RECIBIDO/RECEIVED: 29 OCTUBRE 2016 | ACEPTADO/ACCEPTED: 18 AGOSTO 2017 | PP. 09 - 16

Implementación de un prototipo como sistema detector de intrusos para ataques dirigidos al protocolo IPv6

Implementation of a prototype as an intrusion detector system for attacks directed to the IPv6 protocol

Diego Gustavo Caiza Méndez
Universidad Nacional de Chimborazo
(Ecuador)
diegomix07@hotmail.com

Andrés Santiago Cisneros Barahona
Universidad Nacional de Chimborazo
(Ecuador)

Pablo Martí Méndez Naranjo
Universidad Nacional de Chimborazo
Escuela Superior Politécnica de Chimborazo
(Ecuador)

Henry Mauricio Villa Yánez
Universidad Nacional de Chimborazo
(Ecuador)

Revista Cumbres Vol.3 Nº2
Versión impresa ISSN 1390-9541
Versión electrónica ISSN 1390-3365
http://investigacion.utmachala.edu.ec/revistas/index.php/Cumbres

RESUMEN

El trabajo de investigación incrementó la seguridad de la red local mediante la detección de ataques dirigidos al protocolo IPv6 que pueden comprometer la confidencialidad, integridad y disponibilidad. Las herramientas software utilizadas fueron: Virtual Box que permitió la virtualización de las distribuciones Linux, Security Onion distribución especializada en sistemas detectores de intrusos, Snort como motor del sistema detector, Graylog como gestor de logs IPv6, la suite TCHIPv6 como generador de tráfico IPv6 malicioso y Wireshark como herramienta de análisis de tramas del tráfico IPv6. Se desarrolló, implementó y comparó los resultados de los indicadores considerados en las variables, obtenidos al trabajar sobre la red local de la Facultad de Informática y Electrónica de la ESPOCH, entre el Prototipo I (Security Onion utilizando las reglas personalizadas y acoplado el módulo de gestión de logs) y el Prototipo II (Security Onion utilizando las reglas oficiales de Snort). Se concluyó que el sistema propuesto detectó y gestionó las alertas de intrusión mejorando el nivel de seguridad dentro de la red local.

Palabras clave: Technology and Engineering Sciences, Network Security, Internet Protocol Version 6 (Ipv6), Intrusion Detection System (Ids), Program (Snort), Alerts (Ipv6 Logs).

ABSTRACT

This work increased the security of the local network by detecting attacks directed to the IPv6 protocol that can compromise confidentiality, integrity and availability. The software tools used were Virtual Box, which allowed virtualization of Linux distributions; Security Onion allowed the distribution specialized in intrusion detection systems; Snort was used as the engine of the detector system; Graylog as IPv6 log manager; TCHIPv6 suite as a generator of malicious IPv6 traffic; and, Wireshark as an analysis tool for IPv6 traffic frames. The authors developed, implemented, and compared the results of the indicators considered in the variables obtained by working on the local network of the Faculty of Informatics and Electronics of ESPOCH, between Prototype I (Security Onion using the custom rules and coupled the module of Log management) and Prototype II (Security Onion using Snort's official rules). It was concluded that the proposed system detected and managed intrusion alerts by improving the level of security within the local network.

Keywords: Technology and Engineering Sciences, Network Security, Internet Protocol Version 6 (Ipv6), Intrusion Detection System (Ids), Open Source, Snort, Alerts (Ipv6 Logs)

INTRODUCCIÓN

Con el rápido desarrollo del Internet, el problema de la seguridad de la información, seguido por la naturaleza de complicación, accesibilidad y apertura, se ha convertido en el foco de atención global (Zeng, 2010). Para la comunicación a través de internet es necesario direcciones de protocolo (IP) para lo cual existe IPv4 e IPv6 (Siddika, Hossen, & Saha, 2017).

IPv6, la última versión del Protocolo de Internet, está llamado a coexistir con IPv4, y finalmente a sustituirlo, proporcionando un mayor espacio de direcciones que permita impulsar el crecimiento de internet en los próximos años (Gont, 2014).

