FRAMEWORK EN ESTRUCTURAS CON DIRECCIONAMIENTO IPv6 SOBRE OSSTMM PARA LA CORRECCIÓN DE VULNERABILIDADES DE SEGURIDAD

(Entregado 27/07/2017 – Revisado 27/07/2017)

Calos José Martínez Santander (Universidad Católica de Cuenca) carlos4553@hotmail.com; Yolanda de la Nube Cruz Gavilánez (Empresa de telecomunicaciones CGXS ingenieros) nube5502@gmail.com

Resumen

El presente artículo puntualiza los pasos que se siguen a través de una metodología en la búsqueda y corrección de vulnerabilidades de seguridad en él. Con la Metodología OSSTMM se ejecutó el análisis de Vulnerabilidades en infraestructuras con direccionamiento IPv6 detallando las fases que se siguieron para mitigar las intrusiones que presenta el protocolo IPv6 por medio de la red:

- *Análisis y Evaluación de Riesgos en Infraestructuras con Direccionamiento IPv6, como riesgos Tecnológicos, Riesgos Económicos y Riesgos de seguridad de la información.*
- *Identificación y Búsqueda de Vulnerabilidades IPV6 con las que se obtiene el descubrimiento de direcciones IPv6, Detección de Servidores IPv6, Escaneo de puertos y servicios que corren en la infraestructura IPv6, Ataques IPv6 y Explotación*

Informe del Análisis, Valoración y posible tratamiento de riesgos sobre las vulnerabilidades encontradas en infraestructuras IPv6

Palabras claves: *vulnerabilidad, seguridad, prueba, protocolo de internet versión 6 [ipv6], manual de la metodología abierta de comprobación de la seguridad [osstmm], academia de redes locales [cisco]*

Abstract

This article points out the steps taken through a methodology for finding and fixing. Security, vulnerabilities.

With OSSTMM Methodology Vulnerability analysis, it wasrun on IPv6 routing infrastructure with detailing the steps to be followed to mitigate intrusions presented by the IPv6.protocol.by.the.network:

- *Analysis and Risk Assessment Infrastructure with IPv6 addressing, as Technological Risks, Economic Risks and Risks of information security.*

- *Identification and Vulnerability Search IPV6 with the discovery of IPv6, IPv6 server discovery, scanning ports and services running on the IPv6 infrastructure IPv6 Attacks Operation.and.get.directions.*

- *Analysis Report, evaluation and possible treatment of risks vulnerabilities found in IPv6 infrastructure*

***Keywords**: vulneravility, security, test, prococol internet version 6 [ipv6], the open source security testing methodology manual [osstmm], local networking academy [cisco]*

1. Introducción

Según Herzog (2010) definió una metodología OSSTMM para mejorar la seguridad, que están dirigidas a la implantación de culturas de seguridad de la información facilitando los conceptos y las políticas de seguridad en los procesos de empresas, instituciones públicas y privadas y su interrelación con el recurso humano.

En el contexto internacional la metodología OSSTMM es estandarizada para las buenas prácticas de seguridad a través de canales, ámbitos, Módulos, fases y secciones para implantación de un sistema de seguridad de información, (Franco, D &. Guerrero, C, 2013) la estructura de la metodología abierta de seguridad se presenta a continuación en la tabla1

Tabla 1 Canales y secciones de OSSTMM

CANAL	SECCION	DESCRIPCION
Seguridad Física	Humano	Elemento Humano
	Físico	Todo Objeto Tangible
Seguridad de las comunicaciones	Redes de Datos	Sistemas electrónicos y redes de datos
	Telecomunicaciones	Comunicaciones digitales o analógicas
Seguridad del espectro electromagnético	Comunicaciones inalámbricas	Incluyen las señales electromagnéticas

Fuente: (Aldo Valdez Alvarado, 2013)

En la tabla precedente muestra los canales y secciones que están sujetos a estudio de la metodología OSSTMM para garantizar la seguridad de una organización.

Se conocen trabajos relacionados con OSSTMM como lo es de (Pinzón, A, Talero & Bohada, J, 2014) en la que presenta aspectos como el de realizar pruebas de constantes de

intrusión en cada uno de los elementos que componen la arquitectura utilizando la metodología OSSTMM.

