Herramientas de monitorización y análisis del tráfico en redes de datos

INTRODUCCIÓN

Existen varios tipos de herramientas que se encargan del monitoreo y análisis de la red. En particular, los denominados sniffers son de gran utilidad. La palabra sniffer es una marca registrada de Network Associates, Inc. En la actualidad sniffer es una denominación aceptada para aquellas herramientas cuya función principal es monitorizar y analizar tráfico, o sea, examinar paquetes, protocolos y tramas enviadas a través de la red. La captura y visualización de las tramas de datos por sí sola puede no ser muy útil o eficiente, es por ello que los analizadores de protocolos también muestran el contenido de los datos de los paquetes [1]. Teniendo los paquetes de datos y la información del flujo de tráfico, los administradores pueden comprender el comportamiento de la red, como por ejemplo las aplicaciones y servicios disponibles, la utilización de los recursos de ancho de banda y las anomalías en materia de seguridad, por citar algunos ejemplos. Los sniffers han formado parte de las herramientas de gestión de redes desde hace bastante tiempo y han sido usados fundamentalmente con dos objetivos: apoyar a los administradores en el correcto funcionamiento y mantenimiento de la red a su cargo, o para facilitar a aquellos individuos malintencionados a acceder e irrumpir en computadoras, servidores y dispositivos como routers y switches.

Generalidades

Un sniffer puede estar basado en hardware y/o software, pero todos interceptan y recolectan el tráfico local. Luego de capturar el tráfico, el sniffer provee la posibilidad de decodificarlo y realizar un análisis simple del contenido de los paquetes para luego mostrar los resultados obtenidos de manera que pueda ser interpretado por los especialistas. En esta categoría la información del flujo de tráfico es local, o sea, un sniffer puede capturar aquel paquete que se encuentra circulando por la red a la cual él tiene acceso. Sin embargo, para capturar tráfico de varias redes se pueden habilitar algunas técnicas adicionales o debe ser modificada la infraestructura de la red. Un ejemplo es el empleo de la técnica de puerto espejo para lograr que los conmutadores (switches) copien todos los paquetes de datos hacia un puerto donde se ubica el sniffer [2].Para poder hacer uso de los sniffers de paquetes en redes cableadas se debe tener en cuenta que las tarjetas de red Ethernet están construidas de tal forma que, en su modo normal de operación, sólo capturan las tramas que van dirigidas hacia ellas o vienen con una dirección física de broadcast o multicast donde estén incluidas. Por tanto, en condiciones normales, no todo el tráfico que llega a la interfaz de red es procesado por lo que resulta necesario activar un modo especial de funcionamiento de la tarjeta, conocido como modo promiscuo. En este estado, la tarjeta de red procesa todo el tráfico que le llega, siendo éste el modo de trabajo que un sniffer necesita para llevar a cabo su misión.

En el caso particular de los sniffers de redes inalámbricas, la mayor parte de las veces se pretende ver los datos transferidos entre un punto de acceso y un cliente (computadora o algún otro dispositivo móvil) asociado a este, o entre dos nodos conectados en modo ad hoc. Al igual que en las redes cableadas, se deben chequear algunos aspectos: la tarjeta de red

inalámbrica debe permitir ser puesta en modo monitor, se necesita escoger el sistema operativo donde se trabajará y en dependencia, se deberán instalar los programas y el driver que permita que la tarjeta trabaje ese modo.

Características comunes

En la actualidad los sniffers de paquetes se han vuelto extremadamente populares en el mundo de las redes de comunicaciones, por lo que varias compañías desarrolladoras de software han elaborado su variante de este producto. Existe una buena cantidad de sniffers en el mercado que ofrecen determinadas prestaciones, de las cuales se mencionan a continuación las más relevantes para la gestión de la red:

