ISSN: 1692-7257 - Volumen 1 – Número 29 - 2017
Revista Colombiana de Tecnologías de Avanzada

Recibido: 09 de mayo de 2017
Aceptado:

ANÁLISIS DE UNA RED EN UN ENTORNO IPV6: UNA MIRADA DESDE LAS INTRUSIONES DE RED Y EL MODELO TCP/IP

ANALYSIS OF A NETWORK IN AN IPV6 ENVIRONMENT: A VIEW FROM NETWORK INTRUSIONS AND THE TCP / IP MODEL

Sergio Alberto Alvernia Acevedo[*], Dewar Rico Bautista[**]

[*] **Universidad Francisco de Paula Santander Ocaña,** Facultad de Ingeniería, Ingeniero de sistemas. Semillero de Investigación GNU/Linux And Security (SIGLAS). Grupo de Investigación en Ingenierías Aplicadas (INGAP)
Ocaña, Norte de Santander, Colombia.
Celular: 3177140153. E-mail: saalverniaa@ufpso.edu.co

[**] **Universidad Francisco de Paula Santander Ocaña,** Facultad de Ingeniería, Ingeniero de sistemas, especialista en telecomunicaciones, magíster en ciencias computacionales. Grupo de Investigación en Ingenierías Aplicadas (INGAP).
Ocaña, Norte de Santander, Colombia.
Celular: 3123973390. E-mail: dwricob@ufpso.edu.co.

Resumen: Partiendo de la revisión bibliográfica de las revistas de más alto impacto, se muestran los diferentes énfasis y tendencias teóricas de la discusión sobre el uso que se está haciendo de los analizadores de paquetes, en particular de aquel conocido como *Wireshark*, considerando las aplicaciones que puede tener para la captura de datos que permitan realizar un análisis para la evaluación de una red en un entorno controlado de laboratorio. El contenido y estructura del trabajo es resultado de la dinámica encontrada en torno a tres diferentes propuestas teóricas: Modelo TCP/IP, Intrusiones de red y análisis de una red en un entorno IPv6. La utilidad de este artículo es diversa. En primer lugar, se identificaron interrelaciones a partir de un análisis de las similitudes, diferencias y contraposiciones de los conceptos planteados entre los artículos revisados. Y, en segundo lugar, sirve como evidencia de la necesidad apremiante de las organizaciones por utilizar herramientas que permiten la recopilación de información y una inspección constante del tráfico para realizar un análisis pertinente que permita la detección de anomalías que puedan ser consideradas una amenaza para un sistema y de esta manera tomar decisiones apropiadas para las necesidades de la red.
Palabras claves: Sniffer de paquetes, IPv6, seguridad, TCP / IP.

Abstract: Based on the literature review of the highest impact journals, different emphasis and theoretical trends of discussion about the use being made of packet sniffers, particularly one known as Wireshark, considering the applications may have to capture data to permit realize an analysis to provide an assessment of it in a controlled laboratory environment. The content and structure of the work is the result of the dynamics found on three different theoretical proposals: Model TCP / IP, network intrusions and analysis of a network in an IPv6 environment. The usefulness of this article is diverse. First, interrelations from an analysis of the similarities, differences and conflicts arise between the concepts reviewed articles were identified. And secondly, it serves as evidence of the urgent need for organizations to use tools for gathering information and constant traffic inspection to perform a relevant analysis to the detection of abnormalities that might be considered a threat to a system and thus make appropriate decisions for the needs of the network.
Keywords: *Packet sniffings, IPv6, security, TCP/IP*.

1. INTRODUCCIÓN

La información es uno de los activos más importantes de cualquier organización o persona, mucho más ahora que los datos pueden transportarse con mucha mayor facilidad que en épocas anteriores al uso de las computadoras, por lo cual es necesario reconocer el comportamiento de los datos a través de una red de equipos que permitan tener el control de la información.

Las mejoras en las técnicas que permitió un uso más eficiente de los recursos mejorando las comunicaciones y asegurando que la información compartida pudiera beneficiar a un mayor número de personas de forma instantánea, provocó el surgimiento de nuevas amenazas sobre los datos como la posible pérdida o la falta de control sobre el uso de los mismos. Por lo cual, con las nuevas posibilidades surgidas con los avances tecnológicos empieza una preocupación creciente de los usuarios por conservar la información protegida de otros individuos (Confidencialidad), mantenerla idéntica en el tiempo y en el espacio (integridad) y acceder a ella en cualquier momento (disponibilidad) principios básicos de la seguridad de la información (Krutz & Vines, 2007).

Para asegurar que los datos que es transportada por una red conserven su confidencialidad, integridad y disponibilidad es necesario reparar en las unidades más pequeñas de las comunicaciones, los paquetes "que son las entidades básicas de todo sistema de comunicación". Para reconocer el comportamiento de los paquetes requerimos de una constante revisión de lo que sucede con ellos cuando viajan a través de una red, y a partir de ese análisis generar medidas que ayuden a la detección de intrusiones (Gómez, Pérez, Donoso, & Herrera, 2010).

Comprender que el buen funcionamiento de una red de computadoras no se reduce a la mera interconexión apropiada del hardware sino a la manera como los datos viajan a través de estos medios, para lo cual es necesario reconocer las causas de malos funcionamientos en la red, además de reconocer que un mal funcionamiento puede darse por el ingreso de terceros que quieren afectar las actividades de la red.

Uno de los primeros intentos por establecer el comportamiento de los datos a través de redes previamente establecidas fue instaurado en la empresa de teléfonos *Bell* (*Bell Telephone System*) que esperaba generar un análisis de datos de origen electrónico, recibiendo el nombre Procesamiento de Datos Electrónicos (*Electronic Data Processing, EDP*). En la década de 1970 el Departamento de Defensa de los Estados Unidos empieza a sugerir la necesidad de crear sistemas seguros acuñando el término "sistemas de confianza", proponiendo en 1977 la Iniciativa de Seguridad para señalar cuáles eran los criterios necesarios para que un sistema seguro (Gómez, Pérez, Donoso, & Herrera, 2010) (Department of Defense, 1985).

