WIRESHARK, UNA HERRAMIENTA DE APOYO PARA ANÁLISIS DE TRÁFICO MALICIOSO

SERGIO ALVERNIA ACEVEDO
Estudiante de la Facultad de Ingenierías
Semillero de Investigación GNU/Linux And Security, SIGLAS.
Investigador Grupo INGAP
Universidad Francisco de Paula Santander Ocaña
saalverniaa@ufpso.edu.co

M.Sc. DEWAR RICO BAUTISTA
Director del Semillero de Investigación SIGLAS
Semillero de Investigación GNU/Linux And Security, SIGLAS
Grupo INGAP, Facultad de Ingenierías
Universidad Francisco de Paula Santander Ocaña
dwricob@ufpso.edu.co

Fecha de recepción: 10 de abril de 2014
Fecha de aprobación: 09 de septiembre de 2014

RESUMEN
Los avances al abordar las tecnologías de la información han obligado a los usuarios finales a tener consideración frente a nuevos aspectos que los obligan a comportarse de una manera más responsable y controlada en el momento de manipular la información. Para lo cual, una propuesta para mantener un control sobre la información que transmiten los dispositivos finales son piezas de software conocidas como sniffers, que permiten capturar de manera constante los datos para establecer un análisis del comportamiento de los datos. De los diferentes sniffers que pueden encontrarse hemos elegido la herramienta Wireshark para establecer los posibles usos que puede ofrecer para proponer medidas de seguridad oportunas para una organización por lo cual se hizo una revisión de literatura con respecto a las potencialidades que ofrece la herramienta y una utilización de la misma en un ambiente controlado a nivel local.

PALABRAS CLAVES
Direccionamiento, protocolos, seguridad, tráfico de redes, Wireshark

ABSTRACT
New advances in addressing information technology have forced end users to have account new aspects that require them to behave in a more responsible and controlled, at the time to manipulate information. So, for which a proposal to maintain control on the information conveyed by the end devices are pieces of software called sniffers, that capture data consistently to establish a behavioral analysis of the data. Of different sniffers that can be found we chose the Wireshark tool to establish the possible uses that can offer to propose appropriate safety measures for an organization which was a review of literature on the potential offered by the tool and a use thereof a locally controlled environment.

KEYWORDS
Addressing, Protocols, Security, Network traffic, Wireshark

INTRODUCCIÓN
El desarrollo de una herramienta trae consigo la generación de nuevos retos para su uso, dado que así como la novedad permite la realización de actividades nunca imaginadas, también implica el desarrollo de nuevas habilidades y la consideración de nuevos riesgos. Una novedad que ha golpeado a la humanidad de manera tal que ha cambiado la manera de percibir la realidad completa ha sido la creación de una red de redes conocida como Internet, que ha posibilitado que la comunicación entre las personas sea mucho más eficiente, pero que invita a tener mucho mas cuidado.

Con el rápido crecimiento de las implementaciones tecnológicas ha marcado una gran diferencia en la manera como se recoge, transporta, almacena y procesa la información, lo que permite a las organizaciones establecerse en una zona geográfica mucho más amplia sin una gran inversión en infraestructura y conociendo con facilidad el estado de cualquier oficina con el solo hecho de presionar un botón. Esto es facilitado por el uso de computadoras dado que cualquier institución por pequeña posee una o dos de ellas. (Tanenbaum&Wetrerall, 2011) (Rico, 2007) (Rico, 2011)

Un inconveniente, por lo tanto, de los nuevos avances es que las personas desconocen por completo del funcionamiento de las nuevas tecnologías y las reglas que subyacen a su uso, sus operaciones y mecanismos que hacen posible que pueda enviarse un mensaje de manera relativamente rápida. Por consiguiente, es necesario mantener un control sobre los recursos de la empresa para asegurar que éstos pueden conservar su integridad, verificando la articulación de las medidas necesarias para maniobrar en medio de los riesgos y así no comprometer las actividades que son importantes en una empresa, y deben ser consideradas primordiales para su funcionamiento óptimo (Tittel, 2004).

En consecuencia, comprender que es vital establecer estándares dada la complejidad que genera mantener la interconexión entre las personas y los dispositivos finales que aquellas manejan (Stallings, 2004) (Forouzan, 2002).