- Escucha de tráfico en redes LAN (Local Area Network) y WLAN (Wireless LAN).
- Captura de tráfico a través de las diferentes interfaces de red de la computadora.
- Capacidad de examinar, salvar, importar y exportar capturas de paquetes en diferentes formatos de captura, tales como: PCAP (Packet Capture), CAP, DUMP, DMP, LOG.
- Comprensión de protocolos de las diferentes capas de la arquitectura de comunicaciones, como por ejemplo: DHCP (Dynamic Host Configuration Protocol), GRE (Generic Routing Encapsulation), TCP (Transmission Control Protocol), entre otros.
- Aplicación de filtros para limitar el número de paquetes que se capturan o se visualizan.
- Cálculo de estadísticas y gráficas detalladas con indicadores como paquetes trasmitidos y perdidos, velocidad promedio de transmisión, gráficos de flujo de datos, entre otras.
- Detección de los nodos que se encuentran en la red, ofreciendo información como sistema operativo, fabricante de la interface, entre otras.
- Reconstrucción de sesiones TCP.
- Análisis y recuperación de tráfico VoIP (Voice over IP).
- Generan reportes de tráfico en tiempo real y permiten configurar alarmas que notifiquen al usuario ante eventos significativos como paquetes sospechosos, gran utilización del ancho de banda o direcciones desconocidas [3, 4].

Muchos de estos programas son totalmente gratis y/o de código abierto, aunque no es menos cierto que la gran mayoría de los sniffers comerciales proveen herramientas de análisis más sofisticadas e interfaces de usuario más amigables.

Aplicaciones de los sniffers

Los usos típicos de un sniffer, ya sea por administradores de red o intrusos, incluyen los siguientes [5]:

- Conversión del tráfico de red en un formato entendible por los humanos.

- Visualización de información relevante como un listado de paquetes y conexiones de red, estadísticas detalladas de las conexiones IP, entre otras.
- Captura automática de contraseñas enviadas en claro y nombres de usuario de la red.
- Análisis de fallos para descubrir problemas en la red, como puede ser la no comunicación entre dos computadoras.
- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella.
- Recuperación íntegra de ficheros y mensajes intercambiados.
- Detección de puntos de acceso no autorizados.
- Detección de intrusiones.

Breve caracterización de herramientas

A continuación se describen brevemente algunos sniffers de amplio despliegue en la comunidad internacional, tanto comerciales como de software libre.

Tcpdump

Es un analizador de paquetes que corre en modo consola. Posibilita al usuario interceptar y visualizar paquetes TCP/IP, y otros que estén siendo transmitidos o recibidos en una red a la cual la computadora se encuentra conectada. Se distribuye bajo la licencia BSD (Berkeley Software Distribution), siendo un software libre y de código abierto (SLCA). Funciona en la mayoría de los sistemas operativos: Linux, Microsoft Windows, Solaris, BSD, Mac Os X, HP-UX y AIX, entre otros. Emplea la librería Libpcap para capturar paquetes [6] y WinDump para Windows. Se puede utilizar también en el entorno inalámbrico.

Wireshark

Anteriormente conocido como Ethereal, es uno de los analizadores de protocolos más empleado. Captura los paquetes que circulan por la red y muestra el contenido de cada campo con el mayor nivel de detalle posible. Puede capturar paquetes en redes con diferentes tipos de medios físicos, incluyendo las WLAN [7]. Funciona tanto en modo consola como mediante una interfaz gráfica (Figura 1) y contiene muchas opciones de organización y filtrado de información. Permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con otros protocolos de la capa de enlace) estableciendo la configuración en modo promiscuo.

Sus estadísticas y funciones gráficas son muy útiles, pues identifica los paquetes mediante el uso de colores. Además, examina datos de una red “en caliente” o de un archivo de captura salvado en disco. Incluye un lenguaje completo para la elaboración de filtros, la capacidad de mostrar el flujo reconstruido de una sesión de TCP y la reproducción de conversaciones VoIP.

Wireshark se desarrolla bajo licencia pública general (GNU General Public License) y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac Os X, así como en Microsoft Windows. Hace uso tanto de la

librería Libpcap como de Winpcap para Linux y Windows respectivamente, siendo provistas junto con el instalador [8].

Carga datos almacenados en un archivo .pcap de una captura previa o de otros tipos de capturas entre las que se destacan los formatos: .cap, .pcapng y .ncf de la herramienta Commview.

Para la opción de reconstrucción de sesiones, Wireshark realiza el filtrado automático de aquellos paquetes pertenecientes a la sesión en cuestión, mediante la opción Follow TCP Stream. El programa brinda la posibilidad de guardar la información reconstruida en diferentes formatos (ASCII, EBCDIC, HexDump, C Arrays y Raw). Este procedimiento para la reconstrucción de sesiones es más trabajoso en comparación con otras herramientas como el NetworkMiner, pues requiere mayores conocimientos por parte de los usuarios.

