SERVIDOR VIRTUAL PARA DETECCIÓN DE INTRUSOS Y ATAQUES EN IPV6

D. E. Oneddú[(a)]; E. Zamudio[(b)]; N. B. Ganz[(b)]; M. J. Marinelli[(c)]
(a) Facultad de Ciencias Exactas, Químicas y Naturales; Universidad Nacional de Misiones.
(b) Instituto de Materiales de Misiones; CONICET; Facultad de Ciencias Exactas, Químicas y Naturales; Universidad Nacional de Misiones.
(c) Departamento de Informática; Facultad de Ciencias Exactas, Químicas y Naturales; Universidad Nacional de Misiones.
oneddu@gmail.com

RESUMEN

La migración de IPv4 a IPv6 ha adquirido una importancia muy significativa, la cual cada día preocupa más a los proveedores de Internet, ya que no es posible simplemente dejar de utilizar el protocolo viejo y comenzar a usar el nuevo. Para solventar ésta necesidad de continuidad de negocio, surgen las llamadas técnicas o mecanismos de transición o coexistencia. Estas técnicas permiten la incorporación gradual de IPv6 dentro de una infraestructura IPv4 existente, ya que ambos protocolos no son compatibles por naturaleza.
La seguridad de IPv4 e Ipv6 son totalmente independientes, por lo que se necesita establecer medidas para detectar, identificar, prevenir y tomar una decisión correcta frente a posibles ataques en ambos protocolos. Esto es una realidad que todos los usuarios de internet deben enfrentar en la actualidad y en particular los administradores de red.
El objetivo de esta línea de investigación es detectar de manera oportuna y a tiempo intrusos y/o ataques en un segmento de red IPv6 de una infraestructura en particular. Asimismo, se abordará puntualmente el IPv6, sus principales problemas al implementarlo y sus diferentes tipos de necesidades para configurarlo de manera segura.
Palabras Claves: IPv6, IDS, Servidor Virtual

CONTEXTO

Esta línea de investigación se lleva a cabo en el marco de una propuesta de Tesis de la Maestría en Tecnologías de la Información, de la Facultad de Ciencias Exactas, Químicas y Naturales (FCEQyN), de la Universidad Nacional de Misiones (UNaM). Se proyecta este trabajo de investigación debido a la necesidad e importancia que tiene la ciberseguridad de IPv6 a nivel mundial, lo que nos motivó a investigar soluciones regionales o específicas para las diferentes unidades académicas de la universidad. Se consultó con los referentes informáticos de otras universidades nacionales tomando conocimiento de que si bien ocupan la tecnología IPv6, no tienen la necesidad de preocuparse por la configuración de su seguridad.

1. INTRODUCCIÓN

El agotamiento casi total de las direcciones IPv4 públicas en el 2011, llevó a grandes empresas a nivel mundial a participar del Día de IPv6 [1] en donde se puso a prueba si los servicios continuarían corriendo en dicho protocolo.
El IPv6 definido hace casi 20 años en el RFC 2460 de Diciembre de 1998 [2] prometía ser la solución al agotamiento de las direcciones publicas IPv4. Sin embargo, con el uso masivo actual que está generando IPv6, surgen ciertos inconvenientes no contemplados en la teoría y que son un verdadero problema al momento de utilizar este protocolo. Se podría enumerar algunos problemas de actual importancia en estos días:
En primer lugar, el problema más grande es que todavía se atraviesa la etapa de transición entre ambos protocolos. Esto implica, estar atados al uso ininterrumpido de IPv4 mientras se intenta evolucionar a IPv6. Lo cual infiere

una inversión económica y financiera importante, que en la mayoría de los países de Latinoamérica son muy difíciles de afrontar. Siendo necesario mantener equipos hardware y software funcionando en simultáneo con ambos protocolos. En el caso de los proveedores más importantes a nivel mundial, solamente los equipos de alta gama, es decir, los más costosos tienen la capacidad de realizar NAT64 [3]. En otras palabras, efectuar la traducción de un protocolo a otro. Razón por la cual es necesario un trabajo artesanal, para mantener funcionando satisfactoriamente toda la infraestructura de red y servidores en una organización, como lo es una Universidad Pública Nacional.

En segundo lugar, otro problema es que si bien IPv6 tiene la capacidad de identificar cada MAC address de cada dispositivo unívocamente a nivel mundial mediante la norma EUI64 [4], no existen suficientes Servidores DNS que resuelvan estas IP, o cada organización debe poseer su propio Servidor DNS; y provoca que una vez detectado el IP de un servidor, router o cualquier dispositivo critico de una organización, éste sea propenso a ataques de nivel mundial.

