia



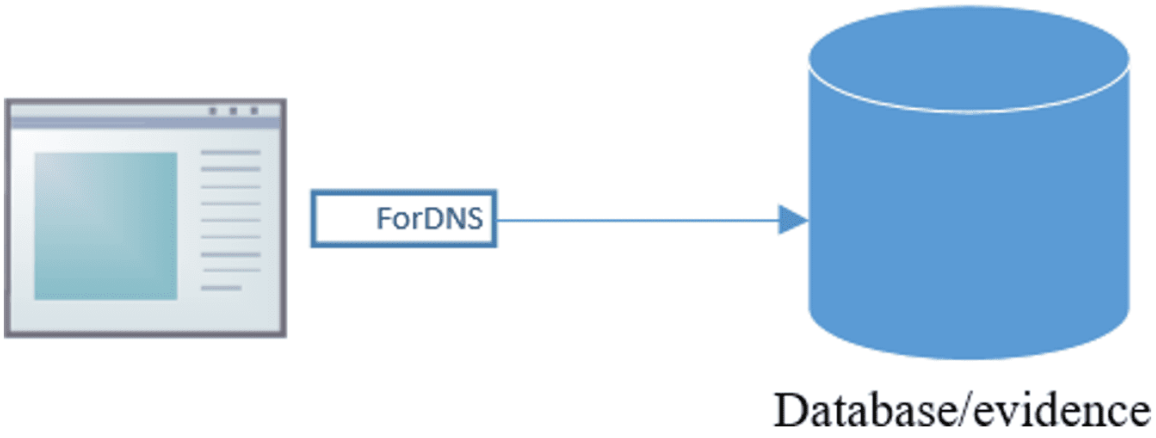
Fuente: Autor (2023).

RC: 149501
Disponible: https://www.nucleodoconhecimento.com.br/ciencias-de-la-computacion/analisis-forense

4.5 REGISTRO DE EVIDENCIA EN LA BASE DE DATOS POR LA HERRAMIENTA FORENSE FORDNS

Como se muestra en la Figura 12, la inserción de evidencia en la base de datos ocurre de la siguiente manera: la herramienta forense (*ForDNS*) analiza la fuente de datos y almacena los siguientes datos en la nueva base de datos: tipo de técnica de intrusión, fecha/hora del ataque, la dirección IP de origen (que identifica al infractor), la dirección IP de destino (que identifica a la(s) víctima(s) y al propietario del servidor DNS), es decir, el origen del ataque, quién fue el objetivo, qué técnica de invasión se adoptó y las consecuencias técnicas de dicho ataque. Estos datos se utilizan para inferir si el delito informático se ha producido de acuerdo con el Código Penal Brasileño.

Figura 9. Almacenamiento de Evidencia



Fuente: Autor (2023).

RC: 149501
Disponible: https://www.nucleodoconhecimento.com.br/ciencias-de-la-computacion/analisis-forense

Figura 10. Banco de Evidencia

Result Grid | Filter Rows: | Edit: | Export/Import: | Wrap Cell Content:

iddnsReport	Timestamp	Source_IP	Destination_IP	Technique_used	Result	Attack_type
1	05/15/2022-16:50:01.946936	192.168.100.10:47052	192.168.100.1:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
2	05/15/2022-16:50:01.950319	192.168.100.10:35006	192.168.100.1:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
3	05/21/2022-11:47:28.810665	192.168.100.10:47401	192.168.100.1:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
4	10/25/2022-16:15:15.941984	192.168.0.10:33396	181.213.132.2:53	DNS HIJACKING	Dns server hijacking. Providing false informatio...	Invasion
5	10/26/2022-22:17:26.184351	192.168.0.10:51114	181.213.132.2:53	DNS HIJACKING	Dns server hijacking. Providing false informatio...	Invasion
6	10/26/2022-22:17:28.606209	192.168.0.10:36981	181.213.132.2:53	DNS HIJACKING	Dns server hijacking. Providing false informatio...	Invasion
7	10/26/2022-22:17:28.804180	192.168.0.10:40837	181.213.132.2:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
8	10/26/2022-22:17:30.412132	192.168.0.10:56182	181.213.132.2:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
9	10/26/2022-22:35:40.158020	192.168.0.10:45021	181.213.132.2:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
10	10/26/2022-22:35:40.276352	192.168.0.10:33766	181.213.132.2:53	DNS HIJACKING	Dns server hijacking. Providing false informatio...	Invasion
NULL	NULL	NULL	NULL	NULL	NULL	NULL

