OFICINA POSTGRADOS

TEMA:

EVALUACIÓN DE LOS MECANISMOS SEGURIDAD DE DNS EN REDES IPV4 E IPV6

Proyecto de Investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de investigación:

Protección de Datos y Comunicaciones

Autor:

Henry Marcelo Barba Palma

Director:

MsC. Alberto Leopoldo Arellano Aucancela

Ambato-Ecuador

Junio 2022

PONTIFICIA UNIVERSIDAD CATÒLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

EVALUACIÓN DE LOS MECANISMOS SEGURIDAD DE DNS EN REDES IPV4 E IPV6

Línea de investigación:

Protección de Datos y Comunicaciones

Autor:

Henry Marcelo Barba Palma

Alberto Leopoldo Arellano Aucancela, Ing. Mg. f._____

Firmado electrónicamente por: ALBERTO LEOPOLDO ARELLANO AUCANCELA

CALIFICADOR

Diego Fernando Ávila Pesantez, Ing. PhD. f._____

Firmado electrónicamente por: DIEGO FERNANDO AVILA PESANTEZ

CALIFICADOR

Galo Mauricio López Sevilla, Ing. Mg. f._____

CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f._____

Pontificia Universidad Católica del Ecuador

OFICINA DE POSGRADOS

DIRECTOR OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

Pontificia Universidad Católica del Ecuador

SECRETARIA GENERAL PROCURADURÍA

SECRETARIO GENERAL PUCESA

Ambato-Ecuador

Junio 2022

DECLARACIÓN Y AUTORIZACIÓN

Yo: **HENRY MARCELO BARBA PALMA**, con **CC. 050251734-5**, autor del trabajo de graduación intitulado: "EVALUACIÓN DE LOS MECANISMOS SEGURIDAD DE DNS EN REDES IPV4 E IPV6", previa a la obtención del título profesional de **MAGISTER EN CYBERSEGURIDAD**, en la escuela de **POSGRADO**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, junio 2022

HENRY MARCELO BARBA PALMA
CC. 050251734-5

AGRADECIMIENTO

A DIOS por obsequiarme la vida y permitirme disfrutar de ella cada día.

Al director de investigación, MsC. Alberto Leopoldo Arellano Aucancela, por los conocimientos, el apoyo y la comprensión para la culminación de esta investigación.

A la Pontificia Universidad Católica del Ecuador Sede Ambato su programa de maestría y docentes quienes han contribuido con sus conocimientos a mi formación profesional.

A la Gerencia Administrativa del Hospital General Latacunga y al área de tecnologías de la información por la confianza, apertura y predisposición hacia este trabajo investigativo.

Henry Marcelo Barba Palma

DEDICATORIA

El presente trabajo de investigación está dedicado: A mis amados padres, pues su ejemplo, valores e infinito amor, han sido mi inspiración y en todo momento la fuente de mi esfuerzo y dedicación. A ellos por ser los pilares fundamentales en mi sendero, el latir de mi corazón, y compañía de mis desvelos con devoto amor y comprensión. Su incondicional apoyo para alcanzar mis metas y culminar esta importante etapa en mi vida personal y profesional pertenece con todo mi cariño y agradecimiento.

Henry

RESUMEN

En el presente proyecto se realiza un estudio y simulación para determinar el mecanismo más adecuado de seguridad DNS (Sistema de nombres de dominio) en redes IPV4 e IPV6. Se inicia con una descripción general de configuración de redes y los equipos servidores de DNS. Luego se realiza una revisión de los mecanismos de seguridad y ataques, para luego evaluar y determinar el método más efectivo. En la fase de diseño se contempla un ambiente simulado para generar ataques DDos y otro ambiente informático para mitigar dichos ataques. A continuación, se realizan de manera ética ataques de denegación de servicio sin afectar a redes externas. Finalmente, se muestran los resultados obtenidos con herramientas informáticas de monitoreo, como WireShark, los cuales permite detectar ciertas irregularidades respecto al servicio estudiado, esto ayudó a la configuración de los parámetros de seguridad en la red tecnológica de la institución para mitigar las vulnerabilidades, los cuales de acuerdo con la metodología diamante empleada para el análisis, pasó de tener una alta probabilidad a media esto disminuyó los riesgos ante este tipo de ataques dentro del Hospital General Latacunga.

Palabras clave: Simulación, software, instalación, generación, seguridad.

ABSTRACT

The following project presents a study and simulation to determine the most adequated DNS (Domain Name System) security system for networks IPV4 and IPV6. It starts with a general description about the setting of the networks and the DNS server equipments. Then, a checking of the security and attack mechanisms is done to evaluate and determine the most effective method. In the design phase, a simulated environment is contemplated in order to generate DDOS attacks and other computing environment to mitigate such attacks. After that, In an ethic way, service denial attacks are done, but without affecting the external networks. Finally, the results obtained are showed with monitoring computing tools as Wireshark. It allows to detect some irregularities about the studied service. It helped to the security parameters setting in the institution's technological network in order to mitigate the vulnerabilities, which, according the diamond methodology used to the analysis, passed from having a high probability to a medium level. It decreased the risks before this kind of attacks that used to happen inside the General Hospital of Latacunga.

Key words: Simulation, software, installation, generation, security.

ÍNDICE GENERAL DE CONTENIDOS

INTRODUCCIÓN

Los servicios DNS tienen cierta susceptibilidad a ataques, el protocolo de la capa de transporte utilizado es UDP, es un protocolo no orientado a la conexión, por lo cual, las tramas de datos pueden llegar o no completas al destino. En los últimos meses sobre todo por el motivo de la pandemia, los ataques de ciberdelincuentes en Latinoamérica incrementaron considerablemente, quienes utilizan técnicas como Denegación de Servicio, Caché Poisoning, envía enlaces a manera de petición de información personal, para posterior hacer uso de dicha información y generar ataques de DDoS.

En Ecuador no existen documentos oficiales con datos comprobados referente a ataques de DNS en los últimos años, esto implica a no tener una certeza de que se hayan vulnerado las seguridades en nuestro país. Sin embargo, de acuerdo con los reportes de efficient IP los ataques a los servidores DNS sufrieron el 80% de las empresas de telecomunicaciones en el año 2019. Las consecuencias fueron interrupciones que afectaron a clientes de todos los ámbitos que dependen de la disponibilidad 24/7 de las redes, al crecer exponencialmente el número de ataques DDoS (Denegación de servicio), al menos el 8% de los ISP (Proveedores de Servicio de Internet) sufren de este tipo de problema, referencia (efficient IP, 2021)

En los últimos años, las tecnologías de la Información y Comunicación (TIC), han influenciado y evolucionado a gran escala a nivel mundial, exige constantemente la utilización de mecanismos de seguridad de DNS en redes IPV4 e IPV6. Los servidores de DNS (Sistema de nombres de dominio), traducen los nombres inteligibles para humanos en identificadores binarios, proporciona información del espacio o nombres de dominio. En un entorno DNS se sitúan varios puntos donde posibles ataques pueden desarrollarse, identificándose como vectores de ataque, que se encuentran tanto localmente en el propio servidor y red local, como en las comunicaciones entre servidores y clientes

Los ciberdelincuentes saben que los servicios de DNS influyen directamente en los negocios, por ello la mayor parte de las organizaciones son víctimas de ataques

basados estos servicios, de acuerdo al reporte del año 2020 de la IDC (International Data Corporation) ubicada en Needham Heights, EEUU, los ataques basados en los servicios de DNS a las organizaciones se estimaron en un 79%. La gran variedad y porcentaje de los ataques DNS muestra que en *phishing* existe un 39%, malware basado en DNS un 34%, ataques DDoS 27%, amplificación de DNS 21%, activación de falso positivo de DNS 19%, y túnel DNS 17%. El 98% de las empresas utilizan algún tipo de solución, pero estas soluciones no son lo suficientemente robustas para garantizar la seguridad de los servicios DNS. Para el año 2020 el tamaño de los ataques de DDoS ha aumentado en un 64%, referencia (efficient IP, 2021).

La utilización de métodos y herramientas desactualizadas en las seguridades de DNS genera un gran problema para el resguardo de la información digital, y el funcionamiento de los sistemas informáticos, puesto que, los servidores de DNS han sufrido ataques de DDos, provoca la intrusión no deseada de equipos externos a la red y el acceso no controlado a la información. En tal virtud algunos equipos informáticos pierden la conectividad lógica de manera total o temporal a los servicios internos, permite que equipos maliciosos accedan a los servicios y a la información interna, e incluso detiene todos los servicios.

Con la evaluación de los mecanismos de seguridad de DNS en redes IPV4 e IPV6, se pretende determinar cuál es el mejor procedimiento para minimizar los riesgos ante los ataques de los ciberdelincuentes a los servidores de DNS, a la vez un aporte muy importante para la comunidad, controla de manera estructurada el acceso a los servicios de DNS.

Mediante la configuración y diseño más efectivo del método de seguridad de DNS, se puede reducir considerablemente el riesgo a amenazas externas y por ende la efectividad en los servicios de DNS.

Como objetivo general se persigue evaluar los mecanismos de seguridad de DNS en redes IPv4 e IPV6, para determinar el procedimiento más efectivo ante el ataque

a los servidores de DNS. Adicional para el desarrollo del presente proyecto, se complementarán los objetivos específicos siguientes:

1. Analizar las técnicas de seguridad de DNS en redes IPV4 e IPV6.
2. Comparar los distintos mecanismos de seguridad de DNS aplicados a las redes de datos.
3. Diseñar e implementar un ambiente de simulación de mecanismos de seguridad y ataque de DNS en redes IPV4 e IPV6.
4. Determinar que técnicas de seguridad DNS en redes IPV4 e IPV6 es la más efectiva en comparación con otros métodos de seguridad DNS.

Se hace uso de la metodología de investigación de campo, puesto que el estudio se realizará en el lugar de los acontecimientos mediante la simulación del servicio. El análisis de los resultados determinará el nivel de efectividad de los mecanismos de seguridad con el fin de mitigar los ciberataques a los servidores de DNS.

También, se hace uso de manera empírica de la metodología diamante, en virtud que la simulación se desarrollará en un ambiente de laboratorio, en el que se generarán ataques a servicios DNS en una red de datos interna, sin afectar a organizaciones o empresas externas, incluso para no incurrir en aspectos legales que afecten directamente al desarrollo del proyecto.

La metodología diamante utiliza el método de clasificación por colores; de manera cualitativa y general, se utilizarán cuatro fases, calificación de la Probabilidad de ocurrencia, vulnerabilidad de los servidores DNS, determinación de los recursos informáticos, identificación de ataques y seguridades DNS, para clasificar de manera cualitativa las amenazas y vulnerabilidades DNS.

Mediante la simulación de ataques DNS con herramientas informáticas, se evaluarán los mecanismos más efectivos de seguridad de DNS en redes IPv4 e IPV6.

Con un adecuado análisis actual de herramientas informáticas, se validarán los mecanismos de seguridad y se minimizarán los riesgos de ataques a los servidores de DNS.

Mediante la configuración y diseño más efectivo del método de seguridad de DNS, se puede reducir considerablemente el riesgo a amenazas externas y por ende la efectividad en los servicios de DNS.

Con una apropiada implementación y evaluación de los mecanismos de seguridad de DNS, se tendrá una mayor confianza del usuario, al brindarle una red de datos efectiva y segura.

CAPÍTULO I: ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Estudio del Direccionamiento IP

IPV4

De acuerdo a CISCO (2021), una dirección IP es una dirección empleada para identificar a un dispositivo en una red IP. La dirección se compone de 32 bits binarios divididos por puntos en cuatro octetos, que conforme la división de los bits, se separan en dirección red y otra correspondiente a la dirección de host, con la ayuda de una máscara de subred. Un octeto está compuesto de 8 bits. Cada octeto se convierte a decimal y se separa con un punto. Por esta razón, una dirección IP se expresa en formato decimal con puntos (por ejemplo, 172.16.11.25). Cada octeto tiene un rango decimal de 0 a 255 ó número binario de 00000000 a 11111111.

La relación se realiza en base a códigos binarios convertidos a decimal de los 32 bits que tienen en total los 4 octetos, la relación sería 2^{32} con lo cual se obtiene el número 4.294.967.296 direcciones.

> En las etapas iniciales del desarrollo del Protocolo de Internet, los administradores de Internet interpretaban las direcciones IP en dos partes, los primeros 8 bits para designar la dirección de red y el resto para individualizar la computadora dentro de la red. Este método pronto probó ser inadecuado, si se comenzaron a agregar nuevas redes a las ya asignadas. En 1981 el direccionamiento internet fue revisado y se introdujo la arquitectura de clases (*classful network architecture*). En esta arquitectura hay tres clases de direcciones IP que una organización recibe de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C.
>
> La implementación de las clases de direcciones IPV4 fue una solución muy importante para esa época. Actualmente por el crecimiento exponencial de

Internet, se ve la necesidad de la creación de subredes e implementaciones con el protocolo IPV6.

Clases de direcciones IP

Clase A: En esta clase se reserva el primer octeto a la identificación de la red, queda los tres siguientes para identificar a los hosts. Los rangos de esta clase están comprendidos entre 1.0.0.0 y 127.255.255.255.

Clase B: En esta clase se reservan los dos primeros octetos a la identificación de la red, queda los dos siguientes para identificar a los hosts. Los rangos de esta clase están comprendidos entre 128.0.0.0 y 191.255.255.255.

Clase C: En esta clase se reservan los tres primeros octetos a la identificación de la red, queda el último para los diferentes hosts. Los rangos de esta clase están comprendidos entre 192.0.0.0 y 223.255.255.255.

Dentro de estas clases hay otra serie de asignaciones:

- ✓ La dirección 0.0.0.0 se utiliza por las máquinas si están arranca o no se les ha asignado una dirección IP.

- ✓ La dirección que tiene su parte de host a cero sirve para definir la red en la que se ubica. Se denomina dirección red.

- ✓ La dirección que tiene su parte de host a unos sirve para comunicar con todos los hosts de la red en la que se ubica. Se denomina Dirección de broadcast.

- ✓ Las direcciones 127.x.x.x se reservan para pruebas de retroalimentación. Se denomina Dirección de bucle local o loopback".

Direcciones Privadas

Según el GRUPO ATICO34 (2021), las direcciones IP privadas son direcciones fijas que se asignan a cada dispositivo conectado a una red privada o doméstica, es decir, la dirección IP que el router asigna a cada ordenador, smartphones, smart TV, tablet, videoconsola o cualquier otro dispositivo conectado a él. De esta manera el router asigna una dirección IP privada a cada dispositivo mientras comparten la misma IP pública.
Las IP's privadas no son accesibles desde Internet y no cambian, a no ser que las asignemos nosotros manualmente:

CLASE A: 10.0.0.0 a 10.255.255.255 (8bits red, 24 bits hosts), permite crear hasta 126 redes distintas y conectar hasta un máximo de 16.777.214 equipos a la red.

CLASE B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts), permite crear un mayor número de redes que el rango A, 16.384 redes, pero con muchos menos equipos conectados a ellas, 65.534 dispositivos.

CLASE C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts), permite tener muchas más redes, 2.097.152, pero conectan muchos menos equipos a cada una de ellas, 254.

Máscara de subred

Sintetiza CISCO (2021), una máscara de red determina qué parte de la dirección IP identifica la red y qué parte de la dirección identifica los host. Las redes de la clase A, B, y C tienen máscaras predeterminadas, también, conocidas como máscaras naturales, como se muestra a continuación:
Clase A: 255.0.0.0
Clase B: 255.255.0.0
Clase C: 255.255.255.0

Una dirección IP de una red de la Clase A que no se haya convertido en subred tendrá un par dirección/máscara similar a: 8.20.15.1 255.0.0.0. Para ver cómo la máscara ayuda a identificar en la dirección las partes de la red y del nodo, pase la dirección y la máscara a números binarios.

8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
Una vez que tiene la dirección y la máscara representadas en binario, la identificación de la red y el ID de host es más fácil. Cualquier bit de dirección que tenga el bit de máscara correspondiente establecido en 1 representa la identificación de red. Cualquier bit de dirección que tenga el bit de máscara correspondiente establecido en 0 representa la identificación de nodo.
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000

---

net id | host id
netid = 00001000 = 8
hostid = 00010100.00001111.00000001 = 20.15.1

1.1.1. IPv6

En referencia Broy de la Cruz (2013) el Internet Protocolo versión 6 (IPv6), es una versión del protocolo Internet Protocolo (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocolo versión 4 (Ipv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet. IPv4 posibilita 4.294.967.296 (2^{32}) direcciones de red distintas, un número muy reducido para asignar una dirección IP a cada persona del planeta, y mucho menos a cada computadora, teléfono, o equipo electrónico que requiera de una dirección IP.

En cambio, IPv6 admite 340.282.366.920.938.463.374.607.431.768.211.456 (2128 ó 340 sextillones de direcciones), cerca de 6,7 * 1017 (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la tierra.

Plantea Percy (2020), Una dirección IPv6 tiene 128 bits, lo que significa que existen 2^{128} direcciones IPV6 disponibles, mucho más que las 2^{32} (≈ 4,3 mil millones) de direcciones disponibles con IPv4. Para tener una idea de este "volumen": 2^{128} representa aproximadamente la cantidad de granos de arena en nuestro planeta.

Actualmente, hacer un plan de direccionamiento que usa el sistema IPv4 limita las opciones disponibles para una organización porque hay relativamente escasas direcciones IPv4 aún disponibles. Con IPv6, al tener una cantidad enorme de direcciones se tiene la posibilidad de tener un sistema de direccionamiento más efectivo donde se asigna las direcciones IPv6 por tipos de uso y/o por ubicación.

En un plan de direccionamiento de IPv6 eficiente, los rangos de direccionamiento de IPv6 se agrupan de manera efectiva y lógica. Esto tiene varias ventajas, incluye:

- Las políticas de seguridad son más fáciles de implementar, como la configuración de listas de acceso (ACL) y firewalls
- Las direcciones son más fáciles de rastrear: la dirección contiene información sobre el tipo de uso o la ubicación donde la dirección está en uso
- Un plan de direccionamiento eficiente es escalable: se expande, por ejemplo, para incluir nuevas ubicaciones o tipos de uso
- Un plan de direccionamiento IPv6 eficiente, también, permite una administración de red más eficiente

Motivación y Orígenes del direccionamiento IP

Manifiesta Broy de la Cruz (2013), IPng fue propuesto por el Internet Engineering Task Force (IETF) el 25 de julio de 1994, con la formación de varios grupos de trabajo IPng. Hasta 1996, se publicaron varios RFC define IPv6, empieza con el RFC 2460.

En muchos aspectos, Ipv6 es una extensión conservadora de IPv4. La mayoría de los protocolos de transporte –y aplicación- necesitan pocos o ningún cambio para

operar sobre IPv6; las excepciones son los protocolos de aplicación que integran direcciones de cada red, como FTP o NTPv3, NTPv4. Ipv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables.

Tipo de direcciones IPv6

Direcciones IPv6 Unicast Global (Global Unicast Addresses): Manifiesta Percy (2020), son direcciones que al ser enrutadas y alcanzadas desde todo el espacio de internet IPv6. Son equivalentes a las direcciones públicas IPv4. Como nota adicional, al configurar en una interfaz de router o switch tiene más de una dirección IPv6 o una dirección IPv6 y una dirección IPv4 simultáneamente donde ésta última capacidad se le conoce como "doble pila" (dual stack).

Direcciones IPv6 de Enlace Local (Link-local Addresses): Son direcciones que son usadas para comunicaciones en un segmento local de red. Este se configura automáticamente en todas las interfaces. Tener en cuenta que los Routers no reenviarán paquetes a redes remotas si éstos tienen como origen o destino una dirección de Enlace local. Sin embargo, su función más importante es ser usado como dirección del siguiente salto en los protocolos de enrutamiento en IPv6.

Direcciones IPv6 Multicast: Identifica un grupo de interfaces. Un paquete enviado a una dirección multicast se envía a todos los dispositivos que se identifican con esa dirección. Los Protocolos de enrutamiento en IPv6 utilizan estas direcciones para comunicarse entre dispositivos.

Protocolo de Enrutamiento IPv6 Multicast
OSPFv3 FF02::5
FF02::6
RIPng FF02::9
EIGRP para IPv6 FF02::A

Dirección IPv6 Anycast: Una dirección anycast se asigna a diferentes interfaces/dispositivos. Un paquete que se envía a una dirección anycast solo se dirige al miembro más cercano del grupo, según las medidas de distancia de los protocolos de enrutamiento. En términos generales, Anycast es un intermedio entre unicast y multicast. La diferencia entre anycast y multicast es que un paquete anycast solo se envía a un dispositivo, mientras que uno multicast se envía a un grupo de dispositivos.

Identificación de los tipos de direcciones

Define (Broy de la Cruz, 2013) Los tipos de direcciones IPv6 se indentifica, toma en cuenta los rangos definidos por los primeros bits de cada dirección.

::/128

La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

::1/127

La dirección de loopback es una dirección que usa un nodo para enviarse paquetes a si mismo (corresponde con 127.0.0.1 de IPv4). No se asigna a ninguna interfaz física.

::1.2.3.4/96

La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo que no se usa.

::ffff:0:0/96

La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales.

fe80::/10

El prefijo enlace local (en inglés link local) específica que la dirección sólo es válida en el enlace físico local.

fec0::

el prefijo de emplazamiento local (en inglés site-local prefix) específica que la dirección sólo es válida dentro de una organización local. La RFC 3819 lo declaró obsoleto, establece que los sistemas futuros no se implementa ningún soporte para este tipo de dirección especial. Se sustituye por direcciones Local IPv6 Unicast.

ff00::/8

El prefijo de multicast. Se usa para las direcciones multicast.
Hay que resaltar que no existen las direcciones de difusión (en inglés broadcast) en IPv6, aunque la funcionalidad que prestan emula y utiliza la dirección multicast FF01::1/128, denominada todos los nodos (en inglés all nodes).

Paquete IPv6

Afirma Broy de la Cruz (2013), un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera (que tiene una parte fija y otra con las opciones) y la carga útil (los datos).

Cabecera fija

Los primeros 40 bytes (320bits) son la cabecera del paquete y contiene los siguientes campos:

- Direcciones de origen (128 bits)
- Direcciones de destino (128 bits)
- Versión del protocolo IP (4 bits)
- Clase de tráfico (8 bits, Prioridad del Paquete)
- Etiqueta de flujo (20 bits, manejo de la Calidad de Servicio)
- Longitud del campo de datos (16 bits)
- Cabecera siguiente (8 bits)
- Límite de saltos (8 bits, Tiempo de Vida)

Hay dos versiones de IPv6 levemente diferentes. La ahora obsoleta versión inicial, descrita en el RFC 1883, difiere de la actual versión propuesta de estándar, descrita en el RFC 2460, en dos campos: hay 4 bits que han sido reasignados desde “etiqueta de flujo” (flow label) a “clase de tráfico) (traffic class).

