ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS DE IP SPOOFING EN REDES IPV6

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

DANIEL ALEJANDRO CAZAR JÁCOME
danielcazar@hotmail.com

DIRECTOR: LUIS ENRIQUE MAFLA GALLEGOS, PhD
enrique.mafla@epn.edu.ec

Quito, junio 2015

DECLARACIÓN

Yo, Daniel Alejandro Cazar Jácome, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Daniel Alejandro Cazar Jácome

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Cazar Jácome Daniel Alejandro, bajo mi supervisión.

Luis Enrique Mafla Gallegos, PhD
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Primero y antes que nada, quiero agradecer a Dios como lo concibo, por proveerme de vida y regalarme momentos de suma felicidad, como éste, el momento que supero un reto más de los tantos que vienen muy pronto. Adicionalmente, un agradecimiento especial a mi tutor de tesis, PhD. Enrique Mafla, porque gracias a su conocimiento y guía trazamos el camino para lograr la realización y culminación del proyecto. Finalmente, agradezco a todas las personas que de una u otra forma siempre han estado presentes.

DEDICATORIA

A mis personas importantes.

A mi mamá y papá, Lilia y Víctor.

A la memoria de mi primo Andrés.

A mis abuelitas y abuelitos.

A mis tías y tíos.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación trata sobre el análisis de IP Spoofing en redes IPv6[1]. Para llevar a cabo el proyecto de titulación lo separamos en 5 fases o capítulos. El primer capítulo aborda las vulnerabilidades de IPv6, la definición del problema y la metodología. Primero describiremos las vulnerabilidades de IPv6 que nos permiten ejecutar la técnica de IP Spoofing tomando en cuenta las máquinas que se verían afectadas por dicha técnica. Segundo, definimos el problema en base al objetivo principal y alcance del proyecto de titulación. Para finalizar, definimos la metodología que será utilizada para el desarrollo de todo el proyecto de titulación.

En el segundo capítulo definimos y configuramos el laboratorio de simulación. Definimos una red que nos permita explotar las vulnerabilidades de IPv6. Utilizamos herramientas de simulación disponibles en la Internet para configurar una red IPv6 dentro del laboratorio de simulación. Utilizamos VMware Workstation para simular los sistemas operativos del cliente, el monitor de red, los atacantes, los servidores, y los monitores. Utilizamos GNS3 para simular las topologías de red. Utilizamos una herramienta de hackeo disponible en la Internet llamada THC-IPv6 para lanzar los ataques que emplean la técnica de IP Spoofing. Finalmente, utilizamos un software de monitoreo de paquetes NDP[2] para alertar la presencia de un ataque sobre una red IPv6.

En el tercer capítulo realizamos las pruebas y análisis de resultados. Las pruebas las realizamos para observar cómo se llevó a cabo el ataque y para observar el efecto que dicho ataque produce sobre el cliente, monitor de red, servidor interno, y servidor público. Para lo cual, primero comparamos los valores iniciales versus los valores durante el ataque. Luego, analizamos las alertas generadas por el software de monitoreo cuando el ataque está siendo ejecutado. Posteriormente, detallamos las

[1] IPv6: Protocolo de Internet versión 6.

[2] El protocolo de Descubrimiento del vecino o en sus siglas cortas NDP está defino en la RFC4861. Es un protocolo de capa 3 del modelo ISO/OSI que forma parte de IPv6. Su función es velar por el correcto funcionamiento de los nodos dentro de un enlace.

direcciones IPv6 que se suplantaron durante el ataque. Para concluir, realizamos un análisis de resultados de cada prueba.

En el cuarto capítulo desarrollamos un plan de mitigación. El objetivo del plan es reducir el riesgo de la técnica de IP Spoofing basándonos en el análisis de resultados del capítulo tres. Para cumplir con este objetivo, realizamos el diseño de la red física a través de la arquitectura modular SAFE[3] de Cisco. Luego, este diseño de la red física lo aseguramos a través de políticas de seguridad IPSec[4]. De esta manera, garantizamos la autenticación de origen del remitente a través del uso de certificados digitales.

Finalmente, en el quinto capítulo escribimos las conclusiones y recomendaciones derivadas de la realización del presente proyecto de titulación.

[3] SAFE es un diseño modular que brinda un plan de seguridad para redes empresariales.
[4] IPSec es un conjunto de protocolos cuya función es proteger las comunicaciones que ocurren sobre el protocolo IPv4 e IPv6.

PRESENTACIÓN

El presente proyecto de titulación tiene como objetivo analizar la técnica de IP Spoofing visto como un punto de origen de ataques MITM y DoS. Para realizar el análisis utilizamos una red configurada con el protocolo IPv6 y de esta manera observamos cómo la técnica afecta a clientes y servicios muy utilizados dentro de medianas y grandes organizaciones.

La red configurada con IPv6 es una propuesta del proyecto de titulación que permite ejecutar los ataques MITM y DoS, y que utilizan la técnica de IP Spoofing. El diseño de la red no contempla ningún equipo ni mecanismo de seguridad como firewalls o listas de control de acceso porque de esta manera podemos observar todo el flujo del ataque, desde que es originado por el atacante, hasta cuando en el otro extremo las víctimas son engañadas con un remitente suplantado o falsificado.

El problema que plantea resolver el proyecto de Análisis de IP Spoofing en redes IPv6 es bien conocido y está definido en algunas fuentes disponibles en la Internet. Sin embargo, utilizamos una laboratorio de pruebas y de esta manera observamos cuales son los puntos de la red IPv6 propuesta dónde es vulnerable a la técnica de IP Spoofing. En la resolución del problema definimos un plan de mitigación que consiste en re-diseñar la red IPv6 propuesta a través de SAFE y definir políticas IPSec para los módulos de SAFE en los que observamos que la técnica de IP Spoofing tuvo éxito.

CAPITULO 1: FUNDAMENTOS TEÓRICOS

En el presente capítulo definimos la estructura del proyecto “Análisis de IP Spoofing en redes IPv6”. Para realizar esta actividad primero describiremos las vulnerabilidades de IPv6 y cómo son explotadas por los ataques locales y remotos. Posteriormente, realizaremos la definición del problema en base al objetivo y alcance del proyecto de titulación. Finalmente, detallaremos la metodología que utilizaremos para el desarrollo de todo el proyecto de titulación.

1.1 VULNERABILIDADES DE IPV6 [W1]

En la fuente [W2] está definida el concepto de vulnerabilidades informáticas como: “Las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo”. Este concepto lo modificaremos un poco para realizar una definición de vulnerabilidades IPv6 según el contexto que tratamos dentro del proyecto de titulación. Definiremos lo siguiente: “Las vulnerabilidades de IPv6 son puntos débiles presentes en el diseño del protocolo IPv6. En lo que se refiere a IP Spoofing, estas vulnerabilidades permiten que un atacante suplante o falsifique la dirección origen IPv6 de sus víctimas”.

Las vulnerabilidades de IPv6 que encontramos para la capa de red del modelo ISO/OSI están dentro de los sub – protocolos de IPv6. Los sub – protocolos que nos permiten ejecutar la técnica de IP Spoofing sobre la capa de red son: ICMPv6[5] y NDP. Adicionalmente, el alcance de IP Spoofing no está limitado a la suplantación, ya que además podemos realizar ataques como: DoS[6] y MITM[7]. En decir, esta

[5] ICMPv6 está definido en la RFC 4443, y es identificado por medio del campo Próxima Cabecera de la cabecera IPv6 configurado con el valor igual a 58. ICMPv6 informa características de la red, realiza diagnósticos, e informa errores en el procesamiento de paquetes.
[6] DoS es un ataque informático cuyo objetivo es denegar sus víctimas, dejándolas fueras de servicio.
[7] MITM es un ataque informático cuyo objetivo es interceptar la información transmitida entre dos partes sin que ellas lo conozcan.

técnica nos permite vulnerar las redes IPv6 a través de la suplantación del remitente, y adicionalmente nos permite realizar denegación de servicio e intercepción de las comunicaciones de las víctimas.

En el presente proyecto de titulación realizamos una división de las vulnerabilidades de IPv6 según el origen. Basados en el origen de las vulnerabilidades de IPv6 tenemos ataques locales y remotos. Definimos que los ataques locales son los ataques que afectan las máquinas de la misma red donde está ubicado el atacante. Mientras que los ataques remotos son los ataques que afectan las máquinas de una red externa a la ubicación del atacante. A continuación describimos estos dos grupos de ataques.

1.1.1 ATAQUES LOCALES

1.1.1.1 DoS con mensajes anuncio de vecino

El ataque DoS con mensajes Anuncio de vecino (NA) es realizado por una máquina atacante que envía mensajes falsificados Solicitud de vecino (NS) con el objetivo de denegar la asignación de direcciones IPv6 en las víctimas. El ataque ocurre en dos pasos como lo podemos observar en la figura 1.1. En el primer paso la víctima ejecuta el proceso DAD[8] y envía un mensaje Solicitud de vecino para preguntar si la dirección IPv6 que pretende utilizar está libre.

En el segundo paso el atacante utiliza la técnica de IP Spoofing y responde con un mensaje Anuncio de vecino informando que él tiene asignada esa dirección IPv6. El paso uno y dos se repiten continuamente para que la víctima no asigne una dirección IPv6 a su interfaz de red. Finalmente, el atacante consigue detener a la víctima en su afán de obtener una dirección IP libre para su configuración dentro de la LAN.

[8] DAD es el mecanismo de detección de direcciones IPv6 duplicadas.

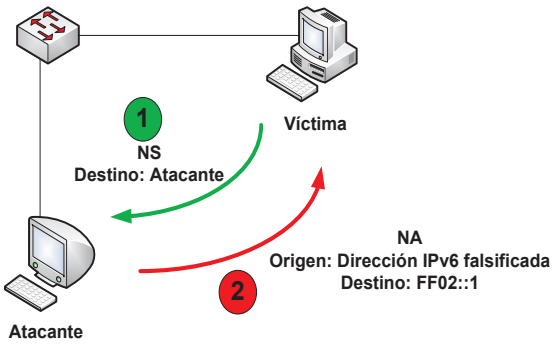

Figura 1.1 Ataque DoS con mensajes NA[9]

1.1.1.2 Mitm con mensajes anuncio de vecino

Este ataque sucede cuando un host A intenta buscar la dirección MAC de un host B que está dentro del mismo segmento de red (véase la figura 1.2). Un atacante ubicado en el mismo segmento que las víctimas A y B ejecuta la técnica de IP Spoofing. El atacante envía mensajes NA suplantados para robar la identidad de A y B. El ataque ocurre de la siguiente manera:

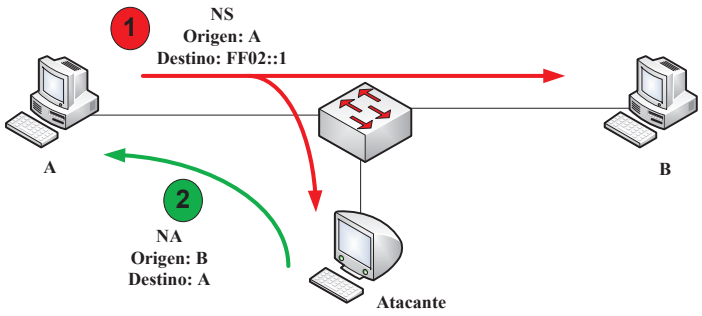

Figura 1.2 MITM con mensajes NA suplantados.[10]

1) El host A envía un mensaje NS para buscar la dirección MAC del host B. Entonces, el atacante se ubica en la misma red del host A para recibir el mensaje NS.

[9] Fuente: Autor del proyecto de titulación.
[10] Fuente: Autor del proyecto de titulación.

2) El host B y el atacante reciben el mensaje NS. El primero (el host B) responde con un mensaje NA, mientras que el segundo (el atacante) también responde con un mensaje NA utilizando la técnica de IP Spoofing, el cual le permite sobrescribir el mensaje NA enviado por el host B. En consecuencia, el host A mapea la dirección IP del host B (dirección IP suplantada por el atacante) con la dirección MAC del host atacante. Ahora, la comunicación se realizará a través del atacante.

1.1.1.3 DoS con mensajes anuncio de router

Como observamos en la figura 1.3, en un ataque DoS con mensajes *Anuncio de router (RA)*, solamente una máquina atacante actúa como varios routers con el objetivo de inundar a todos los host de la LAN. El atacante ejecuta la técnica de IP Spoofing y envía mensajes RA con la dirección de origen de routers falsos, y dirección destino FF02::1. De esta manera, la dirección destino FF02::1 permite que el ataque llegue a todos los hosts que están en la LAN, provocando que cada uno de los hosts configuren direcciones de origen falsas. El código de identificación de esta vulnerabilidad es el CVE-2010-4669 [W3].

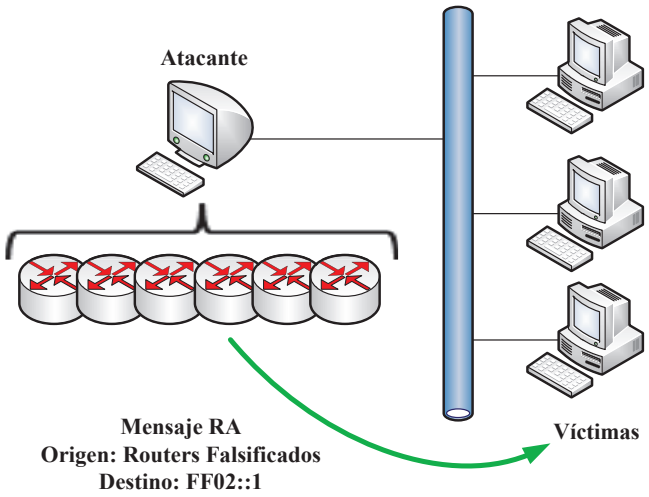

Figura 1.3 Ataque DoS con mensajes RAs.[11]

[11] Fuente: Autor del proyecto de titulación.

1.1.1.4 Smurf local

Smurf local es un ataque que genera una gran cantidad de tráfico de red con mensajes Echo Request con la dirección origen de la máquina víctima, y dirección destino FF02::1 (véase la figura 1.4). Estos mensajes permiten reclutar otras máquinas porque la dirección FF02::1 identifica a todos los hosts del enlace. De esta manera, la máquina que es víctima recibirá respuestas Echo Reply, ya que su dirección origen fue suplantada a través de la técnica de IP Spoofing.

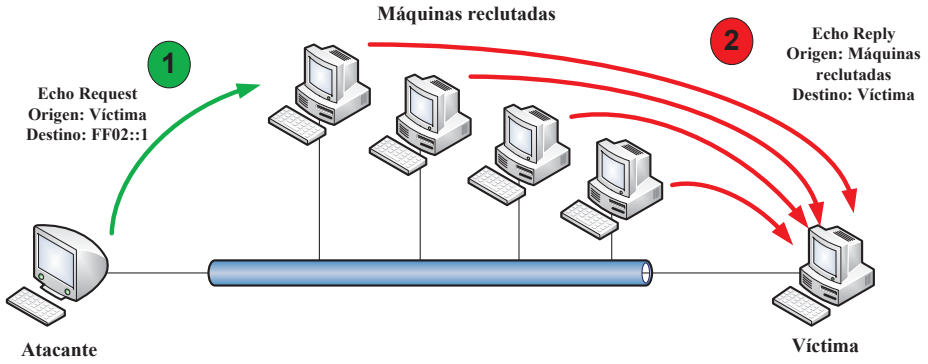

Figura 1.4 Ataque smurf local.[12]

1.1.2 ATAQUES REMOTOS

1.1.2.1 DoS con mensajes icmpv6 paquete demasiado grande

El ataque DoS con mensajes *Paquete demasiado grande* es realizado por una máquina atacante que envía mensajes falsificados *Paquete demasiado grande* para que las víctimas configuren un valor de MTU[13] diferente. El objetivo del atacante es introducir un valor de MTU menor o mayor al verdadero valor MTU del enlace.

El ataque DoS con mensajes Paquete demasiado grande ocurre en tres pasos como los podemos observar en la figura 1.5. El primer paso que realiza el atacante es

[12] Fuente: Autor del proyecto de titulación.
[13] MTU: Unidad máxima de transferencia.

enviar un mensaje Echo Request a la víctima. En el segundo paso la máquina suplantada ignorará el mensaje Echo Reply porque no realizó ninguna petición. En el tercer y último paso, el atacante introduce un valor de MTU diferente del valor real del MTU del enlace a través de un mensaje suplantado de error Paquete demasiado grande, haciendo creer que el mensaje Echo Reply que envió la víctima es demasiado grande.

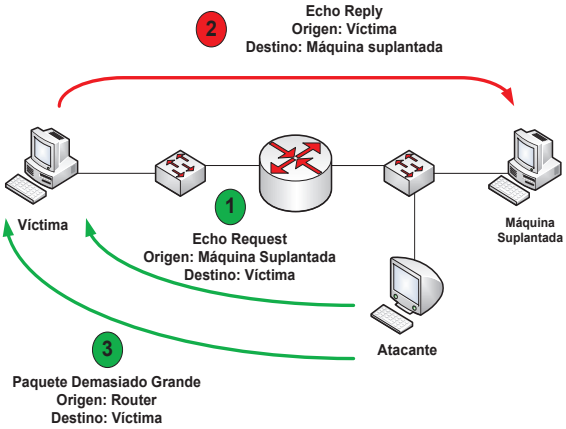

Figura 1.5 Ataque DoS con mensajes Paquete demasiado grande[14]

1.1.2.2 Mitm con mensajes redireccionamiento

Los pasos para llevar a cabo el ataque son los siguientes (véase la figura 1.6):

1) El atacante envía un mensaje suplantado Echo Request con la dirección origen del host B y dirección destino del host A.
2) El host A recibe el mensaje y responde seguidamente con un Echo Reply al host B. El host B no lo procesa porque no realizó ninguna petición Echo Request.
3) El atacante construye un mensaje suplantado redireccionamiento con la dirección origen del router y dirección destino del host A, informando que todo

[14] Fuente: Autor del proyecto de titulación.

el tráfico que esté destinado al host B debe ser enviado a través de la dirección del atacante.

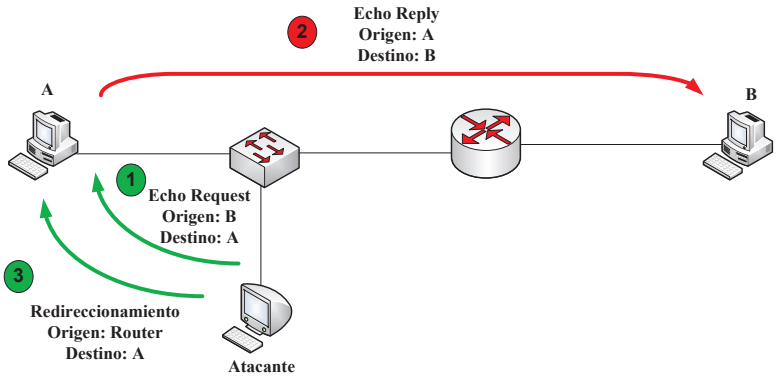

Figura 1.6 MITM con mensajes redireccionamiento.[15]

1.1.2.3 Smurf remoto

Smurf remoto es un ataque que envía una gran cantidad de tráfico de red con mensajes Echo Request con la dirección origen FF02::1, y dirección destino de la víctima (véase la figura 1.7). De esta manera, la víctima enviará respuestas Echo Reply a todos los hosts que estén en su red ya que la dirección origen suplantada fue FF02::1.

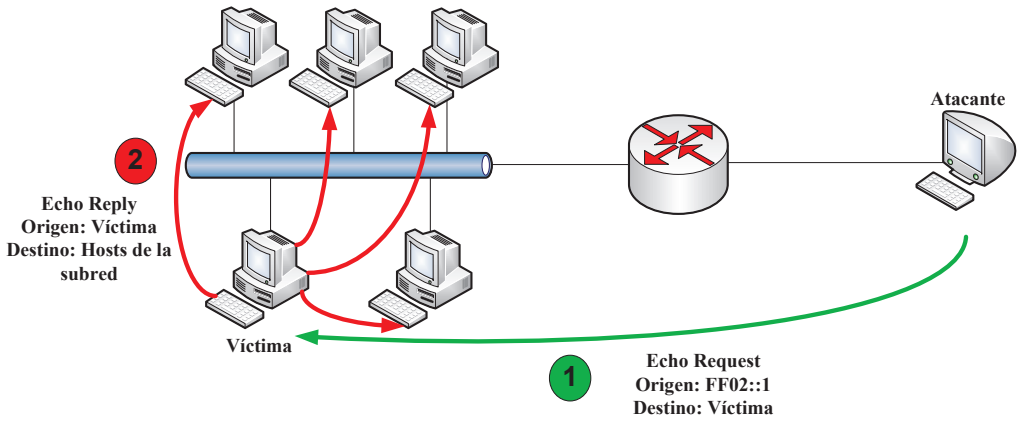

Figura 1.7 Smurf remoto.[16]

[15] Fuente: Autor del proyecto de titulación.

1.2 DEFINICIÓN DEL PROBLEMA

La técnica de IP Spoofing es bien conocida y está definida en algunas fuentes como [W4] [W5] [W6]. Sin embargo, lo que queremos realizar en el presente proyecto de titulación es definir y configurar un laboratorio de simulación que nos permita analizar la técnica de IP Spoofing en redes IPv6. El laboratorio de simulación definirá una Red Propuesta que nos permitirá probar los ataques locales y remotos de la sección 1.1.1 y 1.1.2, respectivamente. El laboratorio será construido a través de herramientas de simulación disponibles en la Internet. De esta manera, realizaremos pruebas en el laboratorio de simulación para observar el impacto que produce la técnica de IP Spoofing en redes IPv6. Cada una de las pruebas tendrá un análisis de resultados que detallan cómo se llevó a cabo el ataque. Este análisis de resultados más la arquitectura SAFE de Cisco e IPSec, nos permitirá finalmente definir la solución a través de un plan de mitigación.

1.3 METODOLOGÍA

Para el desarrollo del proyecto de titulación “Análisis de IP Spoofing en redes IPv6” utilizaremos una metodología sistemática. Esta metodología nos permitirá desarrollar el proyecto siguiendo fases de desarrollo. De esta manera, tendremos a la mano una metodología práctica que nos permitirá eliminar los errores en el momento del desarrollo del proyecto. Las fases a seguir son las siguientes:

- Definición y configuración del laboratorio de simulación.
- Pruebas y análisis de resultados.
- Plan de mitigación.

---

[16] Fuente: Autor del proyecto de titulación.

1.3.1 DEFINICIÓN Y CONFIGURACIÓN DEL LABORATORIO DE SIMULACIÓN

El principal objetivo de esta fase es realizar la definición y configuración del laboratorio de simulación para analizar la técnica de IP Spoofing sobre IPv6. Para cumplir con este objetivo, definiremos una red IPv6 que nos permita probar la técnica de IP Spoofing. La técnica de IP Spoofing la probaremos sobre una red configurada con IPv6 porque este protocolo es nuevo y trae consigo nuevas funcionalidades integradas. Esta actividad nos permitirá conocer cómo los atacantes informáticos utilizan esta técnica en un protocolo que no está totalmente desplegado y que en un futuro cercano será el núcleo de las comunicaciones que conocemos en la actualidad.

1.3.2 PRUEBAS Y ANÁLISIS DE RESULTADOS

En esta fase realizaremos las pruebas y análisis de resultados. Las pruebas serán realizadas sobre el laboratorio de simulación a través de una metodología conocida como Pruebas de Penetración o Hackeo Ético[17]. El análisis de resultados detallará como se llevó a cabo la técnica de IP Spoofing y cuál fue el efecto producido en las víctimas. Estas pruebas y el respectivo análisis de resultados permitirán conocer el nivel real de la seguridad del laboratorio de simulación frente a la técnica de IP Spoofing.

1.3.3 PLAN DE MITIGACIÓN

Esta es la última fase de la metodología utilizada para el proyecto de titulación. En esta fase definimos el plan de mitigación, el cual lo desarrollamos para disminuir los riesgos de las pruebas de la sección anterior. El plan será desarrollado a través de la arquitectura SAFE y mecanismos de seguridad de IPv6. Para lo cual, utilizaremos los

[17] Los test de penetración o hackeo ético consisten en pruebas y análisis que tienen como objetivo simular el comportamiento de un atacante informático. De tal manera, que puedan encontrar vulnerabilidades en las tecnologías de la información, y luego mitigarlas con mecanismos de seguridad preventivos y correctivos.

análisis de resultados realizados en cada una de las pruebas, y definiremos un diseño de red segura con el objetivo de disminuir el riesgo de la técnica de IP Spoofing en redes IPv6.

CAPÍTULO 2: DEFINICIÓN Y CONFIGURACIÓN DEL LABORATORIO DE SIMULACIÓN

El objetivo de este capítulo es definir y configurar el laboratorio de simulación. Para realizar esta actividad, seguimos las fases: entrada, proceso y salida, de la figura 2.1. La representación de la figura 2.1 tiene el siguiente significado: la fase entrada que contiene las vulnerabilidades de IPv6 es utilizada para realizar dos pasos o procesos, primero la definición de la red propuesta, y segundo, la configuración de la red propuesta. Como salida obtenemos el diagrama final de la red propuesta, el cual será utilizado en el siguiente capítulo.