DESARROLLO

La seguridad permite separar cualquier amenaza que pueda afectar un recurso de información relevante, entendiendo como amenaza cualquier actividad que pueda significar un daño potencial para los activos más importante, que en nuestro caso sería la información, (Tittel, 2004) (Halsall, 2004). De modo que es necesario la generación de políticas de seguridad que cumplan con las necesidades de cada organización porque no existe un tipo de seguridad genérica. (Unión Internacional de Telecomunicaciones, 2005).
Deben definirse responsables de la seguridad que reconozca de manera sistemática los requisitos de seguridad y caracterizar los enfoques para encontrar la manera más eficiente de separar la forma como una amenaza puede acceder a los recursos de una organización (Stallings, 2004). Cuando se consideran sólo los beneficios y las ventajas sin considerar los posibles perjuicios como cuando la privacidad es vulnerada, porque al estar la información disponible de forma digital es fácil acceder<< a ella mientras alguien sepa cómo hacerlo. (García, s.f.) (Rico, 2009) (Rico, 2008).

En consecuencia, es necesario saber cómo funciona una red en condiciones normales para que se pueda reaccionar ante las operaciones inusuales y anormales dentro del tráfico que pasa por la red, y que se administra. Una manera de conocer cómo funciona la red normalmente es usando un sniffer o analizador de red en varios puntos de la red. (Orebaugh, Ramirez, Burke, Morris, Pesce& Wright, 2007).

Los sniffers son importantes porque permiten monitorear la red para solucionar problemas y llevar un registro de todas las actividades que generan las actividades de la red (Asrodia&Patel, 2012).

Un sniffer o analizador de red es un programa que captura todos los datos que pasan a través de una tarjeta de red. Para ello se basa en un defecto del protocolo Ethernet (Herrera Joancomartí et al, 2004). El protocolo de Ethernet trabaja enviando la información del paquete a todos los hosts en el mismo circuito. La cabecera del paquete contiene la dirección apropiada de la máquina destino. Solamente la máquina con la dirección que va en la cabecera se supone que acepta el paquete. (Crego, 2005) (Johnson, 2008) (Lobo, 2012).

Fue a comienzos de 1980, cuando comienza a acuñarse la noción de detección de intrusiones, para lo cual se buscaba la manera de establecer la auditoría en las redes que permitiría entender los desvíos y comportamientos de la misma a través del análisis de patrones, lo cual reduce todo a buscar "una aguja en un pajar" (Banerjee,Vashishtha&Saxena, 2010). Esto puede generar esta cantidad de información por analizar, una gran preocupación en un administrador de red, ya que es difícil establecer un análisis de todos y cada uno de los datos que se transmiten. Sin embargo, la labor es necesaria porque permite considerar los malos funcionamientos y tomar medidas con respecto a la seguridad o a la calidad de las transmisión de la información de manera oportuna; y siempre debe considerarse que habrá actividad anormal dentro de la red (Sanders, 2011).

Dentro de los sistemas para detectar intrusiones, puede reconocerse una variedad de implementaciones, pueden ser basados en host o basados en red. Los basados en host buscan detectar el tráfico de información dentro de un servidor y los basados en red monitorean la red para detectar las intrusiones. La plataforma que interesa será la basada en red que lleva un registro de los paquetes, el tráfico IP en tiempo real y trata de descubrir los intrusos que tratan de ingresar al sistema (Farid,Harbi, Bahri, Rahman & Rahman, 2010). Llevar éste registro puede facilitar la instauración de políticas apropiadas que protejan un sistema.
Una de las herramientas para análisis de tráfico en red utilizadas en la actualidad es la herramienta Wireshark (Banerjeeet al, 2010), que es uno entre los diversos sniffers que se encuentran para la captura y análisis del tráfico en la red, su popularidad se debe a que cuenta con una interfaz gráfica que facilita la interpretación de la información capturada; Wireshark tiene la capacidad de "entender" los protocolos utilizados por la red mostrando información relevante para mostrar la manera como han viajado paquetes específicos dentro de la misma (Asrodia&Patel, 2012). A diferencia de otros sniffers como Tcpdump no tiene una interfaz gráfica de usuario y no poder desplegar toda la información que concierne a un paquete en específico(Asrodia&Patel, 2012); lo que hace que Wireshark sea una herramienta apropiada para el análisis de tráfico de red (Crego, 2005), 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 (Seifried, 2010) diferentes, simplificando el trabajo de análisis por poseer filtros que permiten definir criterios para interpretar la información según el protocolo que se desee analizar (Merino, 2011).