En IPv6 la fragmentación se realiza sólo en el nodo origen del paquete, al contrario que en IPv4 en donde los routers fragmentan un paquete. En IPv6, las opciones

son especificadas por el campo “Cabecera Siguiente” (Next Hheader). Un ejemplo: en IPv4 uno añadiría la opción “ruta fijada desde origen” (Strict Source and Record Routing) a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo “Cabecera Siguiente” indica que viene una cabecera de encaminamiento. La cabecera de encaminamiento especifica la información adicional de enrutamiento del paquete, e indica cual cabecera TCP será la siguiente.

Cabeceras de extensión

Define Broy de la Cruz (2013), el uso de un formato flexible de cabeceras de extensión opcionales es una idea innovadora que permite ir añade funcionalidades de forma paulatina. Este diseño es muy importante para el uso del incremento de la tecnología a medida que se vaya necesita entre la cabecera fija y la carga útil, se incrementa.

Define Broy de la Cruz (2013), Hasta el momento, existen 8 tipos de cabeceras de extensión, donde la cabecera fija y las extensiones opcionales incluyen el campo de cabecera siguiente que identifica el tipo de cabeceras de extensión que viene a continuación o el identificador del protocolo de nivel superior. Luego las cabeceras de extensión se encadena utiliza el campo de cabecera siguiente que aparece tanto en la cabecera fija como en cada una de las citadas cabeceras de extensión. Como resultado de la secuencia anterior, dichas cabeceras de extensión se tienen que procesar en el mismo orden en el que aparecen en el datagrama. La cabecera principal, tiene a diferencia de la cabecera de la versión IPv4 un tamaño fijo de 40 octetos. Específica para asignarlos para aplicaciones multicast intra-dominio o entre-dominios (RFC 3306).

Todas o parte de estas cabeceras de extensión tienen que ubicarse en el datagrama en el orden especificado:

Cada cabecera de extensión aparece como mucho una sola vez, salvo la cabecera de opción destino, que aparece como mucho dos veces, una antes de la cabecera de ruteo y otra antes de la cabecera de la capa superior.

Carga útil

La carga útil del paquete tiene un tamaño de hasta 64 KB en modo estándar, o mayor con una opción de carga jumbo (jumbo payload) en el encabezado opcional Hop-By-Hop. La fragmentación es manejada solamente en el host que envía la información del paquete IPv6: los routers conmutan de mejor manera el tráfico, y los hosts se esperan que utilicen el Path MTU discovery.

1.2. El sistema de nombres de dominio DNS

En referencia a Sanchez (2017), Domain Name System o DNS (sistema de nombres de dominio) es un conjunto de protocolos y servicios que permite a los usuarios utilizar un nombre en vez de un número para la conexión a Internet o a una red privada. Su función principal, es traducir los nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red de datos, esto con el propósito de se localiza y direccionar estos equipos a la ruta correspondiente.

Los servidores DNS utilizan una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es la función más importante de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx. es 200.54.127.3, la mayoría de la gente llega a este equipo especifica ftp.prox.mx y no por la dirección IP. Es más fácil recordar un nombre que una dirección numérica que incluso cambia por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a la red de Internet. La empresa SRI (ahora SRI International) alojaba un archivo llamado HOSTS que contenía todos los nombres de dominio conocidos. El crecimiento elevado de la utilización de la red causó que el sistema de nombres centralizado en el archivo hosts no resultara práctico y en 1983, Paul V. Mockapertris publicó los RFC 882 y RFC 883 define lo que hoy en día a evolucionado hacia el DNS moderno. (Estos RFC han quedado obsoletos por la publicación en 1987 de los RFC 1034 y RFC 1035).

DNS dinámico

DNS dinámico es un sistema que permite la actualización en tiempo real de la información sobre nombres de dominio situada en un servidor de nombres. El uso más común que se le da es permitir la asignación de un nombre de dominio de Internet a un ordenador con dirección IP variable (dinámica). Esto permite conectarse con la máquina en cuestión sin necesidad de tener que rastrear direcciones IP.

El DNS dinámico hace posible, uso frecuente gracias a lo descrito, utilizar software de servidor en una computadora con dirección IP dinámica, como la suelen facilitar muchos proveedores de Internet para particulares (por ejemplo, para alojar un sitio web en el ordenador de nuestra casa, sin necesidad de contratar hosting de terceros).

Otro uso útil que posibilita el DNS dinámico accede al ordenador en cuestión por medio del escritorio remoto. Este servicio es ofrecido, incluso de forma gratuita, por No-IP, CDmon y FreeDNS.

1.2.1. Parte de un nombre de dominio

Plantea Broy de la Cruz (2013), un nombre de dominio usualmente consiste en dos o más partes (técnicamente etiquetas), separadas por puntos si se las escribe en forma de texto. Por ejemplo, www.example.com o www.wikipedia.es, a la etiqueta ubicada más a la derecha se le llama dominio de nivel superior.

Las etiquetas de la izquierda especifican un subdominio. Un subdominio expresa dependencia relativa, no dependencia absoluta. Esta subdivisión tiene hasta 127 niveles, y cada etiqueta contiene hasta 63 caracteres, aunque en la actualidad los dominios son casi siempre mucho más cortos.

Plantea ICTEA(2021), El DNS consiste en un conjunto jerárquico de servidores DNS. Cada dominio o subdominio tiene una o más zonas de autoridad que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido. La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios. La jerarquía de los servidores DNS permite resolver primero los dominios de nivel superior hasta llegar a los dominios de segundo y tercer nivel que se utilizan para crear subniveles.

1.2.2. Funcionamiento de DNS

Menciona Sanchez (2017), los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet).

Al realizar una petición, ésta se envía al servidor DNS local del sistema operativo en la computadora de consulta. El sistema operativo en primera instancia comprueba si la respuesta se encuentra en la memoria caché interna, y en el caso de encontrar una respuesta, la petición se envía a uno de los servidores DNS establecidos en la configuración de la tarjeta de red.

Los equipos servidores DNS que reciben la petición, realizan una búsqueda la memoria caché interna, si existen coincidencias emiten una respuesta; caso contrario, inician la búsqueda de la manera recursiva a otros servidores DNS. Una vez encontrada la respuesta, el servidor DNS guardará el resultado en su memoria caché para futuras consultas y devuelve el resultado al host solicitante.

El servidor recursivo obtiene un registro denominado “A”, para la dirección electrónica de los servidores de nombres autorizados almacena en su caché local. Un nombre de dominio incluiye todos los puntos y tiene una longitud máxima de 255 caracteres.

Un nombre de dominio se lo interpreta de derecha a izquierda. El punto en el extremo derecho de un nombre de dominio separa la etiqueta de la raíz de la jerarquía (en inglés, root), conocido, también, como dominio de nivel superior (TLD – Top Level Domain).

Los objetos de un dominio DNS (por ejemplo, el nombre del equipo) se registran en un archivo de zona, ubicado en uno o más servidores de nombres.

1.3. Tipos de servidores DNS

Considera Sánchez (2017), que los tipos de servidores DNS primarios o maestros: Guardan los datos de un espacio de nombres en sus ficheros.
Secundarios o esclavos: Obtienen los datos de los servidores primarios a través de una transferencia de zona.
Locales o caché: Funcionan con el sistema operativo del host, pero no contienen la base de datos para la resolución de nombres. Si se les realiza una consulta, estos a su vez consultan a los servidores DNS correspondientes, almacena la respuesta en su base de datos para agilizar la repetición de estas peticiones en el futuro continuo o libre.

Plantea Sepúlveda (2021), Si se escribe un nuevo URI en el navegador, la computadora usa DNS para enviar una solicitud para que resuelva el URI en una dirección IP. Por ejemplo, un Servidor DNS resuelve la URI www.eclassvirtual.com en la dirección IP 35.214.133.151.

Existen diferentes tipos de registros utilizados para resolver nombres de dominio, los cuales contienen el nombre, la dirección y el tipo de registro. Algunos de estos de registros son los siguientes:

A: Una dirección IPv4 de un dispositivo final
NS: Un servidor de nombres autorizado
AAAA: Una dirección IPv6 de un dispositivo final
MX: Un registro de intercambio de correo

1.3.1. Tipos de resolución de nombres de dominio

Existen dos tipos de consultas que un cliente hace a un servidor DNS, interativa y recursiva:

a) ITERATIVA:

Plantea Sanchez (2017), Las resoluciones iterativas consisten en la respuesta completa que el servidor de nombres pueda dar, consulta la información local (incluye la caché). El servidor encargado de la resolución realiza iterativamente preguntas a los diferentes servidores DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la máquina que contiene la zona autoritativa para el nombre que se desea resolver.

b) RECURSIVA:

Afirma Broy de la Cruz (2013), en las resoluciones recursivas, el servidor no tiene la información en sus datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta.

Si existe más de un servidor autoritario para una zona, Bind utiliza el menos valor en la métrica RTT (round-trip time) para seleccionar el servidor. El RTT permite determinar cuánto tiempo tarda un servidor DNS en responder a una consulta. El proceso de resolución normal de realiza de la siguiente manera:

a) El servidor A recibe una consulta recursiva desde el cliente DNS.
b) El servidor A envía una consulta recursiva al servidor B.
c) El servidor B refiere a A otro servidor de nombres, incluye a un tercer servidor C.
d) El servidor A envía una consulta recursiva al servidor C.
e) El servidor C refiere a A otro servidor de nombres, incluye a un cuarto servidor D.
f) El servidor A envía una consulta recursiva al servidor D.
g) El servidor D responde.
h) El servidor A regresa la respuesta al resolver.
i) El resolver entrega la resolución al programa que solicitó la información.

1.3.2. Tipos de Registros DNS

Menciona Broy de la Cruz (2013),

A= Address – (Dirección): Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.

AAAA= Address – (Dirección): Registro utilizado en IPv6 para la traducción de nombres de hosts a direcciones IPv6.

CNAME= Canonical Name – (Nombre Canónico): El registro CNAME se usa para renombrar servidores como alias, especialmente para los de alojamiento de un dominio. Es muy importante especialmente si se están ejecuta múltiples servicios como ftp, web, entre otros en un servidor con una misma dirección IP. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplohenry.com. y www.ejemplohenry.com). Esta configuración se usa, también, si se ejecutan varios servidores http, con diferentes nombres, sobre el mismo host o equipo servidor de aplicaciones. Se escribe primero el alias y luego el nombre real.

NS= Name Server – (Servidor de Nombres): Define la asociación que existe entre un nombre de dominio y un DNS, es decir este registro especifica cual servidor DNS es autoritativo para el dominio solicitado.

MX (registro)= Mail Exchange – (Registro de Intercambio de Correo): Se utiliza para el intercambio de correo, asocia un nombre de dominio a un listado de servidores de correo. Con la utilización del balanceo de carga, prioriza la utilización del o los servidores de correo específicos.

PTR= Pointer – (Indicador): También, conocido como “registro inverso”, funciona a la inversa del registro A, traduce IP en nombres de dominio. Se usa en el archivo de configuración del Dns reversiva.

SOA= Start of authority – (Autoridad de la zona): Proporciona información sobre el servidor DNS primario de la zona.

HINFO= Host INFOrmation – (Información del sistema informático): Registro definido en la RFC 1035, especifica la información general de un host.

TXT= TeXT – (Información textual): Contiene información de texto adicional, permite a los dominios identificarse en la red. Es utilizado, también, para verificar la procedencia de un dominio.

LOC= Localización: Indica las coordenadas de latitud y longitud de un servidor de dominio.
SRV= Servicios: Indican los servicios que se incluyen bajo el dominio o subdominio. Excepto MX y NS, hay que incorporar el nombre del servicio, protocolo, dominio completo, prioridad del servicio, peso, puerto y el equipo completo.
SPF= Sender Policy Framework: Ayuda a combatir el Spam. En este registro se específica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe consulta SPF para comparar IP desde la cual le llega con los datos de este registro.

1.4. Amenazas y vulnerabilidades DNS

Afirma López Padilla (2014), en un entorno DNS se identifican varios puntos donde posibles ataques se desarrollan. Los vectores de ataque se sitúan tanto en el servidor DNS local, como en las comunicaciones externas.

1.4.1. Vectores de ataque y amenazas en un escenario DNS

Define López Padilla (2014),
Sobre el escenario típico DNS se numeran las 5 áreas principales que presentan una superficie susceptible a amenazas. Estas amenazas se resumen en las siguientes:

a. **Amenazas locales:** en la prevención de las amenazas locales, la solución más sencilla es la implementación de medidas y políticas de seguridad en la red interna. Mecanismos anti spoofing, IDS/IPS, así como la protección de los canales de acceso a los servidores y sus archivos sentarán la línea base de protección en esta área.

b. **Amenazas Servidor** – Servidor: Actualizaciones dinámicas. Presentes si el tamaño de la organización o el número de servidores a administrar obliga a centralizar la administración de los datos a través de DDNS (Dynamic DNS).

Una opción válida para asegurar la comunicación sería de dedicar un canal de comunicación restringido y/o implementar TSIG.

c. **Amenazas Servidor Máster** – Servidor Esclavo: Transferencias de zona. Si una organización cuenta con servidores esclavos, tiene la necesidad de ejecutar transferencias de zonas maestro/esclavo. En estos casos la solución a considerar es la implementación de TSIG (Transaction SIGnature), de modo en las operaciones de transferencia de zona se firmen con una clave conocida por ambas partes. Adicionalmente la seguridad en las comunicaciones usa SSL/TLS. Otras opciones pasarían por un canal de red privado para la transacción, o en caso extremo deshabilitara y realizarla manualmente, lo cual no es una alternativa funcional.

d. **Amenazas Servidor Máster – Servidor Cliente Caché/Resolver.** Como se verá en el apartado Aleatoriedad del ID de transacción y puerto origen, las mejoras implementadas en las versiones recientes de Bind con la introducción de aleatoriedad en los puertos origen de la consulta, así como en los identificadores de mensaje, dificultan la posibilidad de envenenamiento de caché en los servidores DNS, pero, aun así, el ataque es posible.

e. **Servidor – Cliente:** en el flujo de información entre un cliente denominado, también, resolver y un servidor DNS, existe la posibilidad de presentarse ataques locales para interceptar datos y spoofing con el objetivo de direccionar los clientes a un servidor DNS atacante.

1.1.1 Vulnerabilidades y puntos débiles en la especificación DNS

Define López Padilla (2014),

a) Capa de transporte UDP e IP spoofing.

UDP es un protocolo de transporte de red en el que prima la velocidad de la transmisión y sobre el cual se envía y recibe la información sin que se haya establecido previamente una conexión y sin confirmación ni control de entrega/recepción de la misma. Esto posibilita el falseo de direcciones IP (IP spoofing) y la suplantación de mensajes, en las especificaciones de implementación se recomienda, por motivos de rendimiento, usar UDP en las consultas. Se sugiere limitar el uso de TCP para transacciones de transferencias de zona o para aquellas consultas que superan el tamaño máximo, establecido en 512 bytes en mensajes sobre UDP.

b) Debilidad en la identificación y validación de mensajes DNS

Paralelamente al problema del uso del protocolo UDP en el mensaje de transporte de mensaje DNS se añaden debilidades de diseño en el aspecto de la identificación y validación de paquetes que favorecen la falsificación de los mismos. Como se describe en formato genérico de mensaje DNS, en la sección HEADER de un mensaje DNS se destina el campo ID para identificar el mismo. Este identificador, representado por un número de 16 bits, es muy importante para el mecanismo de validación de mensajes de respuesta, posibilita ataques de suplantación de dirección IP con relativa facilidad.

Validación de respuestas

No obstante, el campo ID no es el único elemento que se comprueba al validar una respuesta y según se infiere del RFC1034, los requisitos mínimos para aceptar una respuesta son:

- ✓ El puerto del destino en el datagrama de respuesta es el mismo que el puerto origen del cliente que genera la consulta.
- ✓ El campo ID del mensaje de respuesta es el mismo que el campo ID del mensaje de consulta.

- ✓ El campo ANSWER se refiere al mismo recurso que el campo de pregunta (QUESTION).
- ✓ La sección AUTHORITATIVE contiene un listado de los servidores autoritativos de la sección de respuesta (ANSWER).

Con ésta condiciones si se conoce el recurso solicitado, es sencillo construir una respuesta falsa, de este modo, un atacante si consigue encontrar el ID con el que se emitió la consulta, entonces dispondrá de la información necesaria para falsear una respuesta. Esto, unido a una transmisión sobre UDP, la cual carece de un control/validación de la comunicación, da como resultado que la respuesta falsa será aceptada por el servidor como válida para la consulta realizada previamente.

Identificador de mensaje ID

Debido a la escasa longitud destinada al campo ID del mensaje (16 bits) y a debilidades en la generación de la secuencia de estos, computacionalmente es relativamente sencillo construir un número suficiente de ID´s en un tiempo limitado para conseguir “acertar” con el ID original. Sin embargo, se han mejorado muchos aspectos en la fortificación del ID y otros valores en el mensaje DNS desde que, en 2008 Dan Kaminsky un investigador en seguridad IT, presentó su trabajo sobre “DNS caché Poisoning”, donde demostró lo sencillo que era conseguir falsificar una respuesta a una consulta DNS y de este modo, lograr que el servidor solicitante almacenase la misma en su caché.
Esto convierte al protocolo DNS en un objetivo fácil para dos tipos de ataques DNS como el IP spoofing: DNS Caché Poisoning y Denegación de servicio por amplificación DNS.

1.4.2. Ataques DNS

DNS Caché Poisoning y DNS Spoofing

Plantea López Padilla (2014), en una query DNS se usa el campo ID de la sección HEADER del mensaje para identificar la transacción y su correspondiente

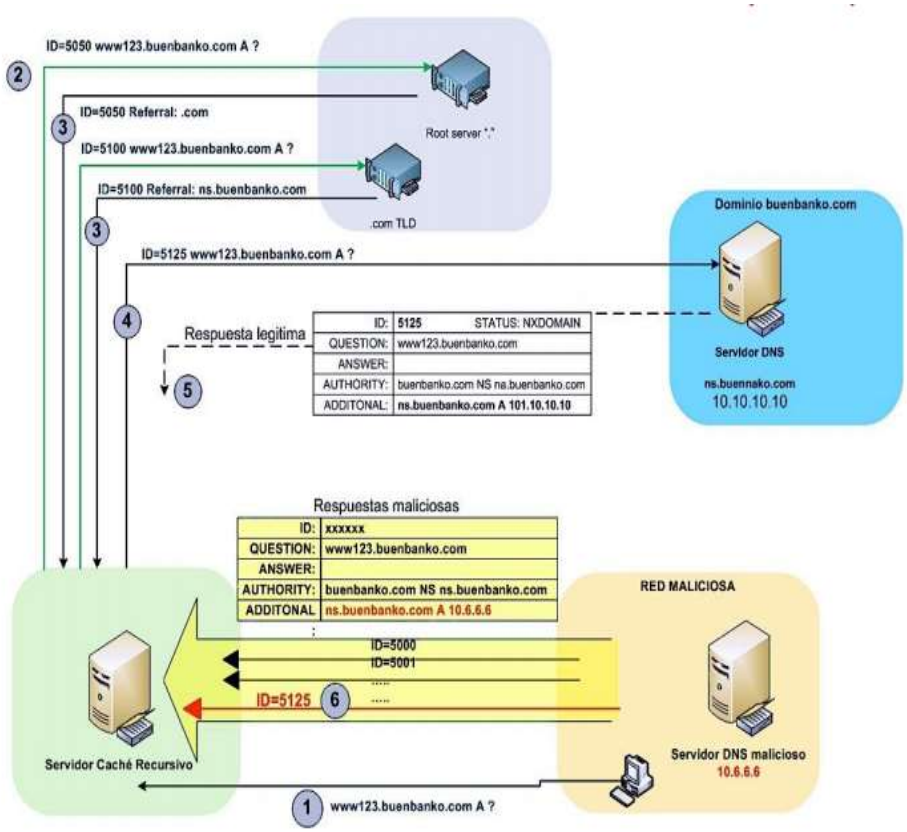
respuesta. Bajo la utilización del protocolo UDP y sin usar ningún mecanismo de control, un atacante envia respuestas simultáneas cada una con distintos ID hasta lograr coincidir con el ID generado en la consulta. Si es así, y se consigue hacer llegar la respuesta falsa antes de que llegue la legitima (condición de carrera), el servidor que ha iniciado la consulta la aceptará y la almacenará en su caché. De este modo, es posible “envenenar” la caché de un servidor DNS recursivo con un registro manipulado. A partir de este momento, durante el tiempo que el registro queda almacenado en la caché (TTL), el servidor víctima redirigirá a una IP ilegítima todas las solicitudes de un resolver que le consulte por el recurso manipulado.

La secuencia que se produce en un envenenamiento caché y que se muestra en la Figura 1 es la siguiente: El atacante, con un servidor DNS bajo su control, solicita un nombre que pertenezca al dominio al cual quiere suplantar (1). Se asegura que este nombre no esté cacheado. El servidor víctima que no encuentra en su caché en el recurso perdido, inicia la secuencia de peticiones iterativas empieza por los servidores raíz (2) y recorrie los TLD que se le indica en el referral (3) hasta que sepa a qué servidor, autoritativo del recurso, dirigir la pregunta (4). En ese instante, el servidor atacante inicia un envío masivo de respuestas (6) con distintos ID con el objetivo de coincidir en una de ellas con el ID de la query del servidor víctima quien originalmente realiza la consulta. En esas respuestas se indica que el servidor autoritativo (AUTHORITY) para el dominio a suplantar se encuentra en la IP del servidor malicioso. Si se consigue hacer llegar la respuesta falseada (6) antes de que llegue la original (5), el servidor víctima almacenará en caché el registro falseado con la IP del servidor legítimo. La respuesta legítima que llegará después será descartada.

En este momento, el envenenamiento de caché o caché poisoning del servidor víctima se ha completado con éxito, y todas las solicitudes de *resolvers* que le lleguen de subdominios pertenecientes al dominio suplantado se dirigirán al servidor malicioso que se encargará de ofrecer las IP bajo su control según le convenga.

Si no se aplica ninguna otra defensa, el atacante sólo tiene que generar con la velocidad necesaria un número de respuestas suficiente para acertar con el ID original. Gráficamente se observa el proceso descrito en la figura 1.1.