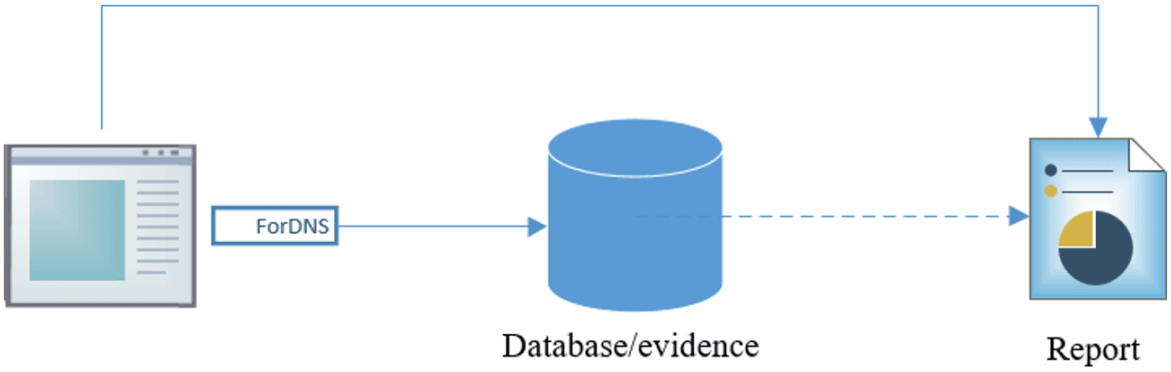
Fuente: Autor (2023).

A pesar de una falta parcial de información en la base de datos, la herramienta propuesta no solo puede determinar las consecuencias del ataque, sino también inferir el tipo de delito basado en la disposición legal (154-A).

4.6 INFORME

El informe generado por la herramienta *ForDNS* recopila la información extraída y la almacena en una nueva base de datos. Este informe servirá como evidencia de la intrusión en dispositivos informáticos criminales, que posteriormente será utilizada por los investigadores y la Policía Judicial.

Figura 11. Registro de evidencia en el informe



Fuente: Autor (2023).

Las Figuras 11 y 12 muestran cómo el informe recopila información sobre delitos, registrándola para la subsiguiente investigación criminal.

Figura 12. Informe generado por la herramienta *ForDNS*

Forensic tool report (ForDNS)	
Date and time of attack	05/15/2022-16:50
IP and logical time of the source	192.168.100.10:35006
Source IP and destination logical time	192.168.100.1:53
Technique used	DNS cache poisoning
Attack type	Invasion
Penal vilation type	Article 154-A of the Brazilian penal code
Data source	Suricata IDS log file

Fuente: Autor (2023).

4.7 CLASIFICACIÓN CRIMINAL DE ATAQUES DE ENVENENAMIENTO DE CACHÉ DE DNS

El artículo 154-A del Código Penal Brasileño (BRASIL, 1940), introducido por la Ley 12.737/2012 (BRASIL, 2012) y modificado recientemente por la Ley 14.155/2021 (BRASIL, 2021), ilustra el delito de intrusión en un dispositivo informático, independientemente de si está conectado a la *World Wide Web*.