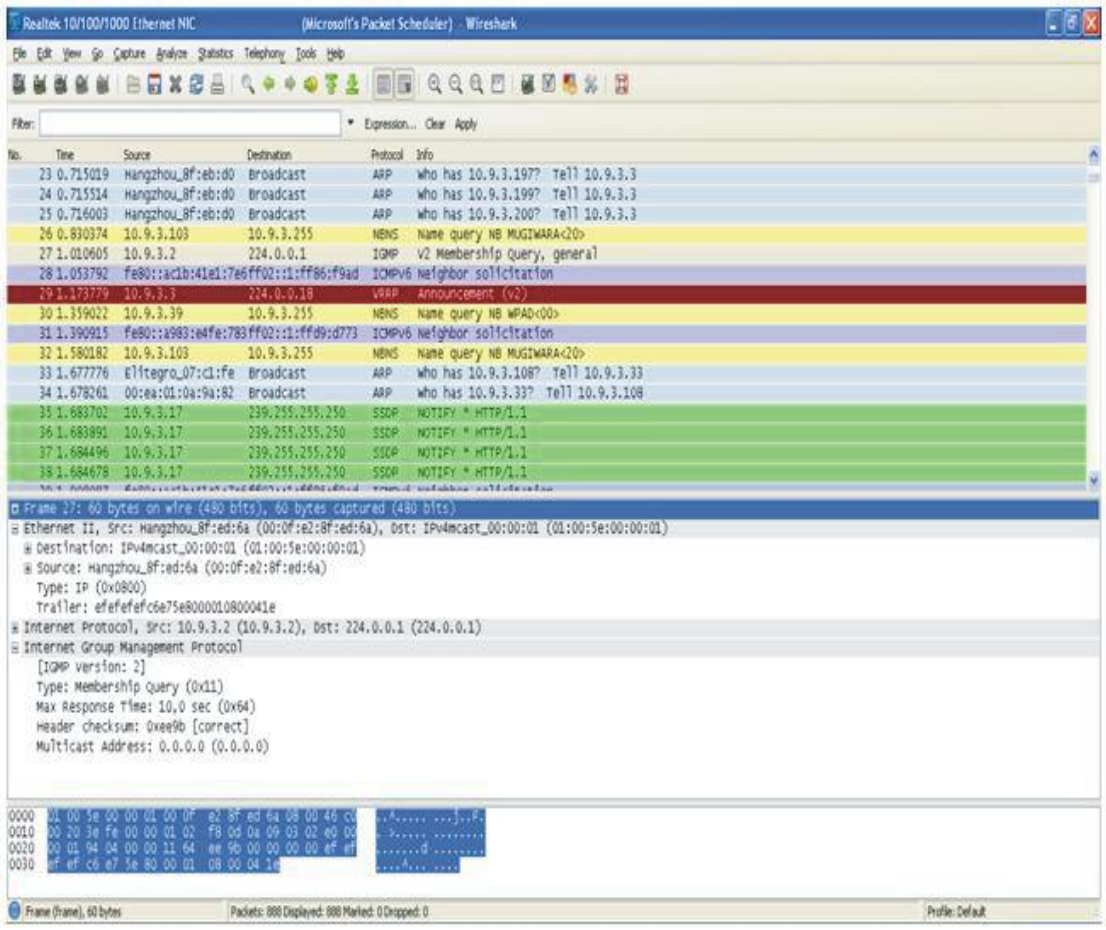

Figura 1. Vista de la herramienta Wireshark

CommView

Es una herramienta comercial de análisis y monitorización, diseñada para los administradores de redes LAN, profesionales de la seguridad, programadores de red y usuarios, que deseen obtener una completa imagen del flujo de tráfico a través de una computadora o segmento de red. Incluye un analizador VoIP para análisis, grabación y reproducción de comunicaciones de voz SIP y H.323 [3, 4].

Corre en cualquier variante del Microsoft Windows y requiere de una red Ethernet de 10/100/1000 Mbps. Para tareas de monitorización remota se puede emplear el CommView Remote Agent. Este permite capturar tráfico de red de cualquier computadora donde esté corriendo, independientemente de la posición física de esta, incrementando de esta forma el rango de la monitorización.

