RESUMEN TRABAJO DE GRADO

AUTORES	**SERGIO ALBERTO ALVERNIA ACEVEDO**
FACULTAD	**INGENIERIAS**
PLAN DE ESTUDIOS	**INGENIERIA DE SISTEMAS**
DIRECTOR	**M.Sc. DEWAR RICO BAUTISTA**
TÍTULO DE LA TESIS	**WIRESHARK:COMO HERRAMIENTA DE APOYO PARA EL ANALISIS DE TRÁFICO MALICIOSO EN UNA RED DE AREA LOCAL**

RESUMEN

LAS REDES DE COMPUTADORAS AYUDAN A LAS ORGANIZACIONES A ESTRUCTURAR LAS ACTIVIDADES DE LA MISMA PARA QUE EXISTA UNA COMUNICACIÓN MUCHA MÁS EFICIENTE ENTRE LAS DEPENDENCIAS QUE LA CONFORMAN, PARA LO CUAL ES NECESARIO MANTENER UNA VIGILANCIA CONSTANTE SOBRE LA INFRAESTRUCTURA UTILIZADA PARA PODER SUSTENTAR LA INTEGRIDAD DE LA INFORMACIÓN. CON ÉSTE PROPÓSITO PLANTEAMOS EL USO *WIRESHARK* COMO UNA HERRAMIENTA QUE PERMITA LLEVAR UNA CONSTANTE SUPERVISIÓN DE LA RED QUE POSIBILITE EL ANÁLISIS DEL TRÁFICO DE RED PARA DETECTAR CUALQUIER ACCIÓN MALICIOSA QUE QUIERA HACER UN INTRUSO EN LA RED PARA AFECTAR EL FUNCIONAMIENTO DE ÉSTA.

CARACTERÍSTICAS

PÁGINAS: 82	PLANOS:	ILUSTRACIONES:	CD-ROM:

WIRESHARK: COMO HERRAMIENTA DE APOYO PARA EL ANALISIS DE TRÁFICO MALICIOSO EN UNA RED DE AREA LOCAL

SERGIO ALBERTO ALVERNIA ACEVEDO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
OCAÑA
2016

WIRESHARK: COMO HERRAMIENTA DE APOYO PARA EL ANALISIS DE TRÁFICO MALICIOSO EN UNA RED DE AREA LOCAL

SERGIO ALBERTO ALVERNIA ACEVEDO

Trabajo de Grado presentado para optar al título de Ingeniero de Sistemas

Director
DEWAR WILMER RICO BAUTISTA
Magister en Ciencias Computacionales

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
OCAÑA
2016

A mis padres JOSE DANIEL ALVERNIA QUINTERIO Y NUBIA ACEVEDO SUAREZ que aceptaron la invitación para criarme y siempre darme lo mejor de sí mismos.

AGRADECIMIENTOS

A la Vida que en algún punto permitió que dos personas se encontrarán y me permitieran disfrutar de este recorrido.

A Dewar Wilmer Rico Bautista, por el acompañamiento en esta travesía y su dedicación para que este trabajo llegara a buen puerto.

A la UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, por brindarme en la infraestructura para desarrollarme como persona al servicio de la región.

A la facultad de Ingenierías, y al plan de estudios de Ingeniería de Sistemas, por darme la oportunidad de ser un profesional y brindarme el soporte mi formación.

A los jurados del proyecto por la dedicación en el desarrollo y mejora del presente trabajo.

A mi novia BRODNY ANDREA GARCIA MARQUEZ por estar apoyándome para alcanzar mis metas.

A mi amigo Diego por mostrarme que siempre se puede avanzar.

Y un agradecimiento a todos los que siempre han brindado su apoyo y su amistad.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCION

Mantener la seguridad de la información que circula por una red es una prioridad para toda organización, dado que la mayoría de las actividades realizadas en el momento actual están relacionados con una red de computadores, y principalmente con la red de redes que es Internet. Por lo cual es importante mantener la preocupación centrada en las transmisiones que ocurren dentro de la red para evitar posibles ataques o malfuncionamiento que puedan afectar el desempeño de la una organización.

En consecuencia, es necesario reconocer el tráfico de una red para reaccionar ante las operaciones inusuales y anormales. Una manera de conocer cómo funciona la red normalmente es usando un *sniffer* o analizador de red en varios puntos de la red.

Una de las herramientas para análisis de tráfico en red utilizadas en la actualidad es la herramienta *Wireshark*, que ha tenido una creciente popularidad debido a su interfaz gráfica que facilita la lectura y la interpretación de la información de los paquetes capturados; *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. Por lo tanto, el uso de la herramienta podría facilitar el descubrimiento de los riesgos y amenazas que generan inconvenientes en el funcionamiento de una organización.

1. WIRESHARK: COMO HERRAMIENTA DE APOYO EN UNA RED DE ÁREA LOCAL PARA EL ANÁLISIS DE TRÁFICO MALICIOSO

1.1 PLANTEAMIENTO DEL PROBLEMA

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 permitían la eficiencia de los recursos de las máquinas que empezaron a construir para mejorar las comunicaciones y permitir que la manera como ésta se compartía para beneficiar a muchas más personas al mismo tiempo expuso a los usuarios a amenazas como la pérdida de los datos o la falta de control sobre los programas que usaban[1].Sin embargo los usuarios desean, junto con la rapidez de los sistemas, conservar la información protegida de otros individuos ajenos a la misma (Confidencialidad), mantenerla idéntica en el tiempo y en el espacio (integridad) y acceder a ella en cualquier momento (disponibilidad)[2] principios básicos de la seguridad de la información.

Es necesario estudiar el comportamiento de los datos en la red para saber cómo tratarlos apropiadamente, por lo cual debemos reparar en las unidades más pequeña de las comunicaciones: "los paquetes de datos que son las entidades básicas de todo sistema de comunicación"[3]. Para reconocer el comportamiento de los paquetes requerimos de una constante revisión de lo que sucede con los paquetes cuando viajan a través de una red, y a partir de ese análisis generar medidas que ayuden a la detección de intrusiones[4].

---

[1]BRINKLEY, Roger. R & SCHELL, Donald. L. (). *Information Security: An Integrated Collection of Essays.* (A. D. Marshal, S. Jajodia, & H. J. Podell, Eds.) Los Alamitos, California, USA: 1995. IEEE Computer Society Press. Annual Computer Security Applications Conference: [En línea] http://www.acsac.org/secshelf/book001/book001.html [citado en 14 de Octubre de 2014]

[2] KRUTZ, R. L., & VINES, R. D. (2007). *The CEH prep guide: The comprehensive guide to certified ethical hacking.* Indianapolis, Indiana, Estados Unidos de América: Wiley Publishing, Inc.

[3] BANERJEE, Usha, ASHUTOSH, Vashishtha & SAXENA, Mukul. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of computer applications, 6*(7), 1-5. 2010 [En línea] http://ijcaonline.net/archives/volume6/number7/1092-1427 [citado en 14 de Octubre de 2014]

[4]GONZALEZ, Diego,[En línea] dgonzalez.net: http://dgonzalez.net/pub/ids/IDS_v1.0.pdf [Citado el 21 de octubre de 2015]

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, recibió el nombre Procesamiento de Datos Electrónicos (*Electronic Data Processing, EDP*)[5].Dentro de los pioneros de los sistemas de detección de intrusiones en la década de 1970 el Departamento de Defensa de los Estados Unidos, quien acuñó el concepto de "sistemas de confianza", propuso la Iniciativa de Seguridad en 1977 que dispone los criterios necesarios sobre un sistema seguro[6]. Estos primeros estándares proponen la importancia de ofrecer criterios que deben ser considerados por los usuarios para fortalecer los controles de seguridad que se construyan para mantener protegido a un sistema[7].

La importancia del seguimiento de los rastros de los datos fue establecida por James Anderson quien define la manera cómo llevar los registros de los comportamientos de los datos, para permitir saber si hay amenazas en el sistema, para lo cual requiere de un entendimiento apropiado de estas [8] [9]. Desde este punto es significativo la recopilación de información de una red a través de la captura de los paquetes (*packet sniffing*) que transitan por ella 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 conocen como *packet sniffers* [10] [11]

Una de las herramientas más populares usadas para la captura de información que permite una disección de los protocolos es *Wireshark*, una aplicación de software libre, capaz de identificar más de 1200 protocolos, descifrando la estructura de cada uno de ellos, permite al

---

[5] Ibíd.

[6] BRINKLEY, Op. cit.

[7] DEPARTMENT OF DEFENSE. *Trusted Computer System Evaluation Criteria [the "Orange Book"]*. Ft. Meade, 1985 MD: National Computer Security Center. [En línea] http://csrc.nist.gov/publications/history/dod85.pdf [citado en 14 de Octubre de 2014]

[8] BANERJEE, Op. Cit.

[9] ANDERSON, James. *Computer Security Threat Monitoring and Surveillance.* Fort Washington:1980 [En línea] http://csrc.nist.gov/publications/history/ande80.pdf [citado en 14 de Octubre de 2014],.

[10] BISWAS, Jhilam & ASHUTOSH, Vashishtha. An Insight in to Network Traffic Analysis using Packet Sniffer. *International Journal of Computer Applications, 94*(11), 39-44. 2014 [En línea] https://www.academia.edu/7847043/An_Insight_in_to_Network_Traffic_Analysis_using_Packet_Sniffer [citado en 14 de Octubre de 2014]

[11] GUPTA, Shilpi & MAMTORA, Roopal. Intrusion Detection System Using Wireshark. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*(11), 358-363. 2012 [En línea] http://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012/V2I11-0205.pdf [Citado el 10 de Noviembre de 2015]

usuario identificar campos relevantes que ofrecen información sobre cada paquete que es capturado[12] [13].

Comprender que el buen funcionamiento de una red de computadoras no se reduce sólo a la 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.

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.

1.2 FORMULACIÓN DEL PROBLEMA

Observando la preocupación que se ha dado desde la década de los 70 hasta ahora en los comienzos del siglo XXI, queda la preocupación por utilizar herramientas que permiten la recopilación de información porque facilitan la observación de los comportamientos del tráfico en una red. ¿*Wireshark* como herramienta ofrece las capacidades para un análisis que permita identificar amenazas para un sistema y de esta manera tomar decisiones apropiadas para las necesidades de la red?

---

[12] OREBAUGH, Angela; RAMIREZ, Gilbert; BURKE, Josh; PESCE, Larry; WRIGHT, Joshua & MORRIS, Greg . Wireshark and Ethereal, Network Protocol Analyzer toolkit. Rockland, 2007 Syngress Publishing Inc. [En línea] http://numenor.cicese.mx/cursos/PSR/Wireshark-book.pdf [Citado el 10 de Septiembre de 2015]

[13] ASRODIA , Pallavi & PATEL, Hemlata. Analysis of various packet sniffing tools for network monitoring and analysis. *International Journal of Electrical,Electronics and Computer Engineering, 1*(1), 55-58. 2012. [En línea] http://www.researchtrend.net/pdf/13 PALLAVI.pdf [citado en 12 de Octubre de 2014],

1.3 OBJETIVOS

1.3.1 General

Implantar las funciones de captura y filtrado de *Wireshark* para el apoyo en una red de área local para el análisis de tráfico malicioso.

1.3.2 Específicos

- Elaborar un Estado del Arte sobre las funciones de la herramienta Wireshark para la monitorización de las redes.
- Definir el diseño de una red para la implementación de la herramienta estudiada en el análisis de protocolos de red más comunes
- 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)

1.4 JUSTIFICACIÓN

El propósito de la siguiente investigación es generar un documento que recoja los hallazgos hechos a través de la revisión de la literatura existente sobre el uso actual que hacen de los analizadores de paquetes, en particular de aquel conocido como *Wireshark*, para sus aplicaciones en el análisis de tráfico para evaluar sus posibilidades como una herramienta para el control del tráfico malicioso, al observar su comportamiento en un entorno controlado de laboratorio. Biswas, Jhilam., y Ashutosh, Vashishtha[14] 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".

[14]BISWAS, Op. cit.

Teniendo en consideración los criterios de utilidad definidos en Tecnológico de Monterrey[15] para que una investigación pueda satisfacer la resolución de un problema, definimos las siguientes expectativas a cumplir:

- Conveniencia: Buscamos plantear el uso de la herramienta *Wireshark* para garantizar una mejor seguridad en las redes de computadoras.

- Relevancia social: Al ofrecer una manera de proteger la información pretendemos sembrar el deseo de salvaguardarla de modos más apropiados.

- Implicaciones prácticas: Buscamos brindar elementos para una mejor estimación de los procesos que se realizan cuando se conservan y se transmiten datos.

- Valor teórico: Consideramos que al evaluar la aplicación de la herramienta *Wireshark* sería útil para futuras investigaciones, además de dedicar recursos para un ítem tan importante de las redes como la seguridad, dado que uno de los primeros pasos para aportar medidas pertinentes a la recolección de datos.

1.5 DELIMITACIONES

1.5.1 Geográfica.

La investigación estará circunscrita a la red de área local del laboratorio del Semillero de Investigación GNU/Linux And Security (SIGLAS) de la Universidad Francisco de Paula Santander seccional Ocaña.

1.5.2 Temporal.

La duración de la investigación será de 24 semanas (8 meses calendario) donde para permitir generar procesos de observación de la herramienta *Wireshark.*

[15] Tecnológico de Monterrey. *Planer y construir borradores*. Obtenido de Crea: Centro de recursos para la escritura académica: [En línea] http://sitios.ruv.itesm.mx/portales/crea/planear/como/planteamiento_tesis.htm [citado el 24 de noviembre de 2014]

1.5.3 Conceptual.

La investigación tendrá en cuenta los conceptos existentes referidos a la seguridad en las redes de computadores, considerando como las amenazas existentes pueden afectar el funcionamiento de una red; lo importante en la transmisión de los datos a través de la red por lo cual es necesario reconocer el comportamiento de los datos en las diferentes capas según el modelo TCP/IP concentrándonos en la capa de transporte y los protocolos usados para empaquetar los datos en dicha capa. La importancia de los analizadores de tráfico (*packet sniffers*) para la recolección del tráfico y su aplicación para la seguridad de una red.

2. MARCO REFERENCIAL

2.1 MARCO HISTORICO.

La preocupación por llevar un registro de las actividades en medios electrónicos surge en 1950 cuando las empresas de teléfonos Bell ("*Bell Telephone System*") determinaron que era necesario procesar los datos electrónicos (*Electronic Data Process*, EDP) para llevar un registro de las actividades de la empresa. Al comienzo de la década de los 70 el departamento de defensa de los Estados Unidos determina directrices y pautas para el control que permitiera generar sistemas de confianza[16].

Con el deseo de usar las múltiples utilidades de las nuevas tecnologías, crearon en el año 1970 grupos especializados conocidos como *penetration tiger teams* con la tarea de evaluar la protección ofrecida por los sistemas operativos, siendo penetrados con facilidad. En 1979 se publica un reporte procedente de la Conferencia Nacional de Computadores (*National Computer Conference)* afirmando que no existía en el momento un producto comercial que garantizara la protección apropiada a los usuarios[17].

James Anderson, unos de los pioneros en la definición en la detección de intrusiones, propone en 1980 el ensayo *Computer Security Threat Monitoring and Surveillance* que buscaba seguir el rastro de información valiosa, por lo cual buscaba la manera de entender los comportamientos de los usuarios[18]. Anderson consideraba que la información de los que los clientes eran guardados en un centro especial, que mantiene este registro que permitía la revisión de los mismos[19].

En 1985, incluyen en el documento "*Trusted Computer System Evaluation Criteria*" mejor conocido como "libro naranja" un apartado para la definición de sistemas de confianza (González, 2010), como la base para abordar los objetivos y los requerimientos que debería perseguir los controles efectivos de seguridad[20].