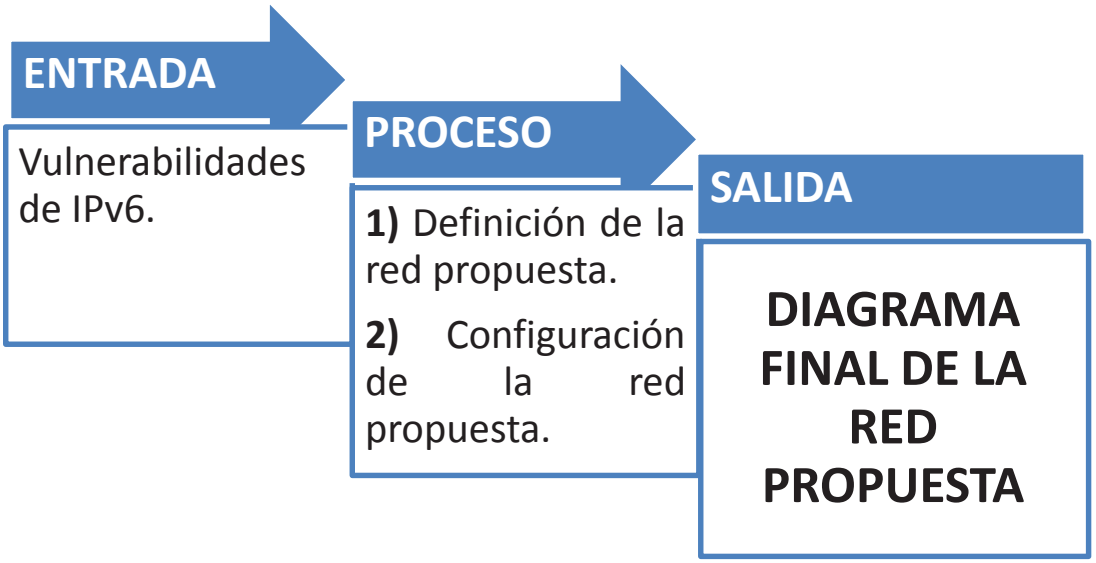

Figura 2.1 Fases de desarrollo del capítulo dos.[18]

2.1 DEFINICIÓN DE LA RED PROPUESTA

En esta sección definimos la red propuesta que nos permite ejecutar los ataques locales y remotos de la sección 1.1.1 y 1.1.2, respectivamente (véase la figura 2.2). Para poder ejecutar los ataques locales nos conectaremos a un switch y de esta

[18] Fuente: Autor del proyecto de titulación.

manera atacaremos todas las máquinas que están conectadas al switch. En cambio, para poder ejecutar los ataques remotos necesitaremos un router y de esta manera crear subredes diferentes para afectar todas las máquinas de otras subredes. Considerando estos lineamientos, en los párrafos siguientes presentaremos la definición de la red propuesta.

En la red propuesta necesitamos dos atacantes, uno ubicado en la red interna, y el otro ubicado en una red externa. Para justificar la ubicación del atacante en la red interna citamos la fuente [W7], en la cual, el Computer Security Institute (CSI) de San Francisco menciona que aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma red. En cambio, para justificar la ubicación del otro atacante en la red externa, consideramos necesario dicha ubicación, porque las redes actuales no son redes independientes, por el contrario, son redes que interactúan con muchos servicios de redes externas, e inclusive tienen la capacidad de brindar servicios públicos.

Sobre la red propuesta detallamos dos consideraciones importantes. La primera: en la red propuesta no utilizamos ningún esquema de seguridad porque de esta manera podemos observar cómo se lleva a cabo IP Spoofing, desde la ejecución de la técnica de IP Spoofing hasta cuando las víctimas reciben los mensajes IPv6 suplantados por dicha técnica. Y la segunda consideración, la red propuesta es un escenario construido para representar una red con soporte IPv6, donde configuraremos la red sin ningún mecanismo de transición a IPv6[19].

En la figura 2.2 presentamos la red propuesta realizada bajo los lineamientos, consideraciones y definiciones expuestas en los párrafos anteriores. La red propuesta está compuesta por las siguientes máquinas:

[19] Los mecanismos de transición a IPv6 son las tecnologías que facilitan y facilitarán la transición de Internet de su infraestructura IPv4 al sistema de direccionamiento de nueva generación IPv6.

- **Monitores:** Son máquinas que tienen software instalado para monitorear los ataques que utilizan la técnica de IP Spoofing en redes IPv6. La función de los monitores es similar a un sistema de detección de intrusos (IDS). Utilizamos los monitores para detectar los ataques locales y remotos de la sección 1.1.1 y 1.1.2, respectivamente.
- **Atacantes:** Son máquinas que tienen herramientas de hackeo IPv6 instaladas. Las máquinas las utilizamos para ejecutar los ataques locales y remotos.
- **Víctimas:** Son máquinas que representan el cliente, los servidores internos y los públicos.
- **Cliente:** Es la estación de trabajo que consume los servicios ofrecidos por los servidores.
- **Servidores:** Son máquinas que brindan un servicio sobre el protocolo IPv6.
- **Monitor de red:** Es una máquina que administra el rendimiento de los servidores de la red propuesta.

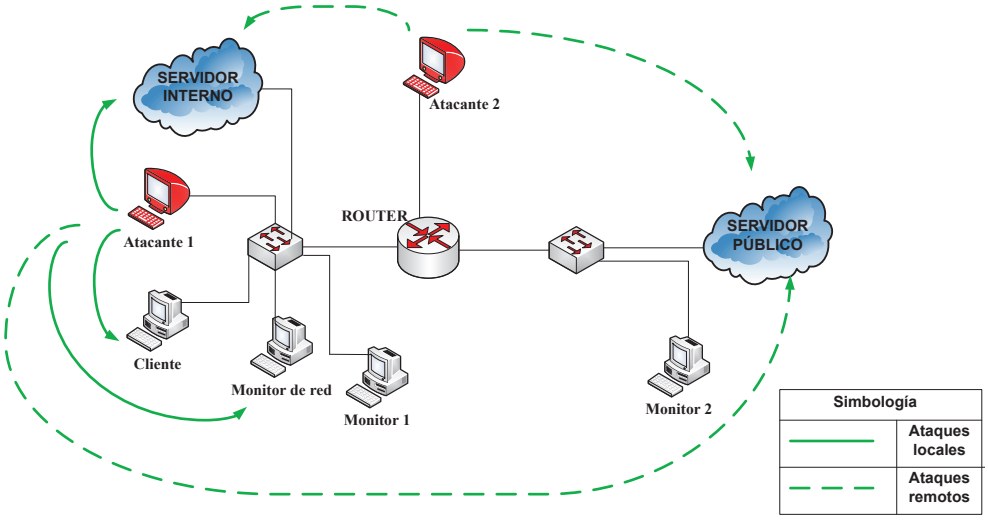

Figura 2.2 Red propuesta.[20]

[20] Fuente: Autor del proyecto de titulación.

2.1.1 MÁQUINAS VIRTUALES

En esta sección elegimos las máquinas virtuales para la red propuesta. Utilizamos VMware[21] para optimizar el tiempo que nos llevaría en realizar un laboratorio con equipos reales, y además para ahorrar en costos de implementación de máquinas físicas. Creamos máquinas virtuales para todas las máquinas participantes de la red propuesta de la figura 2.2. Elegimos el sistema operativo Windows 7 para la máquina del cliente porque es más popular que el resto de sistemas operativos, así lo recoge la estadística presentada en la figura 2.3. Para los servidores elegimos la distribución Windows Server 2008 y Centos 6.2 porque la mayoría de servidores corren sobre estos dos sistemas operativos Windows y Linux. En cambio, dentro de la sección 2.1.3 y 2.1.4 elegimos el sistema operativo del atacante y del monitor, respectivamente.

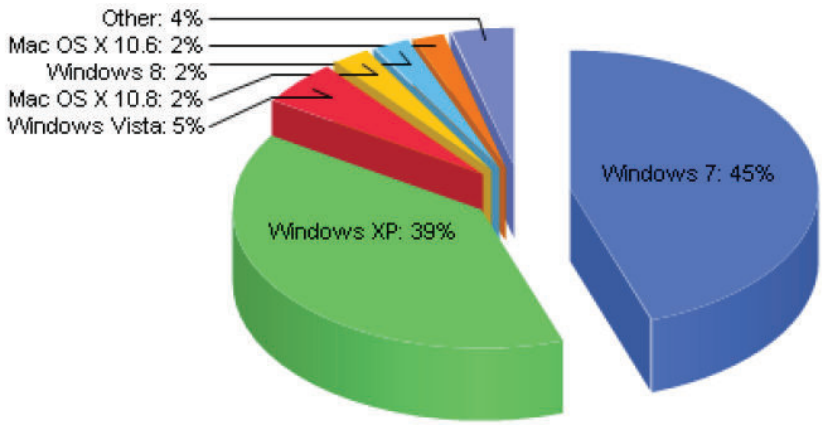

Figura 2.3 Mercado mundial de los sistemas operativos.[W8]

2.1.2 DISPOSITIVO DE RED [L1]

En esta sección elegimos el dispositivo de red que utilizamos en la red propuesta. El dispositivo de red que utilizamos en la simulación de GNS3[22] es un router de Cisco. La elección de dicho router la realizamos bajo el siguiente criterio:

[21] VMware es un sistema de virtualización de sistemas operativos.
[22] GNS3: Simulador gráfico de red.

- El router deberá soportar el protocolo IPv6. Para cumplir con este requerimiento probamos si el router tiene el soporte IPv6 integrado en la IOS. El router que escogemos para emular en GNS3 es un modelo Cisco c7200 porque contamos con más experiencia que las otras series como c1700, o c2600. La comprobación la realizamos digitando el comando **show ipv6 ?**. Enseguida nos muestra una lista de comandos, lo cual significa que el router sí soporta IPv6.

2.1.3 ATACANTE

En esta sección elegimos la herramienta de hackeo para las máquinas atacantes. La herramienta de hackeo que nos permite ejecutar los ataques locales y remotos es THC – IPv6. La ventaja principal por la cual elegimos esta herramienta respecto de otras como SI6 Networks' IPv6 Toolkit[23], y Scapy6[24], es debido a su constante actualización, y porque periódicamente pudimos encontrar en su página Web oficial nuevas versiones con más funcionalidades y mejoras.

2.1.4 MONITOR

En esta sección elegimos el software de monitoreo para detectar los ataques que utilizan la técnica de IP Spoofing. Para detectar los ataques locales y remotos utilizaremos una máquina monitor con el software NDPmon. Aunque existen monitores disponibles como: ramond[25], rafixd[26], IPv6mon[27], la principal ventaja por la que utilizamos NDPmon es debido a su suficiente documentación de apoyo, y porque nos ofrece la facilidad de monitorear la red a través de una interfaz web, característica que no tiene integrada los otros monitores.

---

[23] SI6 Networks' IPv6 está disponible en la siguiente dirección: http://www.si6networks.com/tools/ipv6toolkit/
[24] Scapy6 está disponible en la siguiente dirección: http://www.secdev.org/projects/scapy/
[25] Ramond está disponible en la siguiente dirección: http://ramond.sourceforge.net/
[26].Rafixd está disponible en la siguiente dirección: https://github.com/gws/rafixd
[27] IPv6mon está disponible en la siguiente dirección: http://www.si6networks.com/tools/ipv6mon/

La única desventaja encontrada en esta herramienta es que solamente detecta los ataques que intercambian mensajes NDP. Los mensajes ICMPv6 utilizados en los ataques Smurf local, DoS con mensajes Paquete demasiado grande, y Smurf remoto, no son detectados por este software de monitoreo. Lo que realizamos para observar que se está llevando a cabo la técnica de IP Spoofing, es utilizar Wireshark[28] para analizar mensaje por mensaje como ocurre la técnica.

2.2 CONFIGURACIÓN DE LA RED PROPUESTA

En esta sección configuramos la red propuesta. Para lo cual, primero realizamos el direccionamiento IPv6 en base a la red propuesta definida en la sección 2.1. Una vez realizado el direccionamiento IPv6, configuramos los servicios que brindamos a través de los servidores de la red propuesta. Enseguida mencionamos el direccionamiento IPv6 en la sección 2.2.1 y los servicios en la sección 2.2.2.

2.2.1 DIRECCIONAMIENTO IPV6

En esta sección realizamos el direccionamiento IPv6 de la red propuesta. Las acciones realizadas sobre la figura 2.4 son las siguientes:

- Configuramos manualmente una dirección global en la interfaz de red del atacante 2. Elegimos una dirección global porque el atacante 2 representa una máquina que está ubicada en una red externa.
- Configuramos en el router un prefijo de red del rango de direcciones IPv6 ULA[29] para la interfaz que está conectada hacia la máquina cliente. Esta acción la realizamos para que el router asigne automáticamente la dirección IPv6 ULA a una máquina cliente que representa los usuarios finales de la red interna. Elegimos asignar automáticamente la dirección IPv6 ULA porque es

[28] Wireshark es un analizador de protocolos utilizado en este proyecto de titulación para analizar la técnica de IP Spoofing.
[29] ULA: dirección IPv6 única local.

nuevo método integrado dentro de la funcionalidad de IPv6 que deseamos experimentar.

- Configuramos una dirección IPv6 ULA manualmente en las siguientes máquinas: monitor 1, monitor de red, atacante 1, y servidor interno.
- Configuramos una dirección global manualmente en las siguientes máquinas: monitor 2 y servidor público.

En la tabla 2.1 detallamos las direcciones utilizadas para el cliente, el monitor de red, los monitores, los atacantes, los servidores y las interfaces del router.

Tabla 2.1 Direccionamiento IPv6 de la red propuesta.[30]

Máquina	Asignación de direcciones	Prefijo / Dirección IPv6	Dirección MAC
Cliente	Stateless	FD00::/64	00-0C-29-B6-E2-36
Monitor de red	Manual	FD00::6	00-0C-29-CF-09-5A
Monitor 1	Manual	FD00::7	00-0C-29-FE-FC-A6
Monitor 2	Manual	2800:68:c:214::7	00-0C-29-4E-7C-DD
Atacante 1	Manual	FD00::1	00-0C-29-EB-17-2F
Atacante 2	Manual	2800:68:c:215::1	00-0C-29-1B-82-95
Servidor interno	Manual	FD00::5	00-0C-29-BD-27-97
Servidor público	Manual	2800:68:c:214::6	00-0C-29-C7-66-E7
Fa 1/0	Manual	FD00::100	CA-00-16-30-00-1C
Fa 1/1	Manual	2800:68:c:214::100	CA-00-16-30-00-1D

[30] Fuente: Autor del proyecto de titulación.

Fa 2/0	Manual	2800:68:c:215::100	CA-00-16-30-00-38

2.2.2 SERVICIOS

Los servicios que configuramos en el servidor interno son HTTP[31], DNS[32], y Directorio activo. Para el servidor público solamente configuramos FTP[33]. Utilizamos IIS, DNS, y Directorio Activo de Windows Server 2008 para implementar el servicio HTTP, DNS, y Directorio activo, respectivamente. Utilizamos vsftpd para implementar el servicio FTP. Las acciones realizadas en cada de los servicios son las siguientes:

- Configuramos un dominio dentro del servidor DNS. El dominio para las pruebas será ipspoofing.com.
- Configuramos en el servidor HTTP una página WEB[34] de bienvenida al visitante. La página nos permitirá mostrar la dirección IPv6 del visitante cuando accede al servidor HTTP.
- Configuramos un usuario TTHH en el servidor de Directorio activo. El usuario representará los usuarios finales del área de Talento Humano.

El servicio configurado en el monitor de red es SNMP[35]. Utilizamos PRTG para implementar el servicio SNMP. La acción realizada en el monitor de red es la siguiente:

- Configuramos PRTG[36] para monitorear la carga de CPU y memoria de los servidores internos y público.

[31] HTTP: Protocolo de transferencia de hipertexto.
[32] DNS. Sistema de nombres de dominio.
[33] FTP: Protocolo de transferencia de archivos.
[34] WEB: Red informática mundial.
[35] SNMP: Protocolo simple de administración de red.
[36] PRTG es un monitor de red.

2.3 DIAGRAMA FINAL DE LA RED PROPUESTA

En esta sección presentamos el diagrama final de la red propuesta en la figura 2.4. Este diagrama es el resultado de las secciones 2.1 y 2.2, definición de la red propuesta y configuración de la red propuesta, respectivamente. Este diagrama nos permitirá ejecutar los ataques que utilizan la técnica de IP Spoofing en el siguiente capítulo tres.

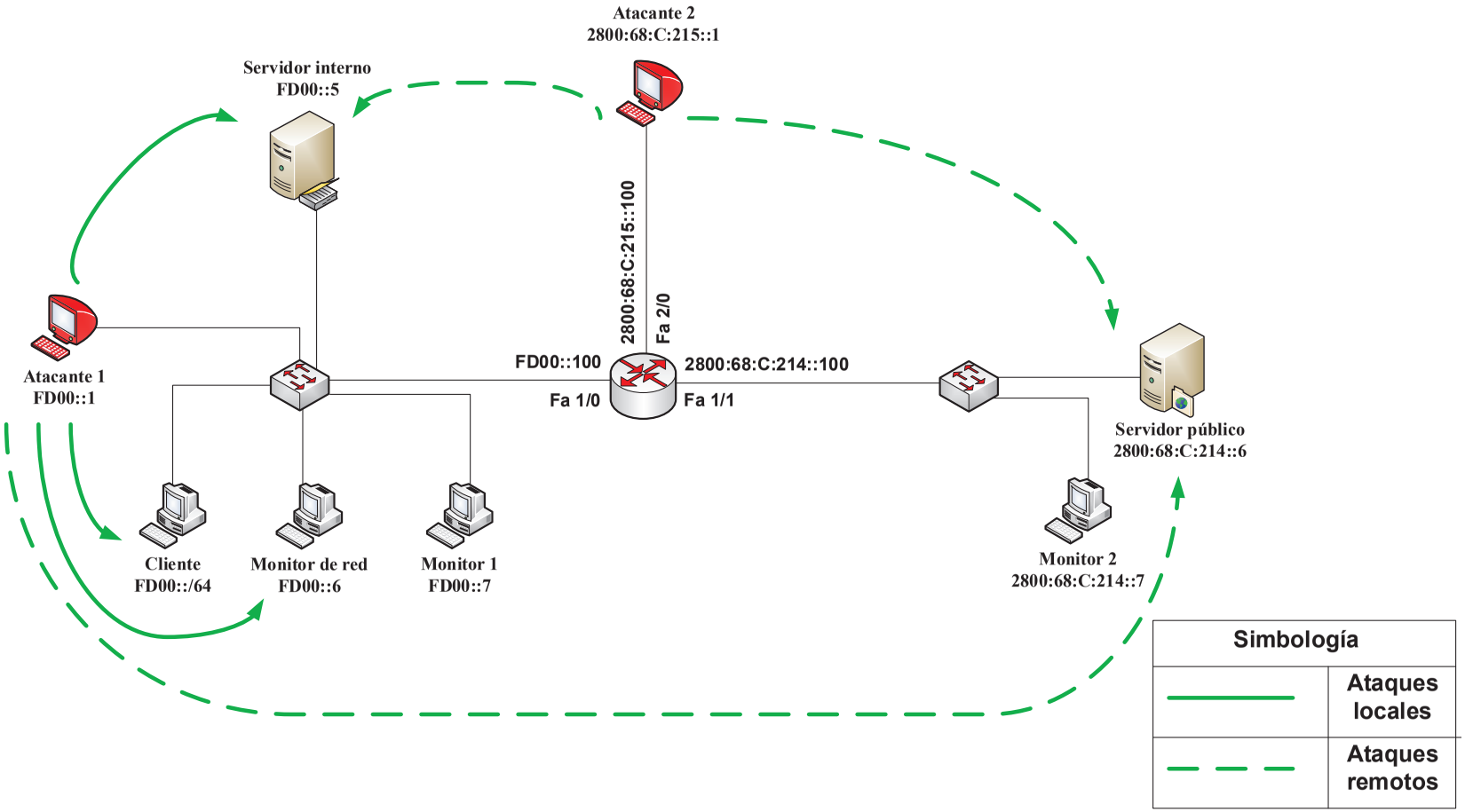

Figura 2.4 Diagrama final de la red propuesta.[37]

[37] Fuente: Autor del proyecto de titulación.

CAPÍTULO 3: PRUEBAS Y ANÁLISIS DE RESULTADOS

El proceso seguido para el proyecto de titulación continúa con la experimentación de las pruebas y análisis de resultados. La actividad para este capítulo sigue las fases de la figura 3.1. Es decir, realizaremos siete tests de penetración a través del diagrama final de la red propuesta de la sección 2.4. Una vez ejecutados los ataques en esta red, realizaremos un análisis de resultados de cada prueba para observar cómo se llevó a cabo la técnica de IP Spoofing.

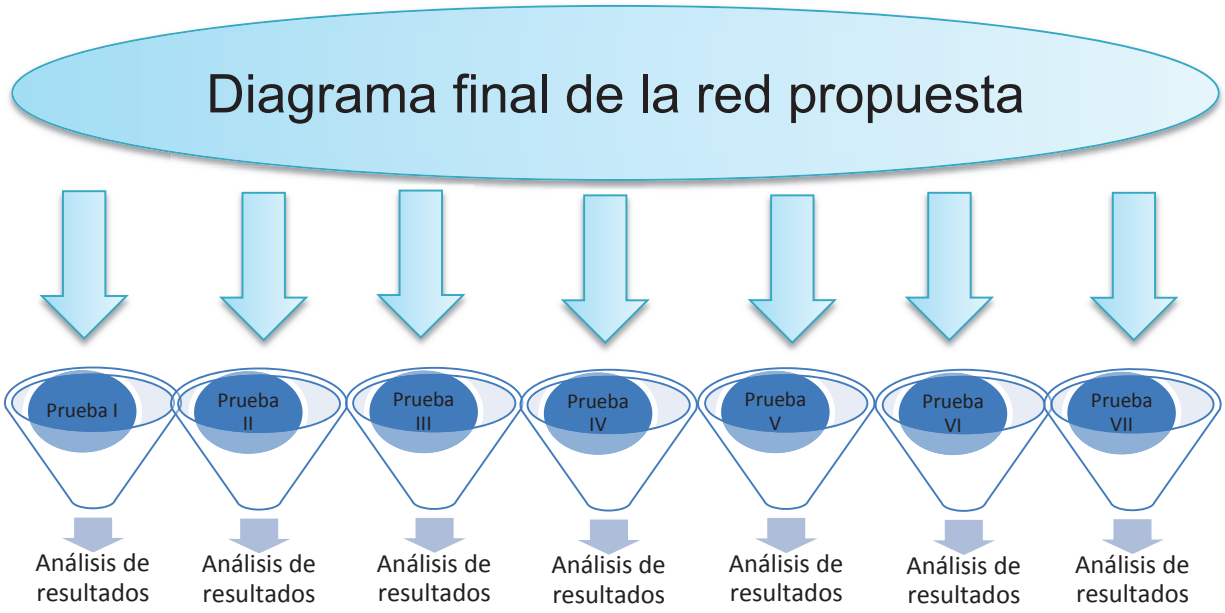

Figura 3.1 Fases del desarrollo del capítulo tres.[38]

La metodología planteada e implementada para cada una de las pruebas de la figura 3.1 toma como referencia la metodología de los tests de penetración. Sin embargo, no consideramos necesario utilizar las fases de reconocimiento y escaneo, ya que la información está definida y es bien conocida. En este sentido, utilizaremos únicamente la fase de penetración en cada una de las pruebas de la figura 3.1. En cada una de las pruebas realizaremos lo siguiente: ejecutar el ataque, procesar los resultados obtenidos (realizamos una comparación entre los valores iniciales y los

[38] Fuente: Autor del proyecto de titulación.

valores durante el ataque, mostramos las alertas del monitor, y detallamos las direcciones IPv6 suplantadas), y como punto final realizamos un análisis de resultados.

Las pruebas I – IV son realizadas para experimentar los ataques locales de la sección 1.1.1. Mientras que las pruebas V – VII son realizadas para experimentar los ataques remotos de la sección 1.1.2. A través de las pruebas observaremos los lugares de la red propuesta que son atacados con la técnica de IP Spoofing. Esto nos servirá para definir un plan de mitigación en el siguiente capítulo del proyecto.

3.1 PRUEBA I

En esta prueba I ejecutamos el ataque de la sección 1.1.1.1. Utilizamos la herramienta dos-new-ip6 en la máquina atacante 1 para realizar el ataque DoS con mensajes anuncio de vecino (véase la figura 3.2). El objetivo de esta prueba es observar que sucede con la asignación de direcciones IPv6 del cliente, del monitor de red, y del servidor interno. Esto lo realizamos cuando las máquinas están encendidas durante toda la ejecución del ataque, y cuando las reiniciamos manualmente durante la ejecución del ataque.

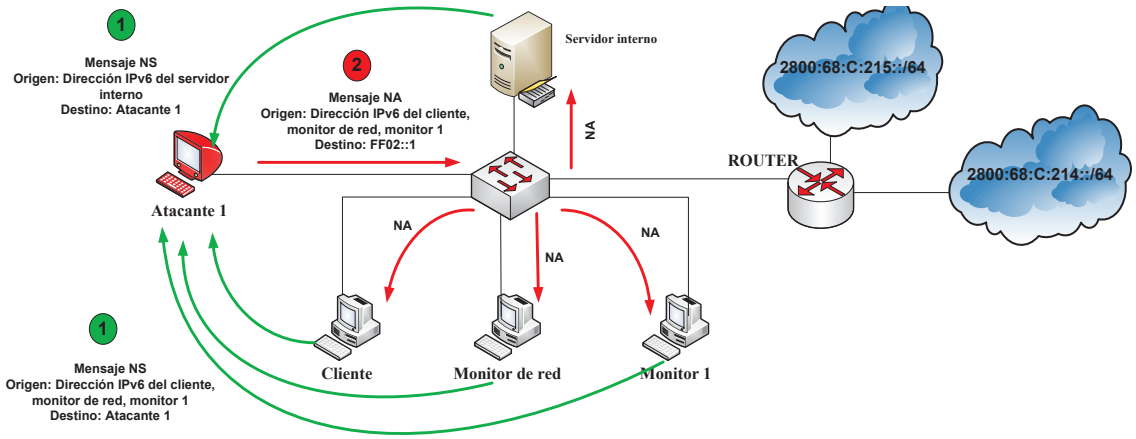

Figura 3.2 Diagrama de la prueba I.[39]

[39] Fuente: Autor del proyecto de titulación.