METODOLOGÍA PROPUESTA

La metodología que se propone para organizar el proyecto será considerada en varias etapas que permitan un avance progresivo del mismo.
En la primera etapa, lo que se ha buscado es obtener la documentación de manera completa teniendo como marco las temáticas principales en el área de análisis de tráfico en bibliografía técnica y artículos en revistas especializadas y así mostrar la importancia de abarcar la necesidad de un conocimiento entorno a la funcionalidad de los analizadores de red sobre el protocolo de red TCP/IP.
Las referencias fueron indagadas en diferentes bases de datos como ACM, Sciencedirect, SCOPUS, entre otras, dentro de las cuales se seleccionaron las referencias más recientes acerca de la herramienta Wireshark, protocolos TCP/IP, tráfico malicioso. Después de lo cual se procedió a escoger las 50 referencias más relevantes que aportaron sus elementos teóricos más significativos a la propuesta, concluyendo con un estado del arte.
En la segunda y tercera etapa lo que buscamos es la apropiación de las funcionalidades de la herramienta Wireshark para el sondeo y observar la utilidad de la misma como herramienta de verificación de seguridad de un sistema.

CONCLUSIONES

Para establecer medidas apropiadas de seguridad que garanticen la seguridad de la información, debe establecerse el uso de herramientas apropiadas para implementar medidas acertadas (Braden, Clark,Crocker&Huitema, 1994).
Es necesario reconocer que la seguridad no se reduce a utilizar firewalls (cortafuegos) para que impidan que cualquier actividad sospechosa pueda ser evitada corriendo con el riesgo de aislarse del flujo de la información.
La buena seguridad depende de que se realice una labor dispendiosa dependiendo de la cantidad de máquinas que sean administradas. El 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.

REFERENCIAS BIBLIOGRÁFICAS

Asrodia, P., &Patel, H. (2012). Network traffic analysis using packet sniffer. International Journal of Engineering Research and Applications, 2(3). Recuperado de http://www.ijera.com/papers/Vol2_issue3/EQ23854856.pdf

Asrodia, P., &Patel, H. (2012). Analysis of various packet sniffing tools for network monitoring and analysis.International Journal of Electrical, Electronics and Computer Engineering, 1(1), 55-58. Recuperado de http://www.researchtrend.net/pdf/13 PALLAVI.pdf

Asrodia, P., & Sharma, V. (2013).Network monitoring and analysis by packet sniffing method.international Journal of Engineering Trends and Technology (IJETT), 4(5), Recuperado de http://www.ijettjournal.org/volume-4/issue-5/IJETT-V4I5P160.pdf

Banerjee, U., Vashishtha, A., &Saxena, M. (2010). Evaluation of the capabilities of Wireshark as a tool for intrusion detection.International Journal of Computer Applications, 6(7), Recuperado de Http://webcache.googleusercontent.com/search?q=cache:beNIKcA0ACUJ:www.researchgate.net/publication/46280039_Evaluation_of_the_Capabilities_of_WireShark_as_a_tool_for_Intrusion_Detection/file/3deec519eb16b798ef.pdf&cd=1&hl=en&ct=clnk&client=ubuntu

Berger,Arthur, Weaver,Nicholas, Beverly,Robert& Campbell, Larry. (2013). Internet nameserver IPv4 and IPv6 address relationships. In Proceedings of the 2013 conference on Internet measurement conference (IMC '13).ACM, New York, NY, USA, 91-104. DOI=10.1145/2504730.2504745 http://doi.acm.org/10.1145/2504730.2504745

Bernal, C. A. (2006). Metodologia de la Investigación (Segunda ed.). Mexico: Pearson Educación

Blanchet, M. (2008, April).Special-use ipv6 address.RFC 5156 Recuperado de http://tools.ietf.org/html/rfc5156

Braden, R., Clark, D., Crocker, S., &Huitema, C. (June 1994). Report of IAB Workshop on Security in the internet Architecture.RFC 1636 (Proposed Standard).

Celeda, P. (September).Network security and behavior analysis. CESNET led working group on network monitoring: Recuperado de http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-cbpd133.pdf

Cicileo, G., Gagliano, R., O'Flaherty, C., Olvera Morales, C., PaletMartinez, J., Rocha, M., y otros. (2009). IPv6 para todos, Guía de uso y aplicación para diversos entornos. Buenos Aires: Asociación Civil Argentinos en Internet.

Crego, M. (2005). Analizador de red (sniffer) en entorno GMU. Cataluña: UOC Universidad virtual. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/551/1/35037tfc.pdf

Czyz,J., Lady,K., Miller,S. G., Bailey,M.,Kallitsis, M.&Karir, M. 2013. Understanding IPv6 internet background radiation.In Proceedings of the 2013 conference on Internet measurement conference (IMC '13). ACM, New York, NY, USA, 105-118. DOI=10.1145/2504730.2504732 http://doi.acm.org/10.1145/2504730.2504732

Deering, S., &Hinden, R. (December 1998). Internet Protocol, Version 6 (IPv6). RFC 2460 (Proposed Standard).Actualizadopor RFCs 5095, 5722, 5871, 6437,6564,6935,6946

Farid, D., Harbi, N., Bahri, E., ZahidurRahman, M., &MofizurRahman, C. (2010).Attacks classification in adaptive intrusion detection using decision tree.Recuperado de http://www.waset.org/journals/waset/v39/v39-16.pdf

Forouzan, B. (2002). Transmisión de datos y redes de comunicación. McGraw-Hill Interamericana S.A.