James Anderson establece que para poder llevar un control adecuado sobre los datos y garantizar la seguridad de un sistema, es necesario llevar un registro (*log)* de los datos y sus comportamientos para identificar las amenazas que puedan sobrevenir sobre un sistema. Desde este punto es significativo la recopilación de información de una red a través de la captura de los paquetes (*packet sniffing*) para detectar comportamientos anómalos o usos indebidos, porque permiten identificar las medidas apropiadas para resolver un problema y logran realizar los correctivos apropiados. La herramienta que permiten realizar este proceso se conoce como *packet sniffers* (Biswas & Ashutosh, 2014) (Gupta & Mamtora, 2012).

Una de las herramientas más populares usadas para la captura de datos que permite una disección de los protocolos es *Wireshark*. *Wireshark* es una aplicación de software libre, capaz de identificar más de 1200 protocolos, descifrando la estructura de cada uno de ellos; permite al usuario identificar campos relevantes que ofrecen información sobre cada paquete que es capturado (Orebaugh, y otros, 2007) (Biswas & Ashutosh, 2014) (Asrodia & Patel, 2012).

Por lo anterior, podemos observar que está preocupación por la seguridad de los datos es una llamada internacional para proponer el uso de herramientas creadas con el propósito de supervisar los tráficos de la red en tiempo real y poder facilitar la detección de amenazas a un sistema, por lo cual es necesario comprender el uso de estas herramientas y aplicarlas a entornos regionales o locales. Por lo tanto, dada la importancia de estar en constante revisión del tráfico de una red, y la proliferación de tecnologías que permiten conexión a redes gran tamaño, como el Internet, proponer el manejo de una herramienta que muestra el flujo de la red y disecciona los paquetes ofrecerá una mayor

comprensión y apropiación del funcionamiento de los elementos que la constituyen. Comprensión que puede permitir a las personas con conocimientos básicos empaparse de las maneras en las cuales la comunicación ocurre, y a aquellos con mayor experiencia tener un mayor control sobre los eventos que ocurren sobre la red que administran.

2. MARCO TEÓRICO

Las computadoras han abierto las posibilidades para que pueda hacerse un uso de la información de manera sofisticada y que se establezcan interconexiones potentes, pero al mismo tiempo con el asombro al ver lo que las computadoras pueden hacer han dejado las puertas abiertas detrás de ellas cuando ingresaron al universo digital llenos de expectativas (Cobb, 1992) (Tanenbaum & Wetrerall, 2011).

"Vivimos en una sociedad…" en la que "'el software ha tomado el control'. Transacciones bancarias, relaciones sociales, reservas aéreas, entre otras, cada vez más actividades de la vida cotidiana son mediadas por líneas de programación que se ejecutan hasta en un dispositivo que cabe en un bolsillo" (Medina, 2014).

Por lo cual sin entrar en discusiones de cómo establecer cuál equipo tiene más valor dependiendo de la información que proteja, debemos considerar tres conceptos importantes: La confidencialidad como la prevención de revelación información sin autorizados. Integridad como la prevención de modificación sin autorización de la información, y, por último, la disponibilidad como la prevención de chequeos sin aprobación de la información y los recursos.

Desde aquí surge la pregunta por mantener un sistema confiable dado que pueden considerarse los aspectos en los cuales falla un sistema, dado que un sistema puede tener problemas de disponibilidad que conlleva la evaluación de sus recursos como el cableado o los equipos y otros puede ser sobre la confidencialidad. Es necesario ser cuidadoso al tener las consideraciones necesarias para conservar las amenazas al mínimo y no comprometer un sistema (González, 2010).

Sin embargo, cuando al establecer que los sistemas sean confiables deben considerarse, como se mencionó arriba, que debe, en primer lugar, existir comunicación entre los sistemas. El propósito principal es manejar una gran cantidad de información entre dispositivos manteniendo la información en movimiento sin comprometerla ni perderla, sin interrupciones, pero para ello primero debe establecerse un camino, para lo cual establecen unas reglas para proceder, dado que existen diferentes tecnologías que sirven para cumplir un mismo objetivo las reglas sugieren una forma de comportamiento que permite que los recursos apunten a interactuar con el menor número de inconvenientes (Stallings W. , 2007) (Stallings W. , 2004).

Por lo tanto, establecer estándares es necesario debido a la complejidad que generan las comunicaciones; los estándares permiten normalizar las funcionalidades en una arquitectura de comunicaciones. Para esto la Organización Internacional de Estandarización (ISO, Internacional Organization for Standarization) estableció dicha arquitectura conocida como el modelo de referencia OSI. (Stallings, 2004) con el mismo propósito se implementó otro modelo que fue desarrollado a nivel experimental en la red financiada por DARPA (Defense Advanced Research Projects Agency) denominado TCP/IP (Transfer Control Protocol/Internet Protocol) que utiliza de cinco capas combinando las capaz de enlace de datos y el físico, considerando las redes físicas interconectadas como una gran red (Forouzan, 2013).

En consecuencia, es necesario reconocer cómo ocurre el tráfico de la información dentro de una red para poder evaluar las maneras como debe que sea protegida de manera adecuada, sin embargo, es difícil reconocer la cantidad de información que es transportada dado la complejidad necesaria para asegurar que los datos lleguen a su destino. Una manera de conocer cómo funciona la red normalmente es usando un sniffer o analizador de red en varios puntos de la red. Los sniffers son importantes porque permiten monitorear la red para solucionar problemas y llevar un registro de todas las actividades que generan las actividades de la red (Asrodia & Patel, 2012).