El IDS, por sí solo, no puede determinar si se ha cometido un delito; se centra únicamente en proteger la red y emitir alertas. Se requieren otros medios por ley para identificar la técnica de invasión, analizar el procedimiento de invasión (escaneo de puertos u otras técnicas preparatorias para el ataque al servicio de DNS) y señalar todos los factores criminales. El presente estudio se centra en los ataques de envenenamiento de caché de DNS, una técnica utilizada para invadir un dispositivo informático, el servidor DNS en este caso, con el fin de obtener, destruir o manipular información que permite la correcta asociación de la dirección IP de un servidor con su sitio web, lo que constituye un delito según el artículo 154-A del Código Penal Brasileño.

4.8 CENÁRIO DE APLICAÇÃO DA FERRAMENTA FORENSE E ANÁLISE DE LOG DO IDS

Este enfoque permite el análisis de intrusiones en servidores DNS en dos escenarios: ataques internos y ataques externos. El enfoque forense fue desarrollado para el análisis del tráfico de red generado por el IDS Suricata. Este IDS identifica y registra los datos de intrusión mediante el análisis del tráfico de red y la identificación de acciones alineadas con las reglas que definen diversas técnicas de intrusión en redes informáticas (Waleed, Jamali y Masood, 2022).

A pesar de poder capturar pruebas de ataque, la identificación y las respuestas eventuales del IDS (para alertar a los servicios de red atacados o bloquear el dispositivo del atacante original), el IDS no identifica si estas ocurrencias son actividades delictivas. Estos datos no solo son volátiles, sino que también se sobrescriben constantemente con la actividad de red más reciente.

En este contexto, el enfoque propuesto tiene la intención de ayudar a capturar hechos señalados por el DME y analizarlos bajo la ley penal brasileña, considerando que no todas las alertas constituyen un delito. Nuestro enfoque considera los siguientes dos escenarios.

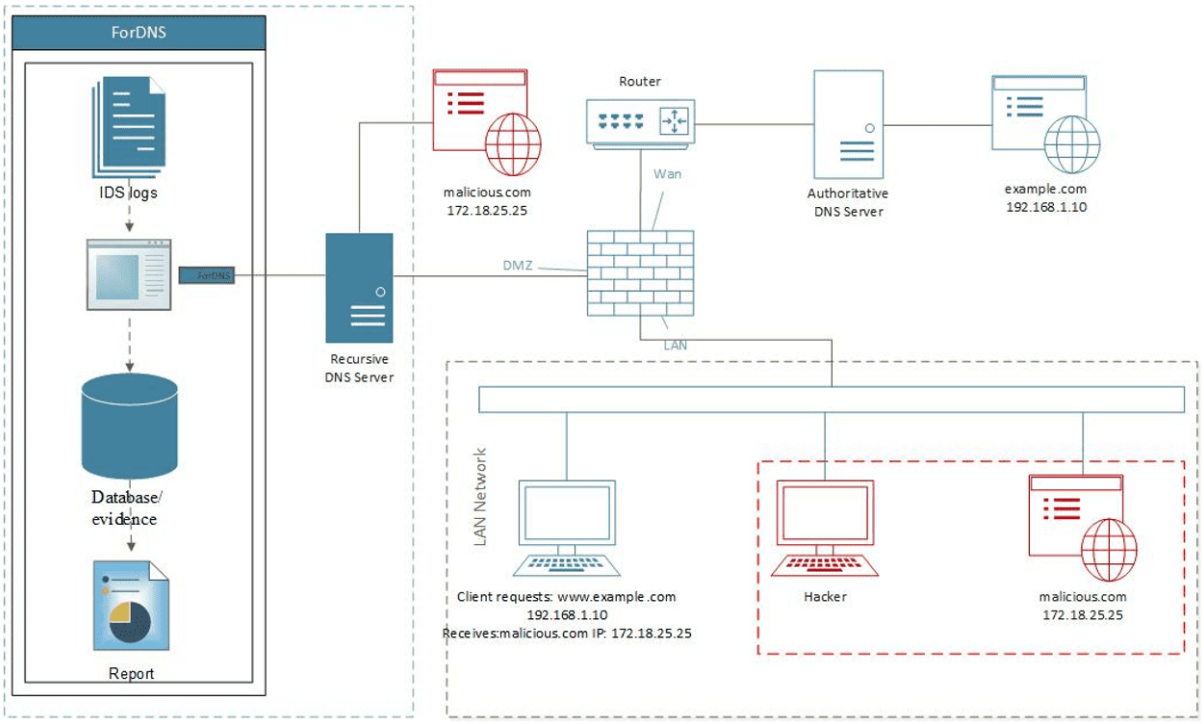
4.8.1 ESCENARIO 1: ATACANTE DENTRO DE LA RED LAN (USUARIO AUTENTICADO) PENETRA EN EL DNS LOCAL

