Análisis y Comparación de la Seguridad en dos Esquemas de Red, Utilizando los Protocolos IPv4 e IPv6

Israel Emanuel Maldonado Beltrán[1]
Daniel Andrés Páez Sánchez[2]
Ing. José Patiño S.[3]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
[1]email: isemmald@espol.edu.ec
[2]email: dapaez@espol.edu.ec
[3]email: jpatino@espol.edu.ec

[1]Ingeniero en Telemática
[2]Ingeniero en Telemática
[3]Director Del Proyecto de Graduación, Máster en Sistemas, Ing. en Telecomunicaciones, ESPOL

Resumen

En los próximos años el protocolo IPv6 reemplazará ineludiblemente al protocolo IPv4. A pesar de esto, la conciencia sobre detalles técnicos y aspectos de seguridad de este "nuevo" protocolo sigue siendo escasa en los administradores de red de distintas organizaciones en Ecuador. Muchos ataques de seguridad realizados en IPv4, aprovechando las vulnerabilidades de una red, también son factibles en IPv6, por lo que nos propusimos evaluar la respuesta de 2 protocolos IPv6 frente a ataques de seguridad.

Se diseñó e implementó virtualmente dos redes de datos conformadas por enrutadores y ordenadores, la primera red fue configurada con el protocolo OSPFv3 y la segunda red con RIPng. Se manejó un modelo cliente-servidor, donde los clientes intercambiaban información con las bases de datos de los servidores interactuando con los aplicativos prestados por éstos. Los esquemas de red implementados simularon un entorno empresarial donde cada nodo de la red representaba las distintas sucursales y matrices que una empresa puede llegar a tener. Se efectuaron distintos tipos de ataques informáticos a las redes implementadas y se midió la respuesta de cada una tomando en consideración los siguientes parámetros: Disponibilidad, integridad y confidencialidad. Finalmente, se obtuvieron datos estadísticos a partir de las pruebas realizadas, los mismos que nos han dado una mejor idea sobre la seguridad en IPv6. Estos resultados sirven como una nueva fuente de información para administradores de red que deseen conocer más detalles sobre la seguridad en IPv6.

Palabras Claves: *OSPFv3, RIPng, Seguridad en Redes, Denegación de Servicio, Disponibilidad, Confidencialidad, Integridad, Tiempo de transmisión, Velocidad de Transmisión, Convergencia.*

Abstract

In the next years, IPv6 will inevitably replace the IPv4 protocol. Although, taking consciousness about technical details and aspects of security of this "new" protocol is still being poor in network administrators from different companies in Ecuador. Many security attacks perfomed in IPv4, exploiting vulnerabilities in a certain network, are also feasible in IPv6. That's why we proposed to evaluate the response from two IPv6 protocols against security attacks.

We designed and implemented two virtual networks conformed by routers and hosts. The first one was configured with OPSFv3 protocol and the second one with RIPng. We used server-client model, where clients share information with the server databases, interacting with the services. The implemented model network simulated a business environment, where each node connected to the network represented different branches and matrices that a company could have. We performed different types of attacks to the network and then we measure the response from both, taking into consideration the following parameters: Availability, integrality and confidentiality. Finally, we got statistical data from the tests, which helped us to have a better idea about how security operates in IPv6.

These results could help as a source of information for network administrators, so they could know more details about security in IPv6.

Keywords: *OSPFv3, RIPng, Network Security, Denial of Service, Availability, Confidenciality, Integrality, Transmission Time, Transmission Rate, Convergence.*

1. Introducción

En el mundo de la informática y las comunicaciones se han incluido los denominados protocolos, los cuales son reglas estrictas de cómo se dará una comunicación. Dentro de estos protocolos, tal vez el que tenga mayor trascendencia, es el protocolo IP; el cual establece los pasos por los que se va a regir una transmisión de datos en una red de información.

Desde un principio, al desarrollar el protocolo IP y otros tantos protocolos de comunicación, el primer interés fue asegurar el establecimiento de la conexión, es decir que la información llegara a su destino. El siguiente objetivo fue que la información se transmitiera en el menor tiempo posible, de tal manera que se desarrollaron sistemas de información sin tener muy presente la seguridad de la misma.