Hay una variedad de aspectos de los protocolos IPv6 que resultan interesantes desde el punto de vista de la seguridad informática. En primer lugar, siendo IPv6 una nueva tecnología, el personal técnico tiene menos confidencia con los protocolos IPv6 que con los protocolos IPv4, y por tal motivo es muy probable que sus implicancias de seguridad sean pasadas por alto durante el despliegue de los mismos. En segundo lugar, las implementaciones de IPv6 son menos maduras que las de IPv4, y por tal motivo es muy probable que se descubran en las mismas un gran número de vulnerabilidades. En tercer lugar, productos tales como firewalls y sistemas de detección de intrusos en red, tienen usualmente menor soporte para los protocolos IPv6 que para los protocolos IPv4. En cuarto lugar, las implicanciones de seguridad de IPv6 y las diversas tecnologías de transición coexistencia en las actuales redes IPv4 son usualmente ignoradas, potencialmente permitiendo que los atacantes aprovechen estas tecnologías para evadir controles de seguridad IPv4 con técnicas no anticipadas (Gont, 2013),

Los atacantes no efectúan el escaneo de direcciones IPv6 mediante la fuerza bruta, sino que intentan mejorar sus métodos de escaneo aprovechando los ya conocidos patrones de asignación de direcciones IPv6 (Shutte, 2013)

La detección de intrusos en redes es un enfoque para proporcionar seguridad a las redes informáticas. Se basa en la creencia de que el comportamiento del atacante será diferente al comportamiento de los usuarios legítimos de la red (Zhang, 2010). Desde hace años, se está avanzando hacia las redes IPv6 y no hay demanda para asegurarlas. Para proporcionar seguridad a la red IPv6 hay necesidad de una mejor detección de intrusos. Actualmente existen muchas herramientas y técnicas para detectar o evitar intrusiones en IPv4, pero en IPv6 muy pocas herramientas de detección de intrusos están disponibles. Como IPv6 es un nuevo protocolo para la comunicación a través de Internet es más vulnerable a los ataques. Dado que cada vez más nuevos ataques aparecen, el mecanismo de defensa tradicional no puede satisfacer la necesidad segura de un nuevo entorno de red (Yao, y otros, 2008).

La próxima generación del protocolo IPv6 trae los nuevos retos para la seguridad de la información (Sumit & Ravreet, 2013). El ataque de la red y la defensa de la red siempre es una contradicción. Aunque algunas de sus nuevas características pueden mejorar la seguridad de la red, las redes IPv6 siguen enfrentándose a graves problemas de amenazas de seguridad, debido a que pocos problemas de seguridad derivan únicamente de la capa IP en el

modelo de red (Huand, Zhang, & Yao, 2009). El ataque de hombre en el medio (MITM) implica dos puntos finales (víctimas) y un tercero (atacante), el cual tiene acceso en el canal de comunicación entre dos extremos y puede manipular sus mensajes (Conti, Dragoni, & Lesyk, 2016). El ataque de denegación de servicios (Dos), causa que un servicio o recurso sea inaccesible a los usuarios legítimos (Zubair, Jwaid, & Salih, 2016). El ataque de reconocimiento obtiene información acerca de la red, realizando escaneos de puertos para determinar servicios activos. (Kun, Hui, & Di, 2016)

En la investigación de Sumit y Ravreet (2013), se analiza un caso específico que es la intrusión por fuerza bruta en la red IPv6 para obtener acceso no autorizado. Los autores despliegan una red IPv6, utilizan dos máquinas virtuales en un host físico Ubuntu, el cual se configura como router para reenviar paquetes entre máquinas virtuales. Una máquina virtual la utilizan como atacante y la otra como víctima. Snort está configurado entre el flujo de paquetes de las máquinas virtuales para analizar los paquetes y detectar la intrusión. En la investigación de Gu-Hsin (2014), se propone utilizar una herramienta común de test de vulnerabilidades IPv6 para atacar a una víctima virtual y generar firmas de ataques IPv6. Utiliza además un sniffer para observar los paquetes de la red y comprobar si cumple con las firmas predefinidas. El sistema sugerido plantea generar un informe para comunicar a los administradores de red si la red IPv6 es vulnerable o no. En la investigación de Saad, Ramadass, & Manickam (2013), se muestra una revisión de literatura relacionada con la seguridad de ICMPv6, se presenta consideraciones y métodos de detección de ataques por inundación del protocolo ICMPv6. Los autores proponen mitigar este tipo de ataques con técnicas neuro difusas y de minería de datos a través del uso de Snort.

La presente investigación implementa una herramienta de seguridad perimetral dentro de la red local para detectar anomalías a causa del protocolo IPv6, por lo que el enfoque original de este proyecto a diferencia de las investigaciones previas monitorea y administra de manera transparente y sencilla para el usuario final, todo esto ejecutado con software libre.