En el contexto regional y nacional, existen pocos estudios que se relacionan con el tema, de la búsqueda y corrección de vulnerabilidades con OSSTMM a través de la red, es así que se ha evidenciado en un más del 50% de empresas, instituciones no cuentan con políticas de seguridad de manera formal.

Se han realizado investigaciones sobre seguridad informática,(La Flecha Diario de Ciencia y Tecnología, 2008) revelando que existe un aumento de actividades ilícitas por parte de personas que a través ataques cibernéticos engañan otras ya sea mediante la publicación de sitios web maliciosos, falsificaciones de empresas legítimas, campañas de spam, etc.

La nueva tecnología que surgió debido al agotamiento de las direcciones IPV4, es el direccionamiento IPV6, misma que al ser nueva tecnología, trae consigo muchos problemas de seguridad igual a los de IPV4 o nuevos problemas que aparecerán ya con el uso en las estructuras de las entidades que son blancos de los hackers.

2. Materiales y métodos

OSSTMM es un manual para análisis, pruebas de seguridad informática, Esta metodología se divide en cuatro (4) Canales que son la seguridad Física, seguridad de las comunicaciones y seguridad del espectro electromagnético y a su vez se subdivide en cinco secciones que es el humano, físico, redes inalámbricas, telecomunicaciones y redes de datos (Herzog, P, 2010).

Este estudio se centró en las redes de datos específica las cuatro (4) fases que está constituida y esta a su vez por dieciséis (16) módulos que tienen sus correspondientes tareas y procedimientos de acuerdo al canal que está siendo evaluado (López, A 2011).

El framework será una herramienta básica a la hora de detectar y corregir errores en cualquier arquitectura que maneje el protocolo IPv6 y mostrara eficiencia y eficacia en el momento que detecte ataques a través de la red, utiliza la metodología OSSTMM que es un método para el análisis, pruebas de seguridad informática, comenzando por la fase de inducción observando los requisitos, alce y limitación de la auditoria, fase de interacción que ve el alcance de las aplicaciones transmitidas, fase de investigación confirma información que el analista descubre termina con la fase de intervención se centrara en los recursos que se valida a los sistemas.

De acuerdo a la metodología se:

Análisis y Evaluación de Riesgos en Infraestructuras con Direccionamiento IPv6.

Se evaluó los riesgos tecnológicos, económicos y riesgos de seguridad de la información, con este análisis puedo saber el tiempo adecuado en el cual puedo realizar un test de seguridad, los equipos hardware y software que se pueden comprometer en el test y por ende su mal funcionamiento que representara pérdidas para la empresa institución, etc.

Identificación y Búsqueda de Vulnerabilidades IPV6.

Como se sabe para un test de intrusión se sigue las siguientes fases:

- Reconocimiento
- Escaneo
- Obtener acceso
- Borrar huellas.

Esta metodología permite de una manera fácil y sin demora, ejecutar todos los pasos de un test de intrusión y recopilar la información necesaria respecto a vulnerabilidades que están presentes en la infraestructura IPv6.

Informe del Análisis, Valoración y posible tratamiento de riesgos sobre las vulnerabilidades encontradas en infraestructuras IPv6.

Las Vulnerabilidades que sean encontradas serán analizadas en primer lugar según su tiempo de aparición es decir si ya hay un parche de seguridad o es Zero-day podrán ser catalogadas como (high - medium - low) y su potencial para causar o comprometer la información en: Confidencialidad – Disponibilidad – Integridad).

3. Resultados y discusión

La tabla 4 muestra cada uno de los ataques que se realizaron en la arquitectura del laboratorio de cisco de la ESPOCH criterio de seguridad el cual fue afectado como puede ser mitigado y su valoración