El hecho de plantear una solución con mucho esfuerzo para luego obtener resultados ineficientes y el hecho de considerar un riesgo mínimo el desprecio de la seguridad fueron unas de las razones por las que la seguridad de la información no fue implementada como una prioridad en los protocolos de comunicación que hoy en día manejamos.

Con el tiempo nos hemos percatado que a pesar de que hemos tenido un alto desarrollo en cuanto a conectividad y velocidad de las comunicaciones, los riesgos de seguridad siempre estarán vigentes existiendo amenazas desde hace varias décadas atrás hasta el día de hoy.

A través de los años se han podido solucionar varios problemas de seguridad con la implementación de nuevos protocolos y medidas de precaución, sin embargo cada vez que se soluciona un problema aparece uno nuevo, por lo que en la actualidad es indispensable la concientización de la seguridad en nuestros entornos de comunicación.

2. Marco Teórico

2.1. OSPFv3

La versión 3 del protocolo OSPF (Open Shortest Path First o su traducción al español, "primero la ruta más corta y despejada") fue diseñada para manejar redes configuradas con el protocolo IPv6. Está definido en la RFC 5340 y continúa siendo un protocolo de estado de enlace.

Entre sus principales características tenemos:

- Está basado en OSPFv2 incluyendo mejorías.
- Distribuye prefijos IPv6.
- Se ejecuta directamente sobre IPv6.
- El método de autenticación ahora hace uso del protocolo IPsec.
- OSPFv3 se ejecuta sobre un enlace en vez de en una subred.

OSPFv3 usa las direcciones IPv6 de enlace local para identificar a los vecinos adyacentes de un determinado enrutador. Por tanto cuando se haga uso del comando "ipv6 ospf neighbor ipv6_address", la dirección configurada debe ser la dirección de enlace local del vecino.

OSPFv3 presenta un nuevo campo llamado "Instance ID" el cual hace posible configurar múltiples instancias OSPFv3 en una sola interfaz. Para que 2 instancias del proceso OSPFv3 establezcan comunicación, es necesario que tengan el mismo valor de "Instance ID", el cual predeterminadamente es 0.

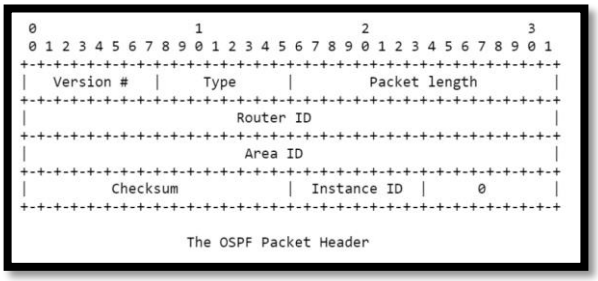

Figura 1. Formato del encabezado de un paquete OSPFv3 [1]

OSPFv3 hace uso de las extensiones de cabecera IPsec AH y ESP del protocolo IPv6 para el manejo de su seguridad. Dejando de lado el mecanismo de autenticación que se manejaba en la versión 2 pues ahora es trabajo de IPv6 y IPsec asegurar el correcto nivel de autenticación a usar. [2]

2.2. RIPng

Definido en la RFC 2080, el protocolo de enrutamiento de información, próxima generación, por sus siglas en inglés (RIPng), conserva ciertas

características de su predecesor, el ya conocido protocolo RIPv2:

- Se mantiene como un protocolo de enrutamiento de tipo “Vector Distancia”, es decir está basado en el algoritmo Bellman-Ford.
- Fue diseñado como un protocolo “puerta adentro” y para redes de baja escalabilidad.
- El número máximo de saltos para alcanzar un destino sigue siendo 15.
- La distancia administrativa del protocolo continúa siendo 120.
- Continúa usando las técnicas de “horizonte dividido” y “envenenamiento reverso” para la prevención de lazos de enrutamiento.