Un *sniffer* o analizador de red es un programa que captura todos los datos que pasan a través de una tarjeta de red. Para ello se basa en un defecto del protocolo *Ethernet* (Herrera y otros, 2004). El protocolo de *Ethernet* trabaja enviando la información del paquete a todos los hosts en el mismo circuito. La cabecera del paquete contiene la dirección apropiada de la máquina destino. Solamente la máquina con la dirección que va en la cabecera se supone que acepta el paquete (Cotton & Vegoda, 2013) (Czyz, y otros, 2013).

Además, mantener una constante supervisión permite considerar los malos funcionamientos y tomar medidas con respecto a la seguridad o a la calidad de las transmisiones de la información de manera oportuna; y siempre debe considerarse que habrá actividad anormal dentro de la red (Sanders, 2011). Dado que la mayor cantidad de información está en movimientos a través de las redes, es necesario monitorear el comportamiento de la red, y detectar el movimiento de los paquetes, dado que esto como unidades más pequeñas de datos, se convierten en elementos importantes y observar en tiempo real sus movimientos puede facilitar el descubrir comportamientos anómalos (Farid y otros 2010).

Una de las herramientas para análisis de tráfico en red utilizadas en la actualidad es la herramienta *Wireshark*, que es uno entre los diversos sniffers que se encuentran para la captura y análisis del tráfico en la red, su popularidad se debe a que cuenta con una interfaz gráfica que facilita la interpretación de la información capturada; *Wireshark* tiene la capacidad de "entender" los protocolos utilizados por la red mostrando información relevante para mostrar la manera como han viajado paquetes específicos dentro de la misma (Asrodia & Patel, 2012). A diferencia de otros *sniffers* como *TCPdump* no tiene una interfaz gráfica de usuario y no poder desplegar toda la información que concierne a un paquete en específico (Asrodia & Patel, 2012) lo que hace que *Wireshark* sea una herramienta apropiada para el análisis de tráfico de red (Hillar, 2004), no sólo por poseer una interfaz gráfica agradable para el usuario sino porque cuenta con la capacidad de identificar 1100 protocolos dentro de los establecidos para comunicaciones de red (Lan, Hussain, & Dutta, 2003; Duran & Iturriago., 2012) diferentes simplificando el trabajo de análisis por poseer filtros que permiten definir criterios para interpretar la información según el protocolo que se desee analizar (Merino, 2011).

3. METODOLOGÍA

La investigación será orientada de manera descriptiva dado que serán abordadas las características potenciales que tiene el analizador de red o sniffer Wireshark para la identificación de tráfico malicioso, poseerá un diseño experimental que permita ver el comportamiento de la herramienta en una red de área local (*LAN*) para establecer la capacidad de la misma para capturar paquetes y diseccionar sus peculiaridades, cuyo propósito es descubrir cómo puede aplicarse dichas particularidades para buscar amenazas en una red para proteger los recursos y la información de una empresa o entidad, entre los años de 2009 a 2015 (Rico Bautista, Edwin, & Carvajal Mora, 2011).

La revisión documental se realizó en revistas de alto impacto publicados en las bases de datos *AMJ, SCOPUS, SCIENCE DIRECT, SciELO, Directory of Open Access Journals (DOAJ), The National Academies Press, REDALYC, y LATINDEX*.

Como criterios de búsqueda, se incluyeron los siguientes descriptores: "analizadores de red", "*IPv6*", "seguridad", "*TCP/IP*". Estos descriptores fueron combinados de diversas formas al momento de la exploración con el objetivo de ampliar los criterios de búsqueda, en el período establecido.

Seguidamente se explican las distintas partes que implicó la revisión documental:

Identificación de bibliografía relevante
El inicio del proceso, consistió en realizar un rastreo documental en bases de datos especializadas, se preseleccionaron artículos y al final se seleccionaron cincuenta referencias, de acuerdo con los criterios de inclusión y exclusión. "No se tomaron en consideración para el análisis aquellos artículos que no hacían alusión a los núcleos temáticos y/o aquellos que no se encontraban en revistas indexadas". (Sánchez , 2011, p. 179)

Generación de áreas temáticas y tipologías
Como acto seguido, se analiza cada documento, se establecen sus áreas temáticas y tipologías, como punto de entrada del proceso de revisión. Partiendo de un formato elaborado en Word con los siguientes campos: título del artículo, autor, año, revista, información de la revista, problema de investigación, objetivos, tipo de investigación, método, descripción, instrumentos utilizados, resultados y núcleo temático. En este aparte, se pretendió identificar puntos de encuentro y diferencia de criterios entre los documentos clasificados que fundamentan la estructura de los ejes descritos para el presente artículo.

Interrelación entre artículos
En este aparte, se pretendió identificar puntos de encuentro y diferencia de criterios entre los documentos clasificados que fundamentan la estructura de los ejes descritos para el presente artículo. Este proceso derivó en un extenso, que tuvo que ser resumido para cumplir con los

lineamientos de publicación de artículos. Finalmente, se realizó un análisis global mediante el cual se identificaron las convergencias y divergencias del análisis de cada uno de los núcleos temáticos, se formularon ciertas hipótesis y conclusiones. (Sánchez , 2011, p. 180)

Las fases y las actividades que continúan son las siguientes:

Definir el diseño de una red para la implementación de la herramienta estudiada en el análisis de protocolos de red más comunes.

- Definir requerimientos de la red local
- Identificar servicios de red a implementar
- Construir la red de área local
- Establecer los servicios de la red

Documentar los hallazgos del uso del software Wireshark como una herramienta útil para la detección de tráfico malicioso aplicada a una red de área local (*Local Network Area, LAN*)

- Recolectar información de hallazgos
- Análisis de la informacion
- Redactar documento final

4. DISCUSIÓN

Los sistemas de comunicación con la rápida interacción que ofrecen al implementarse las nuevas tecnologías han marcado una gran diferencia en la manera como se recoge, transporta, almacena y procesa la información, lo que permite a las organizaciones establecerse en una zona geográfica mucho más amplia sin una gran inversión en infraestructura y conociendo con facilidad el estado de cualquier oficina con el solo hecho de presionar un botón. Esto es facilitado por el uso de computadoras dado que cualquier institución por pequeña posee una o dos de ellas (Tanenbaum & Wetrerall, 2011).