---

[16] GONZALEZ, Op. cit.

[17] BRINKLEY, Op. cit.

[18] BANERJEE, Op. cit.

[19] ANDERSON, James. *Computer Security Threat Monitoring and Surveillance.* Fort Washington:1980 [En línea] http://csrc.nist.gov/publications/history/ande80.pdf [citado en 14 de Octubre de 2014]

[20] DEPARTMENT OF DEFENSE. *Trusted Computer System Evaluation Criteria [the "Orange Book"].* Ft. Meade, 1985 MD: National Computer Security Center. [En línea] http://csrc.nist.gov/publications/history/dod85.pdf [citado en 14 de Octubre de 2014]

De 1984 a 1986 Dorothy Denning and Peter Neumann establecieron modelos para establecer intrusiones en los sistemas llamándolo *Intrusion Detection Expert System* (IDES) proponiendo una correlación entre los comportamientos anómalos y los usos indebidos[21]

En 1988, *Lawrence Livermore Labs* liberó *Haystack project*[22] usado para encontrar patrones de ataques internos en los ordenadores principales de las bases de la fuerza aérea de Estados Unidos (González, 2010). Tambien la *National Computer Security Center* (NCSC) diseñó un sistema conocido como MIDAS (*Multics Intrusion Detection and Alerting System*) para monitorear los sistemas *Dockmaster* de la NCSC un Honeywell DPS 8/70 Multics.[23]

Al tiempo que se diseñan metodologías de seguridad un gusano (Internet Worm) infecta miles de computadoras e interrumpe con las actividades normales de los sistemas por varios días, siendo detectado por medios manuales. En 1989, *Safeguards and Security Group* en Los Alamos *National Laboratory* crea un detector de anomalías conocido como Wisdom and Sense (Sabiduría y sentido) que se caracterizó por usar técnicas no paramétricas[24] para establecer una base que le permita hacer comparaciones posteriores para de ésta manera observar excepciones [25] [26]

En el año 1990 desarrollan un nuevo concepto cuando establecen un instrumento para monitorear la seguridad de las redes, fue desarrollado en la Universidad de California, fue uno de los primeros sistemas en usar el tráfico de redes como fuente primaria de datos, dado que antes de éste la información principalmente era obtenida de los sistemas operativos.

La detección de intrusiones tomó popularidad alrededor de 1997. En ese entonces Gerald Combs desarrolló un programa llamado *Ethereal*, como una herramienta para conocer de manera más extendida la red para conocer los inconvenientes que se presentaran en la misma.

.

[21] GURLEY, Rebecca. *Intrusion Detection.* Indianapolis: 2000. Macmillan Technical Publishing.

[22] MUKHERJEE, B., HEBERLEIN, T., & LEVITT, K. (1994). *Network Intrusion Detection.* IEEE. Retrieved from http://wenke.gtisc.gatech.edu/ids-readings/network_id.pdf [Citado el 10 de Septiembre de 2015]

[23] Un sistema Multics es una arquitectura de capaz que ejecuta los programas como recursos del sistema de manera jerárquica. Considerado uno de los sistemas operativos más seguros (Jaeger, 2008).

[24] No asumen conclusiones acerca de la distribución de los datos.

[25] SHERIF, Joseph., & DEARMOND, Tommy. (, Junio 10). Intrusion Detection: Systems and Models. IEEE Computer Society, 115, 2002. [En línea] http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/8879/1/02-1439.pdf [Citado el 18 de marzo de 2015]

[26] GURLEY, Op. cit.

2.2 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 [27] [28].

> "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" [29]

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 [30]

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

---

[27] COBB, Stephen. *Manual de seguridad para pc y redes locales.* (J. F. Bienvenido, & A. J. Bosch, Trans.) España: 1992. Windcres Books, Mcgrawhill inc.

[28] TANENBAUM, Andrew, & WETRERALL, David. Computer networks.5ta ed.Massachusetts: Pearson Education Inc., 2011. [En línea] http://cse.hcmut.edu.vn/~minhnguyen/NET/Computer Networks - A Tanenbaum - 5th edition.pdf [Citado el 15 de abril de 2015]

[29] MEDINA, L. F. En código abierto. *Revista Arcadia*. [En línea] http://www.revistaarcadia.com/Imprimir.aspx ?idItem=38588 [Citado el 14 de noviembre de 2014]

[30] TITTEL, Ed. Redes de computadoras. España: McGraw-Hill Interamericana S.A. 2004

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.[31] [32]

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[33]. 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 [34].

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[35].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[36].

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[37]. El protocolo

---

[31] STALLINGS, William. Data and Computer communications.8va ed. Upper Saddle River: Pearson Education, Inc., 2007 [En línea] http://memberfiles.freewebs.com/00/88/103568800/documents/Data.And.Computer.Communications.8e.WilliamStallings.pdf [Citado el 15 de abril de 2015]

[32] STALLINGS, William. Fundamentos de Seguridad en redes, aplicaciones y estándares. Mexico:Pearson Educación, 2004

[33] Ibíd.

[34] FOROUZAN, Behrouz.*Transmisión de datos y redes de comunicaciones* (5ta ed.). Madrid: Mcgraw Hill/Interamericana. 2013

[35] OREBAUGH, Angela; RAMIREZ, Gilbert; BURKE, Josh; PESCE, Larry; WRIGHT, Joshua & MORRIS, Greg. Wireshark and Ethereal, Network Protocol Analyzer toolkit. Rockland, 2007 Syngress Publishing Inc. [En línea] http://numenor.cicese.mx/cursos/PSR/Wireshark-book.pdf [Citado el 10 de Septiembre de 2015]

[36] ASRODIA , Pallavi & PATEL, Hemlata. Analysis of various packet sniffing tools for network monitoring and analysis. *International Journal of Electrical,Electronics and Computer Engineering, 1*(1), 55-58. 2012. [En línea] http://www.researchtrend.net/pdf/13 PALLAVI.pdf [citado en 12 de Octubre de 2014],

[37] HERRERA JOANCOMARTÍ, Jordi., ALFARO GARCIA, Joaquín, & PERRAMÓN TORNIL, Xavier. *Aspectos avanzados de seguridad en redes.* Barcelona: Fundación por la Universitat Oberta de

de Ethernet trabaja enviando la información del paquete a todos los hosts[38] 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[39].

Además, mantener una constante supervisión permite considerar los malos funcionamientos y tomar medidas con respecto a la seguridad o a la calidad de la transmisión de la información de manera oportuna; y siempre debe considerarse que habrá actividad anormal dentro de la red[40]. 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[41].

Una de las herramientas para análisis de tráfico en red utilizadas en la actualidad es la herramienta *Wireshark*[42],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[43].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[44] lo que hace

---

Catalunya.2004 [En Línea] http://www.sw-computacion.f2s.com/Linux/012.1-Aspectos_avanzados_en_seguridad_en_redes_modulos.pdf [Citado el 12 de febrero de 2014]

[38] Un hosts es un computador que está conectado a una determinada red desde el cual puede intercambiarse información.

[39] ALVAREZ CREGO, M. *Analizador de red (sniffer) en entorno GNU*. UOC La universidad virtual. [En línea] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/551/1/35037tfc.pdf [citado el 24 de enero de 2014]

[40] SANDERS, Chris. (2011). Practical Packet Analisis. New York: No Starch Press Inc. [En línea] http://repository.root-me.org/R%C3%A9seau/EN%20-%20Practical%20packet%20analysis%20-%20Wireshark.pdf [Citado el 16 de marzo de 2015]

[41] FARID, Dewan; HARBI, Nouria; ZAHIDUR Rahman, MOHAMMAD; Mofizur RAHMAN, Chowdhury. Attacks Classification in Adaptive Intrusion Detection using Decision Tree. *World Academy of Science, Engineering and Technology*, *39*, 86-90. 2010 [En línea] http://waset.org/publications/5652/attacks-classification-in-adaptive-intrusion-detection-using-decision-tree [Citado el 12 enero de 2014]

[42] BANERJEE, Op. cit.

[43] ASRODIA, Pallavi & PATEL, Hemlata. Analysis of various packet sniffing tools for network monitoring and analysis. *International Journal of Electrical,Electronics and Computer Engineering*, *1*(1), 55-58. 2012. [En línea] http://www.researchtrend.net/pdf/13 PALLAVI.pdf [citado en 12 de Octubre de 2014]

[44] Ibíd.

que *Wireshark* sea una herramienta apropiada para el análisis de tráfico de red [45], 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 [46] diferentes simplificando el trabajo de análisis por poseere filtros que permiten definir criterios para interpretar la información según el protocolo que se desee analizar[47].

2.3 MARCO CONCEPTUAL.

2.3.1 Seguridad

"Los aspectos de seguridad de la red incluyen protección de datos frente a accesos no autorizados, protección de datos frente a fallos y modificaciones e implementación de políticas y procedimientos para recuperarse de interrupciones y perdidas." [48]

2.3.2 Detección de intrusiones

Es el proceso en el cual existe una constante vigilancia sobre redes de computadoras y los sistemas para garantizar que no hallan violaciones, por consiguiente hay una búsqueda de información para establecer una línea de tiempo de los eventos para realizar un posterior análisis que permita encontrar señales de la existencia de intrusiones y generar respuestas apropiadas[49].

---

[45] ALVAREZ CREGO, Op. cit.

[46] SEIFRIED, Karl. Diseccionamos el tráfico de red *Wireshark*. *Linux magazine*, 8-9. [En línea] http://www.linux-magazine.es [citado el 12 de noviembre de 2014]

[47] BORJA MERINO, Febrero. *Análisis de tráfico con Wireshark.* Madrid: Inteco_cert. [En línea] https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf [Citado el 25 de junio de 2015]

[48] FOROUZAN, Behrouz. *Transmisión de datos y redes de comunicaciones* (5ta ed.). Madrid: Mcgraw Hill/Interamericana. 2013

[49] GURLEY, Rebecca. *Intrusion Detection.* Indianapolis: 2000. Macmillan Technical Publishing.

2.3.3 Ataque

Un ataque es una acción que es tomada contra un sistema de información o una red que intenta violar las políticas de seguridad del mismo, dando como resultado una amenaza[50].

2.3.4 Amenaza

Una amenaza es una situación dentro de un sistema de información que ofrece la oportunidad para que alguna persona genere una violación de seguridad, por lo cual puede ser potencialmente dañino[51], además el daño puede ser causado desde adentro o desde fuera, por lo cual debe considerarse las estructura física de la computadora, aunque también puede ser intencional o incidental por lo cual es necesaria una revisión del personal de la empresa como son los administradores de red, dados los privilegios con los que estos cuentan al controlar los recursos de cómputo y la información[52].

Categorías generales de amenazas:

- Intercepción
- Interrupción
- Modificación
- Fabricación

Las amenazas son una problemática que debe ser tenida en cuenta porque todo está en la red, la información y los recursos de los negocios dependen de Internet exponiéndolas a ser vulneradas.

2.3.5 Estándares

Los estándares son creados para permitir que redes heterogéneas, es decir, constituidas con dispositivos de diferentes fabricantes puedan interconectarse y de esta manera mantener la

---

[50] KRUTZ, Ronald L.; & VINES, Russell Dean. *The CEH prep guide: The comprehensive guide to certified ethical hacking.* Indianapolis, Indiana, Estados Unidos de América: Wiley Publishing, Inc. 2007

[51] GOMEZ, Julio. *Guía de Campo de hackers: aprende a atacar y a defenderte* (1ra ed.). Mexico: 2010 Alfaomega grupo editor S.A.

[52] GURLEY, Op. cit.

interoperabilidad nacional e internacional de los datos, y la tecnología y los procesos de telecomunicaciones[53].

Los estándares son clasificados como sigue:

De facto. Son aquellos que, establecidos por el uso en una arquitectura de un producto, en consecuencia, son propuestos por fabricantes que desean proponer un nuevo producto, imponiéndose como estándares por su amplia difusión.

De jure. "Aquellos estándares que han sido legislados por un organismo oficialmente reconocido son estándares de jure."[54]

Los estándares permiten que las plataformas están disponibles para quien quiera usarlas, son conocidos como sistemas abiertos, lo que permite que cualquiera que quiera prestar un servicio o elaborar un producto.

2.3.5.1 Estándares de internet

Dentro de las redes manejamos el término red de sistema abierto que está referida a la norma que es usada para establecer redes basadas en un protocolo "bien conocido y comprendido que tiene normas publicadas y disponibles para que cualquiera que desee usarlas" [55]

Para alcanzar el nivel de estándar sigue un procedimiento que comienza con el borrador (draft); éste es un documento sin estatus oficial que tiene un tiempo de vida de 6 meses. Luego de pruebas y recomendaciones de las autoridades que regulan Internet publican un Request For Comment (RFC). "Cada RFC es editado, numerado, y puesto a disposición de todas las partes interesadas. Los RFC pasan por niveles de madurez y se categorizan de acuerdo a su nivel de requisitos" [56]

---

[53] FOROUZAN, Op. cit.

[54] Ibíd.

[55] PARKER, Tim. Aprendiendo TCP/IP en 14 días. México, 1997, Prentice-hall Hispanoaméricana S.A.

[56] FOROUZAN, Behrouz. *Transmisión de datos y redes de comunicaciones* (5ta ed.). Madrid: Mcgraw Hill/Interamericana. 2013

2.3.6 Red

Una red es una aglomeración de dispositivos que permitiendo la interconexión entre ellos[57]. Algunas redes pueden ser construidas para medios corporativos reduciendo la cantidad de máquinas que pueden estar conectadas, esto por razones de seguridad y privacidad. Otras redes pueden estar diseñadas para permitir la interconexión de máquinas a través del tiempo, lo que se conoce como escalabilidad. En un sentido rudimentario podemos decir que para crear una red se necesitan dos elementos importantes: nodos y enlaces. Los primeros son las computadoras y los segundos son los medios de transmisión que pueden ser físicos o inalámbricos[58].

2.3.7 Analizadores de red

Los analizadores de red son herramienta de software que permite monitorear el tráfico de una red. Las computadoras están diseñadas para recibir solo el tráfico que va dirigido específicamente hacia ellas, sin embargo, los analizadores de red pueden capturar todos los paquetes que transiten donde la computadora con esta herramienta se encuentre conectada[59]. Básicamente, cuando los paquetes viajan a través de la red pasan por varios dispositivos intermedios hasta que encuentra su destino, como la cada máquina tiene una dirección física que lo relaciona con la dirección lógica del paquete, permite identificar que paquetes le van dirigidos, sin embargo, puede configurarse al dispositivo para que reciba todos los paquetes sin importar que no corresponda con la máquina y su identificación física[60].

---

[57] Ibíd.

[58] PETERSON, Larry, & DAVIE, Bruce. . Computer Networks: A sysems aproach. San Francisco, 2007, Elsevier Inc.

[59] ASRODIA, Pallavi & PATEL, Hemlata. Analysis of various packet sniffing tools for network monitoring and analysis. *International Journal of Electrical,Electronics and Computer Engineering, 1*(1), 55-58. 2012. [En línea] http://www.researchtrend.net/pdf/13 PALLAVI.pdf [citado en 12 de Octubre de 2014],

[60] ASRODIA, Pallavi & SHARMA, Vishal. Network Monitoring and analysis by packet sniffing method. *International Journal of Engineering trends and Technology (IJETT), 4*(5), 2133-2135. 2013. [En línea] http://www.ijettjournal.org/volume-4/issue-5/IJETT-V4I5P160.pdf [citado en 20 de Octubre de 2014],

2.4 MARCO LEGAL

2.4.1 Leyes para la regulación en las telecomunicaciones en Colombia

Ley 1273 de 2009 "De la protección de la información y de los datos" [61]

CONGRESO DE LA REPÚBLICA

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

Decreta:

Artículo1o.Adiciónese el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos".