3.1.2 ANÁLISIS DE RESULTADOS

- Observamos que el ataque ejecutado en la prueba I denegó el servicio de las máquinas cliente, monitor de red, y servidor interno. En la comparación de resultados del anexo 2 observamos que el ataque fue exitoso sólo cuando las máquinas las reiniciamos manualmente. Este aspecto es crítico para las ventanas de mantenimiento[40] de los servidores, ya que por lo general en estas ventanas se reinician los sistemas operativos de los servidores.

- Observamos en el anexo 4 que el ataque realizó IP Spoofing de las direcciones IPv6 ULA y de enlace local de las máquinas cliente, monitor de red, y servidor interno, justo en el instante que dichas máquinas volvieron a arrancar su sistema operativo. Estas direcciones no pueden ser denegadas en el router de la figura 3.2 porque son direcciones válidas. En este caso deberemos utilizar criptografía para garantizar la autenticación del origen de los paquetes IPv6 que generan las máquinas cliente, monitor de red, y servidor interno.

- Observamos en el anexo 3 que el monitor 1 detectó el ataque ejecutado en la prueba I. El monitor 1 informó a través de la alerta dad dos que existe varias máquinas con direcciones IPv6 duplicadas. Sin embargo, la alerta del monitor 1 no llegó a informar cuales son las máquinas que están utilizando las direcciones IPv6 duplicadas.

- Observamos que el ataque ejecutado en la prueba I utiliza MAC Spoofing. Los mensajes NA falsificados por el atacante 1 utilizan direcciones MAC falsificadas (véase la figura 3.3). Esta técnica permite que el atacante 1 oculte su dirección física para que no sea rastreado. Además, MAC Spoofing fue

[40] Las ventanas de mantenimiento son operaciones de mantenimiento que se realizan durante períodos de inactividad.

utilizado por el atacante 1 para que cada uno de los mensajes NA falsificados tengan una dirección MAC diferente.

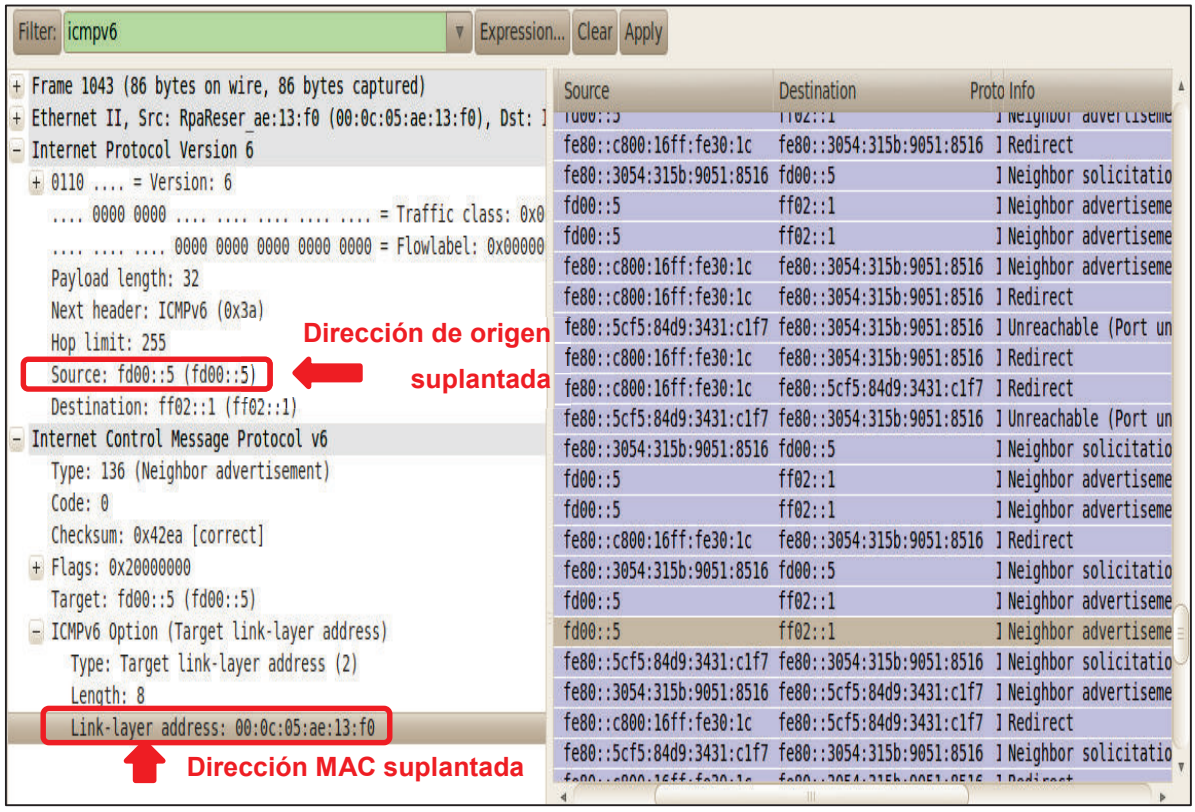

Figura 3.3 Mensaje NA falsificado.[41]

3.2 PRUEBA II

En esta prueba II ejecutamos el ataque de la sección 1.1.1.2. Utilizamos la herramienta parasite6 en la máquina atacante 1 para realizar el ataque MITM con mensajes anuncio de vecino sobre el cliente y servidor interno (véase la figuras 3.4 y 3.5). El objetivo de la prueba II es observar una comunicación atacada con la técnica de IP Spoofing entre cliente – servidor interno. Lo que realizaremos es observar la dirección IPv6 origen de los mensajes de capa aplicación que intercambia el cliente y el servidor interno.

[41] Fuente: Autor del proyecto de titulación.

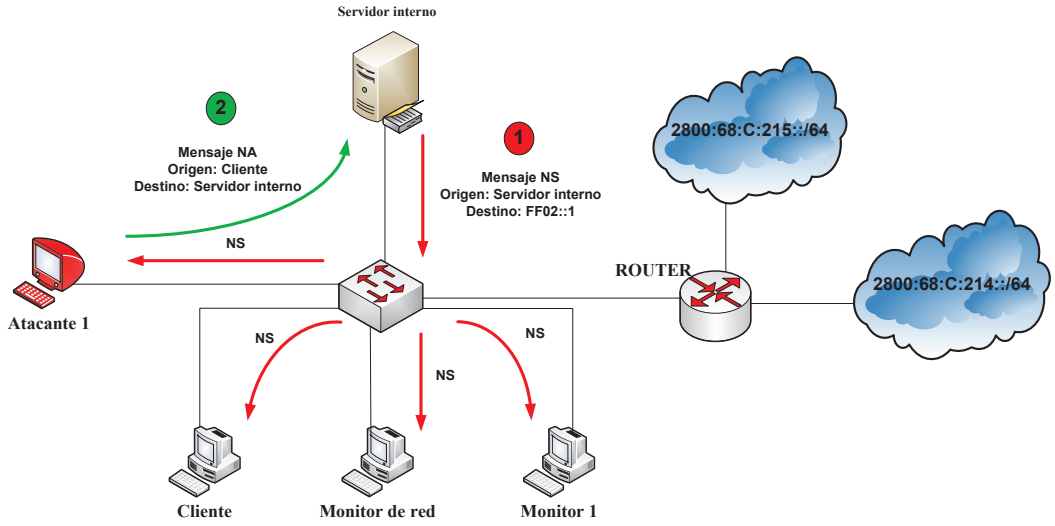

Figura 3.4 Diagrama de la prueba II sobre el servidor interno.[42]

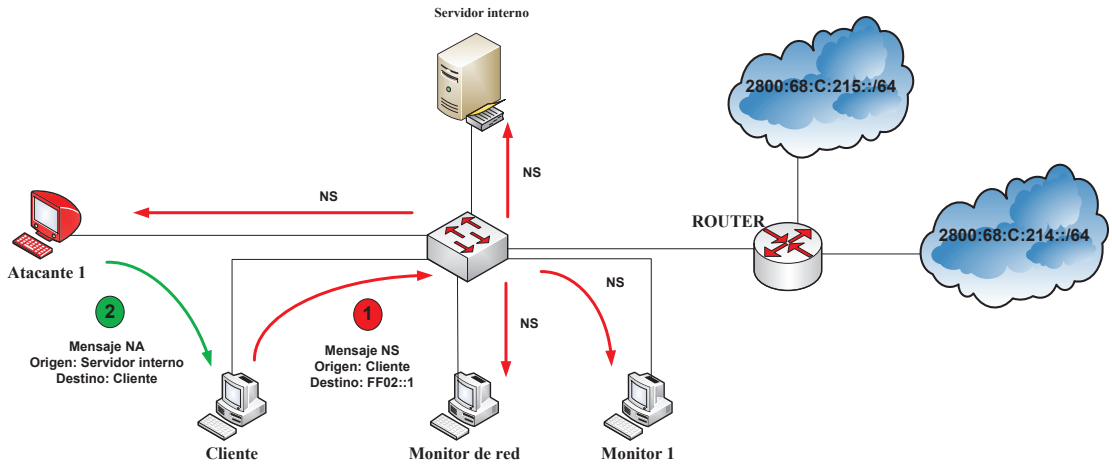

Figura 3.5 Diagrama de la prueba II sobre el cliente.[43]

Las figuras 3.4 y 3.5 detallan los diagramas de la prueba II. La primera figura muestra como realizamos el ataque sobre el servidor interno. Mientras que la segunda figura muestra como realizamos el ataque sobre el cliente. Tanto el ataque sobre el servidor interno y el cliente son realizados al mismo tiempo a través de la herramienta parasite6, sin embargo, para comprender mejor separamos el ataque de la prueba II en dos diagramas.

[42] Fuente: Autor del proyecto de titulación.
[43] Fuente: Autor del proyecto de titulación.

3.2.2 ANÁLISIS DE RESULTADOS

- Observamos en la prueba II que el tráfico HTTP entre el cliente y el servidor interno es interceptado y reenviado por el atacante 1. Tras la ejecución del ataque, la información de la tabla de vecinos del cliente se modificó porque el ataque almacenó un registro falso. El cliente relacionó la dirección MAC de la máquina atacante 1 con la dirección IPv6 del servidor interno y de la puerta de enlace (véase la figura 3.6). Al otro lado de la comunicación el servidor interno experimentó el mismo efecto, relacionó la dirección MAC de la máquina atacante 1 con la dirección IPv6 del cliente (véase la figura 3.7).

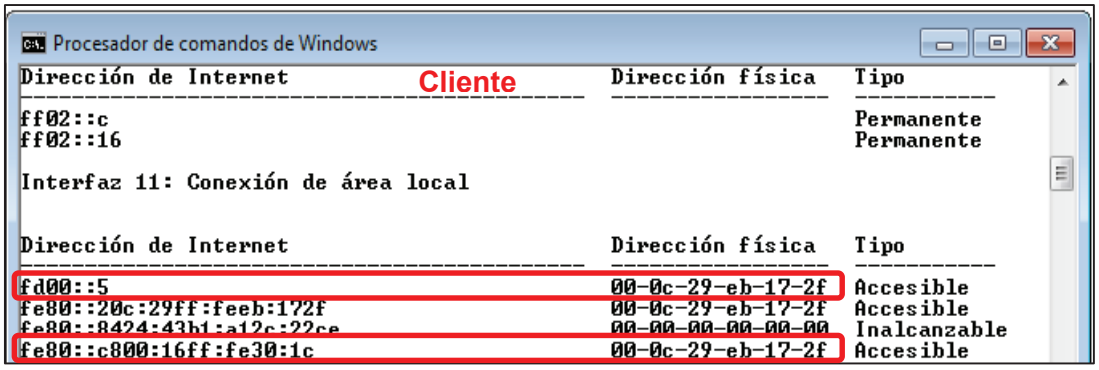

Figura 3.6 Envenenamiento de la tabla de vecinos en el cliente. [44]

- Observamos en la prueba II que al atacante 1 lo podemos rastrear a través de la tabla de vecinos de las máquinas cliente y servidor interno. El rastreo lo podemos realizar porque el registro de la dirección MAC – dirección IPv6 del atacante 1 se guardó tanto en el cliente como en el servidor interno (véase la figura 3.6). El registro guardó la dirección IPv6 fe80::20c:29ff:feeb:172f y la MAC 00-0c-29-eb-17-2f que pertenece al atacante 1.

[44] Fuente: Autor del proyecto de titulación.

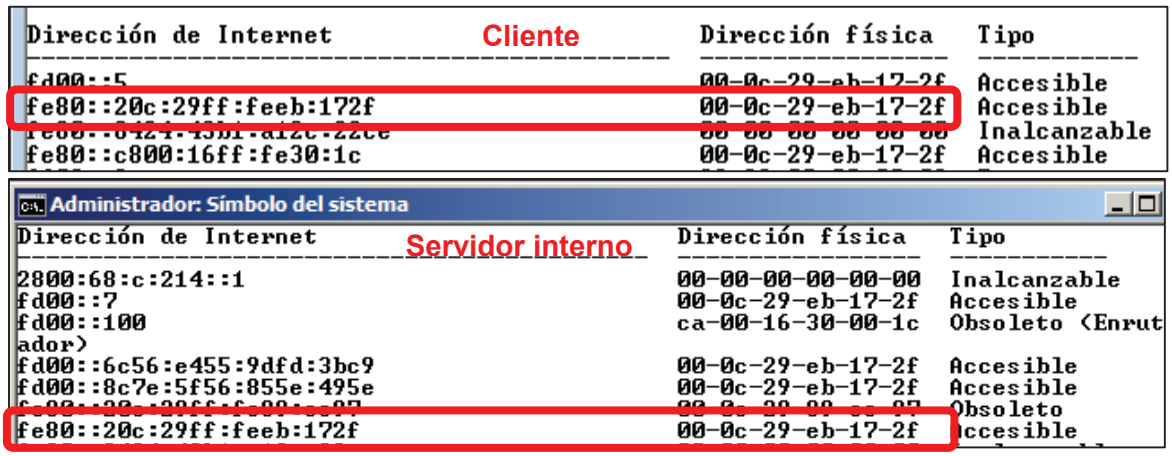

Figura 3.7 Tabla de vecinos del cliente y servidor interno. [45]

- Observamos en la prueba II que el atacante 1 también puede ser rastreado a través de las alertas del monitor 1. Basta con revisar las alertas del monitor 1 encontradas en el anexo 3, y fijarse en la alarma wrong router redirect. El rastreo puede llevarse a cabo porque el atacante 1 no utiliza la técnica de MAC Spoofing, ya que en la ejecución del ataque necesita que los mensajes HTTP sean reenviados a través de su propia dirección MAC.

- Observamos en la prueba II que el atacante 1 reenvía la petición HTTP del cliente al servidor interno, a través suyo. En la figura 3.8 observamos que la petición HTTP del cliente al servidor interno primero es enviada a la máquina atacante 1. En la figura 3.9 observamos que la petición HTTP luego es reenviada al servidor interno utilizando IP Spoofing para simular que la petición HTTP es enviada por el cliente. Estas dos peticiones tienen las mismas direcciones IPv6 de origen y destino. Esta es la razón por la cual Wireshark identifica estas dos peticiones repetidas como TCP Out-Of-Order en la figura 3.8 y 3.9.

[45] Fuente: Autor del proyecto de titulación.

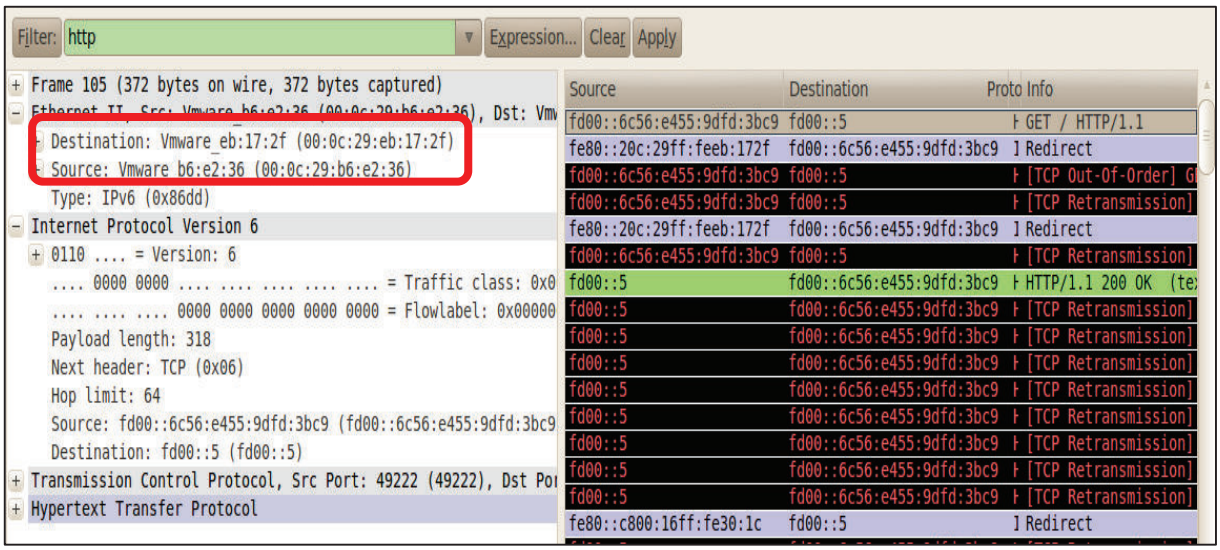

Figura 3.8 Petición HTTP desde el cliente al atacante.[46]

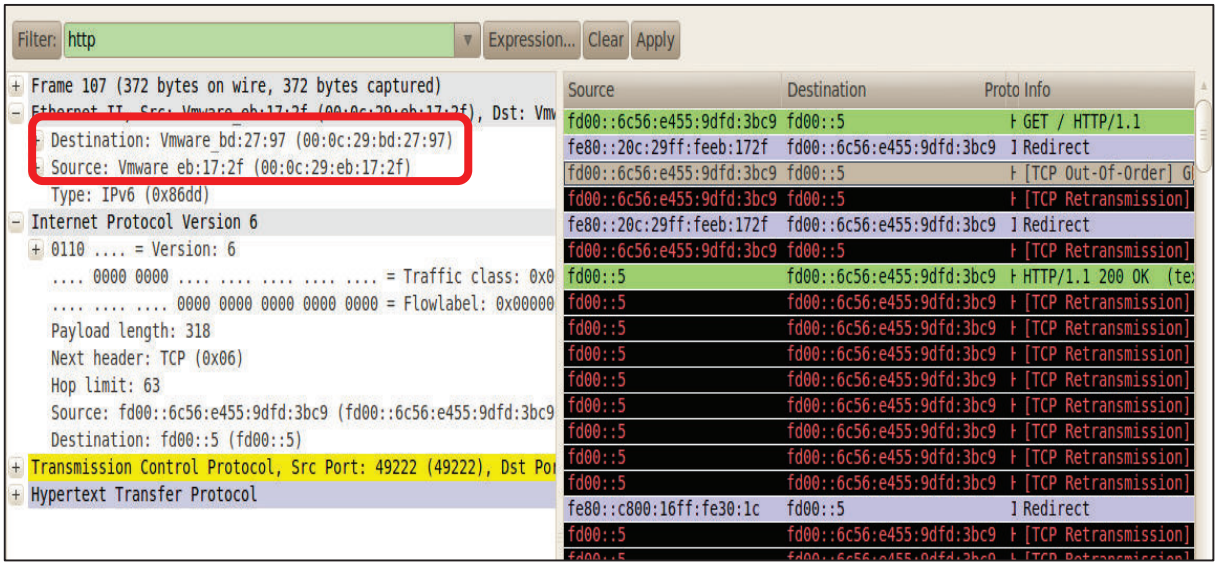

Figura 3.9 Petición HTTP desde el atacante al servidor interno.[47]

3.3 PRUEBA III

En esta prueba III ejecutamos el ataque de la sección 1.1.1.3. Utilizamos la herramienta flood_router6 en la máquina atacante 1 para realizar el ataque DoS con

[46] Fuente: Autor del proyecto de titulación.
[47] Fuente: Autor del proyecto de titulación.

mensajes anuncio de router (véase la figura 3.10). El objetivo de la prueba III es observar el uso de CPU y memoria en las máquinas cliente, monitor de red y servidor interno, cuando el ataque está siendo ejecutado.

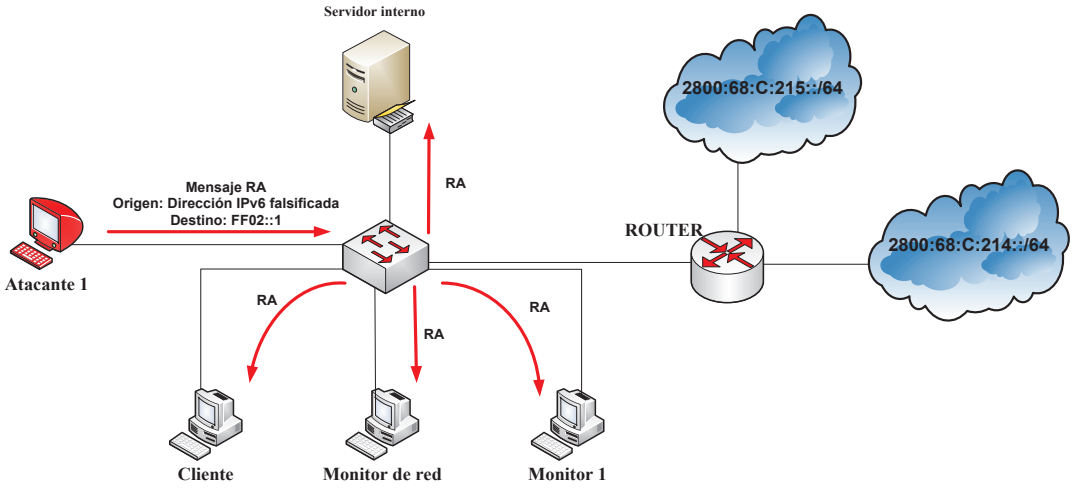

Figura 3.10 Diagrama de la prueba III.[48]

3.3.2 ANÁLISIS DE RESULTADOS

- Observamos en el anexo 3 que el monitor 1 detectó el ataque ejecutado en la prueba III. El monitor 1 informó a través de la alerta wrong ipv6 router, que existe una máquina anunciando prefijos de red falsificados a través de mensajes RA. Sin embargo, la alerta del monitor 1 no llegó a informar cual es la máquina emisora de dichos mensajes RAs falsificados.

- Observamos en la prueba III que la máquina cliente aceptó los mensajes RAs falsificados. Los mensajes RAs falsificados afectaron el rendimiento de la máquina cliente porque provocaron que el uso de CPU llegue hasta el 100% de uso, inclusive provocaron que el sistema de esta máquina se colgara. Este efecto sobre el cliente sucedió de tal manera porque los mensajes RAs

[48] Fuente: Autor del proyecto de titulación.

falsificados tuvieron que ser procesados tan rápido como fueron enviados por el atacante 1.

- Observamos en la prueba III que la máquina servidor interno no aceptó los mensajes RAs falsificados. Esto sucedió porque dentro de la configuración del servidor interno, eliminamos la autoconfiguración stateless a través de la sentencia netsh interface ipv6 set interface 11 routerdiscovery=disabled. De esta manera, la máquina servidor interno no intentó autoconfigurar automáticamente su interfaz de red a través de los mensajes RAs.

- Observamos en la figura 3.11 que cada mensaje RA enviado por el atacante 1 utiliza también la técnica de MAC Spoofing. Esta técnica permite que el atacante 1 no sea rastreado. Además, observamos en la misma figura, que la dirección de origen es una dirección IPv6 de enlace local suplantada, utilizada para que la máquina cliente la configure como la dirección del router de su subred.

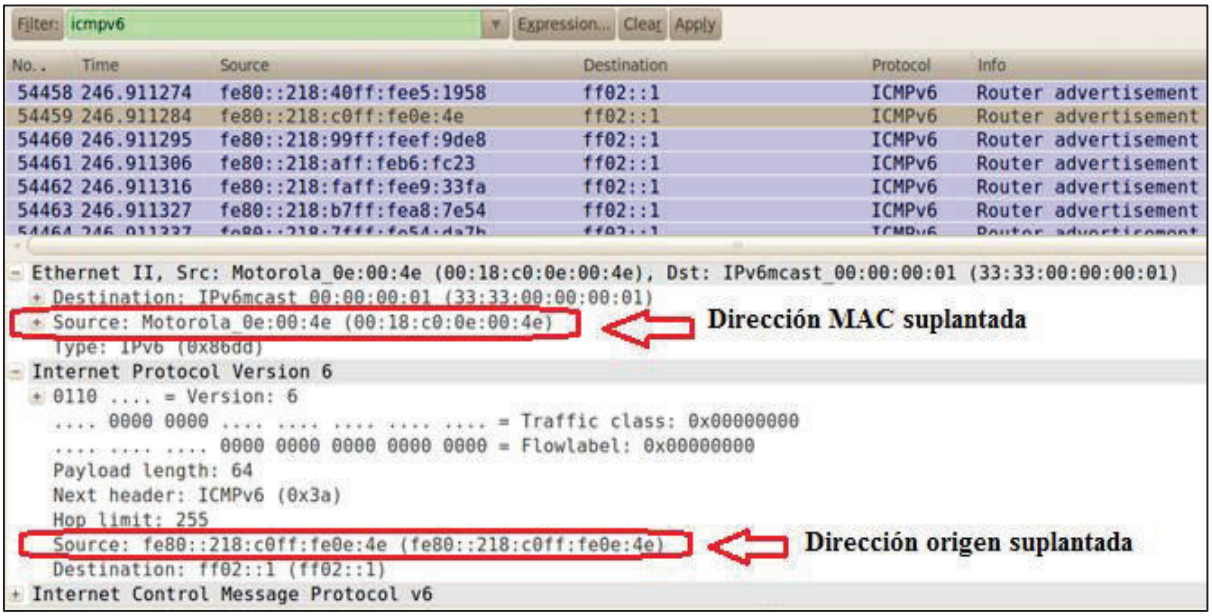

Figura 3.11 Captura del mensaje RA suplantado.[49]

[49] Fuente: Autor del proyecto de titulación.