Para que exista comunicación debe establecerse una arquitectura que permita que los nodos que desean establecer un enlace puedan hacerlo sin ninguna complicación para lo cual deben establecerse “una serie de reglas o convenciones denominadas protocolo” (Stallings W. , 2004). Un ejemplo de éste tipo de comunicación son las redes telefónicas, que aún en la actualidad es una de las redes de mayor tamaño y una de las más importantes, que con la adopción de convenciones comunes entre los fabricantes que permite la integración de tecnologías diversas en un mismo entorno convierte la implementación de redes en una herramienta poderosa para transportar señales tanto analógicas como digitales.

Aunque todavía no se comprenden las implicaciones de su uso en la vida cotidiana. Algunas facetas que pueden verse perjudicadas son la privacidad y la seguridad de los datos almacenados por medios electrónicos (Tricas Garcia, 2004). La seguridad se convierte en una tarea intensiva que requiere ampliar la visión para reconocer el comportamiento de las redes y comprender su estado (Celeda, 2011).

Lo anterior, asumiendo que cada persona tenga un dispositivo electrónico, sin embargo, puede considerarse el caso de una gran empresa con miles de computadores. Si cada computador de dicha organización se conecta con el exterior es una oportunidad para los atacantes para buscar debilidades, romper las defensas y aprovechar los recursos que encuentran para sacar provecho (Braden, Clark, Crocker, & Huitema, 1994).

El responsable de la seguridad debe definir de manera sistemática los requisitos de seguridad y caracterizar los enfoques para satisfacer los requisitos propuestos (Stallings W. , 2004). Cuando se consideran sólo los beneficios y las ventajas sin considerar los posibles perjuicios como cuando la privacidad es vulnerada, porque al estar la información disponible de forma digital es fácil acceder a ella mientras alguien sepa cómo hacerlo (Tricas Garcia, 2004).

Dentro de todo el entramado complejo de las comunicaciones a través de redes de computadores el sistema queda reducido a su entidad más básica: el paquete. Quien permite el flujo de la comunicación a través de muchas réplicas de sí mismo para poder transmitir información. El paquete está contenido dentro de un segmento que contiene información como el protocolo usado, direcciones de destino etc. (Banerjee, Ashutosh, & Saxena, 2010)

Mediante el análisis de investigaciones previas relacionadas con el objeto de estudio, se presentan los siguientes ejes temáticos donde se generaliza, afirma y deduce cómo se relaciona la investigación con los resultados hasta el momento obtenidos.

4.1 Modelo *TCP/IP*

Establecer estándares es necesario debido a la complejidad que generan las comunicaciones; los estándares permiten normalizar las funcionalidades

en una arquitectura de comunicaciones. Para esto la Organización Internacional de Estandarización (ISO, *Internacional Organization for Standarization*) estableció dicha arquitectura conocida como el modelo de referencia OSI (Stallings W. , 2004). Con el mismo propósito se implementó otro modelo que fue desarrollado a nivel experimental en la red financiada por DARPA (*Defense Advanced Research Projects Agency*) denominado TCP/IP (*Transfer Control Protocol/Internet Protocol*) considerando las redes físicas interconectadas como una gran red (Forouzan, 2013).

El modelo de referencia *TCP/IP* es lo que hace que la comunicación sea posible entre dos computadores en cualquier lugar de una red. Aunque no es propiamente una arquitectura por niveles como un modelo de capas (por ejemplo, OSI) permite la interacción de diversos elementos de tecnología involucrados en la comunicación (Barceló Ordinas, Griera, Martí Escalé, Peig Olivé, & Perramon Tornil, 2004). Dado que el modelo está configurado en capas se le conoce como una pila de protocolos (Alvarez Crego, 2005). Los protocolos *TCP* son importantes para Para la clasificación del tráfico es importante para el transporte de archivos compartidos entre usuarios (Adibi, 2010).

Las redes generan su máximo de comunicaciones sobre el protocolo *TCP*. En el estudio realizado por (Razzak A., Handa, & Ramana Murthy, 2014) muestran como del tráfico total de una red, el protocolo *TCP* es usado mucho más que otros protocolos. Y es uno de los protocolos más fáciles de detectar porque establece una conexión a tres pasos y múltiples banderas (flags) para indicar el estado de los puertos (Kumar & Sudarsan, 2014). (Gupta & Mamtora, 2012) las identifican como sigue:

1. Envío de un bit *SYN* desde el host cliente al host servidor
2. Un bit *SYN+ACK* desde el host servidor al host cliente
3. Y finalmente, un bit *ACK* desde el host cliente al host servidor.

Los dos protocolos más representativos son el protocolo para el control de transmisión TCP (*Transmission Control Protocol*) y el protocolo de internet, *IP* (*Internet Protocol*).

La dirección *IP* es un elemento crucial para el funcionamiento de internet. Las direcciones *IP* tienen dos funciones primordiales: direccionar y enrutar. La primera es reconocer hacia quien se dirige y la segunda es saber cómo llegar a su destinatario. Las direcciones *IP* son asignadas a cada interfaz de red (router, computadores, teléfonos móviles, servidores, etc. (Levin & Schmidt, 2014).

La versión 4 de protocolo *IP* fue liberada en 1978 y llego a ser un estándar en 1981. Fue una de las primeras versiones que tuve un despliegue amplio. Teóricamente tenía capacidad para ofrecer 4.3 mil millones de direcciones únicas (Cicileo, y otros, 2009), de las cuales realmente pueden ser usadas como direcciones 3.7 mil millones por host de internet. Cuando crearon *IPv4* no podía imaginarse que habría una posibilidad de agotar tan basto recurso. Por la proyección de una gran demanda de direcciones comenzaron el desarrollo de un nuevo protocolo, *IPv6*, que tiene una cantidad inimaginable de direcciones: 340 sextillones de direcciones IP únicas (Levin & Schmidt, 2014).