2.4.1.1 De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A: *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

---

[61] Congreso de Colombia. *Leyes.* [En línea] http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf [Citado el 10 de Septiembre de 2015]

Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio o de personal confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

2.4.1.2 De los atentados informáticos y otras infracciones.

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240de este Código.

Artículo 269J: *Transferencia no consentida de activos*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Art.236 recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes.

Art 275 elementos materiales probatorios y evidencia física.

g) Mensaje de datos, como el intercambio electrónico de datos, Internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de1999 o las normas que la sustituyan, adicionen o reformen.

2.4.2 Licencias para el uso del Software Libre

2.4.2.1 Licencias GPL [62]. Una de las más utilizadas es la Licencia Pública General de GNU (GNU GPL). El autor conserva los derechos de autor (*copyright*), y permite la redistribución y modificación bajo términos diseñados para asegurarse de que todas las versiones modificadas del software permanecen bajo los términos más restrictivos de la propia GNU GPL. Esto hace que sea imposible crear un producto con partes no licenciadas GPL: el conjunto tiene que ser GPL.

Es decir, la licencia GNU GPL posibilita la modificación y redistribución del software, pero únicamente bajo esa misma licencia. Y añade que, si se reutiliza en un mismo programa código "A" licenciado bajo licencia GNU GPL y código "B" licenciado bajo otro tipo de licencia libre, el código final "C", independientemente de la cantidad y calidad de cada uno de los códigos "A" y "B", debe estar bajo la licencia GNU GPL.

2.4.2.2 Copyleft Invalid source specified. *Copyleft* o copia permitida comprende a un grupo de derechos de autor caracterizados por eliminar las restricciones de distribución o modificación impuestas por el copyright, con la condición de que el trabajo derivado se mantenga con el mismo régimen de derechos de autor que el original. Bajo tales licencias pueden protegerse una gran diversidad de obras, tales como programas informáticos, arte, cultura y ciencia, es decir prácticamente casi cualquier tipo de producción creativa. *Copyleft* dice que cualquiera que redistribuye el software, con o sin cambios, debe dar la libertad de copiarlo y modificarlo más. *Copyleft* garantiza que cada usuario tiene libertad.

2.4.2.3 Creative Commons. Las licencias Creative Commons o CC están inspiradas en la licencia GPL de la *Free Software Foundation*. No son, sin embargo, un tipo de licenciamiento de software. La idea principal es posibilitar un modelo legal ayudado por herramientas informáticas, para así facilitar la distribución y el uso de contenidos.

---

[62] FREE SOFTWARE FOUNDATION, Inc. GNU Operating System: Licencias. [en línea] http://www.gnu.org/licenses/licenses.es.html> [citado el 24 de Octubre de 2014]

2.4.3 Ley 842 de 2003[63]

TITULO IV
CODIGO DE ETICA PARA EL EJERCICIO DE LA INGENIERIA EN GENERAL Y SUS PROFESIONES AFINES Y AUXILIARES

CAPITULO I

Disposiciones generales

Artículo 29. *Postulados éticos del ejercicio profesional.* El ejercicio profesional de la Ingeniería en todas sus ramas, de sus profesiones afines y sus respectivas profesiones auxiliares, debe ser guiado por criterios, conceptos y elevados fines, que propendan a enaltecerlo; por lo tanto, deberá estar ajustado a las disposiciones de las siguientes normas que constituyen su Código de Ética Profesional.
Parágrafo. El Código de Ética Profesional adoptado mediante la presente ley será el marco del comportamiento profesional del ingeniero en general, de sus profesionales afines y de sus profesionales auxiliares y su violación será sancionada mediante el procedimiento establecido en el presente título.
Artículo 30. Los ingenieros, sus profesionales afines y sus profesionales auxiliares, para todos los efectos del Código de Ética Profesional y su Régimen Disciplinario contemplados en esta ley, se denominarán "Los profesionales".

CAPITULO II

Artículo 33. *Deberes especiales de los profesionales para con la sociedad* Son deberes especiales de los profesionales para con la sociedad:
a) Interesarse por el bien público, con el objeto de contribuir con sus conocimientos, capacidad y experiencia para servir a la humanidad.
b) Coopera para el progreso de la sociedad, aportando su colaboración intelectual y material en obras culturales, ilustración técnica, ciencia aplicada e investigación científica.
c) Aplicar el máximo de su esfuerzo en el sentido de lograr una clara expresión hacia la comunidad de los aspectos técnicos y de los asuntos relacionados con sus respectivas, profesiones y su ejercicio;
Artículo 34. *Prohibiciones especiales a los profesionales respecto de la sociedad.* Son prohibiciones especiales a los profesionales respecto de la sociedad:

---

[63] MINISTERIO DE EDUCACION NACIONAL, Ley 842 de 2003 [En Línea] http://www.mineducacion.gov.co/1621/articles-105031_archivo_pdf.pdf [citado el 24 de junio de 2015]

a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga sutítulo y su propia preparación.
b) Imponer su firma, a título gratuito u oneroso, en planos, especificaciones, dictámenes, memorias, informes, solicitudes de licencias urbanísticas, solicitudes de licencias, informes, solicitudes de licencias urbanísticas, solicitudes de licencias de construcción y toda otra documentación relacionada con el ejercicio profesional, que no hayan sido estudiados, controlados o ejecutados personalmente.

Artículo 37. *Deberes de los profesionales para con sus colegas y demás profesionales.* Son deberes de los profesionales para con sus colegas y demás profesionales de la ingeniería:
a) Respetar y reconocer la propiedad intelectual de los demás profesionales sobre sus diseños y proyectos.

Artículo 38. *Prohibiciones a los profesionales respecto de sus colegas y demás profesionales.* Son prohibiciones a los profesionales, respecto de sus colegas y demás profesionales de la ingeniería:

a. Utilizar sin autorización de sus legítimos autores y para su aplicación en trabajos profesionales propios, los estudios, cálculos, planos, diseños y software y demás documentación perteneciente a aquellos, salvo que la tarea profesional lo requiera, caso en el cual se deberá dar aviso al autor de tal utilización.

2.4.4 Ley de derecho de autor

Hace referencia sobre la protección de la información que con intención y sin derecho reproduzca, con infracción del encabezamiento del artículo 41 de esta Ley, en forma original o elaborada, íntegra o parcialmente, obras del ingenioso quien introduzca en el país, almacene, distribuya, venda o ponga de cualquier otra manera en circulación reproducciones ilícitas de las obras del ingenio o productos protegidos por esta Ley.

2.4.5 La legislación de derechos de autor en Colombia

Mediante decisión 351 de la comisión del acuerdo de Cartagena de diciembre de 1993, que está respaldada por la ley 44 de 1993 y por la ley 23 de 1982. Estas normas otorgan amplia e importante protección a los programas de software, convirtiendo ilícita la copia de programas sin consentimiento de los titulares de los derechos de autor, con excepción de la copia de seguridad.

2.4.6 Norma Técnica Colombiana NTC 4490,1160 y 130837 [64]

Estas normas establecen la presentación uniforme de referencias bibliográficas para publicaciones seriadas, libros, folletos y para fuentes de información electrónicas, con el fin de facilitar la identificación de los mismos o de una de sus partes.

2.4.7 Legislación internacional

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile. Dado lo anterior a continuación se mencionan algunos aspectos relacionados con la ley en los diferentes países, así como con los delitos informáticos que persigue.

2.4.7.1 Estados Unidos. Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.Con la finalidad de eliminar los argumentos hipertónicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática. En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C)[65].

---

[64] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Normas colombianas para la presentación de trabajos de investigación. Sexta actualización. Santa fé de Bogotá D.C. ,2002 p.41. NTC NTC 4490,1160 y 130837

[65] HAZAEL, David. *Contribuciones a la economía*,Eumed, 2014. [En línea]: http://www.eumed.net/ce/2012/tcgz.html [Citado el 10 de Septiembre de 2015]

2.4.7.2 Alemania. Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

2.4.7.3 Austria. La Ley de reforma del Código Penal, sancionada el 22 de diciembre de 1987, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además, contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

2.4.7.4. Gran Bretaña. Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización.

2.4.7.5. Holanda. El 1º de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- El *hacking*.
- El *preacking* (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).
- La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).
- La distribución de virus.

2.4.7.6. Francia. En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se consideran aspectos como:
Intromisión fraudulenta que suprima o modifique datos.
Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.
Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.
Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

2.4.7.7. Chile. Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos:

La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.
Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

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.

3.2 METODOLOGÍA

Para saber cómo se comporta la herramienta *Wireshark* en una red construida en un entorno controlado de laboratorio, observar el proceso en el cuál se desarrolla un proceso de tráfico se hará una aproximación a través de cuatro pasos:

- Reconocimiento (Recolección de datos): Se hará una captura de todos los paquetes que transitan por la red, para verificar si es posible seguir el rastro de un ataque[66].
- Métricas: La evaluación se realizará sobre los ataques de red por lo cual se capturarán todas las tramas del tráfico generado para identificar patrones identificativos de un ataque como direcciones y puertos usados para el tráfico[67] [68].
- Caracterización del tráfico: Identificar las características del tráfico. Observar las tramas de datos en su composición general durante la transmisión de datos para reconocer cuales son los protocolos más usados durante el proceso de comunicación[69].

---

[66] LAN, Kunchan; HUSSAIN, Alefiya & DUTTA, Debojyoti . Effect of Malicious Traffic on the Network. *SIGCOMM*. ACM.2003. [En línea] http://www.isi.edu/div7/publication_files/effect_malicious.pdf [Citado el 10 de Septiembre de 2015]

[67] CORONA, Igino., GIACINTO, Giorgio & ROLI, Fabio. Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues. *Elsevier Inc.* (239), 201-225. 2013 [En línea] http://dx.doi.org/10.1016/j.ins.2013.03.022 [citado en 14 de Octubre de 2014]

[68] VILLALÓN Huerta, Antonio. (2002). Seguridad en UNIX y redes. Cuenca: GNU Free Documentation License. [En línea] https://www.rediris.es/cert/doc/unixsec/unixsec.pdf [Citado el 15 de mayo de 2015]

[69] LAN et al, Op. cit.

- Identificar y aislar los patrones de ataque (efectos): Al observar las características generales de ataque, aislar aquellos comportamientos que pueden ser considerados anómalos dentro del comportamiento de la red

3.3 POBLACIÓN

La población está conformada por administrador del laboratorio del Grupo de Investigación en Ingenierías aplicada para la innovación, la gestión y el desarrollo (INGAP).

3.4 MUESTRA

Considerando que la población es solo el administrador del laboratorio del Grupo de Investigación en Ingenierías aplicada para la innovación, la gestión y el desarrollo (INGAP), se toma como muestra toda la población involucrada en el proceso.

4 ESTADO DEL ARTE.

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[70].

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"[71].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 las implementaciones 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, el uso de las computadoras ha complicado el trabajo para poder asegurar la información porque los expertos se muevan sobre un terreno pantanoso de nubes de dispositivos interconectados [72]. Por lo cual, para afrontar las amenazas, siempre crecientes, requiere de una cuidadosa monitorización de todas las actividades que permita reconocer comportamientos y su estado[73], para poder enfrentar adversarios que se mueven y

---

[70] TANENBAUM, Andrew., & WETRERALL, David. Computer networks.5ta ed.Massachusetts: Pearson Education Inc., 2011. [En línea] http://cse.hcmut.edu.vn/~minhnguyen/NET/Computer Networks - A Tanenbaum - 5th edition.pdf [Citado el 15 de abril de 2015]

[71] STALLINGS, William. Fundamentos de Seguridad en redes, aplicaciones y estándares. Mexico:Pearson Educación, 2004

[72] BRADEN, R.; CLARK, D.; CROCKER, S.; HUITEMA, C. *Security in the internet Architecture.* IETF. 1994

[73] CELEDA, Pavel. Network Security Monitoring and behavior analysis. 28. [En línea] http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd133.pdf [citado el 7 de septiembre de 2014]

evoluciona rápido contra muchas tecnologías que se han vuelto obsoletas haciendo vulnerables facetas como son la privacidad y la seguridad de los datos almacenados[74].

El responsable de la seguridad debe definir de manera sistemática los requisitos de seguridad y caracterizar los enfoques para satisfacer los requisitos propuestos[75]. En un universo digital la información se vuelve vital importancia, por lo cual, Llevar un registro de las actividades del sistema se convierte en una actividad que permite identificar potenciales ataques y determinar qué tan comprometido ha quedado el sistema[76].

Además Vislumbrar los peligros que se afrontan en el manejo de la información no sólo se reduce a identificar los ataques que puedan afectar a una entidad, sino el entramado arquitectónico que lo contiene, conformado por su unidad más pequeña: el paquete. Toda transmisión realizada se mueve dentro de patrones que permite una uniformidad comportamiento que permite la interconexión como son los protocolos usado, direcciones de destino etc. [77]

4.1 MODELO TCP/IP

La arquitectura de Internet permite normalizar las funcionalidades de las comunicaciones. Dicha arquitectura proporciona un modelo que permite enmarcar las situaciones en las cuales se desarrolla una transmisión. El modelo fue establecido por la Organización Internacional de Estandarización (ISO, *Internacional Organization for Standarization*) conocido como el modelo de referencia OSI [78] .Aunque en las comunicaciones reales se implementa el modelo TCP/IP (*Transfer Control*

---

[74] TRICAS GARCIA, Fernando. Ética y Seguridad en la red. *Uninet*, 1-13. [En línea] http://doctorado.uninet.edu/2004/cinet2004/ftricas/seguridadYPrivacidad.pdf [citado el 3 de noviembre de 2014]

[75] STALLINGS, William. Fundamentos de Seguridad en redes, aplicaciones y estándares. Mexico:Pearson Educación, 2004

[76] TechTarget-SearchSecurity. *Techtarget-SearchSecurity*. Retrieved from Monitoring Network traffic and Network forensics: [En línea] http://searchsecurity.techtarget.com/ehandbook/How-to-make-threat-monitoring-effective-in-these-tough-times [Citado el 24 de enero de 2016]

[77] BANERJEE, Usha, ASHUTOSH, Vashishtha & SAXENA, Mukul. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of computer applications*, *6*(7), 1-5. 2010 [En línea] http://ijcaonline.net/archives/volume6/number7/1092-1427 [citado en 14 de Octubre de 2014]

[78] STALLINGS, Op. cit.

Protocol/Internet Protocol) desarrollado a nivel experimental en la red financiada por la agencia de defensa DARPA (*Defense Advanced Research Projects Agency*)[79].

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[80]. Dado que el modelo está configurado en capas se le conoce como una pila de protocolos[81]. Los protocolos TCP son importantes para Para la clasificación del tráfico es importante para el transporte de archivos compartidos entre usarios.[82]

Las redes generan su máximo de comunicaciones sobre el protocolo TCP. En el estudio realizado por Razzak et al [83] 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 [84] [85] las identifican como sigue:

1. Envio de un bin 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.

---

[79] FOROUZAN, Behrouz. *Transmisión de datos y redes de comunicaciones* (5ta ed.). Madrid: Mcgraw Hill/Interamericana. 2013

[80] BARCELÓ ORDINAS, José María; GRIERA, Jordi Iñigo; MARTÍ ESCALÉ, Ramón; PEIG OLIVÉ, Enric & PERRAMON TORNIL, Xavier. *Redes de Computadores* (1ra ed.). Barcelona: Fundació per a la Universitat Oberta de Catalunya.2004

[81] ALVAREZ CREGO, M. *Analizador de red (sniffer) en entorno GNU.* UOC La universidad virtual. [En línea] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/551/1/35037tfc.pdf [citado el 24 de enero de 2014]

[82] ADIBI, Sasan. Traffic classification - Packet-, Flow-, and Application-based Aproaches. *International Journal of Advanced Computer Science and Applications (IJACSA), 1*(1), 6-15. 2010

[83] RAZZAK A., H. A., HANDA, S., & RAMANA MURTHY, M. . Providing the Secure Data Transmission in the Network Using Open Source Packet Analyzer. *International Journal of Computer trends and Technology (IJCTT), 12*(1). 2014 [en línea] doi: 10.14445/22312803/IJCTT-V12P103 [citado el 12 de junio de 2015]

[84] KUMAR, Sumit & SUDARSAN, Sithu. An Innovative UDP port Scanning Technique. *International Journal of Future Computer and Communication, 3*(6), 381-384. [en línea] doi:10.7763/IJFCC.2014.V3.332 [citado el 22 de enero de 2015]

[85] GUPTA, Shilpi. & MAMTORA, Roopal. Intrusion Detection System Using Wireshark. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*(11), 358-363. 2012 [En línea] http://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012/V2I11-0205.pdf [Citado el 10 de Noviembre de 2015]

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. [86]

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[87], 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[88].

