INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

SEMINARIO DE TITULACIÓN
"SEGURIDAD DE LA INFORMACIÓN"

TESINA
"HERRAMIENTAS DE SOFTWARE LIBRE PARA EL MONITOREO DE ACTIVIDADES DE USUARIOS EN REDES LAN"

QUE PRESENTAN PARA OBTENER EL TÍTULO DE

INGENIERO EN COMUNICACIONES Y ELECTRÓNICA.

JORGE ZÁRATE AVIÑA

LICENCIADO EN CIENCIAS DE LA INFORMÁTICA

MICHELLE GERALDI ZAMORA PÉREZ

MIREYA ROMERO CHÁVEZ

Asesora:
ESP.LIDIA PRUDENTE TIXTECO

VIGENCIA: DES/ESIME-CUL-2008/23/3/10

México, D.F., Mayo 2011

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

POR LA OPCIÓN DE TITULACIÓN SEMINARIO EN SEGURIDAD DE LA INFORMACIÓN QUE DEBERÁN DESARROLLAR PARA OBTENER EL TÍTULO DE INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

ZÁRATE AVIÑA JORGE

Y PARA OBTENER EL TÍTULO DE LICENCIADO EN CIENCIAS DE LA INFORMÁTICA:

ROMERO CHÁVEZ MIREYA
ZAMORA PÉREZ MICHELLE GERALDI

"HERRAMIENTAS DE SOFTWARE LIBRE PARA EL MONITOREO DE ACTIVIDADES DE USUARIOSEN REDES LAN"

INTRODUCCIÓN

LAS AMENAZAS A LA EMPRESA ENTRAN DE MUCHAS MANERAS Y CON MUCHOS TAMAÑOS DESDE TODAS LAS ÁREAS DEL NEGOCIO: INTERNAS Y EXTERNAS. ESTAS AMENAZAS DESAFÍAN LA CAPACIDAD DE INNOVACIÓN Y COLABORACIÓN MEDIANTE LA VINCULACIÓN A RECURSOS VALIOSOS PARA TRATAR LA COMPLEJIDAD DE LA GESTIÓN DEL RIESGO Y DEL PANORAMA CRECIENTE DE REQUISITOS REGULADORES.
ESTE TRABAJO PRETENDE MOSTRAR UNA COMPARATIVA ENTRE APLICACIONES DE MONITOREO PARA LA ADMINISTRACIÓN DE REDES, LA CUAL SE TRADUZCA EN BENEFICIOS A LA EMPRESA Y QUE SIMPLIFIQUE LAS TAREAS DE CONFIGURACIÓN DE RED DE LOS ADMINISTRADORES DE REDES Y CONVIERTA ASÍ SUS TAREAS EN ACCIONES MÁS EFECTIVAS DENTRO DE LA EMPRESA.

CAPITULADO

México D. F., Mayo de 2011

VIGENCIA: DES/ESIME-CUL-2008/23/3/10

DR. GABRIEL SÁNCHEZ PÉREZ
Coordinador del Seminario

ESP. LIDIA PRUDENTE TIXTECO
Asesora

M. EN C. LUIS CARLOS CASTRO MADRID
Jefe de la carrera de I.C.

AGRADECIMIENTOS

A mi mamá, Yolanda Chávez: Gracias por todo el esfuerzo que hiciste por brindarme todo lo necesario para llegar a este día. Te agradezco tu infinita paciencia, amor, conocimientos, consejos, ejemplos de valor y perseverancia, por enseñarme a luchar con fortaleza y ánimo.

A mi papá, Manuel Romero: Gracias por todo tu apoyo, tu tiempo invertido en mis dudas y aprendizaje que necesité desde pequeña, por enseñarme a valorar mi escuela y mostrarme el camino de la dedicación y disciplina que fue necesaria a lo largo de mi vida estudiantil.

A mis hermanos Jorge M. Romero y Roberto Romero, por su complicidad, amor y tiempo dedicado a mi felicidad, sin ustedes nada hubiera sido igual.

Al amor de mi vida, César Hernández: Gracias por compartir esta maravillosa experiencia conmigo, por tu gran paciencia, tu apoyo, consejos, respaldo, motivación, amor y confianza que día a día cultivaste para que lograra mis metas.

A todos mis compañeros con los que compartí mi vida estudiantil, gracias chicos por cada experiencia y su hermosa amistad.

Romero Chávez Mireya

A mi madre María del Carmen Pérez Tellez quien es la persona más importante en mi vida, por el amor, el rigor, la paciencia y la confianza ante mis tropiezos y mis triunfos, por todas las enseñanzas que me han convertido en la persona que ahora soy. Porque todo lo que he logrado está respaldado por ti, gracias mamá te amo.

A mi padre Martín Salvador Trujano Rosete por ese amor incondicional, apoyo y motivación que me han alimentado siempre. A mis hermanos Gustavo y Ricardo por su paciencia, apoyo y amor incondicional que siempre me han brindado, por la motivación y las enseñanzas, los amo.

A Jesús Alcaraz Chávez el amor de mi vida porque siempre has estado junto a mí para motivarme y darme la confianza que he necesitado en los momentos difíciles, por tu paciencia y sobre todo por el amor que siempre me das, te amo.

Zamora Pérez Michelle Geraldi

A mi padre Jorge I. Zárate Rivera, por ser mi ejemplo a seguir, por todo lo que me brindaste para ser quien soy hoy, por tus enseñanzas de vida, tu cariño, por siempre estar junto a mí, por enseñarme a levantarme y por ser mi gran motivación para ser cada día más exitoso.

A mi madre Bertha A. Aviña Cárdenas por todo tu cariño, tu paciencia y apoyo. Por todo lo que has hecho por mí, por tu confianza y tu ternura. Por llenarme de alegría, por ser mi gran motivación y por impulsarme para ser cada día mejor.

A mi hermana Ivonne Zárate Aviña por las alegrías que me has brindado, el tiempo, los momentos compartidos, tu apoyo y tu cariño.

A mi princesa Diana Farfán Perdomo por siempre estar a mi lado, por tu apoyo incondicional, tu paciencia, tu esfuerzo y confianza. Por todo tu amor, por tus consejos, por llenarme con tu energía, por ser mi motivación y por los increíbles momentos que hemos vivido juntos.

¡Gracias por que todo lo que he logrado, lo he hecho por ustedes, los amo!

Zárate Aviña Jorge

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

OBJETIVO GENERAL

Comparar herramientas de software libre para el monitoreo de usuarios enredes LAN en base a su funcionamiento.

OBJETIVOS ESPECÍFICOS

- Enlistar las herramientas más utilizadas de software libre.
- Revisar las características de cada herramienta enlistada.
- Describir el funcionamiento de las herramientas de monitoreo.
- Aplicar las herramientas en una red.
- Analizar las características, funcionamiento y rendimiento de las herramientas.

ALCANCE

El presente documento enlista y compara, herramientas de software libre, sobre monitoreo de actividades de usuarios en redes locales, esto dirigido a personas especializadas en la operación optima de redes LAN.

La presente investigación es implementada en una organización, para que permita observar los aspectos generales y específicos, así como ventajas y desventajas de dichas herramientas.

La comparación consta de diferentes puntos a detallar tales como: la forma en la que las herramientas arrojan los datos para su interpretación, sus ambientes e interfaces, la posibilidad de crear reportes o históricos y los diferentes tipos de datos que se pueden estudiar y analizar para su posterior interpretación, toma de decisiones y aprovechamiento del software instalado. Así mismo se sugiere en qué tipo de escenario se puede sacar el mayor provecho a las herramientas de software libre que se mencionan.

JUSTIFICACIÓN

En un mundo tan dinámico como el actual, en el que las cosas cambian muy rápidamente, las empresas han tenido que evolucionar en su manera de pensar y se han ido concientizando de la importancia de migrar de sus antiguos métodos de administración y manejo empresarial, basados en el manejo de papelería y con un consumo de tiempo considerable hacia sistemas de información computacionales basados en redes de comunicaciones, incluso inalámbricos, que les ofrecen mejores tiempos de acceso a la información, y de igual manera, una forma más efectiva y confiable de compartir datos en tiempo real.

Para lograr este objetivo, la ingeniería de sistemas ha creado soluciones de manejo en red, mediante las cuales, la empresa puede mantener una interacción entre sus miembros y contar con datos veraces, lo cual se refleja en un mejor servicio hacia el cliente.

Pero no es nuevo para nadie el hecho de la susceptibilidad a fallos ocasionales de los servicios que prestan las redes empresariales que pueden tener una gran variedad de causas y orígenes, y ponen en problemas el cumplimiento de los objetivos y actividades diarias de la empresa. Para tratar de evitar que el momento en que ocurran los fallos en la red, no se puedan solucionar en el mismo instante, o que estos fallos se prolonguen por un tiempo indefinido, y la empresa tenga que asumir costos adicionales, generalmente se encarga a una persona con conocimientos claves para administrar la red, a la cual se le da el nombre de

“Administrador de la Red”. Este es el encargado de solucionar los problemas que se presenten en el menor tiempo posible, para ello sería ideal facilitarle una herramienta única que resida en su equipo de trabajo, la cual le ayude a detectar las fallas y a solucionar inconvenientes en el mismo momento que estos ocurren.

La administración de la red es una tarea vital para cualquier organización y es un campo en el que una herramienta de software puede ser muy útil, ya que ese tiempo adicional en la solución de problemas se ve reflejado en costos, en inconsistencias, en disgustos de usuarios, y en algunos casos, se pueden generar conflictos internos por el hecho de no proveer acceso a los servicios que brinda la red.

