ANÁLISIS DE LA SEGURIDAD AL IMPLEMENTAR UNA RED CON PROTOCOLO IPv6

ABELARDO NAVA MESA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

ANÁLISIS DE LA SEGURIDAD AL IMPLEMENTAR UNA RED CON PROTOCOLO IPv6

ABELARDO NAVA MESA

Trabajo de grado para optar al título de especialista en seguridad informática

Director
Julio Alberto Vargas Fernández
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

Nota de aceptación:

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, _____/ _____/_____/

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ANYCAST: significa alguna difusión y enruta el paquete al mejor destino desde el punto de vista de la red.

ATAQUE: es la ofensiva informática que pretende tomar el control, borrar, alterar o dañar un sistema informático.

CABECERA: parte del paquete del protocolo de internet que contiene la información de enrutamiento incluyendo las direcciones de la fuente y la del destino con opciones o banderas para tratar dicho paquete mientras viaja en una red.

FRAGMENTACIÓN: mecanismo presente en redes con el cual un paquete se separa en bloques más pequeños si estos sobrepasan la MTU definida en alguna interface.

FRAME O TRAMA: unidad de envió de datos usada para indicar la cantidad de bits transmitidos sobre el nivel de enlace de datos del modelo OSI.

GNU: Es un anacronismo recursivo indicando que es un sistema operativo diferente a Unix.

ICMP: protocolo de mensajes de control de internet; es un subprotocolo de control y notificación de errores del protocolo de internet usado tanto en versión 4 como 6.

IETF: acrónimo del inglés *Internet Engineering Task Force,* Grupo de trabajo de ingeniería de internet es una organización abierta, que tiene como objetivos el contribuir a la ingeniería de internet, aportando en diferentes áreas, como transporte, enrutamiento y seguridad.

IOT: acrónimo del inglés *Internet of the things*. El internet de las cosas hace referencia a la facilidad que cualquier dispositivo embebido tiene para conectarse a una red como internet y permitir múltiples aplicaciones como son: diagnóstico médico, automatización a distancia, sensorica, telemétrica, geoposición en tiempo real, etc.

JUMBO *FRAME*: función soportada en algunas tarjetas de red que permite hacer una transferencia de datos de un tamaño superior a los 1500 bytes en MTU; el tamaño del jumbo frame ronda desde los 1518 bytes hasta los 9000 bytes.

MTU: unidad máxima de transmisión que indica la cantidad de datos en bytes que pueden pasar a través del medio generalmente en Ethernet.

MULTICAST: significa multidifusión donde un único emisor transmite a múltiples receptores; generalmente esos receptores se definen en un grupo para recibir a los paquetes multicast.

OSI: modelo de interconexión de sistemas abiertos que sirve de referencia para los protocolos de arquitectura de red definido en siete capas.

PAQUETE: bloque de información que se envía a través del nivel de red del modelo OSI.

PROTOCOLO: conjunto de reglas o normas definidas entre diferentes partes para entablar una comunicación; con este se formalizan las sintaxis, estándar y normas para que exista comunicación entre diferentes sistemas.

RFC: acrónimo del inglés *Request For Comments*. Es una solicitud de comentarios de una serie de publicaciones del grupo de trabajo de ingeniería de internet IETF que describen aspectos funcionales de internet, redes, protocolos, procedimientos, etc.

RIESGO: análisis donde se identifican activos informáticos, vulnerabilidades y amenazas, incluyendo probabilidad de ocurrencia y el impacto de estas (económico, operacional, servicios, etc.).

SPOOFING: son las técnicas usadas por un atacante en la cual se suplanta un elemento de una red para hacerse pasar por otro y capturar datos o información.

UNICAST: significa unidifusión o difusión única donde la información se transmite desde un único emisor hacia un único receptor.

VULNERABILIDAD: debilidad de un sistema informático que se puede explorar para atacarlo o afectarlo.

DPI: acrónimo del inglés *Deep Inspection packet,* Son dispositivos que realizan una inspección de la carga útil de los paquetes, permitiendo funciones avanzadas de seguridad como minería de datos, escuchas ocultas y censura.

WAF: acrónimo del inglés web application firewall, son dispositivos que protegen servidores que contengan aplicaciones web de ataques específicos.

RESUMEN

El presente trabajo de grado tiene como propósito identificar los riesgos, vulnerabilidades y ataques que se presentan en una red que implementa el protocolo IPv6.

Para dar cumplimiento a ese objetivo se realiza una investigación cuantitativa con base en diseño experimental. Con ese diseño se implementa un laboratorio en un ambiente tecnológico controlado para, en primer lugar, la recolección técnica de datos e información y, en segundo lugar, el análisis del contenido tanto en un ambiente de área local como de área amplia.

Las pruebas se realizaron aprovechando la funcionalidad de *router* virtual presente en *firewall* juniper srx-100. Se realizaron también pruebas con *host* físicos y máquinas virtuales usando el software licenciado Windows 10, Windows 7 y distribuciones GNU como Kali Linux y Raspian. Por último, se realizaron capturas de tráfico para ser analizadas por *wireshark* y examinar el comportamiento del protocolo IPv6.

Mediante los resultados obtenidos se pretendió demostrar que es posible realizar un conjunto de pruebas del protocolo y disponer de mejores prácticas de seguridad informática. Además de la presentación de resultados de las pruebas en este trabajo de grado las conclusiones y aspectos metodológicos se publicaron en una página web como medio de consulta para cualquier usuario interesado.

Palabras clave: Ataque, spoofing, protocolo, cabecera, vulnerabilidad

INTRODUCCIÓN

El protocolo IPv6 surge de la necesidad de aumentar la capacidad de direcciones IP utilizables debido a la escasez que se está presentando en el protocolo IPv4. La preparación y despliegue de la IPv6 se está dando a nivel mundial desde el año 2010, además con el aumento de teléfonos móviles y el auge, por ejemplo, del internet de las cosas. Por tanto, en la actualidad se hace necesario un pronto despliegue de esa solución que, con la promesa de conexiones *end-to-end*, permita una verdadera red omnipresente.

El afán por implementar el IPv6 descuida soluciones sobre el aspecto de la seguridad informática. El protocolo IPv6 es más seguro que su antecesor, sin embargo, existen factores que se deben tomar en cuenta, entre ellos: los problemas en sí mismos del protocolo; los problemas durante la migración de IPv4 hacia IPv6; y la falta de experiencia acumulada sobre la seguridad en una red cien por ciento IPv6.

Por lo tanto, la finalidad de este trabajo es ofrecer conocimiento sustentado en la experiencia sobre los aspectos de seguridad y debilidades presentes en el protocolo IPv6, por ello, además del componente teórico sobre la seguridad se desarrollan guías y laboratorios prácticos. La finalidad es proponer una reflexión para técnicos y especialistas en el área sobre la necesidad de reforzar los ambientes que funcionan con una red IPv6 y sobre la importancia de la prevención de vulnerabilidades a la seguridad de redes e informática.

1. PLANTEAMIENTO DEL PROBLEMA

Durante el desarrollo del protocolo IPv6 se han creado expectativas falsas respecto de su fortaleza en términos de seguridad. Entre esas expectativas se mencionan: el uso nativo de Ipsec; no se requiere translación de direcciones y la imposibilidad de escanear los servicios de red. Además, existen problemas tales como la falta de experiencia en implementaciones IPv6 y la escasez de personal capacitado. Por ello, es necesario que se difunda el conocimiento fundamentado en la experiencia sobre la implementación del protocolo en términos de seguridad.

1.1 FORMULACIÓN DEL PROBLEMA

El protocolo IPv6 como cualquier desarrollo tecnológico tiene fallas que pueden ser explotadas en el RCF 4942. En este se indica que algunos ataques factibles a realizar son: denegación de servicio (DoS); hombre en el medio (MiM); falsificar el *router advertisements*; testear y vulnerar los *stack* en los sistemas operativos; sesión *hijaking*; crear *worms* y *exploits* de IPv6[1]. Estos puntos débiles pueden ser evitados o, por lo menos, disminuir la probabilidad de su ocurrencia mediante un buen conocimiento y *hardening* de la infraestructura.

Por ello la pregunta central que se procuró responder en el presente estudio fue:

¿cómo ejecutar un análisis de seguridad en la implementación una red con protocolo IPv6 puede disminuir los ataques e intrusiones en la infraestructura operativa de una red?

[1] DAVIES, E., KRISHNAN, S., SAVOLA, P. IPv6 Transition/Coexistence security considerations. s.l.: IETF, 2007. RFC 4942.

2. JUSTIFICACIÓN

En la actualidad se presenta un agotamiento del direccionamiento publico IPv4 para la región de Latinoamérica y el Caribe[2]. En este contexto es inminente la migración hacia el protocolo IPv6 porque tiene mejores prestaciones funcionales y permite asignar un mayor número de direcciones IP. Sin embargo, es necesario tener en cuenta las consideraciones de seguridad del protocolo IPv6 ya que por tratarse de una tecnología emergente puede presentar problemas de seguridad factibles de ser explotados por atacantes con intenciones maliciosas y que buscan indisponer los servicios de la red o acceder a los datos que se transmiten sobre ella. Por este motivo es de vital importancia detectar las brechas de seguridad sobre este nuevo protocolo, documentarlas y difundirlas a fin de minimizar el riesgo de exposición en el protocolo IPv6.

La finalidad del presente trabajo es que los ingenieros de redes y de seguridad tengan una base de conocimiento para el contexto de la seguridad informática del protocolo IPv6. Se entrega, en primer lugar, una guía práctica con pruebas de laboratorio y, en segundo lugar, análisis específico a ser empleado en cualquier entorno de red a donde se esté migrando el servicio hacia el protocolo IPv6. Con esto en mente, este trabajo de grado también propone entregar a los ingenieros interesados en el área mecanismos que sirvan como reforzamiento (*hardening*) y mejores prácticas de seguridad desde el punto de vista tanto del protocolo como de los dispositivos involucrados: Firewall, IPS/IDS, *router*, *switches*, servidores, etc.

[2] LACNIC. fases-de-agotamiento-de-IPv4. Montevideo: Casa de Internet de Latinoamérica y el Caribe, s.f. [en línea, acceso en 18 de noviembre de 2016].

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un estudio de seguridad sobre la implementación de una red IPv6 en un entorno tecnológico controlado.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar y analizar los tipos de ataques que se pueden desarrollar con el uso del protocolo IPv6.
- Generar un plan de pruebas en los escenarios tecnológicos para el protocolo IPv6.
- Recomendar las mejores prácticas de seguridad informática para los dispositivos de red Ipv6 del entorno tecnológico controlado, y que esta sea base de conocimiento para otras implementaciones de redes Ipv6.
- Socializar los resultados para mejorar las prácticas de seguridad en dispositivos que funcionen con IPv6 mediante una página web de libre acceso donde se subirán las evidencias, pruebas y recomendaciones, encontrados durante el desarrollo del proyecto.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES O ESTADO DEL ARTE

A continuación, se realiza una exploración del material de referencia que desarrolla propuestas para realizar soporte de la seguridad de la información en el protocolo IPv6. Esa exploración se fundamentada en diferentes fuentes tales como: los RFC (*Request For Comments*); publicaciones desarrolladas por la IETF (*Internet Engineering Task Force*); diferentes trabajos de grado enfocados en la seguridad del protocolo IPv6. Entre las referencias que documentaron proyectos se realizó un análisis metódico de sus ventajas y desventajas y de cómo fueron desarrollados para fortalecer la seguridad informática.

Al implementar una nueva tecnología se abre una nueva brecha que puede ser explotada para bien o para mal. El desarrollo del "internet de las cosas" junto a la puesta en marcha del protocolo IPv6 facilita la conectividad de muchos componentes dando origen a una red completamente omnipresente. Con ello es importante que se eduque en el ámbito de la seguridad ya que buenas prácticas de seguridad permiten una mejor puesta en marcha del protocolo y pueden disminuir las probabilidades de ataques y amenazas sobre el entorno de red donde se implementa el protocolo.

4.1.1 RFC4942 IPv6. Consideraciones de seguridad transición-coexistencia

Una de las primeras consideraciones técnicas de seguridad en IPv6 se encuentra en la publicación del RFC4942 del año 2007 creado por un grupo de la IETF[3], esta publicación considera tres temas principales:

4.1.1.1 Problemas del protocolo en sí mismo

Esta temática considera problemas intrínsecos del protocolo que se deben considerar en su puesta en marcha. El temario de que trata es:

- problemas con la cabecera de enrutamiento y host;
- problemas en la cabecera de enrutamiento para móvil IPv6 y otros propósitos;
- lugar y alcance de direcciones multicast;
- Icmpv6 y multicast;
- mensajes de error en icmpv6 y falsos paquetes de errores;

[3] DAVIES, E., KRISHNAN, S., SAVOLA, P. Op. cit.

- identificación y seguridad de paquetes anycast;
- interacción de direccionamiento privado con defensa DdoS;
- DNS dinámicos: autoconfiguración de direcciones, extensión privatizada y Paquete Send;
- extensión de cabeceras Ip;
- fragmentación: reensamble e inspección profunda de paquetes;
- fragmentación relacionada con ataques de Dos;
- direccionamiento link-local y asegurando el *Neighbor Discovery*;
- aseguramiento de paquetes *Router Advertisements*;
- balanceo de carga *Host-to-router*;
- IPv6 móvil;
- direcciones IPv4 mapeadas en IPv6;
- incremento de la transparencia *End-to-End* que incluye los temas redes IPv6 sin NAT y modelo de seguridad empresarial para redes IPv6;
- túneles IPv6 en IPv6.

4.1.1.2 Problemas en los mecanismos de transición de IPv4 a IPv6

En camino hacia la migración IPv4 a IPv6 se pueden presentar riesgos a considerar; en el documento los riesgos que se presentan son:

- problemas y mecanismos específicos de IPv6 transición/coexistencia;
- túneles automáticos y *Relay*;
- túneles IPv6 a través de redes IPv4 pueden romper la seguridad que se asume del protocolo IPv4.

4.1.1.3 Problemas en el despliegue del protocolo IPv6

Cuando se trata de integrar completamente la red IPv6 en un cien por ciento se deben considerar posibles riesgos y amenazas. Estos son tratados bajo los siguientes temas:

- realizar una prueba piloto de IPv6 para evitar problemas de seguridad;
- problemas en servidores DNS;
- esquema de direccionamiento y seguridad en *routers*;
- consecuencias de múltiple direccionamiento en IPv6;
- despliegue de ICMPv6 – problemas por la transparencia de ICMPv6;
- modo transporte de Ipsec;
- reducción de funcionalidades de dispositivos;
- factores operacionales cuando se habilita IPv6 en una red;
- problemas de seguridad en *Proxies Neighbor Discovery*.

4.1.2 RFC7721. Consideraciones de seguridad y privacidad para los mecanismos de generación de direcciones en IPv6

El desarrollo de este RFC culminó en marzo de 2016, gracias a un grupo de la IETF el cual considera los problemas presentes en cuanto a seguridad y privacidad de los mecanismos que usa el protocolo IPv6 para asignar direcciones a los dispositivos *host* y enrutadores[4]. Estos mecanismos pueden ser estándar y no estándar, en el documento se realiza una evaluación de las debilidades en: los Identificadores IEEE, las configuraciones estáticas de las direcciones, la generación de direcciones criptográficas, direcciones temporales y generación con DHCPv6. Además, se incluye la referencia a varios problemas en: el uso del direccionamiento IPv6, la operación de la red, derechos de propiedad intelectual y confirmad ya esto podría limitar la operación en distintos sistemas operativos.

4.1.3 RFC5157. Escaneo de red consecuencias en IPv6

En el documento citado, escrito en marzo de 2008 por IETF, se intenta concientizar acerca de la dificultad de realizar un escaneo de puertos a una red aun con el espacio por defecto en IPv6 con un tamaño de mascara de red de 64 Bit[5]. Esa dificultad consiste en la necesidad de que los administradores de red deben considerar el riesgo y las posibles técnicas que utilizan los gusanos informáticos o *Hackers* para realizar el reconocimiento de una red IPv6. Por lo tanto, la planeación y estrategias forman de una defensa profunda en la red.

Los temas tratados en el documento son: los mecanismos de escaneo tanto en IPv4 como IPv6; las técnicas sobre cómo reducir el espacio de búsqueda en IPv6; cómo afecta esto el *dual-stacking*; defensas contra el escaneo y sobre cómo los atacantes pueden hacer esto *off-link* a través de distintas técnicas y escenarios: obtener información a través de los prefijos IPv6, zonas DNS con los paquetes de advertencia a *host* y en las zonas de transferencia DNS; y análisis de *logs* con la participación de las aplicaciones en uso. También se documenta cómo los atacantes pueden realizar esto *on-link* a nivel general con: técnicas intra-sitios, paquetes multicast u otros servicios de descubrimiento. El documento finaliza explicando las herramientas que mitigan los ataques de escaneo incluyendo temas tales como: el uso de direcciones privadas IPv6, generación de direcciones criptográficas, no uso de direcciones mac en formato EUI-64 y configuración de los *bits options* en DHCP.

[4] COOPER, A., GONT, F. Security and privacy considerations for IPv6 address generation mechanisms. s.l. :IETF, 2016. RFC 7721 [en línea, acceso en 18 de noviembre de 2016].
[5] Ibíd.

4.1.4 RFC6092. Recomendaciones de seguridad para equipos de clientes CPE para proveer Internet residencial con IPv6

El documento escrito por la IETF en el año 2011[6] entrega recomendaciones para los equipos finales de los clientes con el objetivo de proveer capacidades de seguridad en el perímetro del área local de una red IPv6 implementada en hogares y pequeñas oficinas. Dentro del temario de este artículo se considera: el funcionamiento de los protocolos en la capa de internet y transporte; recomendaciones en el uso de filtros en los paquetes no orientados a la conexión UDP, Ipsec; y el intercambio de llaves IKE. Se proponen también recomendaciones en los protocolos orientados a la conexión de filtros en tcp, sctp, dccp y Shim6, todo ello con el fin de evitar el ingreso de personas no autorizadas desde internet a las redes IPv6. Este último grupo de recomendaciones surgen a partir de la limitación presente en la completa transparencia de una red *end-to-end* y, además, de la falta de experiencia con la ingeniería de redes o de internet de las pequeñas oficinas y clientes residenciales.

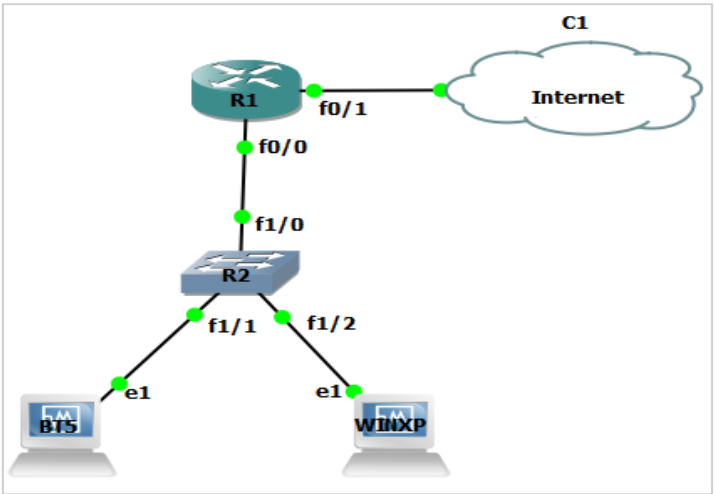
4.1.5 Análisis de la seguridad IPv6, pruebas y recomendaciones

En el proyecto presentado por Nicolás Contador Vilches en la Universidad Nacional Andrés Bello de Viña de Mar (Chile) en el año 2013[7] explica la metodología de cómo hacer las pruebas de seguridad del protocolo IPv6. Este proyecto se enfoca en pruebas de ataques como reconocimiento *man in the middle*, *flooding attacks*, dispositivo falso o *sniffing* en un entorno IPv6. Los laboratorios desarrollados usan el sistema operativo Backtrack 5 RC3 para recrear ataques y toma capturas en un *sniffer* a través de una máquina con Windows Xp, como se muestra en la figura 1.

[6] WOODYATT, J. Recommended simple security capabilities in customer premises equipment (CPE) for providing residential IPv6 internet service. s.l.: IETF, 2011. RFC 6092. [en línea, acceso en 18 de noviembre de 2016].

[7] CONTADOR VILCHES, N.. Análisis de seguridad de IPv6 pruebas y recomendaciones. Tesis de Maestría. Viña del Mar: Universidad Andrés Bello, 2013. 30 p. [en línea, acceso en 18 de noviembre de 2016].

Figura 1. Topología usada en ataque reconocimiento IPv6



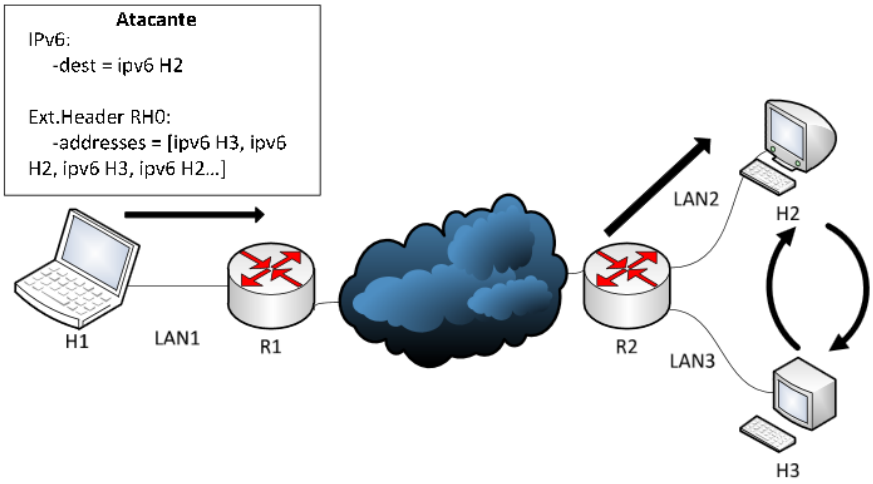
Fuente: CONTADOR VILCHES, Op. cit. p. 19

4.1.6 Análisis de la seguridad en redes IPv6

El proyecto creado por el ingeniero Carlos García Martín en la Universidad Carlos III de Madrid (España)[8] desarrolla metodología y laboratorios bajo técnicas *fuzzing* con la cual evalúa y realiza ataques en IPv6 como *flood route*, NDP *table exhaustion*, *hopbyhop* dos, *destination options* DoS, cache *poisoning*, *flood* Dhcpv6 *solicit.* Un ejemplo de la topología utilizada en este proyecto se observa en la figura 2.

[8] GARCÍA MARTÍN, C. Análisis de seguridad en redes IPv6. Proyecto fin de carrera. Madrid: Universidad Carlos III de Madrid. Escuela Politécnica Superior. Departamento de Ingeniería Telemática, 2012. 143 p. [en línea, acceso en 18 de noviembre de 2016]

Figura 2. Topología usada en ataque de cabecera RH0

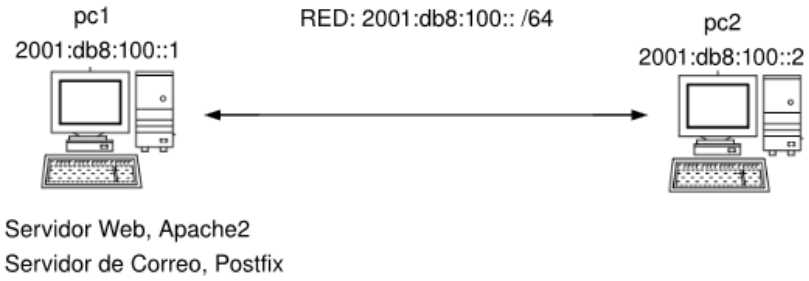


Fuente: GARCÍA MARTÍN, C. Op. cit.

4.1.7 Seguridad en IPv6 con Ipsec

Este proyecto nace en la Universidad de Magallanes en el año 2008 presentado por Javier Enrique Vivar Soto[9]. La metodología y laboratorios del proyecto se concentra en aspectos como el uso de Ipsec bajo sus algoritmos autenticación y encripción y la forma como esta compatibilidad maneja el protocolo IPv6. El laboratorio utiliza encripción Ipsec sobre IPv6 con aplicaciones reales, y de esta manera comprueba que los servicios se pueden proteger al evitar que un *sniffer* lea los datos contenidos en la aplicación o los datos del mismo usuario. La topología utilizada para este laboratorio se puede observar en la figura 3.

Figura 3. Topología de Pruebas Ipsec en protocolo IPv6



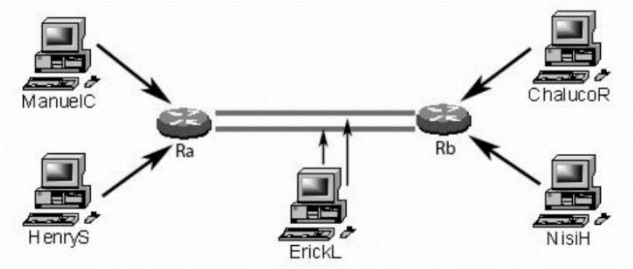
Fuente: VIVAR SOTO, J. E. Op. cit.

[9] VIVAR SOTO, J. E. Seguridad en IPv6 con IPsec. Trabajo de titulación. Punta Arenas: Universidad de Magallanes. Facultad de ingeniería. Departamento de Ingeniería en Computación, 2008. 58 p. [en línea, acceso en 18 de noviembre de 2016]

4.1.8 Seguridad en Ip con el protocolo Ipsec para IPv6

El proyecto surge en la Universidad de San Carlos de Guatemala en el año 2005 a cargo del ingeniero Erick Fernando Luján Montes[10]. Su metodología se fundamenta también en demostrar la ventaja de usar el Ipsec sobre el protocolo IPv6. Además, aporta un laboratorio cuya intención es demostrar que en una red IPv6 es factible intentar realizar un secuestro de sesión a pesar de que el tráfico esté encriptado y engañar a los emisores que creen tener una conversación correcta (ver figura 4). Sin embargo, el autor aclara que existe una dificultad de realizar dicho secuestro.

Figura 4. Laboratorio Ipsec sobre aplicaciones



Fuente: LUJÁN MONTES, E. F. Op. cit.

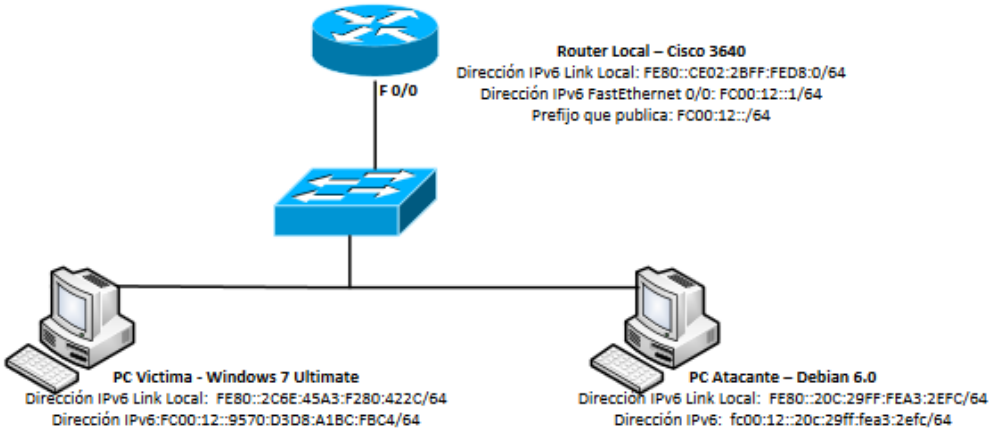
4.1.9 Análisis de Seguridad en el protocolo IPv6

El proyecto surge en la Universidad de Buenos Aires desarrollándose en el año 2013 por el ingeniero Rodrigo Horacio Zapata[11]. En el proyecto se entrega una documentación muy completa acerca del funcionamiento del protocolo IPv6 y de sus diferentes funcionalidades incluyendo vulnerabilidades como las encontradas en la cabecera de extensión, debilidades con el escaneo de redes, y ataques en las técnicas de asignación de direcciones. Se destaca el laboratorio con el cual puede denegar el servicio de un *host* víctima, cuando un atacante intercepta los paquetes NS y responde modificándolos.