A continuación hemos enlistado las diferencias con RIPv2:

- RIPng ha sido diseñado para enrutar redes y prefijos del protocolo IPv6.
- RIPng hace uso del puerto 521 UDP a diferencia del puerto 520 UDP usado por RIPv2.
- El grupo de direcciones multicast del protocolo es FF02::9 en lugar del grupo 224.0.0.9 usado en la versión para IPv4 del protocolo.

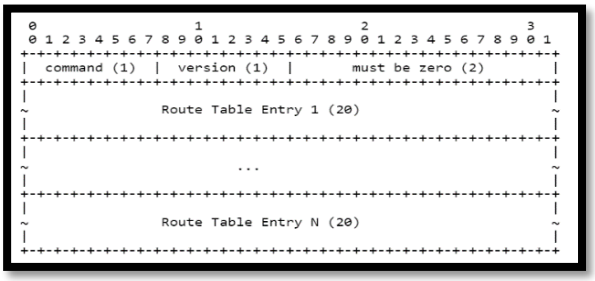

Figura 2. Formato del encabezado de un paquete RIPng [3]

El algoritmo de horizonte dividido evita que un enrutador incluya rutas aprendidas desde un vecino, en actualizaciones que sean enviadas hacia ese mismo vecino. En el caso de una red broadcast, cualquier ruta aprendida desde cualquier vecino, no será incluida en actualizaciones enviadas hacia esa red.

La técnica de envenenamiento reverso sí incluye dichas rutas en las actualizaciones pero les establece una métrica infinita de tal modo que sean inalcanzables y no elegibles para la lógica del enrutador.

2.3. Seguridad en las Redes Informáticas [4]

La autenticación de entidades.- Es el proceso de verificación de la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador.

La confidencialidad de los datos.- Es la propiedad de la información, por la que se garantiza que esté accesible únicamente a personal autorizado.

La integridad de los datos.- Es el estado de protección, corrección y completitud en la estructura de los datos en una aplicación.

El control de acceso.- Es el conjunto de mecanismos y protocolos, a través de los cuales varios dispositivos se ponen de acuerdo para compartir un medio de transmisión común.

El no repudio.- Puede referirse al servicio que proporciona pruebas en la integridad y origen de los datos, o a la autentificación que con un alto aseguramiento puede ser afirmado como genuino.

La disponibilidad.- Es un factor que nos indica cuanto tiempo la información se encuentra a disposición de quienes pueden acceder a ella.

El anonimato.- Es el estado anónimo de una entidad, es decir, que la identidad de dicha entidad es desconocida.

En el presente artículo se tomó en cuenta tres de estos servicios de seguridad, que son la confidencialidad, integridad y disponibilidad de la información.

2.4. Ataque DoS

Es un ataque a una red de computadores donde el objetivo es volver inaccesible un servicio o recurso de red a sus usuarios legítimos. Una forma de llevar a cabo éste ataque es saturar el ancho de banda de una red o recurso de tal modo que se provoque la pérdida de conectividad de dicho recurso. Una ampliación de este ataque es el DDoS, el cual consiste en generar un gran flujo de información desde diferentes puntos de conexión de una red, la forma más común de llevar a cabo estos ataques es una botnet. [5]

El ancho de banda de un servicio no es lo único que se puede saturar, existen otros recursos como el tiempo de procesamiento del CPU o el espacio de disco de un servidor los cuales pueden ser llevados al límite causando irregularidades en el servicio que prestan.

También se podría alterar la información de las tablas de enrutamiento con el fin de volver inalcanzable un destino prestador de algún servicio crítico.

Se podría también obstruir los medios físicos de comunicación entre los clientes y los servidores con objeto de cortar la comunicación.