MATERIALES Y MÉTODOS

El software utilizado para el desarrollo se detalla a continuación: Distribución de Linux Security Onion para la detección de intrusos y control de seguridad de la red (Security Onion Solutions, 2015). Snort se utiliza para realizar el análisis de tráfico en tiempo real y registra los paquetes de las redes IP (Cisco, 2016), es el motor detector de patrones a través de reglas personalizadas de tráfico malicioso. Graylog se utiliza para almacenar todos los registros en un solo lugar para tener visibilidad del 100% (Graylog Inc., 2016), funciona en modo servidor para mostrar y gestionar los logs IPv6 generados. Los procesos realizados durante la investigación son:.

- Análisis y clasificación de los ataques que pueden vulnerar el protocolo IPv6, categorizándoles en: ataques de reconocimiento, ataques de hombre en el medio y ataques de denegación de servicio
- Análisis de los sistemas detectores de intrusos con soporte de IPv6 y bajo código abierto (Snort, Suricata y Bro), definiendo a Snort como el más adecuado debido a las características de: arquitectura, fiabilidad y constante actualización que brinda su software como se muestra en la Tabla I.

Tabla I Cuadro comparativo de los IDS analizados

PARÁMETRO	SNORT	SURICATA	BRO
Soporte IPv6	Sí	Sí	Sí
Gestión de logs IPv6	No	No	No
(Por línea de coman dos)			
Estrategias de detección	Por firmas de tráfico	Por firmas de tráfico	Por patrones de eventos
Firmas IPv6 de detección	Pocas	Pocas	No
Rendimiento con tráfico IPv6	Muy Bueno	Bueno	Bueno
Detección con tráfico IPv6	Muy Bueno	Bueno	Bueno

- Estudio de las herramientas open source que permiten explotar las vulnerabilidades del protocolo IPv6 (Evil Foca, SI6 Network' IPv6 Toolkit, THC-IPv6 Toolkit), definiendo a la suite THC-IPv6 como la óptima por ser la más popular dentro del mundo de la seguridad IPv6.
- Creación de nuevas reglas específicas para ataques realizados con la suite de herramientas de pentesting THC-IPv6.
- Implementación del sistema detector de intrusos desarrollado el cual se lo divide en dos importantes módulos, el módulo de detección de anomalías y el módulo de gestión.
- Fase de pruebas:

El Prototipo I establecido para ejecutar los experimentos de pruebas, se compone de los módulos funcionales indicados en la Figura I:

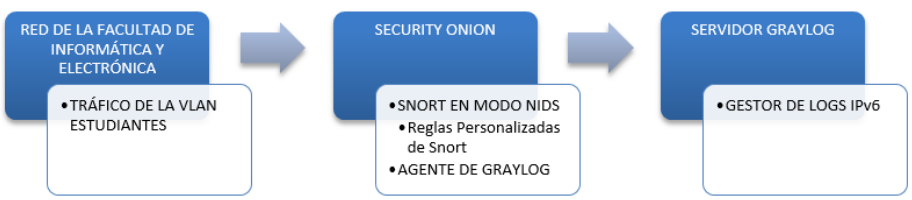

Figura I Estructura general del prototipo I

El Prototipo II establecido para ejecutar los experimentos de pruebas, se compone de los módulos funcionales indicados en la Figura II:

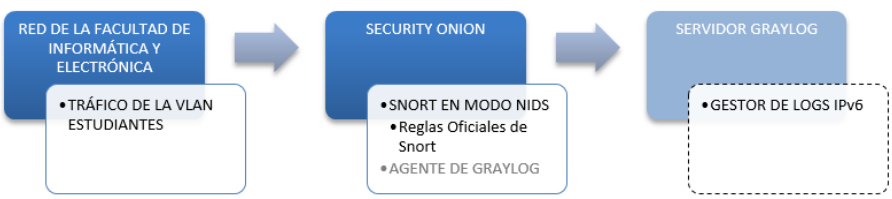

Figura II Estructura general del prototipo II

Ambiente de pruebas

Todas las pruebas se realizan en el mismo escenario debido a que se usa la infraestructura de la red de la FIE (Facultad de Informática y Electrónica) de la ESPOCH (Escuela Superior Politécnica de Chimborazo), específicamente se trabaja con la VLAN de estudiantes aprovechando el tráfico nativo bajo IPv6. El administrador de red de la Dirección de Tecnologías de la Información y Comunicación, configuro un puerto del Switch de distribución del Edificio de la FIE, en modo SPAN (Switched Port Analyzer) permitiéndole al sistema a través de este puerto tener acceso a todo el tráfico que circula en la VLAN.