Parte de esta administración de la red se enfoca en mantener la disponibilidad y la mejora continua de la eficiencia de los servicios ofrecidos. La disponibilidad de la red representa un recurso indispensable para toda empresa que cuente con una infraestructura que sustente su operación.

Actualmente México ocupa el lugar 29 de 30 en la lista de países con mayor ancho de banda y menor costo. La cifra de PYMES (***Pequeñas y Medianas Empresas***) en México se aproxima a los 4.5 millones de las cuales solo el 24% maneja licencias o patentes[1]. Debido a esto es necesario implementar acciones para mejorar el rendimiento de la red evitando así tener que realizar inversiones mayores para incrementar el ancho de banda que proveen los ISPs (***Proveedores de Servicios de Internet***).

[1] Estadísticas obtenidas del perfil estadístico de México y del reporte anual en el sitio Web de la OCDE (Organización para la Cooperación y el Desarrollo Económico).

INTRODUCCIÓN

Las amenazas a la empresa entran de muchas maneras y con muchos tamaños desde todas las áreas del negocio: internas y externas. Estas amenazas desafían la capacidad de innovación y colaboración mediante la vinculación a recursos valiosos para tratar la complejidad de la gestión del riesgo y del panorama creciente de requisitos reguladores.

Este trabajo pretende mostrar una comparativa entre aplicaciones de monitoreo para la administración de redes, la cual se traduzca en beneficios a la empresa y que simplifique las tareas de configuración de red de los administradores de redes y convierta así sus tareas en acciones más efectivas dentro de la empresa.

En este documento se describen algunas aplicaciones de monitoreo de red actuales y eficientes. En los primeros capítulos se encuentra el marco teórico, que define los conceptos de seguridad y explica los principales temas que se ven involucrados y que son tomados en cuenta para el desarrollo de esta tesina. Posteriormente se describen los escenarios donde se hace uso de las herramientas analizadas en este proyecto para brindar una gestión de red adecuada y eficiente.

CAPÍTULO I. SEGURIDAD DE LA INFORMACIÓN

Se puede definir como seguridad de la información a todas aquellas medidas tomadas por el hombre de forma preventiva así como reactiva (controles, políticas, procedimientos, concientización y/o entrenamientos), respecto a los sistemas tecnológicos. Estas medidas permiten resguardar y proteger la información, buscando siempre mantener los principios básicos de la seguridad de la información: confidencialidad, disponibilidad e integridad de la misma.

Estos tres conceptos son de gran importancia, debido a que forman parte del objetivo principal de la seguridad de la información.

- La confidencialidad asegura que solo podrán acceder a la información (usar o modificar, leer o escuchar) las personas autorizadas.

- La integridad asegura que la información con la que se trabaja sea completa y precisa, poniendo énfasis en la exactitud de su contenido así como en los procesos involucrados en el procesamiento.
- La disponibilidad asegura que la información pueda ser utilizada siempre que la persona autorizada requiera hacer uso de ella.

La información puede ser representada en diversas formas: electrónicamente (servidores, PCs, unidades extraíbles, etc.), impresa (papeles, contratos, planes, reportes, formatos, etc.), magnéticamente (discos rígidos, tarjetas de acceso, etc.) u ópticamente (DVDs o CDs en sus diversas presentaciones); puede ser visualizada por video, leída o en alguna conversación de persona a persona[2].

La importancia de la seguridad en la información tiene siempre un efecto significativo pero difiere en cómo es cobrado el efecto de violar esa privacidad.

1.1 ¿Qué es la seguridad?

Se define como el conjunto de medidas tomadas para protegerse contra robos, ataques, crímenes, espionajes y/o sabotajes. La seguridad implica la cualidad o estado de mantenerse seguro, es decir, el evitar exponerse a situaciones de peligro y tomar las medidas necesarias para quedar cubierto frente a contingencias adversas[3].

---

[2]Estándar ISO 17799:2000 y BS 7799-2:2000
[3]H. M. Deitel. Introducción a los Sistemas Operativos. Addison-Wesley Iberoamericana, México, 1987

Ya dentro del campo de la informática, sea cual sea la organización, se define como activo: desde una persona hasta el conjunto de la información. Este activo tiene un valor muy importante para la empresa. La pérdida, alteración o eliminación de éste siempre impacta de manera monetaria, por ello se debe entender la importancia de mantener a todo activo en ausencia de riesgo, mejor dicho seguro en todo momento[4].

La seguridad, no solo requiere de un sistema de protección apropiado, sino también de considerar el entorno externo en el que éste opera. La protección interna no es útil si la consola del operador se encuentra al alcance de personal no autorizado o si los archivos pueden ser extraídos del sistema de cómputo. Estos problemas de seguridad son esencialmente de administración, no problemas del sistema operativo.

La información almacenada en el sistema, así como los recursos físicos del sistema de cómputo, tienen que protegerse contra accesos no autorizados, destrucción o alteración mal intencionado.

1.2 Seguridad informática

El área de informática, enfocada a la seguridad de la misma, toma como parámetros la protección de la infraestructura computacional/tecnológica y todo lo relacionado a ella, sin dejar de lado lo más importante: la información. En colaboración a esto, existen estándares, métodos, protocolos, herramientas y leyes ya establecidas, que ayudan a minimizar los posibles riesgos y vulnerabilidades ante amenazas que están en todo

[4]JuanVoutssas M. Preservación documental digital y seguridad informática. Investig.bibl v.24 n.50 México ene./abr. 2010

momento dentro y fuera de la organización y que claro pueden alterar la infraestructura de la misma.

La seguridad informática trabaja principalmente con todo aquello que la organización toma como un activo y muestra vulnerabilidad ante cualquier tipo de ataque: software, bases de datos, archivos, etc.

Por ello, la seguridad es una forma de protección contra los riesgos, las amenazas y las vulnerabilidades. A continuación se definen los siguientes conceptos para un mayor entendimiento:

- Una amenaza puede ser cualquier circunstancia o evento con el potencial de impactar adversamente sobre un Sistema de Información, mediante el acceso no autorizado, destrucción, revelación, modificación de datos y / o denegación del servicio.
- Una vulnerabilidad es cualquier debilidad que puede ser explotada, ya sea en un sistema de información, procedimientos de seguridad del sistema, controles internos, implementación, etc.
- Un riesgo es la probabilidad de que una amenaza aproveche la vulnerabilidad.
- Un ataque es un tipo de incidente que involucra el acto intencional de intentar evitar llevar a cabo los controles de seguridad de un Sistema de Información, estos se clasifican en:

- Ataque Pasivo. Este tipo de ataque intenta conocer y hacer uso de información, comúnmente este tipo de ataques son fáciles de detectar; por ejemplo:
  - Obtención de contenido de mensajes.
  - Análisis de tráfico.

- Ataque Activo. Este tipo de ataque intenta alterar los recursos del sistema o afectar el funcionamiento del mismo, se caracteriza por ser difícil de prevenir, por ejemplo:
  - Suplantación de identidad.
  - Repetición.
  - Modificaciones de mensajes.
  - Interrupción de servicios.

La seguridad informática está concebida para proteger los activos informáticos de todo ataque que se mencionó anteriormente [5].

1.3 Seguridad en internet

Basados en la idea de que todo puede ser encontrado en internet, todos los días una gran cantidad de personas se dan cita, dedicando una parte significativa de su tiempo,

[5]National Information Systems Security (Infosec). Glossary. September 2000.

a la navegación por este medio, sin embrago, se suele dejar de lado verificar que el lugar donde se navega sea seguro y que aporte un beneficio.

En la situación de niños y adolescentes el riesgo principal es que intercambian demasiada información y no imaginan la clase de ataques con los que se pueden enfrentar (virus, spam, información dañada, etc.).

En el caso de las grandes corporaciones y organizaciones empresariales, la preocupación por la seguridad en Internet se enfoca a las grandes cantidades de información que son manejadas tanto de sus clientes como de sí misma: las organizaciones necesitan proteger la confidencialidad de la información reservada. Por otra parte, los usuarios tienen la responsabilidad de vigilar de cerca todo lo referente a la protección de sus datos y a la identidad de las fuentes y destinatarios de los mismos[6].

Evidentemente la seguridad en internet es un punto crucial, pero cuando se habla sobre aquellas empresas que operan con banca electrónica este concepto tiene un peso aún mayor. Esto debido a que las cuentas bancarias en internet no son más que bases de datos, las cuales se encuentran de alguna forma expuestas. En definitiva, la seguridad afecta a todos: a las grandes compañías (por ser una tentación) y a los usuarios individuales por su vulnerabilidad.

[6] Fuente: La seguridad en Internet es posible por: Rodolfo Lomáscolo, Director General IPS.

Considerando los aspectos anteriores, se enlistan actividades que un gran porcentaje de la población hacen por lo menos una vez al día, todos ellos sin la debida cultura en su uso.

La navegación

La lectura de documentos virtuales o visitas a páginas Web, se denominan comúnmente como “navegación” o “búsqueda”. Visitar museos virtuales, tener acceso a documentos públicos del estado, leer libros completos y ver películas cortas, son sólo algunas de las actividades que pueden ser realizadas por Internet.