García, F. T. (s.f.). Ética y seguridad en la red. Zaragoza: Centro Politécnico Superior de la Universidad de Zaragoza. Recuperado de: http://doctorado.uninet.edu/2004/cinet2004/ftricas/seguridadYPrivacidad.pdf.

Hallberg, B. A. (2007). Fundamentos de redes. (4ta Ed.). MéxicoD.F.:McGraw Hill/Interamericana Editores S.A.

Halsall, F. (2004). Comunicación de datos, redes de computadores y sistemas abiertos. Addison, Wesley and Longman.

Hazeyama,Hiroaki,Yamagishi,Yudai,Ueno, Yukito,Yokoishi, Takehiro, Sato, Hirotaka&Ishibashi,Hisatake. (2011). How much can we survive on an IPv6 network?: experience on the IPv6 only connectivity with NAT64/DNS64 at WIDE camp 2011 Autumn. In Proceedings of the 7th Asian Internet Engineering Conference (AINTEC '11). ACM, New York, NY, USA, 144-151. DOI=10.1145/2089016.2089041 http://doi.acm.org/10.1145/2089016.2089041

Herrera Joancomartí J., Alfaro García J., PerramonTornil X.. (2004). Aspectos avanzados de seguridad en redes. Barcelona: Fundació por a la UniversitatOberta de Catalunya. Recuperado de: http://www.sw-computacion.f2s.com/Linux/012.1-Aspectos_avanzados_en_seguridad_en_redes_modulos.pdf

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

Huerta, A. V. (2002). Seguridad en UNIX y redes.GNU Free DocumentationLicense. Recuperado de: http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1.pdf

Johnson, A. (2008). Routing Protocols and concepts CCNA Exploration Labs and Study guide instructor edition.Cisco Press. Recuperado de: http://www.fruned.com/dwn/Routing-Protocols-and-Concepts-CCNA-Exploration-Labs-and-Study-Guide.pdf

Katz, M. (2013). Redes y seguridad. (1ra ed.). Buenos Aires, Argentina: Alfaomega Grupo Editor Argentino.

Lamping, U. (2004-2011). User's Guide: for Wiresha

roceeding of Passive and Active Measurement Workshop (PAM),Recuperado de http://www.isi.edu/div7/publication_files/effect_malicious.pdf

Lobo, Josué. y Rico, Dewar. (2012). Implementación de la seguridad del protocolo de internet versión 6. Revista Gerencia Tecnología Informática. Informatics Technology Management. rk 1.9.(R. Sharpe, Ed.). Recuperado de:http://www.Wireshark.org/download/docs/user-guide-a4.pdf

Lan, K., Hussain, A., &Hussain, A. (2003). Effect of
malicious traffic on the network.P Universidad Industrial de Santander, ISSN 1657-8236, Vol. 11, No 29, Ene – Abr 2012, pp 35 – 46.

López Monge, A. (2005). Aprendiendo a programar con libpcap. Recuperado de http://www.e- ghost.deusto.es/docs/2005/conferencias/pcap.pdf

Mantora, R., & Gupta, S. (2012). Intrusion detection systemusing Wireshark. International Journal of Advanced Research in Computer Science and Software Engineering, 2(11), Recuperadode http://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012/V2I11-0205.pdf

Markey, J. (2011, Junio 5).Using decision tree analysis for intrusion detection: How-to guide.Recuperado de https://www.sans.org/reading-room/whitepapers/detection/decision-tree-analysis-intrusion-detection-how-to-guide-33678

McClure, S., Scambray, J., & Kurtz, G. (2009).Hackers 6: Secretos y soluciones de seguridad en redes. (10ma ed.). México D.F.: McGraw Hill/Interamericana Editores S.A.