[10] LUJÁN MONTES, E. F. Seguridad en Ip con el protocolo Ipsec para IPv6. Trabajo de graduación. Ciudad de Guatemala: Universidad de San Carlos de Guatemala. Facultad de Ingeniería. Escuela de Ingeniería en Ciencias y Sistemas, 2005. 158 p. [en línea, acceso en 18 de noviembre de 2016].

[11] ZAPATA VALDEZ, R. H. Análisis de Seguridad en el protocolo IPv6. Trabajo final. Buenos Aires: Universidad de Buenos Aires. Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e ingeniería, Especialización en Seguridad Informática, 2013. 77 p. [en línea, acceso en 18 de noviembre de 2016].

Figura 5. Laboratorio explotando vulnerabilidad DAD

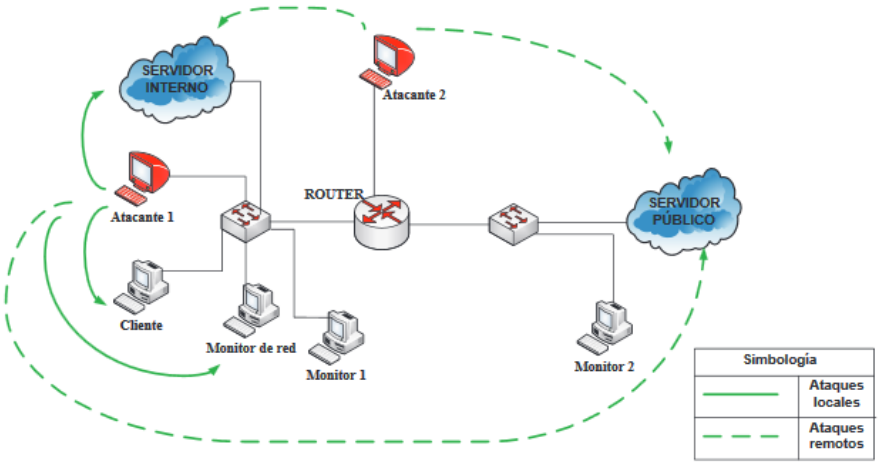


Fuente: ZAPATA VALDEZ, R. H. Op. cit

4.1.10 Análisis de Ip *Spoofing* en redes IPv6

El trabajo desarrollado en la Escuela Politécnica Nacional de Ecuador en el año 2015 por el ingeniero Daniel Alejandro Cazar se destaca por ofrecer un completo escenario de pruebas para desarrollar un laboratorio de búsqueda de vulnerabilidades desde un punto de vista LAN como WAN[12]. En este proyecto se realizan diferentes test como muestra la figura 6, siendo que los ataques incluyen negación del servicio, hombre en el medio y *smurf* local y remoto.

Figura 6. Laboratorio multipropósito para pruebas IPv6



Fuente: CAZAR JÁCOME, D. A. Op. cit.

[12] CAZAR JÁCOME, D. A. Análisis de Ip spoofing en redes IPv6. Proyecto de grado. Quito: Escuela Politécnica Nacional de Ecuador. Facultad de ingeniería Eléctrica y Electrónica, 2015. 118 p. [en línea, acceso en 18 de noviembre de 2016].

4.1.11 *Testing the security of IPv6 implementations*
Este reporte sobre IPv6 fue creado por las consultoras de seguridad Holandesas Fox-IT, Itsec, Madison-Gurkha, Pine Digital Security, Riscure y TNO patrocinado por el Ministerio de Economía holandés en el año 2014[13]. En el reporte se desarrollan consideraciones generales de seguridad de IPv6; el tipo de tráfico IPv6 que se debe filtrar para evitar su vulneración; y las vulnerabilidades en sistemas que usan IPv6 incluyendo algunas que afectan protocolos de enrutamiento.

4.1.12 *Guidelines for the secure deployment of* IPv6
El gobierno de Estados Unidos de América creó una guía escrita por Sheila Frankel, Richard Graveman, Jhon Pearce, Mark Rooks en el año 2010[14] en la cual se desarrolla una introducción completa sobre el funcionamiento de IPv6. Otros temas tratados son: aspectos avanzados del protocolo IPv6; seguridad avanzada y riesgos de seguridad en el direccionamiento IPv6 además de explicar riesgos en ambientes de transición IPv4-IPv6.

4.1.13 Curso seguridad avanzada de redes de datos
En Colombia sobre el tema de seguridad del protocolo IPv6, podemos destacar las observaciones dadas en la data-teca de la Universidad Nacional Abierta y a Distancia, desarrollado por el Docente Jorge Iván Morales Salazar del curso seguridad avanzado en redes de datos[15]. En esta referencia se consideran aspectos sobre las debilidades del protocolo tales como:

- programación sin depurar y vulnerabilidades de aplicaciones;
- la explotación de la transición de IPv4 a IPv6;
- listas negras ineficaces y afectación en correo electrónico;
- ataque DdoS;
- evasión de medidas de seguridad;
- enmascaramiento de puntos de origen;
- seguridad IPv6 Ipsec.

Está claro que este material se desarrolló como fin educativo, teórico y no incluye laboratorios prácticos, no obstante, el documento se destaca como referencia para el desarrollo de proyectos sobre el tema de seguridad.

[13] Nederlandse IPv6 Task Force. Testing the security of IPv6 implementations. S.l.: 2014. [en línea, acceso en 18 de noviembre de 2016].
[14] FRANKEL, S., GRAVEMAN, R., PEARCE, J., ROOKS, M. Guidelines for the secure deployment of IPv6. Gaithersburg: NIST, 2010. 188 p. [en línea, acceso en 18 de noviembre de 2016].
[15] MORALES SALAZAR, J. I. Curso seguridad avanzada de redes de datos. Bogotá: Datateca-UNAD. [en línea, acceso en 1 diciembre de 2016].

4.1.14 Seguridad IPv6

Un material de lectura que se destaca como antecedente es creado por Fernando Gont de la empresa SI6 Networks año 2012[16]. El autor creó una presentación sobre el tema de la seguridad de IPv6 en donde se discuten aspectos como:

- comparación de entre IPv6/IPv4;
- discusión de la seguridad de IPv6;
- implicación de seguridad durante migración y coexistencia;
- seguridad IPv6 en redes IPv4;
- áreas que requieren más trabajo.

Esta referencia se destaca por aclarar un mito común presente desde la creación de IPv6 sobre su seguridad superior comparado con IPv4. Aunque esto en cierto aspecto es verdad, por ser una nueva tecnología va a generar otros problemas sobre todo en el aspecto de la seguridad donde la capacitación y difusión entre los ingenieros sobre este protocolo debe hacerse lo más pronto posible.

4.1.15 IPv6 *security*

A solicitud del gobierno de Hong Kong en el año 2011[17] fue escrito un reporte que explica que tanto IPv4 como IPv6 pueden ser objeto de ataques comunes imposibles de excluir o evitar. Se trata de los ataques en la capa de aplicación, *buffer overflow*, virus y código malicioso; ataques con aplicaciones web; ataques de fuerza bruta y adivinación de contraseñas; introducción de dispositivos intrusos que interfieren en el buen funcionamiento de la red como *switches*, *routers*, servidores DNS, servidores dhcp o *access point*. Los ataques de negación de servicio van a estar presentes en IPv6 y el uso de la ingeniería social va a ser el día a día. Este reporte tampoco incluye componentes prácticos en el análisis de la seguridad de IPv6.

4.1.16 Guía para el aseguramiento del protocolo IPv6

En Colombia, el Ministerio de las Tecnologías de la Información ha trabajado en una guía, para el aseguramiento del protocolo IPv6 que va en su versión 1.3 de

[16] GONT, F. Seguridad en IPv6. s.l.: SI6 Networks, 2012 [en línea, acceso en 18 de noviembre de 2016].
[17] SI6 Networks. Seguridad en IPv6. S.l.: SI6 Networks, 2011. [en línea, acceso en 18 de noviembre de 2016].

05/11/2015[18]. En la guía se entregan lineamientos y políticas de seguridad para aplicar en las entidades del Estado colombiano y su contenido incluye:

- lineamientos de seguridad que involucran el direccionamiento Ip, el uso de Ipsec, creación de vpn y monitoreo de IPv6;
- pilares de la seguridad de la información en IPv6: confidencialidad, integridad, disponibilidad y privacidad;
- análisis de riesgos, valoración de activos, gestión de riesgo durante la migración IPv4 a IPv6, *hacking* ético, *pentesting* en redes IPv4/IPv6;
- lineamientos de seguridad en la nube IPv6;
- mitigación de riesgos en IPv6;
- RFC de seguridad en IPv6.

Estos lineamientos como marco de referencia son importantes porque demuestran el interés de gobierno colombiano en implementar esta tecnología en sus instituciones bajo una buena práctica de la seguridad informática.

4.2 MARCO TEÓRICO

El protocolo IPv6 hace referencia a una nueva tecnología que reemplaza a la versión anterior, es decir, el protocolo IPv4 por tanto la migración hacia este nuevo protocolo es una tendencia que se debería realizar a mediano plazo. En Latinoamérica quien gestiona la reserva de direcciones IPv4 es la Lacnic[19]; esta institución indica que estamos cerca de un agotamiento de IPv4, por lo que en ese escenario IPv6 debería estar listo para ingresar al continente.

4.2.1 Características y funcionamiento del protocolo IPv6

La principal característica de IPv6 es su amplio rango de direcciones Ip asignables comparado con IPv4. Mientras IPv4 tiene un rango máximo de 32 bits divido en 4 octetos para un total de 4.3 mil millones de direcciones IPv6 está basado 128 bits como se muestra a continuación:

a) total, espacio IPv4: 4'294,967,296 ip asignables;

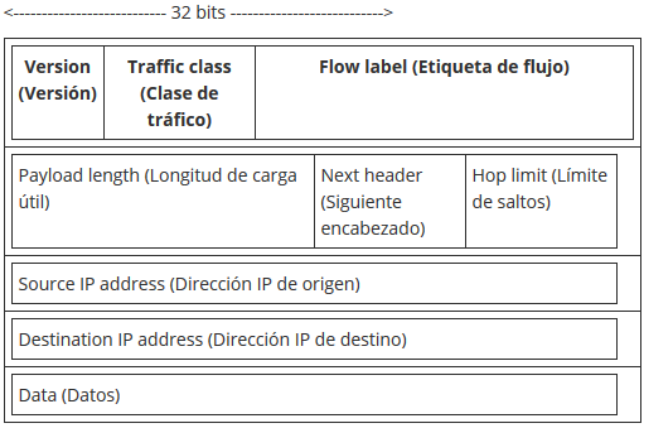
[18] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN DE Colombia. Guía de Aseguramiento del protocolo IPv6. Bogotá: MINTIC, 2015. [en línea, acceso en 18 de noviembre de 2016].

[19] LACNIC. Agotamiento de direcciones IPv4. Montevideo: Casa de Internet de Latinoamérica y el Caribe, s.f. [en línea, acceso en 01 de marzo de 2017].

b) total, espacio IPv6: 340'282,366,920,938,463,463,374,607,431,768,211,456 ips asignables.

Sabiendo de la ventaja que ofrece el Protocolo se deben conocer las partes de su encabezado explicitadas en la figura 7.

Figura 7. Encabezado IPv6



Fuente: http://es.ccm.net/contents/268-protocolo-IPv6

El significado de los campos de la figura antes citada es la siguiente:

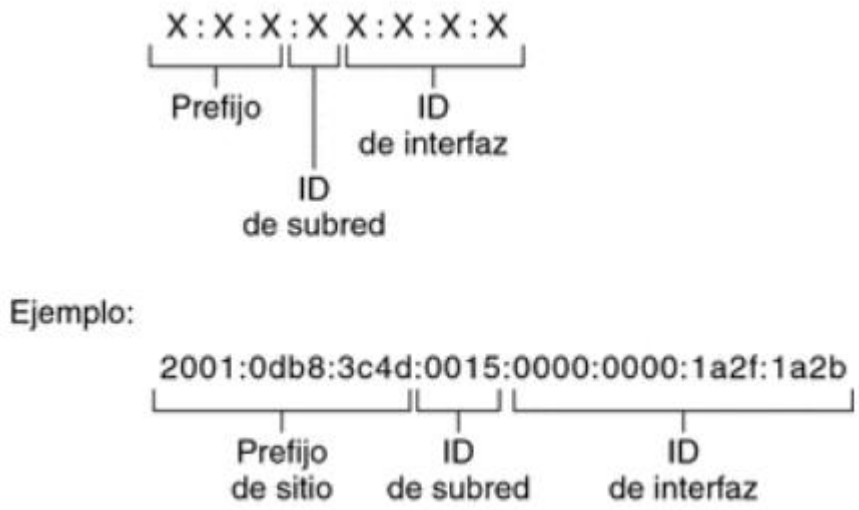
- Versión: al revisar esta parte de la cabecera se identifica que data grama se enruta si es IPv4 o IPv6, usa 4 bits.
- Clase de tráfico: este espacio permite asignar prioridades en el tráfico logrando disminuir la velocidad en tiempo de congestión. Este espacio está codificado a 8 bits; para mantener el tráfico constante en tiempo real se puede asignar valores en este campo de 8 a 15 (audio y video).
- Etiqueta de flujo: es un indicador para facilitar el trabajo de los *routers* y permitir funciones como calidad del servicio o que el *router* pueda llevar a cabo procesamientos particulares, escoger una ruta e información en tiempo real.
- Longitud de carga útil: tiene un tamaño de 2 bytes y contiene el tamaño de la carga útil sin el encabezado, si el valor es 0 se indica que es un jumbo *frame*.
- Siguiente encabezado: identifica el encabezado como lo puede ser un protocolo de capa superior icmp, tcp, etc.
- Límite de datos: reemplaza el espacio-tiempo de vida de IPv4 en IPv6; al llegar a un valor de 0 el paquete se rechaza y se notifica error con paquetes icmpv6.

- Dirección origen y dirección destino: usados para definir el origen y destino del tráfico, estas direcciones tienen una longitud fija de 16 bytes.

El direccionamiento IPv6 se asigna a interfaces no a nodos considerando que en un nodo puede haber muchas interfaces[20] y que se pueden asignar a una interfaz varias direcciones. El IPv6 incluye tres clases de direcciones: 1) unidifusion, unicast – una sola interfaz para un sólo nodo; 2) multidifusion, multicast – un grupo de interfaces, en nodo distintos, donde al enviar un paquete a la dirección multicast se dirigen únicamente a los miembros del grupo multicast; 3) difusión por proximidad, anycast – se agrupan interfaces de distintos nodos y los paquetes se dirigen al grupo de difusión más cercano al remitente.

Las partes de las direcciones IPv6 tienen un tamaño de 128 bits compuesto de 8 campos de 16 bits, unido por dos puntos; cada campo se une por un número hexadecimal como se muestra en la figura 8.

Figura 8. Formato básico dirección IPv6



Fuente: https://docs.oracle.com/cd/E19957-01/820-2981/IPv6-overview-10/

El prefijo de sitio que está más a la izquierda (48 bits) describe la topología pública que el isp o el registro nacional de internet da al sitio. El id de subred de 16 bits describe la topología privada del sitio. El id de interfaz de tamaño 64 bits se configura

20 HINDEN, R., O'DELL, M., DEERING, S. An IPv6 Aggregatable Global Unicast Address Format. s.l: IETF, 1998. RFC 2374. [en línea, acceso en 01 de marzo de 2017].

automáticamente desde la dirección mac de la interfaz o manualmente usando el formato EUI-64.

Hay disponibles numerosas RFC sobre el IPv6, en la tabla que se presenta a continuación aparecen los artículos escritos por la IETF ver el cuadro 1.

Cuadro 1. RFC relacionadas con IPv6

RFC o borrador de internet	Tema	Ubicación
RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*	Describe las características y funciones del protocolo ND (descubrimiento de vecinos) de IPv6	https://www.ietf.org/rfc/rfc2461.txt
RFC 3306, *Unicast-Prefix-Based IPv6 Multicast Addresses*	Describe el formato y los tipos de direcciones IPv6 multidifusión	https://tools.ietf.org/html/rfc3306
RFC 3484: *Default Address Selection for Internet Protocol version 6 (IPv6)*	Describe los algoritmos que se usan en la selección de direcciones predeterminadas de IPv6	https://www.ietf.org/rfc/rfc3484.txt
RFC 3513, *Internet Protocol version 6 (IPv6) Addressing Architecture*	Contiene información exhaustiva sobre los tipos de direcciones IPv6 con abundantes ejemplos	https://www.ietf.org/rfc/rfc3513.txt
RFC 3587, *IPv6 Global Unicast Address Format*	Describe el formato y los tipos de direcciones IPv6 multidifusión	https://tools.ietf.org/html/rfc3587

Fuente: https://docs.oracle.com/cd/E19957-01/820-2981/IPv6-overview-8/index.html

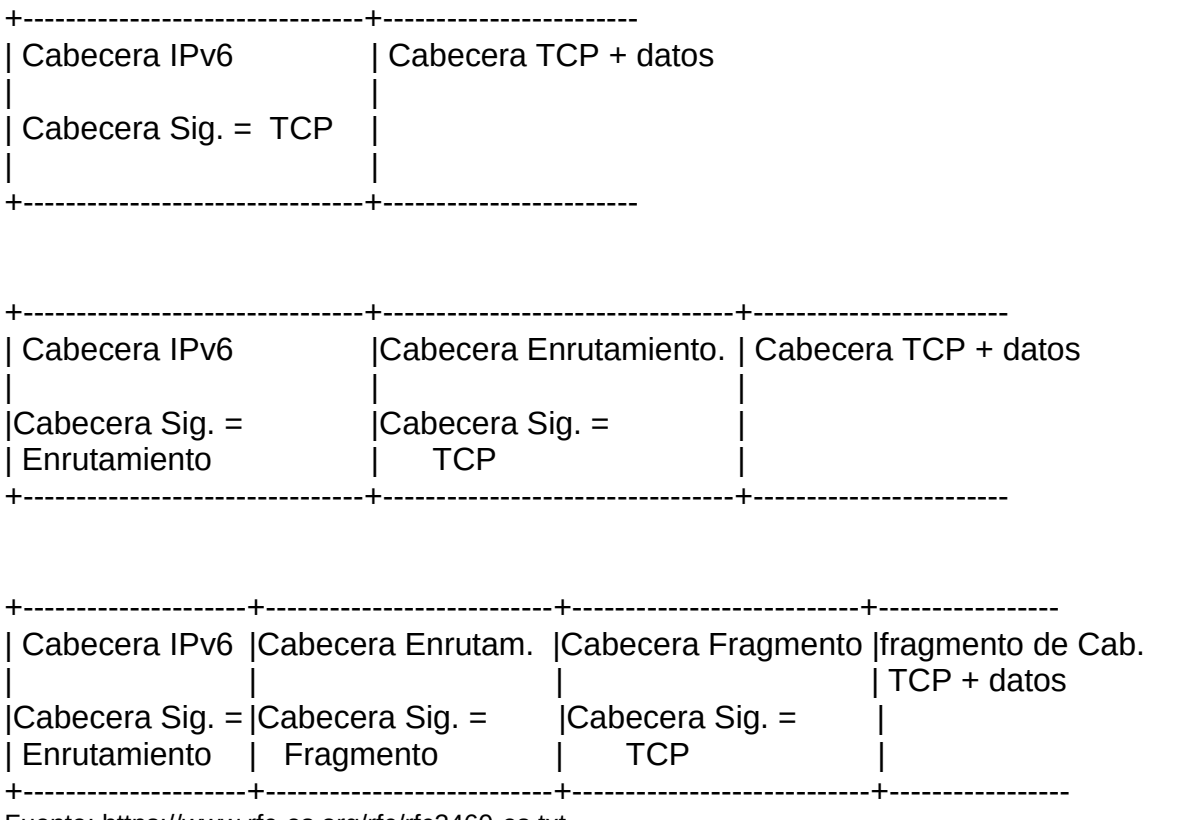
En cuando a seguridad de IPv6 incorpora Ipsec protegiendo los datos cuando se envían en la red. Ipsec usa los servicios criptográficos para ofrecer las siguientes características:

- confidencialidad: cifrando el tráfico para que en caso de ser capturarlo no se pueda des-encriptar sin conocer la llave de cifrado;
- autenticación: el tráfico está firmado digitalmente con la llave de cifrado de manera que el destino corrobora el origen del dialogo Ipsec;
- integridad de datos: contiene una suma de comprobación encriptada con la cual el destinatario comprueba que el paquete no se ha modificado durante la transmisión.

Una nueva particularidad que agrega IPv6 frente a IPv4 son las cabeceras de extensión[21]. Se trata de nuevas opciones que se añaden en la cabecera del paquete, esto se realiza en el espacio *next header* presente en el encabezado IPv6; estas opciones permiten incluir varias funciones en el protocolo que facilitan el desempeño en red y reducen el procesamiento de los paquetes en las capas superiores. En la figura 9 se incluye un ejemplo de funcionamiento cuya particularidad es la factibilidad de incluir tantas cabeceras como se deseen siempre informando en el espacio *next header* la cabecera siguiente. Según recomendación del rfc2460 si un paquete va incluir más de una cabecera debe llevar el siguiente orden:

- cabecera IPv6;
- cabecera Hop-by-hop;
- cabecera Destination;
- cabecera de Routing;
- cabecera de Fragmentacion;

Figura 9. Esquema cabecera de extensión (RFC 2640)



Fuente: https://www.rfc-es.org/rfc/rfc2460-es.txt

[21] DEERING, S., HINDEN, R. Especificación Protocolo Internet, Versión 6 (IPv6). s.l.: IETF, 1998. RFC 2460. [en línea, acceso en 01 de marzo de 2017].

Las cabeceras definidas por el RFC2460 incluyendo sus funciones se describen a continuación:

- hop-by-hop: se identifica por el valor 0 en el campo *next header*, esta cabecera lleva información opcional que puede ser examinada por cada nodo en un paquete;
- routing header: se identifica por el valor 43 en el campo *next header*, es usado por la fuente del tráfico IPv6 para informar a uno o más nodos que serán visitados en el camino del paquete;
- fragment header: la cabecera de fragmentación usa el valor 44 y es usado por la fuente IPv6 para enviar un paquete más grande que el descubierto en el *path* MTU;
- destination header: la cabecera de destino utiliza el valor 60, y lleva información opcional que sólo se examina al nodo destino;
- no next header: utiliza el valor 59, se usa para informar que no hay siguiente cabecera;
- encapsulating security payload (ESP): se identifica valor 50 y se utiliza para proporcionar servicios de seguridad en IPv6[22];
- authentication: se identifica con el valor 51 y su funcionalidad es proporcionar integridad y autenticación de la fuente de datos, y además ofrecer protección durante los reenvíos[23];
- mobility: esta cabecera es una nueva variante a la cabecera de enrutamiento (routing) definida como un tipo 2 y utiliza el valor 62 en el campo de *next header*, permite al paquete que se enrute directamente desde un nodo de una red móvil[24].

4.2.2 Protocolo de mensajes de control de internet ICMPv6

Al igual que su antecesor, el protocolo IPv4, IPv6 requiere controlar y notificar errores durante la transmisión de paquetes, para ello usa el protocolo de mensajes de control ICMPv6 que cuenta con la capacidad de realizar diagnósticos como es el caso del uso de *ping*. También se caracteriza por usar el espacio de *next header* con el valor de 58. Además, ICMPv6 hace parte de manera integral de cualquier implementación de IPv6 por lo tanto debe estar permitido.

El formato de mensajes de este protocolo se puede ver en la figura 10, a continuación:

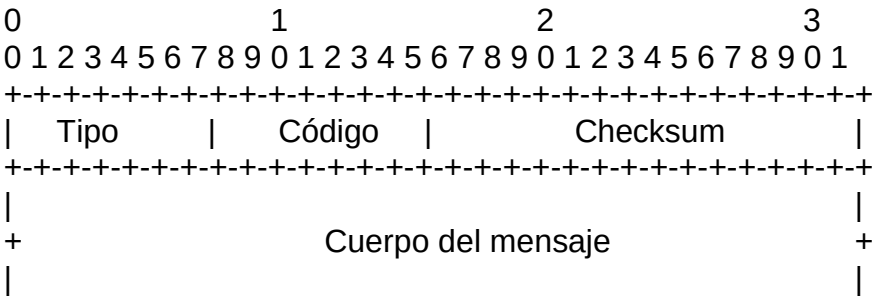
---

[22] KENT, S., ATKINSON, R. IP encapsulating security payload (ESP). s.l.: IETF, 1998. RFC 2406 [en línea, acceso en 01 de marzo de 2017

[23] _____., _____ . Cabecera de Autenticación. s.l. IETF, 2005. RFC 2402. [en línea, acceso en 01 de marzo de 2017].

[24] JOHNSON, D., PERKINS, C., ARKKO, J. Mobility Support in IPv6. S.l.: IETF, 2004. RFC 3775 [en línea, acceso en 01 de marzo de 2017].

Figura 10. Formato de mensajes ICMPv6



Fuente: https://tools.ietf.org/html/rfc2463

Los espacios usados por el protocolo indican lo siguiente. Según el rfc el espacio “tipo” indica el tipo de mensaje y además indica el formato de los datos; el campo de “código” dependerá del tipo de mensaje y es usado para dar granularidad a los tipos de mensajes y el campo “checksum” se usa para corroborar errores.

Los mensajes definidos para la especificación básica son:

- destino inalcanzable: mensaje de error atribuible a cinco causas definidas por los códigos 0 sin ruta de destino, código 1 comunicación prohibida administrativamente, código 2 sin definir, código 3 dirección no alcanzable, código 4 puerto no alcanzable;
- paquete demasiado grande: mensaje de error que le indica a la fuente que la MTU no puede pasar el paquete;
- tiempo excedido: mensaje de error atribuible a dos causas definidas por el código 0 límite de saltos excedido y código 1 tiempo de fragmentación excedido;
- problemas de parámetro: mensaje de error atribuible a tres causas, con código 0 campo erróneo de cabecera, código 1 tipo de cabecera siguiente desconocida y código 2 opción IPv6 desconocida;
- solicitud de eco: mensaje informativo solicitando respuesta al destino;
- respuesta de eco: mensaje informativo enviando respuesta a la fuente.

4.2.3 Descubrimiento de vecino

El descubrimiento de vecino *Neighbor Discovery* (ND) es una nueva característica en IPv6 y sería el equivalente al ARP de IPv4. Esa característica es usada para que los nodos IPv6 que usan el mismo *link* o medio compartido detecten la presencia de los otros nodos, determinando la dirección de enlace *link-local*; también puede

localizar los *routers* y mantiene en su tabla de vecinos la información de alcanzabilidad[25]

Para el uso del descubrimiento de vecinos (ND) se han definido cinco tipos de paquetes, descritos a continuación:

- solicitud de *router* o *Router Solicitation* (RS): utiliza el tipo de paquete ICMPv6 número 133 y es generado cuando una interfaz es activada;
- anuncio de router o *Router Advertisement* (RA): utiliza el tipo de paquete ICMPv6 número 134, se genera en los routers entre 4 y 1800 segundos, o como solicitud a través de la dirección multicast; también informa de otros parámetros como los prefijos, tiempo de vida, límite de salto;
- solicitud de vecino o *Neighbor Solicitation* (NS): utiliza el tipo de paquete ICMPv6 número 135 y es generado por los nodos para determinar la dirección de capa de enlace de los vecinos;
- Anuncio de vecino o *Neighbor Advertisement* (NA): utiliza el tipo de paquete ICMPv6 número 136 y es la respuesta a los paquetes de solicitud de vecino o también para indicar cambios de direcciones;
- Redirección: utiliza el tipo de paquete ICMPV6 número 137 y es usado para informar al *host* de un salto mejor para llegar a un destino.