El Escenario 1 (Figura 13) representa un ataque al DNS recursivo. El atacante crea una página web falsa, similar a un sitio corporativo o institucional. Aplicando técnicas de pirateo, captura credenciales privadas de sistemas.

En este escenario, el atacante envenena la caché del DNS insertando la dirección que conduce a una página web falsa en la caché del servidor DNS recursivo. Al intentar acceder a una página ingresando una URL conocida, los usuarios son redirigidos a una página falsa (casi idéntica a la real). Una vez allí, los usuarios se convierten en víctimas de otros delitos al ingresar datos personales.

En la mayoría de los casos, la información de la caché tiene una duración limitada, y después de varios intentos, los usuarios logran acceder a la página real sin experimentar los efectos de los ataques de envenenamiento de caché.

Figura 13. Contexto de ataque interno recursivo del DNS de *ForDNS*



Fuente: Autor (2023).

Normalmente, as vítimas de envenenamento de cache só ficam cientes dos ataques quando suas consequências se materializam na forma de perdas financeiras, trabalhistas, pessoais ou de outras naturezas. As razões mencionadas e a revelação tardia do ocorrido tornam difícil a identificação do autor. Nesse contexto, a necessidade de uma arquitetura de computadores especializada na detecção e análise de fraudes computacionais, bem como no armazenamento de evidências desses eventos, torna-se primordial.

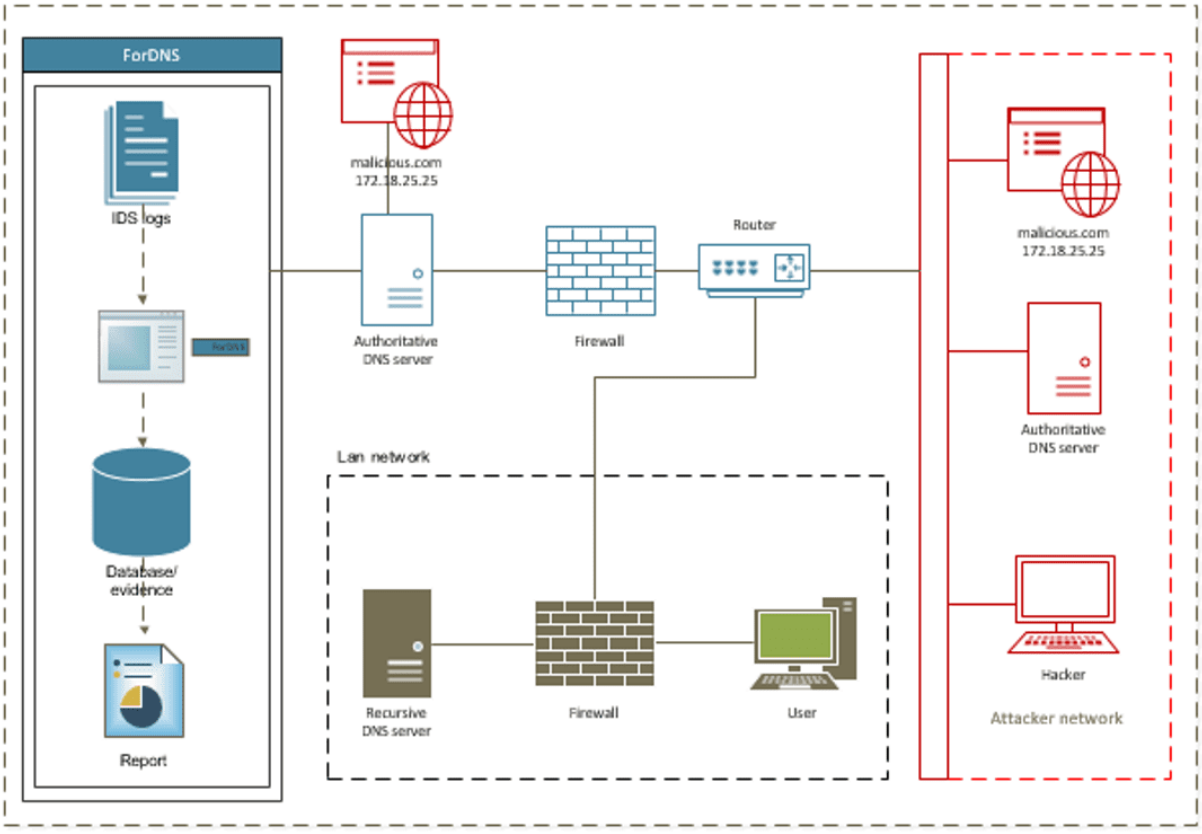
A ferramenta da abordagem *ForDNS,* como mencionado, prioriza a análise desse tipo de ataque e extrai evidências criminais, relatando possíveis crimes que possam se enquadrar no Artigo 154-A do Código Penal Brasileiro.