Merino, F. B. (2011). Análisis de Tráfico con Wireshark.Madrid: INTECO. Recuperado de: http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_Wireshark.pdf

Northcutt, S., & Novak, J. (2003).Network intrusion detection.(3ra Ed.). New Riders Publishing: Recuperado de http://csnotes.upm.edu.my/kelasmaya/pgkm20910.nsf/de8cc2082fc4d31b4825730e002bd111/ccdb136a3174bb5f482577680001cd08/$FILE/ebook-NID-northcutt2002.pdf

Orebaugh A., Ramirez G., Burke J., Morris G., Pesce L. &WrightJ..(2007). Wireshark and Ethereal, Network Protocol Analyzer Toolkit.Syngress media. Recuperado de: http://numenor.cicese.mx/cursos/PSR/Wireshark-book.pdf

Parker, T. (1996). Aprendiendo TCP/IP en 14 días: Prentice-Hall Hispanoamérica S.A.

Paxon, V., Asanovic, V., Lockwood, J., Dharmapurikar, J., Pang, R.,
Sommer, R., & Weaver, N. (2006, Agosto 4).Rethinking hardware support for network analysis and intrusion prevention.Recuperado de http://www.icir.org/vern/papers/hotsec06.pdf

Postel, J. & Reynolds, J. (1988, February). "A Standard for the Transmission of IP Datagrams over IEEE 802 Networks", RFC-1042, Recuperado de http://tools.ietf.org/pdf/rfc1042.pdf

Qaeder, M. A., Khan, A. H., Habeed, A. A., &Hafeez , M. A. (2010). Bottleneck analysis and traffic congestion avoidance.International conference and workshop on emerging trends in technology (ICWETT), Mumbai, India. Recuperado de https://www.researchgate.net/publication/4311348_Bottleneck_Analysis_of_Traffic_Monitoring_using_Wireshark

Ramachandran, V. (2011). Backtrack 5 wireless penetration testing beginner\. Birmighan, UK: Packt Publishing.

Regis do Santos, R., Moreiras, A., Ascenso Reis, E., &Soares da Rocha, A. (2010). Curso IPv6 Básico. Sao Paulo: Internet Society y LACNIC.

Rico, Dewar y Santos, L. M. (2009). Seguridad de Protocolo de Internet: Estado Del Arte. Revista INGENIO, Universidad Francisco de Paula Santander Ocaña, ISSN 2011-642X, Vol. 2, No 1, Diciembre 2009, pp 79 – 90.

Rico, Dewar y Santos, L. M. (2008). IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA. Revista Scientia et Technica, Universidad Tecnológica de Pereira, ISSN 0122-1701, vol. XIV, No 39, Septiembre 2008, pp. 320 -325. Disponible en: <http://www.utp.edu.co/php/revistas/ScientiaEtTechnica/docsFTP/111011320-325.pdf>\

Rico, Dewar y Santos, L. M. (2007). IPv6 en la Universidad de Pamplona: estado del arte. Revista Scientia et Technica, Universidad Tecnológica de Pereira, ISSN 0122-1701, vol. XIII, No 37, Septiembre 2007, pp. 415-420.

Rico, Dewar. (2011). Redes y tecnologías de banda ancha, tecnologías de acceso de banda ancha. Revista Colombiana de Tecnologías de Avanzada, Universidad de Pamplona, ISSN: 1692-7257, vol. 1, No 17, Enero 2011, pp. 113-120.

RTI (2011).Using Wireshark with RTI data distribution service.Sunnyvale, C.A.: Real-Time Innovations, Inc.

Saha, A., & Das, A. (2012).A detailed analysis of the issues and solutions for securing data in cloud.Journal of Computer engineering (IOSRJCE), 4(5), 11-18.Recuperado de http://www.iosrjournals.org/iosr-jce/papers/Vol4-issue5/C0451118.pdf

Sanders, C. (2011).Practical Packet Analysis. No Starch Press Inc. Recuperado de: http://library.pirates-crew.org/Network/No_Starch_Press_-_Practical_Packet_Analysis_[]_(2007)_en.pdf.

Seifried, K. (2010). Diseccionamos el tráfico de red Wireshark. Linux magazine, 8-9. Recuperado de: http://www.linux-magazine.es

Stallings, W. (2004). Fundamentos de Seguridad en redes, aplicaciones y estándares. México: Pearson Educación. Comunicaciones y redes de computadores. (7ma ed.). México: Pearson Educación S.A.

Stuttard, D., & Pinto, M. (2011).The web application hacker's handbook.(2nd Ed.). Indianapolis, Indiana USA: Wiley Publishing Inc.

Sukhai N. B. (2004). Hacking and cybercrime.In Proceedings of the 1st annual conference on Information security curriculum development (InfoSecCD '04).ACM, New York, NY, USA, 128-132. DOI=10.1145/1059524.1059553 Recuperado de: http://delivery.acm.org/10.1145/1060000/1059553/p128-sukhai.pdf?ip=201.245.172.132&id=1059553&acc=ACTIVE%20