Tabla 2. Informe de vulnerabilidades

Ataque realizado	Criterio de seguridad afectado	Herramienta utilizada	Mitigación	Valoración
Descubrimiento de direcciones locales ipv6 mediante búsqueda en segmentos de red ipv4	Confidencialidad	atk6-alive6 -4 192.168.1.0/24 eth0	Debido al funcionamiento de Ipv6 mediante el envío de tráfico a direcciones de multicast, al momento no se puede mitigar el ataque	Low
Detección de nuevas direcciones IP	Confidencialidad	atk6-detect-new-ip6 eth0	Para protegerse ante este ataque se ha definido un mecanismo llamado SEND (Secure Neighbor Discovery) que proporciona seguridad a los mensajes NDP	Low
Detección de servidores de DHCPv6	Confidencialidad	atk6-dump_dhcp6 eth0	Debido a que los paquetes Offer de DHCPv6 se envían en texto plano, al momento no es posible mitigar el ataque	Medium
Detección de routers	Confidencialidad	atk6-dump_router6 eth0	Para evitar ser víctima de este ataque se recomienda bloquear el descubrimiento de routers en su configuración con <<routerdiscovery=”disabled”	Medium
Escaneo de Puertos	Confidencialidad	nmap -6 2001:db8:1:40::3 --open -O	A fin de mitigar un posible ataque de escaneo de puertos, se deberá realizar la implementación de listas de control de acceso a nivel de soluciones de filtrado de paquetes en capa 4	Medium
Ataque de Fragmentación de Paquetes	Disponibilidad	atk6-fragmentation6 eth0 2001:db8:1:10::2	A fin de mitigar un posible ataque de fragmentación, se deberá realizar la implementación de listas de control de acceso a nivel de	Medium

Ataque realizado	Criterio de seguridad afectado	Herramienta utilizada	Mitigación	Valoración
			soluciones de filtrado de paquetes en capa 4	
Ataque ICMPv6 Smurf	Disponibilidad	atk6-smurf6 eth0 2001:db8:1:40::2	Debido al funcionamiento de Ipv6 mediante el envío de tráfico a direcciones de multicast, al momento no se puede mitigar el ataque	High
Denegación de Servicio hibrido dirigido hacia los routers	Disponibilidad	atk6-denial6 eth0 2001:db8:1:40::21	Con las soluciones anteriores sobre estos protocolos es posible mitigar estos ataques.	High
Denegación de Servicio hibrido hacia la victima	Disponibilidad	atk6-denial6 eth0 2001:db8:1:40::22	Con las soluciones anteriores sobre estos protocolos es posible mitigar estos ataques.	High
Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::21	Debido al funcionamiento de Ipv6 mediante el envío de tráfico a direcciones de multicast, al momento no se puede mitigar el ataque	Medium
Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::22	Debido al funcionamiento de Ipv6 mediante el envío de tráfico a direcciones de multicast, al momento no se puede mitigar el ataque	Medium
Explotación de vulnerabilidades en IPv6	Disponibilidad	atk6-exploit6 eth0 2001:db8:1:40::23	Los equipos Cisco disponen de actualizaciones que corrigen esta vulnerabilidad.	Medium
Denegación de servicio global	Disponibilidad	atk6-flood_router26 eth0	A fin de evitar una denegación de servicio a nivel global, se deberá realizar la implementación de listas de control de acceso a nivel de soluciones de filtrado de paquetes en capa 4	High
Análisis de Vulnerabilidades	Integridad, Confidencialidad, Disponibilidad	Nessus	Para evitar un escaneo de vulnerabilidades, se deberá realizar la implementación de listas de control de acceso a nivel de soluciones de filtrado de paquetes en capa 4. Además se deberá realizar la implementación de soluciones anti-malware, así como realizar una correcta	High

Ataque realizado	Criterio de seguridad afectado	Herramienta utilizada	Mitigación	Valoración
			actualización de los sistemas operativos de los activos de información	
Generación de Payloads mediante tunneling IPv6	Integridad, Confidencialidad, Disponibilidad	msfvenom	A fin de evitar una infección a través de payloads, es necesaria la implementación de soluciones IPS, los cuales detecten y cierren las posibles conexiones de las víctimas con su respectivo CCC. Además se deberá contar con soluciones antimalware, las cuales posean sus firmas de datos actualizadas.	High
Ataques Client Side	Integridad, Confidencialidad, Disponibilidad	Metasploit	A fin de evitar una infección a través de payloads, es necesaria la implementación de soluciones IPS, los cuales detecten y cierren las posibles conexiones de las víctimas con su respectivo CCC. Además se deberá contar con soluciones antimalware, las cuales posean sus firmas de datos actualizadas.	High
Ataques de Intercepción de tráfico	Integridad, Confidencialidad, Disponibilidad	atk6-parasite6 eth0	Para evitar este ataque se puede usar el bloquear el descubrimiento de routers especificado en un anterior punto.	High

REALIZADO POR: MARTINEZ, CARLOS, 2015

4. Conclusiones

- Efectivamente el desarrollar un Framework conlleva a un análisis rápido y veras de una infraestructura con direccionamiento IPv6, permitiendo conocer cuáles son las vulnerabilidades existentes en la infraestructura.
- Cuando se hace un análisis de Vulnerabilidades es menester tener una metodología sistemática a seguir para que los resultados de la misma sean óptimos.
- Es importante profundizar el conocimiento en lo que a IPv6 ya que existen vulnerabilidades que a pesar de que su año de aparición fue ya distante del que vivimos, aun no se mitiga esa vulnerabilidad o se difunde un parche de seguridad.