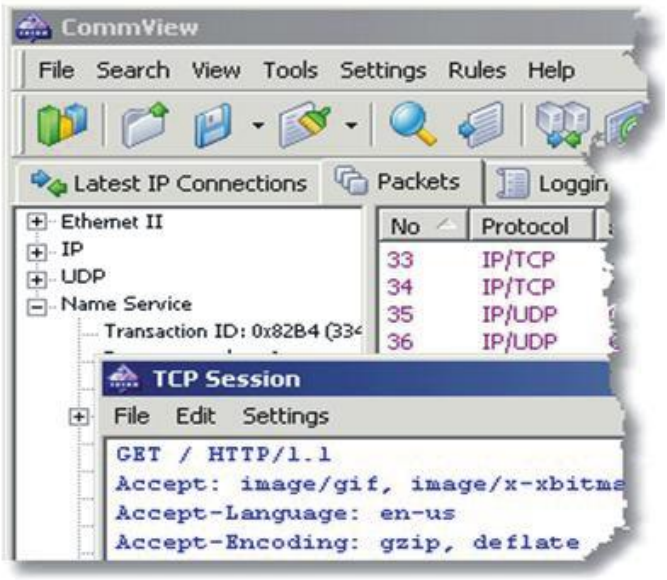

Figura 2. Visualización de la herramienta CommView

La interfaz gráfica del programa es fácil de manipular, consta de cinco pestañas que permiten ver los datos y realizar diversas acciones sobre los paquetes capturados (Figura 2). El procedimiento para la reconstrucción de sesiones es sencillo ya que una vez identificado un paquete perteneciente a una sesión, solo se deberá aplicar la opción Reconstruir Sesión TCP. Este programa representa la sesión reconstruida en varios códigos (ASCII, HEX, HTML, EBCDIC y UTF-8), permitiendo guardar esta sesión como: texto, texto enriquecido, HTML o datos binarios.

Una carencia que se puede apreciar en NetworkMiner es que no se pueden visualizar algunos detalles de los nodos como el del sistema operativo. Existe una versión de esta herramienta para redes 802.11 llamada CommView for Wifi, en la que de cada estación se puede conocer la dirección IP, el canal, el SSID, la potencia de la señal, entre otras características.

Kismet

Se emplea como sniffer y como sistema de detección de intrusiones para redes 802.11. Trabaja con tarjetas inalámbricas que soporten modo monitor y puedan servir para monitorizar tráfico 802.11 a/b/g/n [9]. Soporta además una arquitectura de plugins que permite incluir el trabajo con otros protocolos. Identifica las redes recolectando de forma pasiva los paquetes y permitiendo detectar redes escondidas a través de los datos del tráfico. Este programa funciona sobre varios sistemas como Linux, Microsoft Windows, Solaris, BSD y Mac Os X.

Antes de comenzar a utilizarlo se debe conocer el driver de la tarjeta inalámbrica y la interfaz en que está localizada la misma. Se pueden realizar diversas configuraciones en su archivo de

configuración kismet.conf, como por ejemplo utilizar sonidos, conectar un GPS (Global Positioning System), entre otras [9].

La aplicación se ejecuta desde la consola principal de Linux y se deben poseer permisos de administración para cambiar la configuración de la tarjeta inalámbrica a modo monitor.

NetworkMiner

Es una herramienta que entra en la categoría de análisis forense de redes y que corre en plataformas Windows, aunque con el empleo de Mono, puede igualmente hacerlo en distribuciones de Linux. Su propósito es recopilar información sobre los hosts en lugar de recoger información concerniente al tráfico de la red.

Utilizada tanto en redes cableadas como en inalámbricas, permite ser usada como sniffer pasivo y analizar capturas en formato pcap. Emplea la biblioteca de captura de paquetes estándar Winpcap, que debe estar instalada en la computadora para su funcionamiento. La vista de la interfaz de usuario principal (Figura 3) está centrada en el host.

Hosts es la principal pestaña de la interfaz gráfica. En ella, NetworkMiner muestra los equipos detectados usando un árbol jerárquico desplegable, observándose todas las direcciones IP involucradas con la red de comunicaciones, al mismo tiempo que muchos otros detalles: dirección MAC, nombre del host, sistema operativo, TTL (time to live), y cuánto tráfico ha sido enviado hacia y desde la dirección. La identificación del sistema operativo puede realizarse apoyándose en las bases de datos Satori, p0f y Ettercap [10, 11].

Se ofrecen muchos otros detalles como información de las sesiones de comunicación y del tráfico de DNS (Domain Name Service). Además, la pestaña Cleartext muestra las cadenas de texto plano encontradas en la carga útil de cualquier paquete TCP o UDP (User Datagram Protocol). La pestaña de Credentials puede capturar los detalles de registro de entrada, por ejemplo vía cookies HTTP (Hypertext Transfer Protocol) y las credenciales de usuario (nombres de usuario y contraseñas).