Inundación SYN.- Cuando un cliente desea establecer conexión con un servidor, envía un paquete TCP/SYN, si el servidor acepta la solicitud responderá con un TCP/SYN-ACK y finalmente el cliente responderá con un TCP/ACK (Establecimiento de una conexión TCP de 3 vías). Dada la naturaleza de este proceso, un atacante podría enviar múltiples paquetes TCP/SYN, generalmente con la dirección ip origen falsificada, provocando que el servidor intente iniciar una comunicación respondiendo con un paquete TCP/SYN-ACK a cada solicitud recibida y dado que las direcciones ip origen no existen o bien nunca solicitaron la conexión, la respuesta TCP/ACK jamás será recibida por el servidor. Estos intentos de iniciar una comunicación consumen recursos del servidor y alcanzan el límite de conexiones que se puede establecer disminuyendo así la capacidad del servidor para responder solicitudes de conexión legítimas.

Inundación ICMP.- Esta técnica tiene como objetivo saturar el ancho de banda del sistema víctima enviando de forma continua una gran cantidad de paquetes de tipo ICMP, echo request, los cuales serán respondidos con una gran cantidad de paquetes echo reply. Si el atacante cuenta con un ancho de banda mayor que la víctima, podría fácilmente generar una cantidad de tráfico mayor de lo que la víctima puede manejar. Una variante del ataque ICMP flood es el ataque SMURF, el cual amplifica considerablemente los efectos del ataque ICMP flood. En éste ataque, se envían paquetes ICMP, echo request a una dirección de broadcast usando como origen la dirección ip de la víctima. De éste modo todos los equipos conectados en la red responderán con paquetes echo reply al sistema víctima pudiendo llegar a saturar su ancho de banda. Éste tipo de ataque puede llegar a afectar también a los sistemas intermediarios, es decir a los sistemas que responderán con un echo reply al sistema víctima. [6]

2.5. Ataque de Falseo de Rutas

Este tipo de ataque consiste en el envío de falsas actualizaciones de enrutamiento de tal modo que la tabla de encaminamiento de los enrutadores se vea modificada, dirigiendo el tráfico hacia un destino erróneo, por lo general este destino es el atacante quien desea ésta información en su poder con fines maliciosos. Existen varias herramientas que nos permiten llevar a cabo éste ataque, una de ellas es el software Quagga.

Un atacante astuto podría determinar cuál es el segmento de red donde se aloja un servidor en particular haciendo uso de algún sniffer o alguna otra herramienta de detección de hosts en una red.

Una vez determinado este segmento de red, se puede hacer uso de Quagga para que envíe actualizaciones con una métrica menor hacia el segmento de red que queremos suplantar, de este modo se modificarían las tablas de encaminamiento de los dispositivos de capa 3 haciendo que éstos envíen el tráfico hacia el atacante.

3. Pruebas realizadas sobre OSPFv3 y RIPng

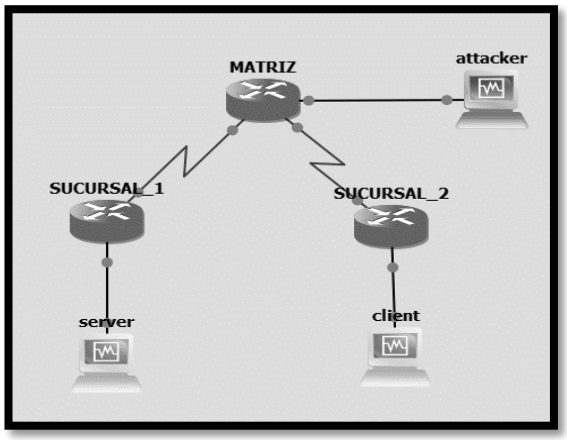

Figura 3. Esquema de red utilizado para ambos protocolos

3.1. Prueba de Disponibilidad

La prueba de disponibilidad consistió en medir el tiempo que le tomó a un archivo estándar de 1MB transmitirse desde el servidor hacia el cliente haciendo uso del protocolo FTP, adicionalmente se calculó la tasa de transferencia de datos.

Primero se midió la respuesta del protocolo en condiciones normales, es decir sin ningún ataque de red ejecutándose. Luego se midió la respuesta del protocolo bajo el efecto del ataque router-advertisements flood el cual se llevó a cabo desde el atacante con la herramienta Flood_router6 que se encuentra dentro de la Suite de herramientas thc-ipv6.