En tercer lugar, otro problema es que IPsec definido dentro de la misma cabecera IPv6 no cumple satisfactoriamente su función de seguridad impenetrable. Además, al utilizar Stateless address autoconfiguration (SLAAC)[1] los sistemas operativos como Windows y Mac OS X, preferirán usar IPv6 en una red siempre que sea posible, lo que hereda el problema descripto en el punto anterior. IPv6 está ideado para autoconfigurarse por completo, por lo tanto, un atacante podría configurar un router fraudulento y obtener automáticamente información de la red de una organización en particular, cuyos usuarios comenzarán a usar su servidor DNS falso.

Es importante destacar que actualmente las diferentes configuraciones hechas en IPv6 no contemplan adecuadamente diferentes tipos y niveles para la seguridad y protección ante ataques de DoS[2] y DDoS[3] con lo cual es importante, además de tener un buen firewall correctamente configurado, algún sistema de detección de intrusos y posteriormente también un sistema de prevención de intrusos.

En este trabajo de investigación se propone desarrollar una alternativa para abordar algunos aspectos de los problemas descriptos, mediante la detección de intrusos y ataques, en el ámbito de redes de datos institucionales como lo son las redes de las Universidades Públicas de la República Argentina. Implicaría la utilización de los equipos ya existentes. Sin tener que adquirir equipamiento nuevo y costoso, como sería la solución de los grandes proveedores. Esta solución no debe afectar al desempeño normal de los equipos ni comprometer su seguridad. Será necesario para esto la configuración de un servidor virtual que detecte ataques en IPv6 mediante un sistema de detección de intrusos (IDS); y que debe trabajar en conjunto con un router de borde IPv6-Only que no interfiera con la arquitectura actual de la red institucional IPv4-Only en producción.

En ningún momento y bajo ninguna circunstancia se tomará la información contenida en el área de datos de los paquetes, en primer lugar por considerarse irrelevante

[1] Autoconfiguración de dirección sin estado es un método en el que a la interfaz del host o enrutador se le asigna un prefijo de 64 bits, y los últimos 64 bits de su dirección son derivados por el host o enrutador con la ayuda del proceso EUI-64 que se describe en las siguientes líneas. SLAAC usa el protocolo NDP para funcionar.

[2] Denegación de Servicio (DoS) es una interrupción en el acceso de un usuario autorizado a una red informática, generalmente una causada con intención maliciosa

[3] Un ataque de denegación de servicio distribuido (DDoS) es un intento de hacer que un servicio en línea no esté disponible al abrumarlo con tráfico de múltiples fuentes. Apuntan a una gran variedad de recursos importantes, presentan un gran desafío para asegurarse de que las personas puedan publicar y acceder a información importante.

para esta investigación, y en segundo lugar por cuestiones de la ley de Protección de Datos Personales[4].

Con lo referente a la legislación, la asignación de dirección IPv6 y las regulaciones que poseen, la Universidad Nacional de Misiones ya tiene su pool de direcciones IPv6 asignados por LACNIC, del cual cada unidad académica cuenta con una porción de dicho pool para uso según sea necesario [5]–[7].

Todas las pruebas en la red de la unidad académica se realizarán sin sugestionar a los usuarios finales de dicha red, es decir, no dar aviso que se está implementando un nueva tecnología, o seguridad de protocolo nuevo en este caso; de esa manera se podrá evaluar la transparencia que tiene el estudio y la notificación que tienen los usuarios con respecto al uso cotidiano de la red. Por otra parte, una vez que esté todo configurado y funcionando, se harán simulaciones de ataques programados y aleatorios, con lo cual se solicitará la ayuda y participación de algunos administradores de red de otras unidades académicas; con el objetivo de obtener retroalimentación, sugerencias y optimización de configuraciones en el estudio de caso.

Toda la investigación será abordad en relación al modelo OSI y no al TCP/IP, es decir siempre que se mencione los niveles o capas será tenido en cuenta en relación al Modelo OSI, a continuación se expone en la siguiente imagen una comparación entre ambos modelos para su mejor comprensión.

Figura 1: Comparación del Modelo OSI y TCP/IP

[8], [9]

Lo admirable de IPv6 es su encabezado, una dirección IPv6 es 4 veces más grande que una IPv4, pero sorprendentemente, el encabezado de una dirección IPv6 es solo 2 veces más grande que el de IPv4. Los encabezados IPv6 tienen un encabezado fijo y cero o más encabezados opcionales (extensión). Toda la información necesaria que es esencial para un enrutador se guarda en el Encabezado fijo. El encabezado de extensión contiene información opcional que ayuda a los enrutadores a entender cómo manejar un paquete / flujo. En la Figura 2 se puede apreciar la estructura del encabezado IPv6.