Experimento 1

El experimento 1 analiza la efectividad de detección del Prototipo I ante el tráfico malicioso inyectado en la VLAN de estudiantes durante la jornada normal de actividades, los pasos requeridos para iniciar la prueba son: iniciar el sistema detector de intrusos (reglas local.rules), conectar la máquina atacante a la VLAN de estudiantes, ejecutar cada uno de los ataques detallados en la Tabla II los mismos que han sido categorizados en tres tipos de acuerdo a su modo de proceder: reconocimiento, hombre en el medio y denegación de servicio.

Experimento 2

El experimento 2 analiza la efectividad de detección del Prototipo II es equivalente al experimento 1 pero con la diferencia que el sistema detector utiliza las reglas (download.rules).

Experimento 3

En el experimento 3 se monitorea el tráfico que circula en la VLAN estudiantes durante un día en la jornada normal de actividades, con esta prueba se identifica la cantidad de alertas denominadas falsas positivas que se originan al utilizar el Prototipo I, como se detallan en la Tabla III.

Experimento 4

El experimento 4 es equivalente al proceso anterior, pero en este caso se utiliza el Prototipo II. De igual manera, el monitoreo se lo realiza durante otro día en la jornada normal de actividades, recopilando los datos para analizarlos y cuyos resultados se muestran posteriormente.

Experimento 5

El experimento 5 verifica la capacidad de presentación y gestión de los logs IPv6 obtenidos durante el proceso de pruebas, debido a que los campos de dirección origen y dirección destino de las alertas tienen direccionamiento IPv6. Esta prueba evidenciará si el Prototipo I cumple con la premisa de gestionar alertas con direccionamiento IPv6.

Experimento 6

El experimento 6 es equivalente al proceso anterior pero aplicado al Prototipo II, esta prueba evidencia si este Prototipo cumple con la premisa de gestionar y administrar las alertas que contengan direccionamiento IPv6.

Tabla II Nombre del ataque ejecutado y categorización

ATAQUE	CATEGORÍA
atk6-alive6 eth0	Reconocimiento
atk6-alive6 -4 192.168.1.0/24 eth0	Reconocimiento
atk6-alive6 -d eth0	Reconocimiento
atk6-parasite6 -l eth0	Hombre en el medio
atk6-parasite6 -l -R eth0	Hombre en el medio
atk6-parasite6 -l -F eth0	Hombre en el medio
atk6-parasite6 -l -H eth0	Hombre en el medio
atk6-parasite6 -l -R -F –H	Hombre en el medio
atk6-fake_router6 eth0 2001:db8:bad::/64	Hombre en el medio
atk6-fake_router6 -H eth0 2001:db8:bad::/64	Hombre en el medio
atk6-fake_router6 -D eth0 2001:db8:bad::/64	Hombre en el medio
atk6-fake_router6 -F eth0 2001:db8:bad::/64	Hombre en el medio
atk6-fake_router6 -H -D eth0 2001:db8:-bad::/64	Hombre en el medio
atk6-flood_advertise6 eth0	Denegación de servicios
atk6-flood_solicitate6 eth0	Denegación de servicios
atk6-flood_router6 eth0	Denegación de servicios
atk6-flood_router6 -F eth0	Denegación de servicios
atk6-flood_rs6 eth0	Denegación de servicios
atk6-flood_rs6 -s eth0	Denegación de servicios
atk6-flood_rs6 -S eth0	Denegación de servicios
atk6-flood_rs6 -s -S eth0	Denegación de servicios
atk6-flood_redir6 eth0	Denegación de servicios
atk6-flood_redir6 -H eth0	Denegación de servicios
atk6-flood_redir6 -F eth0	Denegación de servicios
atk6-flood_redir6 -H -F eth0	Denegación de servicios

Tabla III Intervalos de tiempo experimento 3

INTERVALOS DE TIEMPO	CATEGORIZACIÓN DEL ATAQUE	NÚMERO DE INTERVALO
07:00 – 09:59	Ataque de reconocimiento	Intervalo 1
10:00 – 12:59	Ataque de MITM	Intervalo 2
13:00 – 15:59	Ataque de MITM	Intervalo 3
16:00 – 18:59	Ataque DDos	Intervalo 4
19:00 – 21:00	Ataque DDos	Intervalo 5

RESULTADOS Y DISCUSIÓN

Se crearon nuevas reglas, específicas para detectar los patrones de tráfico IPv6 generados por la suite, como consecuencia de que las reglas que componen el paquete oficial de Snort no cumplieron con la premisa de identificar este tipo de tráfico, los detalles de las reglas creadas se muestran en la Tabla IV.