4.8.2 ESCUENARIO 2: ATACANTE EN LA RED WAN (INTERNET) VULNERA EL DNS PRIMARIO (AUTORITARIO)

El escenario 2, Figura 14, representa un ataque costoso cuyos impactos negativos son mayores que en el Escenario 1, ya que no se limita a un grupo específico, sino que se extiende a todos los demás usuarios de servicios de resolución de nombres de dominio que acceden a un dominio específico.

En este caso, se trata de un ataque DNS remoto, que, según algunos investigadores como Kim y Reeves (2020) y Zhang *et al.* (2021), se conoce como la técnica Kaminsky, donde el objetivo no es el servidor recursivo de una LAN, sino uno de rango más alto, un servidor recursivo de un ISP que solicita un dominio a un servidor DNS autoritario.

Figura 14. *ForDNS* en un contexto de envenenamiento de caché DNS entre el servidor DNS recursivo de un ISP y la negociación con el servidor autoritario.



Fuente: Autor (2023).

RC: 149501
Disponible: https://www.nucleodoconhecimento.com.br/ciencias-de-la-computacion/analisis-forense

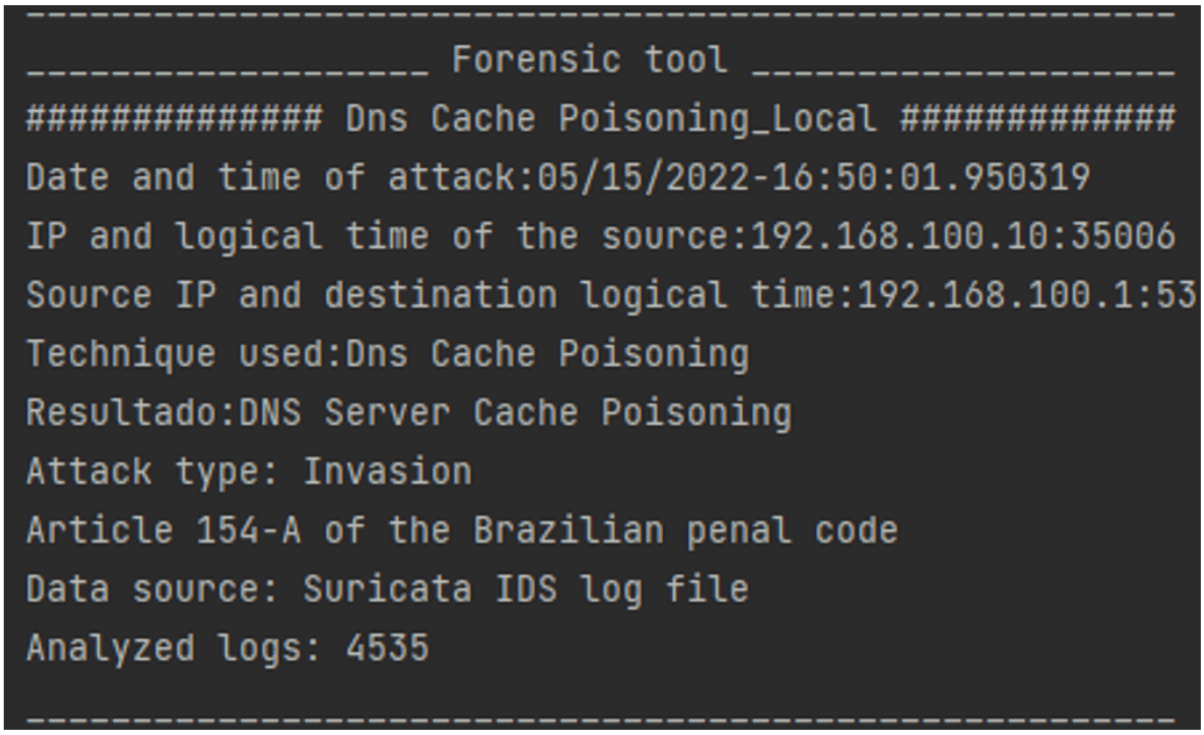
Los atacantes Kaminsky operan de forma remota y no esperan a que los usuarios de una red privada generen una consulta DNS para envenenar la caché de un servidor DNS de un ISP. El atacante comienza transmitiendo la consulta recursiva del ISP a un servidor autoritario y, si no tiene la dirección del dominio en la caché, inicia inmediatamente la consulta al servidor autoritario para ese dominio. Es en este momento que el atacante compite con el servidor DNS autoritario, ya que mientras el autoritario intenta enviar una respuesta auténtica al servidor recursivo, el atacante que se hace pasar por el autoritario envía