Figura 1.1 DNS caché poisoning y DNS Spoofing



Fuente (Guía de seguridad servicios DNS, 2020)

1.5. Ataques de denegación del Servicio

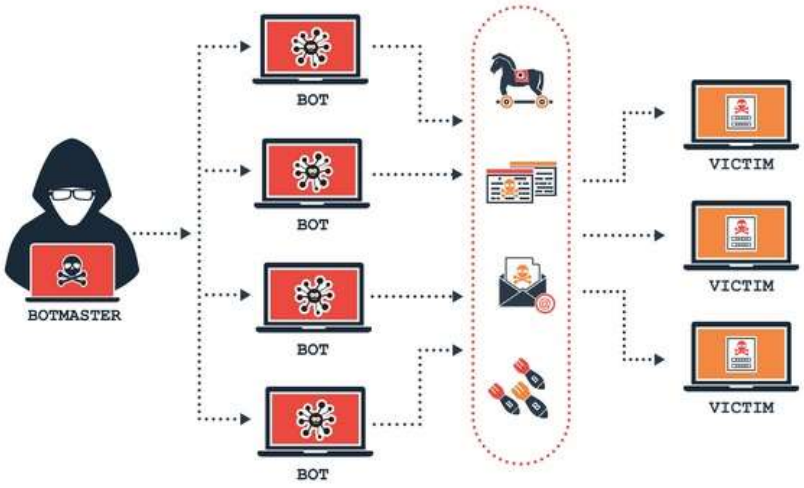
Menciona López Padilla (2014), el Protocolo DNS debido a su vulnerabilidad intrínseca a *spoofing IP*, se convierte en un aliado a la hora de implementar ataques de denegación de servicio. Esto, unido a su amplia distribución y acceso a nivel mundial hacen de este tipo de ataques uno de los más eficaces y utilizados.

Existen dos técnicas para este tipo de ataques: la denegación de servicio o DoS (por sus siglas en inglés Denial of Service) y la denegación de servicio distribuido o DDoS (por sus siglas en inglés Distributed Denial of Service).

En el caso de ataques DDoS, se realizan peticiones o conexiones emplea un gran número de ordenadores o direcciones IP, estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio objeto del ataque. Un ataque DDoS, no es más fácil de detectarlo, en vista que el número de solicitudes proviene de diferentes direcciones IP y el administrador de la red no bloquea la IP específica que está realiza dichas peticiones.

Los servidores que realizan el ataque DDoS son reclutados mediante la infección de un malware convirtiéndose así en bots o zombies en espera para ser controlados de manera remota por un ciberdelincuente.

Figura 1.2 Ataque DDoS

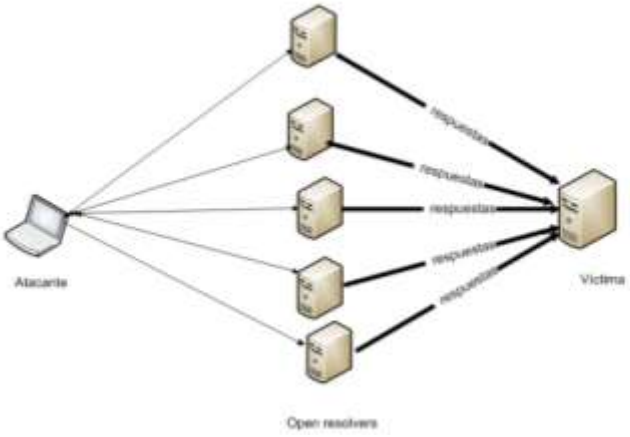


Fuente (OSI, 2018)

1.5.1. Ataque de amplificación DNS

Redacta López Padilla (2014), una vez más, el uso de UDP en el transporte de mensajes DNS, así como la enorme cantidad de servidores recursivos accesibles en Internet (open resolvers) posibilita el uso del servicio para establecer ataques distribuidos de denegación de servicio hacia otros servidores. Uno de los principales ataques basados en DNS, es el de Amplificación DNS.

Figura 1.3 Ataque amplificación DNS



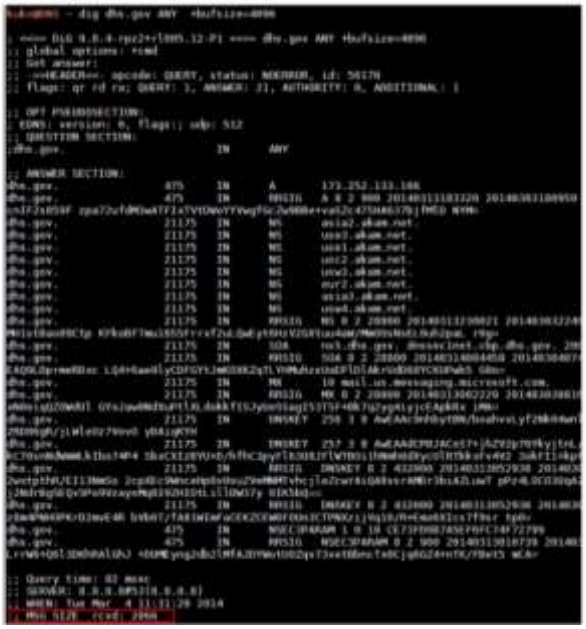
Fuente (Guía de seguridad servicios DNS, 2020)

En un ataque de Amplificación DNS se pretende desbordar la capacidad de respuesta de un servidor haciéndole llegar una gran cantidad de datos DNS. El procedimiento consiste en lanzar consultas DNS a un open resolver falsea la IP de origen con la IP del servidor/host a atacar. Esta técnica se conoce como IP *spoofing* y es ampliamente utilizada en sistemas con base UDP donde la falta de control sobre la conexión posibilita el falsificación o suplantación de direcciones IP.

En las consultas manipuladas, se cambia la dirección IP de origen por la IP objeto del ataque, y se envían de forma masiva a tantos servidores (open *resolvers*) como sea posible. Los *resolvers*, envían la respuesta a la dirección IP indicada. Con una cantidad suficiente de consultas, y solicita recursos cuya respuesta sea mucho mayor que la consulta emitida, se consigue generar un gran volumen de tráfico hacia el host objetivo. Esto provocará la congestión de los recursos de la víctima y la pérdida o denegación del servicio. Si el ataque se lanza de manera simultánea desde varios puntos, el volumen de tráfico es aún más elevado.

En la figura 1.4, se observa claramente el factor de amplificación, donde se obtiene 2066 bytes. Una consulta suele rondar los 66 bytes.

Figura 1.4 Factor de amplificación



Fuente (Guía de seguridad servicios DNS, 2020)

1.1.2 Ataques sobre el registro de dominios DNS HIJACKING

Afirma López Padilla (2014), muchos servicios de registro de dominios que operan con multitud de empresas de gran valor comercial poseen procedimientos automatizados para ofrecer una vía ágil para el control de los registros. Muchos ataques sobre los registradores parten del conocimiento y el análisis de estos procedimientos. Por ejemplo, un atacante usa la información más relevante de una empresa como el servicio de correos electrónicos para intentar a través de *phising* enviar emails de manera masiva hasta lograr el secuestro (*hijacking*) del dominio, luego el atacante procede a redireccionar a una IP bajo su control para recolectar información importante.

Frecuentemente, una mala política de seguridad sobre el control o acceso de la cuenta de administración del registro de dominio, tanto por parte del registrador como por el cliente, desemboca, también, en el compromiso de dominio.

1.2. Seguridades DNS

1.2.1. Medidas contra el ataque de Caché Poisoning

Plantea López Padilla (2014), en el documento de la IETF se describe la problemática del DNS *spoofing* y se trazan líneas base en las implementaciones del software DNS con objeto de detectar y evitar esta amenaza:
"Un resolver, con objeto de validar una respuesta DNS, realiza las siguientes comprobaciones:

- ✓ La sección question del paquete de respuesta es equivalente a la consulta realizada en la query.

- ✓ El campo Id del paquete de respuesta coincide con el Id de consulta.

- ✓ La respuesta procede de la misma dirección y puerto desde la cual la pregunta fue enviada.

- ✓ La respuesta llega a la misma dirección y puerto desde la cual emitió la pregunta.

- ✓ Es la primera respuesta recibida en cumplir las cuatro condiciones anteriores."

Aleatoriedad del ID de transacción y puerto origen

Puesto que el campo ID es clave en la identificación de los mensajes DNS, y desde el ataque de caché poisoning demostrado por Dan Kaminsky, se ha tratado de dificultar la predictibilidad del ID de la transacción, añade aleatoriedad en su generación en las consultas y así hacerlo menos predecible. Esta medida, a pesar de todo, fue insuficiente debido a la limitación del campo ID, 16 bits que resulta en 216= 65535 valores posibles. Posteriormente se introduce la aleatoriedad en el puerto origen de la consulta, que tradicionalmente estaba en el puerto 53. Los puertos disponibles para asignar aleatoriamente descuentan los privilegiados 1 –

1023 son pues del 1024 – 65535 es decir 2/11= 2048 puertos. El resultado total de estas medidas da 211 * 216= 134.215.680 posibles valores. Con este número de posibilidades se dificulta enormemente obtener el ID de la transacción en el tiempo limitado disponible hasta la llegada de la respuesta legitima (sin considerar una denegación de servicio para retrasarla).

• 0 * 20 bit encoding

Como complemento a la aleatoriedad en el ID de transacción y el puerto origen, existen otros factores complementarios que algunos fabricantes como Nominum11 implementan. La técnica 0*20 bit encoding consiste en realizar las consultas DNS alterna aleatoriamente mayúsculas y minúsculas. Puesto que el protocolo DNS no distingue entre ambas, se resolverá de igual forma el dominio WwW.EjEmPlo.Com que www.ejemplo.com, sin embargo la implementación del software solo validará aquella respuesta que coincida en la capitalización de los caracteres con la consulta. De este modo se minimiza la posibilidad de aceptar una respuesta falsa si no es coincidente con el formato original de la consulta.

Validación de respuestas y detección spoofing. Retransmisión sobre TCP

Introduce mecanismos aleatorios para seleccionar ID y puerto origen en la generación de consultas se consigue dificultar el ataque *spoofing*, pero teóricamente aún es imposible. Por ello, se hacen necesarias comprobaciones adicionales sobre la respuesta en sí.

Un buen resolver detecta intentos de *spoofing* aplica criterios como los diseñados en el RFC 5452, de modo que, si aplica esos criterios, se están descarta muchos paquetes en respuestas a una consulta determinada, se abane la petición sobre UDP y se reintente a través de TCP.

Limitar recursión

Una medida complementaria es limitar la recursión y de este modo minimizar el riesgo a ataques DNS. De hecho, la gran cantidad de servidores recursivos que ofrecen su servicio públicamente (conocidos como *open resolvers*) constituye la principal fuente usada para establecer ataques de gran potencia, como los de denegación de servicio por amplificación DNS.

Solución al poisoning: DNSSEC

Se considera que la solución más eficaz para minimizar esta amenaza es con la implementación ***DNSSEC*** (Domain Name System Security Extensions) mediante la configuración de claves de registros comprueba la integridad y autenticidad de los datos.

1.5.2. Seguridad ante ataques de amplificación DNS

Afirma López Padilla (2014), globalmente el problema de denegación de servicio basado en amplificación DNS tiene su origen en la enorme cantidad de servidores DNS distribuidos mundialmente y configurados como open *resolvers*, esto es, que ofrecen su servicio sin ningún tipo de restricción a cualquier solicitante de Internet.

Hay proyectos como Open Resolver Project dirigidos a motivar el control de open *resolvers* dirigida a propietarios de servidores DNS de modo que controlen o limiten las consultas recursivas procedentes de localizaciones ajenas a su red. Los administradores de *resolvers* DNS realiza distintas tareas para prevenir que sus sistemas sean utilizados para establecer ataques de amplificación DNS. Entre las medidas más importantes que se contempla, están *anti-spoofing*, filtrados de tráfico y, técnicas de Rate Response Limit (Límite de respuesta de frecuencia) y la configuración más adecuada de recursividad.

1.5.3. Medidas de seguridad DoS

Menciona INCIBE (2019), que genéricamente y referente a la arquitectura de red, algunos errores comunes a evitar son:

- Colocar los servidores en una misma subred.
- Detrás del mismo router.
- Usar una única línea o ruta de provisión a internet.
- Dentro de un único sistema autónomo (AS).

1.5.4. Medidas de seguridad contra ataques DDOS

Define INCIBE (2019),

a) Limitar la tasa de peticiones

Limitar el número de peticiones que un servidor aceptara durante un tiempo determinado es una buena manera de mitigar ataques de denegación de servicio. Hay que tener claro que limitar la velocidad de peticiones ralentiza los trabajos de raspadores web. También, reduce los intentos de fuerza bruta para iniciar sesión.

b) Implementar un Firewall de aplicaciones web

Un firewall de aplicaciones web es una herramienta que es utilizada para mitigar ataques de Ddos en capa 7. Implementa el WAF (Web Application Firewall) entre internet y el servidor de origen, sirve como proxy de reversa. Protege así el servidor objetivo de numerosos tipos de tráfico maliciosos.

Al filtrar las peticiones usa como base una serie de reglas para identificar herramientas empleadas en ataques Ddos, los ataques en capa 7 son impedidos. Una de las principales características que tiene el WAF es su capacidad para implementar rápidamente reglas personalizadas ante un ataque.

c) Aplica redes de difusión Anycast

Al aplicar una red de difusión Anycast se mitigan ataques de denegación de servicio, al dispersar el tráfico malicioso, se envia a través de una red de servidores hasta una red externa. Esto es algo muy similar a como si se canaliza un río a través de canales más pequeños y separados. Este tráfico se vuelve manejable y se lleva hasta una desembocadura sin que afecte el entorno. Es importante señalar que la efectividad de una red Anycast dependerá del tamaño del ataque y la eficiencia de la red interna.

1.5.6. Medidas contra HIJACKING o secuestro de dominio

Menciona López Padilla (2014), por parte de los servicios de registro de dominios, las medidas que tienen en cuenta para garantizar la protección contra accesos no autorizados y verificación de la autenticidad de las identidades de los registros y/o cambios solicitados. Los clientes a su vez establecen con el registrador el compromiso de mantener una política de seguridad referente al control de acceso, contactos y verificación de identidades para prevenir suplantaciones derivadas de *phising* o ataques de ingeniería social.

Verificación de registro.

Las cuentas de registro de dominios cuentan con un método de verificación como el registro TXT, LOC entre otros para garantizar la autenticidad del solicitante, con el objetivo de minimizar suplantaciones de identidad y hackeo del dominio. Estudios realizados sobre *phising* experiencias con *botnets*, y ataques de *fast-flux* dejan patente la importancia sobre el control cuentas de registros de dominios de actividades cibercriminales.

Fortalecimiento del sistema de autenticación

Implementar políticas y mecanismos fiables mediante la utilización de contraseñas seguras, mantenimiento y transmisión de datos con seguridad en la conexión (SSL, VPN), en virtud que se consideran medidas adicionales altamente recomendables.

Política de renovación

Igualmente, que una verificación de los contactos e identidades de las peticiones de registro es importante mantener una vía de comunicación en cuanto a las renovaciones y cambios que se produzcan en el dominio registrado. Es importante mantener una política interna para la actualización y desactivación de los registros que hayan caducado esto forma parte de un robo de información incluso de un tercero que toma el registro caducado con el objeto de beneficiarse.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Argumentación de la metodología de investigación

A fin de proteger la disponibilidad y confidencialidad de la información, dentro del Hospital de la ciudad de Latacunga, se procedió con la realización de pruebas de vulnerabilidad al servidor DNS de la Institución, para el cual, se hace uso de diversos tipos de investigación, esto con el fin de cumplir no solo con los objetivos planteados en la investigación sino, también, mitigar en su totalidad las vulnerabilidades del servidor DNS.

El enfoque de la investigación es cualitativo, un estudio de campo y como instrumento se utiliza como técnica la encuesta al personal de TICs del Hospital General Latacunga así, también, se realizaron pruebas que permita analizar las vulnerabilidades del servidor DNS.

2.1.1. Enfoque de la investigación

El enfoque de la investigación es de tipo cualitativo, debido a que se recogieron datos de suma importancia acerca del personal de TICs del Hospital General Latacunga.

2.1.2. Investigación de campo

Se utilizó este tipo de investigación, en el Hospital General de Latacunga ubicado las calles Hermanas Páez 1-02 y 2 de mayo, específicamente en el Área de Tecnologías de la Información, lugar donde se suscita el fenómeno de estudio.

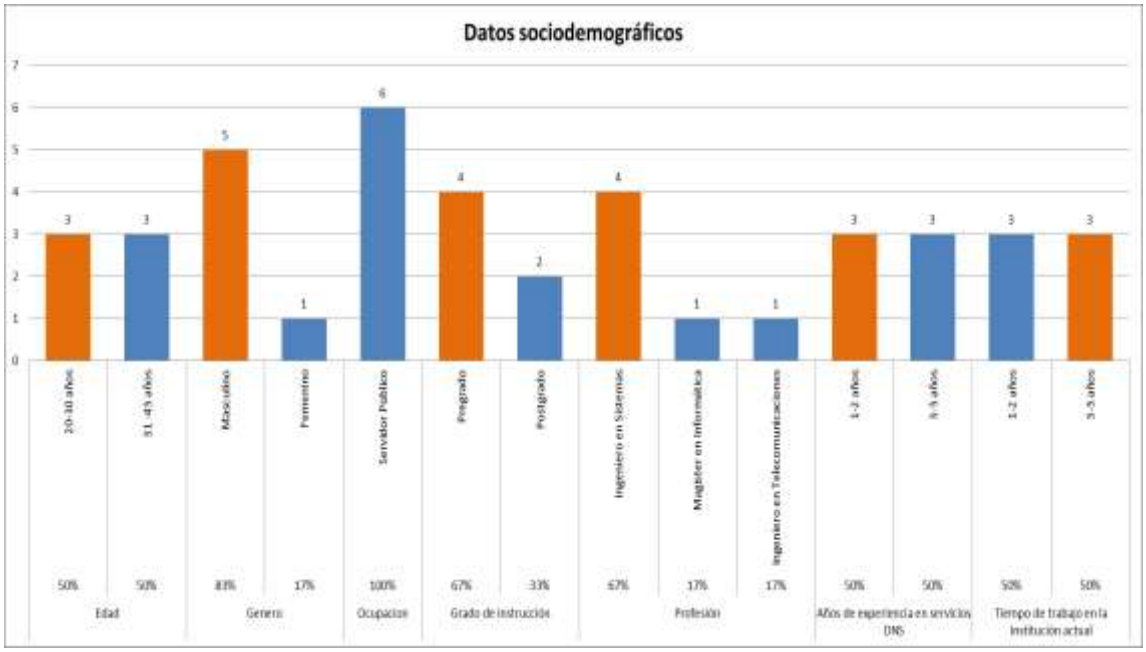
2.1.3. Técnicas e Instrumentos de Investigación

En el presente proyecto se aplicará la técnica de la encuesta, para medir el nivel de conocimiento de los colaboradores del Área de TICs, en métodos de seguridad informática ante ataques DNS.

Encuesta

La encuesta se aplica a 6 personas, para medir el nivel de conocimiento sobre las seguridades de DNS en redes IPV4 e IPV6. Con el fin de recopilar datos sociodemográficos con los siguientes datos: edad, género, ocupación, grado de instrucción, profesión, años de experiencia en el área de tecnologías específicamente, servicios DNS y tiempo de trabajo en la Institución. Los resultados se muestran en la Figura 2.1

Figura 2.1 Datos sociodemográficos



Fuente: Elaboración propia

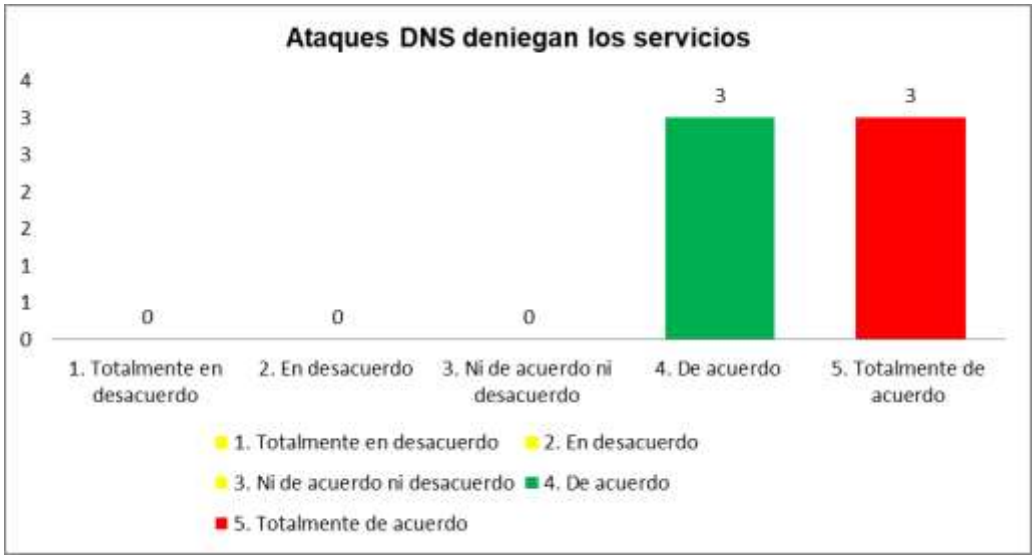
De la encuesta realizada al personal de TICs del Hospital General Latacunga, se concluye que, el 50% tienen un rango de edad entre 20 y 30 años, y el otro 50% está en edades de entre 31 a 45 años, según el género el 83% corresponde al género masculino, mientras que el 17% corresponde al género femenino. Según la ocupación el 100% son servidores públicos.

El grado de instrucción del personal es de 67% correspondiente a pregrado, mientras que el 33% son de postgrado. Por otra parte, en los años de experiencia en servicios DNS, se evidencia que la mitad del personal no poseen más de 2 años

de experiencia, mientras que, la otra mitad no supera los 5 años. En lo referente al tiempo de trabajo, el 3 de los 6 empleados tienen entre 1 y 2 años de antigüedad en la Institución, y los restantes poseen de 3 a 5 años de servicio.