Establecido el nuevo protocolo debe seguirse su adopción y promoción lo que significa un camino lento (Cicileo, y otros, 2009) (Hazeyama, Ueno, & Sato, 2011), dividido en múltiples etapas: En primer lugar, la IANA agoto sus direcciones IPv4 en febrero de 2011, luego los RIR (Registros regionales de internet) y por último las redes expandidas agotaron sus direcciones (Levin & Schmidt, 2014).

El conjunto de direcciones *IPv4* administrados por la IANA, está reduciendo su rango representativo, lo que indica que las direcciones de internet se están agotando. *IPv4* dispone de 4 mil millones de direcciones, pero por el uso generalizado de internet lo ha llevado a su agotamiento.

Con respecto, a la seguridad es mucho más robusto en el protocolo *IPv6*, dado que implementa de forma obligatoria los estándares IPsec (Patterson, 2006) para autenticar como por ejemplo cambiando proponiendo *header* (Kent, 2005) que autentica el paquete a medida que hace saltos a través de la red, aunque eso no significa una garantía contra los ataques que provengan de otras capas, porque según (Hunter, 2004) la creación de soluciones más robustas también crea problemas nuevos para el sistema. Dado que el manejo del flujo de la información para comprobaciones como *ICMP* o las direccione multicast permitirían ataques que incrementen el tráfico para generar la pérdida de servicios (Durdagi & Buldu, 2010) o un ataque MITM (*Man in the middle*, hombre en el medio).

Las direcciones *IP* están relacionadas de forma cercana con los servicios *DNS* (*Domain Name Servers*, Servidores de Nombre de Dominio) para ofrecer un mejor direccionamiento y optimización del tráfico (Braden, Clark, Crocker, & Huitema, 1994). Dado que ambos protocolos interactúan para ofrecer una mejor experiencia de usuario, comprender como los dos interactúan ofrece una mejor manera de resolver problemas de redes y de intrusiones, además dada la existencia de islas IPv4 que conviven con las direcciones IPv6 que ofrecen una mayor complejidad para el comportamiento de la red y afectan la manera como debe observarse el flujo de los datos (Berger, Weaver, & Beverly, 2013).

4.2 Intrusiones de red

Los usuarios de un sistema deben estar conscientes de que cualquier información puede ser vista por terceros y utilizada para sacar un beneficio o perjudicar a los propietarios de la información, todo sistema corre un riesgo.

Existen diferentes amenazas que pueden hacer una intrusión en los sistemas computarizados como los virus, que son programas que pueden infectar a otros modificándolos para incluir una copia de sí mismos. O los gusanos que se reproduce de forma similar a un virus, pero no necesita de otros programas para retransmitirse. Y así entre otros bichos que pueden afectar los recursos o recolectar la información dando acceso a los recursos del sistema para ser utilizado por el creador del software malicioso (Tricas Garcia, 2004).

Entonces reconocemos que las intrusiones en las redes son un intento de acceso no autorizado para falsificar, cambiar o destruir información que hacen que un sistema sea poco confiable (Rastegari, Hingston, & Lam, 2015). Con el avance de las redes de computadoras la taza de intrusiones aumenta cada año. Por lo cual es necesario un proceso que permita identificar las acciones que atente con comprometer la confidencialidad, la integridad o la disponibilidad (CID) de las computadoras o las redes.
Farid y otros (2010) expresa que en una red es necesario recolectar información de las IP de las redes en búsqueda de intrusos que intenten penetrar en la red, para lo cual es necesario:

1) monitorear el uso de los servicios de la red por parte de los usuarios,
2) acceder a las configuraciones del sistema,
3) reconocer los ataques conocidos,
4) identificar actividad anormal,
5) corregir errores de configuración del sistema y
6) almacenar información acerca de los intrusos

(Banerjee, Ashutosh, & Saxena, 2010) recuerda que fue a comienzos de 1980 cuando comienza a acuñarse la noción de detección de intrusiones, con un reporte ofrecido por James Anderson que proponía la recolección de datos para hacer un seguimiento diario a través del análisis y así llevar un registro detallado a través de los años (Anderson, 1980). El registro permitiría entender los desvíos y comportamientos de una red por medio del análisis de patrones para buscar "una aguja en un pajar", lo que genera preocupación en un administrador de red porque es difícil establecer un análisis de todos y cada uno de los datos que se transmiten, sin embargo, la labor es necesaria porque siempre debe considerarse que habrá actividad anormal dentro de la red (Sanders, 2011).

(Abad, Li, Lakkaraju, Yin, & Yurcik, 2004), reconocen que la preocupación por una evaluación de la red no solo debe ser motivada por el mejoramiento del funcionamiento de la red y las características del ancho de banda de la misma, sino que debe permitir la visualización de las intrusiones, a partir del reconocimiento del comportamiento de los usuarios y descubrir los malos usos que de otra manera serían ignorados.

¿Cómo obtener información de la red para poder observar su proceso de tráfico de información? Para eso fueron creados los analizadores de red (*Packet sniffings)* que ofrecen una a técnica de monitoreo para cada paquete que transita por una red y así reconocer las posibles amenazas para la seguridad (Herrera, Alfaro, & Perramón, 2004).
Dado que cuando se envían datos a través de la red, es enviada en la forma de paquetes. Estos paquetes son trozos de la información que está dirigida a un sistema designado, por realmente todos los datos tienen un punto predefinido hacia el cual se dirigen (Asrodia & Patel, Analysis of various packet sniffing tools for network monitoring and analyis, 2012). Los paquetes desde su origen hasta su destino pasan por muchos dispositivos intermedios.