una gran cantidad de respuestas falsificadas al servidor recursivo. Si la respuesta falsificada coincide con la enviada durante la consulta DNS, el servidor recursivo aceptará la respuesta falsificada y almacenará temporalmente los registros maliciosos del dominio en su caché.

El atacante crea la oportunidad de invadir el servidor DNS al falsificar la respuesta de validación entre los servidores y, de esta manera, interrumpir la comunicación entre ambos; suplanta la dirección IP del dominio por una maliciosa; y finalmente obtiene información de terceros.

Este ataque es crítico porque puede realizarse repetidamente, o incluso secuestrar el DNS o dejarlo no disponible mediante un ataque de denegación de servicio distribuido (DDoS). Zhang *et al.* (2021) informa que el envenenamiento de la caché DNS utilizando la técnica Kaminsky inicialmente se dirigía solo al envenenamiento de caché, pero que a partir de 2021 ha estado actuando en conjunto con el secuestro de servidores DNS. Estos ataques duran más tiempo y, por lo tanto, tienen repercusiones más amplias. Tripathi, Swarnkare y Hubballi (2018) afirman que a menudo están respaldados por ataques DDoS que hacen que el servidor DNS original sea inutilizable.

Al igual que en el Escenario I, los usuarios solo se dan cuenta de que han sido atacados cuando las consecuencias se traducen en pérdidas. Por lo tanto, estas estructuras informáticas deben ser monitoreadas para que el servidor DNS, o cualquier servidor de una aplicación informática, esté siendo monitoreado por herramientas de seguridad de la información cuando se produzcan tales fraudes.

Figura 15. Informe forense *(ForDNS)*



Fuente: Autor (2023).