Por ello la responsabilidad de la navegación recaerá en el tiempo de calidad dedicado a la búsqueda, es decir, que se revise con cuidado, dedicación y detalle la información que se obtiene del internet. Sobre todo es importante aprender a respetarla, ya que si bien es necesario el obtenerla, tener conciencia del derecho de autor y hacer buen uso de lo obtenido es fundamental. Esto sería una medida de prevención ante la navegación.

Salas de Chat

“Chatear” (conversar en línea) se ha convertido en una de las formas preferidas de las personas de conectarse a un grupo (sala de Chat) por Internet para compartir intereses similares. Normalmente en la sala de Chat hay más de una conversación a la vez.

Existen dos clases de salas de Chat: moderadas y no moderadas.

El moderador de una sala de Chat hace cumplir las reglas sobre conversaciones apropiadas en una sala de Chat en particular. Y por lo tanto las no moderadas son aquellas salas sin monitoreo, que no pueden evitar cierto tipo inadecuado de conversaciones.

Una medida de prevención sería darse el tiempo de hacer una comparación entre los diversos espacios donde se puede conversar vía internet, así habría una menor incertidumbre en el momento de estar intercambiando ideas entre las personas.

Descarga/Uso Compartido de Archivos

Compartir archivos es otra de las actividades preferidas de los adolescentes, aunque en la actualidad es algo realmente común en cualquier empresa. Se puede compartir archivos por medio de programas relativamente sencillos de obtener, los cuales, permiten a los usuarios conectarse directamente a otra computadora y copiar, cortar, modificar o en general compartir diversos tipos de archivos: música, películas, programas y documentos. El uso del internet con este fin aumenta el riesgo en la seguridad ya que los archivos pueden estar infectados, pueden ser violados derechos de autor o los permisos de acceso pueden no ser los correctos.

Por esto, una de las mejores medidas de prevención será siempre contar con un antivirus, que es un software dedicado a generar alarmas frente a cualquier tipo de

archivo malicioso y en los casos necesarios, eliminarlos antes de que generen un estrago mayor en el equipo[7].

1.4 Seguridad en redes

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas, esto conlleva a que si un problema las afecta, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben ser subestimadas las fallas de seguridad provenientes del interior de la organización.

El tema de la seguridad y privacidad en un sistema de red es un asunto que debe preocupar y tomarse con la mayor seriedad posible ya que las amenazas están presente todo el tiempo, desde realizar actividades de trabajo o de ocio, hacer compras, transacciones bancarias y/o enviar e-mails. Al mismo tiempo, se ve en riesgo la seguridad de la información de esas actividades, por ello es importante definir mecanismos adecuados para que la información de una organización o empresa sea segura. Estos mecanismos y métodos dependerán del nivel de protección que el usuario guste aplicar para el uso normal del equipo. Así se consiguen las garantías de

[7] Guía de seguridad en el internet. Time Warner Cable y CyberAngels.

confidencialidad: protegiendo la integridad y totalidad de la información y sus métodos de proceso; también asegura la disponibilidad que garantiza a los usuarios autorizados acceso a la información y los recursos.

Durante el tiempo que dure el intercambio o solicitud de información de cualquier usuario, la red lleva implícita consigo un tipo de amenaza, como son:

- *Virus.* Son programas con la capacidad de copiarse a sí mismo [8] e infectar un ordenador. Este término también suele ser utilizado, no correctamente, para referir malware, adware y spyware, que son programas que no tienen la capacidad reproductiva. Un verdadero virus puede propagarse de un ordenador a otro (en alguna forma de archivo ejecutable o de código) cuando su anfitrión es llevado al equipo o en un medio extraíble (disquete, CD, DVD o unidad USB)[9].

- *Intruso.* Es la persona que intenta acceder a un sistema informático sin autorización. Un intruso es aquel que hace aplicaciones informáticas sin la calidad suficiente, ese es el tipo de intruso que hay que perseguir y erradicar de la profesión[10].
- *Spam.* Son correos basura no solicitados con los que se bombardea a los mails. Suelen estar relacionados con la publicidad y para ellos la solución son los anti-spam.

---

[8] Dr. Salomón de la Enciclopedia de Virus, 1995, ISBN 1897661002.
[9] JussiParikka (2007) "Contagiosas digital virus. Medios Un equipo de Arqueología", Peter Lang: Nueva York. Digital Formations-series. ISBN 978-0-8204-8837-0, p19.
[10] Batchforthe Java TM in General (2007).Informática sin intrusos, Si pero que es un Intruso.

- *Spyware.* Es el software que, de forma encubierta, utiliza la conexión a Internet para extraer datos e información sobre el contenido del ordenador, páginas visitadas, programas, etc. La solución en estos casos son los anti-spyware.
- *Bugs.* Son errores de programación que pueden provocar errores y daños a la información. Estos pueden ser utilizados para lanzar ataques por parte de intrusos. La medida para solucionar esto es mantener actualizado el software.

Ya mencionadas algunas de las amenazas con las que cualquier usuario podría encontrarse, a continuación se enlistan mecanismos de seguridad para evitar ser víctima de una de ellas.

- *Prevención.* Aumentar la seguridad de un sistema durante su funcionamiento normal, antes de que se produzcan atentados o violaciones a la seguridad (por ejemplo la utilización de contraseñas).
- *Permisos de acceso.* Establecen a que recursos puede acceder un usuario y la seguridad en las comunicaciones (mecanismos basados en la criptografía: cifrado de contraseñas y firmas digitales).
- *Detección.* Localizar y evitar acciones contra la seguridad de la información.Utilizando antivirus, firewalls y anti-spyware.
- *Recuperación.* Se aplica cuando ya se ha producido alguna alteración del sistema. Copias de seguridad.

La seguridad de redes es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos, esto puede incluir:

- Evitar que personas no autorizadas intervengan en el sistema con fines malignos.
- Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema.
- Asegurar los datos mediante la previsión de fallas.
- Garantizar que no se interrumpan los servicios[11].

1.4.1 Seguridad interna

La seguridad, comprendida como una estrategia de desarrollo empresarial, puede propiciar notables beneficios; como se mencionó anteriormente son muchas las amenazas que en cualquier organización existen tanto físicas como lógicas y a las que todo activo de información está expuesto. La clave estriba en desplegar todo el alcance que estrategias, como la destrucción de archivos documentales, pueden ofrecer a los negocios, en general.

Mantener eficientes estrategias de seguridad para la protección de los datos confidenciales de un negocio no solo genera seguridad para los empleados de dicha institución, sino que además fomenta un sentimiento de confianza y

[11]FRISCH, A. (1995) Essential System Administration. O'Reilly&Associate.

gratitud entre el personal. Derivada de esta circunstancia, se puede augurar una productividad sobresaliente para una compañía, puesto que los trabajadores se mostrarán comprometidos con el proyecto derivado del interés de los directores hacia la privacidad de sus datos confidenciales.

Seguridad interna genera confianza y la confianza propicia seguridad externa. Dando una muestra tan clara de responsabilidad civil y ejecutiva, se actúa con enorme provecho, porque se propicia una cultura del cuidado de la información que evitará, a la larga, que se cometan errores o faltas administrativas, por filtraciones gravosas de datos, que pueden poner en riesgo la estabilidad integral del negocio.

Todos los mecanismos y estrategias vinculadas a la obtención de la mejor seguridad interna posible para una empresa, como lo es la destrucción responsable y cuidadosa de archivos documentales obsoletos, se verá reflejada en un incremento de la seguridad externa.

1.4.2 Seguridad externa

Con el fin de evitar robos o fraudes, las medidas de vigilancia o contención directa no siempre resultan las más adecuadas. Lo mejor son las estrategias de prevención, puesto que resultan menos costosas y complicadas de implementar.

La seguridad interna, cuando alcanza un nivel significativo, le otorga una imagen de solidez y dominio sobre sí misma a una compañía, lo que genera confianza entre los consumidores y funciona como un escudo para desalentar la delincuencia. La destrucción documental ayuda a lograr un estado de seguridad interna, cuyos alcances, a mediano plazo, se verán reflejados en menores ocasiones de ilícitos y una mayor preferencia por parte del público.

CAPÍTULO II. ADMINISTRACIÓN DE REDES

2.1 Generalidades de monitoreo

La detección oportuna de fallas así como el monitoreo de los elementos que conforman una red de cómputo, son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema así como con herramientas capaces de notificar las fallas en la red y de mostrar su comportamiento mediante un análisis y recolección de tráfico.

Existen dos puntos de vista para abordar el proceso de monitorear una red: enfoque activo y enfoque pasivo. Aunque son diferentes ambos se complementan.

Monitoreo Activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red o enviando paquetes a determinadas aplicaciones, midiendo sus tiempos de respuesta. Este

enfoque tiene la característica de agregar tráfico en la red. Es utilizado para medir el rendimiento en una red.

Técnicas de monitoreo activo

- Basado en ICMP.
    - Diagnosticar problemas en la red.
    - Detectar retardo, pérdida de paquetes.
    - RTT.
    - Disponibilidad de host y redes.
- Basado en TCP.
    - Tasa de transferencia.
    - Diagnosticar problemas a nivel aplicación.
- Basado en UDP.
    - Pérdida de paquetes en un sentido (one-way).
    - RTT (traceroute).

Monitoreo pasivo

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como: sniffers, routers, computadoras con software de análisis de tráfico y en general dispositivos con soporte para SNMP, RMON y NETFLOW.

Este enfoque no agrega tráfico en la red a diferencia del activo. Es utilizado para caracterizar el tráfico en la red y contabilizar su uso.