4.3 MARCO CONCEPTUAL

Amenaza: acciones o elementos que son capaces de atentar contra la seguridad de la información.

Bit: unidad básica de información que se fundamenta en el sistema binario el cual cuenta con sólo dos dígitos el uno y el cero, de esta manera los sistemas informáticos procesan esta información para ejecutar diferentes tareas.

Byte: unidad de información la cual agrupa un total de ocho bits; se usa tanto en almacenamiento de datos como para indicar cantidad de datos transmitidos en una red.

[25] NARTEN, T., NORDMARK, E. SIMPSON, W. Neighbor Discovery for IP Versión 6 (IPv6). s.l.: IETF, 1998. RFC 2461. [en línea, acceso en 01 de marzo de 2017].

Cabecera: parte de un datagrama generalmente compuesta con la dirección de su origen y el destino, también incluye opciones que pueden contener datos de control como tipo de protocolo, calidad de servicio y otras funciones.

Capa superior: protocolo que está por encima del IPv6, por ejemplo, protocolos de transporte como TCP y UDP, de control como ICMP o enrutamiento como OSPF, BGP.

Confidencialidad: indica que la información sólo debe ser accesible a quien tenga la autorización respectiva.

Datagrama: estructura de un paquete constituida por su cabecera y carga útil.

Disponibilidad: asegurar que los datos estén disponibles cuando se requieran.

Fragmentación: capacidad de partir un paquete en unidades más pequeñas en caso de que no puedan pasar en un enlace o canal de datos.

Frame: unidad de transmisión digital que corresponde a la capa 2 o enlace de datos del modelo OSI

Integridad: indica que los datos no se alteren desde el origen.

Link o enlace: un componente o medio con el cual los nodos se pueden comunicar.

MTU: máxima unidad de transferencia; es el tamaño en bytes que pueden pasar de datos a través de un protocolo de comunicaciones.

Nodo: dispositivo que implemente o tenga una dirección IPv6.

Paquete: unidad de datos que se transmiten en una red conmutada

Protocolo IPv4: es un protocolo de datagramas no fiable, que se caracteriza por utilizar un esquema de direcciones máximo de 32 bits (4 bytes).

Protocolo IPv6: es un protocolo de datagramas no fiable, cuya principal característica es el uso de direcciones de máximo 128 bits.

Red de comunicaciones: conjunto de dispositivos informáticos con la capacidad de intercambiar información a través de señales eléctricas, ópticas o mecánicas con el fin de entregar datos, ofreciendo información a usuarios finales, servicios o recursos.

RFC o *Request For Comments*: serie de publicaciones realizada por la organización *Engineering Task Force* (IETF). Las publicaciones explican aspectos técnicos del funcionamiento de redes de comunicaciones, protocolos, procedimientos y comentarios; de esta manera se garantizan mejores prácticas de trabajo.

Riesgo: problema en potencia. En informática se relaciona con la probabilidad de que ocurra una amenaza.

Router: dispositivo conocido como computadora de enrutamiento; determina de acuerdo a una tabla maestra de rutas o protocolo de enrutamiento cómo los paquetes se encaminan de un origen a un destino.

Solapamiento u *overlapping*: sobre-escritura de un paquete por algún comportamiento no esperado en la red.

Vulnerabilidad: debilidad precisa de un dispositivo hardware o software, estos errores permiten que se puedan explotar ataques.

4.4. MARCO LEGAL

En enero del año 2009 se crea Ley 1273 DE 2009[26] para la protección de la información y de los datos permitiendo judicializar actividades que mediante el uso de medios tecnológicos afecten a individuos y empresas en Colombia. Esta legislación entra en los lineamientos de protección del protocolo IPv6, entre cuyos delitos se pueden mencionar los siguientes:

Acceso abusivo a sistemas informáticos: quien ingrese a un sistema computacional sin autorización, por ejemplo, aplicación de ingeniería social y acceso a una cuenta bancaria o de correo o uso de diccionarios de fuerza bruta para entrar a una base de datos.

Daño informático: se judicializa a la persona que borre, destruya, deteriore o altere datos de un sistema informático no necesariamente se realiza esto por cracking puede ser por vandalismo.

Hurto por medios informáticos y semejantes: en Colombia está presente este delito cuando se usan medios electrónicos para clonar tarjetas, grabar contraseñas, suplantar el usuario y robar dinero o información.

Interceptación de datos: uso de medios tecnológicos para copiar información que se transmita. Ejemplo: hacer una captura por *snifer* sin permiso.

Obstaculización de sistema informático o red de telecomunicaciones: quien impida el acceso a los dispositivos o canales de comunicación. Un ejemplo típico es un ataque de negación de servicio.

Suplantación de sitios web para captura de datos personales: este delito más conocido como *phising* y consiste en suplantar una página legal, por ejemplo, de un banco para tratar de sustraer la información verdadera del usuario.

[26] Colombia. CONGRESO DE LA REPÚBLICA. Ley 1273 (05, ENERO, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. No. 47.223.

Transferencia no consentida de activos: delito en el cual el agresor transfiere activos de cuentas ajenas. En este sentido, la ley protege activos afectados de usuarios a quienes, por ejemplo, se les engañe para que entreguen su información a un tercero.

Uso de software malicioso: se condena a quien cree, distribuya o venda, software que pueda afectar servicios informáticos como virus, troyanos, zombies, bombas lógicas, gusanos, *exploit*, etc.

Violación de datos personales: se condena a quien capture información personal que puede ser de tipo financiero y realice actividades ilícitas como robo de tarjetas o chantajes.

5. DISEÑO METODOLÓGICO

La metodología utilizada fue de tipo cuantitativa experimental[27], esta se fundamenta en la recolección de datos a través de laboratorios y escenarios de pruebas usando el protocolo IPv6. Estas capturas de tráfico fueron los paradigmas cuantitativos que sirven como pruebas de la investigación de diseño experimental.

5.1 POBLACIÓN, MUESTRA Y MUESTREO

La población involucrada en el proyecto son los paquetes que usan el protocolo IPv6 independiente del entorno de funcionamiento, es decir, puede ser paquetes de una red de área local *local*, área *network* o una red de área amplia *wide* área *network*.

La muestra se tomará de las capturas de paquetes realizadas a los equipos en la red en un entorno tecnológico controlado. El muestreo estará basado en los diferentes tipos de información que pueden ser generados por las herramientas de ataques como de los mismos dispositivos ubicados en el laboratorio o entorno tecnológico.

5.2 MÉTODOS, TECNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El método empleado para desarrollar el proyecto se basó en la investigación del funcionamiento del protocolo IPv6. Posteriormente, con este conocimiento, se realizó un diseño de un laboratorio que permitió probar vulnerabilidades que presenta el protocolo.

Las herramientas utilizadas se instalaron bajo una máquina utilizando el sistema operativo Kali Linux, estas son:

- Virtual Box: *software* de virtualización que permite instalar máquinas de arquitecturas x86/amd64. De esta manera se puede disponer de dispositivos para pruebas sin la necesidad de invertir en nuevo *hardware*[28] .

[27] S.N. Tipos de estudio [en línea], 28 de agosto de 2012 [revisado 18 de noviembre 2017]. Disponible en Internet: http://www.tiposde.com/ciencia/estudio/tipos-de-estudio.html

[28] VirtualBox. [página WEB]: Oracle [revisado 18 de noviembre de 2017]. Disponible en Internet: https://www.virtualbox.org

- IPv6 Toolkit: grupo de pruebas para realizar evaluación de la seguridad en dispositivos que usen IPv6, este paquete cuenta con varias herramientas, las cuales incluyen envió al azar de paquete de descubrimiento de vecinos (ND) y una herramienta de búsqueda de equipos[29].
- THC-IPv6 Toolkit: reconocido grupo de herramientas que explotan las debilidades inherentes del protocolo IPv6 e ICMPv6; incluyen una gran librería de paquetes construidos[30].
- Sniffer Wireshark: herramienta que permite capturar y analizar tráfico además de identificar su estructura y contenido[31].

La recolección de datos se hará en un entorno tecnológico controlado usando un dispositivo marca Juniper *model* srx-100 que junto a las demás herramientas se evidenciará los ataques empleados y con este análisis generar las recomendaciones de la seguridad que apliquen.

5.3 PLAN DE PROCESAMIENTO Y ANALISIS DE DATOS

En la validación de datos se usaron las capturas presentadas por los analizadores de tráfico para observar los comportamientos generados por los dispositivos. Se revisó de qué forma afectó un ataque el desempeño de la red en cualquier ambiente de área local o área remota. Finalmente se documentaron estas pruebas y se generaron recomendaciones.

5.4 METODOLOGÍA DE DESARROLLO

Para cumplir los objetivos las actividades desarrolladas en la metodología fueron:

1) Estudio, revisión y lectura del estado de arte actual sobre el protocolo IPv6 incluyendo la RFC tanto de seguridad como el funcionamiento del protocolo IPv6. De esta manera se identificaron las vulnerabilidades más recurrentes con el protocolo IPv6.

[29] SI6 Networks IPv6. Toolkit. [en línea] s.f. [revisado 18 de noviembre de 2017]. Disponible en: https://www.si6networks.com/tools/IPv6toolkit

[30] THC IPv6 Toolkit [página WEB]: s.f. [revisado 18 de noviembre de 2017]. Disponible en Internet: https://www.thc.org/thc-IPv6

[31] Wireshark [página WEB]. s.f. [revisado 18 de noviembre de 2017]. Disponible en Internet: https://www.wireshark.org

2) Diseño de esquema de pruebas basado en un laboratorio, el cual contó como mínimo con tres dispositivos de estudio: uno o varios hosts de servicio; un host cliente y una máquina atacante.

3) Ejecución de los ataques en ambos ambientes local y remota. Se capturaron los datos, anotó que no todos los ataques fueron factibles en este laboratorio y por lo tanto se documentó el posible motivo.

4) Se documentaron y analizaron los resultados obtenidos del laboratorio.

5) Se generaron las recomendaciones para fortalecer la red IPv6 ante la vulnerabilidad.

6) Se capturaron datos y documentaron en el trabajo de grado.

7) Se realizó el montaje de la página web con las evidencias recolectadas.

Los elementos utilizados en el desarrollo de actividades se presentan en el siguiente cuadro:

Cuadro 2. Componentes utilizados

Componentes hardware	Características
Laptop Hp con Windows 10 Home single language	Sistema x64, 16 GB de RAM, procesador i7-6700HQ 2,68GHz
Raspberry pi 3 Model B	Procesador ARMv8 de x64, velocidad 1.6Ghz, 1GB de RAM, puerto ethernet, bluetooth
Router Juniper SRX-100	CAVIUM's Octeon CPU Rev. 0.1, FreeBSD/SMP: Multiprocessor System Detected: 2 CPUs
Virtual machine Windows 7 o Ubuntu	Sistemas operativos virtualizados
Virtual machine Kali linux	Sistema operativo virtualizado

Fuente: autor

Para las actividades anteriores se propuso el siguiente cronograma para cumplir con el desarrollo metodológico antes enunciado.

Cuadro 3. Cronograma de actividades

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8
Estudio RFC protocolo IPv6	x							
Prueba de vulnerabilidades		x	x					
Captura de evidencias		x	x	x				
Análisis y documentación				x	x			
Generación de recomendaciones					x	x		
Documentación de resultados							x	
Crear página web							x	
Entrega de trabajo de grado								x

Fuente: autor

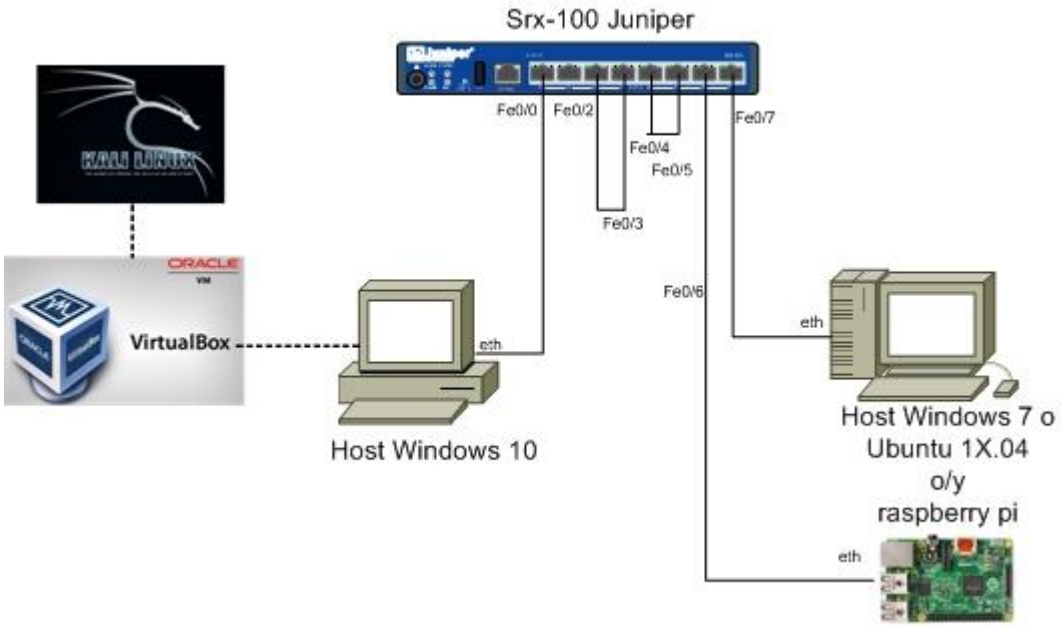
6. DISEÑO E IMPLEMENTACION

6.1 LABORATORIO DE PRUEBAS Y HERRAMIENTAS

El objetivo de trabajar con un ambiente tecnológico controlado es simular una red IPv6 sin mecanismos de transición - sin túneles IPv4-IPv6, 6to4 o Dual Stack -; este no tendrá mecanismos de protección para que los paquetes pasen de manera transparente y lograr observar el comportamiento del protocolo.

Además de promover la captura con un sniffer y observar las reacciones en cuanto ataques se consideraron los dos ambientes de red utilizados: la red de área local (LAN) y red de área remota (WAN). Para ello se utilizó la funcionalidad de *router* virtuales para simular la red de área amplia y la función de *switching* para la red de área local. A continuación, se muestra la propuesta de topología física a implementar; en la figura 10 se indica la distribución física usada en la que se conectan los tres componentes requeridos como son: las máquinas de servicio, cliente y victima donde hay un equipo Juniper srx-100 y que además soporta el protocolo IPv6.

Figura 11. Topología física propuesta

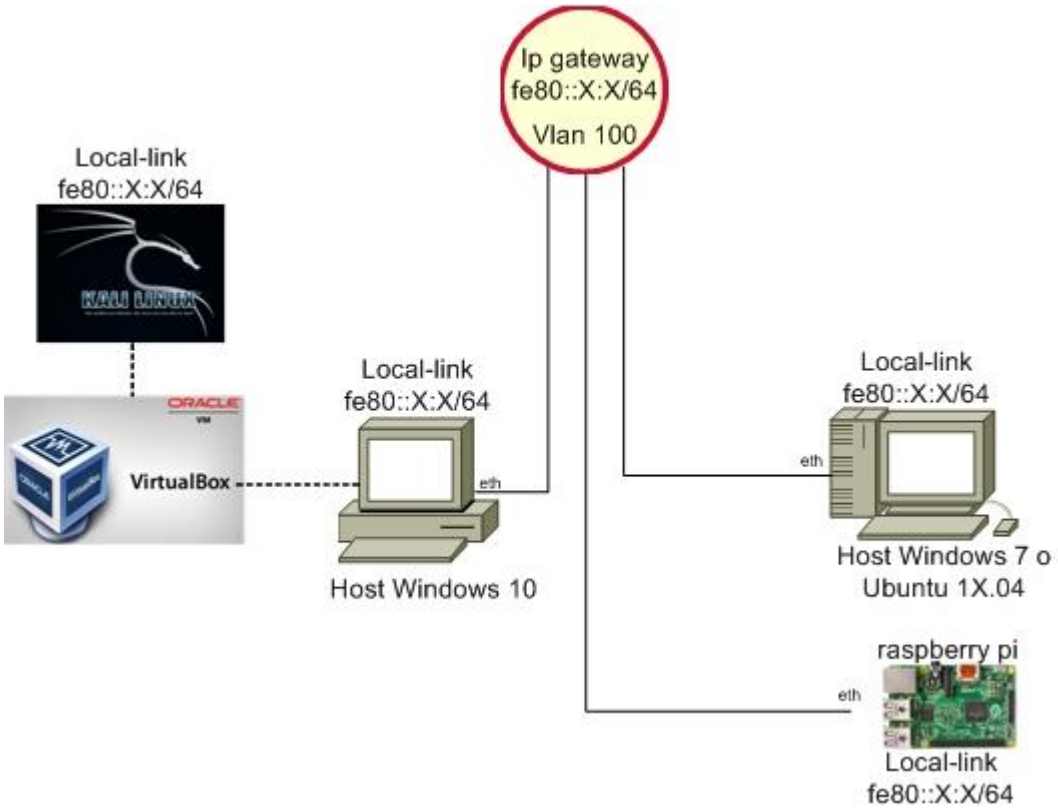


Fuente: autor

6.1.1 Esquema de prueba en área local LAN

La versatilidad de la topología física permite simular un ambiente de área local utilizando la función de *switching* en el equipo SRX-100. El escenario LAN es uno de los más vulnerables porque permite la comunicación directa entre dispositivos sin la necesidad de atravesar un dispositivo adicional. En ese escenario, por ejemplo, no hay un *firewall* que inspeccione el tráfico o un *routers* que redireccione los paquetes entre las redes, esto permite que sea factible de que un atacante conectado a este escenario pueda ser una amenaza. La figura 11 muestra la propuesta lógica configurada en la cual se usan únicamente direcciones de enlace local *local-link* y con una puerta de enlace *Gateway*, configurado sobre el equipo Juniper srx-100 (la configuración del equipo juniper se adjunta en el anexo A).

Figura 12. Topología lógica LAN



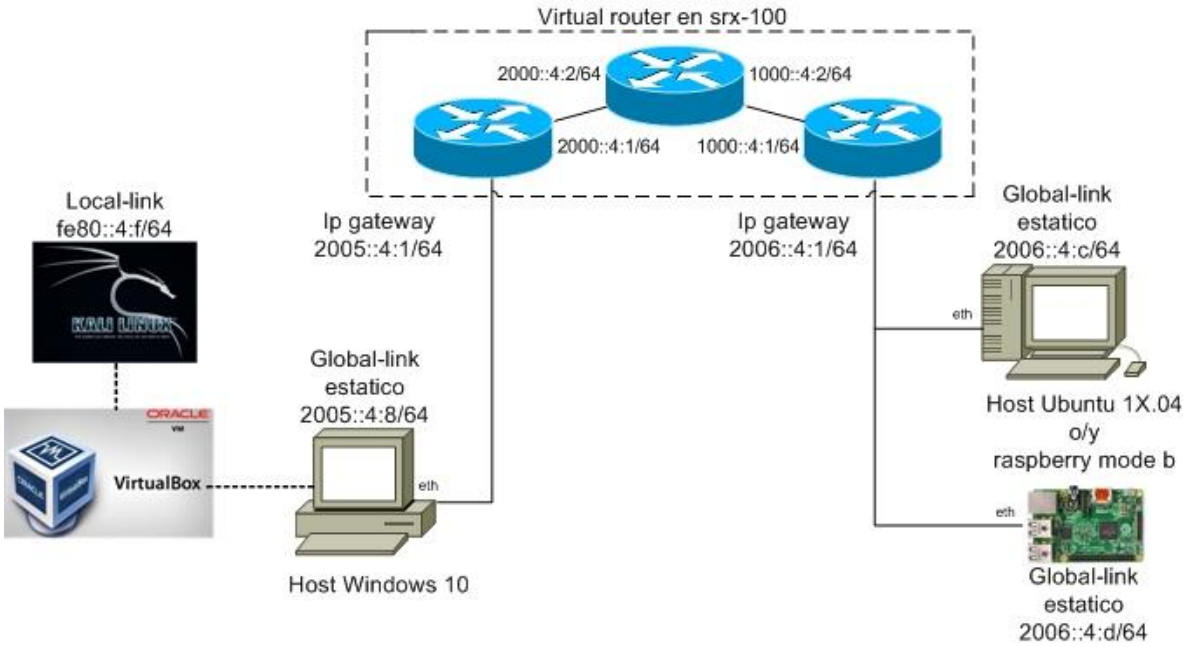
Fuente: autor

6.1.2 Esquema de prueba en área remota

Se considera un escenario de área remota para las pruebas porque es el habitual que un atacante realice pruebas o ataques a otra red de un área distante desde una red externa. La versatilidad de la topología física permite configurar una red de área remota sobre el *router* Juniper srx-100 usando la funcionalidad de *routers* virtuales

con la cual se simulan tres enrutadores en el ambiente tecnológico. La configuración del equipo se adjunta en el anexo B. La figura 13 ilustra el direccionamiento utilizado, usando un esquema con direcciones globales, *global-link*.

Figura 13. Topología lógica Wan



Fuente: autor

Como se observa, la distribución de los tres *routers* virtuales simula una red que permitirá el alcance de redes ubicadas en dos entornos LAN diferentes.

En los ambientes tecnológicos se tiene un *host* con sistema operativo Windows 10 el cual contiene una máquina virtual; el SO operativo Kali Linux contiene un kit de herramientas de ataques para IPv6; y en el lado de las víctimas se cuenta con un Raspberry Model B y *host* que podemos intercambiar usando SO Windows 7 o Ubuntu Linux.

6.2.1 Ficha técnica de equipo Juniper SRX-100

La serie de equipos de seguridad SRX del fabricante Juniper ofrecen capacidades de conectividad, seguridad y manejo de gran cantidad de usuarios. Esos equipos

también cuentan con funciones tanto de *switching*, *routing* y *next generation firewall* todo ello en un sólo dispositivo y reforzado por el sistema operativo JUNOS[32].

El producto utilizado en el laboratorio modelo SRX-100 contiene en su hardware los siguientes elementos:

- ocho puertos ethernet 10/100 y un puerto USB;
- 2 GB DRAM, 2 GB de memoria Flash;
- completa funcionalidad UTM, antivirus, antispam, filtrado web y de contenido y sistema de detección de intrusos.

El equipo también cuenta con las siguientes especificaciones en software:

- uso de protocolos IPv4, IPv6, CLNS;
- protocolos de enrutamiento BGP, OSPF/OSPFv3, IS-IS, Multicast, RIPv2+v2, MPLS;
- encapsulamiento ethernet mac y etiquetas en vlans 8021q;
- capa 2 switching RSTP, MSTP, 802.3ad, IGMP snooping;
- firewall, IPS, APsecure Firewall, Antivirus.

6.2.2 Herramienta de *pentesting* IPv6

Para el *pentesting* se pusieron a prueba dos juegos de herramientas que contienen un grupo de pruebas para comprobar vulnerabilidades en el protocolo IPv6 estas son: IPV6 ToolKit creado por empresa SI6Networks y Thc-IPv6 toolkit creado por Thc. Además de usar una máquina atacante Kali Linux y se capturaron paquetes para el análisis con el *sniffer Wireshark*. A continuación, se describen las herramientas y dónde obtenerlas.

6.2.2.1 IPv6 Toolkit

Este grupo de herramientas tiene la capacidad de enviar una gran cantidad de paquetes basados en el protocolo IPv6. La versión instalada en Kali Linux es la v 1.2.3 se puede situar en cualquier plataforma que soporte FreeBSD, NetBSD, OpenBSD, Linux o Mac OS[33].

Las principales herramientas contenidas en este kit son:

---

[32] SRX Series services gateways for the branch - Juniper especifications SRX-100 [en línea, revisado 18 de noviembre de 2017]. Disponible en Internet: https://www.juniper.net/assets/kr/kr/local/pdf/datasheets/1000281-en.pdf.

[33] SI6 Networks IPv6. Toolkit. [en línea] s.f. [revisado 18 de noviembre de 2017]. Disponible en: https://www.si6networks.com/tools/IPv6toolkit

- Flow6: envía paquetes de prueba a nodos objetivo evaluando la seguridad del espacio en IPv6 *flow label*.
- Frag6: realiza ataques basados en la fragmentación de paquetes IPv6.
- Icmp6: prueba ataques basados en los mensajes de error de ICMPv6.
- Jumbo6: evalúa fallas en manejo de Jumbograms IPv6
- Na6: envía mensajes *Neighbor Advertisement* (NA).
- Ni6: envía mensajes de información de nodo con ICMPv6 y evalúa fallas en el procesamiento de los paquetes.
- Ns6: envía mensajes *Neighbor Solicitation* (NS)
- Ra6: envía mensajes *Router Advertisement* (RA)
- Rd6: envía mensajes de redirección ICMPv6
- Rs6: envía mensajes *Router Solicitation* (RS)
- Scan6: escanea y busca direcciones IPv6
- Tcp6: envía segmentos TCP y permite ejecutar varios ataques basados en TCP

6.2.2.2 THC-IPv6 Toolkit

Este juego de herramientas desarrollado por The Hackers Choice (THC) es un grupo de *pentesters* que desarrollan pruebas de seguridad. El foco de estas herramientas es encontrar fallas y documentarlas para garantizar que la red y la información sean aseguradas. En la Kali Linux se instaló la versión 3 liberada en marzo de 2016[34].

El juego de herramientas puede evaluar varios tipos de vulnerabilidades y realizar ataques como Hombre en el medio, falso NS, falso NA y negación del servicio. Dentro de sus herramientas podemos mencionar:

- Implementation6: ejecuta una verificación en la implementación de IPv6; puede validar algunas características de Firewall y evaluar su seguridad;
- Alive6: muestra direcciones IPv6 vigentes en un segmento;
- Toobig6: implanta un paquete con una MTU específica a un objetivo;
- Trace6: realiza un *traceroute6* rápido y soporta paquetes ICMPv6 reply y TCP-SYN;
- Parasite6: utiliza los mensajes ICMP *Neighbor solicitation*/*advertisement* para aplicar técnicas de suplantación en ataques de hombre en el medio;
- Dnsdict6: enumera un dominio a través de paquetes DNS con fuerza bruta;
- Fake_router6: envía anuncios falsos como si fuera un *router* e intenta ser el *router* por defecto;

[34] THC IPv6 Toolkit [página WEB]: s.f. [revisado 19 de noviembre de 2017]. Disponible en Internet: https://www.thc.org/thc-IPv6

- Redir6: instala una ruta en una *host* víctima y redirige el tráfico a un nuevo host o *Gateway*;
- Detect-new-ip6: detecta un dispositivo activo con IPv6 que se encuentre en una red local;
- Dos-new-ip6: detecta equipos con IPv6 y evita que sus interfaces lleguen a estar activas mediante un ataque de negación de servicio DoS;
- Flood_router6: llena una red local de anuncios de *Router Advertisements* (RA);
- Flood_advertise6: llena una red local de anuncios Neighbor Advertisements (NA);
- Fuzz_ip6: crea paquetes difusos ICMPv6

6.2.2.3 *Sniffer Wireshark*

Un *sniffer* es una herramienta que permite realizar un análisis pasivo, no altera el funcionamiento de los paquetes que pasan en una red. *Wireshark* es el tipo de *sniffer* más conocido porque ofrece un análisis minucioso de los paquetes y protocolos, y porque tiene una interfaz gráfica de fácil uso.