3.4 PRUEBA IV

En esta prueba IV ejecutamos el ataque de la sección 1.1.1.4. Utilizamos la herramienta smurf6 en la máquina atacante 1 para realizar el ataque Smurf local. El objetivo de la prueba IV es observar el ancho de banda y uso de la CPU de las máquinas cliente, monitor de red y servidor interno, durante la ejecución del ataque. El monitor 1 no detectó el ataque de la sección 1.1.1.4 porque los mensajes que intercambia el atacante 1 no son analizados por dicho monitor 1. Por esta razón, en el anexo 3 no contamos con la sección alertas del monitor para la prueba IV.

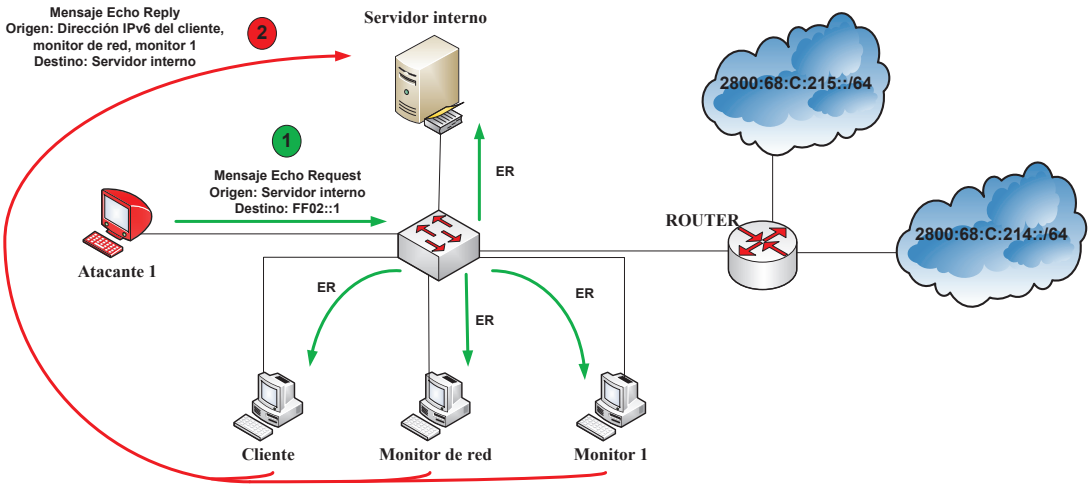

Figura 3.12 Diagrama de la prueba IV.[50]

3.4.2 ANÁLISIS DE RESULTADOS

- Observamos en el anexo 2 que el incremento del uso de la red fue muy pequeño. El uso de la red del cliente, monitor de red y servidor interno no afectó el trabajo de dichas máquinas. En el anexo 2 observamos que antes del ataque el uso de la red en el cliente, monitor de red y servidor interno fue 0%. Mientras que durante el ataque el uso de la red se incrementó en 4,02% para

[50] Fuente: Autor del proyecto de titulación.

la máquina cliente, 5,19 para el monitor de red y 7,94% para la máquina servidor interno.

- Observamos en los resultados del anexo 2 que el uso de CPU se incrementó. En el cliente, monitor de red y servidor interno, obtuvimos 81%, 80% y 97% de uso de CPU. Sin embargo, dichas máquinas no sufrieron denegación de servicio. Los servicios brindados por el servidor interno y el monitor de red no resultaron afectados. Esto sucedió de tal manera porque las máquinas reclutadas fueron muy pocas y no lograron denegar el servicio.

- Observamos en la figura 3.13 que la máquina cliente y monitor de red no fueron reclutados en el ataque de la prueba IV. El sistema operativo del cliente y monitor de red no respondieron los mensajes Echo Request suplantados por el atacante 1. La máquina que respondió dichos mensajes fue el monitor 1, y también la interfaz del router fa 1/0. Sin embargo, las respuestas Echo Reply de estos dispositivos no lograron denegar el servicio del servidor interno.

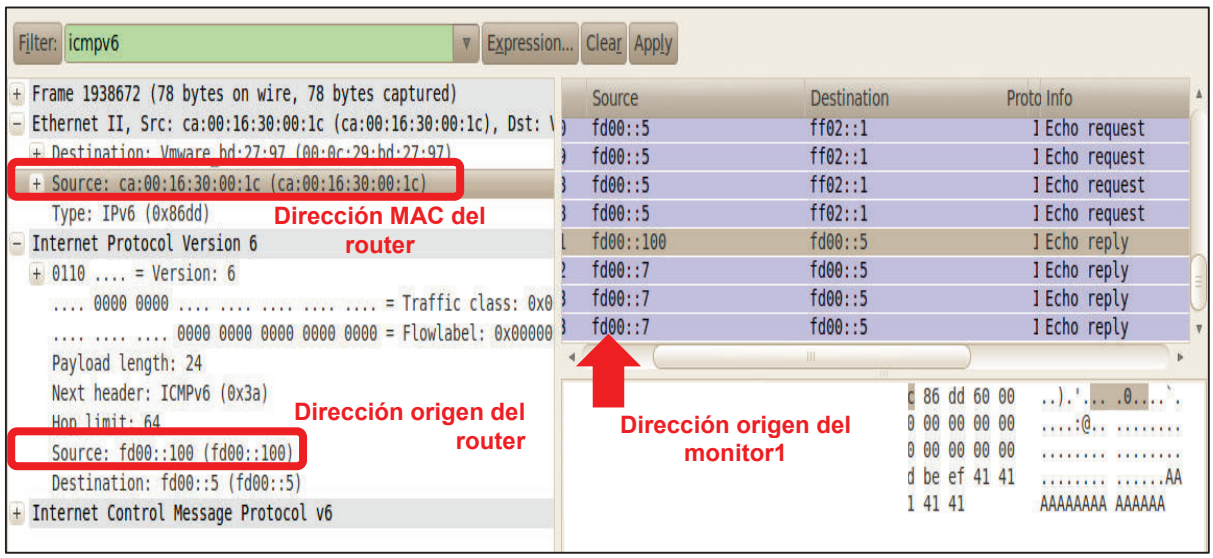

Figura 3.13 Captura del mensaje Echo Reply del router.[51]

[51] Fuente: Autor del proyecto de titulación.

3.5 PRUEBA V

La prueba V es la primera de las pruebas con la cual experimentamos los ataques remotos de la sección 1.1.2.1. Utilizamos la herramienta toobig6 en las máquinas atacante 1 y atacante 2 para realizar el ataque DoS con mensajes ICMPv6 Paquete demasiado grande sobre el servidor interno y público (véase la figura 3.14). El objetivo de la prueba V es observar el MTU establecido entre el cliente – servidor interno, y entre el cliente – servidor público. Experimentamos con varios valores de MTU y de esta manera observamos el nuevo valor de MTU en el cliente y cada uno de los servidores.

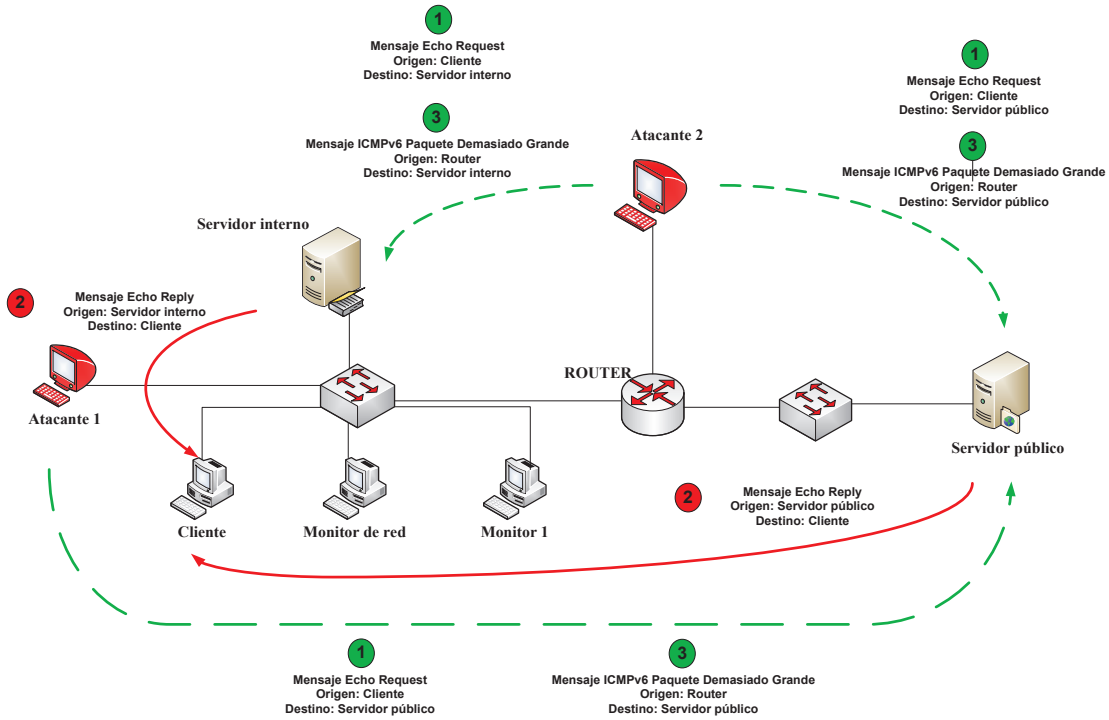

Figura 3.14 Diagrama de la prueba V. [52]

Las direcciones IPv6 de origen con las que experimentamos son:

- Dirección del Cliente.

[52] Fuente: Autor del proyecto de titulación.

- Direcciones obsoletas.
- Direcciones reservadas por la IETF.
- Dirección multicast.
- Direcciones de propósito especial.

3.5.2 ANÁLISIS DE RESULTADOS

- Observamos en la prueba V que la vida del ataque dura hasta que el servidor público o interno recibe en su interfaz de red un mensaje IPv6 RA que le informa el verdadero valor de la MTU del enlace. Hasta que este evento ocurra, observamos que el servidor público o interno añaden una cabecera de fragmentación de 8 bytes (véase la figura 3.15 y 3.16) a los paquetes IPv6 y sus datos (ICMPv6, TCP, FTP, HTTP). Observamos que las capas superiores a la capa de red del modelo ISO/OSI son vulnerables a este tipo de ataque ya que sus mensajes viajan a través de un protocolo en común que es IPv6.

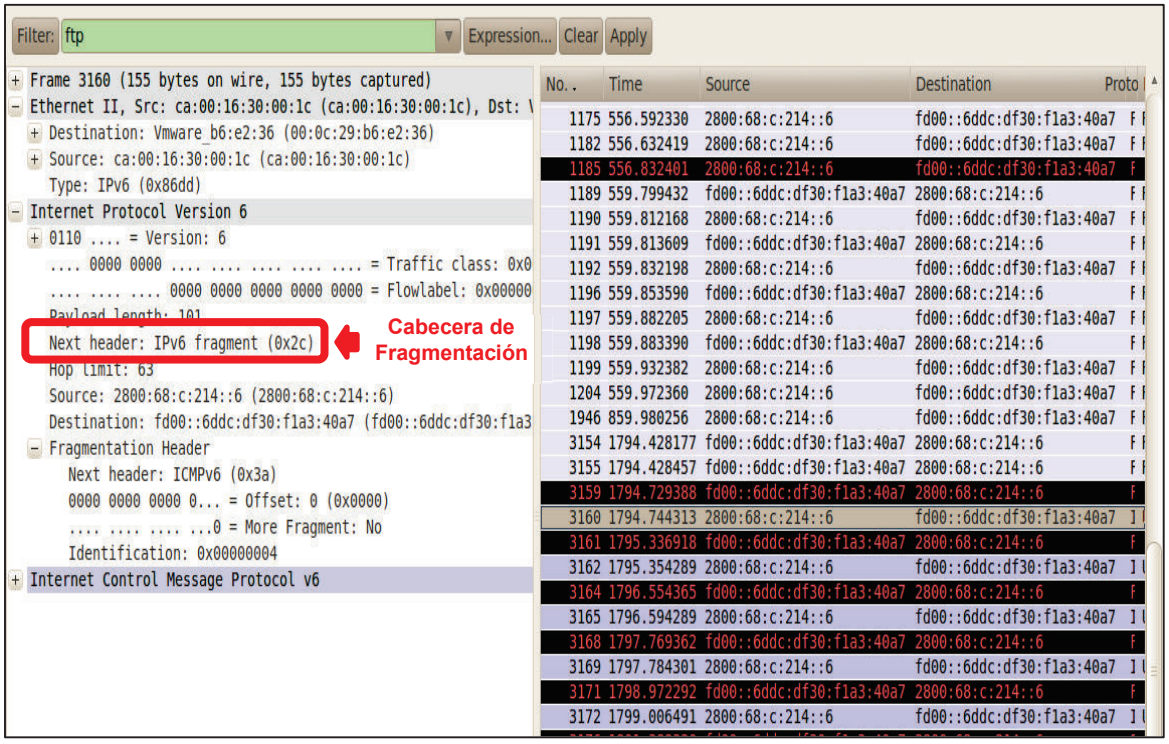

Figura 3.15 Captura de un paquete FTP fragmentado.

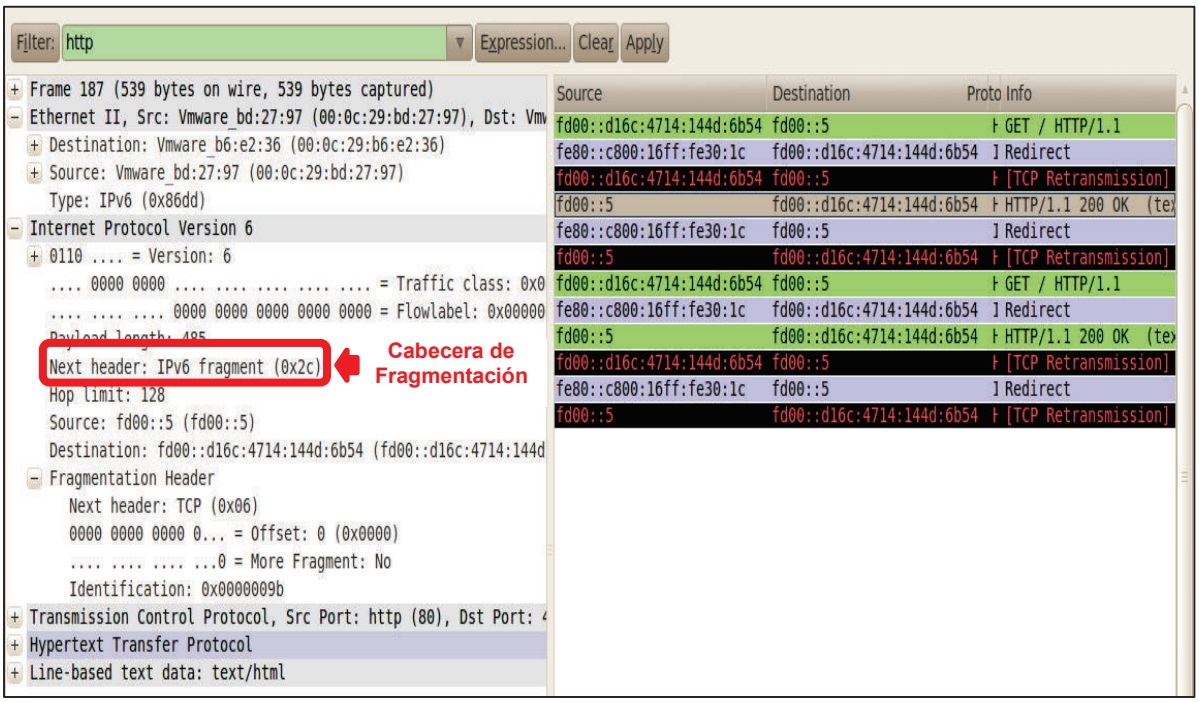

Figura 3.16 Captura de un paquete HTTP fragmentado.

- Observamos en la prueba V que el router de la figura 3.14 permitió el reenvío de las direcciones IPv6 utilizadas con la técnica de IP Spoofing. Estas direcciones de origen deberían ser denegadas en el router porque no son direcciones de origen válidas. El router de la figura 3.14 debería ser capaz de implementar algún tipo de filtrado para denegar estas direcciones IPv6 de origen detalladas en el anexo 4.

3.6 PRUEBA VI

En esta prueba VI ejecutamos el ataque de la sección 1.1.2.2. Utilizamos la herramienta redir6 en la máquina atacante 1 para realizar el ataque MITM con mensajes redireccionamiento. El objetivo de la prueba VI es observar el redireccionamiento del tráfico entre el cliente – servidor interno, y entre el cliente – servidor público. Observamos el tráfico FTP intercambiado entre el cliente y el servidor interno.

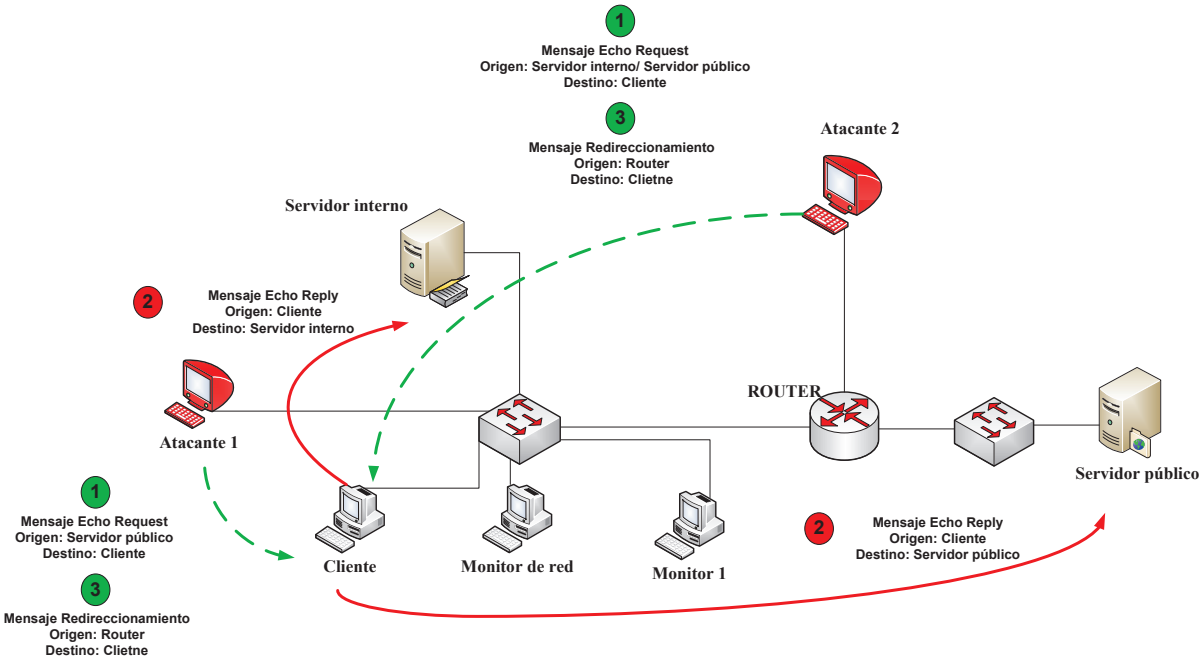

Figura 3.17 Diagrama de la prueba VI. [53]

3.6.2 ANÁLISIS DE RESULTADOS

- Observamos en las alertas del monitor 1 del anexo 3 que el atacante 1 puede ser rastreado a través de su dirección MAC. Esto lo podemos llevar a cabo porque el atacante 1 tuvo la necesidad de introducir su dirección MAC para que todos los mensajes enviados entre cliente – servidor público pasen a través suyo.

- Observamos en la prueba VI que el atacante 1 afectó las rutas guardadas en la tabla de destinos de la máquina cliente. El mejor próximo salto introducido fue la dirección IPv6 de enlace local fe80::20c:29ff:feeb:172f. Este salto obligó al cliente primero dirigir sus paquetes IPv6 a través de la máquina atacante 1. Sucedió porque el cliente confió que el mensaje redireccionamiento fue enviado por el router oficial de la red propuesta.

[53] Fuente: Autor del proyecto de titulación.

- Observamos en la prueba VI que el atacante 1 reenvía los mensajes FTP a través suyo. En la figura 3.18 observamos que el cliente envía un mensaje FTP a la dirección IPv6 del servidor público. Sin embargo, el paquete no es enviado al servidor público, ya que la dirección MAC del mensaje FTP corresponde a la dirección del atacante 1. En la figura 3.19 observamos que el atacante 1 reenvía el mensaje FTP al servidor público haciéndose pasar por el cliente.

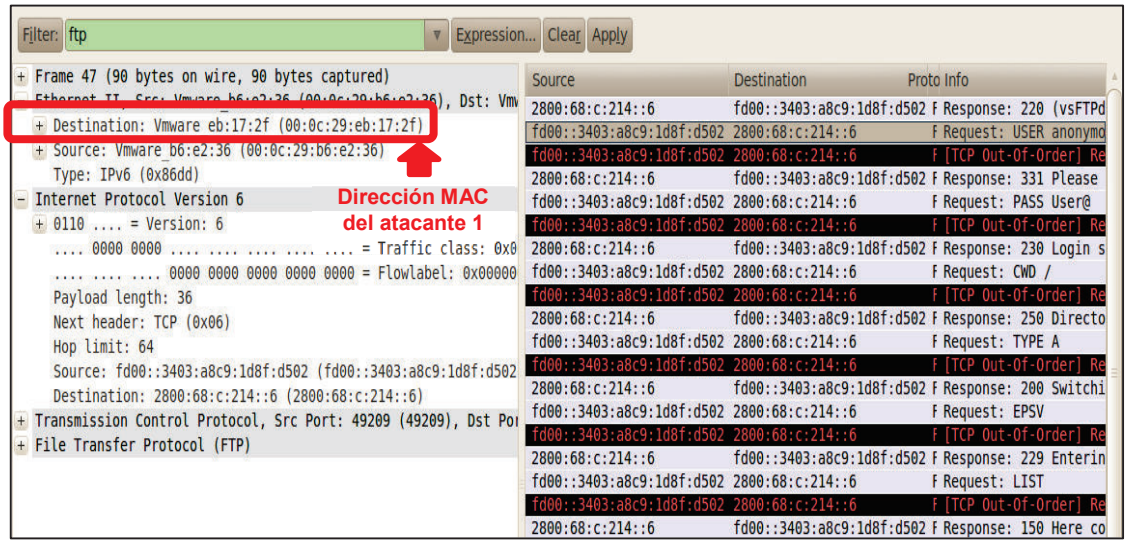

Figura 3.18 Mensaje FTP enviado desde el cliente al atacante 1.

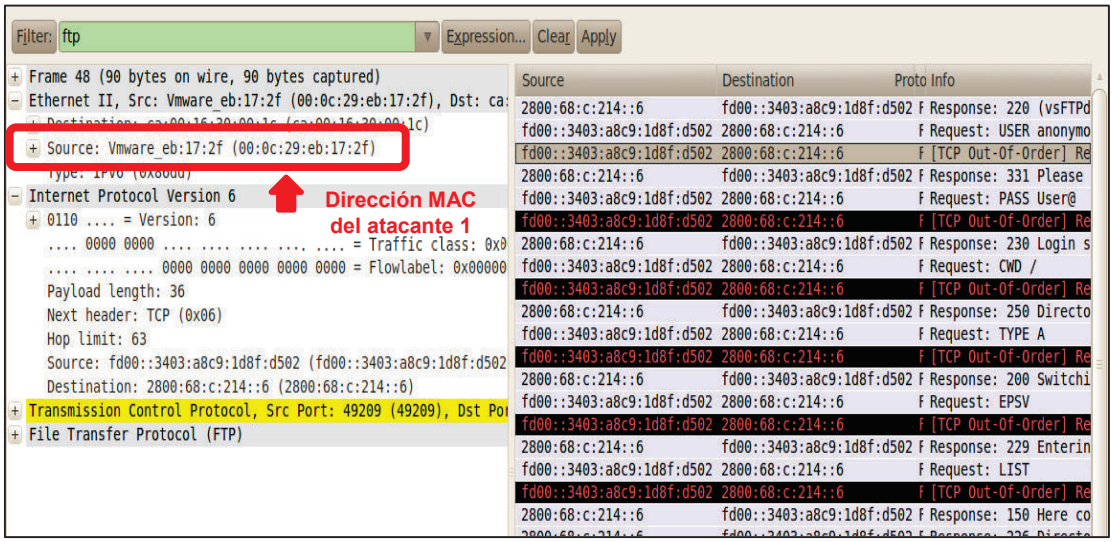

Figura 3.19 Mensaje FTP enviado desde el atacante 1 al servidor público.

- Observamos que las pruebas ejecutadas desde el atacante 2 no dieron resultados. Esto sucedió porque el mensaje redireccionamiento no llegó al cliente. El mensaje redireccionamiento fue denegado por el router c7200. La dirección que utilizó el mensaje de redireccionamiento es una dirección de origen inválida. Por esta razón, el router c7200 no reenvió el mensaje redireccionamiento al cliente.