Técnicas de monitoreo pasivo

- Solicitudes remotas
    - Mediante SNMP

      Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados *traps* que indican que un evento inusual se ha producido.

    - Otros métodos de acceso

      Se pueden realizar scripts que tengan acceso a dispositivos remotos para obtener información importante a monitorear. En esta técnica se pueden emplear módulos de perl, ssh con autenticación de llave pública, etc.

- Captura de tráfico

  Se puede llevar a cabo de dos formas:

  1. Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura.

2. Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

- Análisis de tráfico

  Se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivos *probe* que envíen información mediante RMON o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

- Flujos

  También utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con:

  - La misma IP origen y destino.
  - El mismo puerto TCP origen y destino.
  - El mismo tipo de aplicación.

Los flujos pueden ser obtenidos de Routers o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos[12].

2.2 Protocolos de red

Las redes informáticas se sirven de modelos conceptuales o marcos de trabajo con cabida a una compleja cadena de eventos: el movimiento de datos de una red.

A finales de los sesentas ISO (***International Organization for Standardization, Organización Internacional para la Normalidad***), desarrolló un modelo para la conexión de red: en los entornos de trabajo se le conoce como modelo OSI (***Open System Interconnection, Modelo de Interconexión de Sistemas Abiertos***), para 1984, este modelo pasó a ser el estándar internacional para las comunicaciones en red al ofrecer un marco de trabajo conceptual que permitía explicar el modo en que los datos se desplazan dentro de una red.

Las computadoras que ejecutan sistemas operativos distintos pueden comunicarse entre sí si utilizan el mismo conjunto de protocolos de red. Esto es lo explica que una máquina UNIX, una Macintosh o un PC que esté ejecutando Windows utilicen el TCP/IP para comunicarse en Internet.

---

[12]Monitoreo de Recursos de Red, Vicente Altamirano Carlos, UNAM, Primera edición, México 2005.

2.2.1 Modelo OSI

El modelo OSI se encuentra dividido en 7 capas, cuya estructura se muestra en la figura 2.1, las cuales trabajan de la siguiente forma: suponiendo que un usuario decide enviar un mensaje de correo electrónico a otro usuario de la red, el usuario que envía el mensaje utilizará un cliente o programa de correo como herramienta de interfaz para escribir y enviar el mensaje, esta actividad se produce en la capa de aplicación.

Cuando los datos abandonan la capa de aplicación (la capa insertará un encabezado de capa de aplicación en el paquete de datos), éstos pasan por las restantes capas del modelo OSI. Cada capa proporcionará servicios específicos relacionados con el enlace de comunicación que debe establecerse.

Al margen de la función específica que tenga asignada cada capa, todas adjuntan un encabezado a los datos. Puesto que la capa física está integrada por dispositivos de hardware nunca añade un encabezado a los datos.

Los datos llegan así a la capa física (el entorno tangible de la red) de la computadora destino, desplazándose por el entorno físico de la red hasta alcanzar su destino final: el usuario al que va dirigido el mensaje de correo electrónico.

Los datos se reciben en la capa física de la computadora del destinatario y empiezan a subir por la pila OSI. A medida que los datos pasan por cada capa, el encabezado pertinente se va suprimiendo de los datos. Cuando los datos alcanzan la capa de aplicación, el destinatario puede utilizar su cliente de correo electrónico para leer el mensaje que ha recibido[13].

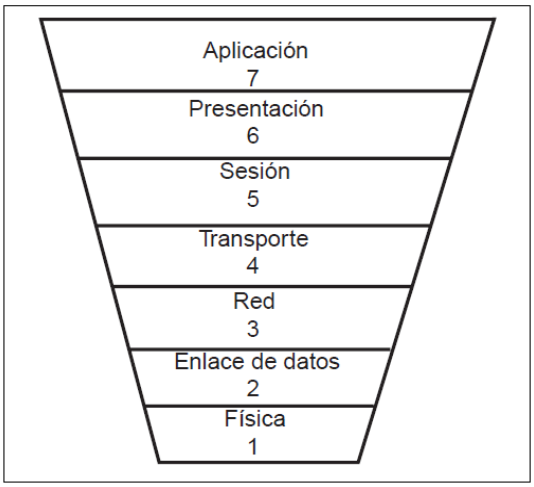


Figura 2.1 Capas del modelo OSI.

2.2.2 TCP/IP

TCP/IP surge alrededor de 1960 pensado como sistema de comunicación basado en redes de conmutación de paquetes desarrollado por el gobierno estadounidense y la agencia de defensa ARPA. En la actualidad TCP/IP constituye la infraestructura tecnológica más grande y desarrollada sobre la que circulan las comunicaciones electrónicas (datos, voz, multimedia). Su expansión se ha dado por el desarrollo de Internet.

---

[13] Modelo OSI y protocolos de red. Capítulo 2.

Hablando de los equipos con una implementación de protocolos TCP/IP, se distinguen dos grupos, todos ellos objetivo de los potenciales ataques:

- *Sistemas.* Son aquellos equipos que engloban clientes de un servicio (como una estación de trabajo con un sistema operativo cliente como Windows, Unix, MacOS, etc.), o un dispositivo móvil (como PDAs o teléfonos móviles), como a los servidores ejecutando un sistema operativo servidor: AS/400, Windows NT/2000, Novell NetWare o Unix (en todas sus variantes: HP-UX, Linux, Solaris, AIX); estos suelen ser el objetivo de los hackers, al ser uno de los contenedores más importantes de información.
- *Dispositivos de red.* Son aquellos encargados de que el tráfico de la red pueda fluir correctamente entre redes, esto engloba a repetidores, puentes, concentradores, conmutadores, routers, firewalls, servidores de terminales, dispositivos de almacenamiento, etc.

Desde el punto de vista de la seguridad, la familia de protocolos TCP/IP puede ser vulnerada en base a dos conceptos inherentes a su diseño:

1. *El formato de los paquetes de los diferentes protocolos*. Independiente de la información transportada, la información contenida en cada uno de los campos de las cabeceras de los protocolos proporciona una fuente muy valiosa de conocimiento.

2. *El modo de funcionamiento de los protocolos.* Es posible analizar la existencia de vulnerabilidades por medio de las etapas que son asociadas a cada proceso en los protocolos ya que esto ofrece la información necesaria.

2.3 Protocolos de monitoreo de red

Una vez que el alcance de un entorno informático se extiende más allá de una LAN y algunas PCs, la gestión de redes eficaz sólo es posible con un conjunto de herramientas automatizadas de gestión de red. Para hacer frente al entorno multifabricante de la instalación típica, es necesario un sistema de gestión de red basado en protocolos normalizados de gestión de red y aplicaciones.

2.3.1 Protocolo SNMP

SNMP (***Simple Network Management Protocol, Protocolo Simple de Gestión de Red***), es el protocolo de nivel aplicación de la suite TCP/IP diseñado para el intercambio de información de administración de los dispositivos de la red.

SNMP permite crear herramientas de gestión que permiten:

- Crear informes del funcionamiento de la red o subred.
- Detectar funcionamientos incorrectos.
- Permiten actuar sobre los elementos de la red: modificando la configuración, desconectando equipos, etc.

Este protocolo recupera información que los dispositivos mantienen en base a datos denominados MIB (***Management Information Base, Base de Información para Gestión***).

Los MIBs contienen, organizados de forma jerárquica, un conjunto de información estadística y valores de control que pueden ser utilizados de forma estándar o como extensiones propias de los diferentes agentes y gestores.

SNMP define dos operaciones:

- Lectura por parte del gestor de un registro del MIB del agente.
- Modificación de alguno de estos valores.

Manejando un MIB y un gestor SNMP se puede:

- Modificar las tablas de ruteo.
- Conocer estadísticas de funcionamiento de un servidor.
- Desconectar una estación de trabajo de la red.
- Ver los paquetes que circulan por una subred.
- Hasta conocer la temperatura de funcionamiento de un concentrador.

Todo esto se muestra de forma gráfica con un ambiente agradable, por ejemplo: muestra iconos para los agentes, planos de los edificios donde se sitúan las redes, mapas de situación, líneas de colores que indican el nivel de tráfico de los enlaces, entre muchas otras cosas.

SNMP es un protocolo basado en UDP, es decir, no orientado a conexión. SNMP define una relación cliente/servidor entre el gestor de red (que actúa de cliente) y los elementos gestionados (que son los servidores llamados 'Agentes SNMP').

Los agentes pueden ser:

- Ordenadores conectados en la red.
- Servidores de ficheros, webs, de correo, etc.
- Bridges.
- Routers.
- Concentradores.
- Hubs de una red Token-Ring.
- Impresoras de red, etc.

Tanto los agentes como el gestor manejan una base de datos de información gestionable llamado MIB.

Ventajas de SNMP

- SNMP es bastante popular y casi todo lo que se puede conectar a una red puede convertirse en un agente SNMP.
- Es bastante flexible, se puede adaptar a las necesidades de gestión de cualquier elemento.

- Es extensible, esto quiere decir que un gestor bien diseñado puede aprender nuevos MIB de forma automática.
- Es la única forma de gestionar una red grande heterogénea (como lo es Internet).

Desventajas de SNMP

- Es difícil de implementar.
- No es muy eficiente, ocupa demasiado ancho de banda.

A continuación se muestra tabla de protocolos de red, especificando puntualmente su función.

Tabla 2.1 Protocolos de red.