Tabla IV Reglas creadas para los ataques con la suite TCH-IPv6

REGLAS IPV6 CREADAS	ATAQUES CON LA SUITE THC-IPV6
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE DE RECONOCIMIENTO IPv6 CON THCIPv6 TOOLKIT"; itype:128; icode:0; dsize:8; classtype:network-scan; sid:10000011; rev:3)	atk6-alive6 eth0 atk6-alive6 -4 192.168.1.0/24 eth0 atk6-alive6 -d eth0
alert icmp $HOME_NET any -> $HOME_NET any (msg:"ATAQUE MITM PARASITE6 CON THCIPv6 TOOLKIT"; dsize:132<>1236; itype:137; icode:0; classtype:policy-violation; sid:10000025;rev:3)	atk6-parasite6 -l eth0 atk6-parasite6 -l -R eth0 atk6-parasite6 -l -F eth0 atk6-parasite6 -l -H eth0 atk6-parasite6 -l -R -F –H
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FAKE-ROUTER6 CON THCIPv6 TOOLKIT"; dsize:156; itype:134; icode:0; detection_filter:track by_dst, count 9, seconds 50; classtype:policy-violation; sid:10000033; rev:3;)	atk6-fake_router6 eth0 2001:db8:-bad::/64 atk6-fake_router6 -H eth0 2001:db8:-bad::/64 atk6-fake_router6 -D eth0 2001:db8:-bad::/64 atk6-fake_router6 -F eth0 2001:db8:-bad::/64 atk6-fake_router6 -H -D eth0 2001:db8:bad::/64
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FLOOD_ADVERTISE6 (NA) CON THCIPv6 TOOLKIT"; itype:136; icode:0; detection_filter:track by_dst, count 50000, seconds 20; classtype:policy-violation; sid:10000018; rev:3)	atk6-flood_advertise6 eth0
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIPv6 TOOLKIT"; itype:135; icode:0; detection_filter:track by_dst, count 50000, seconds 20; classtype:policy-violation; sid:10000020; rev:3)	atk6-flood_solicitate6 eth0
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FLOOD_ROUTER6 (RA) CON THCIPv6 TOOLKIT"; dsize:60; itype:134; icode:0; detection_filter:track by_dst, count 50000, seconds 20; classtype:policy-violation; sid:10000019; rev:3)	atk6-flood_router6 eth0 atk6-flood_router6 -F eth0
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FLOOD_RS6 (RS) CON THCIPv6 TOOLKIT"; itype:133; icode:0; detection_filter:track by_dst, count 50000, seconds 20; classtype:policy-violation; sid:10000021; rev:3)	atk6-flood_rs6 eth0 atk6-flood_rs6 -s eth0 atk6-flood_rs6 -S eth0 atk6-flood_rs6 -s -S eth0
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FLOOD_REDIR6 (RE) CON THCIPv6 TOOLKIT"; itype:137; icode:0; detection_filter:track by_dst, count 50000, seconds 20; classtype:policy-violation; sid:10000022; rev:3)	atk6-flood_redir6 eth0 atk6-flood_redir6 -H eth0 atk6-flood_redir6 -F eth0 atk6-flood_redir6 -H -F eth0

Se acopló el servidor de logs open source Graylog, debido a la falta de soporte de los gestores internos de Security Onion el cual se encarga de la gestión y administración de logs IPv6 a través de una interfaz web, como se muestra en la Figura III.

Se desarrollaron las pruebas utilizando el Prototipo I y el Prototipo II en los experimentos establecidos para los indicadores: Número de alertas positivas verdaderas, Número de alertas falsas positivas, gestión de logs IPv6, replicación de logs IPv6.