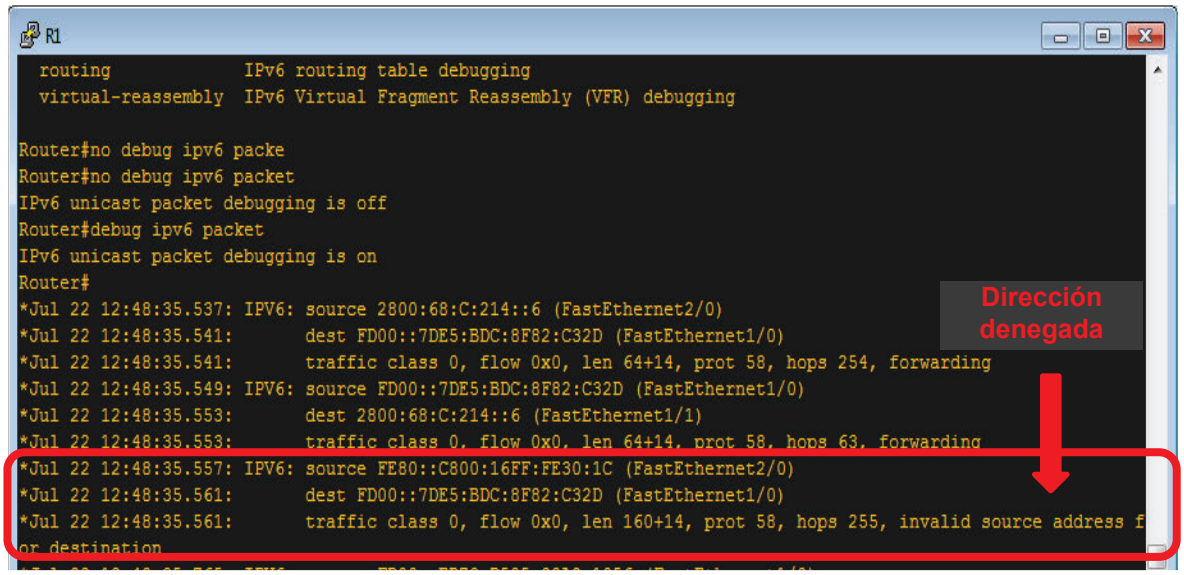

Figura 3.20 Mensaje redireccionamiento denegado por el router c7200.

3.7 PRUEBA VII

En esta prueba VII ejecutamos el ataque de la sección 1.1.2.3. Utilizamos la herramienta rsmurf6 en las máquinas atacante 1 y atacante 2 para realizar el ataque Smurf remoto (véase la figura 3.21). El objetivo es provocar que el servidor interno y público inunden la red con respuestas de los mensajes Echo Request falsificados. Sin embargo, el resultado de esta prueba VII no fue exitosa porque hubo un obstáculo que no permitió completar el ataque, el cual lo detallamos en la sección de análisis de resultados.

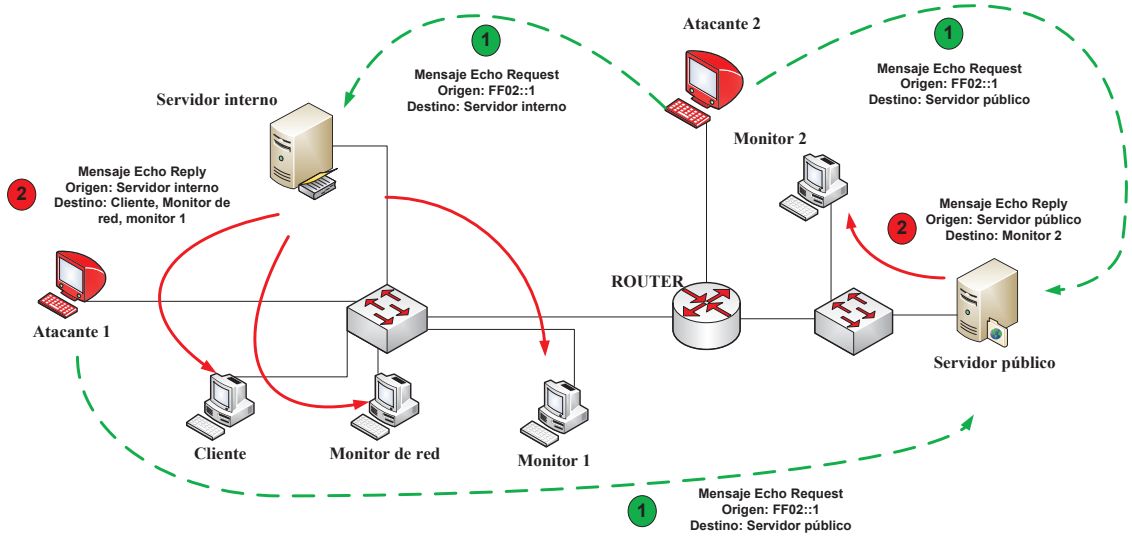

Figura 3.21 Diagrama de la prueba VII. [54]

3.7.2 ANÁLISIS DE RESULTADOS

- En la figura 3.21 observamos que el router c7200 denegó el ataque Smurf remoto. El router revisó los mensajes Echo Request enviados por los atacantes y denegó todos los mensajes Echo Request que contenían la dirección origen multicast FF02::1. Estos mensajes fueron denegados porque utilizaron una dirección IPv6 de origen inválida.

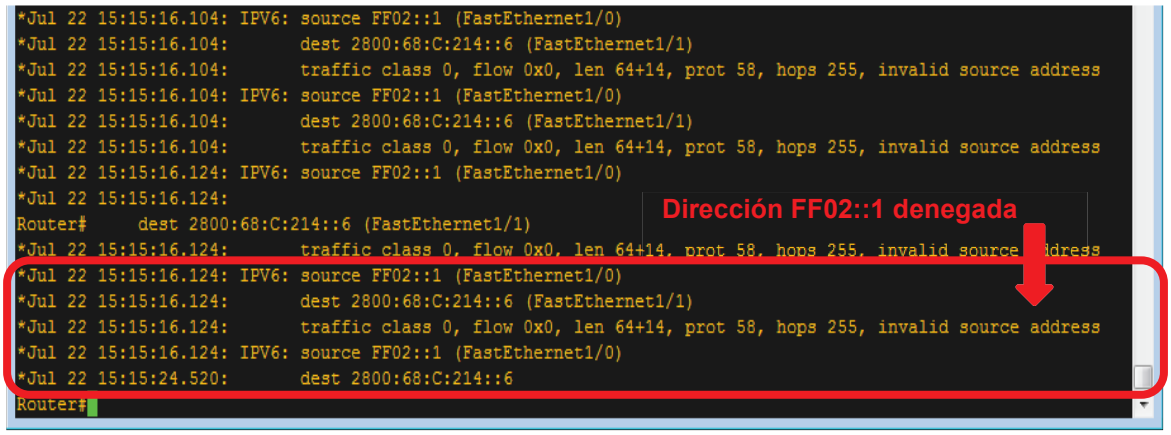

Figura 3.22 Mensajes Echo Request denegados por el router c7200.

[54] Fuente: Autor del proyecto de titulación.

CAPÍTULO 4: PLAN DE MITIGACIÓN

El objetivo de este capítulo es reducir el riesgo que generaron las pruebas realizadas en el capítulo tres. Para cumplir con este objetivo desarrollamos un plan de mitigación, el cual sigue las fases de desarrollo de la figura 4.1. Es decir, para desarrollar el plan de mitigación utilizaremos tres fases: Entrada, proceso y salida. La fase de entrada provee el análisis de resultados de cada prueba del capítulo 3 y es utilizada en la fase de proceso para realizar el diseño de la red física y su correspondiente sistema de seguridad. Como fase de salida, presentamos el diagrama final de la red física.

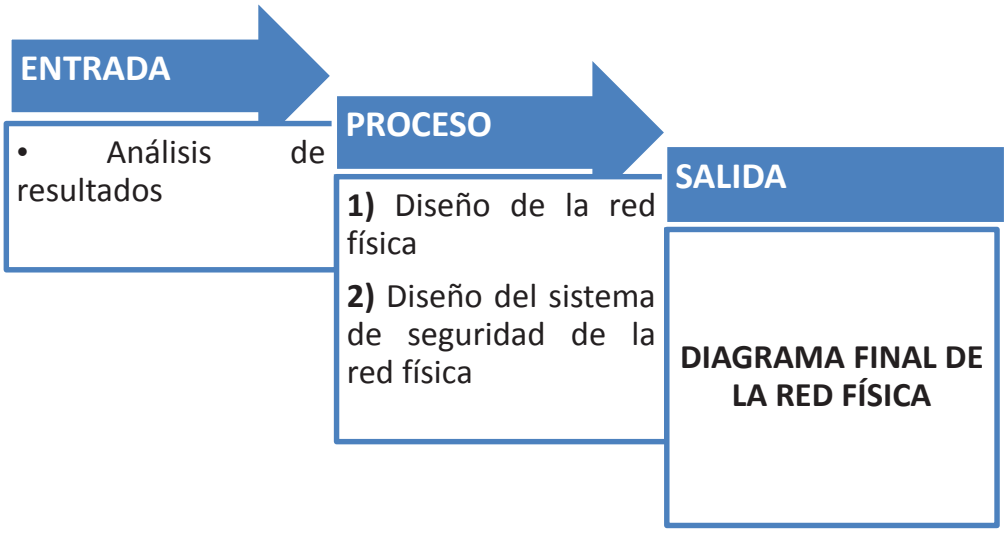

Figura 4.1 Fases del desarrollo del capítulo cuatro.[55]

El diseño de la red física lo realizaremos a través de la arquitectura SAFE de Cisco. Para lo cual, definiremos módulos de SAFE en base a las funciones de la red propuesta de la sección 2.1. El sistema de seguridad de la red física lo realizaremos a través del uso de criptografía, listas de control de acceso y una DMZ. La criptografía la empleamos para asegurar las comunicaciones IPv6 de la red interna.

[55] Fuente. Autor del proyecto de titulación.

Las listas de control de acceso y la DMZ la empleamos para denegar la técnica de IP Spoofing cuando el objetivo del atacante son los servidores públicos.

4.1 DISEÑO DE LA RED FÍSICA [W9]

Para el diseño de la red física utilizaremos la arquitectura modular de Cisco conocida como SAFE. SAFE nos brinda la posibilidad de realizar el diseño seguro de la red propuesta de la sección 2.1 a través de módulos funcionales. Observamos en el capítulo 3 que la mayor parte de las pruebas que ocasionaron un riesgo para la red fueron producidas cuando ejecutamos la técnica de IP Spoofing a través del atacante 1. Esto tuvo un efecto negativo porque muchas funciones de la red están ubicadas en un mismo segmento de red. Adicionalmente, observamos riesgos producidos por la presencia del atacante 2. Es por esta razón, que utilizamos el diseño de SAFE (véase la figura 4.2) para separar las funciones de cada máquina de la red propuesta. Tenemos los siguientes módulos de SAFE para disminuir los riesgos mencionados:

- Módulo de acceso: En este módulo ubicamos el cliente.

- Módulo de gestión: En este módulo ubicamos el monitor de red.

- Módulo de servidores: En este módulo ubicamos el servidor interno.

- Módulo de Internet corporativo: En este módulo ubicamos el servidor público.

- Módulo del Proveedor de servicios de Internet. En este módulo ubicamos el ISP. La seguridad de este módulo estará determinado a través de SLAs[56] y por los propios mecanismos de seguridad del ISP. Esta es la razón principal

[56] SLA: Acuerdo de nivel de servicio.

por la cual no consideramos el diseño del ISP dentro del desarrollo del plan de mitigación.

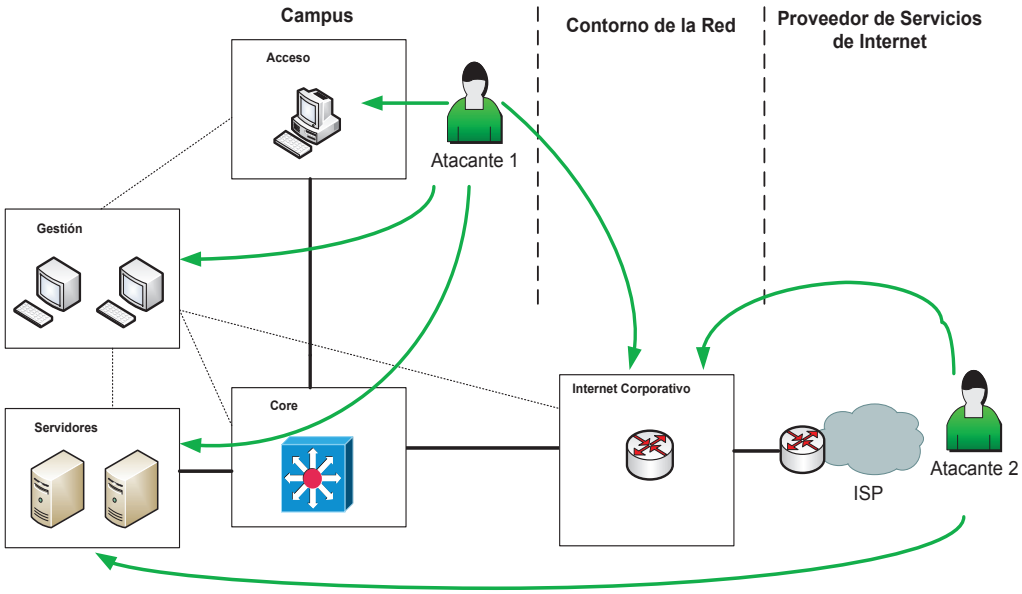

Figura 4.2 Módulos atacados.[57]

Con la nueva división realizada a las funciones de la red propuesta, surgen nuevos objetivos para el atacante 1 (véase la figura 4.2). El atacante 1 podrá remotamente poner en riesgo los módulos de gestión, servidores e Internet corporativo, al igual que lo hizo el atacante 2 en las pruebas del capítulo tres. Entonces, la solución en este caso será utilizar el análisis de resultados de las pruebas dónde el atacante 2 ejecutó los ataques remotos. Bajo esta consideración, en las líneas siguientes encontramos el diseño de los módulos de SAFE para la red física.

4.1.1 MÓDULO DE ACCESO

En este módulo ubicamos el cliente que representa los usuarios finales de la red. El prefijo de red para el módulo de acceso será tomado del rango de direcciones IPv6 del tipo ULA. La asignación de las direcciones IPv6 de los usuarios finales es realizada a través del método de autoconfiguración Stateless. Este método lo

[57] Fuente. Autor del proyecto de titulación.

implementará el módulo de core a través del anuncio del prefijo de red enviado en los mensajes RAs. El diseño del módulo lo presentamos en la figura 4.3.

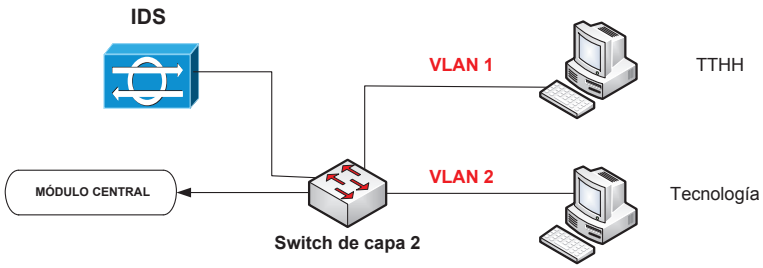

Figura 4.3 Módulo de acceso propuesto.[58]

Los usuarios finales serán creados según un perfil dentro de la red. Es decir, tendremos usuarios finales que pertenecerán a un área de trabajo de la organización. Esto servirá para definir VLANs[59] privadas según el perfil del usuario final. Configuraremos VLANs en el switch de capa 2 (véase la figura 4.3). Segmentaremos el prefijo de red del módulo de acceso para crear las VLANs. Las VLANs que implementaremos en este módulo son creadas y nombradas según los perfiles de los usuarios finales. Por ejemplo, podríamos crear una VLAN 1 para un grupo de usuarios finales que pertenecen al área de Talento Humano y una VLAN 2 para el área de Tecnología. Sin embargo, la creación de las VLANs estará a cargo del administrador de red, el cual deberá analizar las VLANs que necesitará crear.

El IDS de la figura 4.3 lo utilizamos para detectar los ataques generados por el atacante 1. La interfaz del IDS deberá estar en modo promiscuo y conectada a un puerto espejo del switch de capa 2 para enviar todo el tráfico que pasa a través del switch al puerto. La funcionalidad del IDS fue probada a través del monitor 1 de la figura 2.4. Sin embargo, no recomendamos un IDS basado en software porque su rendimiento es superado por un IDS basado en hardware.

[58] Fuente: Autor del proyecto de titulación.
[59] VLAN: Red de área local virtual.

4.1.2 MÓDULO DE CORE

Para este módulo de core optamos por juntar las funcionalidades del módulo de distribución. Este módulo es la parte central de la red física y su objetivo es realizar el enrutamiento y conmutación del tráfico lo más rápido posible de un módulo a otro. Este módulo permite interconectar los módulos de servidores, gestión, Internet corporativo, y acceso, a través de un sólo switch de capa 3 (véase la figura 4.4). El diseño del módulo de core lo presentamos en la figura 4.4.

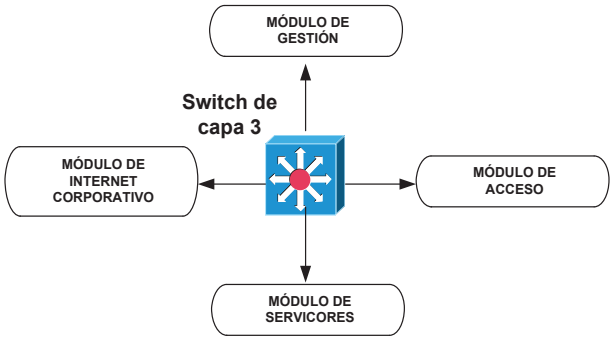

Figura 4.4 Módulo de core propuesto.[60]

4.1.3 MÓDULO DE GESTIÓN

El módulo de gestión es el encargado de administrar los dispositivos de la red física. Utilizamos administración en banda (IB) para gestionar los dispositivos de la red física. Ubicamos el monitor de red y un administrador de red para realizar la administración en banda. Utilizamos un rango de direcciones IPv6 del tipo ULA independiente del resto de la Intranet sólo para la red de gestión. De esta manera, garantizamos que ningún protocolo de enrutamiento publicitará la red de gestión. El diseño del módulo cuenta con un router que actúa como terminal IPSec y de un switch de capa 2. El diseño lo presentamos en la figura 4.5.

[60] Fuente. Autor del proyecto de titulación.

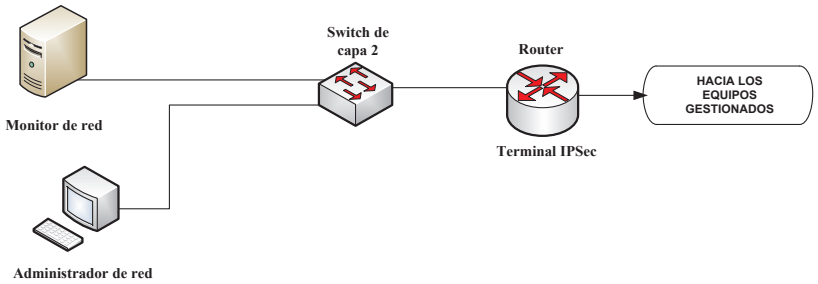

Figura 4.5 Módulo de gestión propuesto.[61]

4.1.4 MÓDULO DE SERVIDORES

El módulo de servidores es el espacio donde ubicamos los servicios internos que utilizarán los usuarios finales. El diseño del módulo de servidores cuenta con un switch de capa 3 como observamos en la figura 4.6. Adicionalmente, separamos las funcionalidades del servidor interno de la red propuesta de la sección 2.1 en dos máquinas independientes, cada una con un rol de servidor específico. Definimos un servidor con el rol WEB para brindar el servicio de páginas web en la red interna. Definimos un servidor con el rol DNS con Directorio activo para resolver los dominios de la red interna. Además, definimos un servidor con el rol Autoridad de Certificación (el diseño de la Autoridad de Certificación la encontramos en la sección 4.2.4.2.) para emitir los certificados digitales a los usuarios finales y a los dispositivos de red. Finalmente, asignamos manualmente un prefijo de red dentro del rango de direcciones IPv6 del tipo ULA para la red del módulo de servidores.

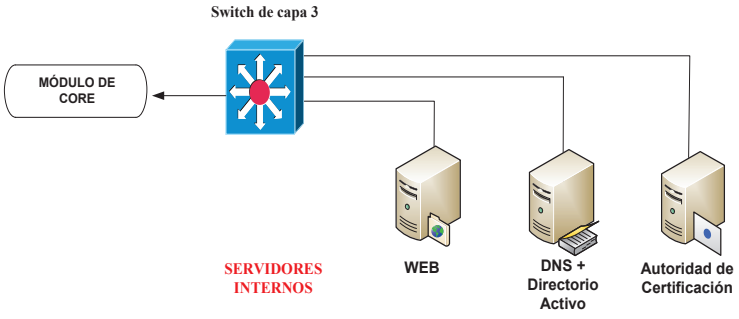

Figura 4.6 Módulo de servidores propuesto.[62]

[61] Fuente. Autor del proyecto de titulación.

4.1.5 MÓDULO DE INTERNET CORPORATIVO

En el módulo de Internet corporativo ubicamos los servicios públicos de la red propuesta de la sección 2.1. El objetivo de este módulo es proporcionar Internet a los usuarios finales y acceso a los usuarios de Internet a los servidores públicos. El diseño de este módulo cuenta con un firewall, un router de borde, y un switch de capa 2. El diseño lo presentamos en la figura 4.7.

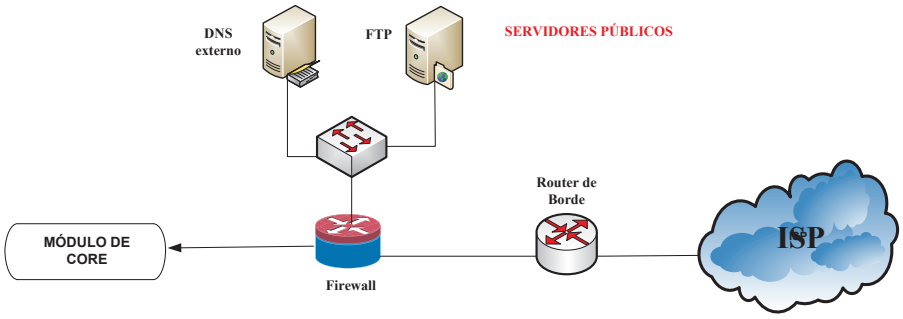

Figura 4.7 Módulo de Internet Corporativo propuesto.[63]

4.2 DISEÑO DEL SISTEMA DE SEGURIDAD DE LA RED FÍSICA

En esta sección diseñamos el sistema de seguridad para la red física de la sección 4.1. El sistema de seguridad abarca los módulos de: acceso, core, gestión, servidores, e Internet corporativo. Los mecanismos de seguridad utilizados dentro de este sistema son: IPSec[L2] para las comunicaciones dentro de la red interna, listas de control de acceso y una DMZ para las comunicaciones dirigidas a los servidores públicos.

Utilizamos IPSec para garantizar la autenticación de origen del remitente de paquetes IPv6. De esta manera, verificamos la identidad del remitente y comprobamos si es la persona que dice ser. Definimos flujos IPv6 que tendrán que utilizar IPSec. Para lo cual, aplicamos políticas [L3] de seguridad IPSec en las

[62] Fuente. Autor del proyecto de titulación.
[63] Fuente. Autor del proyecto de titulación.

comunicaciones que viajan sobre IPv6. Cada una de las políticas de IPSec son definidas para los módulos de acceso, core, gestión y servidores, y son procesadas bajo las dos siguientes consideraciones:

- **Descartar IPSec.-** Definimos los flujos IPv6 que son descartados por IPSec.
- **Aplicar IPSec.-** Definimos los flujos IPv6 que necesitan IPSec para mitigar IP Spoofing.

Para los ataques originados desde el módulo del Proveedor de servicios de Internet, definimos listas de control de acceso y una DMZ. Las listas de control de acceso son utilizadas para filtrar las direcciones de origen que utilizó el atacante 2 en las pruebas V – VII. En cambio, la DMZ es utilizada para restringir flujos de tráfico IPv6 a través de zonas de seguridad del Firewall.

4.2.1 MÓDULO DE ACCESO

En el módulo de acceso mitigaremos las pruebas I – IV. Para cumplir con este objetivo emplearemos IPSec en el módulo de acceso. Consideramos que el atacante 1 podría ubicarse en el área de Tecnología en la VLAN 2. El atacante 1 afectaría las máquinas conectadas al switch de capa 2 configuradas en la VLAN 2. Por esta razón, decidimos utilizar IPSec para crear asociaciones de seguridad entre los usuarios finales del módulo de acceso.

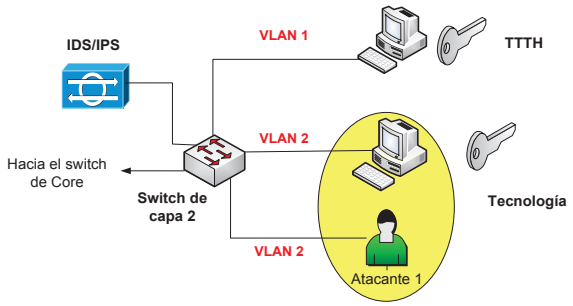

Figura 4.8 Módulo de acceso.[64]

[64] Fuente. Autor del proyecto de titulación.

Las llaves a lado de los usuarios finales de la figura 4.8 representan los certificados digitales[65] utilizados con IPSec. El detalle de los certificados digitales está descrito en la sección 4.2.4.2. A continuación detallamos la política de seguridad IPSec que definimos para el módulo de acceso.

4.2.1.1 Política de seguridad IPSec para el módulo de acceso

Descartar IPSec

Deberemos descartar los mensajes ICMPv6 no autentificados de la siguiente lista, ya que representan un riesgo como observamos en las pruebas I – IV del capítulo 3. Los mensajes que mencionamos a continuación los observamos en el anexo 4 direcciones IPv6 suplantadas pertenecientes a cada prueba – IV del capítulo 3, específicamente, en la columna Mensajes involucrados.