Establecido el nuevo protocolo debe seguirse su adopción y promoción lo que significa un camino lento [89] [90], 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[91].

---

[86] LEVIN, Stanford & SCHMIDT, Stephen. IPv4 to IPv6: Challenges,solutions and lessons. *Telecommunications Policy, 38*, 1069-1068. 2014 [En línea] doi:doi:10.1016/j.telpol.2014.06.008 [citado el 25 de enero de 2015]

[87] CICILEO, Guillermo; et al. *IPv6 para todos, Guía de uso y aplicación para diversos entornos.* Buenos Aires: Asociación Civil Argentinos en Internet. [en línea] http://www.consulintel.es/pdf/ipv6paratodos.pdf [citado el 15 de mayo de 2015]

[88] LEVIN, Op. cit.

[89] CICILEO, Op. cit.

[90] HAZEYAMA, Hiroaki; UENO, Ukito & SATO, Hirotaka. 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.2011. [en línea] http://www.wide.ad.jp/project/document/reports/pdf2011/cd/02-3_wide-memo-camp1109-hack-v6only-questionnaire-01.pdf [citado el 12 de diciembre de 2015]

[91] LEVIN, Op. cit.

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[92] para autenticar como por ejemplo cambiando proponiendo *header* [93] que autentica el paquete a medida que hace saltos a través de la red aunque eso no significa una garantía contra los ataque que provengan de otras capas, porque según [94] 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[95] 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[96]. 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[97].

---

[92] PATTERSON, Kenneth. A criptographic tour of the IPsec standards. *Information Security Technical Report, 11*(2), 72-81.2006 [en línea] doi:10.1016/j.istr.2006.03.004 [citado el 23 de agosto de 2015]

[93] KENT, S. *IP Authentication Header*. IETF. [En línea] doi: http://dx.doi.org/10.17487/RFC4302 [citado el 30 de septiembre de 2015]

[94] HUNTER, Philip. IPv6: Security Issues. *Network Security, 2004*(1), 17-19. [en línea] doi:10.1016/S1353-4858(04)00026-1 [citado el 24 de abril de 2014]

[95] DURDAGI, Emre, & BULDU, Ali. IPv$/IPv6 security and threat comparisons. *Procedia Social and Behavioral Sciences, 2*, 5285-5291. [en línea] doi:10.1016/j.sbspro.2010.03.862 [citado el 28 de mayo de 2015]

[96] BRADEN, R.; CLARK, D.; CROCKER, S.; HUITEMA, C. *Security in the internet Architecture.* IETF. 1994

[97] BERGER, Arthur; WEAVER, Nicholas & BEVERLY, Robert. Internet Nameserver IPv4 and IPv6 address relationships. En ACM (Ed.), *Proceedings of the 2013 conference on Internet measurement conference (IMC '13)* (págs. 91-104). New York: Association for Computing Machinery (ACM). [en línea] doi:10.1145/2504730.2504745 [citado el 23 de Octubre de 2014]

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[98].

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[99]. 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.

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[100].

Banerjee & Saxena[101] recuerdan que fue a comienzos de 1980 cuando comienza a acuñarse la noción de detección de intrusiones, con un reporte ofrecido por James

---

[98] TRICAS GARCIA, Fernando. Ética y Seguridad en la red. *Uninet*, 1-13. [En línea] http://doctorado.uninet.edu/2004/cinet2004/ftricas/seguridadYPrivacidad.pdf [citado el 3 de noviembre de 2014]

[99] RASTEGARI, Samanesh; HINGSTON, Philip & LAM, Chiou-Peng. Evolving statistical rulesets for network intrusion detection. *Applied Soft Computing, 33*, 348-359. [en línea] doi:10.1016/j.asoc.2015.04.041 [citado el 24 de septiembre de 2015]

[100] FARID, Dewan; HARBI, Nouria; ZAHIDUR Rahman, MOHAMMAD; MOFIZUR, Rahman, Chowdhury. Attacks Classification in Adaptive Intrusion Detection using Decision Tree. *World Academy of Science, Engineering and Technology, 39*, 86-90. 2010 [En línea] http://waset.org/publications/5652/attacks-classification-in-adaptive-intrusion-detection-using-decision-tree [Citado el 12 enero de 2014]

[101] BANERJEE, Usha, ASHUTOSH, Vashishtha & SAXENA, Mukul. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of computer applications*, *6*(7), 1-5.

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[102]. 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[103].

Abad et al[104] 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[105].

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[106].Los paquetes desde su origen hasta su destino pasan por muchos dispositivos intermedios.

2010 [En línea] http://ijcaonline.net/archives/volume6/number7/1092-1427 [citado en 14 de Octubre de 2014]

[102] ANDERSON, James. *Computer Security Threat Monitoring and Surveillance*. Fort Washington:1980 [En línea] http://csrc.nist.gov/publications/history/ande80.pdf [citado en 14 de Octubre de 2014],

[103] SANDERS, Chris. (2011). Practical Packet Analisis. New York: No Starch Press Inc. [En línea]http://repository.root-me.org/R%C3%A9seau/EN%20-%20Practical%20packet%20analysis%20-%20Wireshark.pdf [Citado el 16 de marzo de 2015]

[104] ABAD, Cristina; LI, YIfan; LAKKARAJU, Kiran; YIN, Xiaioxin & YURCIK, William. 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.2004 [en línea] doi:10.1.1.5.2004 [citado el 10 de enero de 2015]

[105] HERRERA JOANCOMARTÍ, Jordi., ALFARO GARCIA, Joaquín, & PERRAMÓN TORNIL, Xavier *Aspectos avanzados de seguridad en redes.* Barcelona: Fundación por la Universitat Oberta de Catalunya.2004 [En Línea] http://www.sw-computacion.f2s.com/Linux/012.1-Aspectos_avanzados_en_seguridad_en_redes_modulos.pdf [Citado el 12 de febrero de 2014]

[106] ASRODIA, Pallavi & PATEL, Hemlata. Analysis of various packet sniffing tools for network monitoring and analysis. *International Journal of Electrical,Electronics and Computer Engineering, 1*(1), 55-58. 2012. [En línea] http://www.researchtrend.net/pdf/13 PALLAVI.pdf [citado en 12 de Octubre de 2014],

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 al aplicarse a una red con *switch* no es tan fácil dado que limita la cantidad de tráfico a los nodos conectados al dispositivo intermedio y además de la necesidad de elegir un puerto específico hacia el cual redireccionar el envío de datos.

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.[107]
4. Decodificación. Muestra el contenido del tráfico de red con texto descriptivo para permitir el análisis y reconocer lo que ocurre[108].

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.

---

[107] ASRODIA, Pallavi & SHARMA, Vishal. Network Monitoring and analysis by packet sniffing method. *International Journal of Engineering trends and Technology (IJETT), 4*(5), 2133-2135. 2013. [En línea] http://www.ijettjournal.org/volume-4/issue-5/IJETT-V4I5P160.pdf [citado en 20 de Octubre de 2014],

[108] ASRODIA, Op. cit.

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"[109]

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[110].

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.

4.2.1 WIRESHARK

Uno de los analizadores más populares en la actualidad es *Wireshark*. Fue desarrollado por Gerald Combs [111]. 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.

---

[109] CHAPPEL, Laura. *Wireshark Network Analysis.* San Jose CA: Protocol Analysis Institute. 2012

[110] CELEDA, Pavel. Network Security Monitoring and behavior analysis. 28. [En línea] http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd133.pdf [citado el 7 de septiembre de 2014]

[111] BORJA MERINO, Febrero. *Análisis de tráfico con Wireshark.* Madrid: Inteco_cert. [En línea] https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf [Citado el 25 de junio de 2015]

Banerjee et al[112] 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. Los criterios de selección pueden ser múltiples: protocolos, campos, valores del campo, comparaciones, etc. Wireshark tiene un campo de búsqueda que permite insertar los criterios de filtrado.

4.2.1.1 Tres Secciones de despliegue de información

Dentro de las características importantes de la herramienta en la manera como despliega la información capturada para su mejor visualización en tres ventanas o paneles: de resumen o listado de paquetes, árbol de protocolos o detalle de paquetes, vista de datos o paquetes por byte. Estos paneles o ventanas son importantes porque hacen más comprensible el formato en el cual la información se despliega[113].

En la sección de los paquetes puede verse la captura de cada paquete con el tiempo en el cual fue capturado, la fuente y el destino de procedencia y el protocolo que fue usado en la transmisión (Ver Figura 1). Este despliegue de información es significativo porque permite resaltar con facilidad los protocolos que sean requeridos para un análisis del tráfico en un momento dado, además del intervalo de transmisión de cada

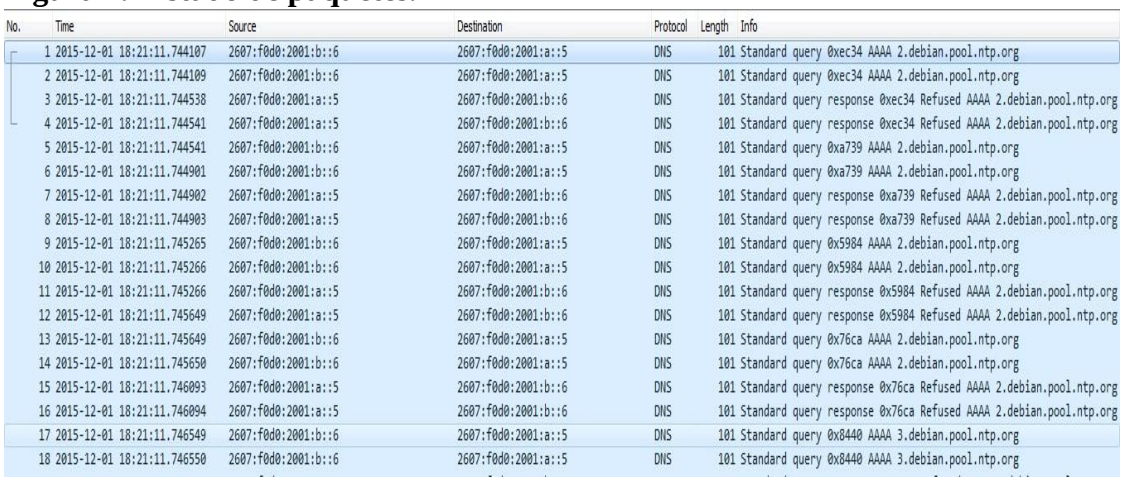
---

[112] BANERJEE, Usha, ASHUTOSH, Vashishtha & SAXENA, Mukul. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of computer applications*, *6*(7), 1-5. 2010 [En línea] http://ijcaonline.net/archives/volume6/number7/1092-1427 [citado en 14 de Octubre de 2014]

[113] SANDERS, Chris. (2011). Practical Packet Analisis. New York: No Starch Press Inc. [En línea] http://repository.root-me.org/R%C3%A9seau/EN%20-%20Practical%20packet%20analysis%20-%20Wireshark.pdf [Citado el 16 de marzo de 2015]

paquete, dado que su frecuencia en la transmisión puede ser irregular[114] [115]; la herramienta permite resaltar con un color específico cada paquete involucrado en una captura, para facilitar la observación de los paquetes que viajan a través de la red.

Figura 1. Listado de paquetes.



No.	Time	Source	Destination	Protocol	Length	Info
1	2015-12-01 18:21:11.744107	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0xec34 AAAA 2.debian.pool.ntp.org
2	2015-12-01 18:21:11.744109	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0xec34 AAAA 2.debian.pool.ntp.org
3	2015-12-01 18:21:11.744538	2607:f0d0:2001:a::5	2607:f0d0:2001:b::6	DNS	101	Standard query response 0xec34 Refused AAAA 2.debian.pool.ntp.org
4	2015-12-01 18:21:11.744541	2607:f0d0:2001:a::5	2607:f0d0:2001:b::6	DNS	101	Standard query response 0xec34 Refused AAAA 2.debian.pool.ntp.org
5	2015-12-01 18:21:11.744541	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0xa739 AAAA 2.debian.pool.ntp.org
6	2015-12-01 18:21:11.744901	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0xa739 AAAA 2.debian.pool.ntp.org
7	2015-12-01 18:21:11.744902	2607:f0d0:2001:a::5	2607:f0d0:2001:b::6	DNS	101	Standard query response 0xa739 Refused AAAA 2.debian.pool.ntp.org
8	2015-12-01 18:21:11.744903	2607:f0d0:2001:a::5	2607:f0d0:2001:b::6	DNS	101	Standard query response 0xa739 Refused AAAA 2.debian.pool.ntp.org
9	2015-12-01 18:21:11.745265	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0x5984 AAAA 2.debian.pool.ntp.org
10	2015-12-01 18:21:11.745266	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0x5984 AAAA 2.debian.pool.ntp.org
11	2015-12-01 18:21:11.745266	2607:f0d0:2001:a::5	2607:f0d0:2001:b::6	DNS	101	Standard query response 0x5984 Refused AAAA 2.debian.pool.ntp.org
12	2015-12-01 18:21:11.745649	2607:f0d0:2001:a::5	2607:f0d0:2001:b::6	DNS	101	Standard query response 0x5984 Refused AAAA 2.debian.pool.ntp.org
13	2015-12-01 18:21:11.745649	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0x76ca AAAA 2.debian.pool.ntp.org
14	2015-12-01 18:21:11.745650	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0x76ca AAAA 2.debian.pool.ntp.org
15	2015-12-01 18:21:11.746093	2607:f0d0:2001:a::5	2607:f0d0:2001:b::6	DNS	101	Standard query response 0x76ca Refused AAAA 2.debian.pool.ntp.org
16	2015-12-01 18:21:11.746094	2607:f0d0:2001:a::5	2607:f0d0:2001:b::6	DNS	101	Standard query response 0x76ca Refused AAAA 2.debian.pool.ntp.org
17	2015-12-01 18:21:11.746549	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0x8440 AAAA 3.debian.pool.ntp.org
18	2015-12-01 18:21:11.746550	2607:f0d0:2001:b::6	2607:f0d0:2001:a::5	DNS	101	Standard query 0x8440 AAAA 3.debian.pool.ntp.org

Fuente. Autor del proyecto

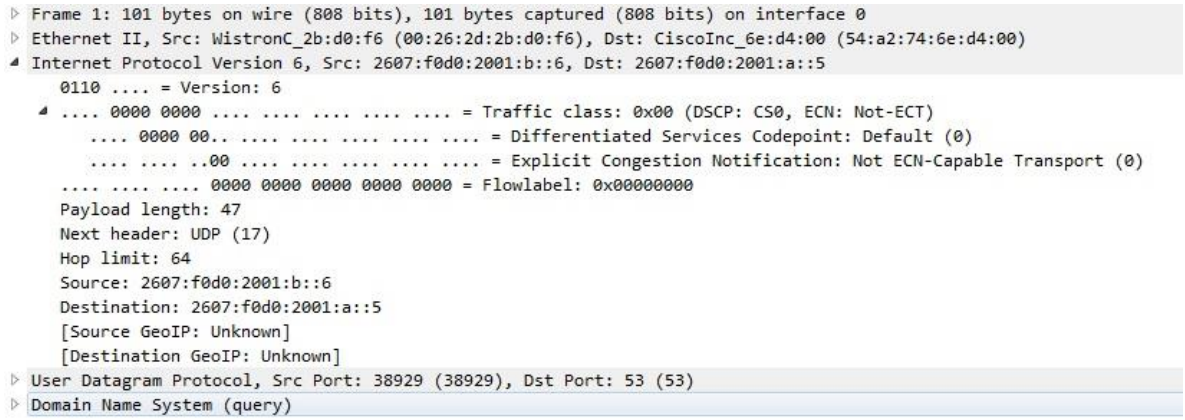
La sección de protocolos contiene el comportamiento de cada protocolo involucrado en la transmisión de un paquete, desplegando varias ramificaciones de los protocolos involucrados. Como se puede observar en la Figura 2 como en el panel se muestra la cantidad de bits del paquete y sobre que interface física ocurrió la transmisión, los dispositivos que intervinieron en la transmisión del paquete con respectivas direcciones MAC, muestra el protocolo de internet (IP) y sus respectivas direcciones de origen y de destino y la versión del protocolo sobre el cual están corriendo, además de los puertos que estuvieron abiertos durante la comunicación y el servicio principal que fue usado dentro del desarrollo de la transferencia.