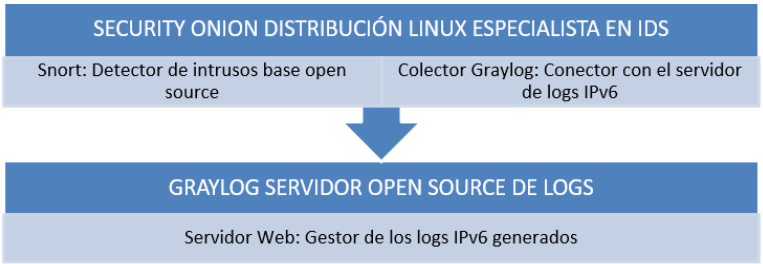

Figura III Módulos del sistema desarrollado

Número de alertas positivas verdaderas

Los resultados finales obtenidos por este indicador, una vez que se concluyó el experimento 1 y 2, se muestran en la Tabla V. Es necesario señalar que por cada ataque detectado se cuantificó al indicador con un valor equivalente a 1, por el contrario; por cada ataque que no es detectado se aplicó un valor igual a 0. Estos resultados muestran la efectividad del Prototipo I durante la fase de detección de patrones de tráfico IPv6 anormal en la VLAN de Estudiantes en la FIE. De un total de 25 ataques generados se detectaron 24 es decir el Prototipo I tiene un 96% de efectividad, mientras el Prototipo II detectó 4 ataques con el 16% de efectividad para este experimento, se debe señalar que en la Prueba 12 el ataque atk6-fake_router6 -F eth0 2001:db8:-bad::/64 tiene un error en su ejecución ya que crea paquetes mal formados, razón por la cual se hace imposible su detección.

Tabla V Resultados del indicador Número de Alertas Positivas del Prototipo I y II

PROT	PRUEBAS																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
I	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
II	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0

Se obtuvieron 24 alertas positivas con el Prototipo I y 4 con el Prototipo II.

Número de alertas falsas positivas

Los resultados obtenidos concluido el experimento 3 y 4, muestran la capacidad del Prototipo I y II para no generar alertas falsas durante el monitoreo de la VLAN de estudiantes en la FIE, es necesario señalar que por cada alerta falsa se cuantifico al indicador con un valor equivalente a 1, por el contrario, por cada ataque verdadero realizado a manera de control se aplica un valor igual a 0. Del período comprendido desde las 07:00 hasta las 21:00 no se detectaron alertas negativas por el Prototipo I por lo que se logra deducir de estos resultados la precisión que tienen las reglas creadas para la detección de los patrones IPv6 maliciosos; a diferencia de las 80895 alertas negativas detectadas por el Prototipo II lo que ocasiona un problema de ineficiencia debido a que está generando alarmas ante ataques inexistentes.

Gestión de logs IPv6

Luego de realizar los experimentos de detección de número de alertas positivas y número de alertas falsas positivas, se registraron los datos estadísticos de los logs IPv6 con el Prototipo I. En las Figuras IV a la Figura VII, se muestran los datos estadísticos obtenidos.

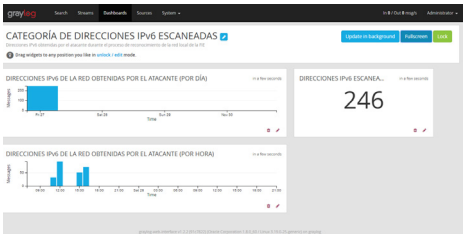

Figura IV Datos estadísticos de las direcciones IPv6 obtenidas por el atacante

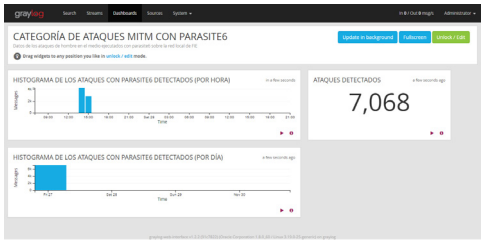

Figura V Datos estadísticos de ataques MITM con la herramienta parasite6

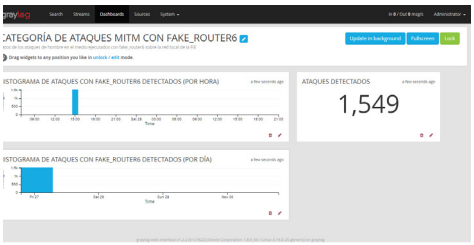

Figura VI Datos estadísticos de ataques MITM con la herramienta fake_router6

Figura VII Datos estadísticos de denegación de servicios con flood_advertise6

Luego de realizar los experimentos de detección de número de alertas positivas y número de alertas falsas positivas, se registraron los datos estadísticos de los logs IPv6 con el Prototipo II. En la Figura VIII se muestra los resultados de la recolección de los logs IPv6 por el gestor Sguil de Security Onion y en la Figura IX se muestra los resultados de la recolección de los logs IPv6 por el gestor Snorby de Security Onion.