Wireshark es un software libre y es además compatible con varios sistemas operativos con Base en Unix como son: Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Android y Mac OS también en Microsoft Windows puede ser instalado. Dentro de sus cualidades se destacan:

- soporte a más de 480 protocolos incluido IPv6;
- reconstrucción de sesiones TCP;
- capacidad de traducción de protocolos TCP IP;
- robustez en modo promiscuo y en modo no promiscuo;
- mantenimiento bajo licencia *General Public License* (GPL)

7. ANALISIS DE ATAQUES A REDES IPV6 Y RESULTADOS

Con las topologías definidas del entorno tecnológico controlado se realizaron las pruebas junto al análisis de los resultados. Para ello realizamos nueve *test* de penetración usando tanto la red de área local y como la de área remota. Una vez se ejecutadas las pruebas realizamos un análisis de los resultados.

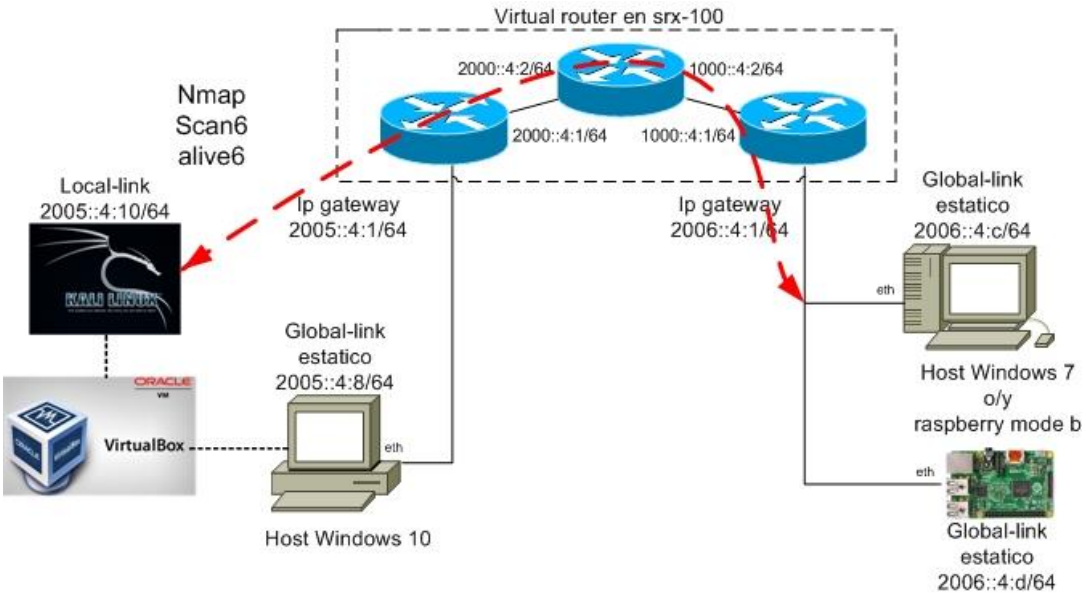
El método utilizado en cada una de las pruebas fue: ejecutar el ataque, tomar las muestras de los paquetes, hacer capturas de los comportamientos en máquinas víctimas y analizar los resultados obtenidos.

Los ataques ejecutados según las técnicas definidas fueron: ataques de escaneo o reconocimiento, fragmentación, hombre en el medio, negación de servicio y las pruebas de explotación de vulnerabilidades.

7.1 ATAQUES DE ESCANEO O RECONOCIMIENTO

El escaneo de puertos es una técnica usada para identificar equipos en una red de la cual no se tiene información (caja negra) y se considera como una fase inicial antes de empezar a utilizar otro tipo de ataques. Una red IPv6 no deja de ser vulnerable a este tipo de técnicas en la cual, con paquetes TCP-SYN, intenta identificar los componentes de una red. En la figura 14 se ilustra la forma como se realiza una secuencia de ataque de reconocimiento usando las herramientas Nmap, scan6 y alive6.

Figura 14. Topología de ataque de reconocimiento WAN



Fuente: autor

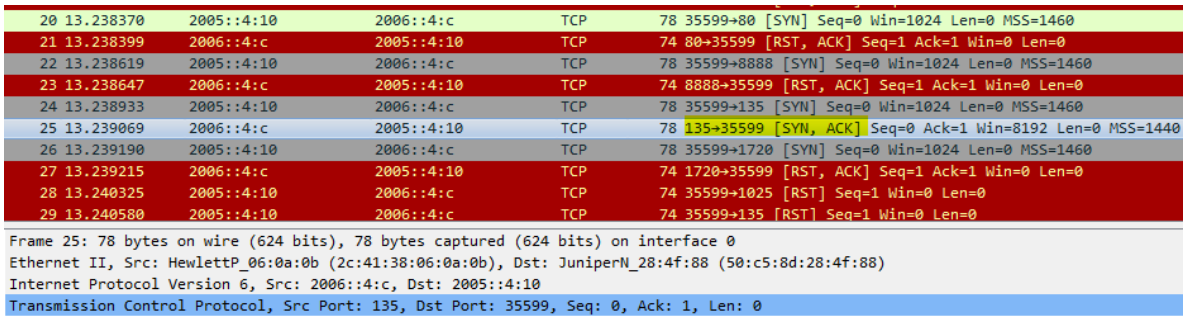
Con el comando descrito en la figura 15 se realiza un escaneo de puertos hacia el *host* victima IPv6 2006::4:c/64. En la figura 16 se capturan los paquetes TCP-SYN y se resalta la respuesta encontrada en el puerto 135. La máquina victima tiene Windows 7.

Figura 15. Ataque y reconocimiento de puertos de host

```
root@kali:~# nmap -6 2006::4:c

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-28 21:40 EST
Nmap scan report for 2006::4:c
Host is up (0.0017s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
445/tcp  open     microsoft-ds
1025/tcp open     NFS-or-IIS
1026/tcp open     LSA-or-nterm
1027/tcp open     IIS
1028/tcp open     unknown
1029/tcp open     ms-lsa
1034/tcp open     zincite-a
5060/tcp filtered sip
5357/tcp open     wsdapi

Nmap done: 1 IP address (1 host up) scanned in 36.75 seconds
root@kali:~#
```

Fuente Autor

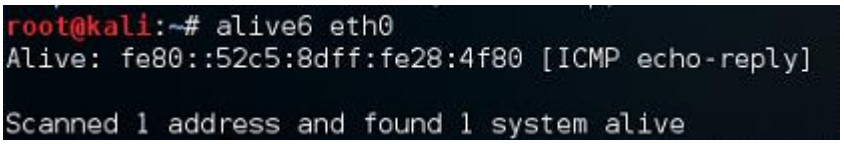
Figura 16. Recepción de paquetes TCP-SYN con Nmap



Fuente: autor

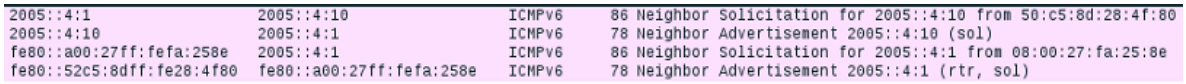
En el entorno WAN se realiza también prueba con la herramienta alive6, pero se evidencia que únicamente detectó la dirección de *link-local* del *router* Juniper srx-100 el resultado se muestra en la figura 17. Los paquetes que envía la herramienta son un *Neighbor Solicitation* (ND) de la máquina atacante a la red y cuyo resultado es un *Neighbor Advertisement* (NA) del equipo Juniper srx- 100 (ver figura 18).

Figura 17. Resultado de herramienta alive6 en ambiente WAN



Fuente Autor

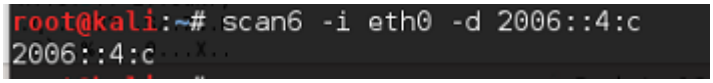
Figura 18. Paquetes usados con herramienta alive6



Fuente: autor

Como prueba final se usó la herramienta scan6, no obstante, se comprueba que únicamente genera ICMPv6 *request* e ICMPv6 *reply* hacia el destino y no prueba de manera diferente la red. En la figura 19 se muestra el resultado en la máquina que usa Kali Linux. En la figura 20 se capturaron con *wireshark* los paquetes usados ICMPv6.

Figura 19. Paquete enviado con scan6



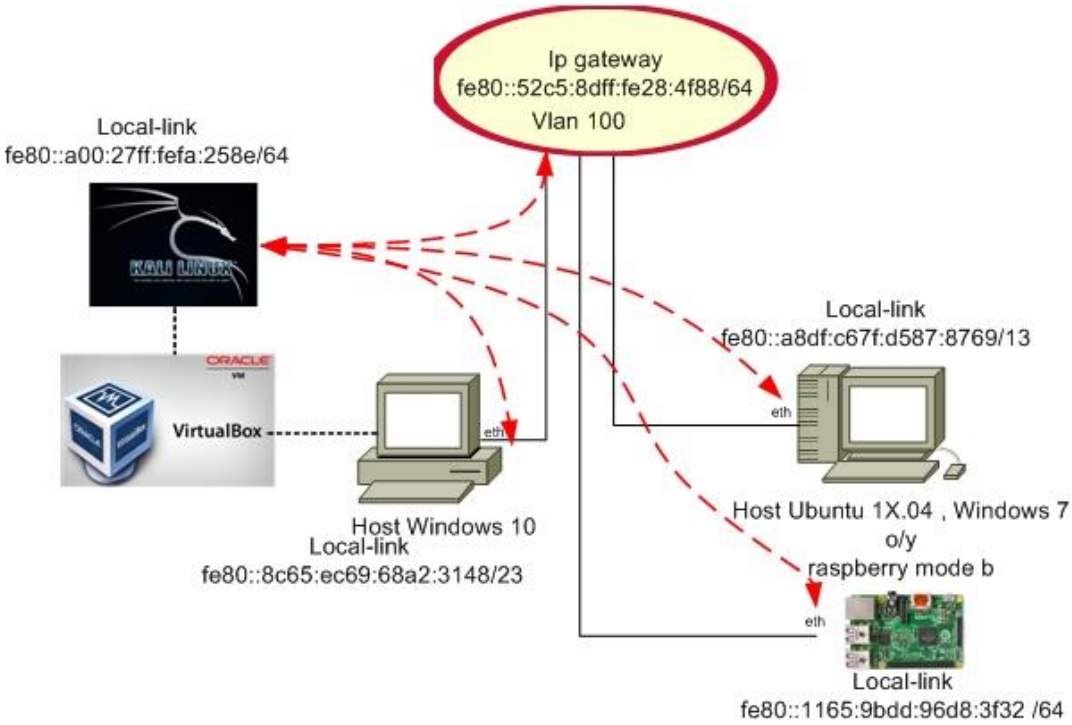
Fuente: autor

Figura 20. Captura de tráfico desde Atacante usando la herramienta scan6

Fuente: autor

En el entorno de pruebas de red de área local se configuró el ambiente únicamente con las direcciones de *link-local* generadas por configuración automática de dirección sin estado (SLAAC). La topología quedó configurada como se observa en la figura 21.

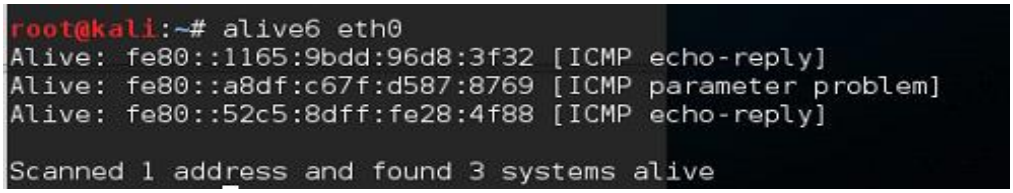
Figura 21. Topología de pruebas LAN



Fuente: autor

Al utilizar la herramienta alive6 se observa con resultado positivo que se descubren los vecinos en el segmento de red (ver figura 22).

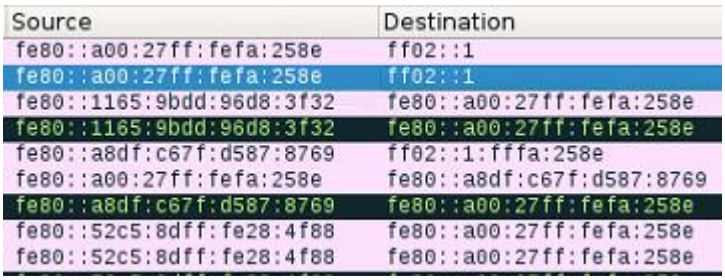
Figura 22. Descubrimiento de vecinos mediante herramienta alive6



Fuente: autor

Al revisar los paquetes capturados por *wireshark* se observa que la herramienta envía inicialmente un paquete al grupo de *multicast* de enlace-local definido como todos los nodos (*all-nodes*) ff02::1, ver figura 23.

Figura 23. Paquete *all-nodes* usado en herramienta alive6



Source	Destination
fe80::a00:27ff:fefa:258e	ff02::1
fe80::a00:27ff:fefa:258e	ff02::1
fe80::1165:9bdd:96d8:3f32	fe80::a00:27ff:fefa:258e
fe80::1165:9bdd:96d8:3f32	fe80::a00:27ff:fefa:258e
fe80::a8df:c67f:d587:8769	ff02::1:fffa:258e
fe80::a00:27ff:fefa:258e	fe80::a8df:c67f:d587:8769
fe80::a8df:c67f:d587:8769	fe80::a00:27ff:fefa:258e
fe80::52c5:8dff:fe28:4f88	fe80::a00:27ff:fefa:258e
fe80::52c5:8dff:fe28:4f88	fe80::a00:27ff:fefa:258e

Fuente Autor

7.1.1 Análisis de resultados

- Con el uso de la herramienta nmap es factible ubicar servicios activos que usen TCP, además de nodos o *host*, en un segmento de red IPv6 sin importar que sea una red de área remota o área local. Sin embargo, si la longitud del prefijo es muy grande /64 implica escanear 1,8x10e19 *host* lo cual complica o complejiza el ataque.

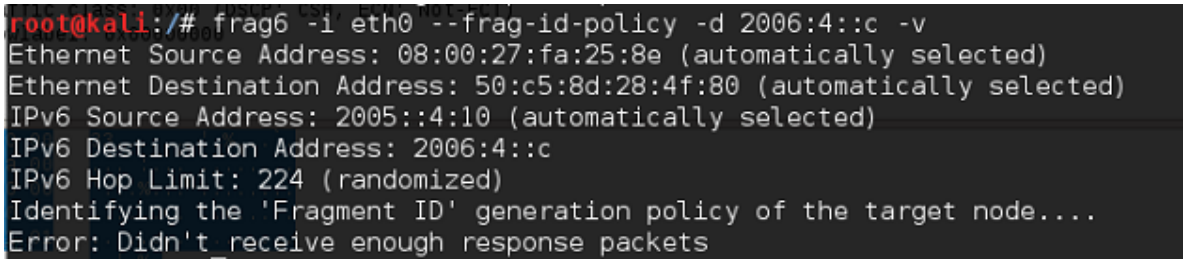
- Un entorno de red de área local es más vulnerable al ser identificados sus componentes usando la dirección multicast ff02::1. Esto porque, como se evidenció, en el laboratorio los *hosts* responden a este tipo de mensajes y el atacante podría una vez identifique componentes avanzar con otra técnica de ataque.

- En la red de área amplia el paquete *multicast* no atravesó los demás segmentos de red, por lo tanto, este tipo de reconocimiento es más difícil de efectuar en estas topologías.

7.2. ATAQUES DE FRAGMENTACIÓN

En IPv6 la fragmentación de paquetes únicamente se permite entre equipos terminales. Las pruebas se realizaron utilizando la topología de área remota descrita en la figura 14; el objetivo de las pruebas fue validar si los sistemas operativos de las víctimas generaban paquetes o respuestas no deseadas al enviar diferentes paquetes fragmentados o fuera de orden; en la prueba se enviaron paquetes fragmentados inferiores de una MTU 1280 Bytes como se muestra en la figura 24.

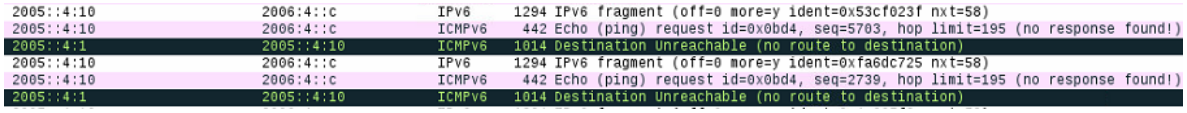
Figura 24. Uso de herramienta frag6



Fuente: autor

En esta prueba los paquetes no salen de la puerta de enlace ya que el equipo Juniper srx-100 descartó estas tramas y no las direccionó en el ambiente de área remota. La captura se observa desde la máquina atacante sin respuestas de la víctima.

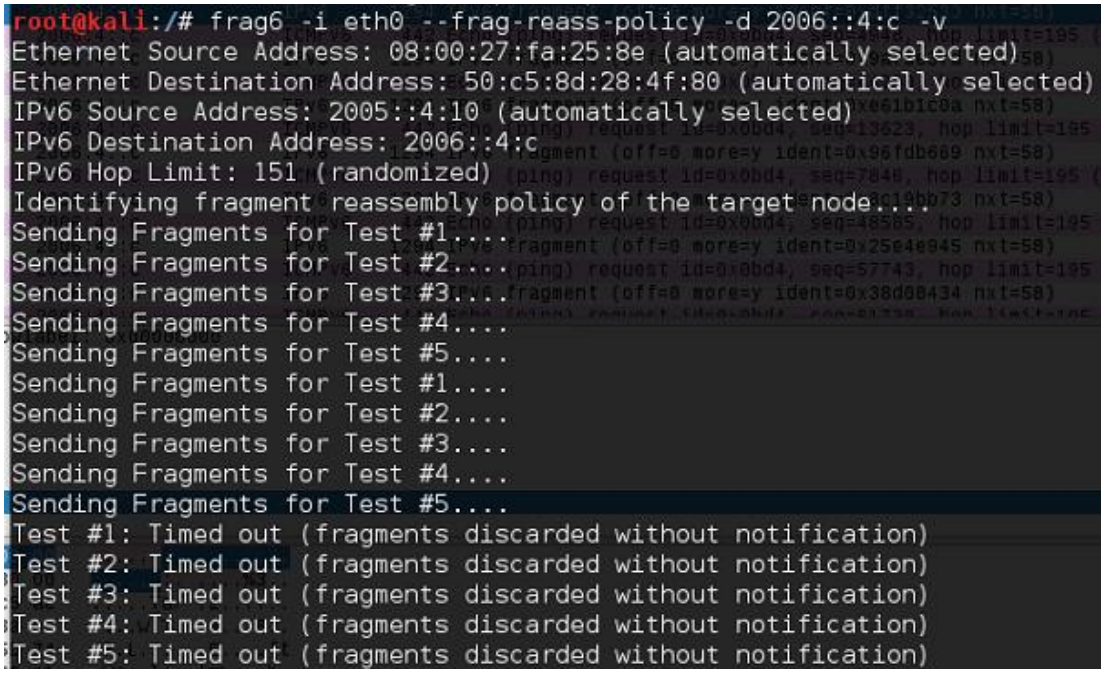
Figura 25. Paquetes enviados con política frag6



Fuente: autor

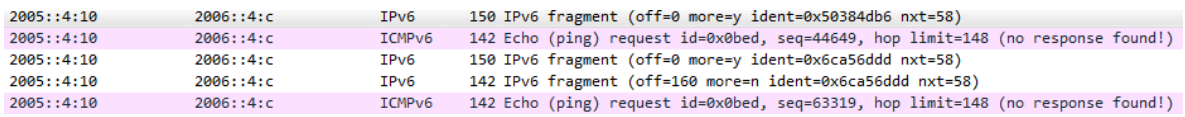
Como ilustran las figuras anteriores, no llega el paquete a la máquina victima prueba en Windows 7.

Figura 26. Uso de política de re-ensamble frag6



Fuente: autor

Figura 27. Paquetes fragmentados y re-ensamblados en destino



Fuente: autor

7.2.1 Análisis de resultados

- Este tipo de ataques dependerán de una mala implantación del *stack* IPv6 en los *host* o nodos. En el laboratorio no se evidenció respuesta anormal ya que los equipos ignoraron este tipo de paquetes. La intención de este tipo de ataque es generar respuestas no deseadas y que indispongan los servicios.

- Utilizando equipos actualizados el *stack* IPv6 no podría ser vulnerable, sin embargo, este tipo de *test* puede permanecer vigente si se encuentran equipos desactualizados. Por lo tanto, no se debe descartar realizar este tipo de pruebas para generar recomendaciones.

7.3 ATAQUES DE IP *SPOOFING*

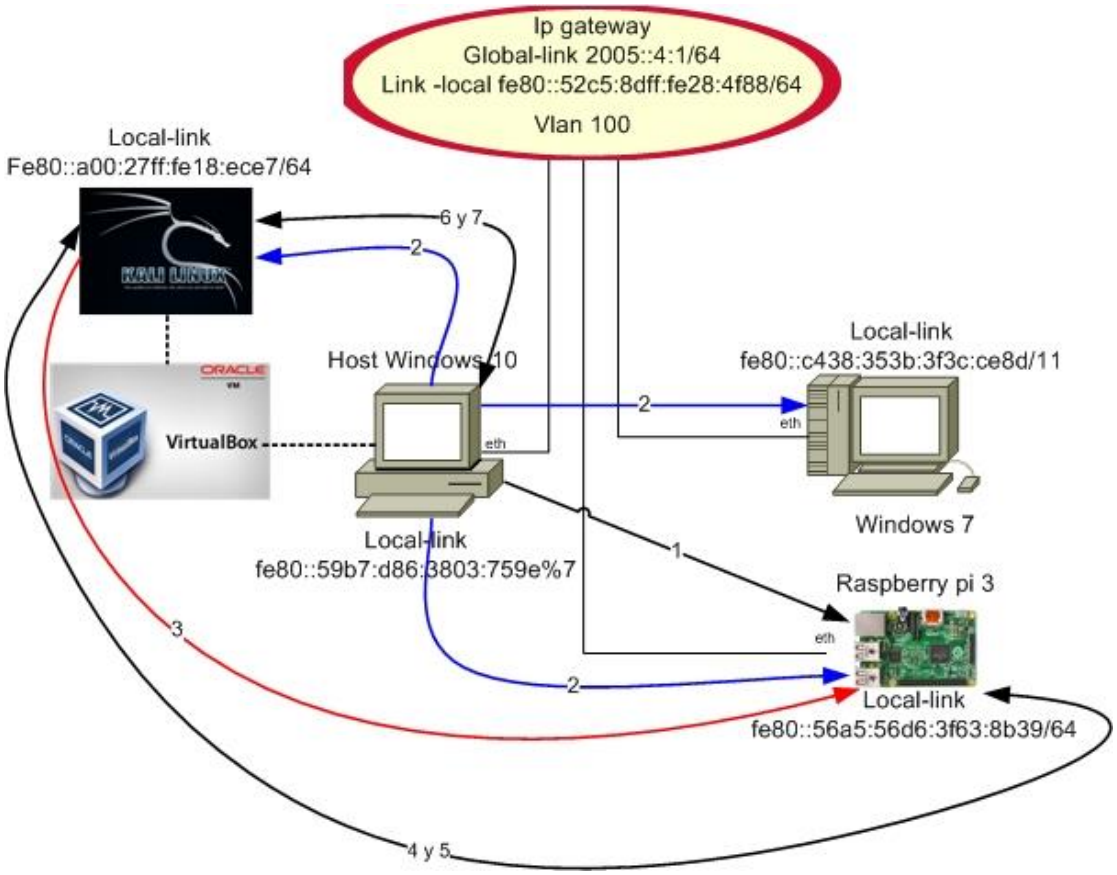
Los ataques de suplantación de identidad conocidos como ip *spoofing*, son factibles en redes IPv6. Para demostrarlo se realizaron pruebas en el laboratorio, las cuales se mencionan a continuación.

7.3.1 Ataque con redirección de tráfico en ambiente LAN

Cuando una *host* requiere conocer dónde está localizada su puerta de enlace o comunicarse con otro *host* usando IPv6 en un ambiente LAN es obligatorio conocer la dirección Mac del destino. Para esto se utilizan las peticiones multicast a través de ICMPv6 (no existen direcciones broadcast como en IPv4). Esto representa una oportunidad para que el atacante pueda realizar una suplantación o ataque de hombre en el medio permitiendo que el tráfico del *host* víctima se redirija a la atacante (ver figura 28). La secuencia del ataque se puede describir así:

1. envía paquete *host* victima (Windows 10) a *host* de servicio (raspberry), por ejemplo, Ping Icmpv6.
2. como no conoce destino (dirección mac) la solicitud llega a todos los *hosts* usando dirección multicast ff02::1 y máquina atacante escucha la solicitud;
3. atacante envía solicitud a *host* de servicio;
4. respuesta del *host* de servicio a víctima;
5. respuesta llega al atacante;
6. atacante envía respuesta a víctima;
7. la víctima no tiene servicio y envía tráfico al atacante.

Figura 28. Topología de prueba de ataque de hombre en el medio



Fuente: autor

Los paquetes suplantados *Neighbor Advertisement* (NA) se alteran con la herramienta parasite6 como se ilustra en la figura 29.

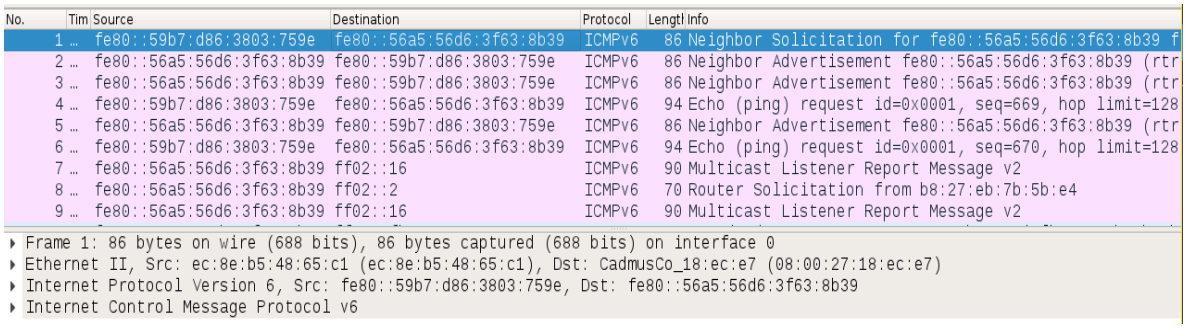
Figura 29. Uso de herramienta parasite6

```
root@kali:~# parasite6 eth0
Remember to enable routing, you will denial service otherwise:
 =>  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Remember to prevent sending out ICMPv6 Redirect packets:
 =>  ip6tables -I OUTPUT -p icmpv6 --icmpv6-type redirect -j DROP
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ...
Spoofed packet to fe80::59b7:d86:3803:759e as fe80::56a5:56d6:3f63:8b39
^[[ASpoofed packet to fe80::59b7:d86:3803:759e as fe80::56a5:56d6:3f63:8b39
```

Fuente: autor

La captura de paquetes ofrece una mejor visión de lo ocurrido en el ataque (ver figura 30). Allí es evidente que la dirección mac del *host* de servicio (raspberry) es suplantada por la de la máquina atacante (mac ec:8e:b5:48:65:c1), con lo cual se logra la redirección del tráfico.

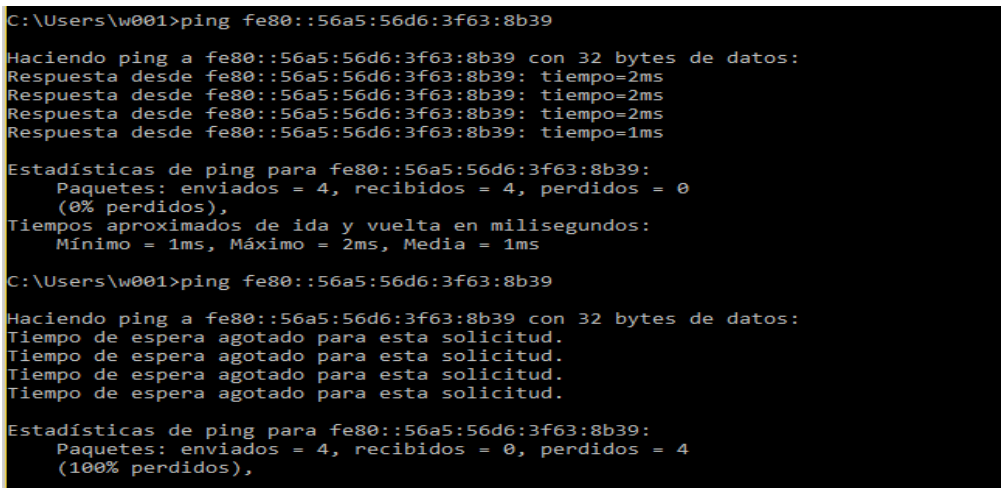
Figura 30. Captura de tráfico durante ataque con parasite6



Fuente: autor

El resultado del ataque, como se observa en la figura 31, es indisponer el servicio ya que no es factible el alcance luego de la redirección del tráfico.