Protocolo	**Descripción**
DNS	Este protocolo se utiliza para poder recordar de manera sencilla las direcciones IP. Gracias a esto se puede asignar a una dirección IP un nombre, además de que es más fiable porque la dirección IP de un servidor puede cambiar pero el nombre no lo hace. Se puede decir entonces que el DNS es un sistema jerárquico y distribuido que permite traducir nombres de dominio en direcciones IP y viceversa.
FTP	File Transfer Protocol o Protocolo de Transferencia de Archivos proporciona una interfaz y servicio para la transferencia de archivos en la red.

HTTP	Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertexto, es el protocolo usado en cada transacción de la World Wide Web.
NFS	El Network File System o Sistema de Archivos de Red, es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.
NTP	El Network Time Protocol, es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable.
SMTP	El Simple Mail Transport Protocol o Protocolo Simple de Transferencia de Correo proporciona servicios de correo electrónico en las redes de Internet e IP.
SNMP	El Protocolo Simple de Administración de Red, es un protocolo que facilita el intercambio de información de administración entre dispositivos de red. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.
SSH	Secure Shell o Intérprete de Órdenes Seguras, es el protocolo que sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos.
TELNET	Es el nombre del protocolo de red que sirve para acceder mediante una red a otra máquina para manejarla remotamente como si se estuviera

	sentado delante de ella.
SSL	Protocolo de Capa de Conexión Segura, proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.
TCP	El Transport Control Protocol o Protocolo de Control de Transporte es un protocolo de transporte orientado a conexión. TCP gestiona la conexión entre las computadoras emisoras y receptoras de forma parecida al desarrollo de las llamadas telefónicas.
UDP	El User Datagram Protocol o Protocolo de Datagrama de Usuario es un protocolo de transporte sin conexión que proporciona servicios en colaboración con TCP.
IP	El Internet Protocol o Protocolo de Internet es la base para todo el direccionamiento que se produce en las redes TCP/IP y proporciona un protocolo orientado a la capa de red sin conexión.
ARP	El Address Resolution Protocol o Protocolo de Resolución de Direcciones hace corresponder las direcciones IP con las direcciones MAC de hardware.

2.4 Monitoreo de usuarios

Un analizador de paquetes (también conocido como un analizador de red, sniffer o analizador de protocolos, para determinados tipos de red) es un programa o una pieza de hardware que puede interceptar y registrar el tráfico que pasa sobre una red o parte de ella. Como las secuencias de datos fluyen a través de la red, la captura succiona cada paquete y si es necesario, descifra los datos en bruto de paquetes, mostrando los valores y analizando su contenido de acuerdo con su correspondiente RFC o sus especificaciones. El software que permite el monitoreo es amplio, ya que permite inspeccionar el tráfico y obtener diversa información de éste, desde los paquetes enviados, hasta las consultas web que el usuario puede estar haciendo.

Modo promiscuo de una red

Las redes Ethernet funcionan basadas en el método CSMA-CD (***Carrier Sense Multiple Access – Collision Detection***). Esto significa que cada nodo en una red Ethernet tiene la capacidad de detectar si está conectado a una red o no hay un enlace válido (Carrier Sense) y que el mismo medio físico es compartido entre varias computadoras (Multiple Access). Al tener un mismo medio compartido, dos computadoras podrían intentar transmitir datos a la vez, lo que llevaría a que ambos flujos de datos se corrompieran, por lo que se hace necesario que haya una detección de colisiones (Collision Detection) y un mecanismo de respuesta a las colisiones. En caso de haber una colisión, ambas computadoras esperarán un tiempo aleatorio e intentarán re-enviar sus paquetes.

Las redes Ethernet originalmente estaban conformadas por un sólo cable que conectaba, una a una, a todas las computadoras. Aún hoy, con los cambios topológicos que han sufrido, toda red Ethernet emula este comportamiento: cualquier paquete que es enviado a la red llega a todos los nodos de la misma (excepto en las redes switcheadas). Esto significa que cada computadora de la red tiene la capacidad de escuchar el tráfico dirigido a cualquier otra computadora de la red.

Procesar un paquete que llega por la red siempre supone trabajo para el sistema operativo. Es por ello que las tarjetas Ethernet por default no reportan al sistema operativo, paquetes que no estén destinados a esa computadora (dando explícitamente su dirección física o MAC) o a todas las computadoras de la red (enviadas a la dirección física de broadcast, FF:FF:FF:FF:FF:FF). Para que el sistema operativo reciba todos los paquetes es necesario desactivar este filtro, lo que es conocido como colocar la interfaz en modo promiscuo.

Una vez que la tarjeta está en modo promiscuo, ésta entregará al sistema operativo todos los paquetes que pasen por su cable. Utilizando bibliotecas como libpcap, programas en espacio de usuario pueden solicitar al kernel que les entregue todos estos paquetes para procesarlos y reportar al usuario los datos obtenidos de ellos. Esto es conocido como sniffing (olfateo en inglés).

Un segmento de red Ethernet que va creciendo en actividad presenta cada vez más colisiones y su rendimiento cae de manera abrupta. Como las redes medianas y grandes son cada vez más comunes, a fines de los 90s comenzaron a popularizarse los

switches; equipos de conectividad Ethernet similares a los concentradores que, en vez de enviar cada paquete a todas las computadoras del segmento, los envía únicamente al puerto donde está conectada la computadora destinatario.

Al aparecer los switches, todo parecía indicar que sniffear las redes sería ya imposible, a menos que fuera hecho desde el segmento donde estuvieran las computadoras en cuestión. Tristemente, esta ilusión no duró mucho tiempo, gracias al advenimiento del ARP spoofing/poisoning. Para no entrar en detalles, se muestra rápidamente cómo funciona el comportamiento entre Ethernet y TCP/IP: El protocolo ARP.

Cada tarjeta de red Ethernet tiene un identificador de 48 bits (supuestamente único) en el mundo, llamado dirección MAC (***Media Access Control, Control de Acceso al Medio***). Las direcciones IP son direcciones de 32 bits y no guardan relación alguna con las direcciones MAC.

Cuando una computadora intenta comunicarse con otra que debe estar (según su dirección IP) en la misma red que ésta, lanza un paquete ARP (***Address Resolution Protocol, Protocolo de Resolución de Direcciones***) de tipo “who-has”, dirigido a todas las computadoras del segmento físico (con la dirección broadcast de Ethernet), con la IP de la máquina destino. A esta solicitud, la computadora dueña de la IP solicitada responde con un nuevo paquete ARP (ya en unicast) a la computadora que originó la solicitud, indicándole su dirección física. Después de esto, ambas conocen ya la relación entre MAC e IP necesaria, y pueden comenzar a enviarse paquetes IP.

Parte del diseño del protocolo ARP estipula que, si una computadora tiene registrada la relación IP-MAC de otra en su tabla de ARP y escucha un nuevo paquete ARP anunciando que la IP en cuestión está relacionada con otra ARP, debe olvidar la relación que tenía declarada y registrar la nueva. Por tanto, una computadora cualquiera en la red puede envenenar fácilmente las tablas ARP de las demás, recibiendo los paquetes destinados a una computadora, aún en otro segmento de una red switcheada, e inclusive actuar como proxy, logrando escuchar (e incluso intervenir) de manera completamente transparente la comunicación. Claro está, quien lo esté haciendo tendrá que cuidar el volver a envenenar las tablas ARP cada que haya una solicitud para mantenerse como escucha.

CAPÍTULO III. HERRAMIENTAS DE MONITOREO

El monitoreo de la red es un mecanismo preventivo y de control para detectar y solucionar problemas diversos. Uno de esos problemas puede ser el ruido en la línea, el cual provoca errores (como direcciones falsas de nodos, etc.).

Existe un gran número de herramientas de monitoreo en el mercado, las cuales se diferencian en distintos aspectos. En dependencia de los objetivos que se persigan una u otra herramienta podrá resultar idónea en correspondencia con su funcionamiento y las preferencias de los administradores.

Actualmente, un punto importante que contemplan los administradores, corresponde al tipo de licenciamiento con las que estas herramientas son distribuidas. Generando un impacto importante, tanto en la parte económica como en la operativa, esto por la alta adaptabilidad (debido a su propiedad de modificar el código, adaptándolo a su medida) y calidad que proporcionan.

El software libre es un asunto cada vez más cotidiano y está dejando de ser asunto de técnicos, entusiastas o usuarios avanzados. Hoy en día la comunidad del software libre dispone de múltiples herramientas de alta calidad.

Las herramientas de monitoreo permiten obtener información) de todos los intentos de conexión que se produzcan en el sistema o sobre otro que se indiquen, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP.

Algunas herramientas permiten tener control sobre todos los paquetes que entran por el interfaz de red de la máquina: IP (TCP, UDP) e ICMP, o analizando paquetes a nivel de aplicaciones (TELNET, FTP, SMTP, LOGIN, SHELL...).

Estas herramientas pueden ser utilizadas junto con otras que permitan definir desde qué máquinas se permiten ciertas conexiones y de cuales se prohíben.

Algunas de estas herramientas no necesitan estar instaladas en la máquina que se quiere controlar (ya que se puede instalar en una máquina cuyo interfaz de red funcione en modo promiscuo, permitiendo seleccionar la dirección IP o máquina que se quiera auditar).

Algunas pueden tener un doble uso, es decir, ofrecen protección ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer sistemas. Por eso es importante que el uso de estas herramientas esté restringido (en la manera que se pueda) para que personal no autorizado no pueda utilizarlas de forma aleatoria y se oculte realmente un ataque. También podrán ser utilizadas para hacer seguimientos en

la red cuando se sospeche que alguna de las máquinas en la red ha sido comprometida.