La mayor parte del personal de TICs del Hospital General Latacunga tiene como mínimo instrucción de pregrado, esto determina que el personal posee un nivel de conocimiento adecuado en el campo de las Tecnologías de la Información. Una vez extraída la información del personal, se procede con la evaluación de conocimientos acerca de ataques DNS, para ello se utilizó la escala de Likert sobre el nivel de acuerdo o desacuerdo acerca de las preguntas planteadas, estas se muestran a continuación:

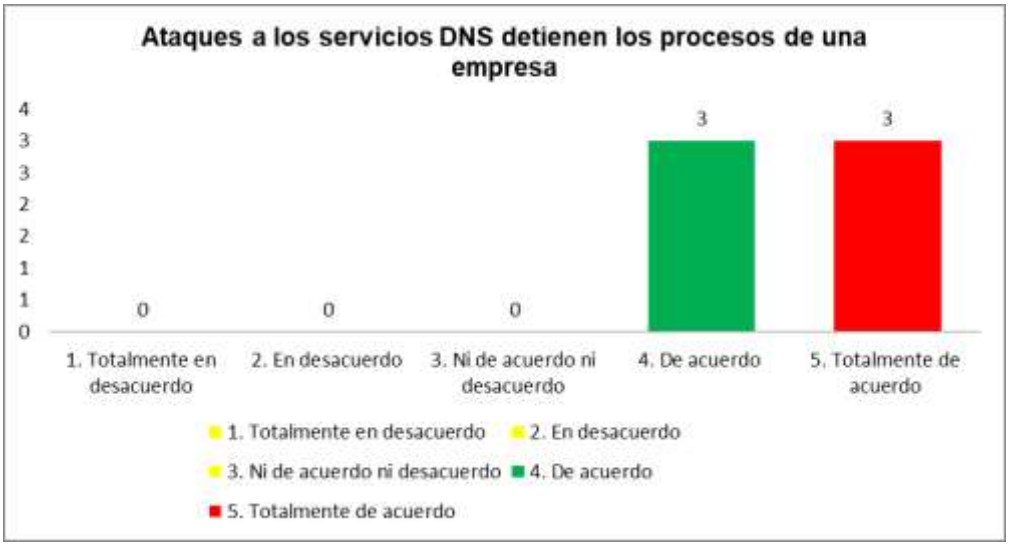
Figura 2.2 Los ataques informáticos a los servidores de DNS, deniega totalmente el servicio de una aplicación



Fuente: Tomado de encuesta al personal de TICs del Hospital General Latacunga

De la pregunta relacionada con los ataques de denegación de servicios el 100% de los encuestados, manifiestan estar de acuerdo y totalmente de acuerdo que los ataques informáticos deniegan totalmente el servicio de una aplicación.

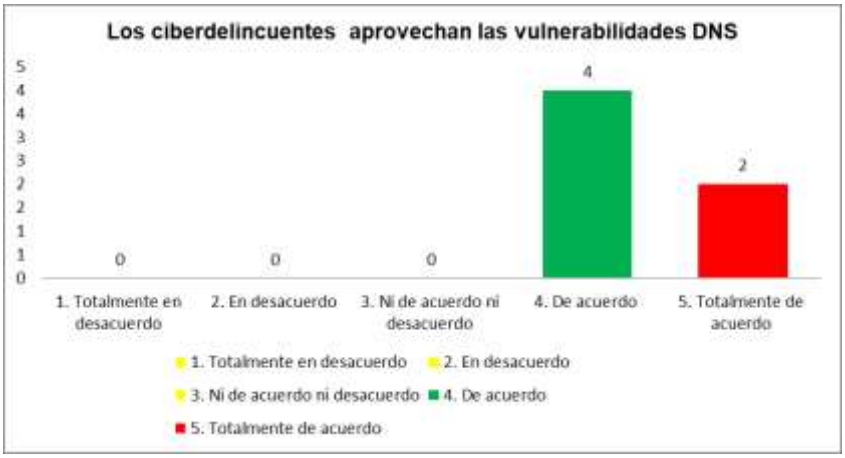
Figura 2.3 Los ataques a los servicios DNS de una empresa, generan gastos excesivos, incluso detiene los procesos internos.



Fuente: Tomado de encuesta al personal de TICs del Hospital General Latacunga

El 100% de los encuestados manifiestan estar de acuerdo y totalmente de acuerdo en que los ataques de los servidores DNS, afecta los procesos internos de una organización, así como incurrir en gastos excesivos.

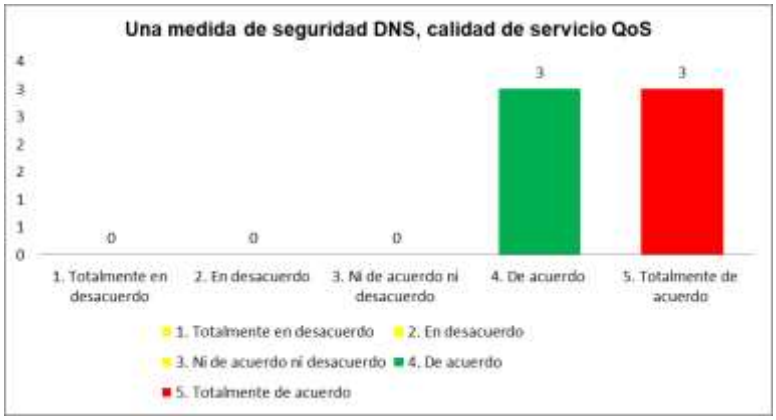
Figura 2.4 Los ciberdelincuentes aprovechan las vulnerabilidades que presentan los equipos servidores de DNS para fines maliciosos.



Fuente: Tomado de encuesta al personal de TICs del Hospital General Latacunga

De acuerdo con los resultados obtenidos 4 de los 6 encuestados, manifiestan estar de acuerdo en que, las vulnerabilidades en un servidor DNS, son aprovechadas por los ciberdelincuentes, los encuestados restantes están totalmente de acuerdo con el enunciado.

Figura 2.5 Una medida de seguridad ante ataques DNS, es limitar las peticiones con la inclusión configuraciones de calidad de servicio QoS.



Fuente: Tomado de encuesta al personal de TICs del Hospital General Latacunga

En la pregunta relacionada a la calidad de servicio QoS como medida de seguridad ante los ataques de DNS, el 100% que corresponde a los ítems de acuerdo y totalmente de acuerdo, manifiesta estar de acuerdo y totalmente de acuerdo que, con la configuración de aplicaciones de Calidad de Servicio, mitigan los ataques de DNS.

Figura 2.6 La configuración de DNSsec agrega una capa de seguridad a los servidores DNS, minimiza los riesgos a ataques informáticos.

Fuente: Encuesta al personal de TICs del Hospital General Latacunga

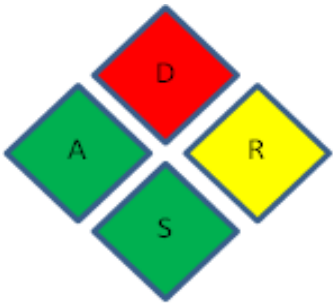
En la pregunta relacionada a las extensiones de seguridad de DNSsec, el 100% corresponde a los ítems de acuerdo y totalmente de acuerdo como medida de protección ante ataques informáticos a los servicios DNS, sin embargo, esto no mitiga en su totalidad ciertas vulnerabilidades.

Las respuestas obtenidas en la encuesta realizada al personal de la Institución, evidencia la necesidad de analizar las vulnerabilidades dentro del servidor DNS, puesto que, a pesar de poseer un conocimiento teórico, el personal no ha realizado pruebas de vulnerabilidades en los equipos del Datacenter, para dichas pruebas es necesario seguir cierta metodología, misma que se detalla a continuación.

2.2. Metodología de Desarrollo

Para el desarrollo de pruebas se usa la Metodología de Diamante, la cual de acuerdo con HSESoft (2021), “La metodología diamante, permite de forma cualitativa evaluar el impacto (Alto, Medio o Bajo) que puedan llegar a tener las amenazas previamente identificadas y categorizadas en 4 grupos que conformarían la evaluación en Diamante”. En la investigación, se propone los siguientes grupos frente a amenazas a los servicios DNS:

Figura 2.7 Metodología diamante.



Fuente: Elaboración propia

Donde:

A. Calificación de la probabilidad de ocurrencia: En esta fase de describe la probabilidad de ocurrencia de acuerdo a tres colores (Verde, Rojo y Amarillo).

D. Vulnerabilidad de los servidores DNS: En esta etapa se determina manera general la vulnerabilidad que presentan los equipos servidores DNS ante los ciberdelincuentes.

R. Determinación de los recursos informáticos: En esta etapa se describirán los escenarios utilizados para la elaboración de los ataques DNS.

S. Identificación de ataques y seguridades DNS: En la etapa de identificación de ataques DNS, se desarrollan en un ambiente simulado ataques DNS en los escenarios descritos en la determinación de recursos y se describen las distintas seguridades DNS ante los ataques simulados.

En la investigación, las fases detalladas anteriormente, se utilizan de la siguiente manera:

- **A: Calificación de la Probabilidad de ocurrencia**

La calificación se realiza mediante colores tiene en cuenta la probabilidad de ocurrencia de un ataque DNS de la siguiente manera:

Figura 2.8 Probabilidad de ocurrencia.

FENOMENO	COMPORTAMIENTO	COLOR ASGINADO
POSIBLE	Es aquel fenómeno que nunca ha sucedido, puede suceder o es factible porque no existen razones históricas y científicas para decir que esto no sucederá, es decir que no se descarta su ocurrencia.	Verde 
PROBABLE	Es aquel fenómeno que ya ha ocurrido en el lugar o en unas condiciones similares, es decir que existen razones y argumentos técnicos científicos para creer que sucederá.	Amarillo 
INMINENTE	Es aquel fenómeno esperado que tiene alta probabilidad de ocurrir o con información que lo hace evidente o detectable.	Rojo 
POSIBLE: Nunca ha sucedido color verde **PROBABLE:** Ya ha ocurrido color amarillo **INMINENTE:** Evidente detectable color rojo		

Fuente: Elaboración propia

Diagnóstico

En virtud al crecimiento tecnológico y al existir una mayor necesidad de servicios tecnológicos en la red de datos, ha aumentado, también, el crecimiento a gran escala de las vulnerabilidades ante la ciberdelincuencia; es así que, para el desarrollo del presente proyecto, se analizó la expectativa desde un punto macro

hasta un micro de los ataques realizados a servidores de DNS más relevantes ocasionados especialmente en los últimos años, éstos son un factor muy importante en las comunicaciones, porque de ello dependen todos los servicios tecnológicos en red, y si un ataque a un servicio DNS llega a tener éxito en su objetivo, causan desde la denegación de un servicio hasta la suplantación y robo de información valiosa, incluso ocasionan que los servicios de toda una empresa se detengan.

Mediante la simulación en laboratorio de ataques y seguridades a los servicios de DNS, el presente proyecto tiene como objetivo principal evaluar los mecanismos de seguridad DNS, y determinar el método de seguridad más adecuado acorde al tipo de ataque generado, con el propósito de brindar un aporte muy importante para toda la comunidad y que puedan minimizar a gran escala los riesgos a los ataques actuales de los servicios DNS.

D: Vulnerabilidad de los servidores DNS.

Análisis de las vulnerabilidades de los servicios DNS

Para el análisis de vulnerabilidades en redes IPv4 e IPv6 se ha planteado los ataques más comunes en servidores DNS, los cuales son:

- Denegación de Servicio
- Envenenamiento Caché
- DNS Spoofing

En cada escenario se utiliza un equipo router y un switch con la suficiente capacidad para la interconexión a de todos los equipos informáticos como la computadora atacante, la víctima y el equipo servidor de DNS. La utilización de varios routers o equipos switch no afecta al diseño en éstos no se configurarán las seguridades.

Las características de memoria RAM (Memoria de acceso aleatorio), disco duro, que se describen son los recomendados para cada sistema operativo, y todos cuentan con interfaz gráfica. En el caso de la máquina atacante para el propósito

del presente proyecto se asignó 8GB con el fin de no tener problemas de rendimiento, desde esta máquina se realizan todos los escenarios.

Para calcular los requisitos mínimos de hardware del servidor de DNS, se estima en base a la cantidad de usuarios a los que se les proporcionará el servicio. Al iniciar el servicio DNS, éste consume alrededor de 4MB de RAM, cada registro en una zona consume alrededor de 100 bytes en el disco duro, y cada consulta consumirá alrededor de 20 KB de RAM. Con esta información se calculan los valores mínimos de memoria RAM y disco duro, toma en consideración la cantidad de usuarios.

EL software que se describe en el presente capítulo se basa en las siguientes versiones: para el atacante Kali Linux versión 2021.1, Windows Server 2019 R2 como el servidor DNS, y el sistema operativo Windows 10 como el cliente.

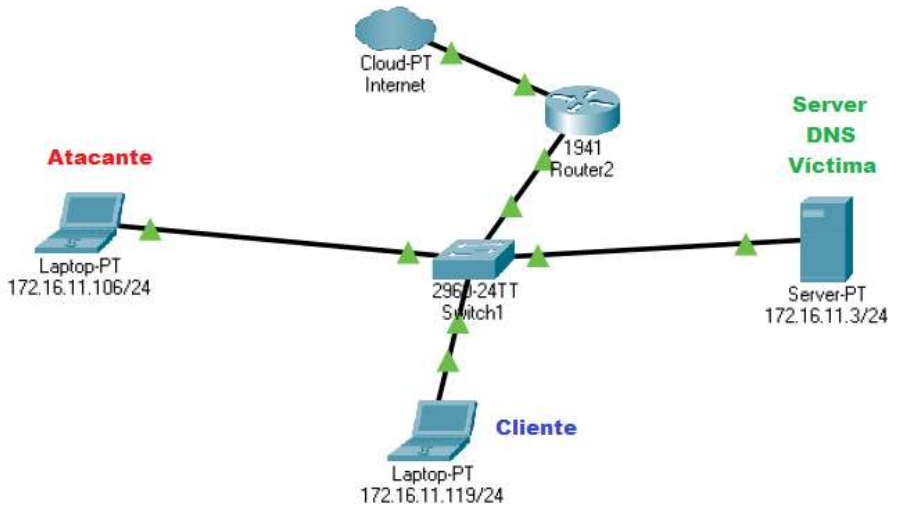
R: Determinación de los recursos informáticos.

Escenario para el ataque denegación de servicio

Este escenario está conformado por un equipo informático atacante, configurado con las herramientas informáticas necesarias para ejecutar el ataque, un equipo servidor DNS local como la víctima y un dispositivo con Windows 10 desde el cual se evalúa el resultado del ataque.

Es importante indicar que en el equipo servidor DNS se tiene configurado, también, el servicio de carpetas compartidas, para lo cual se analizará la disponibilidad de dicho servicio. Además, se tiene una conexión a Internet con el fin que el servidor DNS resuelva peticiones recursivas, consulta a servidores externos. En la figura 2.2 se muestra el escenario del ataque denegación de servicio.

Figura 2.9 Escenario denegación de servicio.



Fuente: Elaboración propia

a) Configuración

Este escenario está diseñado con tres computadoras: Servidor DNS (víctima), el atacante (Kali Linux), y el cliente; las computadoras se encuentran en el mismo segmento de red, el modelo implementado utiliza un router c-data FD-600 500GW y un switch cisco 2960, para conectar los distintos equipos.

La computadora atacante tiene la distribución Kali Linux versión 2021.1, el servidor víctima posee el sistema operativo Windows server 2019, y la máquina cliente tiene Windows 10, el servidor DNS tiene la configuración de consultas recursivas, poniéndose en contacto con otro servidor DNS raíz, para resolver las peticiones del cliente. A continuación, en la tabla 2.1 se describe a manera de resumen los componentes del escenario denegación de servicio.

Tabla 2.1 Especificación de recursos ataque denegación de servicios

Denominación	**Recursos**	**Sistema Operativo/ Distribución**	**Dirección IP**	**Función**
Servidor DNS víctima	Procesador Intel core i7-4770 3.4GHz, Disco Duro de 500GB, Memoria RAM de 8GB	Windows Server 2019	172.16.11.3/24	Servidor recursivo DNS

Atacante	Procesador Intel core i7-7600u 2.8GHz, Disco Duro de 240GB, Memoria RAM de 8GB	Kali Linux 2021.1	172.16.11.106/24	Contiene las herramientas para el ataque DoS
Cliente	Procesador Intel core i7 8550u 1.9GHz, Disco Duro de 1TB, Memoria RAM de 8GB	Windows 10 Pro	172.16.11.119/24	Evaluar el ataque denegación de servicio

Fuente: Elaboración propia

El equipo servidor DNS víctima funciona con Windows Server 2019, por disponibilidad del equipo con licencia original y por ser una versión anterior pero aún en uso, lo hace perfecto para el análisis de ataques, debido a que la versión presenta una vulnerabilidad en un framework. Éste se encuentra configurado como servidor recursivo, es decir necesita escalar las consultas a otros servidores para atender las peticiones del cliente. Además, este servidor acepta las peticiones sin importar el origen y de manera ilimitada.

La computadora atacante, tiene la herramienta informática *hping3* que permite generar paquetes DNS por la línea de comandos, y enviarlos a manera de peticiones. La computadora atacante generará de manera deliberada dichos paquetes para saturar los recursos del equipo víctima (Servidor DNS).

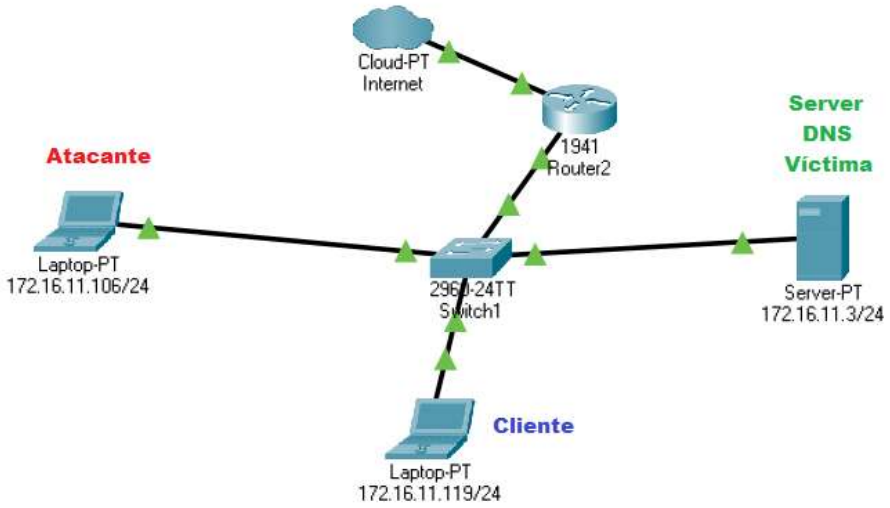
Escenario para el ataque envenenamiento de caché DNS

Este escenario está conformado por un equipo informático atacante, configurado con las herramientas informáticas necesarias para ejecutar el ataque, un equipo servidor DNS local como la víctima el cual es vulnerable a ataques de envenenamiento caché y un dispositivo con Windows 10 desde el cual se evalúa el resultado del ataque. Además, se tiene una conexión a Internet con el fin que el servidor DNS resuelva peticiones recursivas, consulta a servidores externos. En la figura 2.3 se muestra el escenario del ataque envenenamiento caché DNS.

El ataque de envenenamiento caché consiste en realizar directamente al servidor DNS, para lo cual en este escenario se necesita un computador atacante con Kali

Linux versión 2021.1, una máquina cliente con el sistema Operativo Windows 10, y un equipo servidor DNS con Windows Server 2019 R2.

Figura 2.10 Escenario para el ataque envenenamiento caché DNS.



Fuente: Elaboración propia

En la Tabla 2.2 se observa la función que cumple cada equipo en el escenario, denominación, descripción de los recursos, sistema operativo o distribución, dirección IP y función.

Tabla 2.2 Especificación de recursos ataque envenenamiento de caché DNS

Denominación	Recursos	Sistema Operativo/ Distribución	Dirección IP	Función
Servidor DNS víctima	Procesador Intel core i7-4770 3.4GHz, Disco Duro de 500GB, Memoria RAM de 8GB	Windows Server 2019	172.16.11.3/24	Servidor recursivo DNS
Atacante	Procesador Intel core i7-7600u 2.8GHz, Disco Duro de 240GB, Memoria RAM de 8GB	Kali Linux 2021.1	172.16.11.106/24	Contiene las herramientas para el ataque DoS
Cliente	Procesador Intel core i7 8550u 1.9GHz, Disco Duro de 1TB, Memoria RAM de 8GB	Windows 10 Pro	172.16.11.119/24	Evaluar el ataque denegación de servicio

Fuente: Elaboración propia

El equipo servidor DNS víctima funciona con Windows Server 2019, el cual es susceptible a ataques de envenenamiento de caché DNS. Éste se encuentra configurado como servidor recursivo, es decir necesita escalar las consultas a otros servidores para atender las peticiones del cliente.

Además, el servidor DNS acepta las peticiones sin importar el origen y de manera ilimitada. Y tiene configurado de manera estática el puerto origen para realizar las consultas, haciéndolo vulnerable al envenenamiento de caché.

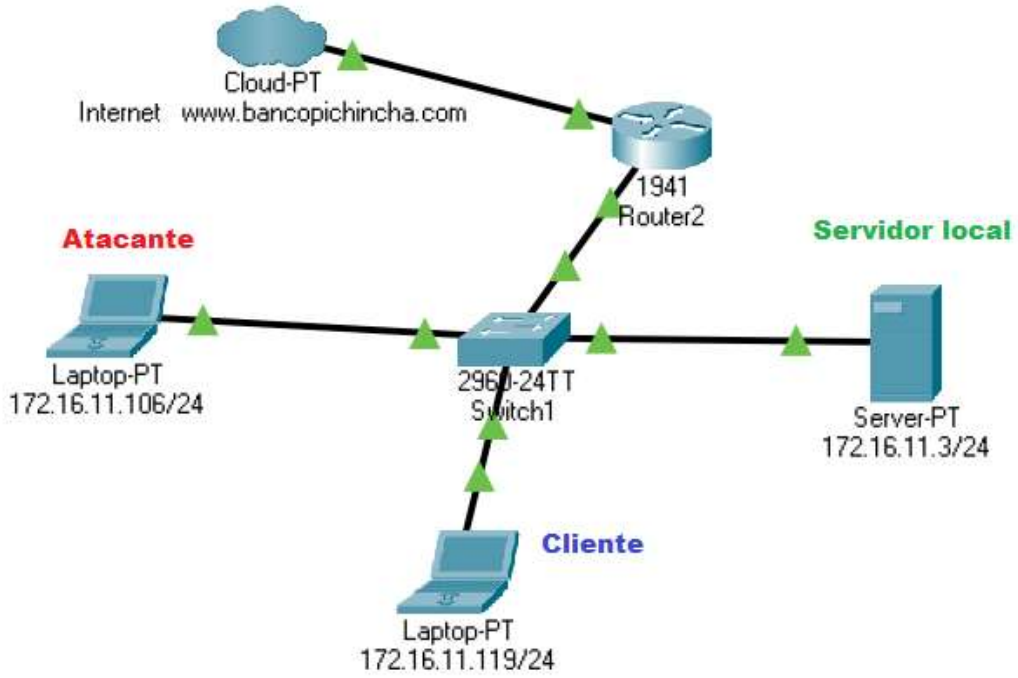
La computadora atacante, tiene la herramienta informática *ettercap,* que permite el envenenamiento de caché DNS.