Los *sniffer* aprovechan una "falla" del sistema Ethernet, dado que cuando un sistema un paquete a un sistema, sólo el host al cual va dirigido puede ver su contenido dado que es identificado a través de su *NIC*, que primer compara la dirección *MAC* del paquete con la del equipo. Si la *MAC* concuerda, acepta el paquete sino lo descarta. Esto

es debido a que la tarjeta de red descarta todos los paquetes que no contenta la dirección *MAC* que la identifica, esta operación es llamada no promiscua, lo que significa que la tarjeta solo se ocupa de sus propios paquetes para leer aquellos que dirigen directamente hacia ella. Aunque la *NIC* puede ser configurada para recibir todos los paquetes para lo cual debe ser configurada en modo promiscuo para que así todos los paquetes lleguen al computador. Y esto usado por los *sniffer* para poder capturar los paquetes que transitan por una red.

Los *Packet sniffers* no son sólo herramientas para hacker. Pueden ser usados para monitorear el tráfico, solucionar problemas de la red y otros propósitos. Los analizadores de red pueden ser usados para capturar contraseñas, nombres de usuario, y cualquier información sensitiva que transite por una red. Aunque es aplicar un analizador de red a una red switcheada no es tan fácil dado que estrecha el tráfico y elige un sistema particular al cual enviar los datos, lo que requiere de algunos métodos.

Componentes básicos de un sniffer.

1. El hardware. La mayoría de los productos trabajan en adaptadores standard de red, algunos pocos requieren hardware especial.
2. Controladores (drivers) de captura. La parte más importante. Cuando captura el tráfico de la red de un cable, lo filtra y lo almacena los datos en un buffer.
3. Buffer. Es un dispositivo de almacenamiento que captura los datos desde la red. Hay dos tipos de buffer. El primero es cuando los datos son capturados de forma continua y el segundo cuando los nuevos paquetes reemplazan los viejos paquetes. (Asrodia & Sharma, 2013)
4. Decodificación. Muestra el contenido del tráfico de red con texto descriptivo para permitir el análisis y reconocer lo que ocurre. (Asrodia & Patel, 2012)

La meta de las herramientas para captura de paquetes es detectar comportamientos anómalos y malos usos. Conocer el origen de incidente en una red es necesario para tomar las contramedidas necesarias y conseguir una protección adecuada.

Una posible definición del análisis de tráfico de red: “el proceso de escuchar y analizar el tráfico, para tener una comprensión dentro de las redes de comunicación para identificar comportamientos anómalos, quiebres en la seguridad, analizar el funcionamiento de las aplicaciones y construir planes de acción, todo esto llevado por profesional de las tecnologías de la información que se responsabiliza por el funcionamiento de la red y su seguridad” (Chappel, 2012)

Un análisis debe ofrecer formas de observar los comportamientos inusuales en el volumen de la transferencia de bytes o paquetes y poder examinar los incidentes sospechosos con herramientas especializadas como los analizadores de paquetes, recolectores de flujo, firewalls y registros del sistema. En consecuencia, pueda tenerse un cuidado situacional para conocer los detalles del tráfico a través de estadísticas, para tener un nivel de conocimiento apropiado. (Celeda, 2011)

Llevar un registro del comportamiento de la red permite construir un modelo que permita predecir el comportamiento de la red para poder descubrir discrepancias que puedan ser identificadas como un posible ataque. La seguridad es una de las preocupaciones primarias de los usuarios al transmitir información a través de una red. La seguridad implica conservar los paquetes que por ella transitan.

Uno de los analizadores más populares en la actualidad es *Wireshark*. Fue desarrollado por Gerald Combs (Borja Merino, 2011). Tiene ricas y poderosas características, corre sobre cualquier plataforma: Windows, OS X, Linux and UNIX. Dado que es de fuente abierto es sostenido y desarrollado por un equipo global de expertos. Además, no sólo funciona sobre redes cableadas, sino que permite capturar al tráfico “desde el aire” dado que soporta los protocolos Wireless.

(Banerjee, Ashutosh, & Saxena, 2010), señalan que la sofisticación de la herramienta al permitir a los administradores, profesionales de las redes y expertos en seguridad captura de paquetes “a través de la red sobre una interfaz de red particular en un tiempo específico”, que permiten aproximarse a los comportamientos de una red y descubrir inconvenientes que causan bajo desempeño, conectividad intermitente y otros problemas comunes en las redes.

La herramienta implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para más de 1000 protocolos soportados. La interfaz es intuitiva y sencilla permitiendo

observar con facilidad las capas que conforman un paquete. Wireshark "entiende" la estructura de los protocolos. Wireshark ofrece dos lenguajes: uno usado para la captura de paquetes y otro para su visualización. El administrador de una red puede concentrarse en aquellos paquetes por los cuales se interesa más y ocultar aquellos que no son necesarios. El criterio de selección puede ser múltiples: protocolos, campos, valores del campo, comparaciones, etc. Wireshark tiene un campo de búsqueda que permite insertar los criterios de filtrado

4.3 Análisis de una red en un entorno IPv6

Siempre habrá intrusos que quieran hacerle daño los recursos de un sistema por lo cual es necesario conocer el sistema y conocer las maneras como puede ser vulnerado, además los atacantes cada vez usan medios más sofisticados y puede introducirse manera anónima para esconder sus ataques (McClure et al, 2012).

Para establecer medidas apropiadas de seguridad que garanticen la seguridad de la información debe establecerse el uso de herramientas apropiadas para implementar medidas acertadas (Braden, Clark, Crocker, & Huitema, 1994). Es necesario reconocer que la seguridad no se reduce a utilizar herramientas preestablecidas que impidan que cualquier actividad sospechosa pueda ser evitada corriendo con el riesgo de aislarse del flujo de la información, sino de la imaginación de los administradores de red que estén en constante vigilancia e investigación sobre los recursos de la organización y las posibilidades de construir ambientes de red más seguros.