- Se ha concluido que a pesar de encontrar las vulnerabilidades en la infraestructura, algunas en IPv6 al momento no tienen una corrección del error que la causa es decir no pueden ser mitigadas

5. Referencias bibliográficas:

- López, A. (2011, diciembre). *«Estudio de metodologías para pruebas de penetración a sistemas informáticos»*. Instituto Politécnico Nacional, México.
- Valdez A. (2013). *Revista de Información, Tecnología y Sociedad* - OSSTMM 3.
- Franco, & Guerrero, C. (2013). *Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC* 27002, 10.
- La Flecha Diario de Ciencia y Tecnologia. (2008, mayo 8). *"Los 10 principales errores de seguridad TI que cometen los departamentos informáticos en las Pymes"*.
- Pinzon, L. C,Talero, M & Bohada, J. (2014). *Pruebas de Intrusión y Metodologías Abiertas. Ciencia, Innovación y Tecnología,* 1(0), 25-38.
- Valdez, A. (2013*). Revista de Información, Tecnología y Sociedad* - OSSTMM 3.
- Universidad Tecnologia Nacional (2002, junio 26). *Seguridad Informatica*.
- Castan,A. (2007, Agosto 15). *Análisis activo y pasivo de redes - analisispa*.
- Choudhary, A. R., & Sekelsky, A. (2010). *Securing IPv6 network infrastructure: A new security model*. En 2010 IEEE International Conference on Technologies for
- Homeland Security (HST) (pp. 500-506). Coello Salas, M. (2013, febrero 7). *Procedimiento formal de Ethical Hacking para la infraestructura tecnológica de los servicios por internet de la banca ecuatoriana*. Escuela Politecnica Nacional, Quito.
- Espinoza C, Maldonado, Valarezo, C, Carrasco,P, Barrera,J, & Gerra M. (2004). *Implementacion_Practica_Utilizando_IPv6*.(Practico No. 1) (p. 84). Quito: Escuela Politecnica del Ejercito del Ecuador.
- Horley,E (2014). *Practical IPv6 for Windows Administrators* - (p. 250). NEW YORK
- Steve Anglin, Mark Beckner, Ewan Buckingham, Gary Cornell, Louise Corrigan, James T. DeWolf, Jonathan Gennick, Jonathan Hassell, Robert Hutchinson, Michelle Lowman, James Markham, Matthew Moodie, Jeff Olson, Jeffrey Pepper, Douglas Pundick, Ben Renow-Clarke, Dominic Shakeshaft, Gwenan Spearing, Matt Wade, Steve Weiss. mre Durda, & Ali Buldu. (2010). *IPV4/IPV6 security and threat comparisons.* P 1- 7
- García, C. (2012, julio). *Análisis de seguridad en redes IPv6*. Universidad Carlos III de Madrid.
- Ghebregziabher, T., Puttonen, J., Hamalainen, T., & Viinikainen, A. (2006). *Security analysis of flow-based fast handover method for mobile IPv6 networks*. En 20th International Conference on Advanced Information Networking and Applications, 2006. AINA 2006 (Vol. 2, p. 5 pp.).

- González, S., & Gustavo, M. (2009, agosto). *Diseño de un laboratorio de análisis de vulnerabilidades y pruebas de penetración en redes de computo* (tesis). Escuela Superior de Ingeniería Mecánica y eléctrica, Instituto Politécnico Nacional, México.
- HUERTA, A. (2010). *Seguridad en Unix y redes*. (Vol. 2). Cataluyna.
- Coellar,J, & Cedeño,J. (2013, febrero 4). *Propuesta para la transición de ipv4 a ipv6 en el ecuador a través de la supertel*. Universidad Católica Santiago de Guayaquil, Guayaquil.
- LÓPEZ, & GACHO, J. (2014, enero). *Factibilidad de ip sec para ipv6 en la red de la universidad politécnica salesiana*, sede ESPE, Quito