Figura 31. Indisponibilidad del servicio luego de ataque de hombre de medio



Fuente: autor

7.3.1.1 Análisis de resultados

- Esta prueba fue exitosa denegando el servicio del *host* víctima y desviando el tráfico a la máquina atacante, sin embargo, el éxito de este ataque es factible solo durante el reinicio de la tarjeta de red de la víctima.

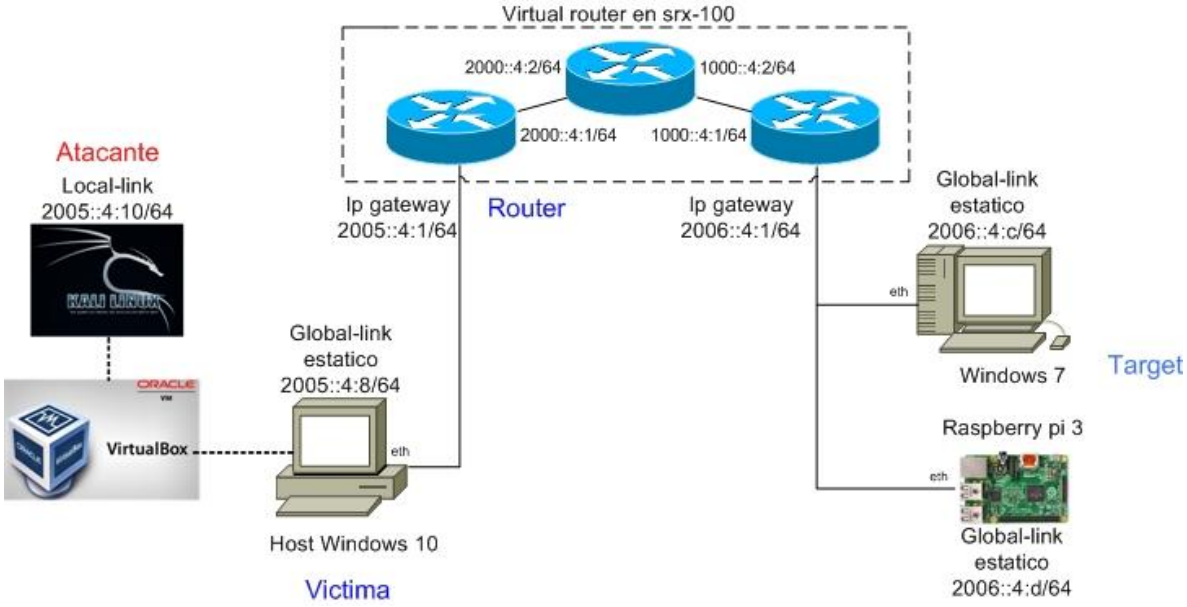
- Si las máquinas en el ambiente de área local están ya registradas, el ataque no es factible.

- La vulnerabilidad se aprovecha en el uso de los paquetes advertencia de vecino *Neighbor Advertisement* (NA), sin embargo, la herramienta parasite6 no modifica la dirección mac de origen del atacante pudiendo ser identificado.

7.3.2. Ataque con redirección de tráfico en ambiente WAN

El objetivo de este ataque es incluir en el *host* victima un falso *router* a través de un paquete de redirección ICMPv6, de esta manera las máquinas objetivo o Target redirigirán su tráfico a la máquina atacante, la topología usada es WAN. El ataque se visualiza en la figura 32.

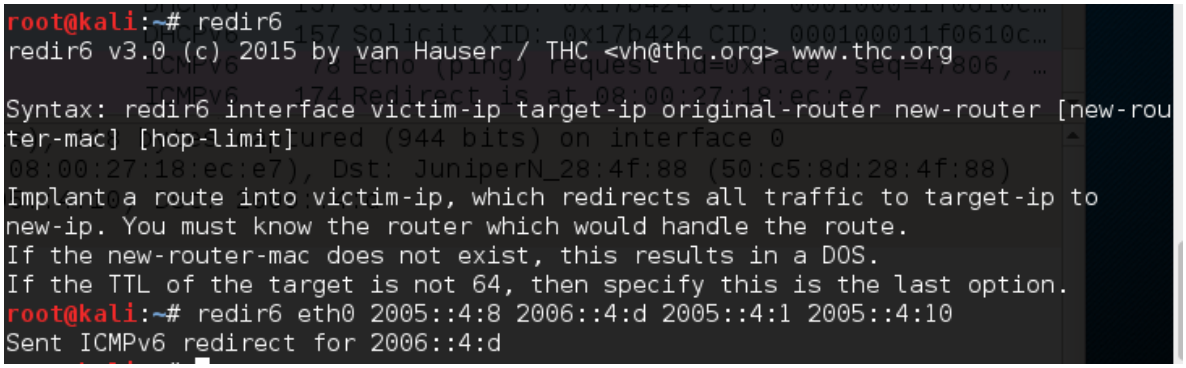
Figura 32. Topología usada con ataque de redirección



Fuente: autor

La herramienta utilizada es redir6 cuya sintaxis utilizada indica lo siguiente: definir la ip de la víctima, la ip del servicio, el router original Gateway, poner la ip del atacante (ver figura 33).

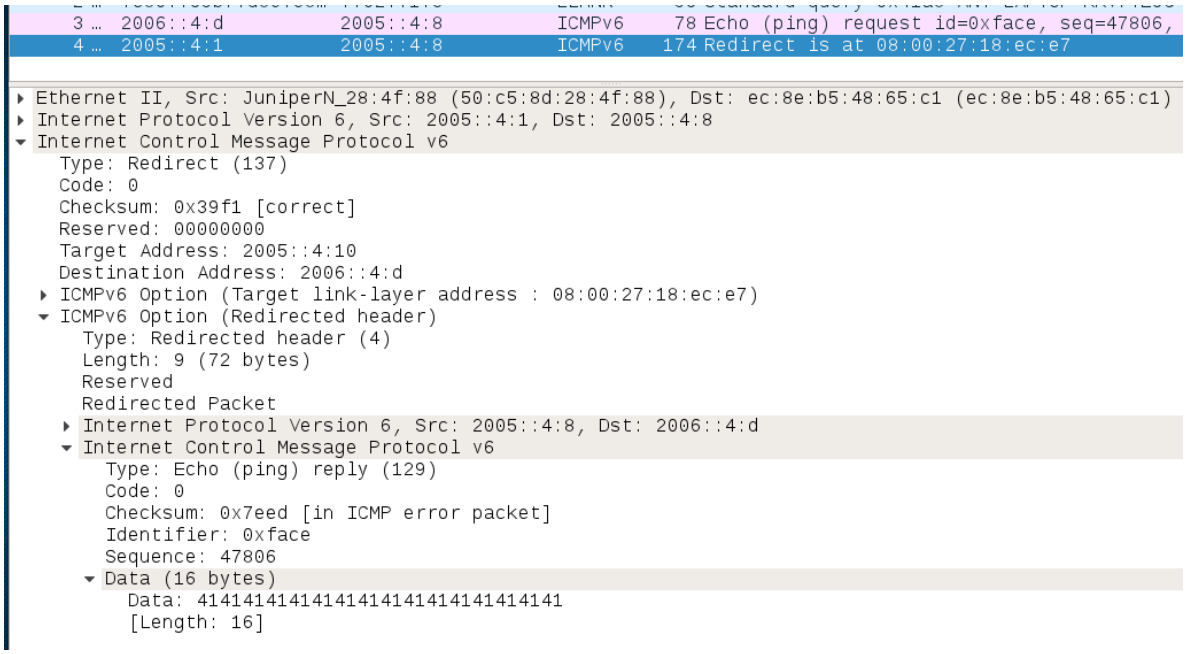
Figura 33. Sintaxis y ataque usando herramienta redir6



Fuente: autor

La captura de tráfico, ver figura 34, indica cómo se construye el paquete desde la máquina atacante, inyectando un paquete ICMPv6 Redirect sobre el *host* víctima. Sin embargo, la máquina victima que usa Windows 10 no se vio afectada y sigue llegando su tráfico sin inconvenientes lo cual indica que no es vulnerable a este tipo de ataques.

Figura 34. Captura de tráfico usando redirección ICMPv6



Fuente: autor

7.3.2.1 Análisis de resultados

Este tipo de ataques definido como bien-conocido no afectó a la máquina víctima. Esta ignora la solicitud de redirección, igualmente un *pentester* puede utilizar esta técnica para validar *hosts* vulnerables a la inyección de rutas inválidas en sus tablas de vecinos y poder hacer ataques de suplantación de identidad.

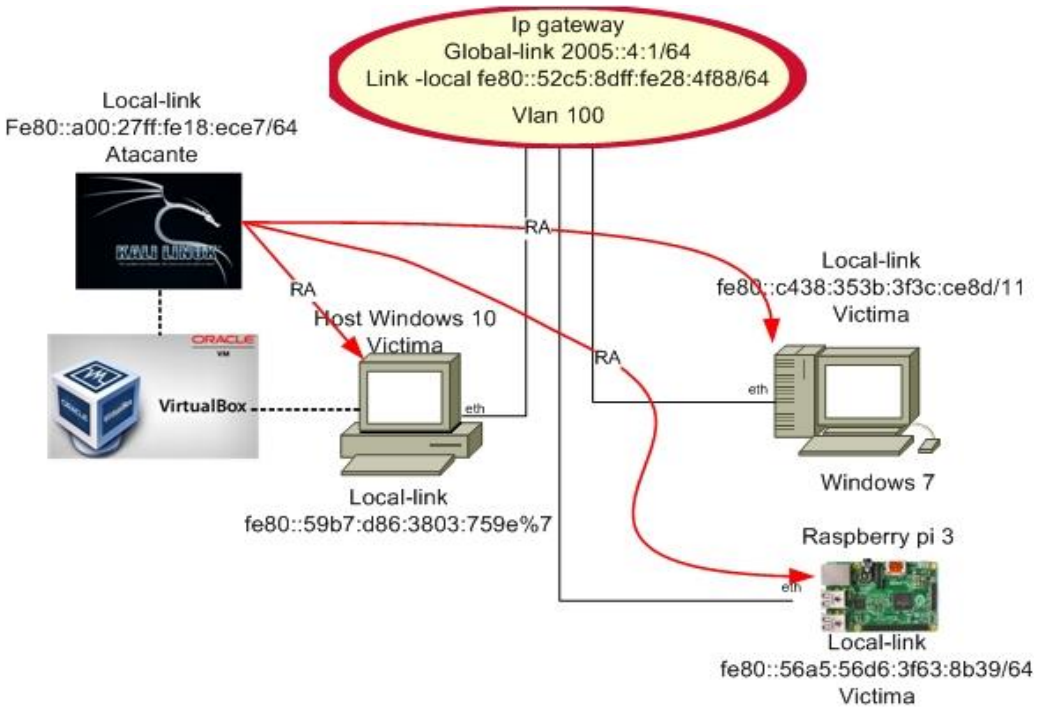
7.4 ATAQUES DE NEGACION DEL SERVICIO

Se puede denegar el servicio tanto de una red como de un dispositivo específico en una red IPv6. Para realizar estos ataques se utilizaron varias pruebas aprovechando las funcionalidades del protocolo IPv6, a continuación, se describen.

7.4.1 Ataque usando paquetes anuncio de *router* RA

Es factible realizar ataques de negación de servicio en un ambiente LAN, usando paquetes de anuncio de enrutadores *Router Adverticement* (RA), con consecuencia de incremento de la CPU de los *hosts* y llenando sus tablas de vecinos. El atacante envía paquetes realizando la solicitud RA al destino la dirección multicast FF02::1, en la figura 35, de esta manera llega a todos los *hosts* logrando el envenenamiento de su tabla.

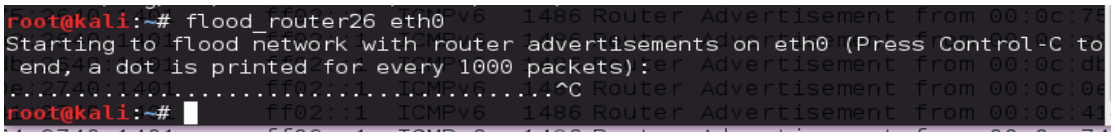
Figura 35. Ataque usando paquetes falsos RA



Fuente: autor

En Kali se usa la herramienta flood_router26 ver figura 36, la cual genera los paquetes RA de manera aleatoria y de esta manera se realiza el ataque

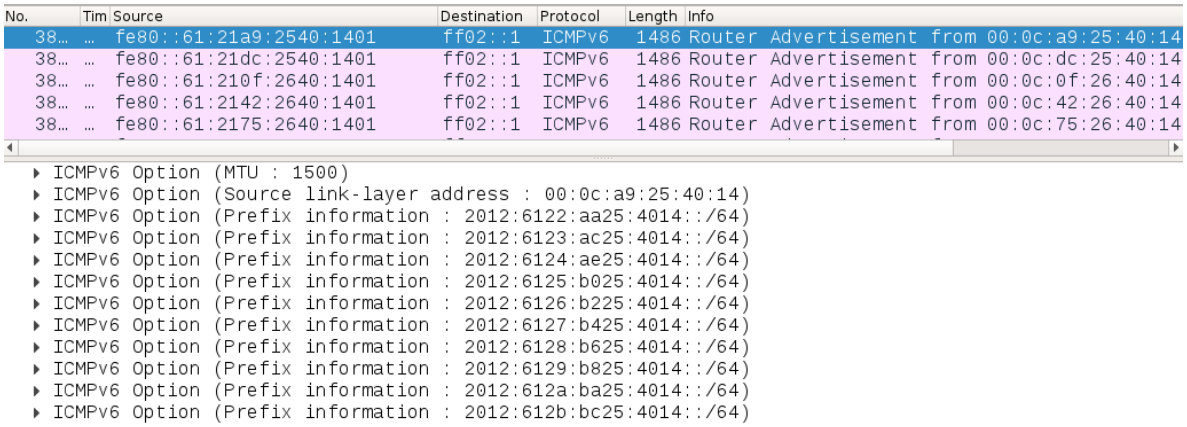
Figura 36. Uso de herramienta flood_router26



Fuente: autor

La captura del tráfico indica que la máquina atacante envía paquetes tipo ICMPv6 tipo RA y dentro de estos se encuentra en el campo de opciones la información del prefijo IPv6 que se anuncia a los *hosts* víctimas, ver figura 37.

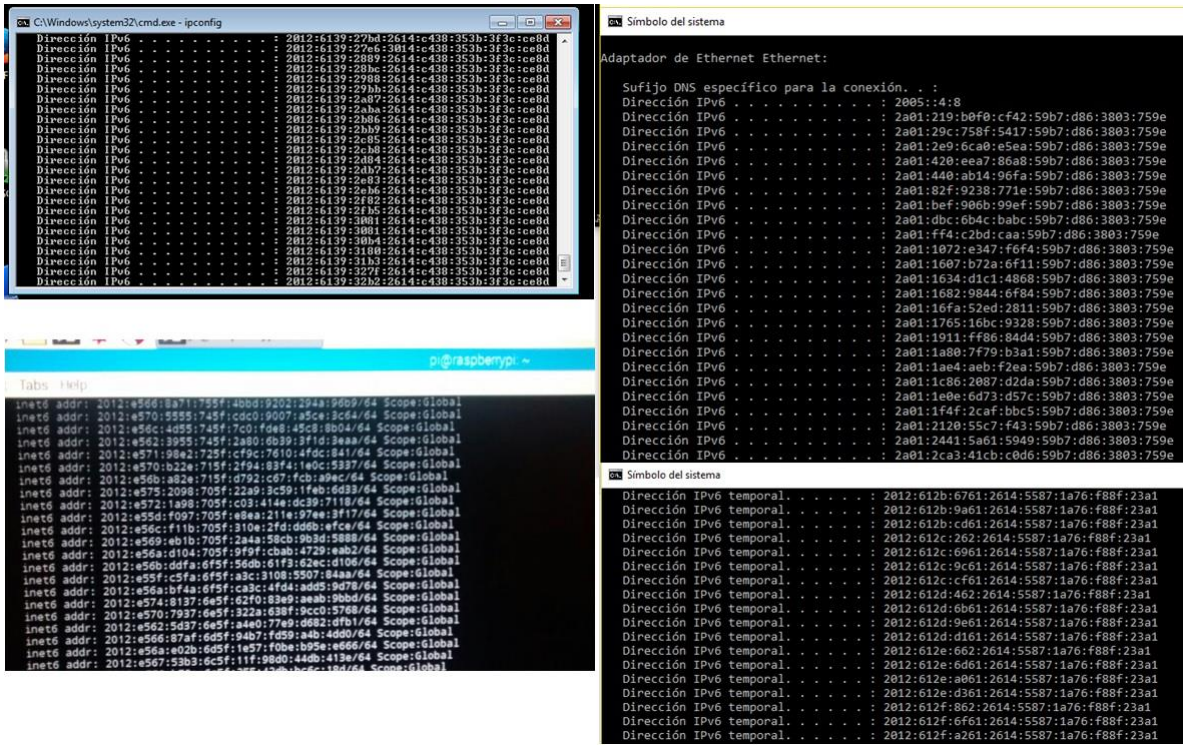
Figura 37. Captura de tráfico durante ataque paquetes RA



Fuente: autor

El resultado más visible en las *host* víctimas se puede consultar por línea de comando en Windows sentencia ipconfig y Linux ifconfig ver figura 38. Al estar llena la tabla con posibles Gateway se evidenciaron bloqueos sobre todo en la máquina con Windows 7. Además, tanto las máquinas con Windows 10 y la raspberry llenaron su tabla con posible *routers* de salida.

Figura 38. Envenenamiento de tabla de rutas IPv6 en equipos víctimas



Fuente: autor

7.4.1.1 Análisis de resultados

- La máquina atacante usa direcciones falsas de fuente lo cual dificulta la detección del origen de los paquetes, por lo tanto, es importante disponer de herramientas que monitoreen la cantidad de tráfico presente en un *switch* para detectar anomalías.

- Se observa también que la técnica de ataque suplanta la dirección mac del origen lo cual dificulta su detección. Pero se puede mitigar el ataque usando una protección a través de *port-security* y limitando las direcciones mac de origen en los puertos.

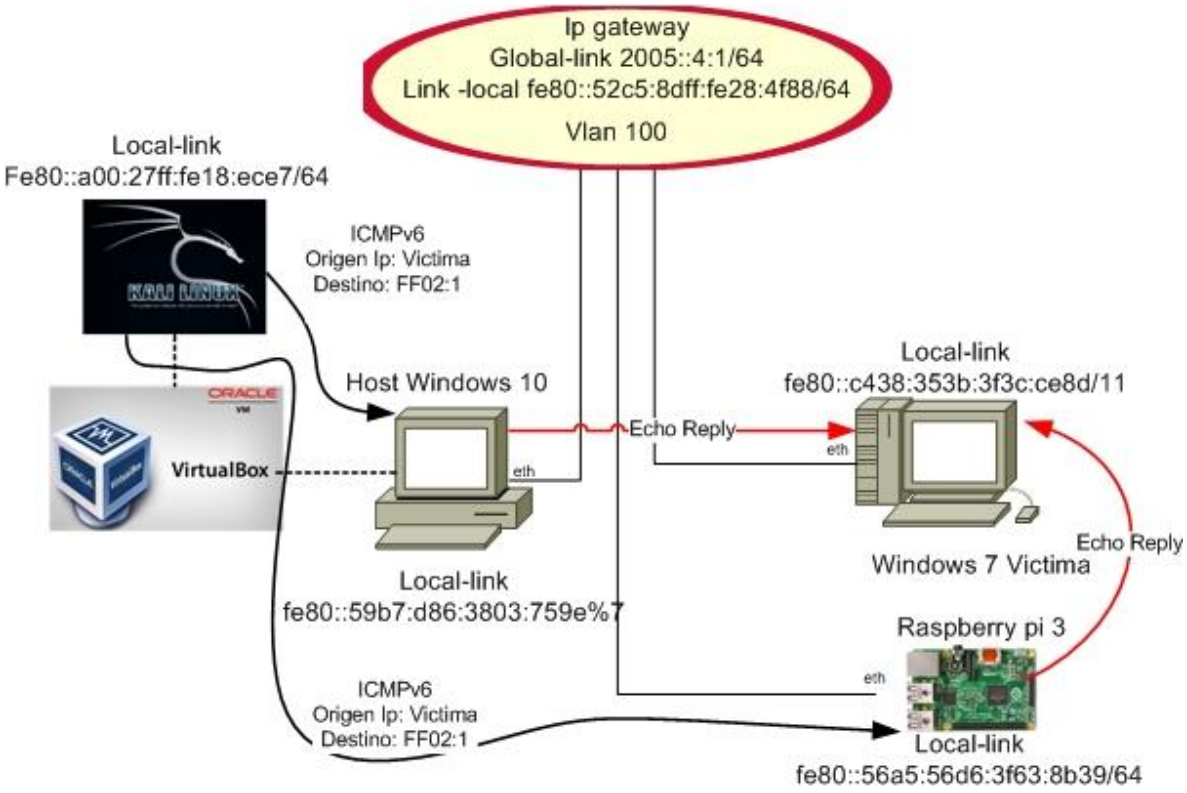
- El ataque llenó la tabla de vecinos de todos los equipos en el ambiente LAN, sin embargo, no afectó el desempeño de la red. Únicamente se detectó el ataque aplicando desde el terminal o línea de comandos una revisión de la configuración de direccionamiento IPv6.

7.4.2 Ataque usando *smurf* locales

Este tipo de ataque utiliza los mensajes echo *request* ICMPv6 con la dirección origen de la víctima y usando como destino la Ip multicast FF02::1. De esta manera

las máquinas en un ambiente LAN que reciben esta petición enviaran paquetes echo-reply, haciendo factible un ataque de negación del servicio. Al respecto ver la figura 39, a continuación.

Figura 39. Ataque usando anuncios multicast



Fuente: autor

La herramienta smurf6 se convoca en Kali Linux (ver figura 40). Es importante considerar que el atacante debe identificar antes la dirección IPv6 del host a suplantar para realizar el ataque.

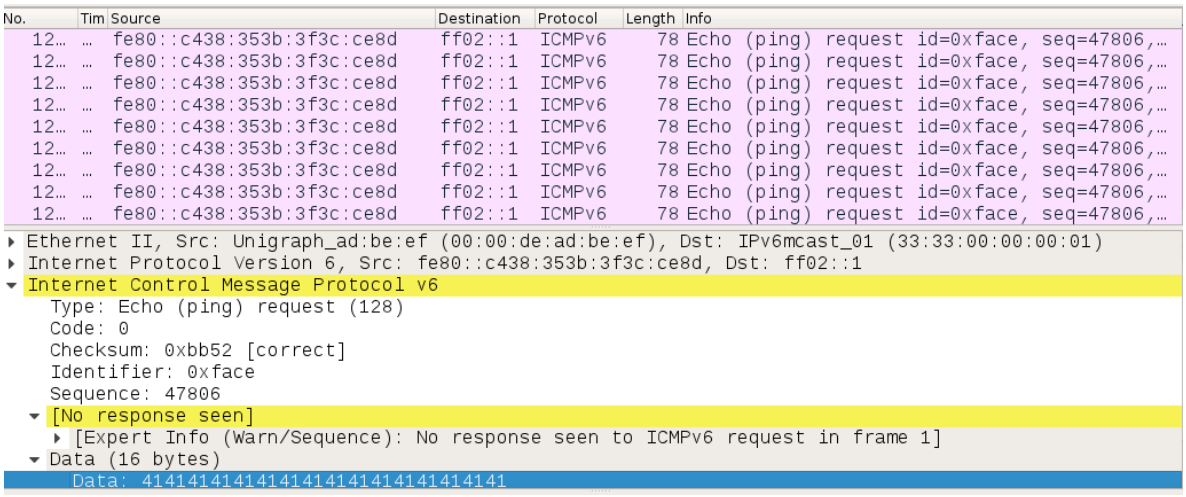
Figura 40. Uso de herramienta smurf6

```
root@kali:~# smurf6 eth0 fe80::c438:353b:3f3c:ce8d
Starting smurf6 attack against fe80::c438:353b:3f3c:ce8d (Press Control-C to end
) ...
```

Fuente: autor

La captura en *wireshark* del tráfico explicada en la figura 41 indica la forma como son enviados los paquetes echo *request* usando la suplantación de la dirección IPv6 de la máquina de Windows.

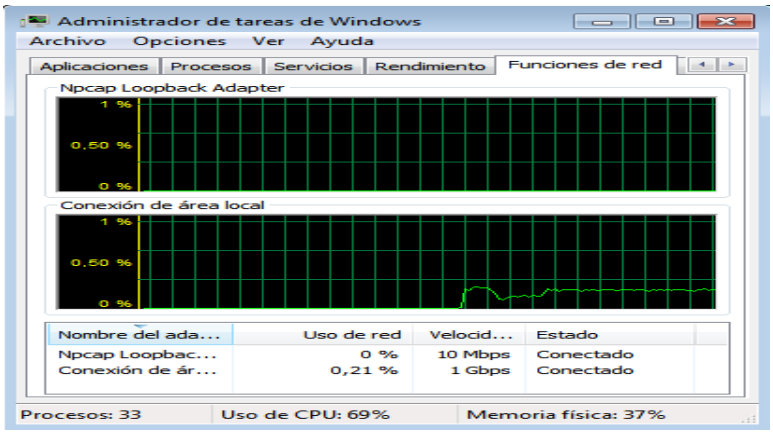
Figura 41. Captura de tráfico *smurf* enviado por máquina atacante



Fuente: autor

Las consecuencias sobre la máquina víctima se observan en la figura 42. Se visualiza el incremento de la CPU a casi un 70% siendo que normalmente está por debajo del 10%. Además, el tráfico no generado por la víctima se incrementó cerca de 21Mbps.

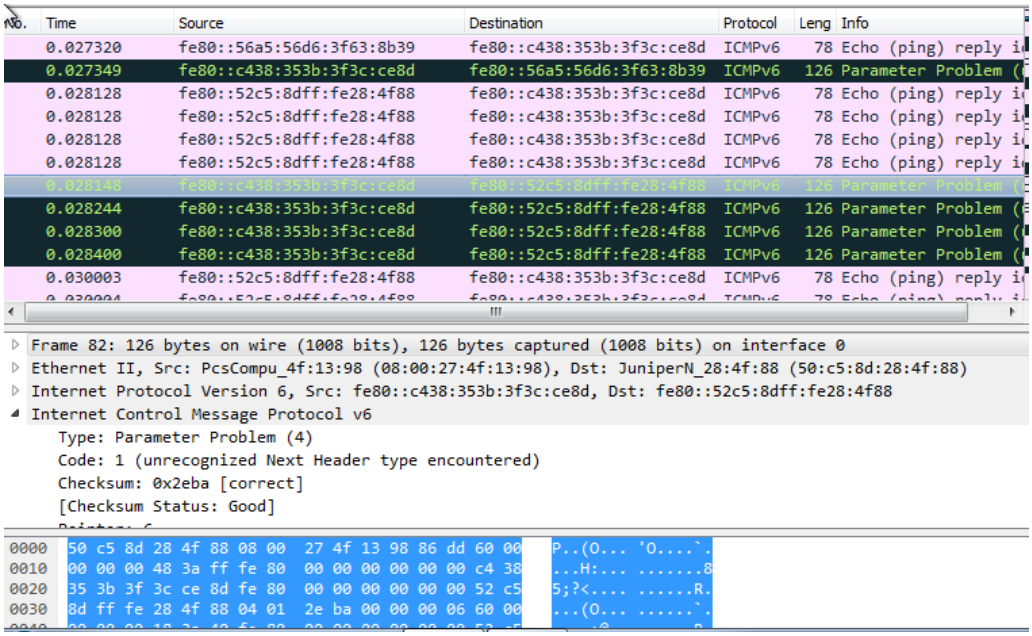
Figura 42. Incremento CPU y trafico host Windows 7



Fuente: autor

Se realiza captura de tráfico sobre la máquina victima donde los paquetes echo-reply llegan a la interfaz (ver figura 43). Además, se presenta un comportamiento anormal de la máquina Windows 7 enviando paquetes con cabecera IPv6 no reconocida.