Escenario para el ataque DNS Spoofing

Este escenario está conformado por un equipo informático atacante, configurado con las herramientas informáticas necesarias para ejecutar el ataque, un equipo servidor DNS primario como la víctima, un dispositivo con Windows 10 Pro. Además, se tiene una conexión a Internet con el fin de evaluar el ataque con un servidor externo. En la figura 2.4 se muestra el escenario del ataque DNS Spoofing.

El ataque de DNS Spoofing, es un extra del envenenamiento ARP redirige el tráfico por el equipo atacante, para lo cual en este escenario se necesita un computador con Kali Linux versión 2021.1 como atacante, una máquina cliente con el sistema Operativo Windows 10 cliente, y un equipo servidor DNS con Windows Server 2019 como la víctima.

Figura 2.11 Escenario para el ataque DNS Spoofing.



Fuente: Elaboración propia

En la Tabla 2.3 se observa la función que cumple cada equipo en el escenario, denominación, descripción de los recursos, sistema operativo o distribución, dirección IP y función.

Tabla 2.3 Especificación de recursos ataque DNS Spoofing

Denominación	**Recursos**	**Sistema Operativo/ Distribución**	**Dirección IP**	**Función**
Servidor DNS víctima	Procesador Intel core i7-4770 3.4GHz, Disco Duro de 500GB, Memoria RAM de 8GB	Windows Server 2019	172.16.11.3/24	Servidor recursivo DNS
Atacante	Procesador Intel core i7-7600u 2.8GHz, Disco Duro de 240GB, Memoria RAM de 8GB	Kali Linux 2021.1	172.16.11.106/24	Contiene las herramientas para el ataque DoS
Cliente	Procesador Intel core i7 8550u 1.9GHz, Disco Duro de 1TB, Memoria RAM de 8GB	Windows 10 Pro	172.16.11.119/24	Evaluar el ataque denegación de servicio

Fuente: Elaboración propia

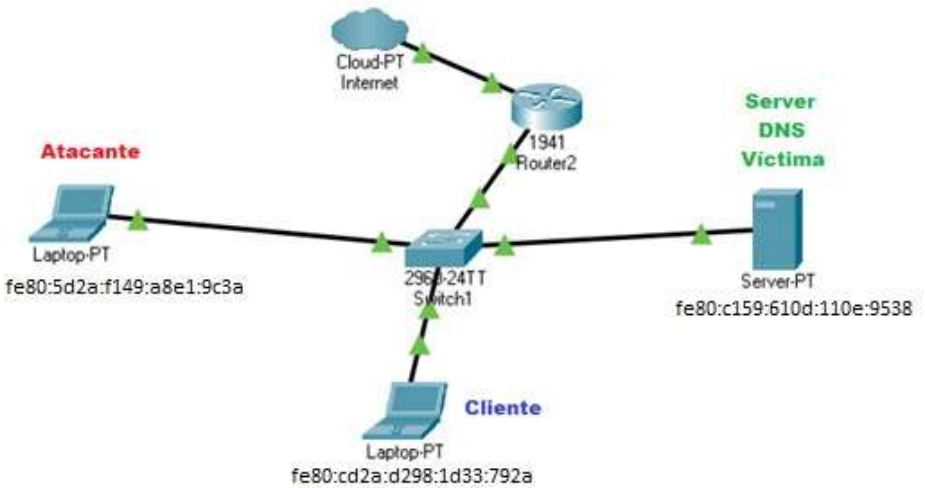
El equipo servidor DNS víctima funciona con Windows Server 2019, el cual es susceptible a ataques de envenenamiento de caché DNS y por ende a ataques DNS Spoofing. El servidor DNS acepta las peticiones sin importar el origen y de manera ilimitada. Y tiene configurado de manera estática el puerto origen para realizar las consultas, haciéndolo vulnerable al ataque DNS Spoofing.

La computadora atacante, tiene la herramienta informática *ettercap,* que permite a más del envenenamiento de caché DNS, realizar ataques de Spoofing.

Escenario para el ataque denegación de servicio IPv6

Este escenario está conformado por un equipo informático atacante, configurado con EvilFOCA, un equipo servidor DNS local como la víctima y un dispositivo con Windows 10 desde el cual se evalúa el resultado del ataque. Además, se tiene una conexión a Internet con el fin que el servidor DNS resuelva peticiones recursivas, consulta a servidores externos. En la figura 2.6 se muestra el escenario del ataque denegación de servicio.

Figura 2.12 Escenario denegación de servicio IPV6.



Fuente: Elaboración propia

b) Configuración

Este escenario está diseñado con tres computadoras: Servidor DNS (víctima), el atacante (Kali Linux), y el cliente; las computadoras se encuentran en el mismo segmento de red, el modelo implementado utiliza un router c-data FD-600 500GW y un switch cisco 2960, para conectar los distintos equipos.

La computadora atacante tiene la aplicación EvilFOCA, el servidor víctima posee el sistema operativo Windows server 2019 con licenciamiento de prueba, y la máquina cliente Windows 10, el servidor DNS tiene la configuración de consultas recursivas, poniéndose en contacto con otro servidor DNS raíz, para resolver las peticiones del cliente.

A continuación, en la tabla 2.4 se describe a manera de resumen los componentes del escenario denegación de servicio.

Tabla 2.4 Especificación de recursos ataque denegación de servicios

Denominación	**Recursos**	**Sistema Operativo/ Distribución**	**Dirección IPV6**	**Función**
Servidor DNS víctima	Procesador Intel core i7-4770 3.4GHz, Disco Duro de 500GB, Memoria RAM de 8GB	Windows Server 2019	fe80::c159:610d:110e:9538	Servidor recursivo DNS
Atacante	Procesador Intel core i7-7600u 2.9GHz, Disco Duro de 1TB, Memoria RAM de 8GB	EvilFOCA	fe80::5d2a:f149:a8e1:9c3a	Contiene las herramientas para el ataque DoS
Cliente	Procesador Intel core i3 3317u 1.7GHz, Disco Duro de 500GB, Memoria RAM de 6GB	Windows 10 Pro	fe80::cd2a:d298:1d33:792a	Evaluar el ataque denegación de servicio

Fuente: Elaboración propia

El equipo servidor DNS víctima funciona con Windows Server 2019 con una versión de prueba. Éste se encuentra configurado como servidor recursivo, es decir necesita escalar las consultas a otro servidor para atender las peticiones del cliente.

Además, este servidor acepta las peticiones sin importar el origen y de manera ilimitada.

La computadora atacante, tiene configurada la herramienta informática *EvilFOCA* que permite generar paquetes DNS a redes IPV6, y enviarlos a manera de peticiones. La computadora atacante generará de manera deliberada dichos paquetes para saturar los recursos del equipo víctima (Servidor DNS).

S: Identificación de ataques y seguridades DNS

La identificación de ataques y seguridades DNS, permite analizar las vulnerabilidades del servicio dentro de la red del Hospital General Latacunga, para lo cual se realizaron pruebas y simulaciones a fin de evaluar el nivel de impacto, así como, también, tratar de mitigar el riesgo e impacto ante ataques al servidor. Para los escenarios propuestos se hizo uso de las herramientas de software para pentesting.

Herramientas de software

Son programas, aplicaciones o instrucciones que permiten gestionar una tarea específica, para el presente caso se utilizan: Kali Linux, Windows Server, Windows 10 y EvilFOCA, como principales programas y aplicaciones para crear, gestionar y mantener un ataque simulado a un equipo servidor DNS específico.

Los resultados de las pruebas de simulación, así como, también, los métodos de protección se detallan en el Capítulo III presentado a continuación.

CAPITULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Al haber concluido las pruebas realizadas en los escenarios propuestos a fin de evaluar las vulnerabilidades que poseen los servidores DNS, y de esta forma realizar las correcciones adecuadas dentro del Hospital General Latacunga, se procede con el análisis de estos.

Dichas pruebas están realizadas mediante la metodología Diamante a fin de evaluar el nivel de vulnerabilidad e impacto que cada uno de estos ataques, dicho resultado se presenta a continuación.

3.1. Análisis de S: Identificación de ataques y seguridades DNS

Implementación de ataque denegación de servicio IPV4

Un ataque de denegación de servicio conocido, también, como ataque DoS, afecta directamente a un recurso informático y que a la vez no esté disponible para los usuarios previstos, afecta una red o un servidor con solicitudes o datos, el atacante inunda los recursos como CPU, memoria RAM, entre otros de un equipo servidor mediante el envío masivo de peticiones. Los comandos principales para generar este tipo de ataques es el siguiente:

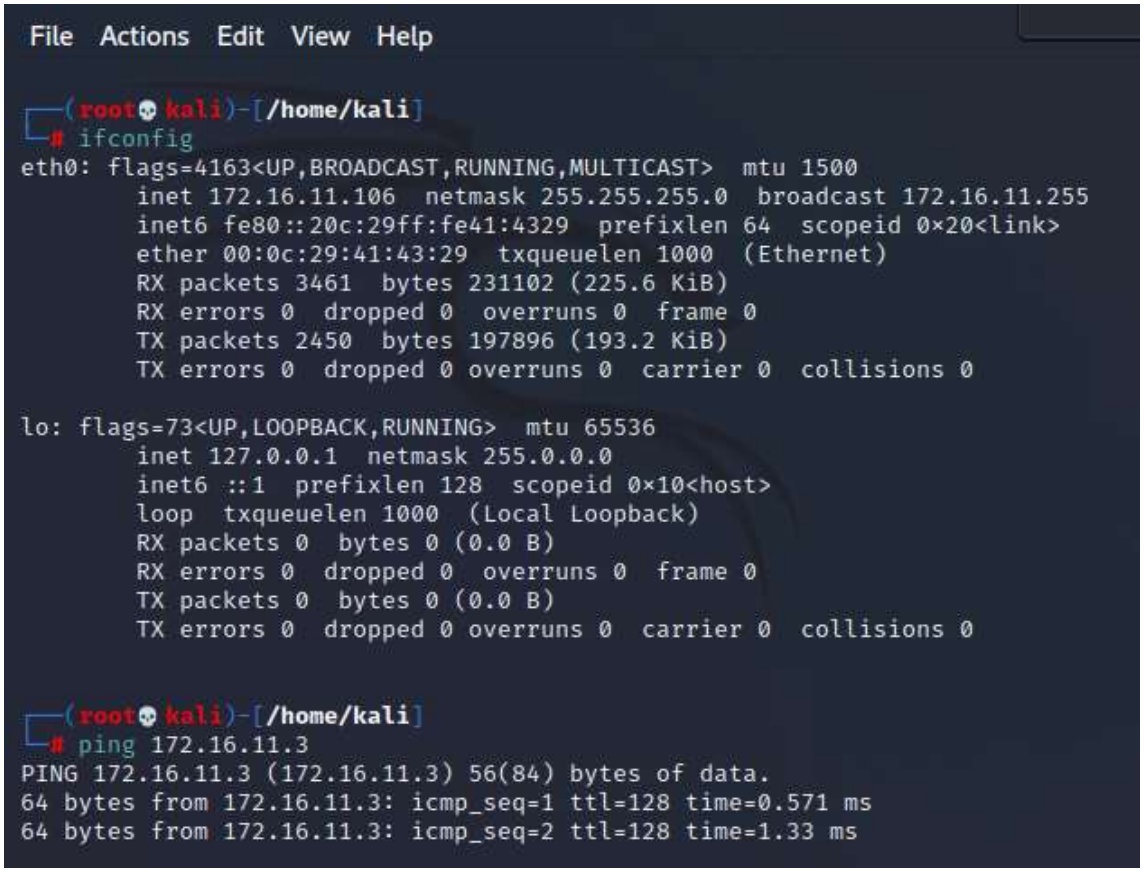
Figura 3.1 Comando para generar peticiones de denegación de servicio

```
hping3 --rand-source --p 80 -S --flood 172.16.11.3
```

Fuente: Elaboración propia

Antes de realizar el ataque se verifica que el atacante tenga comunicación al servidor DNS, como se muestra en la figura 3.2

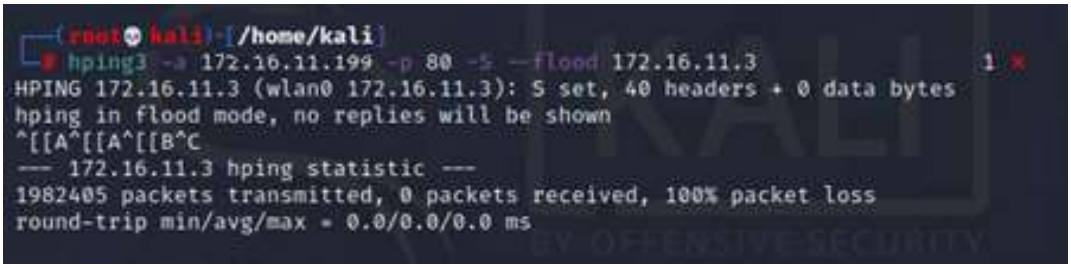
Figura 3.2 Prueba de conectividad al servidor DNS



Fuente: Elaboración propia

Una vez realizado la prueba de conectividad se procede con el ataque mediante el comando mencionado anteriormente, como se muestra en la figura 3.3

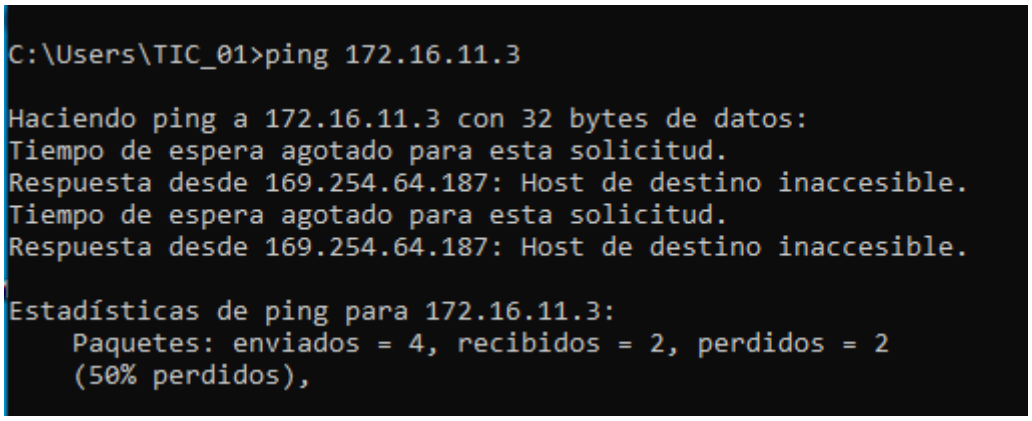
Figura 3.3 Emulador de terminal denegación de servicio



Fuente: Elaboración propia

En la figura 3.4 se aprecia que el servidor DNS atacado, denegó totalmente el servicio a Internet por causa de la saturación de los recursos (CPU, RAM, entre otros).

Figura 3.4 Verificación denegación de servicio



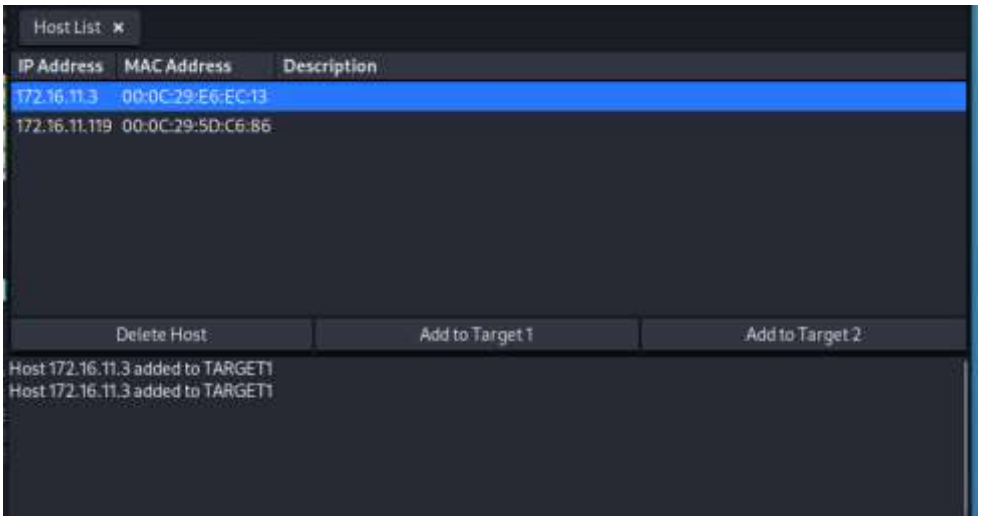
Fuente: Elaboración propia

Implementación de ataque envenenamiento de caché DNS.

Un ataque de envenenamiento de caché del servidor de DNS se produce si un código malicioso vulnera la tabla de nombres de dominio y se ingresan registros fraudulentos. Mediante el envío de peticiones DNS y una inundación de respuestas por parte del atacante, remite a los usuarios legítimos a sitios controlados por el atacante.

Para realizar esta prueba se utiliza la herramienta denominada Ettercap, el cual detecta los hosts de nuestra red como se muestra en la figura 3.5

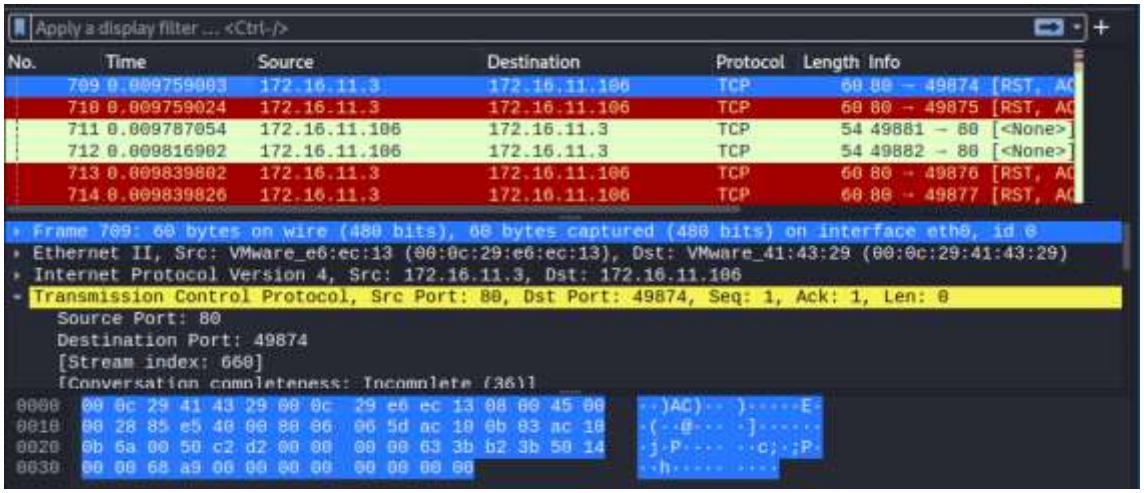
Figura 3.5 Host detectados por Ettercap



Fuente: Elaboración propia

Una vez iniciado el ataque de MITM gracias a la herramienta Wireshark se aprecia la duplicidad del direccionamiento, además, se observa como la caché se almacena en el direccionamiento de la víctima.

Figura 3.6 Análisis envenenamiento Caché



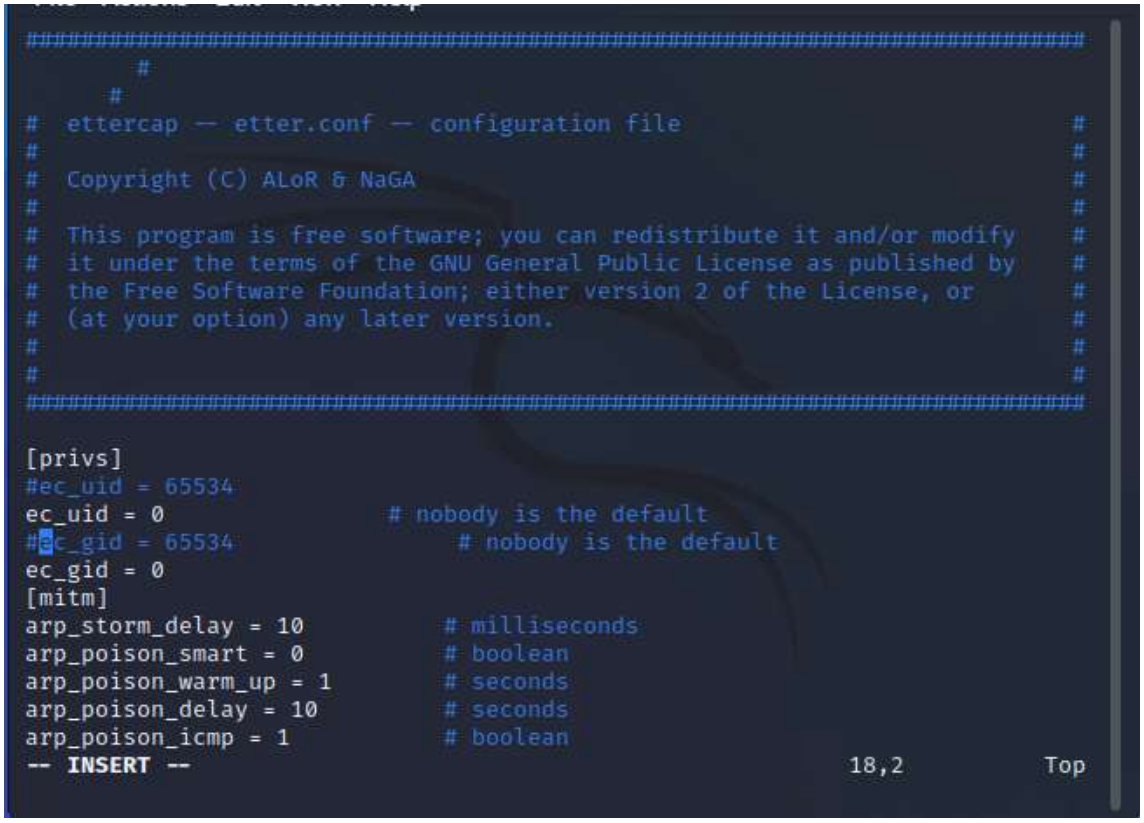
Fuente: Elaboración propia

Implementación de ataque DNS Spoofing.

El ataque de DNS Spoofing, es un extra del envenenamiento ARP redirige el tráfico por el equipo atacante, para lo cual en este escenario se necesita un computador con Kali Linux versión 2021.1 como atacante, una máquina cliente con el sistema Operativo Windows 10 cliente, y un equipo servidor DNS con Windows Server 2019 como la víctima.