Como se describió, la herramienta propuesta es útil para la detección de delitos informáticos, ya que captura y almacena las principales pruebas de intrusión DNS en una base de datos. Utilizando esto, se puede presentar un informe forense como evidencia en virtud del Artículo 154 del Código Penal Brasileño (Figura 15).

5. CONCLUSIÓN

Las infraestructuras de red interconectadas a la *World Wide Web* y los diversos servidores requieren un aparato de protección para salvaguardar la integridad de muchos servicios computacionales accesibles a través de Internet. Los firewalls y los IDS sirven para este propósito de protección y seguridad. El IDS identifica la actividad y la registra en un archivo de historial (registro), tomando algunas decisiones previamente configuradas. Esto constituye, según la legislación penal brasileña, el delito de intrusión en un dispositivo informático. Dado que el archivo de registro registra la volatilidad, que se actualiza con frecuencia debido al gran volumen de datos

y alertas generados por el tráfico de red, tal evidencia se pierde, lo que dificulta la recopilación de pruebas que permitan el enjuiciamiento penal de los autores.

En este estudio, hemos propuesto un enfoque que utiliza una herramienta forense para extraer los datos proporcionados por el IDS e identificar la ocurrencia de un ataque de envenenamiento de caché DNS, así como analizar los diversos elementos constituyentes de los actos delictivos. También permite la provisión de pruebas para investigar el hecho, al autor, a las víctimas y a las consecuencias tecnológicas de la intrusión en el (los) dispositivo(s). Además, registra los datos en una base de datos de evidencias proporcionada con la arquitectura que coteja el tipo de ataques con la legislación pertinente. Por último, también permite a los no especialistas en seguridad de redes registrar las actividades de ataque, preservando los datos históricos para futuras actualizaciones en los sistemas de seguridad y la protección de los servicios de red.

REFERENCIAS

ALHARBI, F.; CHANG, J.; ZHOU, Y.; QIAN, F.; QIAN, Z.; ABU-GHAZALEH, N. Collaborative Client-Side DNS Cache Poisoning attack. **In: IEEE Conference on Computer Communications (INFOCOM)**, 2019, Proceedings. Piscataway: IEEE, 2019. p. 1153-1161.

BRASIL. **Lei nº 12.737, de 30 de Novembro de 2012**. Diário Oficial da União. 03 de Dezembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 5 jun. 2023.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Diário Oficial da União. 27 de maiode 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm Acesso em: 5 jun. 2023.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União, Brasília, DF, 31 dez. 1940. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 5 jun. 2023.

ELDOW, O.; CHAUHAN, P.; LALWANI, P.; POTDAR, M. Computer Network Security IDS Tools and Techniques (Snort/Suricata). **International Journal of Scientific and Research Publications**, v. 6, n. 1, p. 593-597, 2016.

ESKANDARI, M ; JANJUA, Z. H.; VECCHIO, M.; ANTONELLI, F. 'Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices', **IEEE Internet of Things Journal**, Vol. 7 No. 8, pp.6882–6897, 2020.

HMOOD, H. S.; LI, Z.; ABDULWAHID, H. K.; ZHANG, Y. Adaptive caching approach to prevent DNS cache poisoning attack. **Computer Journal**, v. 58, n. 4, p. 973-985, 2015.

HUSSAIN, M. A.; JIN, H.; HUSSIEN, Z. A.; ABDULJABBAR, Z. A.; ABBDAL, S. H.; IBRAHIM. DNS Protection against Spoofing and Poisoning Attacks. **In: International Conference on Information Science and Control Engineering (ICISCE)**, 2016, Proceedings. Piscataway: IEEE, 2016. p. 1308-1312.

KAMINSKY, D. Black Ops 2008**: It's The End Of The Cache As We Know It. Fortune**, 2008, p. 1-18.

KIM, T. H.; REEVES, D. **A survey of domain name system vulnerabilities and attacks. Journal of Surveillance**, Security and Safety, 2020, p. 34-60.