Figura 43. Captura de tráfico smurf sobre máquina víctima



Fuente Autor

7.4.2.1 Análisis de resultados

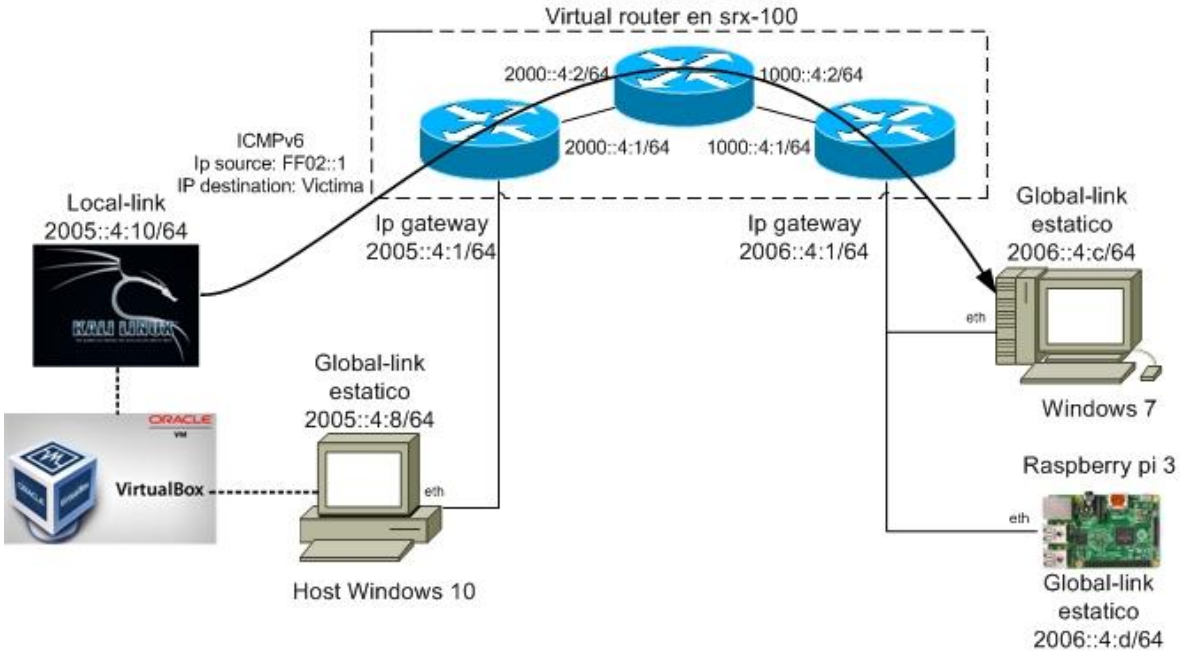
- Se observa que este tipo de ataque aumenta la cantidad de tráfico a la víctima dependiendo de la cantidad de máquinas reclutadas. En el escenario con solamente dos *hosts* se logró incrementar el tráfico de la víctima alrededor de 21Mbps en una red LAN que usa puertos de 100Mbps.

- Aunque el incremento de tráfico fue solo del 20% de la capacidad de la red durante el ataque, el procesamiento de paquetes recibidos en la victima se incrementó a valores cercanos al 70%, lo cual indica la efectividad de este ataque en un ambiente donde se dispone de más *hosts* a reclutar.

7.4.3 Ataque usando *smurf* remoto

Este tipo de ataque se fundamenta en falsificar la dirección de origen multicast FF02::1 hacia el destino de la víctima. Si estos paquetes llegan a destino generan echo-reply a los *hosts* ubicados en el lado remoto. El ataque se genera bajo la topología de ambiente WAN como se muestra en la figura 44.

Figura 44. Ataque usando *smurf* remoto



Fuente Autor

El ataque se convoca con el comando rsmurf6, como lo indica la figura 45.

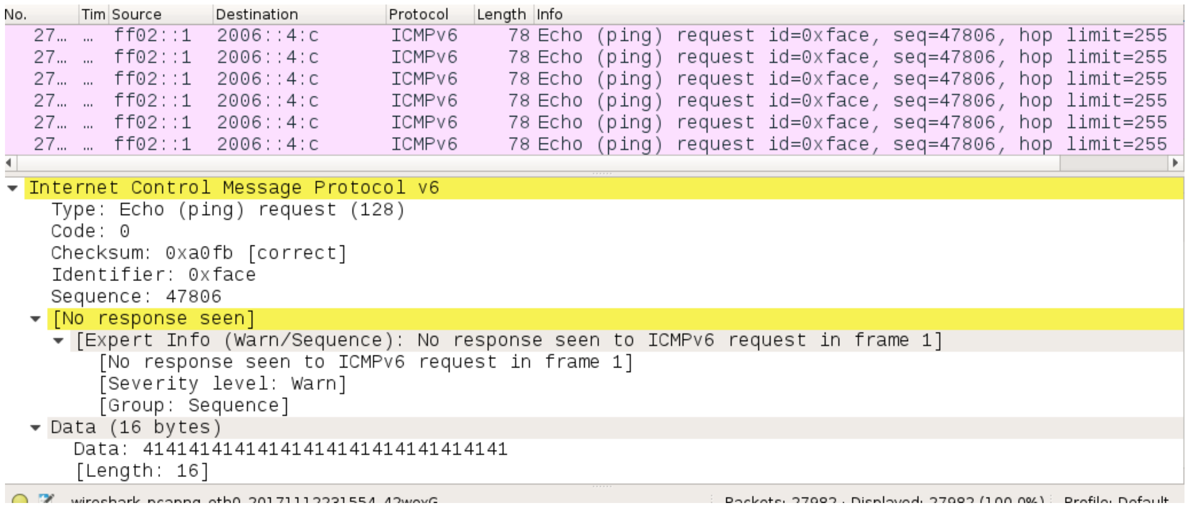
Figura 45. Uso de herramienta rsmurf6

```
root@kali:~# rsmurf6 eth0 2006::4:c
Starting rsmurf6 against 2006::4:c (Press Control-C to end) ...
```

Fuente: autor

En la figura 46 se pueden observar los paquetes generados por la máquina atacante.

Figura 46. Captura de tráfico usando smurf remoto



Fuente: autor

7.4.3.1 Análisis de resultados

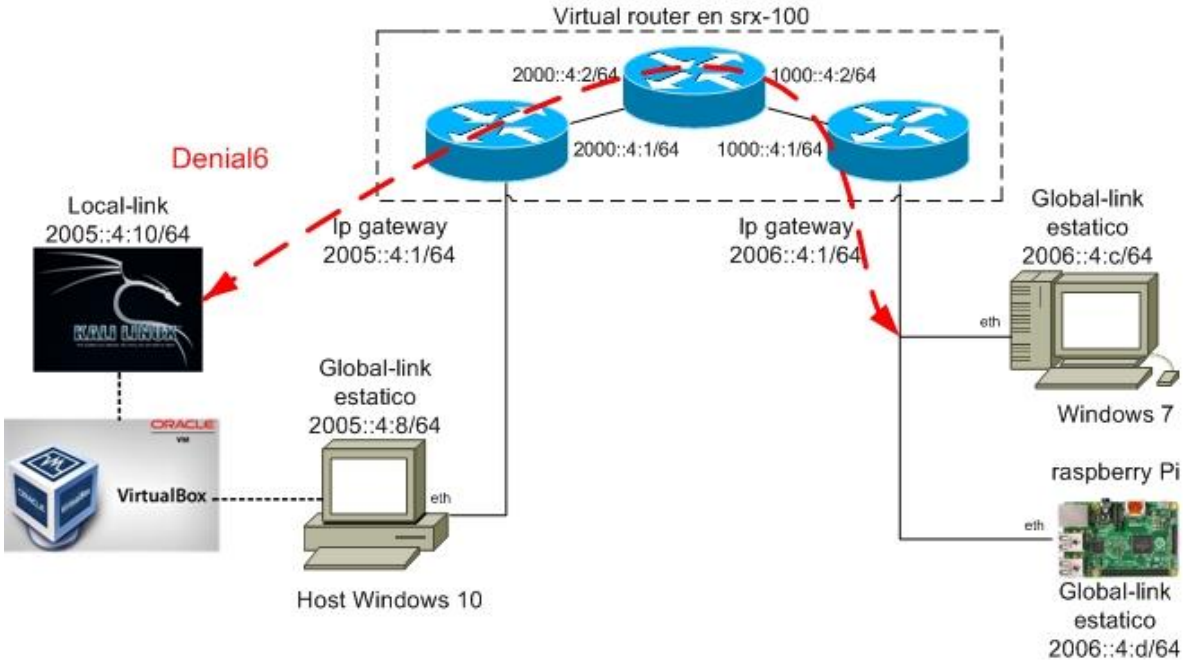
- El ataque de este tipo no fue factible ya que el equipo *router* marca Juniper no identificó los paquetes fuente y no llegaron al destino, en este caso, el host víctima. Tampoco se evidenció un incremento sustancial en el tráfico de red que llega al Gateway.

- Este ataque utiliza la dirección multicast como fuente ff02::1 y por ello el ambiente de área remota no es capaz de difundir esta dirección, en consecuencia, el ataque no es exitoso.

7.4.4 Ataque usando paquetes malformados ICMPv6

Es muy recurrente que IPv6 use los paquetes Icmpv6 ya que su función es pasar mensajes de control en la red. Para explotar vulnerabilidades la herramienta de ataque denial6 utiliza distintas estructuras de paquetes ICMPv6 que se pueden ensayar en los escenarios para probar cómo afecta a una máquina víctima. La topología usada se puede observar en la figura 47.

Figura 47. Topología usando ataque denial6



Fuente: autor

La herramienta permite seleccionar 7 tipos de ataques, sin embargo, no todos fueron efectivos porque no salieron de la interfaz Gateway con dirección IP 2005::4:1. Sólo el test 2 que usa opciones desconocidas del paquete IPv6 logró salir del Gateway y llegar a los destinos remotos. La sintaxis de la herramienta y sus opciones se puede ver en la figura 48.

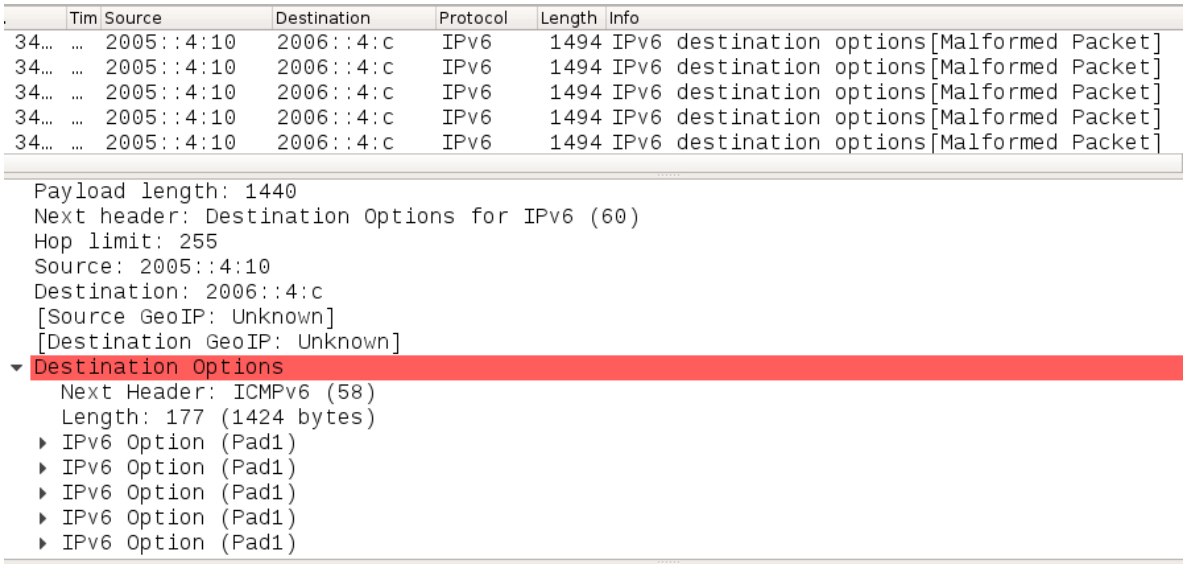
Figura 48. Uso de herramienta denial6

```
denial6 v3.0 (c) 2015 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: denial6 interface destination test-case-number

Performs various denial of service attacks on a target
If a system is vulnerable, it can crash or be under heavy load, so be careful!
The following test cases are currently implemented:
  1 : large hop-by-hop header with router-alert and filled with unknown options
  2 : large destination header filled with unknown options
  3 : hop-by-hop header with router alert option plus 180 headers
  4 : hop-by-hop header with router alert option plus 178 headers + ping
  5 : AH header + ping
  6 : first fragments of a ping with a hop-by-hop header with router alert
  7 : large hop-by-hop header filled with unknown options (no router alert)

root@kali:~# denial6 eth0 2006::4:c 2
Performing denial of service test case no. 2 attack on 2006::4:c via eth0:
A "." is shown for every 1000 packets sent, press Control-C to end...
Test 2: large destination header filled with unknown options.
.....................................................................
...........
```

Fuente: autor

El paquete enviado utiliza un tamaño máximo de MTU 1423 bytes y es identificado por el *sniffer* como paquete malformado (ver figura 49). Pero logra llegar al destino ya que el *router* acepta el paquete y lo encamina al destino de la víctima.

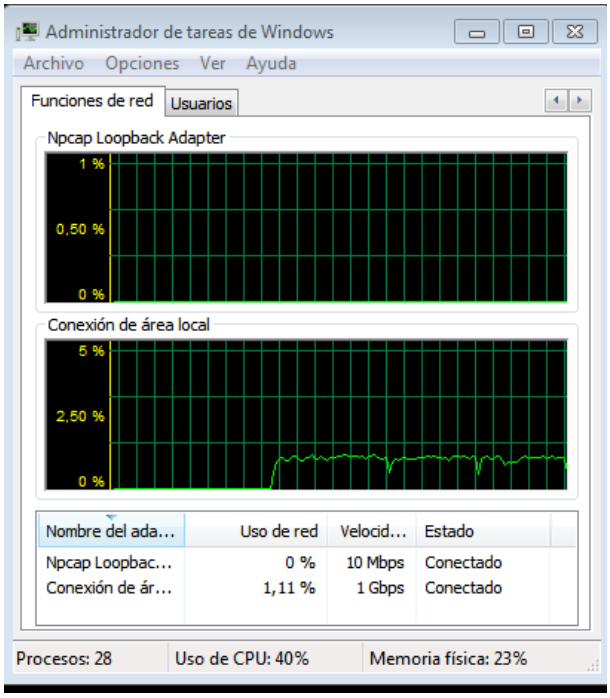
Figura 49. Captura de paquete usando el test 2 con la herramienta denial6



Fuente: autor

La prueba se realizó apuntando a la máquina Windows 7 y al raspberry pi; se observó un incremento de tráfico con respuesta de la máquina Windows 7, además del aumento de la CPU como se muestra en la figura 50.

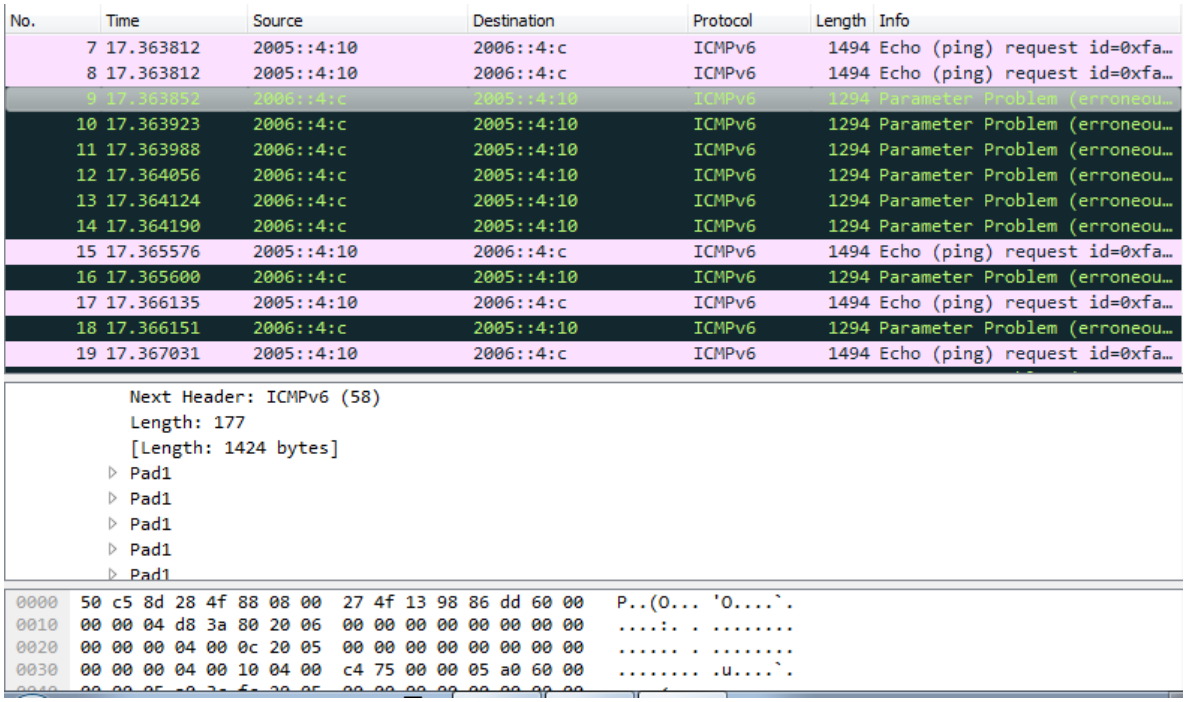
Figura 50. Incremento de tráfico y uso de cpu durante ataque en Windows 7



Fuente: autor

En la máquina víctima los paquetes recibidos son respondidos por el sistema operativo Windows 7. En la captura se aprecia vulnerabilidad en el *stack* del protocolo porque se dio respuesta a la máquina atacante de estos paquetes y se obtuvieron consecuencias tales como el aumento de CPU y lentitud en el funcionamiento de la máquina (ver figura 51).

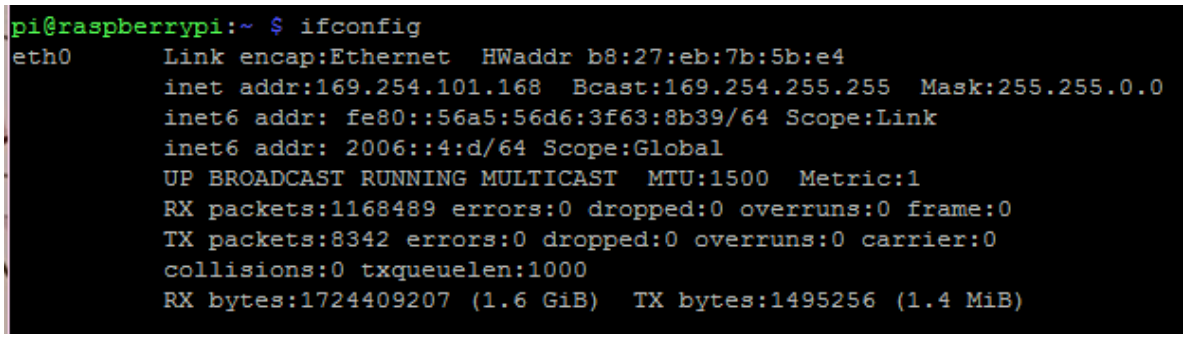
Figura 51. Captura de paquetes en máquina Windows 7 durante ataque denial6



Fuente: autor

En el caso de la *raspberry* este tipo de ataques no afectó su desempeño. Existe un incremento de tráfico en recepción, pero no existe transmisión de vuelta como se ilustra en la figura 52.

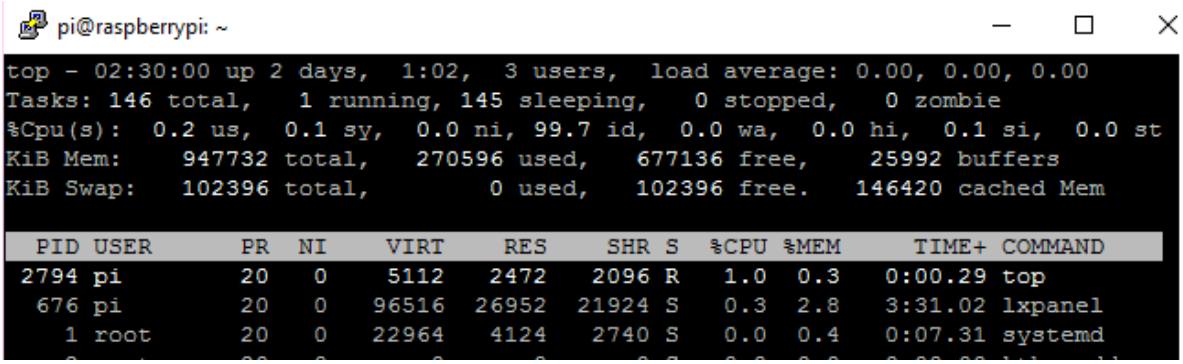
Figura 52. Tráfico de interfaz ethernet



Fuente: autor

El monitoreo de la CPU se hizo durante el ataque sobre el equipo *raspberry* sin observarse incremento en ninguno de sus procesos. Por lo tanto, es posible afirmar que este equipo no es susceptible a ese tipo de ataques (ver figura 53).

Figura 53. Uso de CPU durante ataque denial6



Fuente: autor

7.4.4.1 Análisis de resultados

- Este tipo de ataques demostró vulnerabilidad en el *stack* IPv6 de la máquina victima en este caso de una Windows 7, la cual procesó y envió respuestas a paquetes ICMPv6 que te tenían opciones invalidas en las cabeceras. Este resultado permitió un incremento de su CPU a un valor cercano del 40%.

- El equipo Juniper Srx-100 no se vio afectado por este tipo de tramas las cuales procesó y envió al destino. Con los demás test generó rechazo ya que no identificó esas tramas.

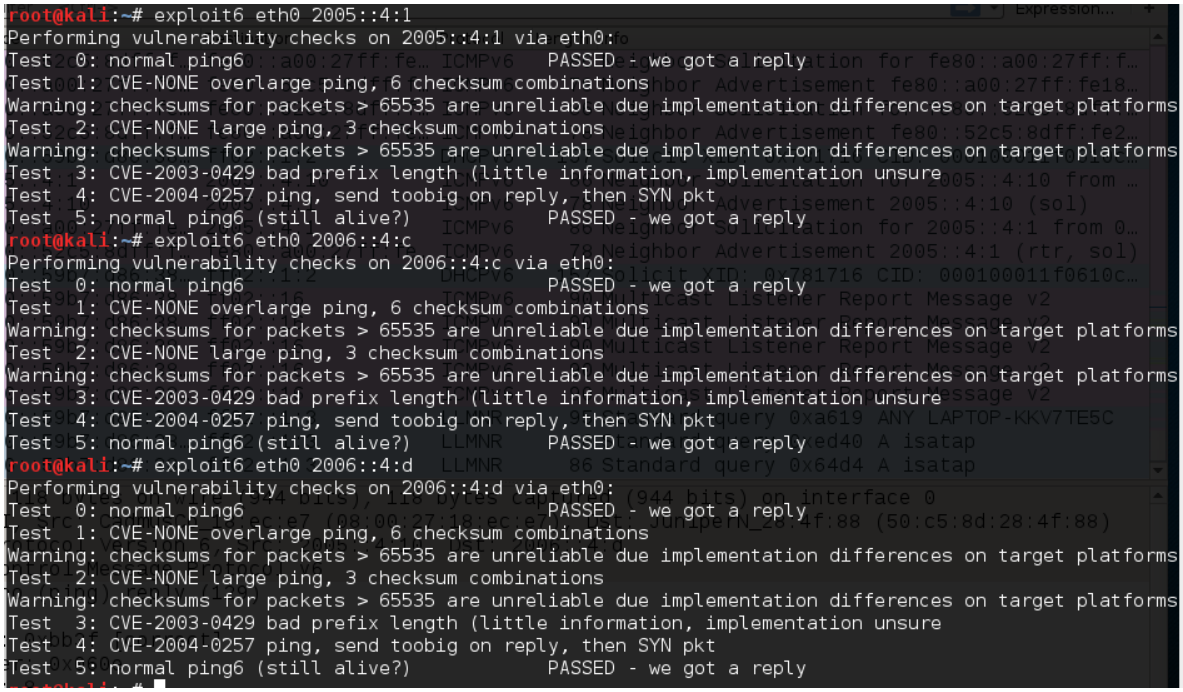
- El *raspberry* no se vio afectado en su *stack* IPv6 porque rechazó las tramas con descarte silencioso y no las procesó. No se observa incremento de tráfico en tarjeta de red ni en procesamiento de CPU.

7.5 PRUEBAS DE EXPLOTACIÓN DE VULNERABILIDADES

Un *pentester* al encontrarse bajo un escenario de auditoria sobre una red IPv6, puede verse beneficiado al utilizar herramientas para evaluar vulnerabilidades en los dispositivos que usen este protocolo.

Kali Linux cuenta con un módulo llamado exploit6 que realiza seis test al objetivo que tenga una dirección IPv6 activa. Los test incluyen conectividad, comprobación de errores y comprobación de vulnerabilidades CVE-2003-0429, CVE-2004-2057. El escenario WAN, en la figura 14, se utilizó para realizar varias pruebas y como objetivos del ataque se tomaron: el equipo Juniper srx-100, el *host* Windows 7 y la *Raspberry* Pi (ver figura 54).

Figura 54. Comprobación sobre objetivos con herramienta exploit6



Fuente: autor

Los resultados de estos test indican lo siguiente:

Test 0: prueba, con un paquete ICMPv6, que el dispositivo esté activo en la red igual que en el test 5. Para el escenario de área remota todos los dispositivos son alcanzables.

Test 1: en esta prueba se envían, dentro de los paquetes ICMPv6, seis combinaciones de *checksum* errados esperando respuestas de echo-reply. En el caso de los dispositivos no se evidenció respuesta en este test.