Con la transición de los protocolos IPv4 a IPv6 es necesario un análisis constante de la red con herramientas como los *sniffers* permite que la seguridad se vaya fortaleciendo cada vez más, ya que al identificar anomalías en el funcionamiento de la red se pueden aplicar los correctivos que sean necesarios. Aunque las nuevas disposiciones de los protocolos de internet son mucho más seguras nunca hay garantía para estar exentos de un ataque.

4. CONCLUSIONES

Biswas & Ashutosh (2014) declaran que: "conocer la Fuente del ataque es uno de los primeros pasos para tomar acciones apropiadas y lograr protección adecuada. Ahí es cuando los analizadores de red son extremadamente útiles para detectar, analizar y mapear el tráfico. Así pues, los analizadores de red identifican amenazas hacia la red y limitan sus efectos dañinos"

De acuerdo a los resultados obtenidos a partir del análisis de los artículos referenciados sobre las intrusiones de red, se genera que se deben establecer medidas apropiadas de seguridad que garanticen la seguridad de la información e integrar el uso de herramientas apropiadas para implementar medidas acertadas.

RECONOCIMIENTO

La Universidad Francisco de Paula Santander Ocaña (UFPSO), mediante la División de Investigación y Extensión (DIE) vincula a docentes, administrativos y estudiantes para que participen en la ejecución y desarrollo de proyectos de investigación. Este articulo muestra resultados de la primera fase de un proyecto inscrito, avalado y financiado en dicha dependencia:

"*Seguridad en redes*", propuesto a través del *Grupo de Investigación en Ingenierías Aplicadas* (INGAP), y a su Semillero de Investigación *GNU/Linux And Security* (SIGLAS).

REFERENCIAS

Abad, C., Li, Y., Lakkaraju, K., Yin, X., & Yurcik, W. (2004). Correlation between NetFlow System and Network views of Intrusion Detection. *Workshop on Link Analysis, Counter-terrorism, and Privacy held in conjunction with SDM*. Minneapolis, MN. doi:10.1.1.5.2004

Adibi, S. (2010). Traffic classification - Packet-, Flow-, and Application-based Aproaches. *International Journal of Advanced Computer Science and Applications (IJACSA), 1*(1), 6-15.

Alvarez Crego, M. (2005). *Analizador de red (sniffer) en entorno GNU*. UOC La universidad virtual. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/551/1/35037tfc.pdf

Anderson, J. (1980). *Computer Security threat monitoring*. Fort Washington, PA. Obtenido de http://csrc.nist.gov/publications/history/ande80.pdf

Asrodia , P., & Patel, H. (2012). Analysis of various packet sniffing tools for network monitoring and analyis. *International Journal of Electrical,Electronics and Computer Engineering, 1*(1), 55-58. Obtenido de

http://www.researchtrend.net/pdf/13 PALLAVI.pdf

Asrodia, P., & Patel, H. (May-Jun de 2012). Network Traffic Analysis Using Packet Sniffer. *International journal of engineering research and applications, 2*(3), 854-856. Obtenido de www.ijera.com/papers/Vol2_issue3/EQ23854 856.PDF

Asrodia, P., & Sharma, V. (May de 2013). Network Monitoring and analysis by Packet Sniffing Method. *International Journal of Engineering Trends and Technology (IJETT), 4*(5), 2133-2135. Recuperado el 22 de Agosto de 2015, de http://www.ijettjournal.org/volume-4/issue-5/IJETT-V4I5P160.pdf

Banerjee, U., Ashutosh, V., & Saxena, M. (2010). Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of computer applications, 6*(7), 1-5. Obtenido de http://ijcaonline.net/archives/volume6/number 7/1092-1427

Barceló Ordinas, J., Griera, J. I., Martí Escalé, R., Peig Olivé, E., & Perramon Tornil, X. (2004). *Redes de Computadores* (1ra ed.). Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Berger, A., Weaver, N., & Beverly, R. (2013). Internet Nameserver IPv4 and IPv6 address Relationships. (págs. 91-104). New York, NY: Association for Computing Machinery (ACM). doi:10.1145/2504730.2504745

Biswas, J., & Ashutosh. (May de 2014). An Insight in to Network Traffic Analysis using Packet Sniffer. International Journal of Computer Applications, 94(11), 39-44. Obtenido de https://www.academia.edu/7847043/An_Insig ht_in_to_Network_Traffic_Analysis_using_P acket_Sniffer

Borja Merino, F. (2011). *Análisis de tráfico con Wireshark.* Madrid: Inteco_cert. Recuperado el 29 de Junio de 2015, de https://www.incibe.es/extfrontinteco/img/File/ intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Braden, R., Clark, D., Crocker, S., & Huitema, C. (1994). *Security in the internet Architecture.* IETF.

Celeda, P. (07 de Septiembre de 2011). Network Security Monitoring and behavior analysis. 28. Obtenido de http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd133.pdf

Chappel, L. (2012). *Wireshark Network Analysis.* San Jose CA: Protocol Analysis Institute.

Cicileo, G., Gagliano, R., O´flaherty, C., Olvera Morales, C., Palet Martinez, J., Rocha, M., & Vives Martinez, Á. (2009). *IPv6 para todos, Guía de uso y aplicación para diversos entornos.* Buenos Aires: Asociación Civil Argentinos en Internet. Obtenido de http://www.consulintel.es/pdf/ipv6paratodos. pdf

Cotton, M., & Vegoda, L. (2013). *Special-Purpose IP address Registries.* Internet Engineering Task Force. Obtenido de http://tools.ietf.org/pdf/rfc6890

Czyz, J., Lady, K., Miller, S., Bailey, M., Kallitsis, M., & Karir, M. (2013). Understanding IPv6 Internet Background radiation. Proceedings of the measurement conference (págs. 105-118). New York: ACM. doi:101145/2504730.2504732.