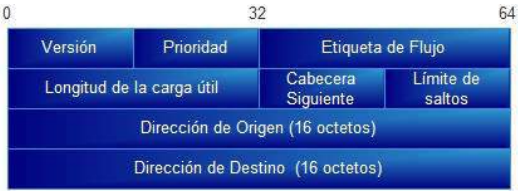

Figura 2: Cabecera IPv6

[8], [9]

Como hemos mencionado anteriormente, la UNaM posee su propio pool de direcciones IPv6 asignado por LACNIC, este pool se segmenta para el uso de las diferentes unidades académicas de dicha universidad. En la siguiente imagen se aprecia el enmascaramiento IPv6 de la UNaM.

[4] Ley 25.326: Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.
Sancionada: Octubre 4 de 2000.
Promulgada Parcialmente: Octubre 30 de 2000.

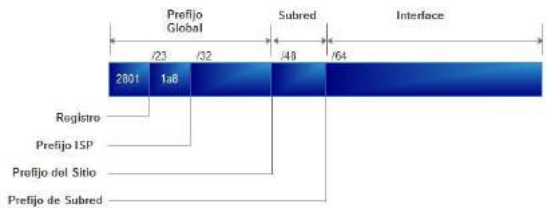

Figura 3: Máscaras IPv6

[10]

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Este trabajo tiene como principal línea de investigación el tratamiento de la seguridad en el contexto de redes IPv6 mediante la virtualización de servidores en datacenter en Universidades Nacionales. Instalando y configurando servicios de detección de intrusos y ataques; así como también la utilización de Maquetas para la enseñanza de ciberseguridad en redes y comunicaciones. También se podrá anexar o incorporar placas SBC como dispositivo router, bridge, firewall, switching, etc. con el mismo fin pedagógico.

3. RESULTADOS ESPERADOS

Se pretende obtener un servidor virtual correctamente configurado con las necesidades básicas para la detección de intrusos y ataques en IPv6, totalmente migrable y exportable a otras instituciones o unidades académicas de las diferentes universidades nacionales. Un producto software multiplataforma totalmente independiente de la infraestructura a la cual se quiere aplicar.

Con respecto a las enseñanzas de redes y comunicaciones se pretende desarrollar maquetas para diferentes trabajos practicos que ayuden a los alumnos a compreder el complejo mundo de las comunicaciones y conocer cuales son los elementos a tener en cuenta en la utilización de ciberseguridad

4. FORMACIÓN DE RECURSOS HUMANOS

Este proyecto es parte de un plan de tesis de maestría en Tecnologías de la Información, en el cual se prevén incorporar becarios, tesistas, ayudantes de cátedra para Sistemas Operativos, Comunicación y Redes I y Comunicación y Redes II de las Carreras de Analista en Sistemas de Computación, Licenciatura en Sistemas de Información y Profesorado Universitario en Computación, de la Facultad de Ciencias Exactas, Químicas y Naturales (FCEQyN), de la Universidad Nacional de Misiones (UNaM).

5. BIBLIOGRAFÍA

[1] Ole J. Jacobsen, “The Internet Protocol Journal,” *Cisco Syst.*, vol. 171, no. 5, p. A20, 2011.

[2] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” *RFC 2460*, 1998. [Online]. Available: https://www.ietf.org/rfc/rfc2460.txt. [Accessed: 10-Jul-2017].

[3] G. Tsirtsis and P. Srisuresh, “Network Address Translation - Protocol Translation (NAT-PT),” *RFC 2766*, 2000. [Online]. Available: https://www.ietf.org/rfc/rfc2766.txt. [Accessed: 07-Feb-2016].

[4] J. Abley, “Resource Records for EUI-48 and EUI-64 Addresses in the DNS,” *RFC 7043*, 2013. [Online]. Available: https://tools.ietf.org/html/rfc7043. [Accessed: 13-Jul-2017].

[5] “IPv6 Subredes y DNS UNaM,” 2016. [Online]. Available: http://www.tcpiputils.com/browse/ipv6-address/2801:1a8::-2801:1a8:ff:ffff:ffff:ffff:ffff:ffff. [Accessed: 06-Feb-2016].

[6] IANA, “IPv6 Global Unicast Address Assignments,” 2016. [Online]. Available: http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml. [Accessed: 05-Feb-2016].

[7] "Asociación Redes de Interconexión Univeristaria." [Online]. Available: http://www.riu.edu.ar/topologia.html. [Accessed: 27-Feb-2016].

[8] A. S. Tanenbaum, *Redes de computadoras*. Pearson Educación, 2003.

[9] W. Stallings, *Comunicaciones y Redes de Computadores*, Séptima Ed. Pearson Educación, 2004.

[10] R. Graziani, "CiscoPress - IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6," *IPv6 Fundam.*, p. 456, 2013.