En la pestaña Images se muestran las imágenes en miniatura que han sido extraídas del tráfico de la red. La pestaña Files permite reconstruir archivos tanto descargados como subidos a sitios web a través de los protocolos de extracción de archivos: FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), HTTP y SMB (Server Message Block).

Existen dos variantes de NetworkMiner, una edición gratuita y otra profesional. La edición profesional presenta más opciones que la gratuita, entre ellas la Geolocalización IP y el protocolo de identificación de puerto independiente (PIPI) [10].

Presenta algunas limitaciones, pues no posee la opción de identificar y escuchar llamadas de VoIP y no muestra estadísticas del tráfico. Adicionalmente, el trabajo con las sesiones puede llegar a ser incómodo ya que no se relacionan con los hosts origen y destino de las mismas.

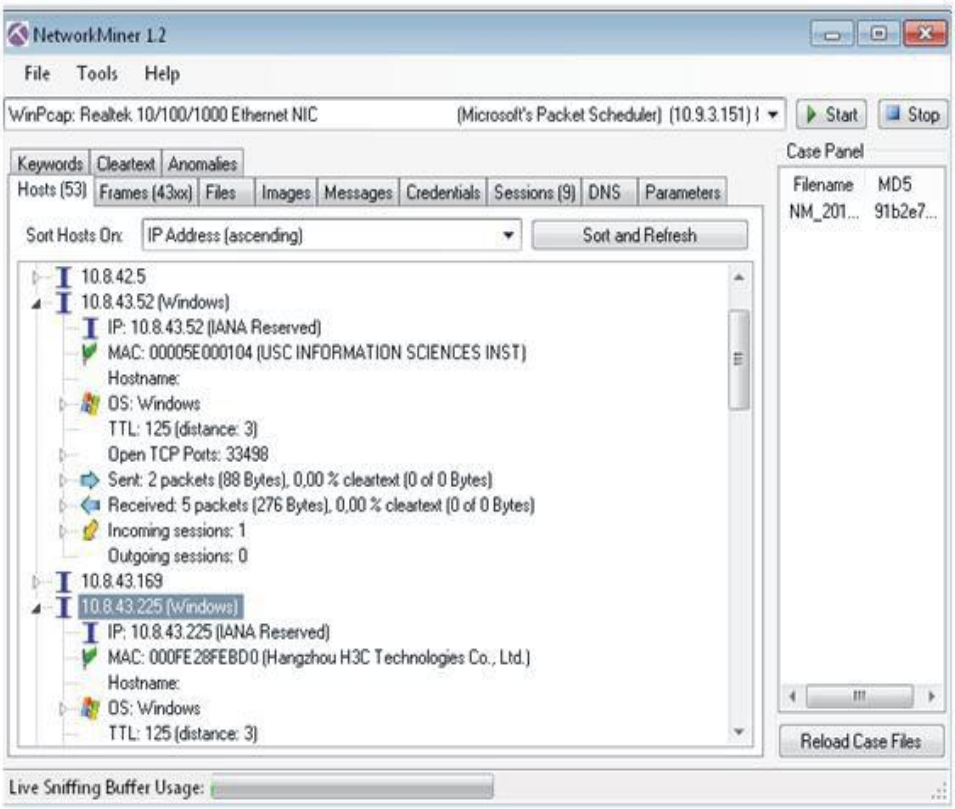

Figura 3. Ventana de presentación del NetworkMiner.

OmniPeek

Es un analizador de red comercial bastante completo, capaz de realizar capturas en el entorno inalámbrico. Ofrece una interfaz gráfica intuitiva y fácil de usar (Figura 4) que los ingenieros pueden utilizar para analizar con rapidez los paquetes que circulan por la red y solucionar problemas que puedan presentarse en la misma.

Proporciona visibilidad en tiempo real y análisis de la red desde una única interfaz, incluyendo Ethernet, Gigabit Ethernet, 10 Gigabit, conexión inalámbrica 802.11a/b/g/n, VoIP y vídeo [12]. Usando la interfaz de usuario para la visualización de las condiciones de red se pueden analizar rápidamente, profundizar y corregir los cuellos de botella a través de varios segmentos.