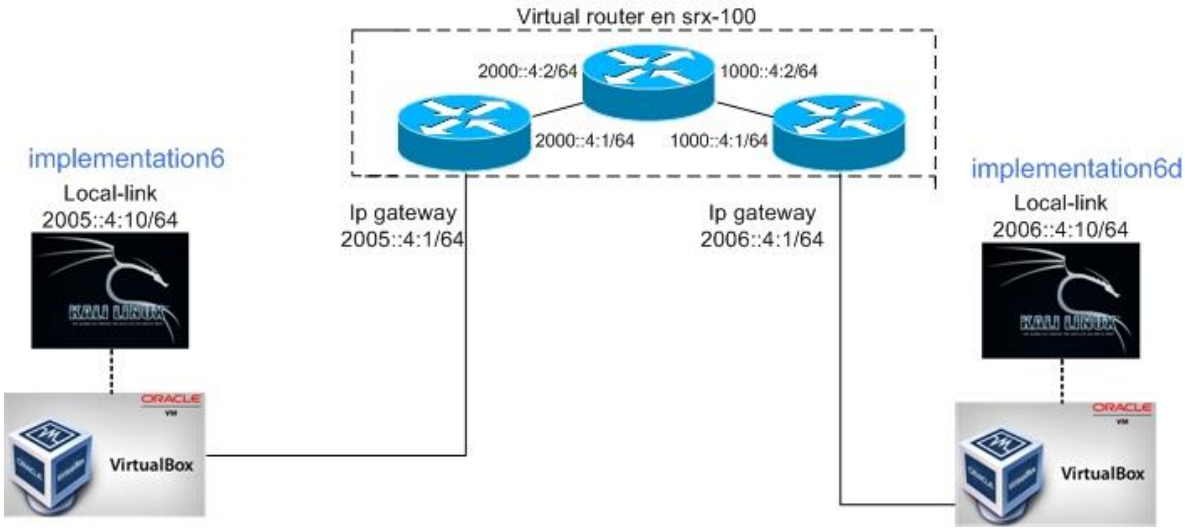
Test 2: prueba parecida a la número 1 con sólo tres combinaciones de *checksum*. Ninguna respuesta para los dispositivos evaluados.

Test 3: la vulnerabilidad CVE-2003-0429 permite a atacantes remotos causar denegación de servicio usando inválidas longitudes de prefijos IPv6 y causar un sobre flujo del *buffer*. En la prueba ningún dispositivo dio respuesta.

Test 4: esta vulnerabilidad CVE-2004-2057 envía una respuesta ICMPv6 de paquete *toobig*, si la máquina es vulnerable envía una respuesta. Para los dispositivos evaluados no se obtuvo respuesta

Si el *pentester* desea validar errores de implementación sobre el *stack* IPv6 en una red, o certificar los tipos de paquetes que pueden atravesar un Firewall o red, se puede realizar la siguiente prueba empleando dos máquinas que usen las herramientas implementation6 e implementation6d, una de ellas como cliente genera los paquetes y la otra como receptor de las pruebas. A través de 57 test se puede analizar cuáles de los paquetes que tienen alteraciones en sus estructuras IPv6 pasan la red y de esta manera indicar los riesgos presentes. Para la prueba se utiliza la topología descrita en la figura 55.

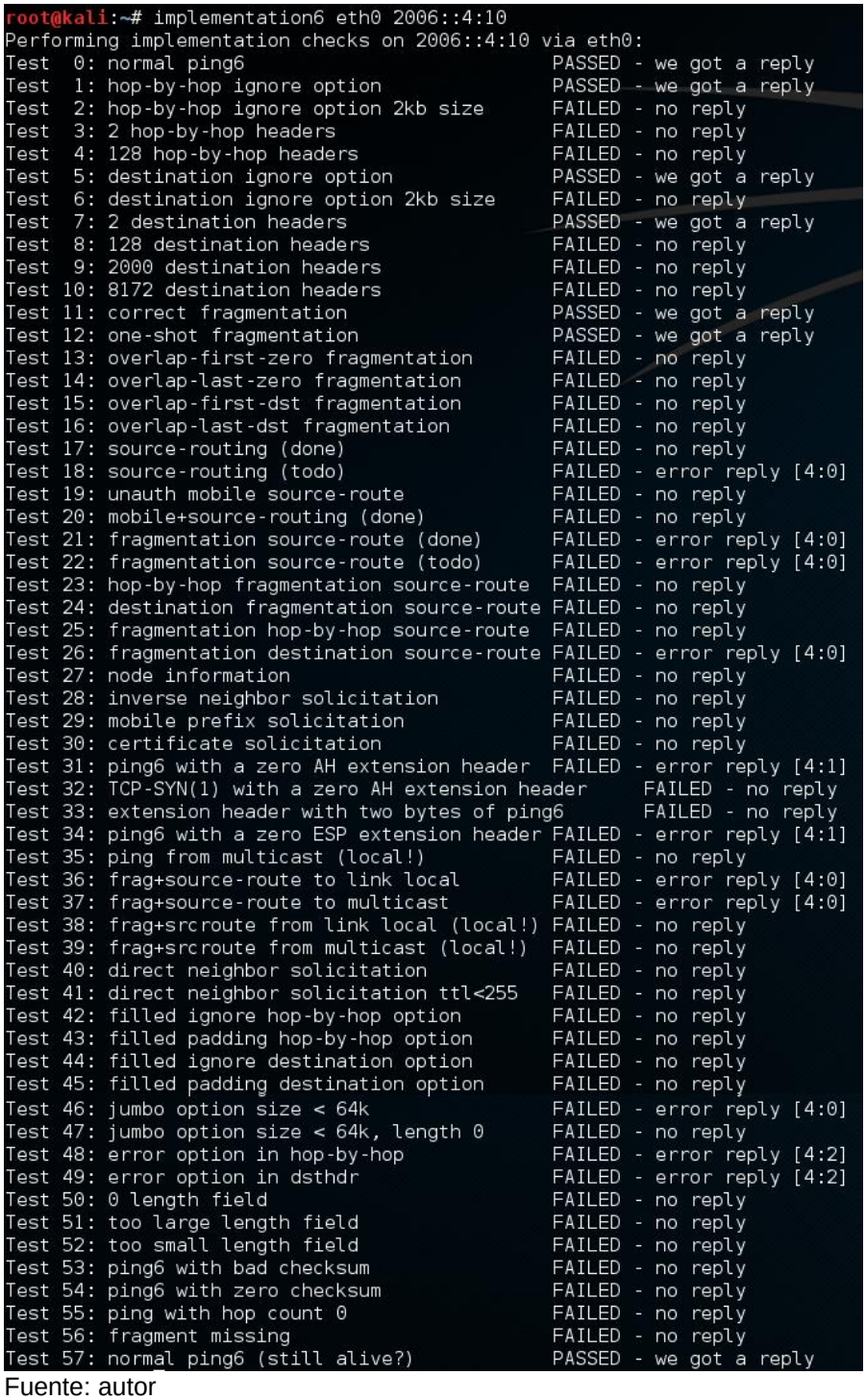
Figura 55. Topología de área remota usando herramientas implementation6



Fuente: autor

La sintaxis usada para ejecutar la herramienta, cada test y una descripción del tipo de paquetes que se evalúan se puede ver en la figura 56. Es posible afirmar que estos test ayudan al evaluador a encontrar problemas con el *stack* IPv6 en una red, no obstante, se aclara que únicamente hacen pruebas punto a punto definidas entre un cliente y un servidor.

Figura 56. Uso de herramienta implementation6

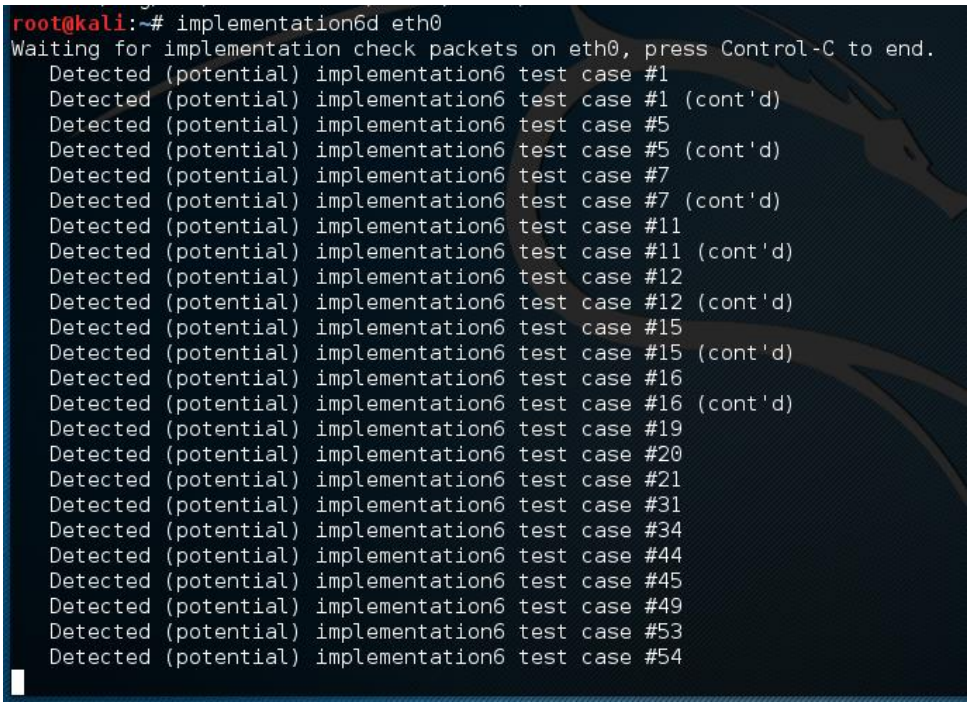


Fuente: autor

Los resultados de la prueba se muestran en la figura 57 e indican que los siguientes paquetes pueden pasar por la red y, por lo tanto, el *pentester* puede considerarlos

como potenciales riesgos de la implementación en el *stack* IPv6 para la red propuesta.

Figura 57. Resultados de la evaluación implementation6d



Fuente: autor

La descripción de estos resultados se ofrece a continuación:

- Test 1 hop-by-hop ignore option: los paquetes con cabecera *hop by hop* pasan y con la opción ignorar activa los nodos no rechazaron los paquetes.

- Test 5 destination ignore option: paquetes hacia destino con opción ignorar activa atraviesan los nodos.

- Test 7 two destination header: paquetes con dos cabeceras de destino pasan a través de los nodos.

- Test 11 correct fragmentation: paquetes fragmentados pasan sin problemas por los nodos.

- Test 12 one shot fragmentation: paquete con cabecera de fragmentación activa sin carga útil.

- Test 15 overlap-first-dst fragmentation: solapamiento de paquete fragmentado en el primer paquete del destino.

- Test 16 overlap-last-dst fragmentation: solapamiento de paquete fragmentado en el último paquete del destino enviado.

- Test 19 unauth mobile source-route: paquetes de cabecera móvil sin autenticación pasan por los nodos sin problemas.

- Test 20 mobile source-routing: paquete de cabecera móvil con cabecera de fuente de enrutamiento pasa por los nodos.

- Test 21 fragmentation source-route: paquete fragmentado y con opción fuente de ruta pasa por los nodos.

- Test 31 ping6 with a zero AH extensión header: ICMPv6 con cabecera de autenticación de valor cero pasa por los nodos.

- Test 34 ping6 with a zero ESP extensión header: ICMPv6 con cabecera Ipsec y con carga útil encapsulada con valor de cero pasa por los nodos.

- Test 44 filled ignore destination option: bits en uno, en todos los campos de opciones en cabecera destino.

- Test 45 filled padding destination option: bits en uno, en los campos de relleno en la cabecera destino.

- Test 49 error option in dst hdr: paquetes con la opción de error en cabecera de destino pasan por los nodos.

- Test 53 ping6 with bad checksum: ICMPv6 con valores errados en *checksum* atraviesa por los nodos.

- Test 54 ping6 with zero checksum: ICMPv6 con valor cero en *checksum* atraviesa por los nodos.

7.6 RECOMENDACIONES DE SEGURIDAD

En esta sección se encuentran las recomendaciones de seguridad de acuerdo con cada ataque efectuado y descrito en el numeral 7.1.

7.6.1 Recomendaciones contra ataques de escaneo

Para este tipo de pruebas o ataques en un ambiente de red de área amplia el uso de un *firewall stateless* o *staful* permite que únicamente las sesiones válidas sean desde una zona de confianza a zona de desconfianza (internet). Por lo tanto, este escenario no debe ser excluyente. Aunque se piensa que tener un amplio *pool* de direcciones IPv6 *dificulta* el escaneo con aplicaciones como Nmap con soporte del protocolo IPv6 y recursos adecuados se puede encontrar una máquina expuesta a un ataque o un servicio vulnerable.

Respecto a los escenarios en red de área local con el uso del grupo *multicast* por defecto ff02::1 es sencillo localizar los *hosts* que pertenecen a este grupo. Para dificultar el ataque de reconocimiento se debe configurar el direccionamiento de *local-link* en cada equipo a través de un método, como por ejemplo Dhcpv6, ya que el riesgo se presenta cuando se asigna la dirección de manera automática.

Recomendaciones RFC7707 para la mitigación de escaneo de redes:

- emplear la recomendación de plan direccionamiento del RFC7217 porque oculta patrones asignados a las direcciones y reemplazar las direcciones asignadas por los identificadores IEEE;
- usar un detector de intrusos (IPS) en la red;
- aplicar filtrado de paquetes (listas de acceso) IPv6 donde sea factible, usar a criterio del administrador de red la recomendación RFC4890 la cual indica algunas recomendaciones de filtrado de los paquetes ICMPv6;
- configurar manualmente las direcciones MAC en las máquinas virtuales porque de esta manera se genera un patrón no predecible de direccionamiento y ayuda a resistir a un escaneo de redes;
- evitar el uso de direccionamiento secuencial utilizando DHCPv6. Idealmente el servidor DHCP6 tendrá una dirección aleatoria de un gran *pool*;
- usar por defecto las subredes de prefijos IPv6 en un tamaño /64;
- recomendación general: evite asignar direcciones con patrones predecibles.

El escaneo de redes se facilita en las siguientes situaciones, cuando los nodos:

- están identificados en secuencia, ::1, ::2, ::3 , etc.;

- tienen sus direcciones IPv6 en la misma zona DNS;

- responden un ICMPv6 *echo-request* enviado a todos los nodos con una dirección local multicast FF02::1;

- responden una cabecera de extensión invalida y se envía a todos los nodos la dirección local multicast FF02::1;

- envían ICMPv6 con paquetes de solicitación de vecinos (NS) tipo 135 a un *router* por defecto desconocido, este envía un ICMPv6 advertencia de *router* (RA) tipo 134.

7.6.2 Recomendaciones contra ataques de fragmentación

Este tipo de ataques se pueden dar en cualquier dispositivo que no tenga depurada su pila de protocolo IPv6. Bajo la recomendación del RFC5722, de manera general, si se detectan paquetes con solapamiento en sus fragmentos deben ser descartados.

Las recomendaciones al respecto son:

- tener un sistema IPS/IDS que alerte sobre respuestas no deseadas de solapamiento en una red de área local;

- realizar test periódicamente y evaluar si hay respuestas no deseadas con fragmentación de paquetes en los dispositivos de la red;

- mantener actualizados los sistemas operativos de los dispositivos que utilicen el protocolo IPv6;

- realizar procesos de *hardening* o blindaje en las estaciones de trabajo para evitar respuestas no deseadas ante este tipo de paquetes.

7.6.3 Recomendaciones contra ataques de *ip spoofing*

Estos ataques se aprovechan de vulnerabilidades conocidas usando paquetes tanto de la parte de control ICMPv6 como de los usados en descubrir vecinos *Neighbor Discovery*.

Las recomendaciones que se pueden realizar al respecto son:

- Usar cifrado y autenticación. Aunque se consideró, al inicio, que nativamente IPv6 se iba a usar Ipsec por defecto, esto no es del todo cierto. Por lo tanto, es

responsabilidad de los administradores usar tanto Ipsec que se fundamenta en la autenticación y cifrado de paquetes. Es importante también usar certificados digitales y https en las aplicaciones para evitar vulnerabilidades en capas superiores.

- Sobre los *gateways* deben documentarse las capacidades de filtrado de paquetes IPv6 de los dispositivos y denegar paquetes como la advertencia de enrutadores *router advertisement*.

7.6.4 Recomendaciones contra ataques de negación del servicio

Como indicado en el apartado anterior 7.2.3. estos paquetes se podrían evitar usando una implementación de Ipsec. Se debe considerar un fuerte filtrado de paquetes a través de un *Deep inspection packet* para evitar que paquetes con contenidos en su *payload* alterados afecten los dispositivos de la red.

7.6.5 Recomendaciones frente a fallas de implementación del protocolo IPv6

Es muy difícil controlar las fallas si hay alteraciones en los paquetes ya que a diferencia de IPv4, el protocolo IPv6 utiliza varios paquetes ICMPv6 para el control de la red y filtrarlos con un firewall afectaría el desempeño. De esta manera, un *pentester* debe evaluar la red y considerar cuáles paquetes filtrar, además de incluir en los filtros las capas superiores de los protocolos TCP, UDP, SIP, etc., para que los paquetes alterados no vulneren equipos.

7.6.6 Informe final de resultados

En el cuadro 4 se presenta un resumen general de los resultados de los ataques generados en el laboratorio incluyendo las recomendaciones generadas y propuestas en el apartado precedente.

Cuadro 4. Informe de resultados y recomendaciones

Tipo de ataques	Técnica de ataque usada	Escenario	Resultados de ataques	Recomendaciones
Ataque de escaneo	Tcp-syn con herramienta Nmap	WAN	Exitoso	-Usar longitud de prefijo /64. -Evitar usar direccionamiento con patrones predecibles.

Tipo de ataques	Técnica de ataque usada	Escenario	Resultados de ataques	Recomendaciones
Ataque de escaneo	Envío de paquetes ND usando herramienta alive6	LAN	Exitoso	-No es factible evitar los paquetes reconocidos del protocolo. -Tener instalado un IPS/IDS y verificar comportamientos de red anómalos.
Ataque de fragmentación	Envío de paquetes ICMPv6 con cabecera de fragmentación activa herramienta frag6	WAN	No exitoso	-Mantener actualizado los sistemas operativos de los dispositivos en la red. -Instalar un equipo IPS/IDS para validar comportamientos de red. -*Pentesting* de equipos de forma periódica.
Ataque de Ip *spoofing* (suplantación)	Suplantación de paquetes NA usando herramienta parasite6	LAN	Exitoso	-Vulnerable únicamente durante el registro del equipo en la red. -Instalar un IPS/IDS para validar comportamientos anómalos. -Factible detectar el origen de paquetes NA en la red por parte del administrador. -Uso de paquetes de encripción y autenticación tanto Ipsec como https.
Ataque de Ip *spoofing* (suplantación)	Inyección de paquetes ICMPv6 Redirect usando herramienta redir6	WAN	No exitoso	-Mantener actualizados sistemas operativos. -Utilizar Firewall y filtrar paquetes ICMPv6 no necesarios a criterio del administrador como Redirect. -Uso de paquetes de encripción y autenticación tanto Ipsec como https.

Tipo de ataques	Técnica de ataque usada	Escenario	Resultados de ataques	Recomendaciones
Ataque de DoS (negación de servicio)	Inyección de paquetes RA con herramienta flood_router26	LAN	Exitoso	-Usar función de port-security en *switches* para evitar gran cantidad de direcciones mac fuente. -Uso de ipsec solicitando descubrimiento de routers en modo seguro.
Ataque de DoS (negación de servicio)	Inyección de paquetes multicast en destino herramienta smurf6	LAN	Exitoso	-No se observa factibilidad de filtrar estos paquetes en ambientes LAN ya que están permitidos por defecto en la red.
Ataque de DoS (negación de servicio)	Inyección de paquetes multicast como fuente herramienta rsmurf6	WAN	No exitoso	-Los *router* deben estar actualizados para evitar que pasen tráfico multicast dirección ff02::1 de origen.
Ataque de DoS (negación de servicio)	Uso de paquetes ICMPv6 con paquetes malformados herramienta denial6	WAN	Exitoso	-Se recomienda uso de *deep inspection packet* para comprobar contenido de paquetes.
Pruebas evaluación fallos en implementación del protocolo Ipv6	Pentesting usando herramientas	WAN	parcial	-Evaluar tipos de paquetes ICMPv6 e IPv6 que deben ser filtrados, tanto en switches, router y firewall considerar como guía los evaluados. -Mantener actualizados sistemas operativos para evitar vulnerabilidades antiguas en el stack ipv6.

Fuente: autor

8. RESULTADOS E IMPACTO

Las pruebas ejecutadas dentro del trabajo de grado evaluaron el comportamiento del protocolo ipv6 a través de un entorno tecnológico controlado, bajo dos tipos de escenario tanto red de área local como red de área amplia, según los resultados descritos en el numeral anterior la cantidad de ataques con capacidad de afectar una red fue del 60%, frente a un 30% de ataques no exitosos y un 10% con éxito parcial.

También se logró evidenciar que es más factible realizar ataques en una red de área local con un mayor índice de éxitos, de cuatro ataques efectuados el éxito del ataque fue del 100 %, lo que demuestra que este tipo de escenarios son más vulnerables cuando no cuente con un reforzamiento de la seguridad o componente que lo proteja, en escenarios de área remota la efectividad de ataques fue del 40%.

Las herramientas de evaluación de protocolo Ipv6, fueron diseñadas para alterar tanto los comportamientos como espacios de cabecera y contenido en los paquetes Ipv6, lo cual ofrece una cantidad considerable de ataques a evaluar, por lo tanto, futuros proyectos pueden ser desarrollados realizando diferentes pruebas usando distintos módulos bajo las herramientas THC-Ipv6 Toolkit como Ipv6 Toolkit.

Este tipo de proyectos tienen un impacto en las organizaciones y personas que deseen implementar Ipv6 en su red, ya que pueden identificar tipos de vulnerabilidades presentes e inherentes del protocolo Ipv6 que facilitan ataques como son suplantación de identidad, robos de información, ataques de negación del servicio y bajo las recomendaciones ofrecidas pueden tomar decisiones para mitigar este tipo de riesgos.

9. DIVULGACION

El método de divulgación y como objetivo plasmado fue la publicación de una página web donde se dejó evidencia del trabajo realizado con las plantillas de configuración de los laboratorios, capturas, teoría y resultados, el enlace a la página se puede consultar en el anexo C, se destaca que al ser un hosting gratuito de Google la página estará vigente mientras el autor la mantenga pública.

También el presente trabajo de grado, luego de su aprobación, quedará publicado en el *link* de repositorios de la Universidad Nacional Abierta y a Distancia, dejando el material disponible para futuras consultas.

10. CONCLUSIONES

Es factible desarrollar un entorno tecnológico controlado para simular ataques que impliquen la utilización del protocolo IPv6. En ese entorno el componente más costoso fue el equipo Juniper srx-100 que aun así se destaca ofreciendo una ventaja en cuanto a la versatilidad de configuración que permite crear ambientes de área local como de área remota para simular ataques a través del uso de máquinas virtuales y dispositivos que soportan el protocolo IPv6.

El protocolo IPv6 hace uso intrínseco de los paquetes ICMPv6 y *Neighbor Discovery* y es más recurrente no filtrar paquetes ICMP, a diferencia del protocolo IPv4. Se debe evaluar de una manera más estricta qué tipo de señales de control permitir y/o restringir ya que el uso de esas señales y descubrimiento es necesario en cualquier entorno de red local o remoto.

El escaneo de red a través de paquetes tcp-syn es factible en IPv6 y aunque estos paquetes generalmente se consideran válidos también pueden ser usados para generar ataques de negación del servicio. Por lo tanto, se tiene una dificultad al identificar qué tipos de tráfico son válidos en una red.

En los esquemas de seguridad perimetral se debe considerar el uso de un equipo de seguridad de aplicaciones (WAF), ya que hay una exposición a ataques a nivel de red que un *firewall stateless* o *stateful* no son capaces de gestionar por las funcionalidades que incluye el protocolo como son el uso ICMPv6.

Con el uso extendido de ICMPv6 en las redes IPv6 se debe recurrir de manera más exigente a la utilización de mecanismos de seguridad como Ipsec. Esa estrategia garantiza la autenticación, confiabilidad e integridad. Al igual que en la versión anterior del protocolo se debe recurrir a la protección de las capas superiores usando, por ejemplo, certificados digitales y el protocolo https.

Los laboratorios como componentes prácticos ofrecen la oportunidad de recrear ataques que permanecen vigentes. De forma didáctica, los laboratorios permiten identificar patrones y comportamientos en los entornos de red para que los administradores de red e ingenieros de seguridad tomen decisiones que conlleven a una mejor protección de la seguridad de la información.

BIBLIOGRAFÍA

ATLASIS, Antonios. Penetration Testing tools that (do not) Support IPv6. En: ERNW providing security, 2014. Disponible en Internet: https://books.google.com.co/books?id=RBpUVS9mDkUC&pg=PT2&lpg=PT2&dq=Penetration+Testing+Tools+that+%28do+not%29+SupportIPv6&source=bl&ots=yGD1AosTNE&sig=J_mZcT9JJ_rg6_01zYi6O5apSJ4&hl=es-419&sa=X&redir_esc=y#v=onepage&q=Penetration%20Testing%20Tools%20that%20%28do%20not%29%20SupportIPv6&f=false

CAZAR JÁCOME, D. A. Análisis de Ip spoofing en redes IPv6. Proyecto de grado. Quito: Escuela Politécnica Nacional de Ecuador. Facultad de ingeniería Eléctrica y Electrónica, 2015. 118 p. Disponible en Internet: http://bibdigital.epn.edu.ec/bitstream/15000/10917/1/CD-6335.pdf

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05, ENERO, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. No. 47.223.