La configuración del ataque se basa en dos partes, la primera es editar el archivo ettercap.conf como se muestra en la figura 3.7

Figura 3.7 Configuración archivo ettercap.conf

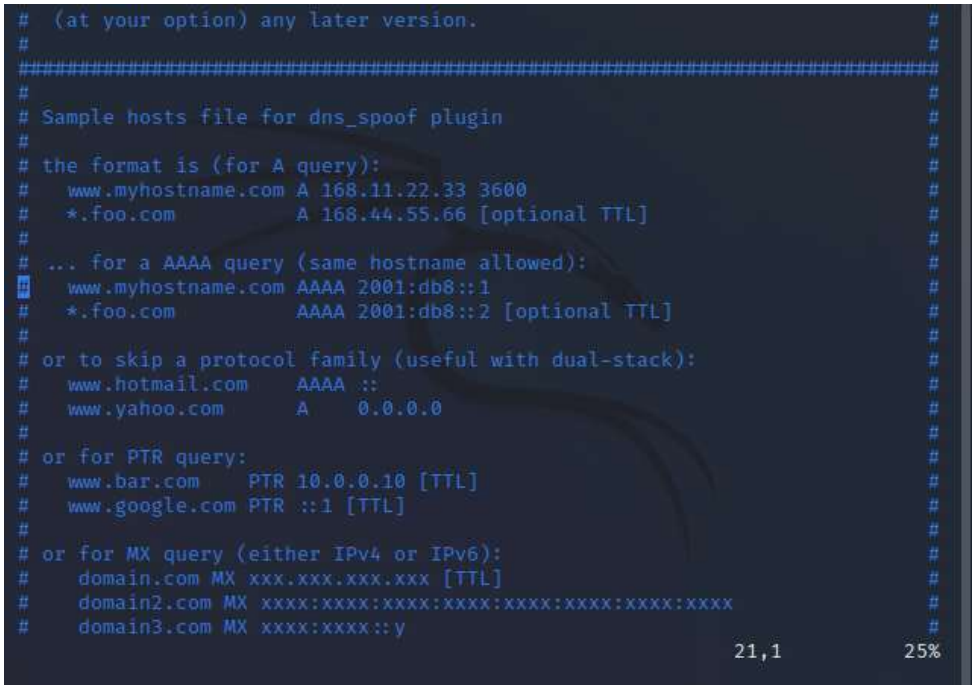


Fuente: Elaboración propia

Los servidores DNS permiten la resolución de nombres en direcciones IP, muchos de los atacantes se benefician de este nodo, dentro de la ruta de comunicación si se consulta a un sitio web, alteran las direcciones IP de los servidores DNS.

Previamente se ingresa al simulador de Terminal como usuario root, y y ubicarse en la carpeta *./etc/ettercap*, luego configurar el archivo *etter.dns* con el comando ./nano etter.dns. Una vez que se ha ingresado al archivo se configura la dirección IP del atacante como se observa en la figura 3.8

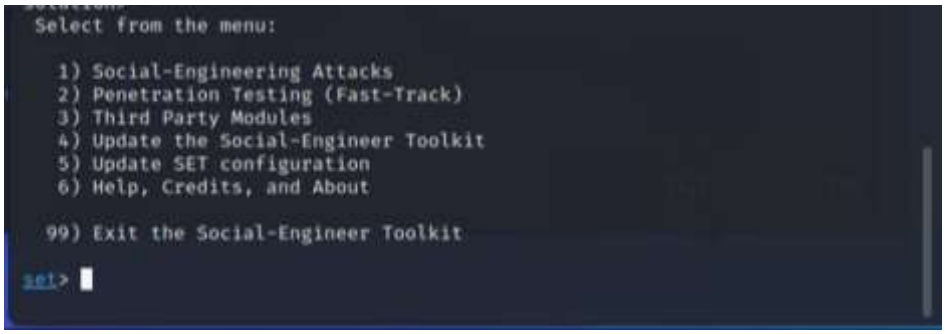
Figura 3.8 Emulador de terminal configuración de archivo etter.dns



Fuente: Elaboración propia

Luego, ejecutamos nuevamente el comando de la figura 3.1 para envenenar la caché y pasar al proceso de suplantación de una dirección IP, seguido ingresamos en otra ventana el comando ***setoolkit***, para ingresar al menú de configuración de la suplantación de una dirección electrónica y que ésta sea monitoreada por el atacante.

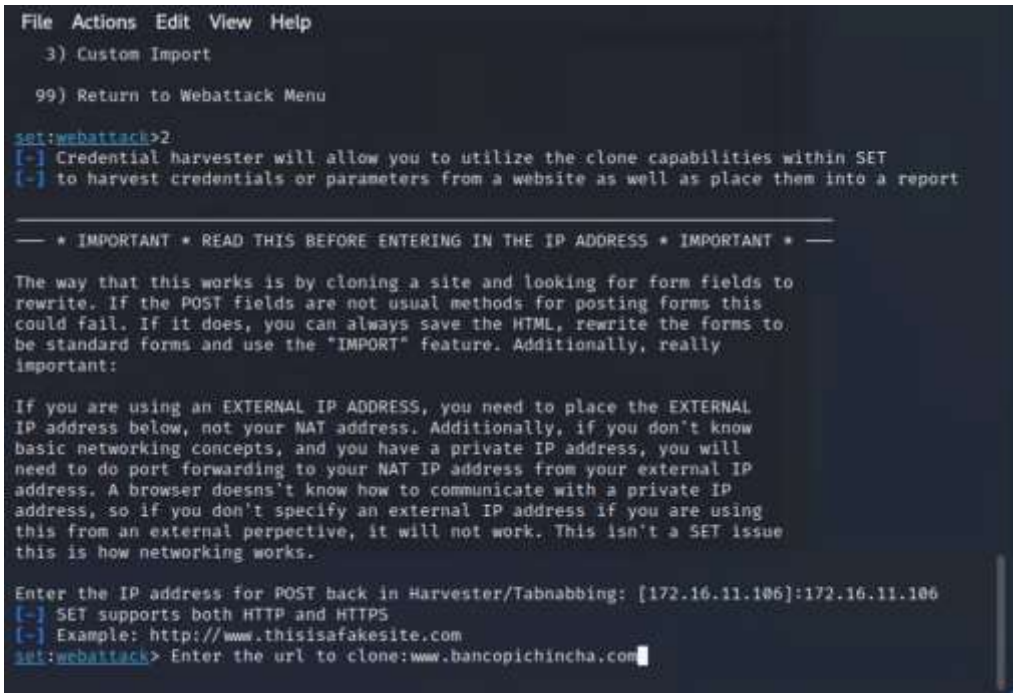
Figura 3.9 Emulador de terminal configuración setoolkit-menú



Fuente: Elaboración propia

En el menú de la figura 3.9, seleccionamos la opción 1-> ataques de ingeniería social y seguidamente la opción 2->ataques a los vectores de sitios web, luego escogemos la opción 3-> método de ataque1 de recolección de credenciales, después seleccionamos la opción 2->Clonador de Sitios y en el terminal aparece la pantalla de la figura 3.10.

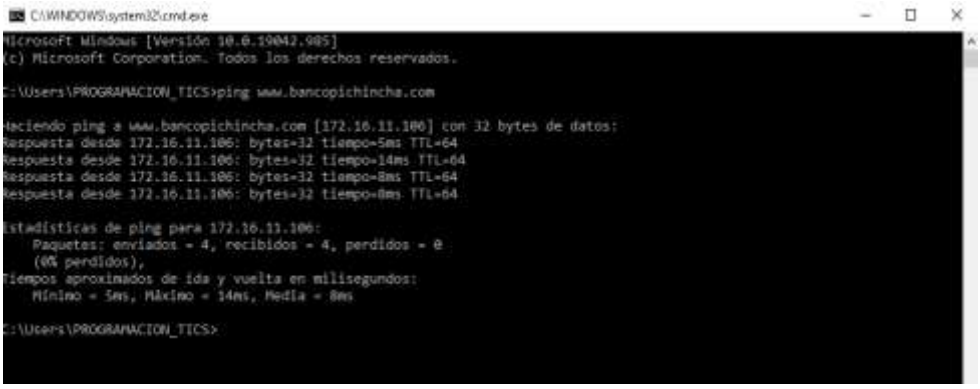
Figura 3.10 Emulador de terminal setoolkit en ejecución



Fuente: Elaboración propia

Finalmente, en la figura 3.11, se realiza una prueba desde el computador del cliente y se observa que al hacer ping a la dirección clonada www.bancopichincha.com, la respuesta se obtiene desde la IP del atacante 172.16.11.106, esto se lo configura en el archivo *etter.dns*, con el comando *nano*.

Figura 3.11 Verificación inundación de caché con un registro falso

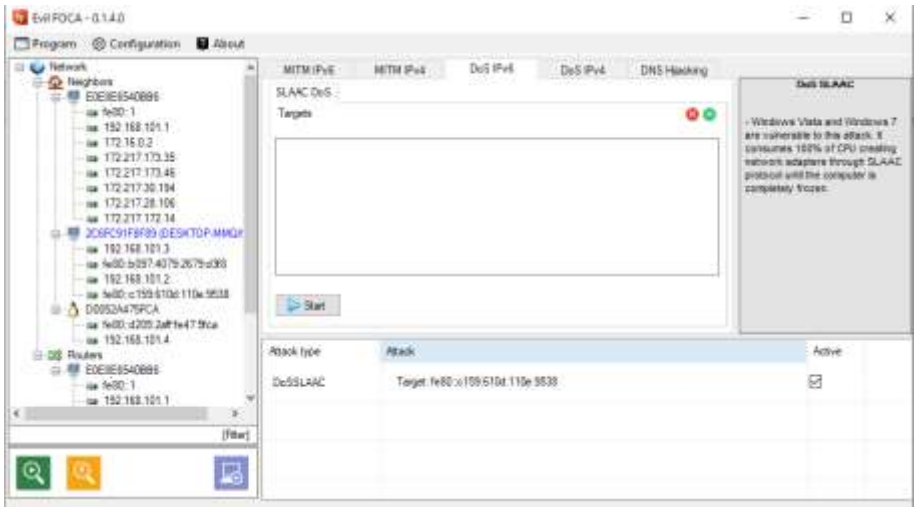


Fuente: Elaboración propia

Implementación de ataque denegación de servicio IPV6

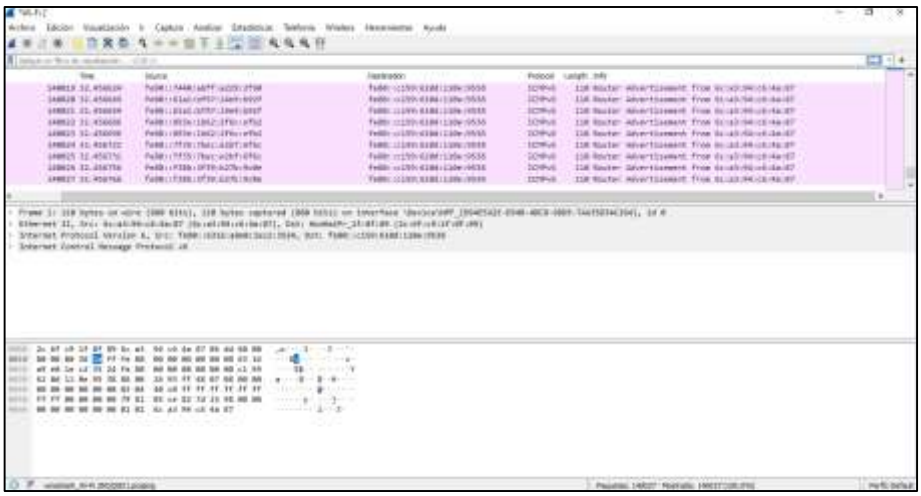
Un ataque de denegación de servicio conocido, también, como ataque DoS, afecta directamente a un recurso informático y que a la vez no esté disponible para los usuarios previstos, afecta una red o un servidor con solicitudes o datos, el atacante inunda los recursos como CPU, memoria RAM, entre otros de un equipo servidor mediante el envío masivo de peticiones. Para la simulación de ataques en redes IPV6 se utiliza la herramienta informática EvilFOCA, en la figura 3.12 se muestra la pantalla principal de la aplicación.

Figura 3.12 Aplicación EvilFOCA (Ataque DoS IPV6)



Fuente: Elaboración propia

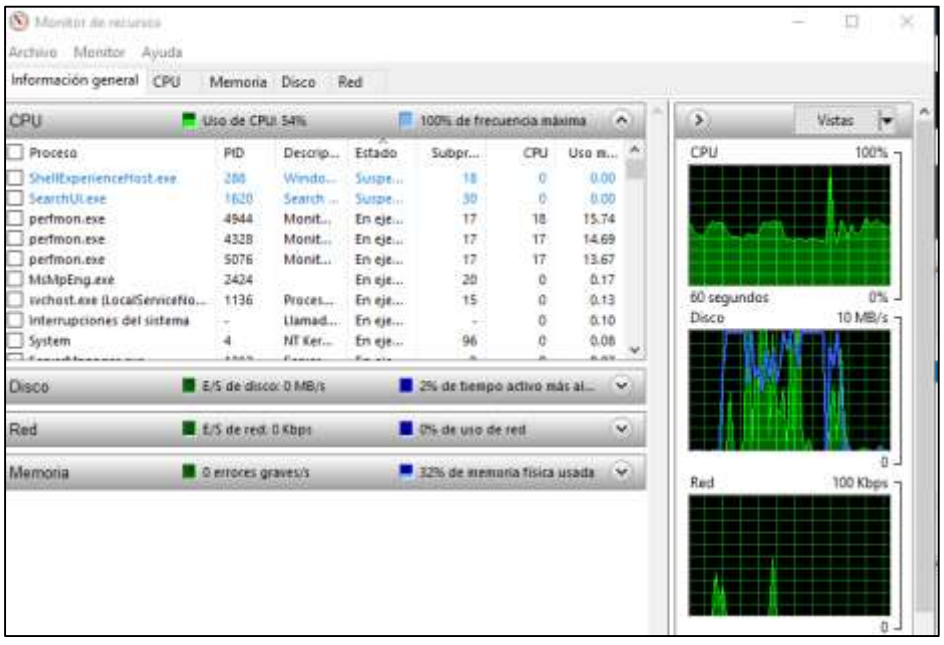
Figura 3.13 Captura de paquetes IPV6



Fuente: Elaboración propia

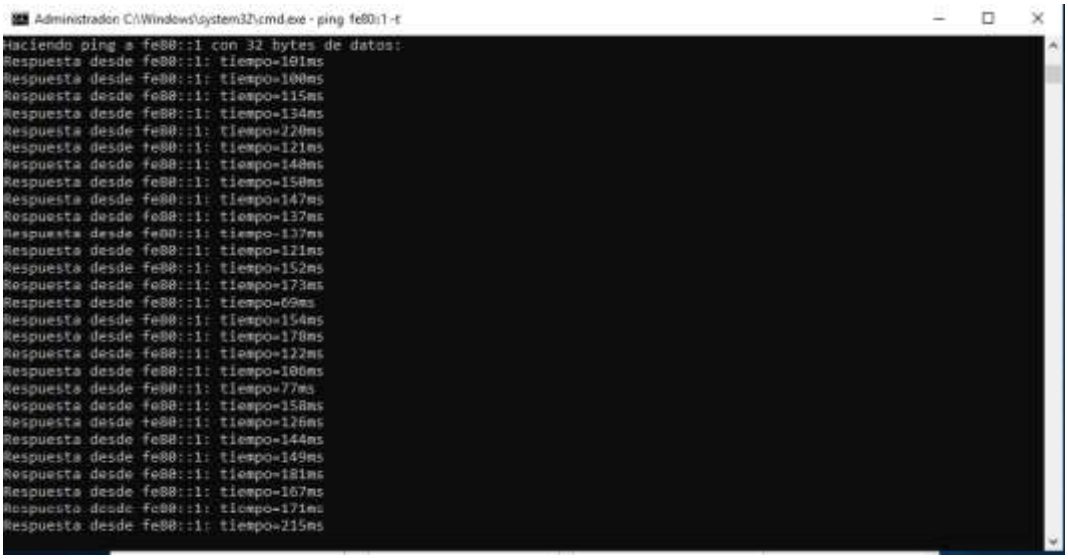
En la figura 3.14 se visualiza que los paquetes enviados cada vez cambian de origen para evitar ser detectados y el destino de ataque es el mismo *fe80::c159:610d:110e:9538* que es la dirección IPv6 del equipo víctima, de esta manera aumenta el uso de los recursos como (CPU, RAM, entre otros), en el equipo víctima como se muestra en la figura 2.17.

Figura 3.14 Verificación consumo de recursos con ataques IPV6



Fuente: Elaboración propia

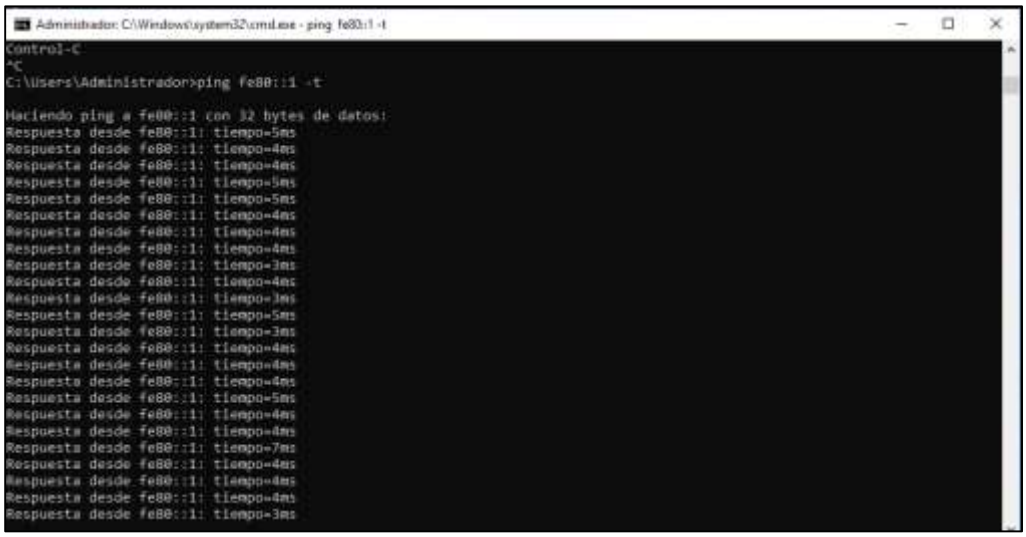
Figura 3.15 Verificación en la consola de Windows con ataque DNS IPV6



Fuente: Elaboración propia

En la figura 3.16 se observa que se realizan peticiones de ping desde el equipo servidor víctima a la dirección IPV6 fe80::1, que es la del servidor DNS principal de salida a Internet, obteniéndose una respuesta en tiempos promedio de 150ms, que es un valor alto para equipos que se encuentran a un solo salto, y al detener el ataque, los tiempos bajan considerablemente a un promedio de 4ms como se observa en la figura 2.19.

Figura 3.17 Consola de Windows sin ataques DNS IPV6



Fuente: Elaboración propia

3.2. Análisis de mecanismos de seguridad ante ataques DNS

Mecanismo seguridad ante ataque denegación de servicio

Uno de los mecanismos de seguridad ante este tipo de ataques es la utilización de equipos totalmente actualizados de preferencia administrables como routers y firewalls. Los cuales permitan generar listas de control de acceso (ACL) para hacer un seguimiento del acceso en función de las IP solicitantes. Prever con un ancho de banda considerable, de preferencia mucho mayor a la capacidad requerida, con el fin de evitar saturación de la red. Además, la utilización de CDN (red de distribución de contenidos) ayuda a minimizar los retrasos de carga de contenidos, a la vez a reducir el riesgo de colapso en caso de ataques por denegación de servicio.

Uno de los mecanismos a nivel de software es la utilización de logs que son registros que se generan de manera automática y se guardan en el servidor. Los logs guardan toda la información generada que depende del tipo de servidor, permite detallar la hora y criticidad de eventos relacionados a consultas, configuración, entre otras; y en el caso de existir un ataque de denegación de servicio, los logs servirán para identificar el origen y tomar medidas correctivas como la restricción del servicio.

Con la utilización de los firewalls, se restringe, filtra o se limita el tráfico en base a un conjunto de normas o reglas. De este modo el servidor DNS limita o bloquear el tráfico que ingresa por el puerto UDP 53, y en caso de un ataque de denegación de servicio con un excesivo número de peticiones DNS, éstas sean rechazadas.

Mecanismo de seguridad ante el envenenamiento de caché DNS

La manera de evitar que un servidor recursivo no sea víctima de un ataque de envenenamiento de caché es que rechace la mayor parte de las respuestas del atacante. La aleatoriedad del puerto es una solución muy efectiva, genera de forma aleatoria el puerto de origen con el cual el servidor DNS realiza las consultas a los

servidores de mayor jerarquía. Hay que tener presente que el ID y puerto coincide con los de la consulta.

La probabilidad de ataque es casi nula, se tiene 2^{11} combinaciones de números de puertos y 2^{12} combinaciones de ID, con ello la probabilidad de que el servidor DNS acepte una respuesta del atacante es casi nula, esto se configura en el archivo ***/etc/named.conf*** del servidor DNS en Linux.

Mecanismo de seguridad ante el ataque DNS Spoofing

Los ataques DNS Spoofing son una variedad del envenenamiento caché por ello el primer punto a considerarse es la aleatoriedad del puerto, genera de forma aleatoria el puerto de origen con el cual el servidor DNS realiza las consultas a los servidores de mayor jerarquía, minimiza considerablemente el ataque.

Adicional en este tipo de ataques hay que tener presente que la suplantación de un sitio web, dirección IP, o incluso la suplantación de un correo, conlleva un aspecto visual un poco o muy distinto a la página original, por ello hay que ser muy precavidos si utilicemos un sitio web revisa la dirección electrónica o url sea la correcta y que no se redirija a enlaces distintos, para el caso de los correos electrónicos, intentarán sacarnos contraseñas o datos personales, y como una opción muy efectiva se suele activar el protocolo SPF (Sender Policy Framework).

Para la evaluación de los mecanismos de seguridad de DNS, se realizarán simulaciones tanto en redes IPV4 como en IPV6, se analizarán los resultados obtenidos y se compararán con los mecanismos de seguridad descritos en el presente capítulo, determina el método más efectivo de conformidad a los resultados alcanzados.

3.3. Análisis de amenazas y vulnerabilidades

Análisis de amenazas y vulnerabilidades en redes IPV4

Para el análisis de los ataques DNS IPV4 se toma en consideración un escenario de ámbito general, y mediante herramientas de software libre para el ataque se utiliza un equipo con Kali Linux, un servidor víctima con Windows Server 2019 R2 y un computador con Windows 10 como cliente; y, mediante la metodología diamante se clasifican los ataques como se muestra en la Figura 3.18.