Dentro de sus principales características se pueden citar [13]:

- Comprensible gestión de rendimiento y monitorización total de la red, incluyendo segmentos de red en oficinas remotas.
- Inspección profunda de los paquetes.
- Análisis para identificar los nodos que se están comunicando, qué protocolos y subprotocolos están siendo transmitidos y qué características del tráfico están afectando el rendimiento de la red.
- Total monitorización de video y voz sobre IP en tiempo real.

• Monitorización del rendimiento de las aplicaciones y análisis en el contexto de la actividad de la red en general, incluyendo la habilidad de monitorear el tiempo de respuesta, el RTT (Round Trip Time), la capacidad de respuesta de los servidores, entre otros.

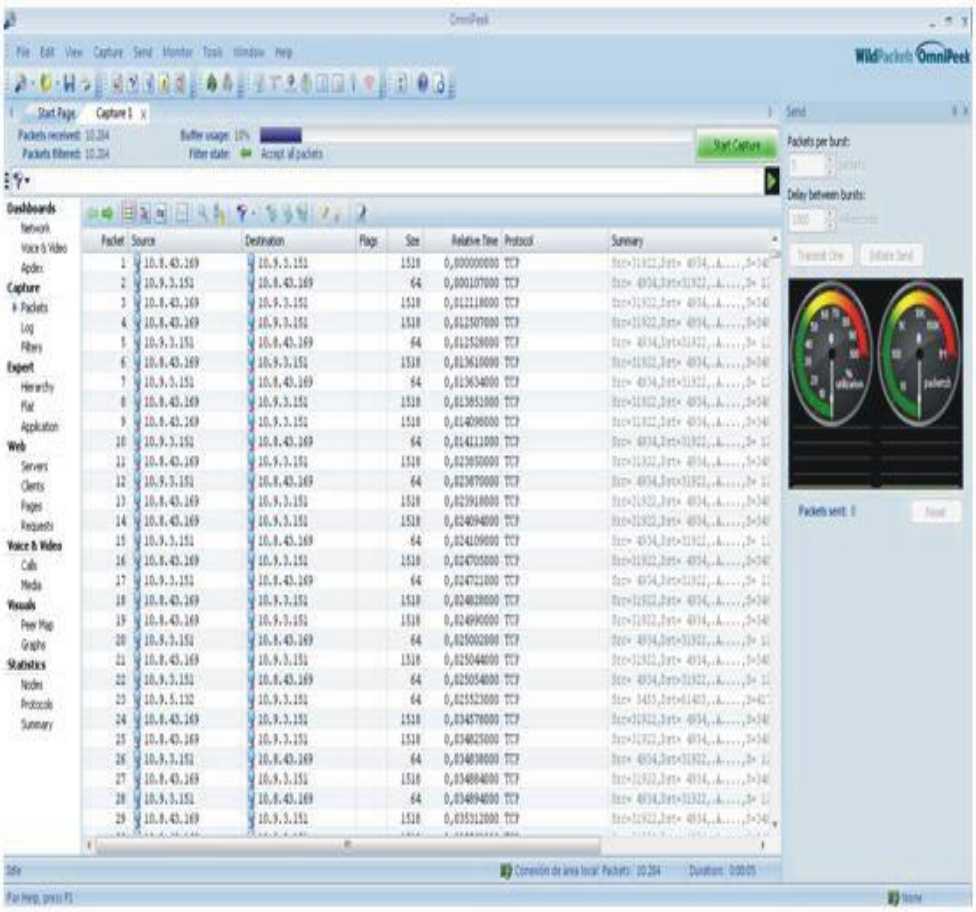

Figura 4. Interfaz gráfica del OmniPeek.

Existen variantes de distribución de esta herramienta, cada una con características particulares: OmniPeek Basic, OmniPeek Professional, OmniPeek Enterprise y OmniPeek Connect [13].

Es el software más completo de los analizados por el colectivo de autores, en cuanto a identificación y detalles de los nodos, visualización de estadísticas, identificación de llamadas VoIP, entre otros.

Otras herramientas útiles

Las prestaciones de las herramientas que se describirán a continuación raras veces se pueden encontrar en un sniffer tradicional, sin embargo pueden ser de gran utilidad en la monitorización y supervisión de actividad en las redes inalámbricas locales.