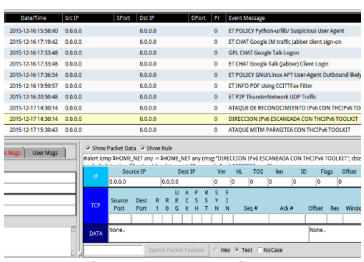

Figura VIII Sguil gestor interno de Security Onion no compatible para IPv6

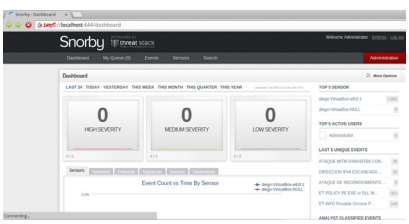

Figura IX Snorby gestor interno de Security Onion no compatible para IPv6

De acuerdo con estos resultados obtenidos al monitorear el tráfico de la red se determina que el Prototipo I permite la presentación de las alertas o logs IPv6 generados, así como facilita su gestión a través de dashboards en la interfaz web de Graylog para efectuar el análisis en detalle de logs IPv6

recolectados. Los resultados obtenidos por el Prototipo II indican la imposibilidad de presentación y mucho menos la gestión de las alertas o logs IPv6 generados, lo cual limita claramente el uso del prototipo.

Replicación de logs IPv6

La replicación de logs tiene el objetivo de almacenar en tiempo real los logs IPv6 generados. En la Figura X se muestra el archivo que contiene los logs IPv6 generados por el Prototipo I, el cual se guarda en el módulo de Security Onion en la ruta /nsm/sensor_data/diego-VirtualBox-eth3/snort-1.

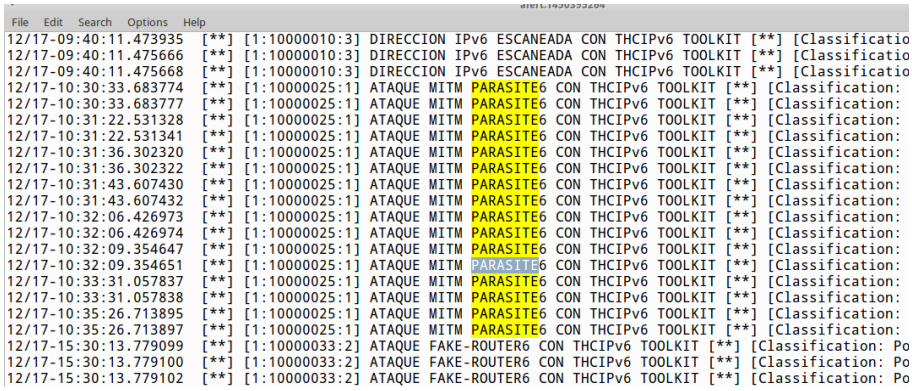

Figura X Archivo de logs IPv6 alojado en el módulo de Security Onion

En la Figura XI se muestran los logs IPv6 almacenados en el servidor Graylog, en el cual se detalla la información recolectada durante los distintos ataques realizados en las pruebas.

Figura XI Log IPv6 alojado en el servidor Graylog

Por lo tanto, se verifica que ambos ficheros manejan los mismos registros de alertas IPv6 en tiempo real en el Prototipo I. El Prototipo II solo almacena los logs IPv6 en la distribución Security Onion dentro de la ruta en la ruta /nsm/sensor_data/diego-VirtualBox-eth3/snort-1, debido a que su estructura no se está acoplada al módulo del servidor Graylog. De acuerdo con estos resultados obtenidos al monitorear el tráfico de la red se determina que el Prototipo I si cumple con el objetivo de replicar los logs IPv6 generados, a diferencia de los resultados obtenidos al monitorear el tráfico de red con el Prototipo II.

Discusión

Comparando los resultados obtenidos en la presente investigación con otros autores que han realizado contribuciones previas acerca de este tema, se indica que los resultados han sido obtenidos con el despliegue y monitoreo de la red en un ambiente real. Específicamente se trabajó en la red local de la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo; en comparación con los resultados obtenidos de otras investigaciones las cuales han sido por lo general en ambientes controlados o virtuales. Se han creado reglas específicas basadas en patrones de tráfico IPv6 anormal, lo cual permite al motor del sistema detector de intrusos reconocer este tráfico con mayor sencillez originando robustez y seguridad en el sistema; en relación con otros estudios cuya definición de reglas es inferior por lo que es más limitada y vulnerable. Se definen claramente los métodos y procedimientos a utilizar, conjuntamente con las reglas para la implementación y monitoreo de la red de forma clara y práctica, demostrando la confiabilidad en el proceso y en los resultados obtenidos; en relación a otros estudios existentes en los que se generaliza y teoriza la forma de realizarlo, por lo que sus resultados no pueden demostrar la efectividad de la propuesta planteada. Se acopló el servidor de logs open source Graylog, debido a la falta de soporte de los gestores internos de Security Onion, el cual permite a través de su colector el almacenamiento de los logs en su base de datos interna, la gestión de los registros y permite el análisis en un solo sistema centralizado, lo cual brinda grandes ventajas para el monitoreo de las redes y análisis de vulnerabilidades; en comparación a estudios anteriores que utilizan el Snort estándar, el cual no posee gestión de logs IPv6, limitando su funcionalidad y beneficios.