- ICMPv6 Solicitud de vecino.
- ICMPv6 Anuncio de vecino.
- ICMPv6 Solicitud de router.
- ICMPv6 Anuncio de router.
- ICMPv6 Echo Request.
- ICMPv6 Echo Reply.

Aplicar IPSec

Utilizaremos asociaciones de seguridad para asegurar el tráfico ICMPv6 entre: los hosts de los usuarios finales, los usuarios finales y los servidores internos, y los usuarios finales y los servidores públicos. Deberemos definir asociaciones de seguridad separadas. Las asociaciones de seguridad serán definidas para los siguientes procesos que probamos en el capítulo 3:

[65] Certificado Digital: Es una estructura de datos que relaciona una identidad con la clave pública del propietario de la identidad.

- El proceso ND (Descubrimiento del vecino).
- El proceso RD (Descubrimiento del Router).
- El proceso de diagnóstico que ofrece ICMPv6. Es decir, el conjunto de mensajes Echo Request – Echo Reply.
- Adicionalmente, consideramos el mensaje ICMPv6 Paquete demasiado grande y el mensaje ICMPv6 Redireccionamiento porque la técnica de IP Spoofing puede tener como objetivo otras subredes como los segmentos que contienen los servidores internos y servidores públicos.

Las asociaciones de seguridad que definimos para el módulo de acceso deberán tener las siguientes características:

- Deberemos crear asociaciones de seguridad con el protocolo AH[66] (identificador de protocolo igual a 51) en modo túnel para brindar servicio de autenticación de origen a los mensajes ICMPv6 mencionados anteriormente. Cada asociación de seguridad deberá definir un algoritmo de autenticación AH basado en una función hash unidireccional. El algoritmo deberá ser mínimo HMAC con SHA-1-256. Las claves serán manejadas automáticamente a través de IKE[67]. Para lo cual, deberemos utilizar una Autoridad de Certificación[68] local que emita certificados digitales a los hosts de los usuarios finales del módulo de acceso. El detalle del diseño de la Autoridad de Certificación la encontramos descrita en la sección 4.2.4.2. Adicionalmente, el algoritmo de intercambio de llaves deberá ser Diffie-Hellman.

[66] AH: Cabecera de autenticación.
[67] IKE: Intercambio de claves de Internet.
[68] Autoridad de Certificación: Es un organismo encargado de velar por las claves públicas, para conseguir esto, firma y distribuye correctamente los certificados.

4.2.2 MODULO DE CORE

El módulo de core mitigará las pruebas locales y remotas en las que interviene el router de la red propuesta de la sección 2.1. Específicamente mitigaremos las pruebas III, V y VI. Para cumplir con este objetivo implementaremos túneles IPSec en el switch de capa 3 [69] de la figura 4.9. Utilizaremos IPSec para garantizar la autenticación del origen de los paquetes IPv6 destinados al switch de capa 3 del módulo de core. En la sección 4.2.2.1 detallamos la política de seguridad IPSec que deberemos implementar en el switch de capa 3 del módulo de core.

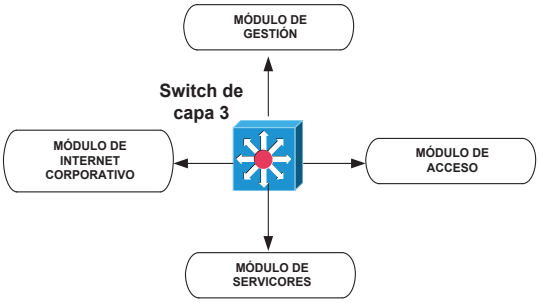

Figura 4.9 Módulo de core.[70]

4.2.2.1 Política de seguridad IPSec para el módulo de core

Descartar IPSec

Deberemos descartar los paquetes IPv6 no autentificados. Deberemos descartar los siguientes mensajes ICMPv6 no autentificados, ya que representan un riesgo como observamos en las pruebas III, V y VI del capítulo 3.

- ICMPv6 Solicitud de router.
- ICMPv6 Anuncio de router.

[69] Los switches de capa 3 tienen la capacidad de realizar el enrutamiento entre VLANs configuradas en el módulo anterior.
[70] Fuente. Autor del proyecto de titulación.

- ICMPv6 Echo Request.
- ICMPv6 Echo Reply.
- ICMPv6 Redireccionamiento.
- ICMPv6 Paquete demasiado grande.

Aplicar IPSec

Utilizaremos asociaciones de seguridad para manejar tráfico ICMPv6 entre los hosts de los usuarios finales y el switch de capa 3 del módulo de core. Deberemos definir asociaciones de seguridad separadas. Las asociaciones serán para los siguientes procesos y mensajes que observamos en las pruebas III, V y VI:

- El proceso RD (Descubrimiento del Router).
- El proceso de diagnóstico que ofrece ICMPv6. Es decir, el conjunto de mensajes Echo Request – Echo Reply.
- El mensaje ICMPv6 Redireccionamiento.
- El mensaje ICMPv6 Paquete demasiado grande.

Las asociaciones de seguridad que crearemos en el módulo de core deberán tener las siguientes características:

- Deberemos crear asociaciones de seguridad con el protocolo AH (identificador de protocolo igual a 51) en modo túnel para brindar servicio de autenticación de origen. Cada asociación de seguridad deberá definir un algoritmo de autenticación AH basado en una función hash unidireccional. El algoritmo deberá ser mínimo HMAC con SHA-1-256. Las claves serán manejadas automáticamente a través de IKE. Para lo cual, deberemos utilizar una Autoridad de Certificación local que emita certificados a los hosts de los usuarios finales y al switch de capa 3 del módulo de core que actúa como

Security Gateway[71]. El detalle del diseño de la Autoridad de Certificación la encontramos descrita en la sección 4.2.4.2. Adicionalmente, el algoritmo de intercambio de llaves deberá ser Diffie-Hellman.

4.2.3 MÓDULO DE GESTIÓN

La división de las funcionalidades de las máquinas de la red propuesta de la sección 2.1 mitigó los ataques locales de las pruebas I – IV pero puso en riesgo el módulo de gestión a ataques remotos. Por esta razón, utilizamos el diseño del módulo de gestión de la figura 4.10 para mitigar las pruebas remotas V y VI. En este sentido, ubicaremos el monitor de red y un administrador de red en la VLAN gestión (véase la figura 4.10), y su configuración será realizada en el switch de capa 2.

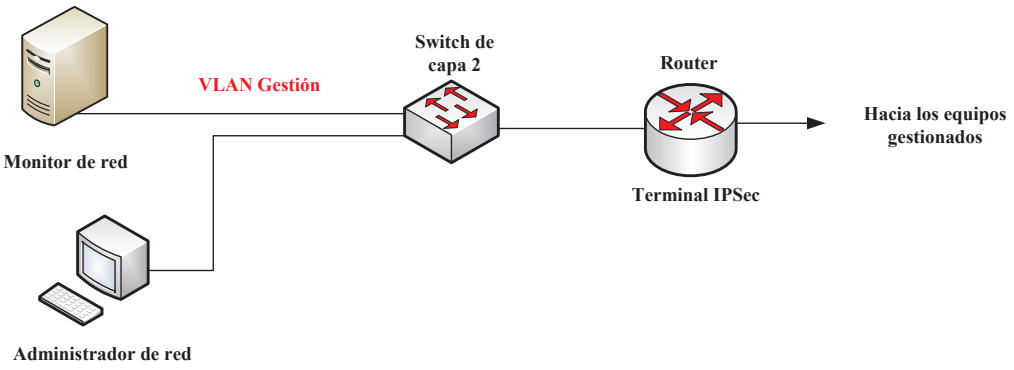

Figura 4.10 Módulo de gestión.[72]

Implementaremos IPSec en el router de la figura 4.10 para garantizar la confidencialidad de la información de gestión, y autenticación del origen del remitente de paquetes IPv6. El router será utilizado como un extremo del túnel IPSec. El otro extremo del túnel será un dispositivo de red que es administrado remotamente. Como requisito, este extremo también deberá implementar IPSec. El router del módulo de gestión será capaz de dejar pasar sólo tráfico de gestión. La asignación

[71] Security Gateway: Es un sistema intermedio que implementa los protocolos IPsec. Por ejemplo, un router, un switch de capa 3, o un firewall implementando IPsec es un security gateway.
[72] Fuente. Autor del proyecto de titulación.

de las direcciones IPv6 de las interfaces del router será manual. Enseguida detallamos la política de seguridad IPSec que deberemos implementar en el router del módulo de gestión.

4.2.3.1 Política de seguridad IPSec para el módulo de gestión

Descartar IPSec

- No se permitirá que desde los dispositivos gestionados se envíe tráfico diferente al tráfico de gestión.
- No se permitirá que tráfico diferente al tráfico de gestión atraviese el Security Gateway.
- Se deberá descartar todo tráfico no autentificado.

Aplicar IPSec

Utilizaremos la asociación de seguridad entre el router y los dispositivos gestionados (véase la figura 4.11). La zona confiable de la figura 4.11 será garantizada a través de controles de acceso físicos. En cambio, la zona desconfiable será asegurada a través de IPSec en el router, el cual actúa como un Security Gateway. Deberemos definir asociaciones de seguridad separadas. Las asociaciones serán para los siguientes procesos que observamos en las pruebas V y VI:

- El proceso de diagnóstico que ofrece ICMPv6. Es decir, el conjunto de mensajes Echo Request – Echo Reply.
- El mensaje ICMPv6 Paquete demasiado grande.
- El mensaje ICMPv6 Redireccionamiento.

Las asociaciones de seguridad que crearemos para el módulo de gestión deberán tener las siguientes características:

- Deberemos crear asociaciones de seguridad con el protocolo ESP[73] (identificador de protocolo igual a 50) en modo túnel para brindar servicio de confidencialidad sobre el tráfico de gestión y autenticación del origen de los datos. La asociación de seguridad deberá especificar un algoritmo de encriptación ESP que utilice criptografía simétrica. En consecuencia, el algoritmo deberá ser mínimo AES-256. El algoritmo de autenticación ESP deberá ser mínimo HMAC con SHA-1-256. Las claves serán manejadas automáticamente a través de IKE. Para lo cual, deberemos utilizar una Autoridad de Certificación para que emita certificados digitales a los dispositivos gestionados y al router que actúa como Security Gateway. El detalle del diseño de la Autoridad de Certificación la encontramos descrita en la sección 4.2.4.2. Adicionalmente, el algoritmo de intercambio de llaves deberá ser Diffie-Hellman.

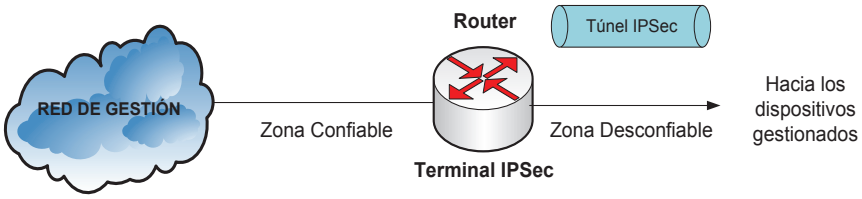

Figura 4.11 Implementación de IPSec para el router del módulo de gestión.[74]

4.2.4 MÓDULO DE SERVIDORES

La división de las funcionalidades de las máquinas de la red propuesta de la sección 2.1 mitigó los ataques locales de las pruebas I – IV pero puso en riesgo el módulo de servidores a ataques remotos. Por esta razón, utilizaremos el diseño del módulo de servidores de la figura 4.12 para mitigar las pruebas remotas V y VI. Para lo cual, en el switch de la figura 4.12 crearemos y administraremos la VLAN servicios internos. Los mecanismos de seguridad utilizados para mitigar IP Spoofing dentro del diseño

[73] ESP: Encapsulating Security Payload.
[74] Fuente. Autor del proyecto de titulación.

del módulo de servidores son: políticas de seguridad IPSec en la sección 4.2.4.1, y controles de acceso físico para el cuarto de cómputo en la sección 4.2.4.3.

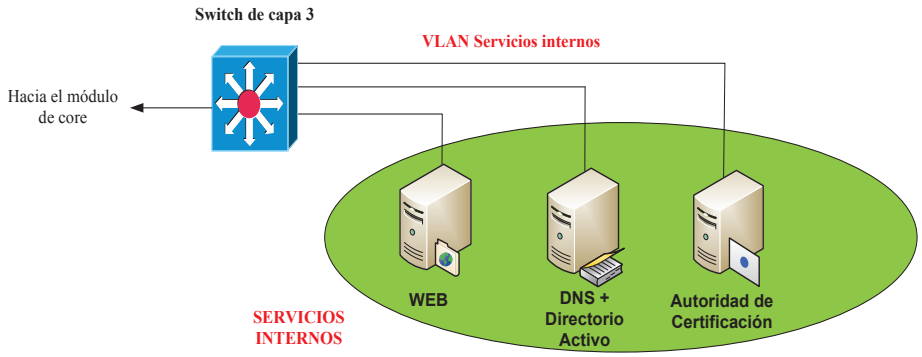

Figura 4.12 Módulo de servidores.[75]

4.2.4.1 Política de seguridad ipsec para el módulo de servidores

Descartar IPSec

Se deberá descartar todo el tráfico no autenticado.

Aplicar IPSec

Utilizaremos asociaciones de seguridad para manejar tráfico entre el Security Gateway y los usuarios finales que acceden a los servidores internos (véase la figura 4.13). Deberemos definir asociaciones de seguridad separadas. Las asociaciones serán para los siguientes procesos que observamos en las pruebas V y VI:

- El proceso de diagnóstico que ofrece ICMPv6. Es decir, el conjunto de mensajes Echo Request – Echo Reply.
- El mensaje ICMPv6 Paquete demasiado grande.

[75] Fuente. Autor del proyecto de titulación.

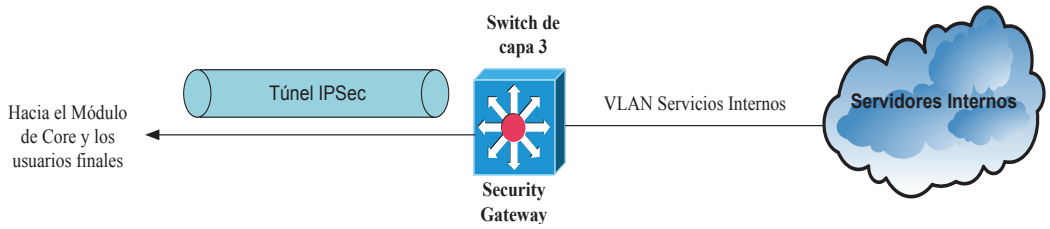

Figura 4.13 Implementación de IPSec para el Switch de capa 3 del módulo de servidores.[76]

Las asociaciones de seguridad que crearemos en el módulo de servidores deberán tener las siguientes características:

- Deberemos implementar una asociación de seguridad con el protocolo AH (identificador de protocolo igual a 51) en modo túnel para brindar servicio de autenticación de origen. La asociación de seguridad deberá especificar un algoritmo de autenticación AH basado en una función hash unidireccional. El algoritmo deberá ser mínimo HMAC con SHA-1-256. Las claves serán manejadas automáticamente a través de IKE. Para lo cual, deberemos utilizar una Autoridad de Certificación que emita certificados a los clientes y al switch de capa 3 del módulo de servidores que actúa como Security Gateway. El detalle del diseño de la Autoridad de Certificación la encontramos descrita en la sección 4.2.4.2. Adicionalmente, el algoritmo de intercambio de llaves deberá ser Diffie-Hellman.

4.2.4.2 Autoridad de certificación

La autoridad de certificación la utilizaremos para emitir certificados digitales X.509 versión 3 a usuarios finales y a dispositivos de red. Como observamos en la figura 4.7, la autoridad de certificación será implementada de forma centralizada en la VLAN servicios internos del módulo de servidores.

[76] Fuente. Autor del proyecto de titulación.

La razón por la cual empleamos certificados digitales es gracias al beneficio ofrecido para establecer comunicaciones autenticadas a nivel de capa de red. Utilizamos los certificados digitales para ofrecer el servicio de autenticación del origen, y confidencialidad. Los tipos de certificados que emitirá deberán ser los siguientes de la tabla 4.1:

Tabla 4.1 Tipos de certificados digitales[77]

Tipo de Certificado	Descripción
Personal	Serán certificados de uso personal para identificar los usuarios finales.
Dispositivos de red	Serán certificados para identificar los dispositivos de comunicación como: router, y switch de capa 3.

Utilizaremos la autoridad certificadora para emitir certificados de acuerdo a la tabla 4.2. Esta autoridad de certificación formará parte de una PKI[78] local para emitir certificados válidos sólo para la Intranet. El algoritmo empleado para la firma digital de los certificados será RSA[79] porque requiere menos tiempo de cómputo que otros algoritmos de firma digital.

Recomendamos que el período de validez de los certificados de usuarios finales deba ser mínimo de un año, ya que consideramos la vigencia mínima de un contrato de trabajo de un año calendario. Para los dispositivos de red, recomendamos que el período de validez de los certificados digitales sea mínimo tres años, ya que consideramos el tiempo de vida del dispositivo. La longitud de clave mínima que recomendamos es 2048 bits, la cual permite garantizar la seguridad del algoritmo como lo cita la fuente [W11].

[77] Fuente. Autor del proyecto de titulación.
[78] PKI: Infraestructura de clave pública.
[79] RSA de sus autores Rivest, Shamir y Adleman, es un sistema criptográfico de clave pública desarrollado en 1977.

Tabla 4.2 Atributos del certificado digital.[80]

Tipo de Certificado	Longitud de la clave	Validez	Firma digital
Personal	De 2048 a 4096 bits	Hasta un año calendario	RSA
Dispositivos de red	De 2048 a 4096 bits	Hasta tres años	RSA

4.2.4.3 Control de acceso físico para el cuarto de cómputo [T1]

Definimos controles de acceso físico para manejar la seguridad física del cuarto de cómputo donde ubicaremos a los servidores. Los controles de acceso físico deberán ser capaces de prohibir el ingreso de personal no autorizado. Este control permitirá que el personal no autorizado, no se conecte directamente al switch de capa 3 de los servidores internos de la figura 4.12, y ejecute los ataques locales de las pruebas I – IV. Para lo cual, establecemos los siguientes requerimientos que deberemos tomar en cuenta:

- Servicio de guardianía las 24 horas del día, los 7 días de la semana.
- Credenciales para identificar fácilmente a los empleados y visitantes de la organización.
- Control de acceso a través de un sistema biométrico (huella digital). Este sistema garantizará que todo acceso de los empleados al cuarto de equipos esté registrado. En cambio, para controlar el acceso de los visitantes deberemos utilizar procedimientos de autorización e identificación de visitantes.
- Sistema de video vigilancia mediante cámaras IP. Este sistema deberá ser implementado como una infraestructura independiente. Las cámaras IP deberán estar conectadas a un switch, y el switch deberá estar conectado a

[80] Fuente. Autor del proyecto de titulación.

un servidor de video vigilancia. El switch deberá tener como características: Power over Ethernet (PoE), administración remota, y configuración vía web. El período en el cual deberá estar la información guardada por el sistema de video vigilancia no es tema del proyecto de titulación, sin embargo, recomendamos un período mínimo de 6 meses.

- Puerta con cerradura especial para el ingreso al cuarto de cómputo.

4.2.5 MODULO DE INTERNET CORPORATIVO

Utilizaremos el módulo de Internet corporativo para mitigar las pruebas remotas V y VI. Para cumplir con este objetivo emplearemos listas de control de acceso y una DMZ. En el router de borde de la figura 4.14 debemos configurar listas de control de acceso para mitigar los ataques originados desde el Proveedor de servicios de Internet. Denegaremos los siguientes prefijos de red que probamos en la prueba V y que las encontramos detalladas en el anexo 4:

- Prefijo de la red 6bone. 3FFE::/16
- Prefijo Sitio local. FEC0::/10
- Prefijo de documentación. 2001:DB8::/32
- Prefijos de direcciones reservadas. 0000::/8 0100::/8 0200::/7 0400::/6 0800::/5 1000::/4 4000::/3 6000::/3 8000::/3 a000::/3 c000::/3 e000::/4 f000::/5 f800::/6 fe00::/9
- Prefijo de la dirección IPv4 mapeada. ::FFFF:0:0/96
- Prefijo de la dirección IPv4 compatible. 0000::IPV4/128
- Prefijo de la dirección Traducción IPv4 – IPv6. 64:FF9B::/96
- Prefijo de red ULA de los usuarios finales de la Intranet.

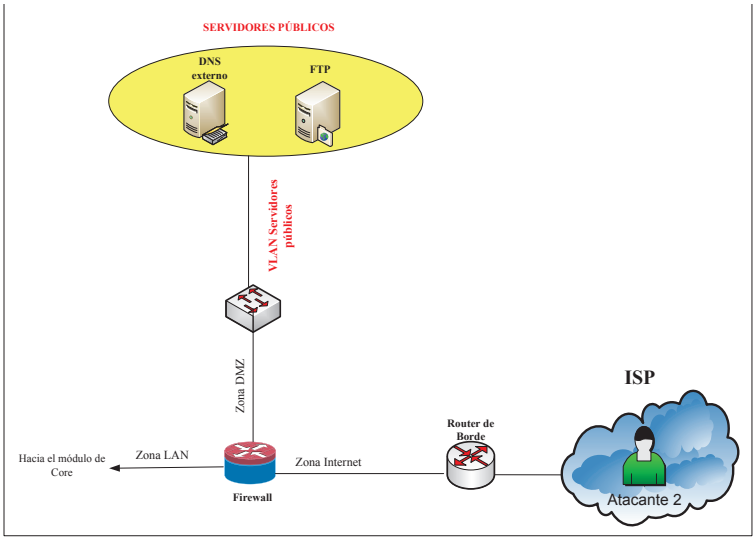

Figura 4.14 Módulo de Internet Corporativo.[81]

Utilizaremos un firewall para definir una DMZ con servicios públicos expuestos a redes externas (véase la figura 4.14). La DMZ nos permitirá protegernos del atacante 1 ubicado en el módulo de acceso, y del atacante 2 ubicado en el Proveedor de servicios de Internet. Emplearemos políticas de seguridad para permitir o denegar el tráfico que intenta ingresar a la DMZ. El firewall implementará zonas de seguridad en cada una de sus interfaces. Cada interfaz estará conectada a una zona de seguridad. La tabla 4.3 muestra las tres zonas que se necesitará crear.

Tabla 4.3 Definición de las zonas de seguridad.[82]

Zonas de Seguridad	Definición
Internet	Comprende los enlaces hacia redes externas.
DMZ	Comprende los servicios públicos de la red.
LAN	Comprende la Intranet.

[81] Fuente. Autor del proyecto de titulación.
[82] Fuente. Autor del proyecto de titulación.

Las políticas del firewall deberán lucir como las reglas de la tabla 4.4. Esta tabla indica que tipo de accesos están permitidos o denegados, y además, describe el tipo de tráfico que puede atravesar el firewall. Cada fila de la tabla es una regla en particular que será aplicada a cada una de las zonas de seguridad mencionadas en la tabla anterior.

Tabla 4.4 Políticas de las zonas de seguridad.[83]

Zona Emisora	Zona Receptora	Acción	Descripción de la política
Internet	LAN	Denegar	Todo tráfico que venga desde la Internet cuyo destino sea la LAN, será denegado.
Internet	DMZ	Permitir	Permitirá acceder sin restricción a los servicios públicos de la DMZ.
DMZ	LAN	Permitir	Permitirá tráfico HTTP.
LAN	DMZ	Permitir	Permitirá acceder sin restricción a los servicios públicos de la DMZ.
LAN	Internet	Permitir	Sólo permitirá tráfico hacia servidores Web HTTP.
DMZ	Internet	Permitir	Permitirá realizar consultas DNS para peticiones de dominios externos.

El DNS externo de la figura 4.14 será creado para que resuelva peticiones de dominios externos. Asignaremos manualmente un rango de direcciones IPv6 del tipo

[83] Fuente. Autor del proyecto de titulación.

unicast global en los servicios públicos, router de borde, y en las interfaces del firewall donde definimos la zona DMZ y la zona Internet. La zona LAN será configurada con una dirección IPv6 ULA.

En total existen 65535 puertos de los cuales 1024 son puertos conocidos. Del total de puertos conocidos utilizaremos únicamente los puertos de la tabla 4.5. En este sentido, debemos limitar en las reglas de firewall solamente los puertos conocidos que vamos a permitir, ya que los puertos no utilizados representan una puerta por la cual puede acceder un atacante. Es decir, no deberemos crear reglas de firewall con valor ANY en los campos puerto origen o destino.

Tabla 4.5 Reglas del Firewall

Protocolo	Puerto
FTP	21 (TCP)
DNS	DNS: 53 (UDP, TCP)
IKE	IKE: 500 (UDP)
SNMP	161, 162 (UDP)

4.3 DIAGRAMA FINAL DE LA RED FÍSICA

En esta sección mostramos el diagrama final del diseño de la red física. El diagrama de la figura 4.15 es el resultado del diseño a través de SAFE utilizando el análisis de resultados de las pruebas del capítulo tres.