InSSIDer

InSSIDer es un programa para escanear y analizar el funcionamiento de las redes 802.11 al alcance del ordenador donde se esté ejecutando. Para utilizarlo no hace falta realizar ninguna configuración, sólo se debe tener instalado Microsoft.NET Framework 2.0 o superior. Es una herramienta de software libre, liberada bajo la licencia de Apache 2.0 y funciona en los sistemas operativos Windows XP SP2, Vista o Windows 7 (32 ó 64 bits) [14, 15] y también puede emplearse en los sistemas operativos Linux [16].

Una vez activo, InSSIDer va recogiendo datos de las conexiones cercanas y muestra información útil como las direcciones MAC, el SSID, el RSSI (Receive Signal Strength Indication), el canal, el fabricante del punto de acceso, el tipo de seguridad activada (WEP o WPA), la tasa de datos y el tipo de red. Además, muestra un gráfico de barras que representa la intensidad y la localización de cada una de las redes detectadas en los canales accesibles por la tarjeta de red.

La versión 2.0 tiene también las siguientes características:

- Gráfico de amplitud de la señal en dB en el tiempo.
- Pestañas de gráficos separadas para los canales de 2.4 y 5 Ghz. Para los canales de 5 GHz se divide el gráfico en dos: menores (36-64) y superiores (100-165).
- Sistema de filtrado que permite mostrar solo las redes que cumplen ciertos criterios (ideal para la detección de puntos de acceso).
- Ficha de estado del GPS, que muestra datos detallados de GPS como la ubicación, velocidad, altitud, entre otros y los niveles de señal de satélites a la vista (hasta 12).

NetStumbler

NetStumbler también conocido como Network Stumbler, es una herramienta libre que facilita la detección de LANs inalámbricas usando los estándares 802.11a/b/g [17]. Permite escanear de forma muy rápida el espectro 802.11, posibilitando ver redes cercanas, el nivel de señal con que se cuenta, la relación señal-ruido, la velocidad, el canal e incluso la marca de los equipos. También se pueden verificar las configuraciones de la red, encontrar ubicaciones con poca cobertura dentro de una WLAN, representar gráficos de relación señal-ruido, detectar las causas de una interferencia inalámbrica y ubicar antenas direccionales para enlaces WLAN de larga distancia [18].

Soporta aplicaciones adicionales, como por ejemplo stumbverter, que es un programa capaz de ubicar las capturas de NetStumbler en un mapa GPS. Corre en todos los sistemas operativos de Microsoft Windows. Una versión recortada denominada MiniStumbler está disponible para el sistema operativo Windows CE.

Limitaciones de los sniffers

Como se pudo apreciar en las secciones anteriores los sniffers son de gran utilidad y presentan muchas aplicaciones, pero a su vez, poseen una serie de limitaciones las cuales se mencionan a continuación:

- Generalmente una misma herramienta no reúne todas las prestaciones necesarias para la monitorización y análisis de tráfico.

- Existen limitaciones en las interfaces inalámbricas con las que pueden trabajar en modo monitor.

- Algunas solo trabajan en modo consola.

- Existen muchos problemas con la gestión de la información de captura y las estadísticas en el momento de trabajar con casos de estudio, entre otros.

- No realizan tareas activas para el reconocimiento de las redes, los nodos y otros.

Otra limitación, para la monitorización de redes, es el uso de encriptación. Muchos intrusos se aprovechan de la encriptación para esconder sus actividades, ya que a pesar de que los administradores pueden apreciar que está teniendo lugar una comunicación, son incapaces de ver su contenido en un período corto de tiempo [19].

En particular, los sniffers inalámbricos presentan limitaciones adicionales, algunas de ellas se mencionan en este artículo [20]:

- La medición de la potencia de señal recibida es relativa a la localización del sniffer inalámbrico, pues esta no será la misma a medida que más alejado o cercano a los puntos de acceso y al cliente remoto se encuentre el sniffer.

- Un sniffer inalámbrico es capaz de capturar solamente el tráfico del área local donde está instalado, siendo un impedimento que el administrador deba moverlo de segmento a segmento de red, o tenga la necesidad de instalar múltiples sniffers.

- Se agudizan las dificultades con los driver de interfaces inalámbricas que permiten trabajar en modo monitor.

Conclusiones

En este artículo se ha proporcionado una panorámica bastante abarcadora sobre las herramientas de monitorización y análisis del tráfico de las redes de datos, incluyendo aquellas de comunicación inalámbrica, las cuales tienen un despliegue creciente en los últimos años. Además, se han revelado detalles importantes de la operación de estas herramientas y otros aspectos que deben considerarse a la hora de seleccionar una solución para estas tareas de la gestión de la red, así como las principales limitaciones que pueden afectar su cumplimiento eficiente.