CONCLUSIONES

El Prototipo I detecta un número mayor de ataques, el registro de alertas falsas es nulo, además permite la gestión y análisis de los logs IPv6 y cumple con el objetivo de replicar en tiempo real los logs IPv6 generados, en contraste de los resultados obtenidos al monitorear el tráfico de red con el Prototipo II.

El módulo del manejo de logs IPv6 incluido facilita la gestión de los sucesos detectados con actividad anormal para ayudar al administrador la toma de decisiones en la red local.

El Prototipo I es adaptable a cualquier Red Lan que tenga soporte del protocolo IPv6, independientemente de la infraestructura que posea, con lo cual se cumple la premisa de escalabilidad.

REFERENCIAS BIBLIOGRÁFICAS

Cisco. (2016). *Snort*. Recuperado el 2015, de https://www.snort.org/faq/what-is-snort

Conti, M., Dragoni, N., & Lesyk, V. (2016). *A Survey of Man In The Middle Attacks*. IEEE Communications Surveys & Tutorials (págs. 1-26). IEEE.

Gont, F. (2013). *Hacking IPv6 Networks*. Obtenido de http://www.es.hackingipv6networks.com/trainings/hacking-ipv6-networks

Gont, F. (2014). *Mitos sobre la seguridad en IPv6: desmontando falsas ideas*. Obtenido de http://searchdatacenter.techtarget.com/es/cronica/Mitos-sobre-la-seguridad-en-IPv6-desmontando-falsas-ideas

Graylog Inc. (2016). *Graylog*. Obtenido de https://www.graylog.org/

Gu-Hsin, L. (2014). *A Light-Weight Penetration Test Tool for IPv6 Threats*. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), (págs. 49-52).

Huand, S., Zhang, H., & Yao, G. (2009). *Research of NIDS in IPV6 Based on Protocol Analysis and Pattern Matching*. Knowledge Discovery and Data Mining (págs. 542-545). IEEE.

Kun, W., Hui, Q., & Di, H. (2016). *Network security situation evaluation method based on attack intention recognition*. Computer Science and Network Technology (ICCSNT) (págs. 919-924). IEEE.

Saad, R., Ramadass, S., & Manickam, S. (2013). *A study on detecting ICMPv6 flooding attack based on IDS*. Australian Journal of Basic and Applied Sciences, (págs. 175-181).

Security Onion Solutions. (2015). *Introduction to Security Onion*. Obtenido de https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion

Shutte, M. (2013). *Design and Implementation of an IPv6 Plugin for the Snort Intrusion Detection System*. Magdeburger Journal zur Sicherheitsforschung, 2, 409-452.

Siddika, F., Hossen, A., & Saha, S. (2017). *Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow*. Networking, Systems and Security (NSysS). IEEE.

Sumit, K., & Ravreet, K. (2013). *IPv6 Network Security using Snort*. Journal of Engineering, Computers & Applied Sciences (JEC&AS), (págs. 17-22).

Yao, G., Guan, Q., Lin, L., Huang, S., Zhu, G., Zhand, H., & Gao, Z. (2008). *Research and Implementation of Next Generation Network Intrusion Detection System Based on Protocol Analysis*. Computing, Communication, Control, and Management (págs. 353-357). IEEE.

Zeng, Z. (2010). *Intrusion Detection System of IPv6 Based on Protocol Analysis*. Multimedia Technology (ICMT). IEEE.

Zhang, Y. (2010). *Study on Instrution IPv6 Detection System on LINUX*. Computational Intelligence and Industrial Applications, 2009. PACIIA 2009 (págs. 5-8). IEEE.

Zubair, A., Jwaid, A., & Salih, A. (2016). *Analysing denial of service attack traffic signature in IPv6 local network using correlation inspection*. Future Technologies Conference (FTC) (págs. 1008-1013). IEEE.