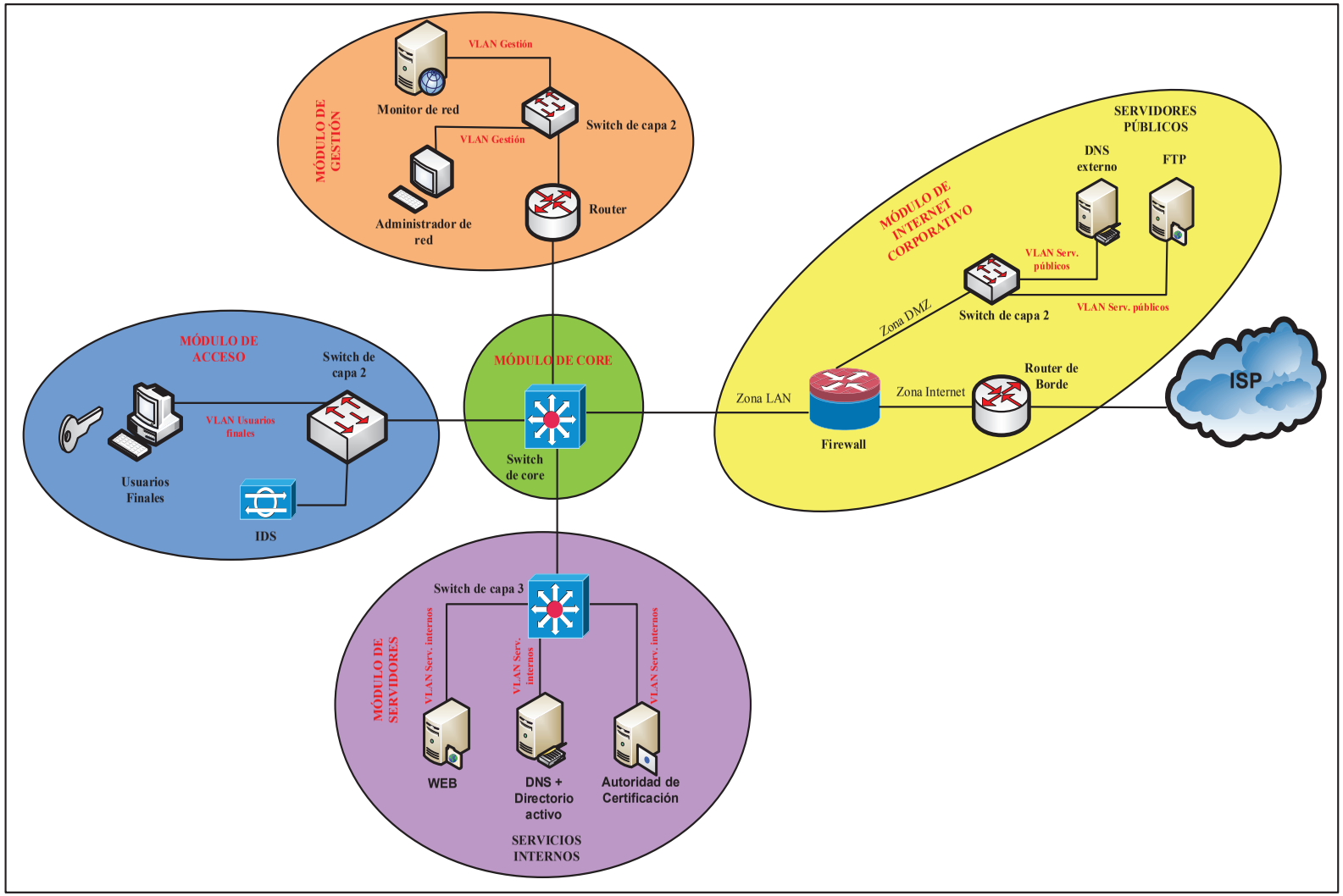

Figura 4.15 Diagrama final de la red física.[84]

[84] Fuente. Autor del proyecto de titulación.

4.3.1 REQUISITOS MÍNIMOS DE EQUIPOS [T2]

En la tabla 4.6 describimos el dimensionamiento de los equipos que encontramos en el diagrama final de la red física de la figura 4.15. El cálculo del throughput y backplane lo realizamos como lo define la fuente [T3]. El cálculo del throughput lo encontramos en el anexo 5. En cada módulo del diseño de la red física calculamos el throughput y backplane para dimensionar cuál es la velocidad mínima que necesitan los dispositivos de red.

El throughput lo calculamos en el anexo 5 con la fórmula 4.1. Para calcular el throughput consideramos la longitud del paquete de la capa de enlace. El tamaño mínimo del paquete de la capa de enlace es 64 bytes, más los siguientes campos: 7 bytes de preámbulo, 1 byte delimitador, y 12 bytes de GAP. En total tenemos los 64 bytes, más los 20 bytes. El backplane lo calculamos con la fórmula 4.2. Para calcular el backplane consideramos el número de puertos del diagrama final de red física de la sección 4.3, y la capacidad de cada puerto.

$$\textbf{Throughput} = \frac{\textbf{\# puertos} * \textbf{capacidadPuerto}}{\textbf{longuitud del paquete}} \qquad \textbf{fórmula 4.1}$$

$$\textbf{Backplane} = \textbf{\# puertos} * \textbf{capacidadPuerto} * \textbf{2} \qquad \textbf{fórmula 4.2}$$

Enseguida detallamos el dimensionamiento de los equipos del diagrama final de la red física en la tabla 4.6.

Tabla 4.6 Requisitos mínimos de equipos.[85]

Equipos	Requisitos mínimos
Router de borde	• 2 puertos RJ – 45 10/100/1000 full dúplex

[85] Fuente. Autor del proyecto de titulación.

	• Backplane = 2 * 1000 * 2 = 4 Gbps • Throughput = 23,81 Mpps • Administración remota • Configuración vía web • Soporte IPv6 • Soporte ACLs IPv6 • Enrutamiento IPv6 estático y dinámico
Firewall en Hardware	• 3 puertos RJ – 45 10/100/1000 full dúplex • Backplane = 3 * 1000 * 2 = 6 Gbps • Throughput = 35,72 Mpps • Soporte de VLANs. Estándar IEEE 802.1Q • Administración remota • Configuración vía web • Soporte IPv6
Switch de capa 2 módulo de Internet corporativo	• 3 puertos RJ – 45 10/100 full dúplex • Backplane = 3 * 100 * 2 = 0,6 Gbps • Throughput = 3,57 Mpps • Administración remota • Configuración vía web • Soporte de VLANs. Estándar IEEE 802.1Q • Soporte IPv6
Switch de core	• 4 puertos RJ – 45 10/100 full dúplex • Backplane = 4 * 100 * 2 = 0,8 Gbps • Throughput = 4,76 Mpps • Enrutamiento IPv6 estático y dinámico • Soporte de VLANs. Estándar IEEE 802.1Q • Fuente de alimentación con redundancia interna para asegurar la disponibilidad del módulo de core.

	• Soporte IPSec • Soporte IPv6 • Administración remota • Configuración vía web • Soporte autoconfiguración Stateless de IPv6
Switch de capa 2 módulo de gestión	• 2 puertos RJ – 45 10/100 full dúplex • Backplane = 2 * 100 * 2 = 0,4 Gbps • Throughput = 2,38 Mpps • Administración remota • Configuración vía web • Soporte de VLANs. Estándar IEEE 802.1Q • Soporte IPv6
Switch de capa 2 módulo de acceso	• 2 puertos RJ – 45 10/100 full dúplex • 1 puerto en modo espejo • Backplane = 3 * 100 * 2 = 0,6 Gbps • Throughput = 3,57 Mpps • Administración remota • Configuración vía web • Soporte de VLANs. Estándar IEEE 802.1Q • Soporte IPv6
Switch de capa 3 módulo de servidores	• 4 puertos RJ – 45 10/100 full dúplex • Backplane = 4 * 100 * 2 = 0,8 Gbps • Throughput = 4,76 Mpps • Administración remota • Configuración vía web • Direccionamiento IPv6 estático y dinámico • Soporte de VLANs. Estándar IEEE 802.1Q • Fuente de alimentación con redundancia interna para asegurar la disponibilidad del módulo de

	servidores • Soporte IPSec • Soporte IPv6
IDS	• 1 puerto RJ – 45 10/100 full dúplex. El puerto deberá trabajar en modo promiscuo para escuchar el tráfico IPv6 que generan los usuarios finales. • Soporte IPv6
Servidor DNS externo[86]	• Procesador a 1 GHz • Memoria interna de 512 MB • Capacidad del disco de 8GB • 1 puerto RJ45 • Licencia sistema operativo Windows Server 2008 • Soporte IPv6
Servidor FTP[W10]	• Memoria RAM: 2 GB • Capacidad del disco de 1TB. La capacidad de disco consideramos un 1TB porque es un servicio público que almacenará gran cantidad de información por rangos de tiempo largos. • 1 puerto RJ45 • Sistema operativo Centos • Soporte IPv6
Servidor WEB[86]	• Procesador a 1 GHz • Memoria interna de 512 MB • Capacidad del disco de 8GB • 1 puerto RJ45 • Licencia sistema operativo Windows Server

[86] Los requisitos mínimos fueron sacados de la página oficial de *Microsoft.* son los requisitos mínimos para instalar Windows Server 2008.

<table>
<tr>
<td></td>
<td>
2008
• Soporte IPv6

Cálculo del ancho de banda

Ponemos a consideración un estimado de 100 usuarios simultáneos que accederán al servidor WEB, con un tiempo de refresco de aproximadamente 60 segundos. El tamaño promedio de la página Web que alojará el servidor consideramos que será de 1KB, que es el tamaño de la página web utilizada en este proyecto de titulación. Con esta información, el cálculo del ancho de banda sigue de la siguiente manera:

$$\mathbf{AB} = \frac{\mathbf{T\ [KB]}}{\mathbf{t\ [seg]}} * \frac{\mathbf{8bits}}{\mathbf{1Byte}} * \mathbf{\#usuarios\ simultáneos}$$

Dónde:

T: Tamaño de la página Web. Unidad en Kilobytes.
t: tiempo promedio en que el usuario final accede al servidor Web.

$$\mathrm{AB} = \frac{1\ [\mathrm{KB}]}{60\ [\mathrm{seg}]} * \frac{8\mathrm{bits}}{1\mathrm{Byte}} * 100\ \mathrm{usuarios\ simultáneos}$$
$$= 13{,}33\ \mathrm{Kbps}$$

$$\mathbf{AB = 13,33\ Kbps}$$
</td>
</tr>
<tr>
<td>Servidor DNS interno + Directorio activo[86]</td>
<td>
• Procesador a 1 GHz
• Memoria interna de 512 MB
• Capacidad del disco de 8GB
</td>
</tr>
</table>

	• 1 puerto RJ45 • Licencia sistema operativo Windows Server 2008 • Soporte IPv6
Autoridad de Certificación[W10]	• Procesador a 1 GHz • Memoria RAM 1GB • Capacidad del disco de 5GB • 1 puerto RJ45 • Sistema operativo Centos • Soporte IPv6

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

En este capítulo redactamos las conclusiones y recomendaciones que alcanzamos a través del desarrollo de este proyecto de titulación.

5.1 CONCLUSIONES

- Con pocos recursos podemos analizar ataques informáticos sin la necesidad de emplear equipos reales. Esto lo logramos construyendo un laboratorio de simulación parecido a un ambiente real a través de herramientas disponibles en la Internet, con el cual simulamos estaciones de trabajo, servidores, router, switches, y una red IPv6 dentro de una máquina física.

- En las secciones de análisis de resultados observamos que los mensajes ICMPv6 de capa 3 pueden ser fácilmente vulnerados con la técnica de IP Spoofing. Dichos mensajes son utilizados en procesos muy críticos en la operación de las redes IPv6. Procesos como el anuncio del vecino utilizado para la comunicación IPv6 entre vecinos, o el proceso de descubrimiento del router utilizado para encontrar el router oficial, o el proceso de diagnóstico utilizado para conocer si un extremo de la comunicación IPv6 está arriba.

- El sistema de seguridad diseñado a través de IPSec permite autenticar los mensajes IPv6. Proponemos utilizar certificados digitales para confiar en el remitente y garantizar la autenticidad de los mensajes IPv6. Dicha confianza es brindada a través de la Autoridad Certificadora y sus certificados deben estar firmados con RSA y mínimo 2048 bits la longitud de clave. Adicionalmente, los certificados de usuario tendrán una vigencia de un año, y los de dispositivos de red tendrán una vigencia de tres años.

5.2 RECOMENDACIONES

- Recomendamos utilizar este proyecto de titulación en las entidades públicas para definir políticas de seguridad IPSec. Para lo cual, estas entidades deberán llegar a un acuerdo en las políticas IPSec que serán aplicadas en cada una de ellas. Estas políticas deberán ser las mismas en cada una de las entidades para que el túnel IPSec se levante.

- Recomendamos que el proveedor de servicios de Internet configure reglas de filtrado en sus dispositivos de borde. Estos dispositivos deberán denegar direcciones obsoletas, especiales, y reservadas por la IETF. Inclusive, recomendamos que el proveedor de servicios de Internet deniegue aquellas direcciones de su pool de direcciones que todavía no asigna a sus clientes. De esta manera, el rango de direcciones IPv6 que podría suplantar el atacante con la técnica de IP Spoofing se reducirá notablemente.

- Recomendamos definir, publicar, mantener y comunicar una política de seguridad a todos los usuarios internos de la red. La política debe estar presente desde que los usuarios internos ingresan a la organización hasta cuando se desvinculan de ella. El objetivo es minimizar los riesgos de seguridad asociados a los usuarios internos. En este sentido, recomendamos establecer controles en: la contratación de los colaboradores, el desarrollo de la actividad laboral, y la finalización de la relación entre la organización y el colaborador.

- Recomendamos que el administrador de red revisé periódicamente una base de datos de vulnerabilidades de IPv6. En nuestro caso recomendamos revisar NIST. Esta acción permitirá que el administrador esté actualizado y con el conocimiento necesario sobre los ataques que son reportados por los expertos de NIST en lo que se refiere a IPv6.

- Recomendamos utilizar navegación segura para el servidor interno de la red física solamente si la información que intercambia el servidor WEB es transaccional. De esta manera, deberemos utilizar HTTPS a través de certificados digitales ya que contamos con una autoridad de certificación local que nos autentica ante las otras partes de la Intranet.

- Recomendamos ejecutar un proceso de blindaje a las estaciones de trabajo de los usuarios finales, servidores y dispositivos de red que conforman el diagrama final de red física de la figura 4.15. El objetivo es eliminar configuraciones erróneas y certificar el correcto funcionamiento de los servidores.

REFERENCIAS BIBLIOGRÁFICAS

Libro

[L1] ZIRING Neal, “Router Security Configuration Guide Supplement - Security for IPv6 Routers”, Estados Unidos, 2006.

[L2] STALLINGS William, “Cryptography and Network Security Principles and Practice”, 5th edición, Estados Unidos, 2011.

[L3] FRANCISCONI Hugo Adrian, “IPSec en Ambientes IPv4 e IPv6”, Mendoza, Argentina, 2005.

Tesis de grado

[T1] TORRES Zambrano, DAVID Fernando, “Diseño del Data Center para CERT – Ecuador”, Quito, 2013.

[T2] AGUIRRE Ponce, ARSENIO Antonio; CARCHI Alvear, PABLO Rodrigo, “Análisis, Diseño e Implementación de un Prototipo de Notarías Digitales”, Quito, 2011.

[T3] JÁCOME Zambrano, GERMÁN Paolo; QUIROGA Chauca, LICETH Alejandra, “Diseño de una Red Multiservicios para el Centro de Rehabilitación Médico No. 3 y la Dirección Provincial MIES-INFA en Portoviejo”, Quito, 2013.

Internet

[W1] THC, Revisado en Febrero 2013: https://www.thc.org/papers/vh_thc-ipv6_attack.pdf

[W2] Wikipedia, Revisado en Enero 2013:
http://es.wikipedia.org/wiki/Vulnerabilidad#En_inform.C3.A1tica

[W3] National Vulnerability Database, Revisado en Febrero 2013:
http://web.nvd.nist.gov/view/vuln/search-advanced

[W4] Sans, Revisado en Febrero 2013:
http://www.sans.org/reading-room/whitepapers/threats/introduction-ip-spoofing-959

[W5] Wikipedia, Revisado en Febrero 2013:
http://en.wikipedia.org/wiki/IP_address_spoofing

[W6] Wikipedia, Revisado en Febrero 2013:
http://66.14.166.45/sf_whitepapers/tcpip/IP%20Spoofing%20-%20An%20Introduction.pdf

[W7] Wikipedia, Revisado en Enero 2013:
http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica#Tipos_de_amenaza

[W8] Net Market Share, Revisado en Marzo 2013:
http://marketshare.hitslink.com

[W9] Cisco, Revisado en Junio 2013:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf

[W10] Wikipedia, Revisado en Junio 2013
http://es.wikipedia.org/wiki/CentOS

[W11] Wikipedia, Revisado en Agosto 2014
http://es.wikipedia.org/wiki/RSA

ANEXOS

ANEXO 1: Configuración del router de la red propuesta

ANEXO 2: Comparación de resultados

ANEXO 3: Alertas del monitor 1

ANEXO 4: Direcciones ipv6 suplantadas

ANEXO 5: Cálculo del throughput

ANEXO 1: CONFIGURACIÓN DEL ROUTER DE LA RED PROPUESTA

En este anexo detallamos la configuración realizada en las interfaces del router de la red propuesta. Las interfaces del router son: fa 1/0, fa 1/1 y fa 2/0. La configuración de la interfaz fa 1/0 del router la realizamos manualmente. Para configurar la interfaz fa 1/0 es necesario ingresar al modo config, asignar una dirección IPv6 ULA, y habilitar el procesamiento IPv6 en la interfaz con el comando **ipv6 enable** como observamos en las siguientes líneas:

```
Router# config terminal
Router(config)# interface fastethernet1/0
Router(config-if)# ipv6 address FD00::100/64
Router(config-if)# ipv6 enable
Router(config-if)# exit
```

Luego configuramos los mensajes RAs en la interfaz fa 1/0 junto con los parámetros para soportar la autoconfiguración stateless. Para configurar los mensajes RAs y la autoconfiguración utilizamos el comando **ipv6 nd.** De esta manera, el router habilita la autoconfiguración de direcciones IPv6 para que la máquina cliente configure una dirección IPv6 en base al prefijo de red FD00::/64. Lo descrito observamos en las siguientes líneas:

```
Router(config)# interface fastethernet1/0
Router(config-if)# ipv6 nd prefix FD00::/64
Router(config-if)# exit
```

Luego, para que el router comience a procesar tráfico IPv6 usamos el comando **ipv6 unicast-routing**. Esto provocará el envío automático de mensajes RA en la interfaz fa 1/0. Lo descrito observamos en las siguientes líneas:

```
Router(config)# ipv6 unicast-routing
```

```
Router(config)# exit
```

Para configurar la interfaz 1/1 y 2/0 es necesario ingresar al modo config, asignar la dirección IPv6 global 2800:68:c:214::100 para la interfaz fa 1/1 y 2800:68:c:215::100 para la interfaz 2/0, y habilitar el procesamiento IPv6 en cada interfaz con el comando **ipv6 enable**. Lo descrito observamos en las siguientes líneas:

```
Router# config terminal
Router(config)# interface fastethernet1/1
Router(config-if)# ipv6 address 2800:68:c:214::100/64
Router(config-if)# ipv6 enable
Router(config-if)# interface fastethernet2/0
Router(config-if)# ipv6 address 2800:68:c:215::100/64
Router(config-if)# ipv6 enable
Router(config-if)# exit
```

Finalmente, revisamos la configuración realizada usando el comando **show ipv6 interface brief**. El resultado de digitar el comando nos arroja una dirección IPv6 enlace local generada automáticamente y una dirección IPv6 global configurada manualmente. Lo descrito observamos en las siguientes líneas:

```
Router# show ipv6 interface brief
FastEthernet0/0            [administratively down/down]
        unassigned
FastEthernet1/0            [up/up]
        FE80::C800:16FF:FE30:1C
        FD00::100
FastEthernet1/1            [up/up]
        FE80::C800:16FF:FE30:1D
        2800:68:c:214::100
FastEthernet2/0            [up/up]
```

FE80::C800:16FF:FE30:38

2800:68:c:215::100

ANEXO 2: COMPARACIÓN DE RESULTADOS

PRUEBA I

La tabla 2.1 detalla el direccionamiento IPv6 inicial de las máquinas cliente, monitor de red, y servidor interno. La tabla 2.2 detalla el direccionamiento IPv6 con las máquinas encendidas durante todo el ataque. Y la tabla 2.3 detalla el direccionamiento IPv6 cuando las máquinas las reiniciamos durante el ataque.

Tabla 2.1 Direccionamiento IPv6 inicial.

Máquina	Asignación de direcciones	Direcciones IPv6	Dirección IPv6 enlace local
Cliente	Stateless	Fd00::b4a:15c3:51a:ba96 Fd00:c0a5:8ff:27f5:6f0e	Fe80::8c7e:5f56:855e:495e
Monitor de red	Manual	Fd00::6	Fe80::20c:29ff:fecf:095a
Servidor interno	Manual	Fd00::5	Fe80::d89d:580d:a3a5:c88e

Tabla 2.2 Direccionamiento IPv6 con las máquinas encendidas durante todo el ataque.

Máquina	Asignación de direcciones	Direcciones IPv6	Dirección IPv6 enlace local
Cliente	Stateless	Fd00::b4a:15c3:51a:ba96 Fd00:c0a5:8ff:27f5:6f0e	Fe80::8c7e:5f56:855e:495e
Monitor de red	Manual	Fd00::7	Fe80::20c:29ff:fecf:095a
Servidor interno	Manual	Fd00::5	Fe80::d89d:580d:a3a5:c88e

Tabla 2.3 Direccionamiento IPv6 cuando las máquinas las reiniciamos durante el ataque.

Máquina	Asignación de direcciones	Direcciones IPv6	Dirección IPv6 enlace local
Cliente	Stateless	–	–
Monitor de red	Manual	–	–
Servidor interno	Manual	–	–

PRUEBA II

La tabla 2.4 y 2.5 detallan los registros de la tabla de vecinos[87] iniciales y después del ataque.

Tabla 2.4 Registros iniciales de la tabla de vecinos.

Máquina	Dirección IPv6	Dirección MAC	Descripción
Cliente	Fd00::5	00-0C-29-BD-27-97	Servidor interno
	Fe80::c800:16ff:fe30:1c	CA-00-16-30-00-1C	Puerta de enlace
Servidor interno	Fd00::7	00-0C-29-89-CC-97	Monitor 1
	Fd00::100	CA-00-16-30-00-1C	Puerta de enlace
	Fd00::6c56:e455:9dfd:3bc9	00-0C-29-B6-E2-36	Cliente
	Fe80::20c:29ff:fe89:cc97	00-0C-29-89-CC-97	Monitor 1
	Fe80::c800:16ff:fe30:1c	CA-00-16-30-00-1C	Puerta de enlace

[87] La tabla de vecinos es una tabla que tiene almacenada la correspondencia entre dirección IPv6 y dirección MAC. La tabla se la puede revisar en sistemas Windows a través del comando *netsh interface ipv6 show neighbors*.

Tabla 2.5 Registros de la tabla de vecinos durante el ataque.

Máquina	Dirección IPv6	Dirección MAC	Descripción
Cliente	Fd00::5	00-0C-29-EB-17-2F	Atacante 1
	Fe80::20c:29ff:feeb:172f	00-0C-29-EB-17-2F	Atacante 1
	Fe80::c800:16ff:fe30:1c	00-0C-29-EB-17-2F	Atacante 1
Servidor interno	Fd00::7	00-0C-29-EB-17-2F	Atacante 1
	Fd00::100	CA-00-16-30-00-1C	Puerta de enlace
	Fd00::6c56:e455:9dfd:3bc9	00-0C-29-EB-17-2F	Atacante 1
	Fd00::8c7e:5f56:855e:495e	00-0C-29-EB-17-2F	Atacante 1
	Fe80::20c:29ff:fe89:cc97	00-0C-29-89-CC-97	Monitor 1
	Fe80::20c:29ff:feeb:172f	00-0C-29-EB-17-2F	Atacante 1
	Fe80::c800:16ff:fe30:1c	00-0C-29-EB-17-2F	Atacante 1

PRUEBA III

Las tablas 2.6 y 2.7 detallan los valores iniciales y durante el ataque. Los valores de las tablas 2.6 y 2.7 son valores máximos observados en las máquinas cliente, monitor de red y servidor interno.

Tabla 2.6 Valores iniciales de la prueba III.

Máquina	Uso de CPU	Uso de la memoria
Cliente	3%	31%

Monitor de red	11%	38%
Servidor interno	9%	41%

Tabla 2.7 Valores durante el ataque de la prueba III.

Máquina	Uso de CPU	Uso de la memoria
Cliente	100%	61%
Monitor de red	11%	40%
Servidor interno	9%	59%

PRUEBA IV

En las tablas 2.8 y 2.9 muestro los valores antes y durante la ejecución del ataque, respectivamente.

Tabla 2.8 Valores antes del ataque.

Máquina	Uso de la red	Uso de CPU
Cliente	0%	4%
Monitor de red	0%	5%
Servidor interno	0%	7%

Tabla 2.9 Valores durante el ataque.

Máquina	Uso de la red	Uso de CPU
Cliente	4,02%	81%

Monitor de red	5,19%	80%
Servidor interno	7,94%	97%

PRUEBA V

La tabla 2.10 muestra los valores iniciales y finales obtenidos en la prueba V.

Tabla 2.10 Valores iniciales y finales de la prueba V.

	MTU Inicial (Bytes)	**MTU Final (Bytes)**
Cliente – Servidor interno	1500 [88]	1500
Cliente – Servidor público	1500	1500

PRUEBA VI

Las tablas 2.11 y 2.12 detallan la información de la tabla de destinos[89] antes, y durante el ataque, respectivamente. La dirección Fd00::5 corresponde a la dirección del servidor interno. Mientras que la dirección 2800:68:c:214::6 corresponde a la dirección del servidor público.

Tabla 2.11 Valores iniciales de la prueba VI.

Máquina	**Dirección de destino**	**Dirección de próximo salto**
Cliente	Fd00::5	Fd00::5

[88] El valor de la MTU fue observado en sistemas Windows a través del comando *netsh interface ipv6 show subinterfaces.* Mientras que en sistemas Linux a través del comando *ifconfig.*
[89] La tabla de destinos es una tabla con información del siguiente salto. Para revisar su contenido en sistemas Windows se digita el comando *netsh interface ipv6 show destinationcache*.