Y el panel de bytes o vista de datos contiene unas filas que comienzan con un número de cuatro dígitos que indica el número de bytes en un octeto, los números en hexadecimal indican la cantidad de bytes involucrados en el octeto y la última sección muestra la representación en ASCII de cada octeto. No todos los bytes pueden ser mostrados en ASCII por lo cual son sustituidos por puntos (.)(Ver Figura 3).

[114] ORZACH, Yoram. Network analysis using Wireshark cookbook. Birmighan, UK, 2013, Packt Publishing.

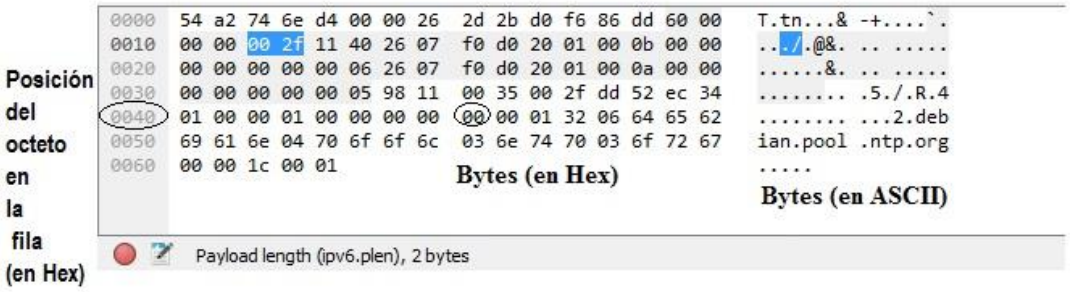
[115] SANDERS, Op. cit.

Figura 2. Panel de protocolos.



Fuente. Autor del proyecto

Figura 3. Panel de bytes.



Fuente. Autor del proyecto

4.3.1.2. Detección en modo promiscuo

La herramienta *Wireshark* permite configurar la captura de paquetes en modo promiscuo, lo que permite activar la interfaz para recibir todos los paquetes que lleguen a la interfaz[116] [117] [118]. Por defecto, por una interfaz sólo recibe los paquetes que son destinados a la dirección MAC correspondiente a un determinado equipo en una red.

[116] BANERJEE, Op. cit.

[117] ASRODIA, Op. cit

[118] BISWAS, Op. cit.

Para casos específicos donde se desea diagnosticar una maquina en específico de una red, puede elegirse capturar sólo los paquetes direccionados o enviados a la interfaz que se desea conocer. *Wireshark* permite configurar un filtro para capturar sólo aquellos paquetes que coincidan con el filtro que se desea establecer y obtener los paquetes que desean ser recibidos para su posterior análisis[119]. Establecer filtro para las capturas permite distinguir el tráfico en el caso de que existan diferentes servicios funcionando en la misma red. *Wireshark* permite analizar un servicio corriendo en un puerto determinado, esto facilitaría focalizar el análisis al tráfico que desea ser estudiado[120].

4.3 ANÁLISIS DE UN 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[121].

Para establecer medidas apropiadas de seguridad que garanticen la seguridad de la información debe establecerse el uso de herramientas apropiadas para implementar medidas acertadas[122]. 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.

---

[119] OREBAUGH, Op. cit.

[120] SANDERS, Op. cit.

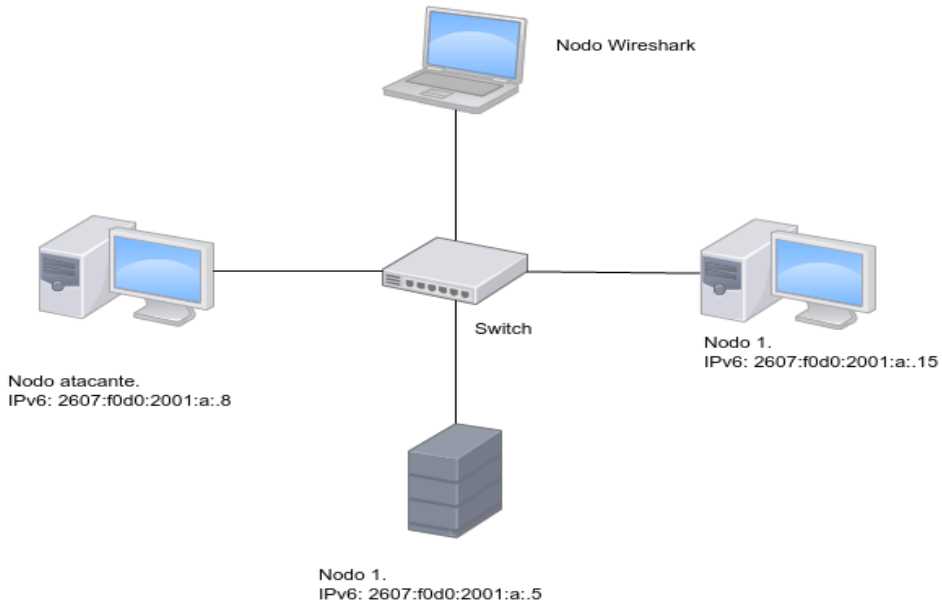
[121] MCCLURE, Stuart; SCAMBRAY, Joel & KURTZ, George.*Hacking Exposed 7* (7ma ed.). New York: McGraw-Hill.2012

[122] BRADEN, Op. cit.

5 DISEÑO DE LA RED

5.1 TOPOLOGIA DE RED 1

Figura 4. Red LAN con witch cisco 2945



Fuente. La topología de estrella está conformada por 5 dispositivos: Un *switch*. Cuatro nodos en la red: Un nodo atacante (IP 2607:f0d0:2001::8/64), un nodo servidor (IP 2607:f0d0:2001::5/64), un nodo cliente (IP 2607:f0d0:2001::15/64) y el nodo para capturar paquetes. Autor del Proyecto.

5.1.1 Direccionamiento.

Las direcciones IPv6 asignadas a la red estarán contenidas en la asignación: 2607:f0d0:2001:/64.En el switch estarán todos los nodos en la misma red.

Tabla 1. Especificaciones para el nodo atacante.

ID.		Atacante	
Sistema Operativo		Kali Linux	
DHCPv4	192.168.1.100	IPv6	2607:f0d0:2001:a::10
NetMask		Mask	64
DNS		DNS	2607:f0d0:2001:a::5

Fuente. Autor del Proyecto.

Tabla 2. Especificaciones para el servidor.

ID.		Servicios	
Sistema Operativo		Ubuntu Server	
IPv4	192.168.1.5	**IPv6**	2607:f0d0:2001:a::5
NetMask	255.255.255.0	**Mask**	64
DNS server	192.168.1.5	**DNS server**	2607:f0d0:2001:a::5
Dominios	v6.test.com	**server.test.com**	

Fuente. Autor del proyecto

Tabla 3. Especificaciones para el nodo con Wireshark

ID.		Sniffer	
Sistema Operativo		Windows 7	
IPv4	Sin definir	IPv6	Sin definir
NetMask	Sin definir	Mask	Sin definir
DNS	Sin definir	DNS	Sin definir

Fuente. Autor del Proyecto

Tabla 4. Especificaciones para un nodo de la red.

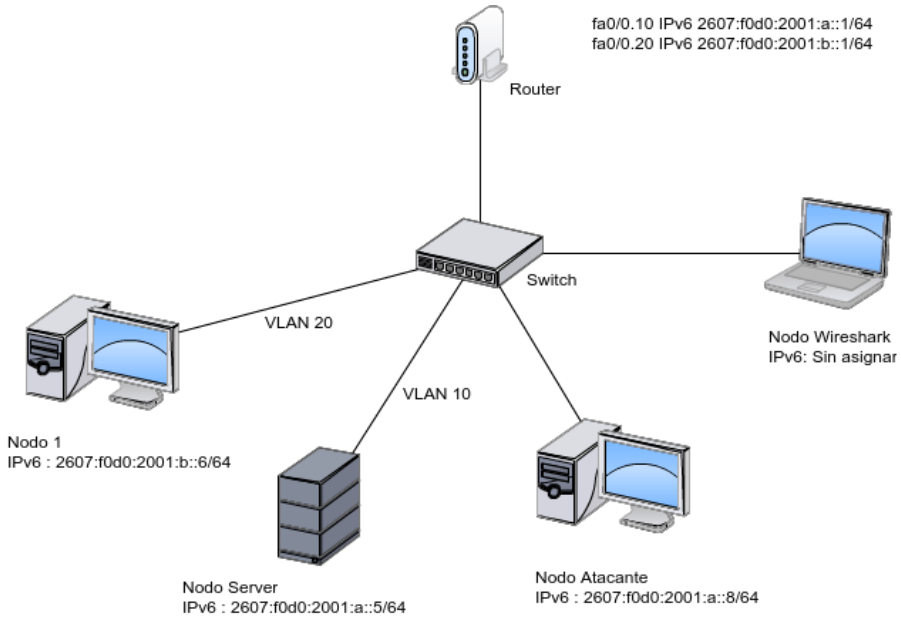
ID.		Host	
Sistema Operativo		Linuxmint	
IPv4	Sin definir	IPv6	2607:f0d0:2001:a::15
NetMask	Sin definir	Mask	64
DNS server	Sin definir	DNS	2607:f0d0:2001:a::5

Fuente. Autor del proyecto

El escenario fue configurado con un computador que ofrece los servicios Web y DNS a través del servidor Apache y DNS para el entorno. Al momento de la ejecución de la captura estaban activos todos los servicios, aunque no se hicieron solicitudes a la página web configurada dentro del servidor. El servicio DHCP está configurado para direcciones IPv4 configurado en el sistema, por lo cual el nodo atacante tiene una IP especificada por el servicio.

5.2 TOPOLOGIA DE RED 2

Figura 5. Topología de estrella.



Fuente. La topología de estrella está conformada por 6 dispositivos: dos dispositivos intermedios: un *router* y un *switch*. Cuatro nodos en la red: Un nodo atacante (IP 2607:f0d0:2001::8/64), un nodo servidor (IP 2607:f0d0:2001::5/64), un nodo cliente (IP 2607:f0d0:2001::6/64) y el nodo para capturar paquetes. Autor del Proyecto.

5.2.1 Direccionamiento.

Utilizaremos las direcciones 2607:f0d0:2001:/64.
Los nodos de la VLAN 10 pertenecen a la red 2607:f0d0:2001:a::/64
Los nodos de la VLAN 20 pertenecen a la red 2607:f0d0:2001:b::/64

Tabla 5. Especificaciones para el nodo atacante.

ID.		Atacante	
Sistema Operativo		Kali Linux	
DHCPv4	192.168.1.100	IPv6	2607:f0d0:2001:a::10
NetMask		Mask	64
DNS		DNS	2607:f0d0:2001:a::5

Fuente. Autor del Proyecto

Tabla 6. Especificaciones para el servidor.

ID.		Servicios	
Sistema Operativo		Ubuntu Server	
IPv4	192.168.1.5	IPv6	2607:f0d0:2001:a::5
NetMask	255.255.255.0	Mask	64
DNS server	192.168.1.5	DNS server	2607:f0d0:2001:a::5
Dominios	v6.test.com	server.test.com	

Fuente. Autor del Proyecto

Tabla 7. Especificaciones para el nodo con Wireshark.

ID.		Sniffer	
Sistema Operativo		Windows 7	
IPv4	Sin definir	IPv6	Sin definir
NetMask	Sin definir	Mask	Sin definir
DNS	Sin definir	DNS	Sin definir

Fuente. Autor del Proyecto

Tabla 8. Especificaciones para un nodo de la red

ID.		Host	
Sistema Operativo		Linuxmint	
IPv4	Sin definir	IPv6	2607:f0d0:2001:a::15
NetMask	Sin definir	Mask	64
DNS server	Sin definir	DNS	2607:f0d0:2001:a::5

Fuente. Autor del Proyecto

Tabla 9. Especificaciones para el router 1900.

ID.	Router
Protocolos	Ipv4, Ipv6, rutas estáticas
Encapsulaciones	VLAN 802.1q
Puertos basados en RJ-45	2
Aceleración de cifrado integrad en Hardware (Ipsec + SSL)	
Puerto de consola	1
Fuentes de alimentación	CA

Fuente. www.cisco.com[123]

[123] http://www.cisco.com/web/LA/docs/pdf/1941_data_sheet_c78_556319.pdf

6. REALIZACIÓN DE LABORATORIOS.

Las pruebas realizadas para la presente investigación fueron desarrolladas en una Red de Área Local bajo una arquitectura cliente servidor, para la aplicación de la herramienta se establecieron diversos escenarios para la captura del tráfico entre los diversos hosts conectados.

La estructura de los laboratorios está provista por los siguientes puntos:

- Título
- Objetivos
- Tráfico generado
- Resultados

6.1 Laboratorios realizados

6.1.1 Laboratorio Uno

6.1.1.1 Título. Captura de paquetes en un escenario de red con arquitectura tipo estrella y direccionamiento IPv6

6.1.1.2 Objetivos.

Realizar la captura de paquetes concentrando el tráfico, que transcurre por uno o varios puertos del switch, en un puerto específico (port mirroring).

Llevar a cabo el ataque de ARP spoofing capturando el tráfico a diversas máquinas del entorno.

6.1.1.3 Tráfico generado. La transmisión de datos fue realizada en la Topología 1 generando tráfico ICMPv6 para verificar si los nodos se reconocían entre sí. De ésta manera, se percibió todo el intercambio configurando en el switch un puerto como *port mirroring* que permite escuchar toda la actividad que pasa a través de switch.