CONTADOR VILCHES, N.. Análisis de seguridad de IPv6 pruebas y recomendaciones. Tesis de Maestría. Viña del Mar: Universidad Andrés Bello, 2013. 33p. Disponible en Internet: https://profesores.ing.unab.cl/~druete/archivos/cursos/TM/Presentaciones/Presentaci%C3%B3n%201/Tesis%20Proyecto%20Magister%20-%20Nicolas%20Contador.doc>

COOPER, A., GONT, F. Security and Privacy Considerations for IPv6 Address Generation Mechanisms. s.l. :IETF, 2016. RFC 7721. Diponible en Internet: https://tools.ietf.org/html/rfc7721

DAVIES, E., KRISHNAN, S., SAVOLA, P. IPv6 Transition/Coexistence security considerations. s.l.: IETF, 2007. RFC 4942. Disponible en Internet: https://www.ietf.org/rfc/rfc4942.txt

FRANKEL, S., GRAVEMAN, R., PEARCE, J., ROOKS, M. Guidelines for the secure deployment of IPv6. Gaithersburg: NIST 2010. 188 p. Disponible en Internet: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=907211

FLORENTINO, Adilson Aparecido. Segurança em Redes IPv6. En: Portal do IPv6, [Base de datos en linea] [Citado en 28 de Noviembre de 2016]Disponible en ftp://ftp.registro.br/pub/gts/gts19/03-SegurancaRedesIPv6.pdf

GARCÍA MARTÍN, C. Análisis de seguridad en redes IPv6. Proyecto fin de carrera. Madrid: Universidad Carlos III de Madrid. Escuela Politécnica Superior. Departamento de Ingeniería Telemática, 2012. 143 p. Disponible en Internet: https://e-archivo.uc3m.es/bitstream/handle/10016/16707/PFC_Carlos_Garcia_Martin.pdf

GONT, F. Seguridad en IPv6. s.l.: SI6 Networks, 2012. Disponible en Internet: https://www.si6networks.com/presentations/wIPv6ld/fgont-wIPv6ld2012-seguridad-IPv6.pdf

HINDEN, R., O'DELL, M., DEERING, S. An IPv6 Aggregatable Global Unicast Address Format. s.l: IETF, 1998. RFC 2374. Disponible en Internet: http://www.ietf.org/rfc/rfc2374.txt?number=2374

SALAZAR, Jayson Y SCHAEFER, Rafael. Penetration Testing in the Age of IPv6. En: Haxpo, 2014. Disponible en Internet: http://haxpo.nl/materials/haxpo2015ams/D3%20-%20R.%20Schaefer%20and%20J.%20Salazar%20-%20Pentesting%20in%20the%20Age%20of%20IPv6.pdf

JOHNSON, D., PERKINS, C., ARKKO, J. Mobility Support in IPv6. S.l.: IETF, 2004. Disponible en Internet: https://tools.ietf.org/html/rfc3775

LACNIC. fases-de-agotamiento-de-IPv4. Montevideo: Casa de Internet de Latinoamérica y el Caribe, s.f. Disponible en Internet: http://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-IPv4

_____. Agotamiento de direcciones IPv4. Montevideo: Casa de Internet de Latinoamérica y el Caribe, s.f. Disponible en Internet: http://www.lacnic.net/web/lacnic/agotamiento-IPv4>

LUJÁN MONTES, E. F. Seguridad en Ip con el protocolo Ipsec para IPv6. Trabajo de graduación. Ciudad de Guatemala: Universidad de San Carlos de Guatemala. Facultad de Ingeniería. Escuela de Ingeniería en Ciencias y Sistemas, 2005. 158 p. Disponible en Internet: http://biblioteca.usac.edu.gt/tesis/08/08_0261_CS.pdf

KENT, S., ATKINSON, R. IP encapsulating security payload (ESP). s.l.:IETF, 1998. RFC 2406. Disponible en Internet: https://tools.ietf.org/html/rfc2406

_____., _____ . Cabecera de Autenticación. s.l. IETF, 2005. RFC 2402. Disponible en Internet: https://www.rfc-es.org/rfc/rfc2402-es.txt

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN DE Colombia. Guía de Aseguramiento del protocolo IPv6. Bogotá: MINTIC, 2015. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf>

MINISTRY OF DUTCH ECONOMIC. Testing the security of IPv6 implementations. Dutch: s.f. Disponible em Internet: https://www.tno.nl/media/3274/testing_the_security_of_IPv6_implementations.pdf

MORALES SALAZAR, J. I. Curso seguridad avanzada de redes de datos. Bogotá: Datateca-UNAD. Disponible en Internet: http://datateca.unad.edu.co/contenidos/233015/233015Exe/leccin_23_seguridad_enfocada_a_IPv6.html

NARTEN, T., NORDMARK, E. SIMPSON, W. Neighbor Discovery for IP Versión 6 (IPv6). s.l.: IETF, 1998. RFC 2461. Disponible en Internet: https://tools.ietf.org/html/rfc2461

NEDERLANDSE IPV6 TASK FORCE. Testing the security of IPv6 implementations. S.l.: 2014. Disponible en Internet: http://new.IPv6-taskforce.nl/cms/wpcontent/uploads/testing_the_security_of_IPv6_implementations.pdf

RIVERO CORVALAN, Nicolás. IPv6 – Atacando el Neighbor Discovery. En: Consejo Federal de Decanos de Ingeniería, 2013. Disponible en Internet: http://conaiisi.frc.utn.edu.ar/PDFsParaPublicar/1/schedConfs/8/38-470-1-DR.pdf

SANTOS DEL RIEGO, A. Ataques a IPv6: THC-IPv6. Galicia: Universidad de la Coruña, (2010). Disponible en Internet: http://www.tic.udc.es/~nino/blog/psi/2010/IPv6.pdf

CHOWN, T. IPv6 implications for network scanning. s.l.: IETF, 2008. RFV 5157. Disponible em Internet: https://tools.ietf.org/html/rfc5157

SI6 Networks IPv6. Seguridad en IPv6. S.l.: SI6 Networks, 2011. Disponible en Internet: https://www.si6networks.com/presentations/wIPv6ld/fgont-wIPv6ld2012-seguridad-IPv6.pdf

_____. Toolkit. s.f. Disponible en Internet: https://www.si6networks.com/tools/IPv6toolkit

S.N. Tipos de estudio [en línea], 28 de agosto de 2012 [revisado 18 de noviembre 2017]. Disponible en Internet: http://www.tiposde.com/ciencia/estudio/tipos-de-estudio.html.

TEIXEIRA, Fabiano de Assis. MEDIDAS DE SEGURANÇA PARA AS PRINCIPAIS VULNERABILIDADES DO PROTOCOLO ipv6. Trabajo de conclusión de curso. Serra: Instituto Federal do Espírito Santo. Curso Superior de Tecnología em Redes de Computadores, 2014, 84 p. Disponible em Internet: http://labseg.ifes.edu.br/wp-content/uploads/2014/11/Vulnerabilidades-do-protocolo-IPv6-Versao-final.pdf

THE GOVERNMENT OF THE HONG KONG. IPv6 SECURITY. En: The Government of the Hong Kong Special Administrative Region, 2011. Disponible en internet: http://www.infosec.gov.hk/english/technical/files/IPv6s.pdf

THC IPv6 Toolkit [página WEB]: s.f. [revisado 18 de noviembre de 2017]. Disponible en Internet: https://www.thc.org/thc-IPv6

VIVAR SOTO, J. E. Seguridad en IPv6 con IPsec. Trabajo de titulación. Punta Arenas: Universidad de Magallanes. Facultad de ingeniería. Departamento de Ingeniería en Computación, 2008. 58 p. Disponible en Internet: http://www.umag.cl/biblioteca/tesis/vivar_soto_2008.pdf

VIRTUALBOX [página WEB]: Oracle [revisado 18 de noviembre de 2017]. Disponible en Internet: https://www.virtualbox.org/.

WIRESHARK [página WEB]. s.f. [revisado 18 de noviembre de 2017]. Disponible en Internet: https://www.wireshark.org

WOODYATT, J. Recommended simple security capabilities in customer premises equipment (CPE) for providing residential IPv6 internet service. s.l.: IETF, 2011. RFC 6092. Disponible en Internet: https://tools.ietf.org/html/rfc6092.

ZAPATA VALDEZ, R. H. Análisis de Seguridad en el protocolo IPv6. Trabajo final. Buenos Aires: Universidad de Buenos Aires. Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e ingeniería, Especialización en Seguridad Informática, 2013. 77 p. Disponible en Internet: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0820_ZapataValdezRH.pdf

NORMA TÉCNICA COLOMBIANA - NTC 1486. [en línea] [Revisado en Diciembre 1 de 2017]. Disponible en Internet: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

ANEXOS

ANEXO A. CONFIGURACIÓN DE FIREWALL AMBIENTE LAN

root@IPV6-LAB-ISP> show configuration | display set
set version 12.1X46-D30.2
set system host-name IPV6-LAB-ISP
set system root-authentication encrypted-password "1NxNjcxrK$pIY7J.8fS/a9WOs3SCnF5/"
set system login user abelardo uid 2004
set system login user abelardo class super-user
set system login user abelardo authentication encrypted-password "1dZGAHbEs$NGgGO/m0wwuygO3BHBT961"
set system services ftp
set system services ssh root-login allow
set system services ssh protocol-version v2
set system services telnet
set system services web-management http
set system syslog archive size 100k
set system syslog archive files 3
*set system syslog user * any emergency*
set system syslog file messages any critical
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands error
set system max-configurations-on-flash 30
set system max-configuration-rollbacks 30
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set interfaces fe-0/0/0 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/0 unit 0 family ethernet-switching vlan members lab-lan
set interfaces fe-0/0/1 unit 0 family inet6 address 2001:db8:0:1:2a0:a502:0:1da/64
set interfaces fe-0/0/2 unit 0 family inet6 address 2000::4:1/64
set interfaces fe-0/0/3 unit 0 family inet6 address 2000::4:2/64
set interfaces fe-0/0/4 unit 0 family inet6 address 1000::4:2/64
set interfaces fe-0/0/5 unit 0 family inet6 address 1000::4:1/64
set interfaces fe-0/0/6 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/6 unit 0 family ethernet-switching vlan members lab-lan
set interfaces fe-0/0/7 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/7 unit 0 family ethernet-switching vlan members lab-lan
set interfaces vlan unit 0 family inet
set interfaces vlan unit 0 family inet6 address 2006::4:1/64
set interfaces vlan unit 100 family inet6 address 2010::4:1/64
set security forwarding-options family inet6 mode flow-based
set security policies default-policy permit-all

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces all
set routing-instances CLIENTE-1 instance-type virtual-router
set routing-instances CLIENTE-1 interface fe-0/0/1.0
set routing-instances CLIENTE-1 interface fe-0/0/2.0
set routing-instances CLIENTE-1 routing-options rib CLIENTE-1.inet6.0 static route 1000::/64 next-hop 2000::4:2
set routing-instances CLIENTE-1 routing-options rib CLIENTE-1.inet6.0 static route 2006::/64 next-hop 2000::4:2
set routing-instances CLIENTE-2 instance-type virtual-router
set routing-instances CLIENTE-2 interface fe-0/0/5.0
set routing-instances CLIENTE-2 interface vlan.0
set routing-instances CLIENTE-2 routing-options rib CLIENTE-2.inet6.0 static route 2005::/64 next-hop 1000::4:2
set routing-instances ISP instance-type virtual-router
set routing-instances ISP interface fe-0/0/3.0
set routing-instances ISP interface fe-0/0/4.0
set routing-instances ISP routing-options rib ISP.inet6.0 static route 2005::/64 next-hop 2000::4:1
set routing-instances ISP routing-options rib ISP.inet6.0 static route 2006::/64 next-hop 1000::4:1
set vlans default vlan-id 1
set vlans default l3-interface vlan.0
set vlans lab-lan vlan-id 100
set vlans lab-lan l3-interface vlan.100

ANEXO B. CONFIGURACIÓN DE FIREWALL AMBIENTE WAN

root@IPV6-LAB-ISP> show configuration | display set
set version 12.1X46-D30.2
set system host-name IPV6-LAB-ISP
set system root-authentication encrypted-password "1NxNjcxrK$pIY7J.8fS/a9WOs3S
CnF5/"
set system login user abelardo uid 2004
set system login user abelardo class super-user
set system login user abelardo authentication encrypted-password "1dZGAHbEs$NG
gGO/m0wwuygO3BHBT961"
set system services ftp
set system services ssh root-login allow
set system services ssh protocol-version v2
set system services telnet
set system services web-management http
set system syslog archive size 100k
set system syslog archive files 3
*set system syslog user * any emergency*
set system syslog file messages any critical
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands error
set system max-configurations-on-flash 5
set system max-configuration-rollbacks 5
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set interfaces fe-0/0/0 unit 0 family inet6 address 2005::4:1/64
set interfaces fe-0/0/1 unit 0 family inet6 address 2001:db8:0:1:2a0:a502:0:1da/64
set interfaces fe-0/0/2 unit 0 family inet6 address 2000::4:1/64
set interfaces fe-0/0/3 unit 0 family inet6 address 2000::4:2/64
set interfaces fe-0/0/4 unit 0 family inet6 address 1000::4:2/64
set interfaces fe-0/0/5 unit 0 family inet6 address 1000::4:1/64
set interfaces fe-0/0/6 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/6 unit 0 family ethernet-switching vlan members default
set interfaces fe-0/0/7 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/7 unit 0 family ethernet-switching vlan members default
set interfaces vlan unit 0 family inet
set interfaces vlan unit 0 family inet6 address 2006::4:1/64
set security forwarding-options family inet6 mode flow-based
set security policies default-policy permit-all
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces all

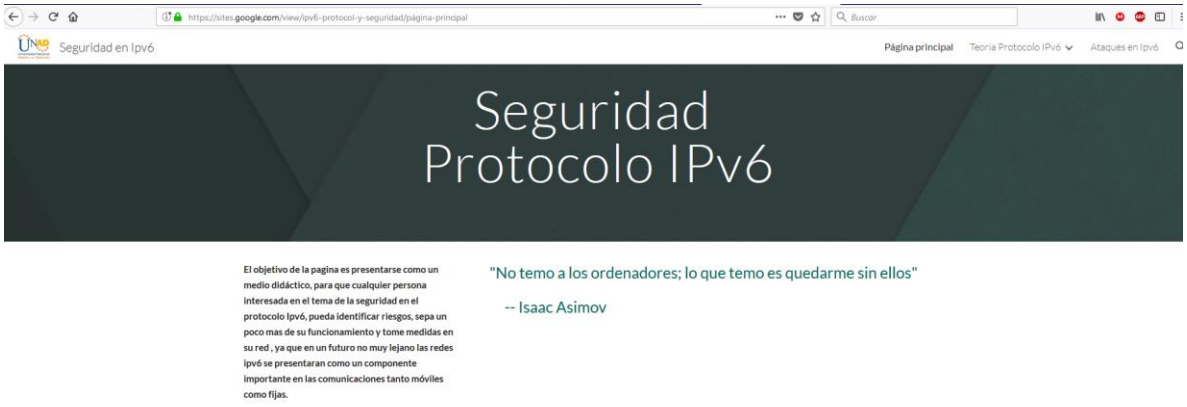
set routing-instances CLIENTE-1 instance-type virtual-router
set routing-instances CLIENTE-1 interface fe-0/0/0.0
set routing-instances CLIENTE-1 interface fe-0/0/1.0
set routing-instances CLIENTE-1 interface fe-0/0/2.0
set routing-instances CLIENTE-1 routing-options rib CLIENTE-1.inet6.0 static route 1000::/64 next-hop 2000::4:2
set routing-instances CLIENTE-1 routing-options rib CLIENTE-1.inet6.0 static route 2006::/64 next-hop 2000::4:2
set routing-instances CLIENTE-2 instance-type virtual-router
set routing-instances CLIENTE-2 interface fe-0/0/5.0
set routing-instances CLIENTE-2 interface vlan.0
set routing-instances CLIENTE-2 routing-options rib CLIENTE-2.inet6.0 static route 2005::/64 next-hop 1000::4:2
set routing-instances ISP instance-type virtual-router
set routing-instances ISP interface fe-0/0/3.0
set routing-instances ISP interface fe-0/0/4.0
set routing-instances ISP routing-options rib ISP.inet6.0 static route 2005::/64 next-hop 2000::4:1
set routing-instances ISP routing-options rib ISP.inet6.0 static route 2006::/64 next-hop 1000::4:1
set vlans default vlan-id 1
set vlans default l3-interface vlan.0

root@IPV6-LAB-ISP>

ANEXO C. PAGINA WEB

Para la construcción de la página *web* se utilizó el gestor *web* de google conocido como *google site*. El gestor permitió crear una página web sin pago de *hosting*. La pantalla inicial de la página se puede consultar en el *link*:

https://sites.google.com/view/IPv6-protocol-y-seguridad/p%C3%A1gina-principal



ANEXO D. RESUMEN ANALITICO RAE

Título del Documento.	ANÁLISIS DE LA SEGURIDAD AL IMPLEMENTAR UNA RED CON PROTOCOLO IPV6
Autor	NAVA MESA, Abelardo
Palabras Claves	ataque, riesgo, amenaza, ipv6, cabecera, fragmentación, icmp, paquete, frame, spoofing, link, nodo, interfaz, protocolo

Descripción

Este trabajo se concentra en desarrollar un ambiente de pruebas a través de un laboratorio o ambiente tecnológico controlado con el fin de no romper la ley 1273 de 2009, y realizar pruebas y recomendaciones del protocolo Ipv6, tuvo como propósito identificar los riesgos, vulnerabilidades y ataques que se presentan en una red que implemente el protocolo Ipv6. Para dar cumplimiento los objetivos, se planteó una investigación cuantitativa con base en diseño experimental, con la cual se implementa un laboratorio en un ambiente tecnológico controlado con este se realiza la recolección técnica de datos e información y el análisis del contenido tanto en un ambiente de área local como de área amplia. Las pruebas se realizan aprovechando la funcionalidad de router virtual presenten en firewall juniper srx-100 y también con host físicos y máquinas virtuales usando software licenciado como es Windows 10, 7 y distribuciones GNU como Kali Linux y raspian, también se realizan capturas de tráfico para ser analizadas por wireshark y examinar el comportamiento del protocolo IPv6. Los resultados mostraron en mayor medida como se puede llevar a cabo un test de pruebas del protocolo y como es factible generar recomendaciones y mejores prácticas, para resguardar los resultados dentro de los objetivos se presenta una página web donde cualquier usuario pueda disponer de estos como información de consulta.

Fuentes Bibliográficas	CAZAR JÁCOME, D. A. Análisis de Ip spoofing en redes IPv6. Proyecto de grado. Quito: Escuela Politécnica Nacional de Ecuador. Facultad de ingeniería Eléctrica y Electrónica, 2015. 118 p. Disponible en Internet: http://bibdigital.epn.edu.ec/bitstream/15000/10917/1/CD-6335.pdf CONTADOR VILCHES, N.. Análisis de seguridad de IPv6 pruebas y recomendaciones. Tesis de Maestría. Viña del Mar: Universidad

Andrés Bello, 2013. 33p. Disponible en Internet: https://profesores.ing.unab.cl/~druete/archivos/cursos/TM/Presentaciones/Presentaci%C3%B3n%201/Tesis%20Proyecto%20Magister%20-%20Nicolas%20Contador.doc>

COOPER, A., GONT, F. Security and Privacy Considerations for IPv6 Address Generation Mechanisms. s.l. :IETF, 2016. RFC 7721. Diponible en Internet: https://tools.ietf.org/html/rfc7721

DAVIES, E., KRISHNAN, S., SAVOLA, P. IPv6 Transition/Coexistence security considerations. s.l.: IETF, 2007. RFC 4942. Disponible en Internet: https://www.ietf.org/rfc/rfc4942.txt

FRANKEL, S., GRAVEMAN, R., PEARCE, J., ROOKS, M. Guidelines for the secure deployment of IPv6. Gaithersburg: NIST 2010. 188 p. Disponible en Internet: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=907211

FLORENTINO, Adilson Aparecido. Segurança em Redes IPv6. En: Portal do IPv6, [Base de datos en linea] [Citado en 28 de Noviembre de 2016]Disponible en ftp://ftp.registro.br/pub/gts/gts19/03-SegurancaRedesIPv6.pdf

GARCÍA MARTÍN, C. Análisis de seguridad en redes IPv6. Proyecto fin de carrera. Madrid: Universidad Carlos III de Madrid. Escuela Politécnica Superior. Departamento de Ingeniería Telemática, 2012. 143 p. Disponible en Internet: https://e-archivo.uc3m.es/bitstream/handle/10016/16707/PFC_Carlos_Garcia_Martin.pdf

GONT, F. Seguridad en IPv6. s.l.: SI6 Networks, 2012. Disponible en Internet: https://www.si6networks.com/presentations/wIPv6ld/fgont-wIPv6ld2012-seguridad-IPv6.pdf

VIVAR SOTO, J. E. Seguridad en IPv6 con IPsec. Trabajo de

	titulación. Punta Arenas: Universidad de Magallanes. Facultad de ingeniería. Departamento de Ingeniería en Computación, 2008. 58 p. Disponible en Internet: http://www.umag.cl/biblioteca/tesis/vivar_soto_2008.pdf

Contenido: Durante el desarrollo del protocolo IPv6 se ha creado una falsa expectativa respecto a su seguridad por ejemplo (el uso de *Ipsec* va a ser nativo, no se requiere uso de *nat*, será imposible escanear los servicios de red además la falta de experiencia en implementaciones IPv6 y la falta de personal capacitado hace necesario que se difunda el conocimiento del protocolo sobre todo en seguridad.

El protocolo IPv6 como cualquier desarrollo tecnológico tiene fallas que pueden ser explotadas, algunos ataques factibles a realizar serian denegación de servicio (*DoS*), hombre en el medio (*MiM*), falsificar el *router advertisements*, testear y vulnerar los *stack* en los sistemas operativos, sesión *hijaking*, crear *worms* y *exploits* de IPv6; lo cual teniendo un buen conocimiento y *hardening* de la infraestructura evita o baja la probabilidad de una explotación de estos puntos débiles.
Por lo tanto, se formula esta pregunta ¿Cómo el análisis de la seguridad al implementar una red con protocolo IPv6 puede disminuir los ataques e intrusiones en una infraestructura operativa de una red?, y para lograr responderla se define un objetivo principal, Realizar un estudio de la seguridad en el protocolo IPv6 en un entorno tecnológico controlado, Para esto es necesario cumplir varios propósitos descritos a continuación:
Revisar el estado de arte actual del protocolo IPv6 con este objetivo se buscan trabajos anteriores y para observar que metodologías y laboratorios han utilizado para el desarrollo de este tipo de proyectos, también se ha de identificar y analizar los tipos de ataques que se pueden desarrollar con el uso del protocolo IPv6 a través de la lectura de rfc y de los trabajos anteriores se puede cumplir este objetivo, Generar un plan de pruebas en los escenarios tecnológicos para el protocolo IPv6 para esto se crean laboratorios en entornos de red de área amplia y área local para generar ataques y probar vulnerabilidades que estén presentes en el protocolo y afecten la seguridad de la información y con esto hacer una demostración práctica sin afectar un red que este en producción ya que los laboratorios están en ambientes tecnológicos controlados, luego de superado esto se puede proceder con el siguiente objetivo, Recomendar las mejores prácticas de la seguridad informática para los dispositivos de red que funcionen con IPv6 este se fundamenta en analizar los hallazgos presentes y fundamentándose en la documentación técnica que se encuentra presente del protocolo Ipv6 finalmente y como último objetivo específico es crear una página web donde se subirán las evidencias, pruebas y recomendaciones, encontrados durante el desarrollo del proyecto, se aprovecha que google sites permite realizar publicaciones gratuitas y por lo tanto los laboratorios y recomendaciones de la monografía se dejan en on line.
El corazón del proyecto es el uso de un firewall marca juniper modelo srx-100 el cual permite dentro de su configuración crear el ambiente de pruebas con el cual se prueba el protocolo Ipv6, se deja descripción de las plantillas implementadas para

crear dos ambientes tecnológicos controlados un de red de área remota y uno de red de área local , en el ambiente de área remota o amplia se simula a través del uso del concepto de routers virtuales para que con un solo equipo físico simular tres routers y permitir el paso de tráfico Ipv6 en este ambiente, luego se modifica por líneas de comando la configuración para simular una red de área local usando un vlan específica, además con estos dos laboratorios se usan los dos tipos de direccionamientos que utiliza Ipv6 las direcciones de global-link y local-link, con la disposición de direccionamiento se integra una máquina virtual en virtual box que contiene kali Linux y con esta se realizaran los ataques sin embargo kali Linux permite construir paquetes a través del software scapy pero al ser un poco dispendioso el uso y construir uno a uno los paquetes Ipv6 se decide usar dos herramientas de pruebas del protocolo Ipv6 como son Ipv6 Toolkit y THC-IPv6 Toolkit, cada herramienta ofrece una amplio set de pruebas que se usan para probar en cada host víctima y determinar qué tipos de ataques son efectivos, el primer ataque definido son los escaneo de redes y se demostró en las pruebas que si no se asegura las definiciones de seguridad en Ipv6 de cada host independiente del sistema operativo se puede identificar fácilmente una red Ipv6. En las siguientes pruebas se estima realizar ataques tanto de fragmentación de paquetes, jumbo frames y observar el comportamiento de las víctimas frente a este tipo de ataques y realizar el análisis respectivo, además se incluye laboratorios de las técnicas spoofing y las recomendaciones para mitigar riesgos en la red.

Metodología

El método empleado para desarrollar el proyecto se basó en la investigación del funcionamiento del protocolo IPv6. Posteriormente, con este conocimiento, se realizó un diseño de un laboratorio que permitió probar vulnerabilidades que presenta el protocolo

METODOLOGÍA DE DESARROLLO

Para cumplir los objetivos las actividades desarrolladas en la metodología fueron:

1. Estudio, revisión y lectura del estado de arte actual sobre el protocolo IPv6 incluyendo la RFC tanto de seguridad como el funcionamiento del protocolo IPv6. De esta manera se identificaron las vulnerabilidades más recurrentes con el protocolo IPv6.
2. Diseño de esquema de pruebas basado en un laboratorio, el cual contó como mínimo con tres dispositivos de estudio: uno o varios hosts de servicio; un host cliente y una máquina atacante.
3. Ejecución de los ataques en ambos ambientes local y remota. Se capturaron los datos, anotó que no todos los ataques fueron factibles en este laboratorio y por lo tanto se documentó el posible motivo.
4. Se documentaron y analizaron los resultados obtenidos del laboratorio.
5. Se generaron las recomendaciones para fortalecer la red IPv6 ante la vulnerabilidad.
6. Se capturaron datos y documentaron en el trabajo de grado.
7. Se realizó el montaje de la página web con las evidencias recolectadas.

Conclusiones

Es factible desarrollar un entorno tecnológico controlado para simular ataques que impliquen la utilización del protocolo IPv6. En ese entorno el componente más costoso fue el equipo Juniper srx-100 que aun así se destaca ofreciendo una ventaja en cuanto a la versatilidad de configuración que permite crear ambientes de área local como de área remota para simular ataques a través del uso de máquinas virtuales y dispositivos que soportan el protocolo IPv6.

El protocolo IPv6 hace uso intrínseco de los paquetes ICMPv6 y *Neighbor Discovery* y es más recurrente no filtrar paquetes ICMP, a diferencia del protocolo IPv4. Se debe evaluar de una manera más estricta qué tipo de señales de control permitir y/o restringir ya que el uso de esas señales y descubrimiento es necesario en cualquier entorno de red local o remoto.

El escaneo de red a través de paquetes tcp-syn es factible en IPv6 y aunque estos paquetes generalmente se consideran válidos también pueden ser usados para generar ataques de negación del servicio. Por lo tanto, se tiene una dificultad al identificar qué tipos de tráfico son válidos en una red.

En los esquemas de seguridad perimetral se debe considerar el uso de un equipo de seguridad de aplicaciones (WAF), ya que hay una exposición a ataques a nivel de red que un *firewall stateless* o *stateful* no son capaces de gestionar por las funcionalidades que incluye el protocolo como son el uso ICMPv6.

Con el uso extendido de ICMPv6 en las redes IPv6 se debe recurrir de manera más exigente a la utilización de mecanismos de seguridad como Ipsec. Esa estrategia garantiza la autenticación, confiabilidad e integridad. Al igual que en la versión anterior del protocolo se debe recurrir a la protección de las capas superiores usando, por ejemplo, certificados digitales y el protocolo https.

Los laboratorios como componentes prácticos ofrecen la oportunidad de recrear ataques que permanecen vigentes. De forma didáctica, los laboratorios permiten identificar patrones y comportamientos en los entornos de red para que los administradores de red e ingenieros de seguridad tomen decisiones que conlleven a una mejor protección de la seguridad de la información.

Recomendaciones.

Las recomendaciones iniciales que genera el proyecto son:

- Activación de reglas de firewall en cada sistema operativo inmersa en una red Ipv6.
- Usar cifrado y autenticación, aunque se consideró que nativamente Ipv6 iba usar Ipsec por defecto esto no es del todo cierto, por lo tanto, es responsabilidad de los administradores usar tanto Ipsec que se fundamenta en la autenticación y cifrado de paquetes, también es importante usar en las aplicaciones certificados digitales y https para evitar vulnerabilidades en capas superiores.
- Realizar test y auditorías a los sistemas operativos y sus nuevas versiones ya que no todos los stack ni en Linux ni en Windows tienen las mismas reacciones frente a los paquetes Ipv6.
- Sabiendo que la capa de red es vulnerable en Ipv6 se va a extender el uso de Firewall de aplicaciones para revisar capas superiores y que no se presenten riesgos en los sistemas, host o aplicaciones que usen Ipv6.
- Capacitar al personal ingenieros de redes y seguridad en el funcionamiento y debilidades del protocolo Ipv6
- No es factible evitar los paquetes reconocidos del protocolo (ICMPv6, ND).
- Tener instalado un IPS/IDS y verificar comportamientos de red anómalos.
- Realizar pentesting de equipos de forma periódica.

- Mantener actualizados sistemas operativos.
- Utilizar Firewall y filtrar paquetes ICMPv6 no necesarios a criterio del administrador como Redirect.
- Usar función de port-security en switches para evitar gran cantidad de direcciones mac fuente.
- Los router deben estar actualizados para evitar que pasen tráfico multicast dirección ff02::1 de origen.
- Se recomienda uso de deep inspection packet para comprobar contenido de paquetes.
- Mantener actualizados sistemas operativos para evitar vulnerabilidades antiguas en el stack ipv6.