LENCSE, G. Benchmarking Authoritative DNS Servers. **IEEE Access**, v. 8, p. 130224-130238, 2020.

LISKA, A.; STOWE, G. DNS reconnaissance. **In: DNS Security. Cham: Springer**, 2016. p. 75-91.

NAQASH, T.; UBBAID, F. B.; ISHFAQ, A. Protecting DNS from cache poisoning attack by using secure proxy. In: **International Conference on Emerging Technologies (ICET)**, 2012, Proceedings. Piscataway: IEEE, 2012. p. 288-292.

NETO, H.; ÁVILA, C.; LACERDA, W. S. Computer Network Intrusion Detection System Using Artificial Neural Networks. In: **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)**, 2017, Proceedings. Porto Alegre: SBC, 2017. p. 206-213.

NEWTON, H.; BLICHE, S. Computer Network Forensics Assistance Methodology Focused on Denial of Service Attacks. **International Journal of Computer Applications**, v. 177, n. 33, p. 1-11, 2020.

OISF - Open Information Security Foundation. **Suricata user guide**. p. 206, 2016. Disponível em: <https://suricata.readthedocs.io/ en/suricata-6.0.0/>. Acesso em: 10 out. 2022.

OISF - Open Information Security Foundation. **Suricata IDS V.6**. 2023. Disponível em <https://suricata.io/features/>. Acesso em: 6 jun. 2022.

STEINHO, U.; WIESMAIER, A.; ARAÚJO, R. The State of the Art in DNS Spoofing. **In: International Conference on Applied Cryptography and Network Security (ACNS)**, 2006, Proceedings. Berlin: Springer, 2006.

TRIPATHI, N.; SWARNKAR, M.; HUBBALLI, N. DNS spoofing in local networks made easy. In: **IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)**, 2018, Proceedings. Piscataway: IEEE, 2018. p. 1-6.

VAZÃO, A. P. H. **Implementação de sistema SIEM open-source em conformidade com o RGPD. Dissertação** (Mestrado) — Escola Superior de Tecnologia e Gestão, Instituto Politécnico, 2021. Disponível em: <http://hdl.handle.net/10400.8/5567>. Acesso em: 5 jun. 2021.

WALEED, A.; JAMALI, A. F.; MASOOD, A. 'Which open-source IDS Snort, Suricata or Zeek'. **Computer Networks**, Vol. 213 No. June, pp. 109-116, 2022.

WANG, W.; ZANG, T.; LAN, Y. The Rapid Extraction of Suspicious Traffic from Passive DNS. In: **International Conference on Information Systems Security and Privacy (ICISSP)**, 2018, Proceedings. SciTePress, 2018. p. 190-198.

WANG, Z. Poster: on the capability of dns cache poisoning attacks. In: **Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security**. [s.n.], 2014. p. 1523–1525.

ZHANG, H.; *et al*. Study on the latent state of kaminsky-style dns cache poisoning: Modeling and empirical analysis. **Computers Security**, v. 110, p. 1–15, 2021. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404821002698>.

Enviado: 14 de junio de 2023.

Aprobado: 29 de junio de 2023.

[1] Estudiante de maestría en Ciencias de la Computación (UFMA), Licenciado en Sistemas de Información (Estácio), Tecnólogo en Gestión Ambiental (CEST), Especialista en Gestión Pública (UFMA), Especialista en Redes de Computadoras (AVM), Tec. en Informática (IFMA/ETC-BRASIL). ORCID: 0009-0001-1336-4044. CURRÍCULO LATTES: http://lattes.cnpq.br/4129979584830810.
[2] Asesor. Doctor en Informática, Máster en Ingeniería Eléctrica con Área de Concentración en Ciencias de la Computación, Licenciado en Ciencias de la Computación y Licenciado en Derecho. ORCID: 0000-0001-8799-1799. CURRÍCULO LATTES: http://lattes.cnpq.br/1531971102610447.