6.1.1.4 Resultados.

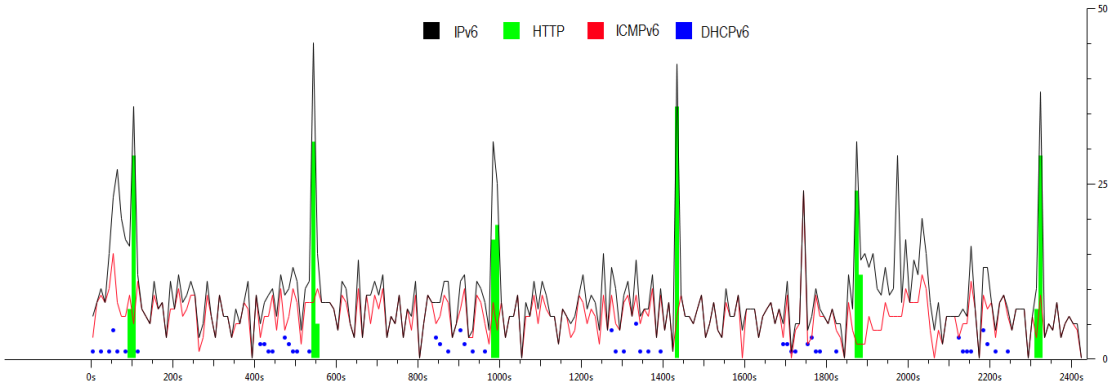
Para la captura del tráfico el dispositivo con la herramienta Wireshark debe ser posicionado de forma apropiada en la red (ver ANEXO A). De donde se procede a realizar el escaneo de toda la transmisión de paquetes que ocurre en la red.

Figura 6. Captura transmisión IPv6

	Source	Destination	Protocol	Length	Info
5-10-01 19:34:21.095013000	fe80::28ec:8487:2226:42d2	ff02::1:2	DHCPv6	146	Solicit XID: 0x3eeb86 CID: 000100011b1545ca00262d262730
5-10-01 19:34:22.319829000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:23.200636000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:23.718627000	fe80::28ec:8487:2226:42d2	ff02::1:3	LLMNR	84	Standard query 0x7754 A wpad
5-10-01 19:34:23.818784000	fe80::28ec:8487:2226:42d2	ff02::1:3	LLMNR	84	Standard query 0x7754 A wpad
5-10-01 19:34:24.200672000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:28.972175000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:29.699933000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:30.699943000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:31.699969000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:32.700065000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:33.700091000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:34.700163000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:35.700159000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:36.700301000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:37.094527000	fe80::28ec:8487:2226:42d2	ff02::1:2	DHCPv6	146	Solicit XID: 0x3eeb86 CID: 000100011b1545ca00262d262730
5-10-01 19:34:38.995517000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:39.700432000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:40.700454000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:41.971560000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:42.699556000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:43.699530000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30
5-10-01 19:34:44.699626000	2607:f0d0:2001:a::15	ff02::1:ff00:5	ICMPv6	86	Neighbor Solicitation for 2607:f0d0:2001:a::5 from 00:26:2d:26:27:30

Fuente. Autor del proyecto

Figura 7. Comportamiento del tráfico

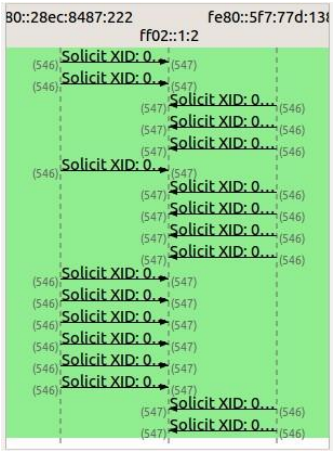


Fuente. Autor del proyecto

En la Figura 6 podemos observar el comportamiento de los protocolos que son más notorios en la transmisión realizada. Puede observarse la línea negra de la gráfica como la totalidad de los paquetes IPv6 del tráfico de la red, las barras rojas son la transmisión de paquetes ICMPv6 que coincide con las hondas más baja de la totalidad de los paquetes del protocolo IP involucrado y las barras verdes están relacionados con paquetes del protocolo HTTP que surgió en la comunicación realizada. Los puntos azules son las solicitudes DHCPv6 enviadas por los dos hosts involucrados en la comunicación IPv6.

Cabe aclarar que el protocolo DHCPv6 es stateless (SLAAC) llamado de este modo porque permite obtener una dirección propia con la información local que disponga, usadas para la comunicación local de la red[124]. En la captura encontramos un paquete DHCPv6 solicitando *router* que no encontrara respuesta alguna dado que no hay *routers* conectados en el esquema de red.
Dentro de la captura de paquetes puede distinguirse una dirección de destino FF02::1:2, lo cual es cumpliendo una especificación del protocolo de Internet versión 6 que requiere que el sistema operativo asigne direcciones de enlace-local a cada interface de red que tenga direcciones operativas; dentro de esas especificaciones la dirección mencionada más arriba, es una dirección por defecto que indica que debe direccionarse una petición de *router* a todos los enlaces locales de la red. El ataque puede distinguirse en la Figura 8 que al filtrar la peticiones DHCP (filtro dhcpv6), las solicitudes se realizan en intervalos muy cortos sin que exista respuesta alguna, llenando la caché de solicitudes que pueden desbordar el equipo.

Figura 8. Peticiones DHCPv6 a ff02::1:2



Fuente. Autor del proyecto

124 THOMSON, S., Narten, T. & JINMEI, T. R. IPv6 Stateless Address Autoconfiguration. 2007. The Internet Society. [RFC 4862]

6.1.2 Laboratorio Dos

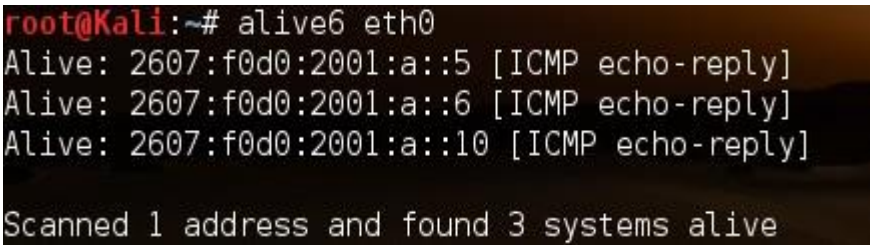
6.1.2.1 Titulo. Recolección de información y explotación de las vulnerabilidades del entorno con topología de estrella.

6.1.2.2 Objetivos.

- Recolectar información de los nodos que conforman la topología de la red
- Descubrir las vulnerabilidades de los equipos dentro de la red.

6.1.2.3 Tráfico generado. La transmisión de datos fue realizada en la Topología 2 iniciando una verificación de los nodos existentes en la red configurada (Ver Figura 4) con el comando *alive6,* que permite hacer ping a los equipos de la red recibiendo una replicación por parte de estos y de esta manera reconocer los equipos que están involucrados en la configuración de la misma. Como muestra la Figura 9 vemos que existen 3 nodos existentes en la red.

Figura 9. Hosts activos de la red.



Fuente. Autor del proyecto

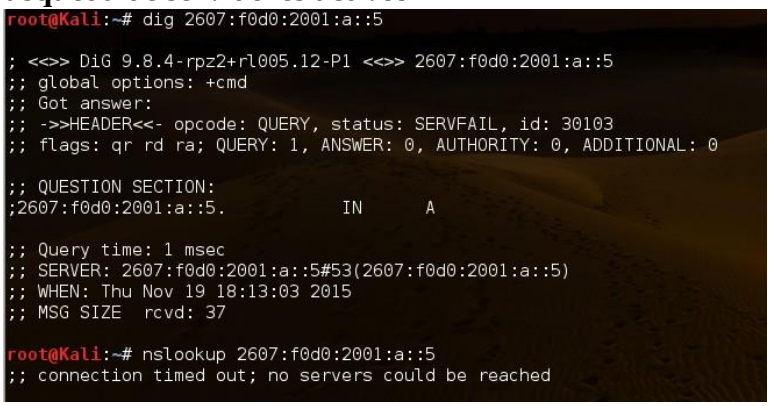
Para recolectar más información, se verifica con el comando *dnsdict6* para la URL v6.test.com y de esta manera verificar a cual dirección IP pertenece para descubrir que equipo de la red presta la resolución DNS dentro de la red configurada. En la Figura 10 podemos observar que obtenemos la Ipv6 2607:f0d0:2001:a::5 como la correspondiente al equipo del servidor además de una url alternativa: server.test.com.

Figura 10. Reconocimiento del DNS.

Fuente. Autor del proyecto

Con la dirección IP obtenida se puede proceder a buscar muchos más datos ue puedan servir para la exploración posterior de la red, para lo cual se utiliza el comando *dig*. Como puede verse en la Figura 11 no ha sido obtenida otra información relevante distinta a la ya obtenida. A la vez puede observarse el uso del comando *nslookup* para verificar si la dirección IP utilizada devuelve el dominio utilizado más arriba para conseguir la dirección IP, sin embargo los resultados no fueron positivos.

Figura 11. Búsqueda de servidores activos



Fuente. Autor del proyecto

Dentro de la recolección de información, dado que se ha identificado la dirección del servidor, se ha lanzado el comando *nmap* con las siguientes opciones: -6 para habilitar el escaneo de IP version 6; -T4 es para controlar el tiempo y hacerle de una manera maś rápida indicada por la opcion número 4 que acelera el proceso de escaneo; -A habilita otras opciones disponibles por defecto en la herramienta *nmap*, lo cual puede ser una función muy agresiva dentro de una red. Por último, -v para incluir todos los *hosts* de salida. El uso del comando se puede observar en la Figura 12.

Figura 12. Puertos activos con nmap

Fuente. Autor del proyecto

Con la aplicación de la herramienta *nmap* se ha obtenido los puertos activos en el servidor junto con los respectivos servicios y la herramienta de software utilizada para prestar el servicio dentro del equipo.

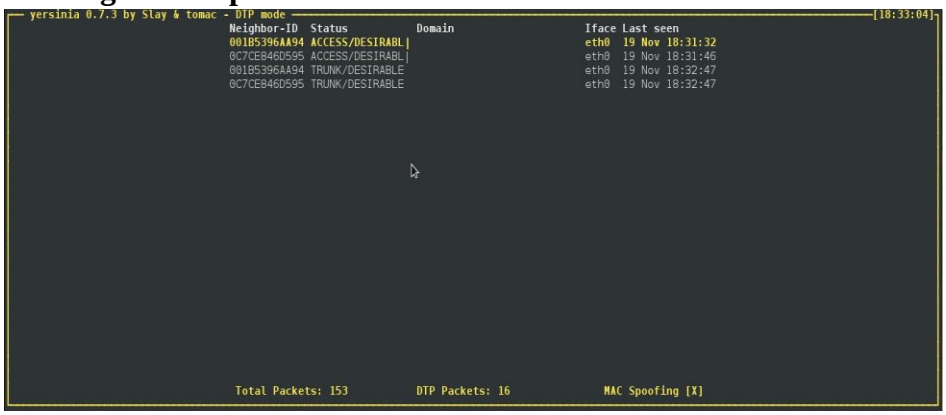
Tabla 10. Puertos activos con nmap

Puerto	Estado	Servicio	Versión
53/tcp	Abierto	domain dns-nsid	bind 9.9.5
80/tcp	Abierto	http	Apache httpd 2.4.10
139/tcp	Abierto	netbios-ssn	Samba smbd 3.X
445/tcp			

Fuente. Autor del Proyecto

Dentro de la etapa de ataque del laboratorio se ha usado una herramienta conocida como *Yersinia* que permite vulnerar los puertos de switch para hacer cambios en las las VLAN configuradas en él, insertando un nuevo nodo en la VLAN descubierta por la herramienta. Este proceso se realiza a través del envio de un paquete DTP (*Dinamic Trunking Protocol*) que facilita la negociación de puertos *trunk* entre *switches.* Como vemos en la Figura 13 la herrmaienta busca los puertos que se ha comunicado con el switch y al descubrir la configuración *desirable* comienza a negociar una comunicación *trunk* con la red VLAN configurada en el *switch.*

Figura 13. Configuración puerto trunk con Yersinia



Fuente. Autor del proyecto

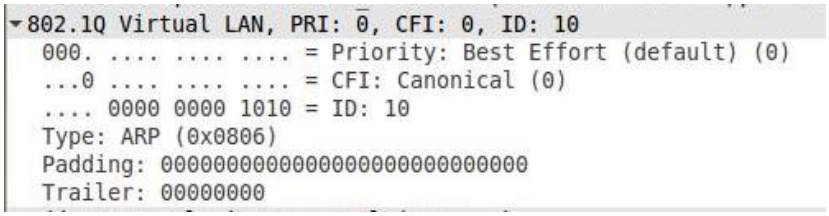
El ataque requiere de la herramienta *Wireshark* para capturar la comunicación entre el equipo atacante y el *switch* involucrado en la comunicación. Como vemos en la Figura 14, los paquetes resaltados con verde son los paquetes involucrados en la comunicación. El ataque ha sido resaltado con un filtro de color que está incorporado en la herramienta para identificar los paquetes del interés del usuario que la usa.
La herramienta *Wireshark* despliega en el panel de información de los paquetes la ID de una de las VLAN configuradas en el *switch.* (Ver Figura 5)

Figura 14. Captura de paquetes en el nodo tacante.

Fuente. Autor del proyecto.

Se puede configurar el nodo atacante con el ID de la VLAN (Ver Tabla 11) que ha sido obtenido para que el switch considere al nodo como participante de la configuración de la red virtual configurada y recibir cualquier destidanada a los *hosts* de la misma.

Figura 15. Información sobre el protocolo 802.1q



Fuente. Autor del proyecto

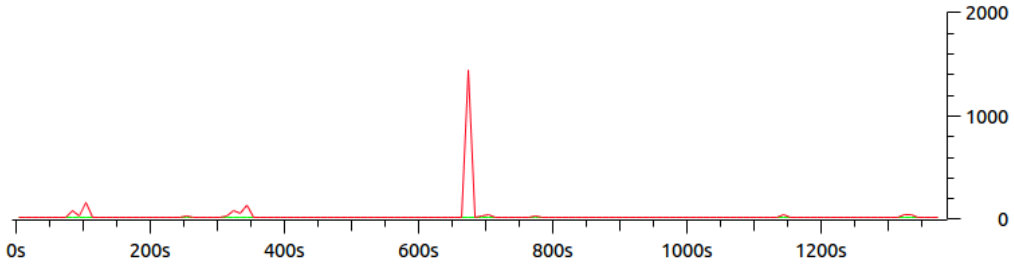
Tabla 11. Configuración de puerto.

vconfig add eth0 10 Added VLAN with VID == 10 to IF -:eth0:-

Fuente. Autor del proyecto

6.1.2.4 Resultados. Durante la realización del ataque se esperaba que el nodo atacante pudiera configurarse como parte de una de las VLAN establecidas dentro del *switch* de la topología, sin embargo, aunque el nodo atacante pudo configurarse con el ID de una de las VLAN no hubo recepción de los paquetes que transitaban por ella, por lo cual el ataque realizado no fue exitoso, el nodo atacante no pudo establecer comunicación con la VLAN de la cual obtuvo el ID. Se cree que es posible que las especificaciones del ataque pueden no ser las óptimas al realizar un ataque configurada en una red configurada con el protocolo de Internet versión 6.

Figura 16. Comportamiento del tráfico durante el ataque



Fuente. Autor del proyecto

Aunque podemos concluir por el tráfico capturado que hubo un aumento de tráfico de una IP que no estaba registrada en las VLAN intentado comunicarse con uno de los nodos configurados en ellas.

En la Figura 16 al aplicar el filtro sobre la captura (!ipv6.src == 2607:f0d0:2001:a::5 and !ipv6.src == 2607:f0d0:2001:b::6) genera un pico en rojo que muestra la constante llegada de paquetes de la dirección IP vinculada con el nodo atacante, mientras de forma solapada en la línea verde fosforescente revela la comunicación de los nodos vinculados a las otras VLAN.