El análisis de tráfico tiene que realizarse de manera permanente, por los múltiples aportes que tiene para las diferentes funcionalidades de la gestión de las redes. Por tal motivo, los autores consideran que este artículo puede ser de interés para todos los especialistas que realizan o planifican implementarlo.

Referencias Bibliográficas

1. Thomas, G., Using Ethereal for Network Troubleshooting. The extension, 2006. 7(1). Contemporary Control Systems, Inc.

2. So-In, C. A Survey of Network Traffic Monitoring and Analysis Tools. Computer Systems Analysis Lecture, 2006 Available from: http://www.cse.wustl.edu/~jain/cse567-06/net_traffic_monitors3.htm

3. CommView. [cited 2012 2 de febrero]; Available from: http://www.tamos.com/products/commview/.

4. TamoSoft, I. CommView® Network Monitor and Analyzer for MS Windows. Documentación de ayuda, 2003 Availablefrom: http://www.tamos.com

5. Sniffing (networkwiretap, sniffer) FAQ. 2000 [cited 2012 10 de febrero]; Available from: http://www.robertgraham.com/pubs/sniffing-faq.html.

6. Van Jacobson, C.L.a.S.M., all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA. tcpdump(8) - Linux man page. 2010 [cited 2012 15 de febrero]; Available from: http://linux.die.net/man/8/tcpdump.

7. Lamping, U., R. Sharpe, and E. Warnicke Wireshark User's Guide for Wireshark 1.7. Manual de usuario, 2011 Available from: http://www.tamos.com

8. Mas, A.M., Redes Locales Inalámbricas WiFi. Conferencia. Asignatura: Redes y Servicios de Radio, 2005. Universidad Politécnica de Madrid Conferencia. Asignatura: Redes y Servicios de Radio

9. Lee, T.B. Hypertext Transfer Protocol -- HTTP/1.0. 1996 [cited 2012 16 de febrero]; Available from: http://www.faqs.org/rfcs/rfc1945.html.

10. Forensics, E.i.n.s.m.a.n. NetworkMiner. 2011 [cited 2012 17 de febrero]; Available from: http://www.netresec.com/?page=NetworkMiner.

11. Williams, M. Capture and analyse your network traffic with the free NetworkMiner. 2011[cited 2012 17 de febrero]; Available from: http://www.softwarecrew.com/2011/05/capture-and-analyse-your-network-traffic-with-the-free-networkminer/.

12. WildPackets, I. Getting the Most from Your Wireless Network. White Paper, Available from: http://www.wildpackets.com/downloads.

13. OmniPeek Network Analyzer. [cited 2012 17 de febrero]; Available from: http://www.wildpackets.com/products/network_analysis_and_monitoring/omnipeek_network_analyzer.

14. Góngora, A. InSSIDer: Analiza el estado de las redes WiFi accesibles desde tu PC. [cited 2012 17 de febrero]; Available from: http://inssider.uptodown.com/.

15. Klew, W. inSSIDer, escáner de redes Wi-Fi. 2008 [cited; Available from: http://www.visualbeta.es/5885/windows/inssider-escaner-de-redes-wi-fi/.

16. inSSIDer 2 for Linux (alpha). [cited 2012 20 de febrero]; Available from: http://www.metageek.net/products/inssider/linux/.

17. Lendoiro, D. Seguridad en Redes Wireless 802.11 a/b/g., Available from:http://doc-gulo.org/docu/jornadasI/Seguridadwifigulo.pdf.

18. Weiss, A. Introduction to NetStumbler. 2010 [cited 2012 20 de febrero]; Available from: http://www.wi-fiplanet.com/tutorials/article.php/3589131.

19. Scarfone, K., et al. Technical Guide to Information Security Testing and Assessment. Publicación especial 800-115, NIST: National Institute of Standards and Technology Available from: http://csrc.nist.gov/publications/PubsSPs.html.

20. Ramesh Babu H. Siddamallaiah, G.S., Piriyapatna S. Satyanarayana A Perspective on Traffic Measurement Tools in Wireless Networks. Wireless Engineering and Technology. 1, 14-19 2010Artículo Available from: http://www.SciRP.org/journal/wet.