	2800:68:c:214::6	fe80::c800:16ff:fe30:1c

Tabla 2.12 Valores durante el ataque de la prueba VI.

Máquina	Dirección de destino	Dirección de próximo salto
Cliente	Fd00::5	Fd00::5
	2800:68:c:215::6	Fe80::20c:29ff:feeb:172f

ANEXO 3: ALERTAS DEL MONITOR 1

PRUEBA I

La figura 3.1 muestra las alertas que se generaron cuando realicé la prueba I sobre las máquinas cliente, monitor de red, y servidor interno.

Time	Probe	Reason	Ethernet Address 1	Ethernet Address 2	IPv6 Address
Sun Jul 14 16:47:06 2013	eth1	new IP	0:50:56:c0:0:1	0:0:0:0:0:0	fd00::fc82:96ee:1563:a3c5
Sun Jul 14 16:47:05 2013	eth1	new staton	0:50:56:c0:0:1	0:0:0:0:0:0	fe80::8424:43b1:a12c:22ce
Sun Jul 14 16:47:03 2013	eth1	dad dos	0:c:83:ac:89:a3	0:0:0:0:0:0	fe80::c4fe:121d:ddc7:72e6
Sun Jul 14 16:47:03 2013	eth1	dad dos	0:c:83:ac:89:a3	0:0:0:0:0:0	fe80::c4fe:121d:ddc7:72e6
Sun Jul 14 16:47:03 2013	eth1	dad dos	0:c:be:63:7e:77	0:0:0:0:0:0	fe80::7556:38fb:e220:cc83
Sun Jul 14 16:47:03 2013	eth1	dad dos	0:c:be:63:7e:77	0:0:0:0:0:0	fe80::7556:38fb:e220:cc83
Sun Jul 14 16:47:02 2013	eth1	dad dos	0:c:cc:b8:ac:7f	0:0:0:0:0:0	fe80::5cf5:84d9:3431:c1f7
Sun Jul 14 16:47:02 2013	eth1	dad dos	0:c:cc:b8:ac:7f	0:0:0:0:0:0	fe80::5cf5:84d9:3431:c1f7
Sun Jul 14 16:47:02 2013	eth1	dad dos	0:c:a3:dd:ee:8a	0:0:0:0:0:0	fe80::5dc6:2bd6:6d1e:5516
Sun Jul 14 16:47:02 2013	eth1	dad dos	0:c:a3:dd:ee:8a	0:0:0:0:0:0	fe80::5dc6:2bd6:6d1e:5516
Sun Jul 14 16:47:01 2013	eth1	dad dos	0:c:6:16:99:9c	0:0:0:0:0:0	fe80::69b9:42cf:f234:caeb
Sun Jul 14 16:47:01 2013	eth1	dad dos	0:c:6:16:99:9c	0:0:0:0:0:0	fe80::69b9:42cf:f234:caeb
Sun Jul 14 16:47:01 2013	eth1	dad dos	0:c:44:90:e0:6b	0:0:0:0:0:0	fe80::6899:d62c:67d7:e2d7
Sun Jul 14 16:47:01 2013	eth1	dad dos	0:c:44:90:e0:6b	0:0:0:0:0:0	fe80::6899:d62c:67d7:e2d7
Sun Jul 14 16:47:00 2013	eth1	new staton	0:c:29:b6:e2:36	0:0:0:0:0:0	fe80::8c7e:5f56:855e:495e
Sun Jul 14 16:47:00 2013	eth1	dad dos	0:c:b3:eb:31:6f	0:0:0:0:0:0	fe80::8c7e:5f56:855e:495e
Sun Jul 14 16:47:00 2013	eth1	dad dos	0:c:b3:eb:31:6f	0:0:0:0:0:0	fe80::8c7e:5f56:855e:495e
Sun Jul 14 16:47:00 2013	eth1	unknown mac vendor	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Sun Jul 14 16:47:00 2013	eth1	new staton	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Sun Jul 14 16:47:00 2013	eth1	new staton	0:c:29:bd:27:97	0:0:0:0:0:0	fd00::7183:dd9c:848d:2489
Sun Jul 14 16:47:00 2013	eth1	new IP	ca:0:16:30:0:1c	0:0:0:0:0:0	fd00::100
Sun Jul 14 16:47:00 2013	eth1	NA router flag	ca:0:16:30:0:1c	0:0:0:0:0:0	fd00::100
Sun Jul 14 16:47:00 2013	eth1	dad dos	0:c:e6:a6:be:ff	0:0:0:0:0:0	fd00::7183:dd9c:848d:2489
Sun Jul 14 16:47:00 2013	eth1	dad dos	0:c:e6:a6:be:ff	0:0:0:0:0:0	fd00::7183:dd9c:848d:2489
Sun Jul 14 16:47:00 2013	eth1	new staton	0:c:20:11:da:db	0:0:0:0:0:0	fe80::b836:f7f7:cb77:3512
Sun Jul 14 16:47:00 2013	eth1	new staton	0:c:b9:59:b4:4c	0:0:0:0:0:0	fd00::b836:f7f7:cb77:3512
Sun Jul 14 16:47:00 2013	eth1	dad dos	0:c:c5:f1:b4:b3	0:0:0:0:0:0	fd00::3c64:5300:46c4:cbcb
Sun Jul 14 16:47:00 2013	eth1	dad dos	0:c:c5:f1:b4:b3	0:0:0:0:0:0	fd00::3c64:5300:46c4:cbcb

Figura 3.1 Alertas de la prueba I.

PRUEBA II

La figura 3.2 muestra las alertas que se generaron cuando realicé la prueba II sobre las máquinas cliente y servidor interno.

Time	Probe	Reason	Ethernet Address 1	Ethernet Address 2	IPv6 Address
Mon Jul 15 09:21:33 2013	eth1	wrong router redirect	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:33 2013	eth1	wrong router redirect	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:33 2013	eth1	wrong ipv6 hop limit	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:34 2013	eth1	wrong router redirect mac	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:34 2013	eth1	wrong ipv6 hop limit	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:35 2013	eth1	wrong router redirect ip	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:36 2013	eth1	wrong ipv6 hop limit	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:37 2013	eth1	wrong router redirect	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:37 2013	eth1	wrong ipv6 hop limit	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:37 2013	eth1	wrong router redirect mac	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:37 2013	eth1	wrong ipv6 hop limit	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:38 2013	eth1	wrong ipv6 hop limit	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:38 2013	eth1	wrong router redirect mac	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:38 2013	eth1	wrong ipv6 hop limit	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:38 2013	eth1	wrong router redirect ip	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:38 2013	eth1	wrong ipv6 hop limit	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:38 2013	eth1	wrong router redirect	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 15 09:21:38 2013	eth1	wrong ipv6 hop limit	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:38 2013	eth1	wrong ipv6 hop limit	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:38 2013	eth1	wrong router redirect mac	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c
Mon Jul 15 09:21:38 2013	eth1	wrong ipv6 hop limit	ca:0:16:30:0:1c	0:0:0:0:0:0	fe80::c800:16ff:fe30:1c

Figura 3.2 Alertas de la prueba II.

PRUEBA III

La figura 3.3 muestra las alertas que se generaron cuando realicé la prueba III sobre las máquinas cliente y servidor interno.

Time	Probe	Reason	Ethernet Address 1	Ethernet Address 2	IPv6 Address
Sat Dec 1 13:39:20 2012	eth0	wrong ipv6 router	0:18:7:3e:e6:af	0:0:0:0:0:0	fe80::218:7ff:fe3e:e6af
Sat Dec 1 13:39:20 2012	eth0	wrong ipv6 router	0:18:e3:1:b8:a7	0:0:0:0:0:0	fe80::218:e3ff:fe01:b8a7
Sat Dec 1 13:39:20 2012	eth0	wrong ipv6 router	0:18:25:a4:96:a8	0:0:0:0:0:0	fe80::218:25ff:fea4:96a8
Sat Dec 1 13:39:20 2012	eth0	wrong ipv6 router	0:18:19:a8:87:0	0:0:0:0:0:0	fe80::218:19ff:fea8:8700
Sat Dec 1 13:39:20 2012	eth0	wrong ipv6 router	0:18:ea:52:3a:a3	0:0:0:0:0:0	fe80::218:eaff:fe52:3aa3
Sat Dec 1 13:39:20 2012	eth0	wrong ipv6 router	0:18:93:47:65:29	0:0:0:0:0:0	fe80::218:93ff:fe47:6529
Sat Dec 1 13:39:20 2012	eth0	wrong ipv6 router	0:18:4a:ac:e1:d1	0:0:0:0:0:0	fe80::218:4aff:feac:e1d1
Sat Dec 1 13:39:20 2012	eth0	wrong ipv6 router	0:18:c1:43:64:fb	0:0:0:0:0:0	fe80::218:c1ff:fe43:64fb
Sat Dec 1 13:39:21 2012	eth0	wrong ipv6 router	0:18:d5:c5:24:3a	0:0:0:0:0:0	fe80::218:d5ff:fec5:243a
Sat Dec 1 13:39:21 2012	eth0	wrong ipv6 router	0:18:c1:5e:b3:a3	0:0:0:0:0:0	fe80::218:c1ff:fe5e:b3a3
Sat Dec 1 13:39:21 2012	eth0	wrong ipv6 router	0:18:e4:a8:78:48	0:0:0:0:0:0	fe80::218:e4ff:fea8:7848
Sat Dec 1 13:39:21 2012	eth0	wrong ipv6 router	0:18:3b:48:9d:5f	0:0:0:0:0:0	fe80::218:3bff:fe48:9d5f
Sat Dec 1 13:39:21 2012	eth0	wrong ipv6 router	0:18:fe:d5:e6:b1	0:0:0:0:0:0	fe80::218:feff:fed5:e6b1
Sat Dec 1 13:39:21 2012	eth0	wrong ipv6 router	0:18:88:cc:a1:0	0:0:0:0:0:0	fe80::218:88ff:fecc:a100
Sat Dec 1 13:39:21 2012	eth0	wrong ipv6 router	0:18:91:df:1a:2e	0:0:0:0:0:0	fe80::218:91ff:fedf:1a2e
Sat Dec 1 13:39:21 2012	eth0	wrong ipv6 router	0:18:38:92:a4:1e	0:0:0:0:0:0	fe80::218:38ff:fe92:a41e
Sat Dec 1 13:39:22 2012	eth0	wrong ipv6 router	0:18:4e:f9:e9:f0	0:0:0:0:0:0	fe80::218:4eff:fef9:e9f0
Sat Dec 1 13:39:22 2012	eth0	wrong ipv6 router	0:18:2a:49:b8:45	0:0:0:0:0:0	fe80::218:2aff:fe49:b845
Sat Dec 1 13:39:22 2012	eth0	wrong ipv6 router	0:18:1:e0:9:a5	0:0:0:0:0:0	fe80::218:1ff:fee0:9a5

Figura 3.3 Alertas de la prueba III.

PRUEBA VI

La figura 3.4 muestra las alertas que se generaron cuando realicé la prueba VI sobre las máquinas servidor interno y servidor público.

Time	Probe	Reason	Ethernet Address 1	Ethernet Address 2	IPv6 Address
Mon Jul 22 12:15:03 2013	eth3	new station	0:50:56:c0:0:1	0:0:0:0:0:0	fd00::ed73:d585:98a2:1056
Mon Jul 22 12:15:00 2013	eth3	changed ethernet address	0:c:29:eb:17:2f	ca:0:16:30:0:1c	fd00::1
Mon Jul 22 12:15:00 2013	eth3	NA router flag	0:c:29:eb:17:2f	0:0:0:0:0:0	fd00::1
Mon Jul 22 12:15:00 2013	eth3	NA router flag	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 22 12:15:00 2013	eth3	new IP	ca:0:16:30:0:1c	0:0:0:0:0:0	fd00::100
Mon Jul 22 12:15:00 2013	eth3	NA router flag	ca:0:16:30:0:1c	0:0:0:0:0:0	fd00::100
Mon Jul 22 12:14:55 2013	eth3	new station	0:c:29:eb:17:2f	0:0:0:0:0:0	fd00::1
Mon Jul 22 12:14:55 2013	eth3	new station	0:c:29:b6:e2:36	0:0:0:0:0:0	fd00::7de5:bdc:8f82:c32d
Mon Jul 22 12:14:55 2013	eth3	NA router flag	0:c:29:eb:17:2f	0:0:0:0:0:0	fd00::1
Mon Jul 22 12:14:55 2013	eth3	ethernet mismatch	ca:0:16:30:0:1c	0:c:29:eb:17:2f	fd00::1
Mon Jul 22 12:14:55 2013	eth3	wrong ipv6 hop limit	ca:0:16:30:0:1c	0:0:0:0:0:0	fd00::1
Mon Jul 22 12:14:55 2013	eth3	unknown mac vendor	ca:0:16:30:0:1c	0:0:0:0:0:0	fd00::1
Mon Jul 22 12:14:55 2013	eth3	changed ethernet address	ca:0:16:30:0:1c	0:c:29:eb:17:2f	fd00::1
Mon Jul 22 12:14:55 2013	eth3	NA router flag	ca:0:16:30:0:1c	0:0:0:0:0:0	fd00::1
Mon Jul 22 12:14:55 2013	eth3	ethernet mismatch	ca:0:16:30:0:1c	0:c:29:b6:e2:36	fd00::7de5:bdc:8f82:c32d
Mon Jul 22 12:14:55 2013	eth3	wrong ipv6 hop limit	ca:0:16:30:0:1c	0:0:0:0:0:0	fd00::7de5:bdc:8f82:c32d
Mon Jul 22 12:14:55 2013	eth3	changed ethernet address	ca:0:16:30:0:1c	0:c:29:b6:e2:36	fd00::7de5:bdc:8f82:c32d
Mon Jul 22 12:14:55 2013	eth3	changed ethernet address	0:c:29:b6:e2:36	ca:0:16:30:0:1c	fd00::7de5:bdc:8f82:c32d
Mon Jul 22 12:14:55 2013	eth3	new station	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f
Mon Jul 22 12:14:55 2013	eth3	NA router flag	0:c:29:eb:17:2f	0:0:0:0:0:0	fe80::20c:29ff:feeb:172f

Figura 3.4 Alertas de la prueba VI.

ANEXO 4: DIRECCIONES IPV6 SUPLANTADAS

PRUEBA I

La tabla 4.1 detalla las direcciones IPv6 falsificadas que se crearon cuando las máquinas se reiniciaron durante el ataque.

Tabla 4.1 Direcciones IPv6 falsificadas cuando las máquinas se reiniciaron durante el ataque.

Máquina	Dirección IPv6 origen	Dirección IPv6 falsificada	Mensaje involucrado	MAC Spoofing	IP Spoofing exitoso
Cliente	Fd00::1	Direcciones de enlace local y dirección ULA que intenta configurar el Cliente	NA	√	√
Monitor de red	Fd00::1	Direcciones de enlace local y dirección ULA que intenta configurar el Monitor	NA	√	√
Servidor interno	Fd00::1	Direcciones de enlace local y dirección ULA que intenta configurar el Servidor interno	NA	√	√

PRUEBA II

En la tabla 4.2 detallo los NA, los mensajes HTTP intercambiados desde el servidor interno al cliente, y los mensajes HTTP intercambiados desde el cliente al servidor interno que utilizan la técnica de IP Spoofing en la prueba II.

Tabla 4.2 Mensajes suplantados en la prueba II.

Máquina	Dirección IPv6 origen	Dirección IPv6 suplantada	Mensaje involucrado	MAC Spoofing	IP Spoofing exitoso

Cliente	Fd00::1	Fd00:6c56:e455:9dfd:3bc9	NA	X	√
	Fd00::1	Fd00:6c56:e455:9dfd:3bc9	Mensajes HTTP intercambiados desde el cliente al servidor interno		
Servidor interno	Fd00::1	Fd00::5	NA	X	√
	Fd00::1	Fd00::5	Mensajes HTTP intercambiados desde el servidor interno al cliente		

PRUEBA III

La tabla 4.3 detalla las direcciones IPv6 falsificadas creadas durante la prueba III. La tabla sólo describe un mensaje RA de entre todos los mensajes RAs falsificados por el atacante 1.

Tabla 4.3 Ejemplo de un mensaje RA falsificado en la prueba III.

Máquina	Dirección IPv6 origen	Dirección IPv6 origen falsificada	Mensaje involucrado	MAC Spoofing	IP Spoofing exitoso
Cliente	Fe80::20c:29ff:feeb:172f	Fe80::218:7ff:fe3e:e6af	RA	√	√
Servidor Interno	Fe80::20c:29ff:feeb:172f	Fe80::218:e3ff:fe01:b8a7	RA	√	√

PRUEBA IV

En la tabla 4.4 detallo la dirección de origen suplantadas en los paquetes IPv6 de la prueba V. Las direcciones IPv6 origen suplantada de la tabla 4.4 corresponde a la dirección origen del servidor interno.

Tabla 4.4 Mensajes suplantados en la prueba IV.

Dirección IPv6 origen	Dirección IPv6 origen suplantada	Dirección IPv6 destino	Mensaje involucrado	MAC Spoofing	IP Spoofing exitoso
Fd00::1	Fd00::5	Ff02::1	Echo Request	√	√

PRUEBA V

En la tabla 4.5 detallo las direcciones de origen suplantadas en los paquetes IPv6 de la prueba V. Las direcciones IPv6 destino para cada cada una de las filas de la tabla 4.5 corresponden a las direcciones del servidor interno y público. La dirección origen FD00::1 corresponde al atacante 1. Mientras que la dirección origen 2800:68:c:215::1 corresponde al atacante 2.

Tabla 4.5 Direcciones de origen suplantadas de la prueba V.

Servidor atacado	Dirección IPv6 origen	Dirección IPv6 origen suplantada	Significado de la dirección IPv6 suplantada	Mensaje involucrado	MAC Spoofing	IP Spoofing exitoso
Servidor público	FD00::1	FD00::2892:ff59:448e:96d6	Dirección del Cliente	Echo Request, y Paquete demasiado	X	√
	2800:68:c:215::1					

Servidor interno	2800:68:c:215::1			grande		
Servidor público	FD00::1	3FFE::/16	Dirección Obsoleta de la red 6bone	Echo Request, y Paquete demasiado grande	X	√
Servidor público	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	FEC0::/10	Dirección Obsoleta Sitio local	Echo Request, y Paquete demasiado grande	X	√
Servidor público	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	0000::172.16.0.62/128	Dirección Obsoleta IPv4 compatible	Echo Request, y Paquete demasiado grande	X	√
Servidor público	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	0000::/8	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	X
Servidor público	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					

Servidor público	FD00::1	0100::/8	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	0200::/7	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	0400::/6	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	0800::/5	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
dor públi	FD00::1	1000::/4	Dirección Reservada por	Echo Request, y	X	√

	2800:68:c:215::1		la IETF	Paquete demasiado grande		
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	4000::/3	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	6000::/3	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	8000::/3	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	A000::/3	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado	X	√
	2800:68:c:215::1					

Servidor interno	2800:68:c:215::1			grande		
Servidor público	FD00::1	C000::/3	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	E000::/4	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	F000::/5	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	F800::/6	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					

Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	FE00::/9	Dirección Reservada por la IETF	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	FF00::/8	Dirección Multicast	Echo Request, y Paquete demasiado grande	X	X
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	::1/128	Dirección Loopback	Echo Request, y Paquete demasiado grande	X	X
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	::/128	Dirección No especificada	Echo Request, y Paquete demasiado grande	X	X
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					

Servidor público	FD00::1	::FFFF:0:0/96	Dirección IPv4 mapeada	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	2001:DB8::/32	Dirección de Documentación	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					
Servidor público	FD00::1	64:FF9B::/96	Traducción IPv4 – IPv6	Echo Request, y Paquete demasiado grande	X	√
	2800:68:c:215::1					
Servidor interno	2800:68:c:215::1					

PRUEBA VI

La tabla 4.6 detallo los mensajes Echo Request y Redireccionamiento que utilizan la técnica de IP Spoofing para la prueba VI. La dirección fd00::1 corresponde a la dirección del atacante 1. Mientras que la dirección 2800:68:c:215::1 corresponde a la dirección del atacante 2.

Tabla 4.6 Mensajes suplantados en la prueba VI.

Servidor atacado	Dirección IPv6 origen	Dirección IPv6 suplantada	Mensaje involucrado	MAC Spoofing	IP Spoofing exitoso
Servidor interno	2800:68:c:215::1	Fd00::5	Echo Request	√	√
		fe80::c800:16ff:fe30:1c	Redireccionamiento[90]		X
Servidor público	Fd00::1	2800:68:c:214::6	Echo Request	√	√
		fe80::c800:16ff:fe30:1c	Redireccionamiento		
	2800:68:c:215::1	2800:68:c:214::6	Echo Request	√	√
		fe80::c800:16ff:fe30:1c	Redireccionamiento		X

PRUEBA VII

La tabla 4.7 muestra el mensaje Echo Request que utiliza la técnica de IP Spoofing para la prueba VII. La dirección fd00::1 corresponde a la dirección del atacante 1. Mientras que la dirección 2800:68:c:215::1 corresponde a la dirección del atacante 2.

Tabla 4.7 Mensajes falsificados en la prueba VII.

Dirección IPv6 origen	Dirección IPv6 origen suplantada	Dirección IPv6 destino	Mensaje falsificado	MAC Spoofing	IP Spoofing exitoso
FD00::1	FF02::1	2800:68:C:214::6	Echo Request	√	X

[90] Estos mensajes fueron descartados por el router c7200. No aceptó la dirección origen fe80:c800:16ff:fe30:1c

2800:68:C:215::1	FF02::1	2800:68:C:214::6	Echo Request	√	X
2800:68:C:215::1	FF02::1	FD00::5	Echo Request	√	X

ANEXO 5: CÁLCULO DEL THROUGHPUT

En este anexo realizamos el cálculo del throughput para los dispositivos de red del diagrama final de la red física del plan de mitigación. Para realizar el cálculo del throughput consideramos los requisitos mínimos de los dispositivos de dicho diagrama. Enseguida presentamos el cálculo del throughput para los módulos de acceso, core, gestión, servidores e Internet corporativo.

MÓDULO DE ACCESO

En esta sección realizamos el cálculo del throughput del switch de capa 2 del módulo de acceso.

$$\text{Throughput} = \frac{3 * 100 \frac{\text{bits}}{\text{segundo}}}{(64 + 20) \frac{\text{bytes}}{1\text{paquete}} . \frac{8\text{bits}}{1\text{byte}}} = 3{,}57\text{M} \frac{\text{paquetes}}{\text{segundo}}$$

$$\mathbf{Throughput = 3,57Mpps}$$

MÓDULO DE CORE

En esta sección realizamos el cálculo del throughput del switch de capa 3 del módulo de core.

$$\text{Throughput} = \frac{4 * 100 \frac{\text{bits}}{\text{segundo}}}{(64 + 20) \frac{\text{bytes}}{1\text{paquete}} . \frac{8\text{bits}}{1\text{byte}}} = 4{,}76\text{M} \frac{\text{paquetes}}{\text{segundo}}$$

$$\mathbf{Throughput = 4,76Mpps}$$

MÓDULO DE GESTIÓN

En esta sección realizamos el cálculo del throughput del switch de capa 2 del módulo de gestión.

$$\text{Throughput} = \frac{2 * 100 \frac{\text{bits}}{\text{segundo}}}{(64 + 20) \frac{\text{bytes}}{1\text{paquete}} . \frac{8\text{bits}}{1\text{byte}}} = 2{,}38\text{M} \frac{\text{paquetes}}{\text{segundo}}$$

$$\mathbf{Throughput = 2,38Mpps}$$

MÓDULO DE SERVIDORES

En esta sección realizamos el cálculo del throughput del switch de capa 3 del módulo de servidores.

$$\text{Throughput} = \frac{4 * 100 \frac{\text{bits}}{\text{segundo}}}{(64 + 20) \frac{\text{bytes}}{1\text{paquete}} . \frac{8\text{bits}}{1\text{byte}}} = 4{,}76\text{M} \frac{\text{paquetes}}{\text{segundo}}$$

$$\mathbf{Throughput = 4,76Mpps}$$

MÓDULO DE INTERNET CORPORATIVO

En esta sección realizamos el cálculo del throughput del router de borde, firewall y del switch de capa 2 del módulo de Internet corporativo.

$$\text{Throughput}_{\text{ router de borde}} = \frac{2 * 1000 \frac{\text{bits}}{\text{segundo}}}{(64 + 20) \frac{\text{bytes}}{1\text{paquete}} . \frac{8\text{bits}}{1\text{byte}}} = 23{,}81\text{M} \frac{\text{paquetes}}{\text{segundo}}$$

$$\mathbf{Throughput}_{\mathbf{\ router\ de\ borde}} \mathbf{= 23,81Mpps}$$

$$\text{Throughput}_{\text{ firewall}} = \frac{3 * 1000 \frac{\text{bits}}{\text{segundo}}}{(64 + 20) \frac{\text{bytes}}{1\text{paquete}} \cdot \frac{8\text{bits}}{1\text{byte}}} = 35{,}72 \frac{\text{paquetes}}{\text{segundo}}$$

$$\textbf{Throughput}_{\textbf{ firewall}} = \mathbf{35,72Mpps}$$

$$\text{Throughput}_{\text{ switch de capa 2}} = \frac{3 * 100 \frac{\text{bits}}{\text{segundo}}}{(64 + 20) \frac{\text{bytes}}{1\text{paquete}} \cdot \frac{8\text{bits}}{1\text{byte}}} = 3{,}57 \frac{\text{paquetes}}{\text{segundo}}$$

$$\textbf{Throughput}_{\textbf{ switch de capa 2}} = \mathbf{3,57Mpps}$$