6.1.3 Laboratorio tres

6.1.3.1 Titulo. Provocación de un ataque DoS a través del aumento del flujo de tráfico.

6.1.3.2 Objetivos.

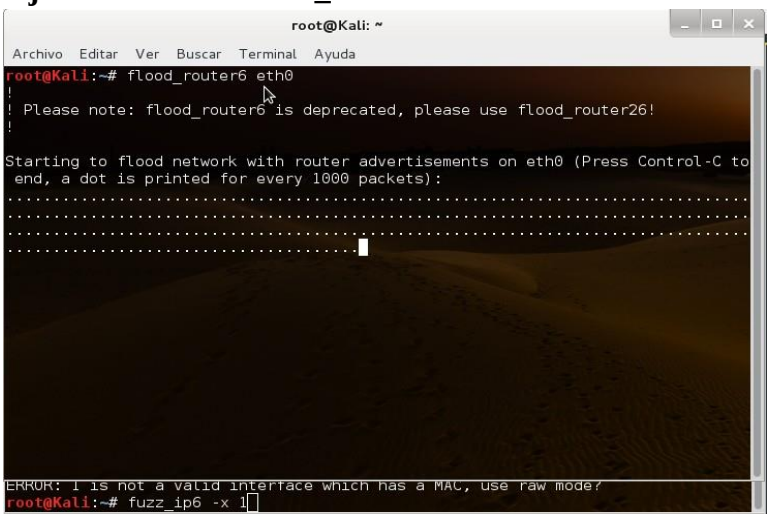
Realizar a ataques para aumentar el flujo de tráfico de la red
Observar la cantidad de paquetes transmitidos dentro de la red
Identificar cuáles pueden ser los posibles ataques DoS

6.1.3.3 Tráfico generado. La transmisión de datos fue realizada en la Topología 2. Los *hosts* y los *routers* en IPv6 usan el protocolo *Neighbor Discovery* para generar un enlace con aquellos nodos con los cuales quieren establecer comunicación, manteniendo contacto con aquellos que puedec mantener contacto y eliminar de la caché aquellos que pueden ya no ser válidos.

El protocolo *Neighbor Discovery* define cinco diferentes paquetes ICMP: Router Solicitation que es enviada por el host cuando se activa en la red solicitando información al *router; Router Advertisement* es la respuesta del *router* con información de la red; *Neighbor Solicitation* verifica si un host es todavía alcanzable, *Neighbor Advertisements* que responde la solicitud anterior y verifica si un enlace a cambiado; por último *Redirect* usada por el *router* para avisar cual es el mejor salto para alcanzar el destino.

El comando *flood_router6* utiliza el paquete *Router Advertisement* que permite crear un flujo local falsificando la presencia del router en la red llevando a una denegación de servicio. El comando crea direcciones IP aleatorias como se observa en la Figura 19.

Figura 17. Flujo del comando flood_router6



Fuente. Autor del proyecto

6.1.3.4 Resultados. Puede saturarse el tráfico de una red generando flujo que interfiera en las comunicaciones dentro de la red. Se observa que el 100 % de los paquetes involucrados en la comunicación el 71.14 % corresponden al protocolo ICMPv6. Es decir que de un total de 74.098 paquetes que fueron transmitidos con el protocolo de internet versión 6, 52.714 fueron mensajes de comunicación de paquetes para verificar la conexión entre los nodos de la red, de los cuales el 89.8 % fueron dirigidos a la dirección ff02::1, un total de 47.339 paquetes. Por consiguiente, se deduce la posibilidad de un ataque de denegación de servicio (DoS).

Figura 18. Porcentaje por paquetes Ipv6

Protocol	% Packets
Frame	100,00 %
Ethernet	100,00 %
Internet Protocol Version 6	100,00 %
Internet Control Message Protocol v6	71,14 %
User Datagram Protocol	28,86 %
Domain Name Service	28,27 %
Hypertext Transfer Protocol	0,59 %

Fuente. Autor del proyecto

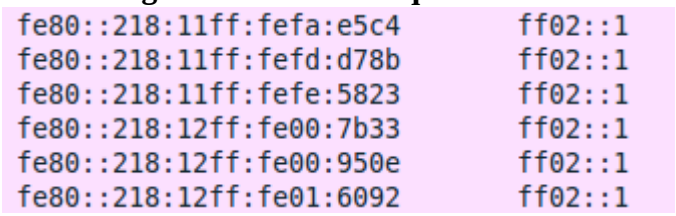
A través de la herramienta *Wireshark* se observa que la captura de paquetes muestra un crecimiento anormal de direcciones IPv6 inexistente en la red configurada; de la cantidad anormal de direcciones IP se reconoce un patrón de crecimiento consecutivo. En la dirección resaltada en la Figura 14 se nota que la dirección siguiente es la 11 y así sigue creciendo cambiando una pequeña parte de los segmentos de la dirección, se

puede ver el cambio en la Figura 15 del segmento 11ff al segmento con valor 12ff, mostrando un raro comportamiento en el flujo de la transmisión.

Figura 19. Direcciones IP generadas en el ataque

Fuente. Autor del proyecto.

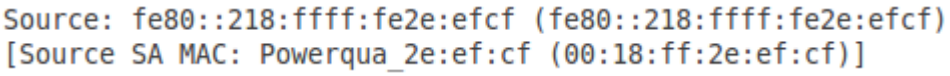
Figura 20. Direcciones IP generadas en el ataque



Fuente. Autor del proyecto.

La herramienta *Wireshark* posibilita el observar que las direcciones MAC de las correspondientes direcciones IPv6 cambian también de forma aleatoria, como se percibe en la Figura 20, mostrada en el panel de protocolos de la herramienta.

Figura 21. Nombre del dispositivo con dirección MAC e IPv6



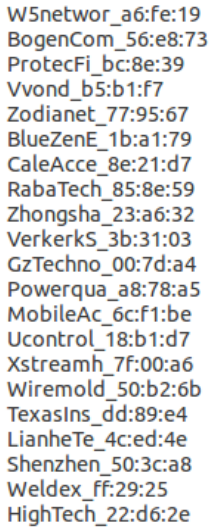
Fuente. Autor del proyecto.

El *sniffer* permite considerar la información de forma global en el menú *Statistics*, en la opción Endpoints, que despliega todos los nodos involucrados en alguna comunicación de la red. La Figura 21 exhibe la cantidad exagerada de direcciones MAC que estuvieron involucradas, indicando un flujo que aparece como dañino para la estabilidad de toda la red.

En la Figura 23 los segmentos TCP contienen el *flag Router Advertisement* activados desde diferentes IP, que no reciben respuesta. Este flujo irregular de repuestas a solicitudes no hechas hacia un router puede ser generado por una característica de la herramienta *Wireshark* del menú Statistics en la opción Flow Graph con lo cual se sigue

el comportamiento de las conexiones TCP, al resaltar las conexiones activas y la orientación de la comunicación.

Figura 22. ID de router falsificados

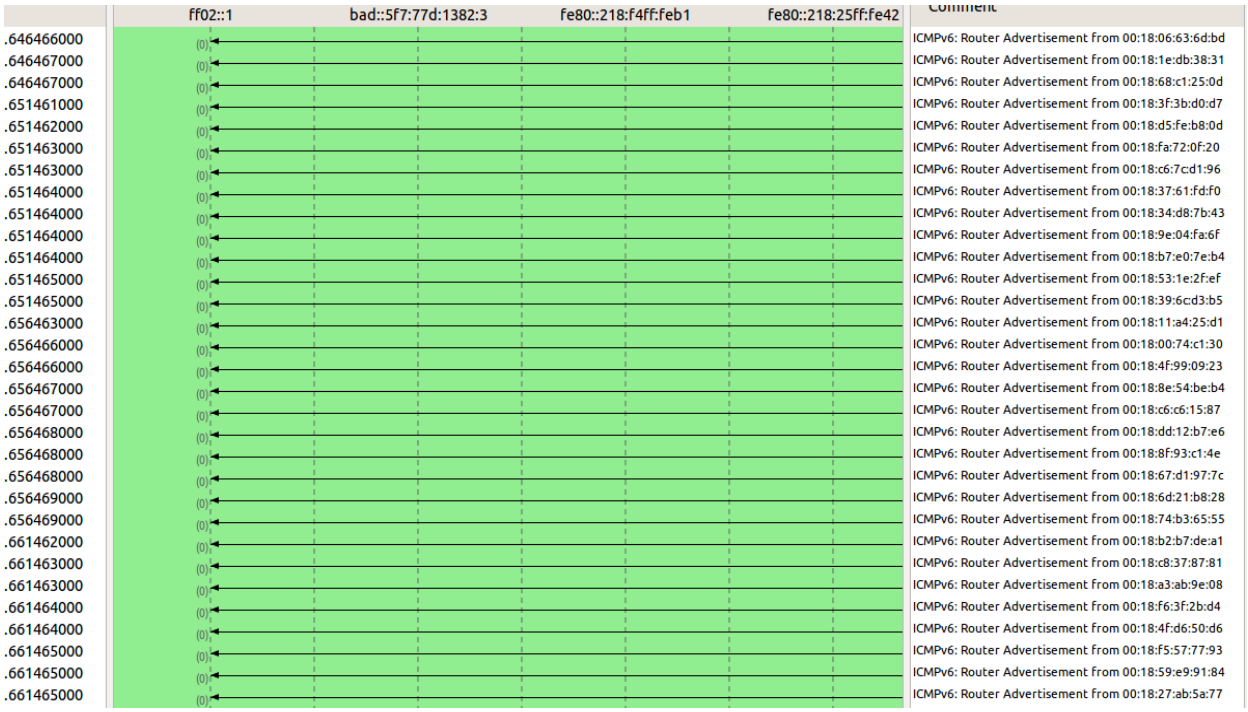


Fuente. Autor del proyecto.

En la primera columna registra intervalos muy cortos entre cada envío del *Router Advertisement* hacia la dirección IP por defecto P ff02::1. Lo anterior, se muestra desventajoso porque por cada conexión se genera una estructura llamada TCB (*Transmission Control Block)* que facilita identificar cada enlace establecido, si la cantidad es muy elevada provoca un colapso en la capacidad del sistema para responder solicitudes de conexión. [125]

[125] BORJA MERINO, F. (2011). *Análisis de tráfico con Wireshark.* Madrid: Inteco cert. Recuperado Junio 29, 2015. https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Figura 23. Flujo de peticiones hacia ff02::1



Fuente. Autor del proyecto.

7 CONCLUSIONES.

La herramienta *Wireshark* ha adquirido notable importancia por su versatilidad para la evaluación de los problemas y comportamientos del tráfico, hecho que se evidencia en la creciente proliferación de documentación que recomienda el uso de la misma tanto para la comprensión de los protocolos en el proceso de comunicación, como por la cantidad de información que ofrece para evaluar el funcionamiento de un entorno de red.

La herramienta *Wireshark* posee diversos filtros que permiten clasificar los paquetes capturados para su clasificación y la identificación de las anomalías dentro de los mismos.

Los ataques configurados en la plataforma Kali Linux para el protocolo IPv6 permitieron con éxito ataques DoS, aunque otros ataques más invasivos como la intrusión en la configuración de una VLAN no está actualizado para el protocolo en su versión 6, por lo cual se permitió identificar con la herramienta *Wireshark* las cantidades de solicitudes que generaban problemas en el funcionamiento de la red.

La herramienta *Wireshark* muestra una gran utilidad para distinguir el comportamiento de los paquetes al clasificarlos en diferentes utilidades estadísticas que permiten evaluar el desarrollo de una transmisión en el tiempo con los componentes involucrados en la misma.

La herramienta en el momento actual de su desarrollo, presenta la información al usuario de forma amigable al permitir diferenciar las diversas capturas de tráfico, y establecer filtros que discriminan los paquetes que desean ser evaluados; sin embargo para identificar anomalías que representen un riesgo para el sistema requiere de la observación de cada paquete para poder clasificarlo como una amenaza.

8 RECOMENDACIONES

Actualizar la documentación sobre la herramienta *Wireshark* dado que gracias a su facilidad de uso y sus capacidades para identificar gran cantidad de protocolos, el interés por la herramienta se perfila de forma creciente dando oportunidades para profundizar en su uso y descubrir múltiples aplicaciones de la misma.

Wireshark al ser un desarrollo de código abierto permite crear funcionalidades que permitan mejorarla para configurar según las necesidades de investigación para el descubrimiento de anomalías.

BIBLIOGRAFIA

ABAD, Cristina; LI, YIfan; LAKKARAJU, Kiran; YIN, Xiaioxin & YURCIK, William. 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.2004 [en línea] doi:10.1.1.5.2004 [citado el 10 de enero de 2015]

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

ALVAREZ CREGO, M. *Analizador de red (sniffer) en entorno GNU*. UOC La universidad virtual. [En línea] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/551/1/35037tfc.pdf [citado el 24 de enero de 2014]

ANDERSON, James. *Computer Security Threat Monitoring and Surveillance.* Fort Washington:1980 [En línea] http://csrc.nist.gov/publications/history/ande80.pdf [citado en 14 de Octubre de 2014]

ASRODIA , Pallavi & PATEL, Hemlata. Analysis of various packet sniffing tools for network monitoring and analysis. *International Journal of Electrical,Electronics and Computer Engineering, 1*(1), 55-58. 2012. [En línea] http://www.researchtrend.net/pdf/13 PALLAVI.pdf [citado en 12 de Octubre de 2014],

ASRODIA, Pallavi & SHARMA, Vishal. Network Monitoring and analysis by packet sniffing method. *International Journal of Engineering trends and Technology (IJETT), 4*(5), 2133-2135. 2013. [En línea] http://www.ijettjournal.org/volume-4/issue-5/IJETT-V4I5P160.pdf [citado en 20 de Octubre de 2014],

BANERJEE, Usha, ASHUTOSH, Vashishtha & SAXENA, Mukul. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of computer applications, 6*(7), 1-5. 2010 [En línea] http://ijcaonline.net/archives/volume6/number7/1092-1427 [citado en 14 de Octubre de 2014]

BARCELÓ ORDINAS, José María; GRIERA, Jordi Iñigo; MARTÍ ESCALÉ, Ramón; PEIG OLIVÉ, Enric & PERRAMON TORNIL, Xavier. *Redes de Computadores* (1ra ed.). Barcelona: Fundació per a la Universitat Oberta de Catalunya.2004

BERGER, Arthur; WEAVER, Nicholas & BEVERLY, Robert. Internet Nameserver IPv4 and IPv6 address relationships. En ACM (Ed.), *Proceedings of the 2013 conference on Internet measurement conference (IMC '13)* (págs. 91-104). New York: Association for Computing Machinery (ACM). [en línea] doi:10.1145/2504730.2504745 [citado el 23 de Octubre de 2014]

BISWAS, Jhilam., & ASHUTOSH, Vashishtha. An Insight in to Network Traffic Analysis using Packet Sniffer. *International Journal of Computer Applications, 94*(11), 39-44. 2014 [En línea] https://www.academia.edu/7847043/An_Insight_in_to_Network_Traffic_Analysis_using_Packet_Sniffer [citado en 14 de Octubre de 2014]

BORJA MERINO, Febrero. *Análisis de tráfico con Wireshark.* Madrid: Inteco_cert. [En línea] https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf [Citado el 25 de junio de 2015]

BRADEN, R.; CLARK, D.; CROCKER, S.; HUITEMA, C. *Security in the internet Architecture.* IETF. 1994

BRINKLEY, Roger. R & SCHELL, Donald. L. (). *Information Security: An Integrated Collection of Essays.* (A. D. Marshal, S. Jajodia, & H. J. Podell, Eds.) Los Alamitos, California, USA: 1995. IEEE Computer Society Press. Annual Computer Security Applications Conference: [En línea] http://www.acsac.org/secshelf/book001/book001.html [citado en 14 de Octubre de 2014]

CELEDA, Pavel. Network Security Monitoring and behavior analysis. 28. [En línea] http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd133.pdf [citado el 7 de septiembre de 2014]

CHAPPEL, Laura. *Wireshark Network Analysis.* San Jose CA: Protocol Analysis Institute. 2012

CICILEO, Guillermo; et al. *IPv6 para todos, Guía de uso y aplicación para diversos entornos.* Buenos Aires: Asociación Civil Argentinos en Internet. [en línea] http://www.consulintel.es/pdf/ipv6paratodos.pdf [citado el 15 de mayo de 2015]

COBB, Stephen. *Manual de seguridad para pc y redes locales.* (J. F. Bienvenido, & A. J. Bosch, Trans.) España: 1992. Windcres Books, Mcgrawhill inc.