3.1 Software libre

La definición de Software Libre publicada por FSF (***Free Software Foundation, Fundación por el Software Libre***) hace énfasis en definir al software libre como un asunto de libertad y no de precio. Es muy común que exista cierta confusión entre usuarios respecto al término “free software”, la confusión debido a que en inglés *free* significa tanto libre como gratuito, así la FSF determina que el término sea utilizado en su aceptación de libertad como en libertad de expresión como “free speech” y no en términos de gratitud como “free ticket” (Boleto gratis)[14].

Una definición más moderna, cuenta con cuatro puntos. Mencionando lo que define al software libre, lo tenga o no el que recibe dicho software:

Tabla 3.1 Software Libre.

Libertad	**Descripción**
0	La libertad de usar el programa, con cualquier propósito.
1	La libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a tus necesidades.
2	La libertad de distribuir copias del programa, con lo cual se puede

14 FUENTE: Free Software Foundation. «La Definición de Software Libre». Consultado el 16 de noviembre de 2009. «El "software libre" es una cuestión de libertad, no de precio. Para entender el concepto, debería pensar en "libre" como en "libre expresión", no como en "barra libre".».

	ayudar.
3	La libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie.
Las libertades 1 y 3 requieren acceso al código fuente porque estudiar y modificar software sin su código fuente es muy poco viable.	

Se debe recordar que “software libre” no significa “software no comercial”. Cuando se habla de un software libre, indica que debe encontrarse disponible para uso comercial, desarrollo comercial y distribución comercial. Actualmente este término ha dejado de ser inusual y se ha convertido en una parte importante y común.

Analógicamente, el “software gratis” en ocasiones incluye el código fuente; sin embargo, este tipo de software no es libre en el mismo sentido que el término de “software libre”, a menos que se garanticen los derechos de modificación y redistribución de las versionas una vez modificadas.

Actualmente se ha iniciado el uso del término FOSS o FLOSS(***Free and Open Source Software, Software Libre y de Código Abierto***), aunque esto no quiere decir que los términos “libre” y “open” se inicien a utilizar como sinónimo, realmente la confusión y el mal uso de estos términos continua siendo de lo más común.

3.1.1 Ventajas del software libre

- *Escrutinio Público:* Debido a que son muchas las personas que tienen acceso al código fuente, eso lleva a un proceso de corrección de

errores muy dinámico, no hace falta esperar que el proveedor del software saque una nueva versión.

- *Software de dominio público:* Este tipo de software no tienen licencias de uso, por lo tanto corre el peligro de dejar de serlo si alguien lo utiliza con el fin de apropiárselo, modificando algún aspecto de dicho software.
- *Manejo de la Lengua:*
    - *Traducción:* Este punto se refiere a que cualquier persona capacitada puede traducir y adaptar un software libre a cualquier lengua.
    - *Corrección ortográfica y gramatical:* Una vez traducido el software libre puede presentar errores de este tipo, los cuales pueden ser subsanados con mayor rapidez por alguna otra persona a la que se le facilite más.
- *Mayor seguridad y privacidad:* Los sistemas de almacenamiento y recuperación de la información son públicos. Cualquier persona puede ver y entender cómo se almacenan los datos en un determinado formato o sistema.
- *Garantía de continuidad:* El software libre puede seguir siendo usado aun después de que haya desaparecido la persona que lo elaboro, dado que cualquier técnico informático puede continuar desarrollándolo, mejorándolo o adaptándolo (el tema de adaptación es una de las partes que más suelen ser vistas como ventajas sobre todo en las organizaciones).

- *Ahorro en costos:* Principalmente se disminuye el de adquisición, de implantación de soporte o costo y mantenimiento así como el interoperabilidad.

3.1.2 Desventajas del software libre

- *Dificultad en el intercambio de archivos:* Esto se da mayormente en los documentos de texto (usualmente generados por Word), ya que si se quisiera abrir con un software libre, envía errores y muchas veces se pierden datos. Pero está claro que si Microsoft Word creara sus documentos con un código abierto o un formato abierto claramente este tipo de errores no sucederían.
- *Mayores Costos de implantación e interoperabilidad:* Esto dado que el software constituye “algo nuevo”, ello supone afrontar un costo de aprendizaje, de instalación, de migración y de interoperabilidad.
- *Mayor curva de aprendizaje:* Si se ponen a dos señoras que nunca han tocado una PC, probablemente tardaran lo mismo en aprender a usar una Windows que Gnome o KDE.
- *El software libre no tiene garantía proveniente del autor:* Los contratos de software propietario tampoco se hacen responsables por daños económicos, y de otros tipos por el uso de sus programas.

El software generalmente se vende como está, sin garantías explicitas del fabricante, sin embargo, puede haber garantías específicas para situaciones muy específicas.

En el presente trabajo, se abordarán tres herramientas que se emplean en el monitoreo del tráfico generado en la red para realizar un análisis el cual permita emitir acciones preventivas y/o correctivas a distintas fallas o vulnerabilidades.

3.2 Wireshark

Wireshark es una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado denominado como analizador de protocolos de red, analizador de paquetes, packet sniffer o sniffer. Wireshark permite analizar los paquetes de datos en una red activa como también desde un archivo de lectura previamente generado, un caso particular es generar un archivo con TCPDUMP y luego analizarlo con Wireshark.

A partir del año 2006 Ethereal es conocido como Wireshark y hoy en día está categorizado como uno de los TOP 10 como sniffer.

3.2.1 Características

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.

- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Es importante tener presente que Wireshark no es un IDS (***Intrusion Detection System, Sistema de Detección de Intrusos***) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red. Sin embargo, permite a los profesionales de IT analizar y solventar comportamientos anómalos en el tráfico de la red.

3.3 TCPDUMP

Una de las actividades más comunes en la administración de una red o administración de seguridad es la del análisis de tráfico de dicha red. No sólo el tráfico que fluye a través de una LAN sino que también se debe analizar el tráfico entrante y saliente hacia internet a través de los servicios que se tengan instalados, proxys, etc. Esto es así porque, como se sabe, es necesario para la detección de problemas y sobre todo para detectar tráfico no esperado, presencia de puertas traseras, escaneos y cualquier otra intrusión.

Existen muchas herramientas que pueden ser muy útiles dependiendo del S.O. y tipo de red por ejemplo. Una de estas herramientas, es TCPDUMP, basado en la librería de captura de paquetes (pcap) y que además funciona en plataformas tanto Linux / UNIX como Windows esta última hace uso de la librería Winpcap. Estas dos librerías son usadas por otras herramientas como Ethereal o Snort e incluyen un lenguaje de filtro común para todos. Quizás Windump / Tcpdump no sea la herramienta perfecta atendiendo a la interpretación fácil de los datos reportados, pero sí que es de las mejores en cuanto a su potencia y cantidad de datos de que provee.

3.3.1. Características

- Tcpdump imprime una descripción del contenido de los paquetes en una interfaz de red que coincidan con la expresión lógica.

- Funciona en plataformas tanto Windows como Linux / UNIX.
    - Tcpdump para Linux.
    - Windump para Windows.
- Captura paquetes IP, TCP, ICMP y UDP.
- Puede ser modificado fácilmente para adaptarlo a cualquier protocolo, simplemente cambiando las definiciones de las cabeceras.
- Se pueden utilizar algunos filtros, como número de puerto, host específico, etc. Por ejemplo:

Tabla 3.2 Simplest Codings.

Expresión	**Descripción**
IP	Captura todos los paquetes IP.
TCP	Captura todos los paquetes TCP.
Port 80	Captura los paquetes TCP por el puerto 80.
IP host 10.1.2.3	Captura los paquetes con origen/destino en el host 10.1.2.3.

3.4 NTOP

Ntop es una herramienta sencilla, de software libre sobre monitoreo. Esta herramienta trabaja bajo Linux, Mac SO X, FreeBSD, Solaris y las versiones de 32-bit de Windows. Ntop proporciona una gran visibilidad de la red, algunos de sus principales usos es conocer cuáles son los hosts que consumen la mayor parte del ancho de banda (los principales transmisores), así como los protocolos y las aplicaciones más utilizados en la red. Ntop también profundiza incluso hasta llegar a mostrar qué compañeros de host en particular se han puesto en contacto, así como el tráfico de host local de la matriz que indica la cantidad de información que se aloja en su red está siendo intercambiados entre sí. Como advertencia cabe mencionar que para conseguir la verdadera visibilidad de la red, la red debe ser enrutada y no utilizada por PAT***(Port Address Translation, Traducción de Direcciones de Puertos)***. Ntop verá cada máquina detrás de un router PAT como un único dispositivo (aunque con múltiples conexiones de PAT) es decir, genera un escudo, que incluso Ntop no puede ver.

Ntop es un ejemplo de herramienta de monitoreo utilizada para conocer qué es lo que está sucediendo en la red en tiempo real.

Hay que recordar que antes de hacer un plan encaminado a resolver un problema con la red es muy importante que primero se lleve a cabo un análisis e investigación. Ntop es una herramienta que puede proporcionar las bases para ello, puede vigilar: IPs, IPX (familia de protocolos desarrollado por Novell) y AppleTalk (familia de protocolos utilizado por Apple); NTOP puede medir los siguientes tipos de tráfico:

- Datos enviados/recibidos: paquetes y volumen, clasificado de acuerdo a la red / IP.
- Tráfico Multicast.
- Historiales de sesión TCP.
- Anchos de banda (análisis).
- VLANs y BGP Sistema Autónomo [AS] estadísticas de tráfico.
- VoIP (SIP, Cisco SCCP) Monitoreo.