Como última prueba de disponibilidad se midió el tiempo de convergencia de la VPN luego de recuperarse de una baja de la interfaz física del router.

El número de mediciones realizadas fue 47 de acuerdo a la fórmula del número mínimo de observaciones en investigación:

$$n = \frac{(W - W^2)\,[Z_\beta + 1.4\,(Z_\alpha)]^2}{W^2} \quad (1)$$

Los valores usados fueron los siguientes:

- Z_α (Nivel de confianza) = 2.576 (99%)
- W (Diferencia mínimo observable) = 0.3 (30%)

- Z_β (Poder estadístico) = 0.842 (80%)

3.2. Pruebas de Confidencialidad e Integridad

Para las pruebas de confidencialidad e integridad hicimos uso del servicio web proporcionado por APACHE, que se encuentra dentro de WAMP en la máquina del servidor.

En el atacante usamos Quagga para habilitar el enrutamiento OSPFv3 y RIPng dependiendo del caso. Configuramos Quagga de tal modo que se enviaron actualizaciones de enrutamiento hacia la puerta de enlace del atacante indicándole que posee una mejor ruta (menor métrica) hacia la red del servidor. De éste modo el atacante pudo recibir información transmitida desde el cliente cuyo destino legítimo era el servidor violando así la confidencialidad de la información.

Luego realizamos los mismos pasos pero ésta vez teniendo habilitado un túnel VPN-IPSec entre la puerta de enlace del servidor y la del cliente.

Una vez obtenida la información del cliente (SIN VPN SOLAMENTE) configuramos Quagga para que le indique a la puerta de enlace que tiene una mejor ruta hacia la red del cliente y así poder enviar información alterada desde el atacante hacia el servidor como si fuese el cliente legítimo, de éste modo se llevó a cabo la prueba de integridad de la información. Para poder cuantificar ésta prueba, se midió el tiempo que nos llevó pasar de engañar al cliente a engañar al servidor pues debe ser un tiempo muy corto para que el usuario no perciba la transición y se dé cuenta que "algo no anda bien".

En primera instancia, se consideró la configuración manual de los archivos de Quagga así como el cambio de IP dentro del host atacante para poder pasar de engañar al cliente a engañar al servidor pero esto demandaba de varias acciones que en conjunto tomaban de 2 a 4 minutos aproximadamente, lo que resultó ineficiente para un ataque de este tipo. Para solucionar este inconveniente, se automatizó este proceso haciendo uso de scripts y así poder efectuar el ataque en un menor tiempo (aproximadamente 40 segundos).

Para una mayor precisión en cuanto a la medición de este tiempo, se tomó en cuenta los mensajes debug de los enrutadores.

4. Resultados

4.1. Disponibilidad – OSPFv3 vs RIPng

Tabla 1. Tiempo y velocidad de transmisión condiciones normales

TIEMPO DE TRANSMISION [s]	**OSPFv3**	**RIPNG**
Media	7,925	8,05
Desviación estándar	0,179	0,291
Varianza	0,0323	0,0847
Mínimo	7,675	7,608
Máximo	8,412	9,205
VELOCIDAD DE TRANSMISION [Kb/s]	**OSPFv3**	**RIPNG**
Media	123,20	121,762
Desviación estándar	2,75	4,22
Varianza	7,59	17,81
Mínimo	116,02	106,03
Máximo	127,17	128,29

Tabla 2. Tiempo y velocidad de transmisión bajo ataque flood

TIEMPO DE TRANSMISION [s]	**OSPFv3**	**RIPNG**
Media	107,28	133,20
Desviación estándar	35,780	29,51
Varianza	1280,220	870,69
Mínimo	44,072	72,26
Máximo	177,41	195,39
VELOCIDAD DE TRANSMISION [Kb/s]	**OSPFv3**	**RIPNG**
Media	10,251	7,728
Desviación estándar	3,733	2,093
Varianza	13,936	4,382
Mínimo	5,501	4,995
Máximo	22,146	13,506