CONGRESO De COLOMBIA. *Leyes.* [En línea] http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf [Citado el 10 de Septiembre de 2015]

CORONA, Igino., GIACINTO, Giorgio & ROLI, Fabio. Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues. *Elsevier Inc.*(239), 201-225. 2013 [En línea] http://dx.doi.org/10.1016/j.ins.2013.03.022 [citado en 14 de Octubre de 2014]

DEPARTMENT OF DEFENSE. *Trusted Computer System Evaluation Criteria [the "Orange Book"]*. Ft. Meade, 1985 MD: National Computer Security Center. [En línea] http://csrc.nist.gov/publications/history/dod85.pdf [citado en 14 de Octubre de 2014]

DURDAGI, Emre., & BULDU, Ali. IPv$/IPv6 security and threat comparisons. *Procedia Social and Behavioral Sciences, 2*, 5285-5291. [en línea] doi:10.1016/j.sbspro.2010.03.862 [citado el 28 de mayo de 2015]

FARID, Dewan; HARBI, Nouria; ZAHIDUR Rahman, MOHAMMAD; Mofizur RAHMAN, Chowdhury. Attacks Classification in Adaptive Intrusion Detection using Decision Tree. *World Academy of Science, Engineering and Technology, 39*, 86-90. 2010 [En línea] http://waset.org/publications/5652/attacks-classification-in-adaptive-intrusion-detection-using-decision-tree [Citado el 12 enero de 2014]

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

FREE SOFTWARE FOUNDATION, Inc. GNU Operating System: Licencias. [en línea] http://www.gnu.org/licenses/licenses.es.html> [citado el 24 de Octubre de 2014]

FUNDACIÓN COPYLEFT. Copyleft. [en línea] <http://fundacioncopyleft.org/es/9/que-es-copyleft> [Citado el 14 de octubre de 2015]

GOMEZ, Julio. *Guía de Campo de hackers: aprende a atacar y a defenderte* (1ra ed.). México: 2010 Alfaomega grupo editor S.A.

GONZALEZ, Diego, [En línea] dgonzalez.net: http://dgonzalez.net/pub/ids/IDS_v1.0.pdf [Citado el 21 de octubre de 2015]

GUPTA, Shilpi, & MAMTORA, Roopal. Intrusion Detection System Using Wireshark. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*(11), 358-363. 2012 [En línea] http://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012/V2I11-0205.pdf [Citado el 10 de Noviembre de 2015]

GURLEY, Rebecca. *Intrusion Detection.* Indianapolis: 2000. Macmillan Technical Publishing.

HAZAEL, David. *Contribuciones a la economía*,Eumed, 2014. [En línea]: http://www.eumed.net/ce/2012/tcgz.html [Citado el 10 de Septiembre de 2015]

HAZEYAMA, Hiroaki; UENO, Ukito & SATO, Hirotaka . 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.2011. [en línea] http://www.wide.ad.jp/project/document/reports/pdf2011/cd/02-3_wide-memo-camp1109-hack-v6only-questionnaire-01.pdf [citado el 12 de diciembre de 2015]

HERRERA JOANCOMARTÍ, Jordi., ALFARO GARCIA, Joaquín, & PERRAMÓN TORNIL, Xavier *Aspectos avanzados de seguridad en redes.* Barcelona: Fundación por la Universitat Oberta de Catalunya.2004 [En Línea] http://www.sw-computacion.f2s.com/Linux/012.1-Aspectos_avanzados_en_seguridad_en_redes_modulos.pdf [Citado el 12 de febrero de 2014]

HUNTER, Philip. IPv6: Security Issues. *Network Security, 2004*(1), 17-19. [en línea] doi:10.1016/S1353-4858(04)00026-1 [citado el 24 de abril de 2014]

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Normas colombianas para la presentación de trabajos de investigación. Sexta actualización. Santa fé de Bogotá D.C. ,2002 p.41. NTC 1486.

JAEGER, Trent. Multics. In T. Jaeger, *Operating System Security*. Morgan & Claypool. 2008 Eumed.net http://www.cse.psu.edu/~tjaeger/cse443-s12/docs/ch3.pdf [Citado el 24 de Octubre de 2015]

KENT, S. *IP Authentication Header*. IETF. [En línea] doi: http://dx.doi.org/10.17487/RFC4302 [citado el 30 de septiembre de 2015]

KRUTZ, Ronald L.; & VINES, Russell Dean. *The CEH prep guide: The comprehensive guide to certified ethical hacking.* Indianapolis, Indiana, Estados Unidos de América: Wiley Publishing, Inc. 2007

KUMAR, Sumit & SUDARSAN, Sithu. An Innovative UDP port Scanning Technique. *International Journal of Future Computer and Communication, 3*(6), 381-384. [en línea] doi:10.7763/IJFCC.2014.V3.332 [citado el 22 de enero de 2015]

LAN, Kunchan; HUSSAIN, Alefiya & DUTTA, Debojyoti. Effect of Malicious Traffic on the Network. *SIGCOMM.* ACM.2003. [En línea] http://www.isi.edu/div7/publication_files/effect_malicious.pdf [Citado el 10 de Septiembre de 2015]

LEVIN, Stanford & SCHMIDT, Stephen. IPv4 to IPv6: Challenges,solutions and lessons. *Telecommunications Policy, 38*, 1069-1068. 2014 [En línea] doi:doi:10.1016/j.telpol.2014.06.008 [citado el 25 de enero de 2015]

Mcclure, Stuart; SCAMBRAY, Joel & KURTZ, George.*Hacking Exposed 7* (7ma ed.). New York: McGraw-Hill.2012

MEDINA, L. F. En código abierto. *Revista Arcadia*. [En línea] http://www.revistaarcadia.com/Imprimir.aspx ?idItem=38588 [Citado el 14 de noviembre de 2014]

MINISTERIO DE EDUCACION NACIONAL, Ley 842 de 2003 [En Línea] http://www.mineducacion.gov.co/1621/articles-105031_archivo_pdf.pdf [citado el 24 de junio de 2015]

MUKHERJEE, B., Heberlein, T., & LEVITT, K. (1994). *Network Intrusion Detection.* IEEE. Retrieved from http://wenke.gtisc.gatech.edu/ids-readings/network_id.pdf [Citado el 10 de Septiembre de 2015]

NATIONAL COMPUTER SECURITY CENTER. (1985). *Trusted computer system evaluation Criteria. [The orange book]*. Fort Meade: Deparment of Defense. [En línea] http://csrc.nist.gov/publications/history/dod85.pdf [Citado el 10 de Septiembre de 2015]

OREBAUGH, Angela; RAMIREZ, Gilbert; BURKE, Josh; PESCE, Larry; WRIGHT, Joshua & MORRIS, Greg. Wireshark and Ethereal, Network Protocol Analyzer toolkit. Rockland, 2007 Syngress Publishing Inc. [En línea] http://numenor.cicese.mx/cursos/PSR/Wireshark-book.pdf [Citado el 10 de Septiembre de 2015]

ORZACH, Yoram. Network analysis using Wireshark cookbook. Birmighan, UK, 2013, Packt Publishing.

PARKER, Tim. Aprendiendo TCP/IP en 14 días. México, 1997, Prentice-hall Hispanoaméricana S.A.

PATTERSON, Kenneth. A criptographic tour of the IPsec standards. *Information Security Technical Report, 11*(2), 72-81.2006 [en línea] doi:10.1016/j.istr.2006.03.004 [citado el 23 de agosto de 2015]

PETERSON, Larry. & DAVIE, Bruce. . Computer Networks: A sysems aproach. San Francisco, 2007, Elsevier Inc.

RASTEGARI, Samanesh; HINGSTON, Philip & LAM, Chiou-Peng. Evolving statistical rulesets for network intrusion detection. *Applied Soft Computing, 33*, 348-359. [en línea] doi:10.1016/j.asoc.2015.04.041 [citado el 24 de septiembre de 2015]

RAZZAK A., H. A., HANDA, S., & RAMANA MURTHY, M. Providing the Secure Data Transmission in the Network Using Open Source Packet Analyzer. *International Journal of Computer trends and Technology (IJCTT), 12*(1). 2014 [en línea] doi: 10.14445/22312803/IJCTT-V12P103 [citado el 12 de junio de 2015]

SANDERS, Chris. (2011). Practical Packet Analisis. New York: No Starch Press Inc. [En línea] http://repository.root-me.org/R%C3%A9seau/EN%20-%20Practical%20packet%20analysis%20-%20Wireshark.pdf [Citado el 16 de marzo de 2015]

SEIFRIED, Karl. Diseccionamos el tráfico de red *Wireshark*. *Linux magazine*, 8-9. [En línea] http://www.linux-magazine.es [citado el 12 de noviembre de 2014]

SHERIF, Joseph, & DEARMOND, Tommy. (Junio 10). Intrusion Detection: Systems and Models. IEEE Computer Society, 115, 2002. [En línea] http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/8879/1/02-1439.pdf [Citado el 18 de marzo de 2015]

STALLINGS, William. Fundamentos de Seguridad en redes, aplicaciones y estándares. Mexico:Pearson Educación, 2004

STALLINGS, William. Data and Computer communications.8va ed. Upper Saddle River: Pearson Education, Inc., 2007 [En línea] http://memberfiles.freewebs.com/00/88/103568800/documents/Data.And.Computer.Communications.8e.WilliamStallings.pdf [Citado el 15 de abril de 2015]

TANENBAUM, Andrew, & WETRERALL, David. Computer networks.5ta ed.Massachusetts: Pearson Education Inc., 2011. [En línea] http://cse.hcmut.edu.vn/~minhnguyen/NET/Computer Networks - A Tanenbaum - 5th edition.pdf [Citado el 15 de abril de 2015]

TECHTARGET-SEARCHSECURITY. *Techtarget-SearchSecurity.* Retrieved from Monitoring Network traffic and Network forensics: [En línea] http://searchsecurity.techtarget.com/ehandbook/How-to-make-threat-monitoring-effective-in-these-tough-times [Citado el 24 de enero de 2016]

TECNOLÓGICO DE MONTERREY. *Planer y construir borradores*. Obtenido de Crea: Centro de recursos para la escritura académica: [En línea] http://sitios.ruv.itesm.mx/portales/crea/planear/como/planteamiento_tesis.htm [citado el 24 de noviembre de 2014]

TITTEL, Ed. Redes de computadoras. España: McGraw-Hill Interamericana S.A. 2004

TRICAS GARCIA, Fernando. Ética y Seguridad en la red. *Uninet*, 1-13. [En línea] http://doctorado.uninet.edu/2004/cinet2004/ftricas/seguridadYPrivacidad.pdf [citado el 3 de noviembre de 2014]

VILLALÓN Huerta, Antonio. (2002). Seguridad en UNIX y redes. Cuenca: GNU Free Documentation License. [En línea] https://www.rediris.es/cert/doc/unixsec/unixsec.pdf [Citado el 15 de mayo de 2015]

ANEXOS

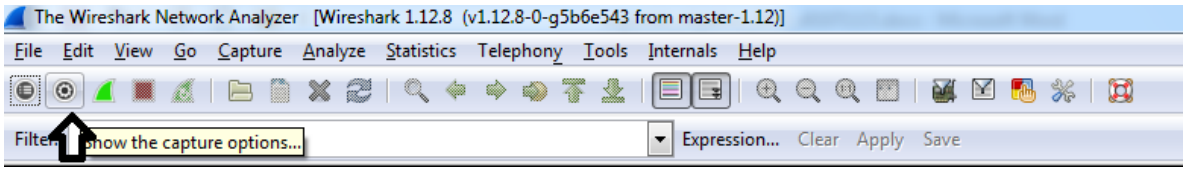
ANEXO A. Locación de Wireshark.

Para comenzar el uso de la herramienta es importante decidir dónde colocar la herramienta para realizar el test de una red.[126] Lo ideal sería colocarlo en el lugar donde se quiere monitorizar el flujo de la información y conectarlo al mismo *switch*, donde se puede configurar el *port mirroring* para permitir que todo el tráfico que entra y sale puede ser capturado por la herramienta.
Cuando no se tiene acceso a los dispositivos que quieren evaluarse puede llevarse a cabo un MitM (*Man in the Middle*). Debe entenderse que es un método ofensivo y es preferible usar en entornos no críticos del sistema donde se perciba que es necesario capturar el tráfico. El método se conoce con *ARP spoof* que consiste en contaminar la caché de los equipos involucrados con IP/MAC falsas, para que reenvíen el tráfico a la maquina donde se encuentra instalada la herramienta.

Interfaz de captura.

La herramienta *Wireshark* ofrece varias opciones para iniciar una captura de paquetes. En la Figura 1. Muestra el botón que lista las interfaces de captura disponibles, donde al hacer clic despliega una ventana con las interfaces activas en la cuales puede realizarse la captura, como muestra la Figura 2.

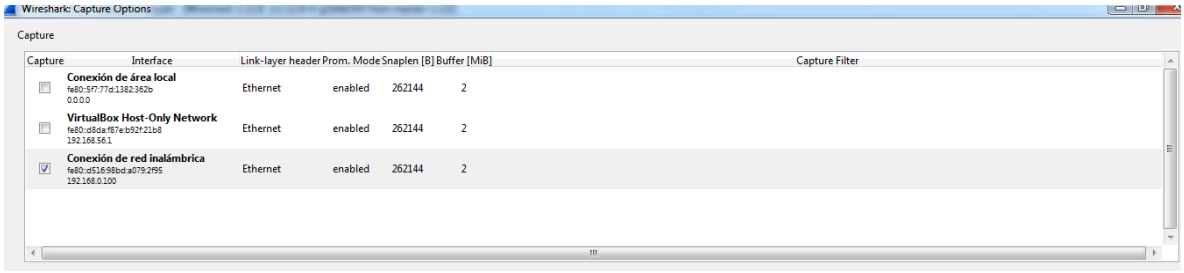
Figura 24. Botón para elegir interfaz de red.



Fuente. Autor del proyect

126 ORZACH, Yoram. Network analysis using Wireshark cookbook. Birmighan (UK). Packt Publishing. 2013.

Figura 25. Opciones de captura.



Fuente. Autor del proyecto

ANEXO B. Configuración de las VLAN

Configuración en el switch.

```
Switch>enable
Creación  y configuración  VLAN 10
Switch#vlan database
Switch(vlan)#vlan 10 name red1
Switch(vlan)#exit
Switch(config)#interface fastethernet 0/1-2
Switch(config-if)#switchport mode access vlan 10
Router>enable
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#interface GigabitEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q  10
Router(config-subif)#ip address 2607:f0d0:2001:a::5/64
```

```
Creación  y configuración  VLAN 20

Switch#vlan database
Switch(vlan)#vlan 20 name red2
Switch(vlan)#exit
Switch(config)#interface fastethernet 0/3-4
Switch(config-if)#switchport mode access vlan 20
Router>enable
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0.20
Router(config-if)#no shutdown
Router(config-if)#interface GigabitEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q  20
Router(config-subif)#ip address 2607:f0d0:2001:b::6/64
```

```
Creación  y configuración  VLAN 99

Switch#vlan database
Switch(vlan)#vlan 99 name manegement
Switch(vlan)#exit
Switch(config)#interface fastethernet 0/5
Switch(config-if)#switchport mode access vlan 99
Switch(config-if)#switchport mode trunk
```