Además Ntop ofrece opciones para vigilar el tráfico y sus características:

- Red de flujos (configurables por el usuario).
- Utilización de los protocolos (Número de peticiones, picos y tormentas, positivos y negativos) así como su distribución.
- Matriz de tráfico de la red.

- Monitoreo de ARP e ICMP.
- Reconocimiento de diferentes protocolos populares P2P.

Los datos que genera NTOP generalmente no son persistentes, es decir, son almacenados y utilizados por la memoria y son perdidos al reiniciar el servidor o después de un cierto tiempo.

De manera predeterminada, también se puede almacenar la información en una base de datos para el análisis posterior (aunque hay secuencias de comando que permiten hacer eso).

3.4.1 Características

- Su interfaz muy sencilla y vía web.
- Dispone de gran variedad de informes: globales de carga de red, de tráfico entre elementos, de sesiones activas de cada elemento, etc.
- Ntop está escrito en lenguaje C y el código fuente es compatible con varias plataformas, (Windows, Linux, *BSD, Solaris y MacOSX).
- Para capturar los paquetes, la interfaz de red de la máquina que ejecute NTOP debe entrar en modo promiscuo, lo que implica que hay que disponer de * permisos de administrador en dicha máquina.
- NTOP usa por defecto el puerto 3000/TCP para el servidor web de la interfaz.

- En Linux, NTOP está presente en las principales distribuciones y es fácilmente instalable desde el gestor de paquetes de software de la distribución.
- Analiza protocolos TCP/UDP/ICMP.
- Dentro de TCP/UDP es capaz de agruparlos por tipo de servicio que se esté utilizando como FTP, HTTP, SSH, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.
- Entre las que se incluyen Linux, Free BSD, Windows®, SolarisTM, HP-UX y AIX.

CAPÍTULO IV. IMPLEMENTACIÓN DE HERRAMIENTAS DE MONITOREO

El objetivo de esta Tesina es comparar herramientas de software libre para el monitoreo de usuarios por lo que se realizó la implementación de las herramientas sobre una distribución Linux basada en Debian llamada Ubuntu en su versión de escritorio 10.10 debido a su facilidad de uso e instalación del sistema y a que su implementación se realiza mediante licencia gratuita. Facilita la instalación y manejo de diversas herramientas de administración de red, debido a su reducido consumo de recursos a comparación de sistemas operativos de licencias comerciales. Se configuró el equipo de tal modo que se comporte como servidor haciendo de éste la puerta de enlace para todos los demás equipos de la red, logrando así que todo el tráfico de los equipos de la red pase por la interfaz del servidor.

A este ambiente se le adicionaron equipos con los siguientes sistemas operativos: Windows XP, Windows 7, Ubuntu 10.10 x64 y Ubuntu 10.10 x86 así como máquinas

virtuales utilizando Virtual Box con el fin de robustecer la red donde se implementan las siguientes herramientas.

Los equipos se conectan en una red LAN como se muestra en la figura 4.1.

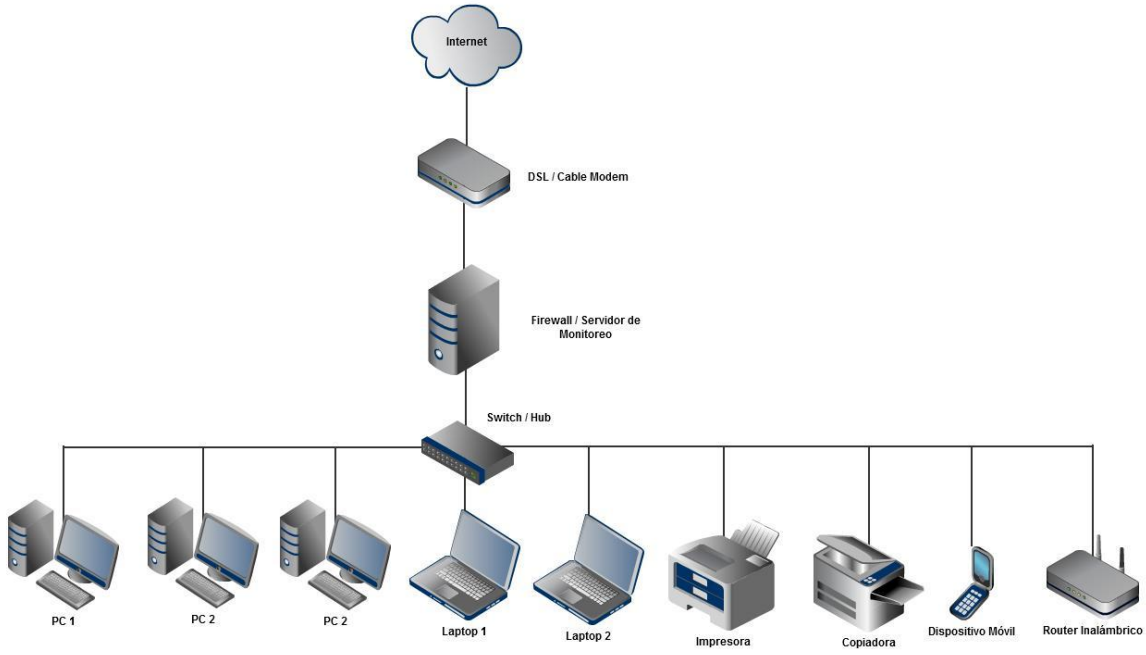


Figura 4.1 Diagrama de Red.

4.1 Wireshark

4.1.1. Captura de paquetes

Una de las principales funciones de Wireshark es capturar paquetes con la finalidad de que los administradores de redes puedan hacer uso de estos y realizar el análisis necesario para tener una red segura y estable. Como requisito para el proceso de capturar datos se requiere ser administrador o

contar con estos privilegios; es necesario identificar exactamente la interfaz que se quiere analizar. Es necesario iniciar la aplicación con privilegios de root en distribuciones de Linux para evitar conflictos al detectar la interfaz sobre la cual se quiere efectuar la captura.

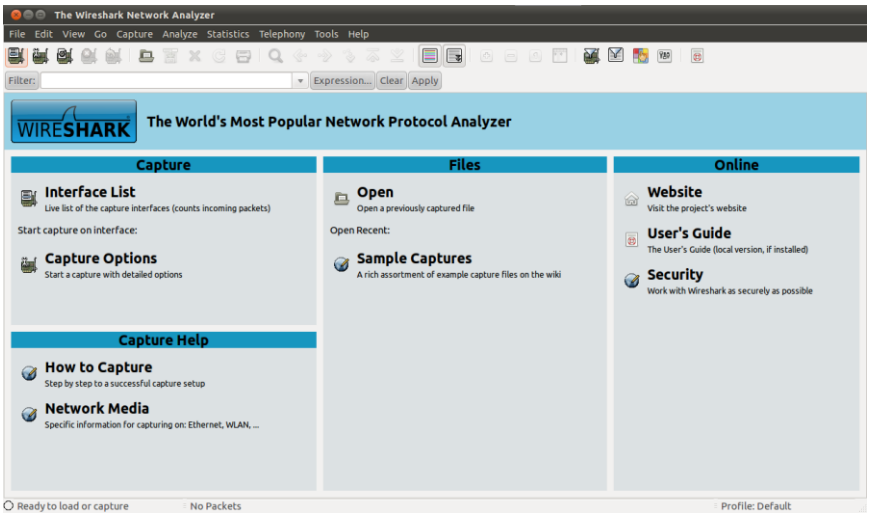


Figura 4.2 Ventana de trabajo de Wireshark.

Wireshark cuenta con cuatro maneras para iniciar la captura de los paquetes:

1. Haciendo doble clic en el ícono  se despliega una ventana donde se listan las interfaces locales disponibles para iniciar la captura de paquetes.

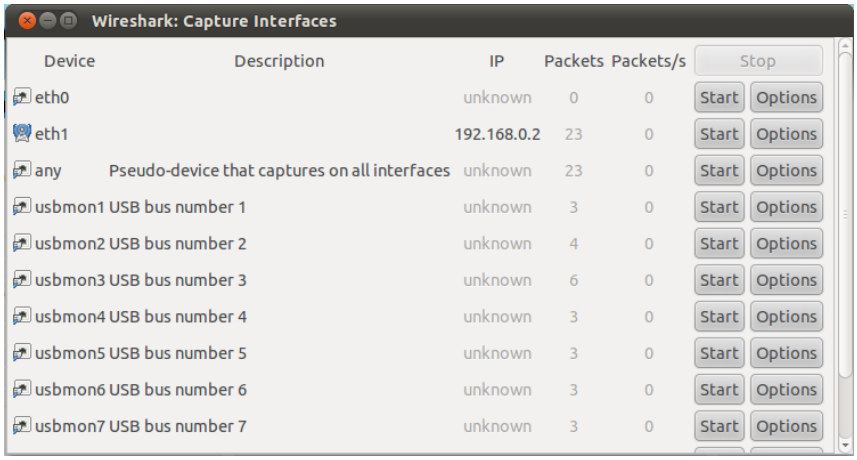


Figura 4.3 Interfaces locales.