Tabla 3. Tiempo de convergencia de la VPN

TIEMPO DE CONVERGENCIA [s]	**OSPFv3**	**RIPNG**
Media	24,865	17,817
Desviación estándar	6,546	4,468
Varianza	42,851	19,967
Mínimo	14,480	10,192
Máximo	44,200	31,824

4.2. Confidencialidad – OSPFv3 vs RIPng

Tabla 4. Porcentaje de información recibida por el atacante y el servidor con VPN y sin VPN

CON VPN	OSPFv3	RIPNG
Porcentaje recibido por el ATACANTE	0%	0%
Porcentaje recibido por el SERVIDOR	100%	100%
SIN VPN	**OSPFv3**	**RIPNG**
Porcentaje recibido por el ATACANTE	100%	100%
Porcentaje recibido por el SERVIDOR	0%	0%

4.3. Integridad – OSPFv3 vs RIPng

Tabla 5. Tiempo requerido para efectuar un ataque de integridad y porcentaje de información modificada

TIEMPO [s]	OSPFv3	RIPNG
Media	10,042	11,717
Desviación estándar	0,0408	2,656
Varianza	0,001	7,052
Mínimo	10	16,245
Máximo	10,187	11,287
PORCENTAJE DE INFORMACIÓN MODIFICADA	100%	100%

5. Conclusiones y Recomendaciones

1. En la prueba de disponibilidad pudimos observar que el protocolo RIPng se vio más afectado por el ataque DOS, teniendo un tiempo 24,16% mayor al que obtuvimos con el tiempo de transmisión con OSPFv3, así mismo la velocidad de transmisión disminuyó en el mismo porcentaje. En consecuencia, podemos concluir que OSPFv3 resulta ser más resistente a los ataques DOS.

2. En cuanto a la prueba de confidencialidad, el empate entre los dos protocolos es evidente y también lo es la manera en que la tecnología de seguridad implementada, en este caso la VPN, es efectiva para contrarrestar este tipo de ataque en ambos protocolos.

3. Para la prueba de integridad se pudo modificar y hacer llegar la misma cantidad de información al servidor. Para el tiempo de conmutación se obtuvieron resultados similares en ambos protocolos una vez enviadas las falsas actualizaciones de enrutamiento. Los resultados de RIPng variaron un poco más que los de OSPFv3 y en el peor de los casos tuvieron un tiempo de convergencia un poco mayor siendo esto un beneficio para la seguridad pues un posible atacante tardaría más en llevar a cabo un ataque de este tipo.

4. Finalmente declaramos ganador al protocolo OSPFv3 pero con ventaja mínima pues en las dos últimas pruebas hubo un empate en cuanto a los resultados, mientras que, en las pruebas de disponibilidad, se pudo notar que OSPFv3 ofreció una mejor respuesta frente a ataques de este tipo.

5. Se recomienda realizar futuros análisis comparativos con otros protocolos de enrutamiento IPv6 como son IS-IS y EIGRPv3, con el fin de mostrar ventajas o desventajas que puedan presentar estos protocolos en términos de seguridad.

6. Se recomienda efectuar las pruebas considerando una red de mayor tamaño y otros servicios de red para poder ampliar los resultados ya obtenidos.

7. Se recomienda efectuar las pruebas implementando otros posibles sistemas de seguridad de redes informáticas para observar la respuesta de los protocolos.

6. Referencias

[1] Coltun R., Ferguson D., Moy J., Lindem A., *OSPF for IPV6*, https://tools.ietf.org/html/rfc5340, Julio de 2008.

[2] Francisconi H., *IPsec en Ambientes IPv4 e IPv6*, Agosto de 2005.

[3] Malkin G., Minnear R., *RIPng for IPv6*, https://www.ietf.org/rfc/rfc2080.txt, Enero de 1997.

[4] Wikipedia.com, *Seguridad de la Información*, http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n.

[5] García J., *Ataques en redes de datos IPv4 e IPv6*, 2012.

[6] Castro M., Díaz G., Alzórriz I., Sancristóbal E., *Procesos y herramientas para la seguridad de redes*, 2013.