Durán Acevedo Christian M, Iturriago Ali Xavier. (2012). Automatización de un Sistema de Suministro de Agua Potable a Través de la Tecnología Zigbee. Revista colombiana de tecnologías de Avanzada 1 (19), Pág. 36 – 42.

Durdagi, E., & Buldu, A. (2010). IPv$/IPv6 security and threat comparisons. *Procedia Social and Behabvioral Sciences, 2*, 5285-5291. doi:10.1016/j.sbspro.2010.03.862

Farid, D., Harbi, N., Zahidur Rahman, M., & Mofizur Rahman, C. (2010). Attacks Classification in Adaptive Intrusion Detection using Decision Tree. *World Academy of Science, Engineering and Technology, 39*, 86-90. Obtenido de http://waset.org/publications/5652/attacks-classification-in-adaptive-intrusion-detection-using-decision-tree

Forouzan, B. (2013). *Transmisión de datos y redes de comunicaciones* (5ta ed.). Madrid: Mcgraw Hill/Interamericana.

Gupta, S., & Mamtora, R. (Noviembre de 2012). Intrusion Detection System Using Wireshark. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*(11), 358-363. Obtenido de http://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012/V2I11-0205.pdf

Hazeyama, H., Ueno, U., & Sato, H. (2011). How much can we survive on an IPv6 network? *Proceedings of the 7th Asian Internet Engineering Conference (AINTEC '11)* (págs. 144-151). New York: ACM. Obtenido de http://www.wide.ad.jp/project/document/repo

rts/pdf2011/cd/02-3_wide-memo-camp1109-hack-v6only-questionnaire-01.pdf

Herrera Joancomartí, J., Alfaro Garcia, J., & Perramón Tornil, X. (2004). *Aspectos avanzados de seguridad en redes.* Barcelona: Fundación por la Universitat Oberta de Catalunya. Obtenido de http://www.sw-computacion.f2s.com/Linux/012.1-Aspectos_avanzados_en_seguridad_en_redes_modulos.pdf

Hillar, G. (2004). Redes: diseño y actualización y reparación (5ta ed.). Buenos Aires: Editorial Hispano Americana S.A.

Hunter, P. (2004). IPv6: Security Issues. Network Security, 2004(1), 17-19. doi:10.1016/S1353-4858(04)00026-1

Katz, M. (2013). Redes y seguridad (1ra ed.). Buenos Aires: Alfa-Omega Grupo Editor Argentino.

Kent, S. (2005). IP Authentication Header. IETF. doi: http://dx.doi.org/10.17487/RFC4302

Kumar, S., & Sudarsan, S. (Dec de 2014). An Innovative UDP port Scanning Technique. International Journal of Future Computer and Communication, 3(6), 381-384. doi:10.7763/IJFCC.2014.V3.332

Lan, K.-c., Hussain, A., & Dutta, D. (2003). Effect of Malicious Traffic on the Network. doi:10.1.1.12.4873

Levin, S., & Schmidt, S. (2014). IPv4 to IPv6: Challenges,solutions and lessons. Telecommunications Policy, 38, 1069-1068. doi:doi:10.1016/j.telpol.2014.06.008

Merino, F. B. (2011). Análisis de Tráfico con Wireshark. Madrid: INTECO. Recuperado de: http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_Wireshark.pdf McClure, S., Scambray, J., & Kurtz, G. (2012). Hacking Exposed 7 (7ma ed.). New York: McGraw-Hill .

Patterson, K. (2006). A criptographic tour of the IPsec standards. Information Security Technical Report, 11(2), 72-81. doi:10.1016/j.istr.2006.03.004

Rastegari, S., Hingston, P., & Lam, C.-P. (2015). Evolving statistical rulesets for network intrusion detection. Applied Soft Computing, 33, 348-359. doi:10.1016/j.asoc.2015.04.041

Razzak A., H. A., Handa, S., & Ramana Murthy, M. (Jun de 2014). Providing the Secure Data Transmission in the Network Using Open Source Packet Analyzer. International Journal of Computer trends and Technology (IJCTT), 12(1). doi: 10.14445/22312803/IJCTT-V12P103

Rico Bautista, D. W., Edwin, Q. H., & Carvajal Mora, H. R. (2011). Redes y tecnologías de banda ancha. Tecnologías de acceso de banda ancha. Revista Tecnologias de Avanzada, 1(17), 113–120.

Sánchez, A. (2011). Manual de redacción académica e investigativa: cómo escribir, evaluar y publicar artículos. Medellin, Antioquia, Colombia: Fundación Universitaria Católica del Norte.

Sanders, C. (2011). *Practical Packet Analisis.* New York: No Starch Press Inc. Obtenido de http://repository.root-me.org/R%C3%A9seau/EN%20-%20Practical%20packet%20analysis%20-%20Wireshark.pdf

Stallings, W. (2004). *Comunicaciones y redes de computadores.* Madrid: Pearson Educación S.A.

Stallings, W. (2007). *Data and computer communications* (8va ed.). Upple Saddle River: Pearson Education, Inc.

Stallings, W. (2011). *Network security essentials applications and standards.* Prentice Hall.

Tanenbaum, A., & Wetrerall, D. (2011). *Computer networks* (5ta ed.). Massachusetts: Pearson Education Inc. Obtenido de http://cse.hcmut.edu.vn/~minhnguyen/NET/Computer Networks - A Tanenbaum - 5th edition.pdf

Tricas Garcia, F. (2004). Etica y Seguridad en la red. *Uninet*, 1-13. Obtenido de http://doctorado.uninet.edu/2004/cinet2004/ftricas/seguridadYPrivacidad.pdf

Villalón Huerta, A. (2002). *Seguridad en UNIX y redes.* Cuenca: GNU Free Documentation License. Recuperado el 15 de Mayo de 2015, de https://www.rediris.es/cert/doc/unixsec/unixsec.pdf