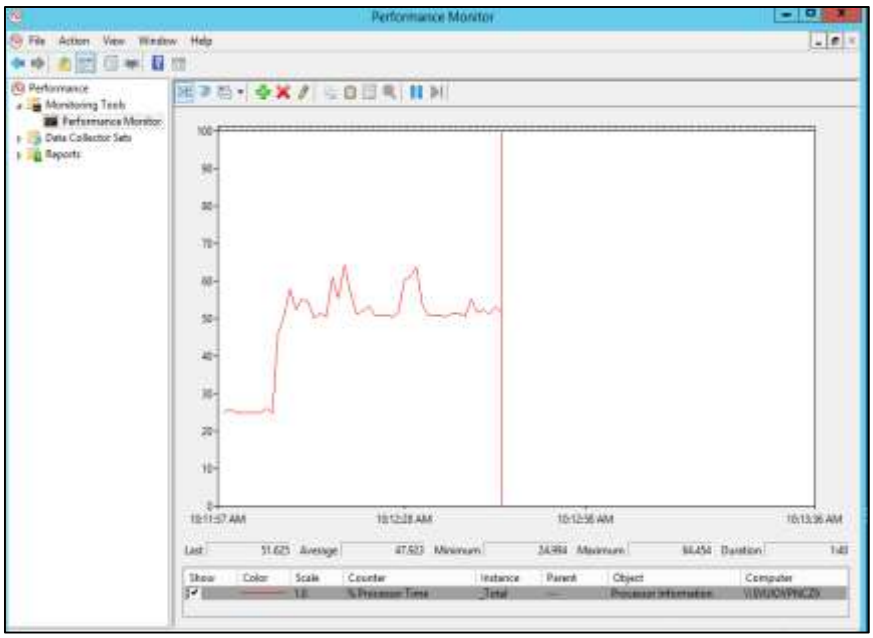
Figura 3.18 Análisis de amenazas

Amenaza	Descripcion de la amenaza	Calificación	Color
Denegación de servicio	El equipo servidor víctima DNS tiene configuraciones básicas de DNS y no se realizan análisis de eventos	INMINENTE	
Envenenamiento caché DNS	EL equipo servidor víctima no tiene una capacidad suficiente de memoria RAM y no tiene una configuración para minimizar el envenenamiento caché DNS	INMINENTE	
Ataque DNS spoofing	EL equipo servidor DNS victima no tiene un método para limitar el ataque spoofing	INMINENTE	

Fuente: Elaboración propia

Para el análisis de amenazas en IPV4, se considera de manera general los ataques con los comandos ***hping3 y ettercap*** para la generación de ataques de denegación de servicio, suplantación de direcciones IP y envenenamiento caché, para ello monitoreamos el tiempo de procesador; en la figura 3.19, se observa que en el instante del ataque, el consumo de recursos del servidor víctima aumenta de manera inmediata, bloquea totalmente todos los servicios, permite al computador atacante con Kali Linux realizar su objetivo.

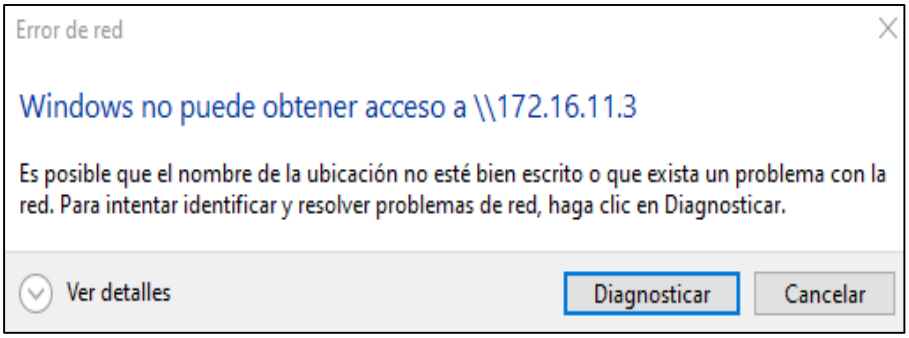
Figura 3.19 Monitor del procesador en el tiempo real de ataque



Fuente: Elaboración propia

En la figura 3.20, se observa que el servicio de carpetas compartidas se ha denegado totalmente, impide acceder a los recursos del equipo servidor víctima con Windows Server 2019 R2

Figura 3.20 Denegación del servicio de carpetas compartidas

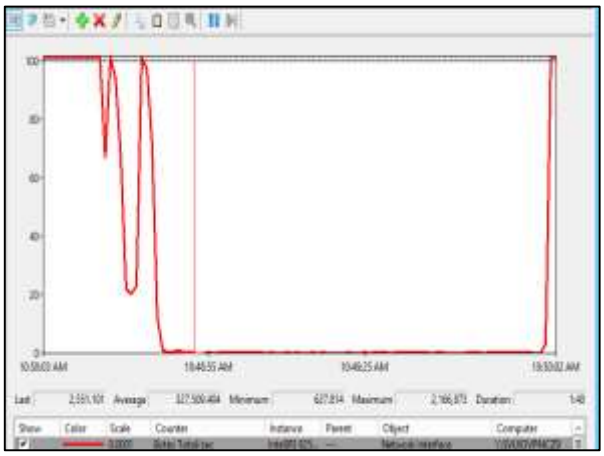


Fuente: Elaboración propia

En la figura 3.21 se observa que se ha monitorizado los recursos de la interface de Red, en el cual en un intervalo aproximado de 5 segundos se realizan los ataques al servidor víctima con Windows Server 2019 R2 y el consumo del recurso de la red se eleva considerablemente, y al detener los ataques, en teoría en ese instante,

también, baja el consumo de la red, sin embargo en la práctica de laboratorio como se muestra en la figura 3.4 se verifica que después de detener el ataque, existe aún una variación en el consumo de la red aproximadamente entre 10 a 20 segundos después de detener el ataque.

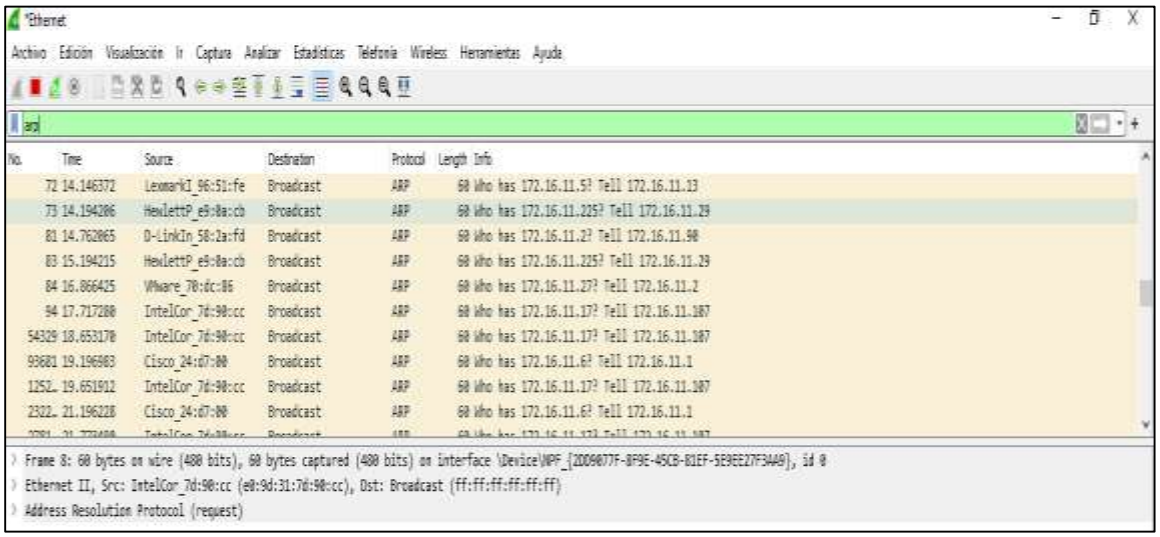
Figura 3.22 Monitor de recursos de Red en ataque DNS



Fuente: Elaboración propia

En la figura 3.23 con la herramienta informática Wireshark, se muestra que en el instante del ataque de apenas 90 tramas que se han transmitido con el protocolo ARP, inmediatamente sube a 54329 tramas a la vez con direcciones IP distintas.

Figura 3.23 Captura de paquetes con Wireshark



Fuente: Elaboración propia

3.2.2. Análisis en redes IPV6

Para el análisis de los ataques DNS IPV6 para el ataque se utiliza un equipo con EvilFOCA, un servidor víctima con Windows Server 2019 y un computador con Windows 10 como cliente; y, mediante la metodología diamante se clasifican los ataques como se muestra en la Figura 3.24.

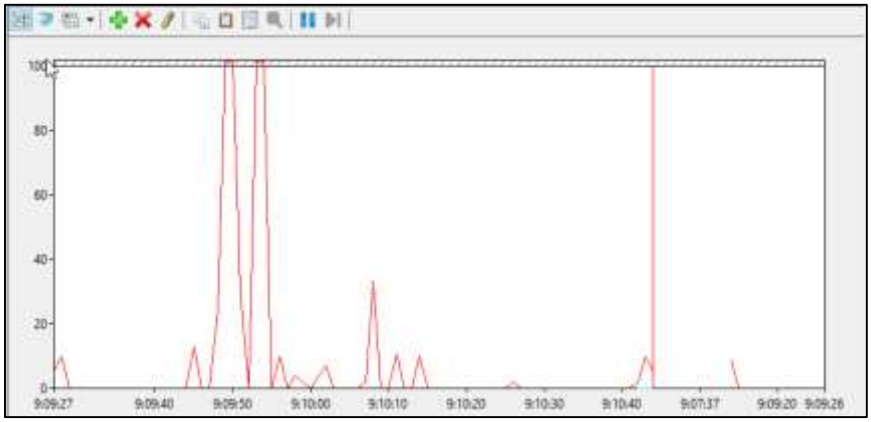
Figura 3.24 Análisis de amenazas IPV6

Vulnerabilidad	Descripcion de la amenaza	Calificación	Color
Denegación de servicio	Saturación total de los recursos informáticos	PROBABLE	

Fuente: Elaboración propia

Para el análisis de amenazas en IPV6, se utiliza la herramienta informática EvilFOCA para la generación de ataques de denegación de servicio, en la figura 3.25, se observa que, en el instante del ataque, el consumo de recursos del servidor víctima aumenta de manera inmediata, permite al computador atacante realizar su objetivo.

Figura 3.25 Monitor del procesador en el tiempo real de ataque en IPV6



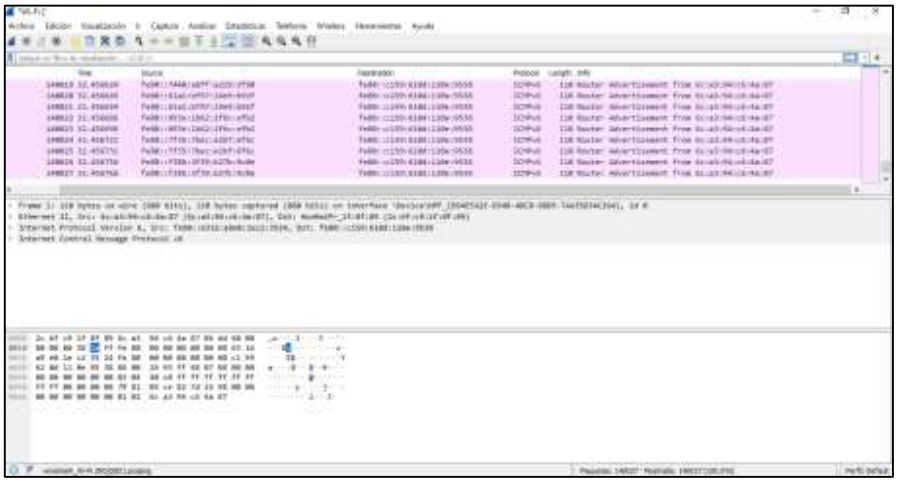
Fuente: Elaboración propia

En la figura 3.25, se observa que el uso de los recursos se eleva considerablemente en un tiempo aproximado de 5 segundos y luego se estabiliza nuevamente el

equipo servidor víctima tiene un procesador de alta capacidad, el escenario cambiaría si se realizara con un procesador de baja capacidad.

En la figura 3.27 se observa la captura de los paquetes con la herramienta informática Wireshark.

Figura 3.27 Captura de paquetes con Wireshark

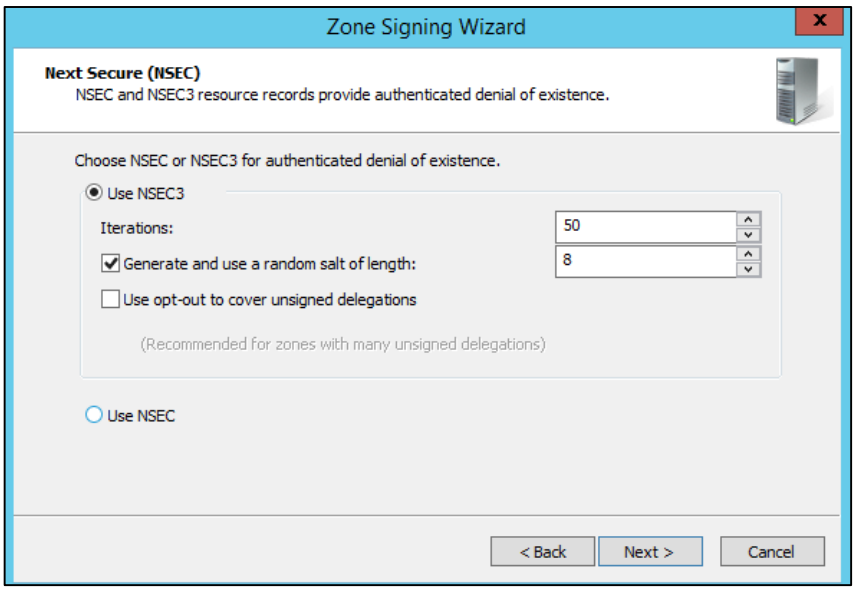


Fuente: Elaboración propia

3.4. Análisis de seguridades DNS

Para las pruebas de laboratorio se implementaron las herramientas DNSsec, y la configuración de la calidad de servicio QoS con la limitación del ancho de banda y por último se instaló un antivirus con licencia original con características de protección de red. En la figura 3.28 se muestra la configuración del servicio de DNSsec en Windows Server 2019 en la que incluso se configura el número de interacciones permitidas, en DNSsec se crean llaves de seguridad permite la integridad y seguridad de un mensaje.

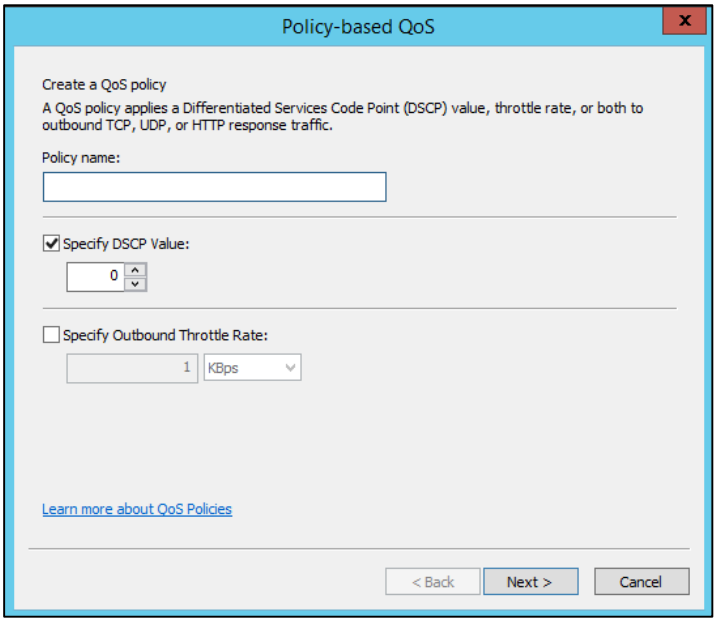
Figura 3.28 Configuración de DNSsec



Fuente: Elaboración propia

En la figura 3.29 se muestra la pantalla principal de la creación de las políticas basadas en la calidad del servicio QoS, en la que se especifica el ancho de banda, esto se aplica mediante políticas de grupo a todos los usuarios del dominio.

Figura 3.29 Políticas de QoS



Fuente: Elaboración propia

En la figura 3.30 se ha utilizado el antivirus ESET NOD32 con licenciamiento original para simular las veces de un firewall y seguridades de red mediante la aplicación de reglas de filtrado, y se observa que está actua ante la duplicación de direcciones IP.

Figura 3.30 Bloqueo a suplantación de IP

Fuente: Elaboración propia

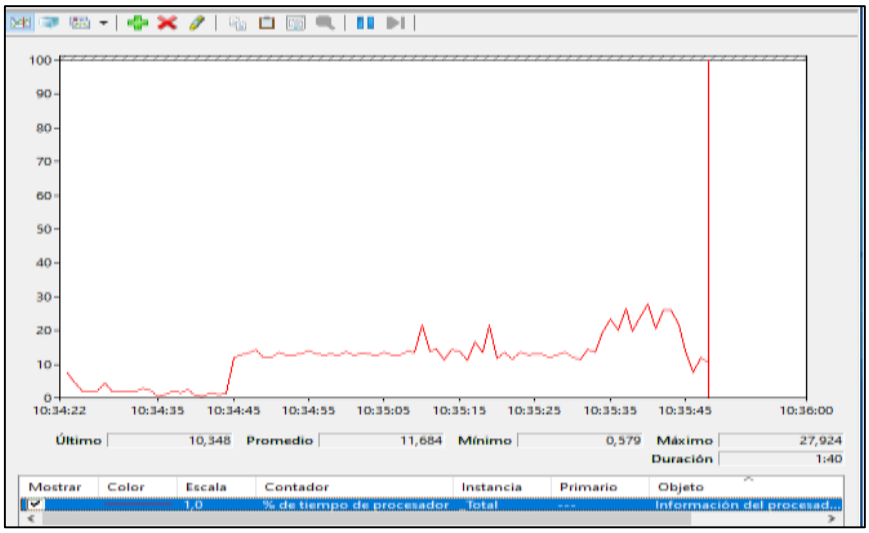
Figura 3.31 Bloqueo a amenazas envenenamiento caché

Fuente: Elaboración propia

En la figura 3.32, continua con el análisis se observa que el antivirus mediante la configuración de reglas en el firewall interno ha bloqueado el envenenamiento caché mediante el protocolo ARP.

Una vez implementadas las configuraciones de seguridad DNSSEC, Calidad de Servicio QoS, y el antivirus configurado manera de Firewall con reglas y seguridades de red, en la figura 3.19 se verifica que el consumo de los recursos disminuye en gran parte e intenta estabilizarse, es decir se ha logrado minimizar considerablemente la vulnerabilidad.

Figura 3.33 Monitor de recursos con seguridades implementadas en el servidor víctima



Fuente: Elaboración propia

En la figura 3.34 se observa que se accede a los servicios del servidor víctima con Windows Server 2019 R2, como carpetas compartidas y sistemas que se administran en el servidor, aunque con un pequeño tiempo de demora en la conexión, esto quiere decir que se ha minimizado considerablemente el riesgo y que al momento no se ha logrado bloquear al 100% los ataques, pero si se han disminuido en un gran porcentaje.

Figura 3.1 Acceso a carpetas compartidas

Fuente: Elaboración propia

3.5. Evaluación de Mecanismos de seguridad

En la figura 3.35, se muestra un resumen de la calificación de las amenazas analizadas en el laboratorio, aún sin la implementación de seguridades DNS.

Figura 3.35 Calificación de amenazas antes de la implementación de seguridades de laboratorio.

Amenaza	Descripcion de la amenaza	Mecanismo se seguridad implementado	Calificación de ocurrencia	Color
Denegación de servicio	El equipo servidor víctima DNS tiene configuraciones básicas de DNS y no se realizan análisis de eventos	Ninguno	INMINENTE	
Envenenamiento caché DNS	EL equipo servidor víctima no tiene una capacidad suficiente de memoria RAM y no tiene una configuración para minimizar el envenenamiento caché DNS	Ninguno	INMINENTE	
Ataque DNS spoofing	EL equipo servidor DNS victima no tiene un método para limitar el ataque spoofing	Ninguno	INMINENTE	

Fuente: Elaboración propia

Como se observa en la figura 3.35, se analizan tres amenazas, la denegación de servicio, envenenamiento caché DNS y Ataque Spoofing, y se califican como INMINENTE, esto quiere decir que existe una probabilidad muy alta de ocurrencia, de acuerdo a los escenarios de ataques, el servidor víctima fue afectado en todos los casos, bloquea totalmente los servicios, inunda la caché, y suplanta las direcciones IP.

En la figura 3.36 se muestran los resultados después de la implementación de los mecanismos de seguridad DNS, la denegación de servicio se califica como PROBABLE, esto quiere decir que existen razones y argumentos que sucederá, en el escenario se accede a los servicios pero con ciertos tiempos de demora en la conexión, y en lo referente al envenenamiento caché DNS y Ataque DNS Spoofing, se califica como POSIBLE, quiere decir que no se descarta la ocurrencia de que suceda o afecte al equipo servidor victima en el escenario de seguridades del epígrafe *3.1 Análisis de seguridades DNS*, se verifica que se ha bloqueado este tipo de ataques, sin embargo el equipo atacante sigue genera peticiones al servidor DNS víctima; y con la actualización y evolución de la tecnología es probable que este tipo de mecanismo de seguridad deje de ser fiable.

Figura 3.36 Evaluación Amenazas después de la implementación de seguridades en laboratorio IPv4

Amenaza	Descripcion de la amenaza	Mecanismo de seguridad implementado	Calificación de Ocurrencia	Color
Denegación de servicio	El equipo servidor víctima DNS tiene configuraciones básicas de DNS y no se realizan análisis de eventos	Implementación de DNSSEC con la configuración de llaves Configuración de QoS Configuración de Reglas en Antivirus	PROBABLE	
Envenenamiento caché DNS	EL equipo servidor víctima no tiene una capacidad suficiente de memoria RAM y no tiene una configuración para minimizar el envenenamiento caché DNS	Implementación de DNSSEC con la configuración de llaves Configuración de QoS Configuración de Reglas en Antivirus	POSIBLE	
Ataque DNS spoofing	EL equipo servidor DNS victima no tiene un método para limitar el ataque spoofing	Implementación de DNSSEC con la configuración de llaves Configuración de QoS Configuración de Reglas en Antivirus	POSIBLE	

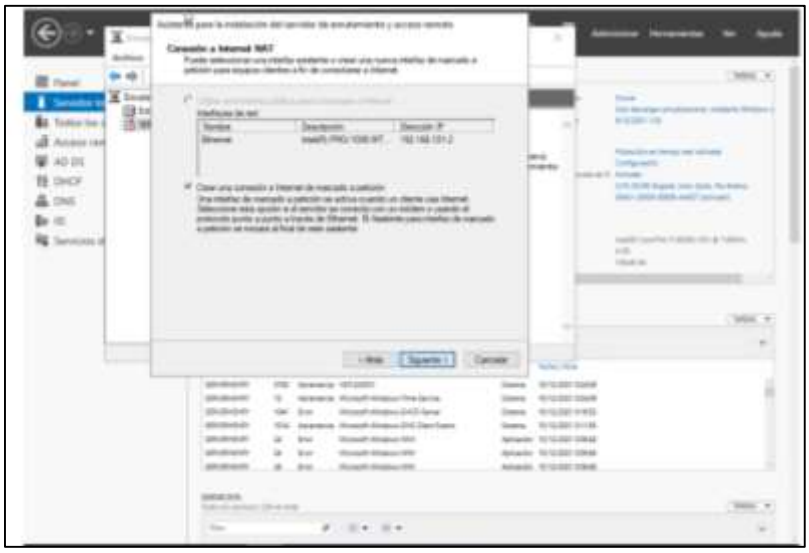
Fuente: Elaboración propia

Configuración de reglas de navegación en Firewall Server 2019

Para el escenario de análisis de seguridades ante ataques DoS se realizó la configuración de enrutamiento y acceso mediante reglas de navegación, para lo cual se instaló la herramienta informática (Enrutamiento y Acceso Remoto) en un equipo con Windows Server 2019 y dos tarjetas de red, para el enlace a Internet y otra para el acceso LAN, y con la ayuda del aplicativo EvilFOCA y un cliente con Windows 10, se realizaron las pruebas de seguridades, en la figura 3.37, se observa

una parte de la configuración de Iptables NAT, misma que se configura en el menú administrador del servidor.

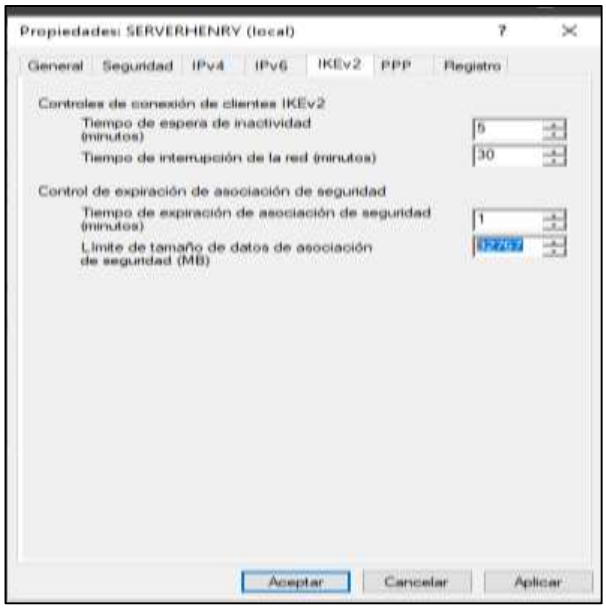
Figura 3.37 Configuración de reglas de navegación de Server 2019



Fuente: Elaboración propia

Para el bloqueo tanto en IPV4 como en IPV6 se configuró la herramienta informática *IKEv2* (Internet Key Exchange) protocolo de túneles que se basa en IPSec (Seguridad del Protocolo de Internet), actua en la capa de red.

Figura 3.38 Configuración de IKEv2



Fuente: Elaboración propia

En la figura 3.39 se ilustra la configuración de reglas en IPV6, en la que se ingresa el prefijo IPV6 y se define la tarjeta de red a ser utilizada.

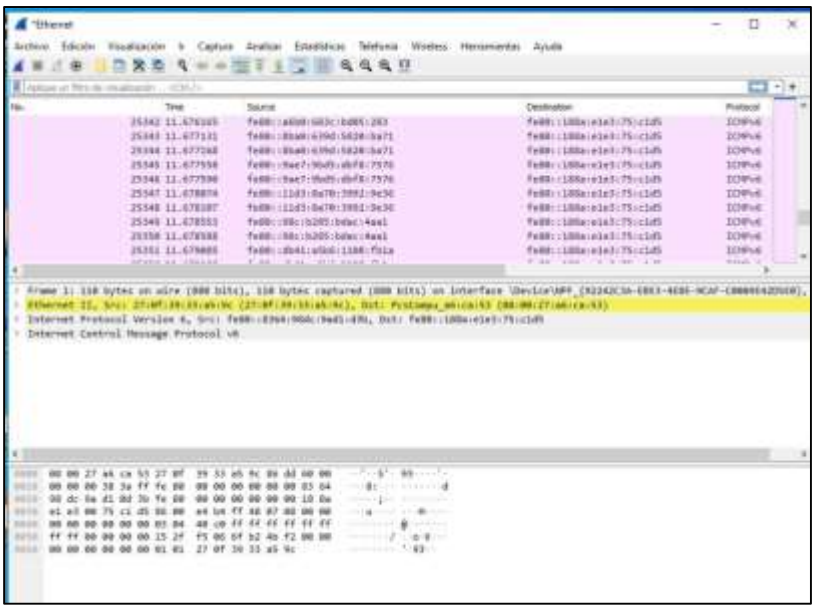
Figura 3.39 Configuración de reglas con IPV6

Fuente: Elaboración propia

En las pruebas de laboratorio se simularon tanto en IPV4 como en IPV6, y al momento de realizar un ataque ético a la computadora víctima, ésta se bloquea en el tiempo configurado conforme la figura 3.39.

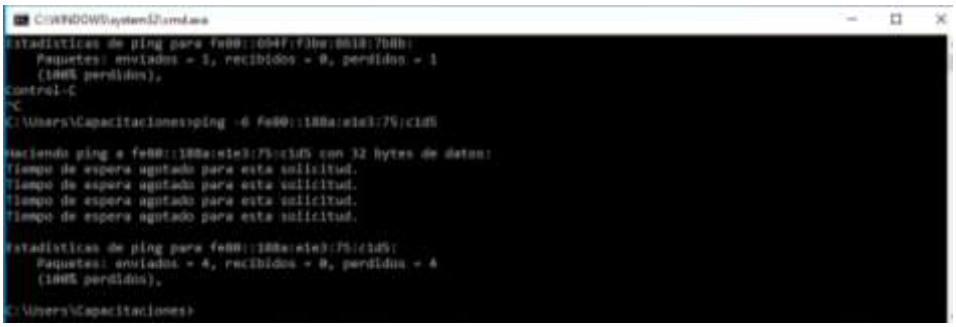
En la figura 3.40 se muestra la captura de los paquetes en el momento del ataque utiliza direcciones IPV6. Y en la figura 3.27 y 3.28 se muestra el resultado del bloqueo de la conexión generada por parte del equipo Windows server en base a la herramienta IPtables establecida.

Figura 3.40 Captura de paquetes IPV6



Fuente: Elaboración propia

Figura 3.41 Bloqueo a direccionamiento IPV6



Fuente: Elaboración propia

Figura 3.42 Bloqueo a direccionamiento IPV4

Fuente: Elaboración propia

Comparación

Para el proyecto de investigación adicional se tomó en consideración el estudio de varios autores evalua los mecanismos de seguridad en referencia a la simulación de laboratorio realizado.

Figura 3.43 Mecanismo de seguridad denegación de servicio Autor 1

Amenaza	Mecanismo de seguridad	Calificación de Ocurrencia	Color
Denegación de servicio	Uso de Balanceadores de Carga Uso de cortafuegos Modificación de los servidores web Reducir el tiempo syn-received Habilitar syn-cache Análisis de tráfico Antivirus	PROBABLE	

Fuente: Tomado a partir de CCN (2013)

En lo que respecta al mecanismo de seguridad de la figura 3.29, el cual plantea el citado, se lo ha calificado como PROBABLE, es decir que existen razones y argumentos de que suceda, por ejemplo un balanceador de carga lo que va hacer es distribuir los paquetes para que el servicio intente de alguna manera mantenerse, pero el ataque sigue presentándose y afecta a los servicios DNS, y en lo referente a la utilización del antivirus se crean reglas para que sea efectivo y al reducir los tiempos de syn-received, también, se corre el riesgo de impedir las

conexiones a usuarios legítimos. Con este análisis no se afirma que el mecanismo del Autor 1 sea inadecuado.

Figura 3.44 Mecanismo de seguridad denegación de servicio Autor 2

Amenaza	Mecanismo de seguridad	Calificación de Ocurrencia	Color
Denegación de servicio	Permitir la realización de consultas recursivas solo a un grupo específico de direcciones IP. Un Servidor DNS no tiene que permitir la recursión a nadie más que a los host estrictamente indispensables. consultar periódicamente reportes de seguridad. Mantener actualizado el software de servicios DNS.	PROBABLE	

Fuente: Tomado a partir de Sánchez (2012)

En la figura 3.45 se observa que el autor citado, plantea las recomendaciones de mecanismos de seguridad DNS de manera general, con el fin de mitigar riesgos de ser víctima ante la denegación de servicios, lo cual se lo califica como PROBABLE, existen razones y argumentos de que el ataque suceda, porque no especifica una herramienta de software o hardware para minimizar los riesgos ante ataques de denegación de servicios.

Figura 3.45 Mecanismo de seguridad envenenamiento caché Autor 1

Amenaza	Mecanismo de seguridad	Calificación de Ocurrencia	Color
Envenenamiento caché DNS	Aleatoriedad de ID de transacción y puerto de origen. Validación de respuestas y deteción. Limitar la recursión. Implementación de DNSSEC	PROBABLE	

Fuente: Tomado a partir de López Padilla (2014)

En la figura 3.45 se observa que los mecanismos de seguridad del autor citado ante el ataque envenenamiento caché DNS se califica como PROBALE, existen razones de que el ataque afecte a los servicios DNS, la herramienta DNSSEC es una medida de seguridad que mitiga el riesgo, ante lo cual es necesario de otras herramientas informáticas como firewalls.

Figura 3.46 Mecanismo de seguridad envenenamiento caché Autor 2

Amenaza	Mecanismo de seguridad	Calificación de Ocurrencia	Color
Envenenamiento caché DNS	Utilización de DNSSEC Utilización de cookie de DNS RFC 7873	PROBABLE	

Fuente: Tomado a partir de Lorenzo (2020)

En la figura 3.46 se observa que los mecanismos de seguridad del autor citado ante el ataque envenenamiento caché DNS se califica como PROBALE, existen razones de que el ataque afecte a los servicios DNS, la herramienta DNSSEC es una medida de seguridad que mitiga el riesgo y la cookie DNS RFC 7873 son mecanismos de seguridad de transacciones de DNS ligero que proporciona una protección limitada a los servicios DNS.

Figura 3.47 Mecanismo de seguridad ataque DNS Spoofing Autor 1

Amenaza	Mecanismo de seguridad	Calificación de Ocurrencia	Color
Ataque DNS spoofing	Filtrado de paquetes en el router: Registros se realicen a travéz de conexiones cifradas.	PROBABLE	

Fuente: Tomado a partir de IONOS (2020)

En la figura 3.47 se observa que los mecanismos de seguridad ante el ataque DNS Spoofing citado por el autor citado se califica como PROBALE, existen razones que el ataque afecte a los servicios DNS, la configuración del filtrado de paquetes reenvía o deniega los paquetes según las reglas de filtrado, eso conlleva a utilizar equipos de alta gama para tener una configuración óptima minimiza los riesgos a gran escala y en lo referente a los registros SSL, tiene cierta desventaja que por desconocimiento la mayor parte de empresas solo utilizan en los dominios principales o simplemente no los utilizan por temor a no ser encontrados en la web.

Figura 3.48 Mecanismo de seguridad ataque DNS Spoofing Autor 2

Amenaza	Mecanismo de seguridad	Calificación de Ocurrencia	Color
Ataque DNS spoofing	Configuración de ingress/egress flitering.	PROBABLE	

Fuente: Tomado a partir de CCN (2013)

En la figura 3.48 se observa que el mecanismo de seguridad planteado por el autor citado, ante el ataque DNS Spoofing, se califica como PROBABLE, existen razones que el ataque afecte a los servicios DNS, la configuración *Ingress filtering*, activa o desactiva el filtro de entrada de un puerto para asegurarse que una trama de datos es originalmente de la red solicitada; y si se requiere implementar en redes empresariales esto conlleva a implementar equipos de alta gama y altos costos que pocas empresas lo implementan y prefieren contratar los servicios externos para asegurar sus sitios web, además si se deniega el servicio al router, las reglas implementadas para Spoofing quedarían descartadas.

Figura 3.49 Resumen de evaluación de mecanismos obtenidos de la simulación de laboratorio IPV4 e IPV6

Amenaza	Descripción de la amenaza	Mecanismo de seguridad implementado	PORCENTAJE APROXIMADO DE REDUCCIÓN DE VULNERABILIDADES
Denegación de servicio	El equipo servidor víctima DNS tiene configuraciones básicas de DNS y no se realizan análisis de eventos	Configuración de Iptables Configuración de IKEv2, IPSec	98%
Envenenamiento caché DNS	EL equipo servidor víctima no tiene una configuración para minimizar el envenenamiento caché DNS	Configuración de Iptables Configuración de IKEv2 Configuración de Reglas en Antivirus	95%
Ataque DNS spoofing	EL equipo servidor DNS víctima no tiene un método para limitar el ataque spoofing	Implementación de DNSSEC con la configuración de llaves Configuración de QoS Configuración de Reglas en Antivirus	85%

Fuente: Elaboración propia

En la figura 3.49 se muestra un resumen del porcentaje aproximado de la reducción de las vulnerabilidades después de la implementación de las seguridades DNS en las simulaciones de laboratorio, determina que la propuesta implementada con las herramientas de laboratorio como la implementación de Iptables con el protocolo IKEv2, DNSSEC, políticas de QoS y la utilización de un antivirus con licenciamiento original configurado con reglas de firewall, es adecuada en ataques de denegación de servicios verificó que el equipo servidor configurado con dos tarjetas de red LAN y WAN, bloquea totalmente la computadora del atacante.

CONCLUSIONES

Se concluye:

- El análisis de las técnicas de seguridad de DNS en las redes con IPv4 e Ipv6, determinó que, dichas vulnerabilidades se presentan por malas configuraciones en la red, más que en el propio SO. Esto ayudó a mitigar las inseguridades ante ataques informáticos mediante dicho servicio, a la red de datos del Hospital General Latacunga.

- La comparación de los diversos mecanismos de seguridad DNS en la red de datos, permitió realizar pruebas que protejan los servicios tecnológicos del Hospital General Latacunga en los cuales se determinó que, DNSsec es un mecanismo muy confiable ante ataques de envenenamiento caché, uno de los vectores de ataques más utilizados por los ciberdelincuentes.

- El desarrollo de pruebas y mecanismos de seguridad en un ambiente simulado permitió mantener la operatividad tecnológica de la Institución, de igual forma, dichas pruebas realizadas no afectaron la información sensible del Hospital esto evita que, dicho establecimiento se vea afectado durante los estudios planteados.

- La comparativa realizada entre los diversos mecanismos de seguridad al protocolo DNS, evidenció como DNSsec brinda una capa de autenticidad al servicio, lo que permite disminuir el riesgo ante ataques de suplantación, o de interceptación de tráfico conocidos como Man in the Middle, esto permite obtener una comunicación más segura y confiable entre el cliente y servidor.

RECOMENDACIONES

De acuerdo con las evidencias encontradas en esta investigación de campo, se recomienda.

- Analizar las técnicas de seguridad de varias fuentes para determinar el mecanismo más efectivo y se reduce considerablemente el riesgo ante los ataques a los servicios DNS.

- Utilizar un mecanismo de seguridad acorde a las necesidades actuales en base al análisis de ataques a los servicios de DNS, para mantener un escenario totalmente actualizado y sistematizado en seguridades de DNS.

- Utilizar herramientas informáticas adecuadas para las simulaciones de ataques a los servicios de DNS de laboratorio, y se determina el método más adecuado de seguridad de DNS.

- Determinar un mecanismo de seguridad que sea el resultado de un análisis comparativo tanto de pruebas de laboratorio como el de análisis de diferentes fuentes para reducir en un gran porcentaje el riesgo a ataques y mejorar el servicio de DNS.

BILIOGRAFÍA

Baena, G. (2017). *Metodología de la Investigación (3ra ed.).* Recuperado el 19 de junio de 2021, de Metodología de la Investigación (3ra ed.): http://www.bib lioteca.cij.gob.m x/Archivos/Materiales_de_consulta/Drodas_de_Abuso/Articulos/metodologia%20de%20l a%20investigacion.pdf

Broy de la Cruz, H. (2013). *Instalación, Administración y Soporte de Redes.* Lima: MACRO empresa editora.

Cabezas, N. A. (2018). *Introducción a la metodología de la investigación científica (Primera ed.).* Sangolquí, Ecuador: Comisión Editorial de la Universidad de las Fuerzas Armadas ESPE.

Casas, J. R. (2003). *La encuesta como técnica de investigación.* Recuperado el 19 de junio de 2021, de La encuesta como técnica de investigación.: https ://core .ac.u k/do wnl oad /pdf /82245762.pdf

CCN, C. N. (junio de 2013). *Guía de seguridad de las TIC.* Recuperado el junio de 2021, de Guía de seguridad de las TIC: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/528-ccn-stic-820-proteccion-contra-denegacion-de-servicio/file.html

CISCO. (19 de mayo de 2021). *Direccionamiento de IP y conexión en subredes para los usuarios nuevos*. Obtenido de Direccionamiento de IP y conexión en subredes para los usuarios nuevos: Una máscara de red ayuda a saber qué parte de la dirección identifica la red y qué parte de la dirección identifica el nodo. Las redes de la clase A, B, y C tienen máscaras predeterminadas, también, conocidas como máscaras naturales, como se muestra aquí:

Dirección General del Servicio Civil. (octubre de 2018). *Guía Metodológica para el Diseño y Desarrollo de Investigaciones.* Recuperado el 11 de junio de 2021, de Guía Metodológica para el Diseño y Desarrollo de Investigaciones: http://w ww.dg sc.go.cr /docu mento s/desarrollo/Guia-Metodol%C3%B3gica-FINAL-nov-2018.pdf

GRUPO ATICO34. (16 de marzo de 2021). *Dirección IP Privada y Pública. Qué son y sus diferencias*. Obtenido de Dirección IP Privada y Pública. Qué son y sus diferencias: https://protecciond atos-lopd.com/empresas/direccion-ip-privada-publica/#Direccion_de_IP_privada_Que_es

Herrera, J. (27 de Abri de 2009). Las vulnerabilidades de seguridad DSN. *Las vulnerabilidades de seguridad DSN*.

HSESoft. (2021). *Metodología diamante para la identificación de amenazas.* Recuperado el 05 de junio de 2021, de Metodología diamante para la identificación de amenazas: https://hse.software/2020/11/09/metodologia-diamante-para-la-identificacion-de-amenazas/

ICTEA. (2021). *Base de conocimientos*. Recuperado el 24 de julio de 2021, de https://www.ictea.com/cs/index.php?rp=/knowledgebase/217/What-is-DNS-Domain-Name-System.html

INCIBE. (09 de julio de 2019). *Medidas de prevención contra ataques de denegación de servicio*. Obtenido de Medidas de prevención contra ataques de denegación de servicio: https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio

IONOS. (15 de mayo de 2020). *IP spoofing*. Recuperado el 2021, de IP spoofing: https://www.ionos.es/digitalguide/servidores/seguridad/ip-spoofing-fundamentos-y-contramedidas/

López Padilla, A. (2014). Guia de seguridad en servicios DNS. *INCIBE*, 73.

Lorenzo, J. A. (16 de noviembre de 2020). *Nuevo ataque de envenenamiento de la caché DNS*. Recuperado el junio de 2021, de Nuevo ataque de envenenamiento de la caché DNS: https://www.redeszone.net/noticias/seguridad/sad-dns-nuevo-metodo-envenenamiento-cache-dns/

Parreño, A. (2016). *Metodoligía de la Investigación en salud.* Recuperado el 19 de junio de 2021, de Metodoligía de la Investigación en salud: http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/pdf/13/metodolog%C3%ADa%20de%20la%20investigaci%C3%B3n%20en%20salud.pdf

Percy. (07 de diciembre de 2020). *Plan de direccionamiento IPv6 - Parte 1*. Obtenido de Plan de direccionamiento IPv6 - Parte 1: https://learningnetwork.cisco.com/s/article/plan-de-direccionamiento-ipv6-parte-1

Sánchez, E. (diciembre de 2012). *Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC).* Recuperado el 2021, de Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC): http://sedici. unlp.edu.ar/bit stream/ha ndle/1091 5/27062/Documento_completo.pdf?sequence=1&isAllowed=y

Sanchez, E. (Abril de 2017). Un estudio comparativo en Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNS). *Un estudio comparativo en Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNS)*. La PLata, Buenos Aires, Argentina.

Sepúlveda, M. (07 de junio de 2021). *Configuración de Servidores DNS y DHCP en Packet Tracer*. Obtenido de Configuración de Servidores DNS y DHCP en Packet Tracer: https://e classvirtual. com/configuracion-de-servidores-dns-y-dhcp-en-packet-tracer/

ANEXOS

Anexo 1. Formato de encuesta

Pontificia Universidad Católica del Ecuador | Sede Ambato

OFICINA DE INVESTIGACIÓN Y POSTGRADOS

Tema de Investigación: EVALUACIÓN DE LOS MECANISMOS SEGURIDAD DE DNS EN REDES IPV4 E IPV6

El siguiente cuestionario tiene el propósito de: Determinar el nivel de conocimiento sobre los ataques y mecanismos de seguridad de DNS en redes IPV4 e IPV6.

Esta investigación guardará la estricta confidencialidad y los resultados obtenidos serán utilizados exclusivamente con fines académicos científicos.

A.- Datos sociodemográficos del personal de TICs

1	Edad	
2	Género	
3	Ocupación	
4	Grado de Instrucción	
5	Profesión	
6	Años de experiencia en servicios DNS	
7	Tiempo de trabajo en la Institución actual	

Instrucciones: Señale con una X, donde crea conveniente y de acuerdo a la siguiente escala en cada uno de los 5 ítems propuestos:

B.- Conocimientos

Totalmente en desacuerdo 1	En desacuerdo 2	Ni de acuerdo ni desacuerdo 3	De acuerdo 4	Totalmente de acuerdo 5

Ítem	Descripción	1	2	3	4	5
1.	Los ataques informáticos a los servidores de DNS deniegan totalmente el servicio de una aplicación.					
2.	Los ataques a los servicios DNS de una empresa, generan gastos excesivos, incluso detiene los procesos internos.					
3.	Un ciberdelincuente aprovecha las vulnerabilidades que presentan los equipos servidores de DNS para fines maliciosos					
4.	Una medida de seguridad ante ataques DNS, es limitar las peticiones con la inclusión configuraciones de calidad de servicio QoS					
5.	La configuración de DNSsec agrega una capa de seguridad a los servidores DNS, minimiza los riesgos a ataques informáticos					

Se agradece su colaboración.