Dos botones se visualizan por cada interfaz

- Start, para iniciar.
- Options, para configurar.

2. Otra opción es seleccionar con el Mouse el icono  en la barra de herramientas, se despliega la siguiente ventana donde se muestra opciones de configuración para la interfaz.

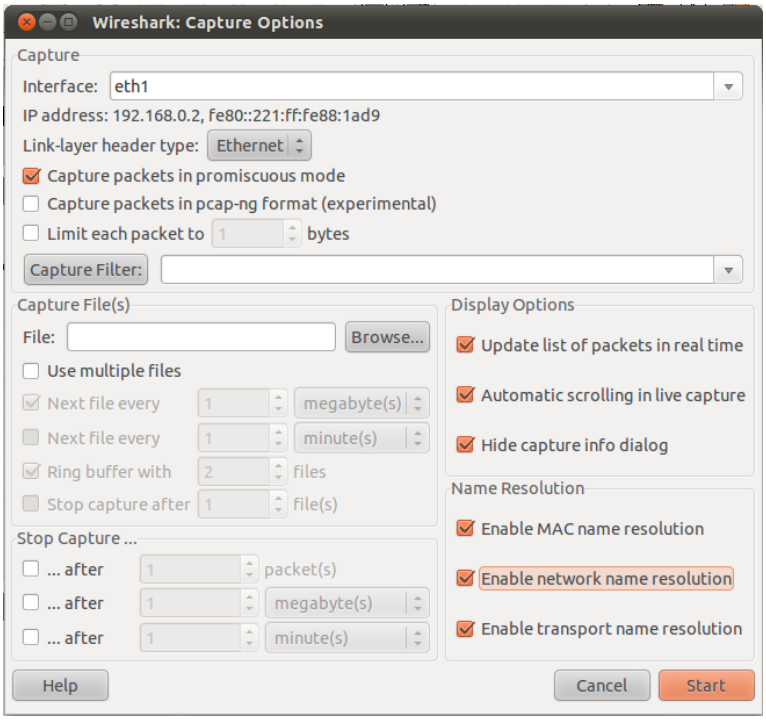


Figura 4.4 Operaciones de configuraciones para interfaz.

3. Si es el caso donde se ha predefinido las opciones de la interfaz, haciendo clic en  se inicia la captura de paquetes inmediatamente.

4. Otra manera de iniciar la captura de paquetes es desde la línea de comandos ejecutando lo siguiente:

```
$ Wireshark –i eth0 –k
```

Donde –i eth0corresponde a la interfaz por la cual se desea iniciar la captura de paquetes y –k es pata iniciar la captura inmediatamente.

Detener/Reiniciar la captura de paquetes

Para detener la captura de paquetes podemos aplicar una de las siguientes opciones:

- Haciendo uso del icono  desde el menú *Capture* o desde la barra de herramientas.
- Haciendo uso de ctrl+E.
- La captura de paquetes puede ser detenida automáticamente, si una de las condiciones de parada definidas en las opciones de la interfaz se cumple, por ejemplo: si se excede cierta cantidad de paquetes.

Para reiniciar el proceso de captura de paquetes se debe seleccionar el icono  en la barra de herramientas o en desde el menú *Capture*.

4.1.2 Filtrado de paquetes

Wireshark hace uso de libpcap para la definición de filtros. Su sintaxis consta de una serie de expresiones conectadas por conjugaciones (*and/or*) con la opción de ser negada por el operador *not*.

```
$ [not] Expresión[and|or [not] expresión…]
```

La siguiente expresión define un filtro para la captura de paquetes desde/hacia los host con dirección IP x.y.z.w y a.b.c.d

```
$ ip.addr==172.17.250.1 and ip.addr==172.17.1.81
```

Expresiones de filtrado

Wireshark proporciona una poderosa herramienta para construir filtros más complejos. Permite comprar valores así como también combinar expresiones dentro de otra expresión.

Cuando es bien conocido el campo por el cual se requiere hacer el filtrado es recomendable hacer uso de *Filter Expresion* desde la barra de herramientas para filtros presionando *Expression…* facilitando la construcción de la expresión o fórmula seleccionando el campo (*field name*), el operador (Relation) y el valor contra el cual se quiere comparar como se muestra en la figura 4.5.

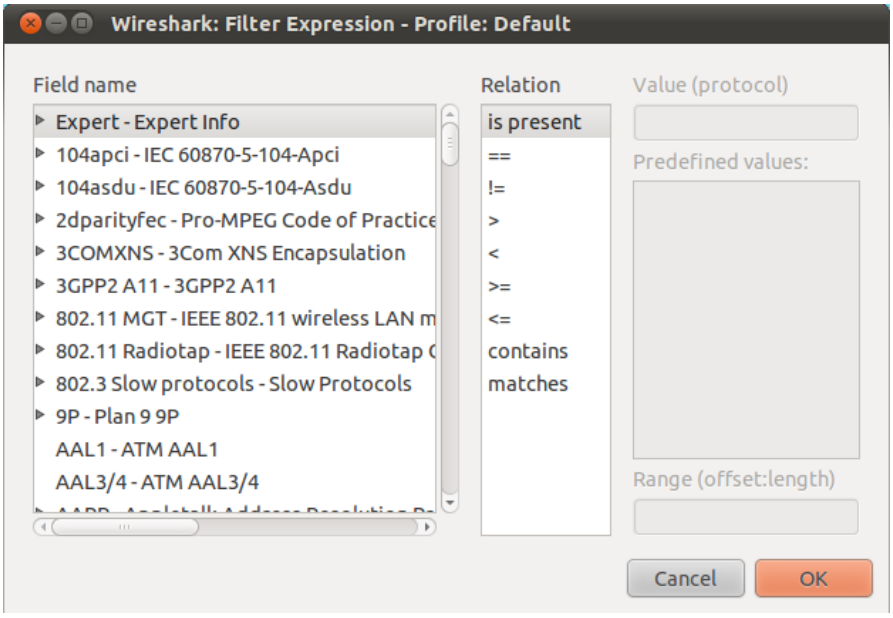


Figura 4.5 Filtros y/o expresiones.

Es muy común que ciertos filtros y/o expresiones requieran ser utilizado en un futuro, para esto Wireshark permite definir los filtros y/o expresiones y guardarlas.

Para guardar o abrir un filtro existente (previamente creado y guardado) se debe seleccionar *Display Filter* en el menú *Analize* o *Capture Filter* que se encuentra en el menú *Capture* como se muestra en la figura 4.6.

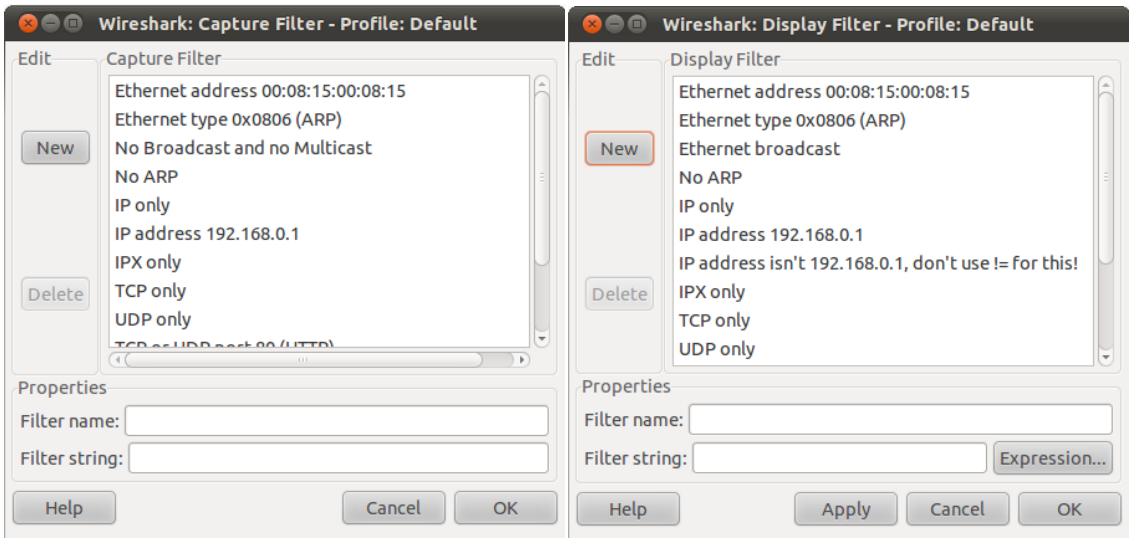
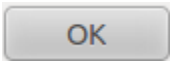


Figura 4.6 Creación de filtros.

Para definir un filtro se debe presionar el botón 

se indica el nombre del filtro y la expresión y presionar 

para salvar los cambios.

Manipulando las paquetes capturados (análisis)

Una vez que se tienen capturados los paquetes estos son listados en el panel de paquetes capturados de la ventana de captura la cual despliega la lista de paquetes ordenados secuencialmente. Se muestra el número de paquete capturado, el tiempo en segundos, las direcciones IP fuente y destino, el protocolo e información relacionada a las peticiones realizadas.

Al seleccionar uno de estos se despliega el contenido del paquete en el resto de los paneles que son panel de detalles de paquetes y panel en bytes.

Expandiendo cualquier parte del árbol que muestra las cabeceras de los protocolos del paquete, se puede seleccionar un campo en particular cuyo contenido se muestra resaltado en negritas en el panel de bytes. En la figura 4.7 se identifica en campo TTL de la cabecera del IP.

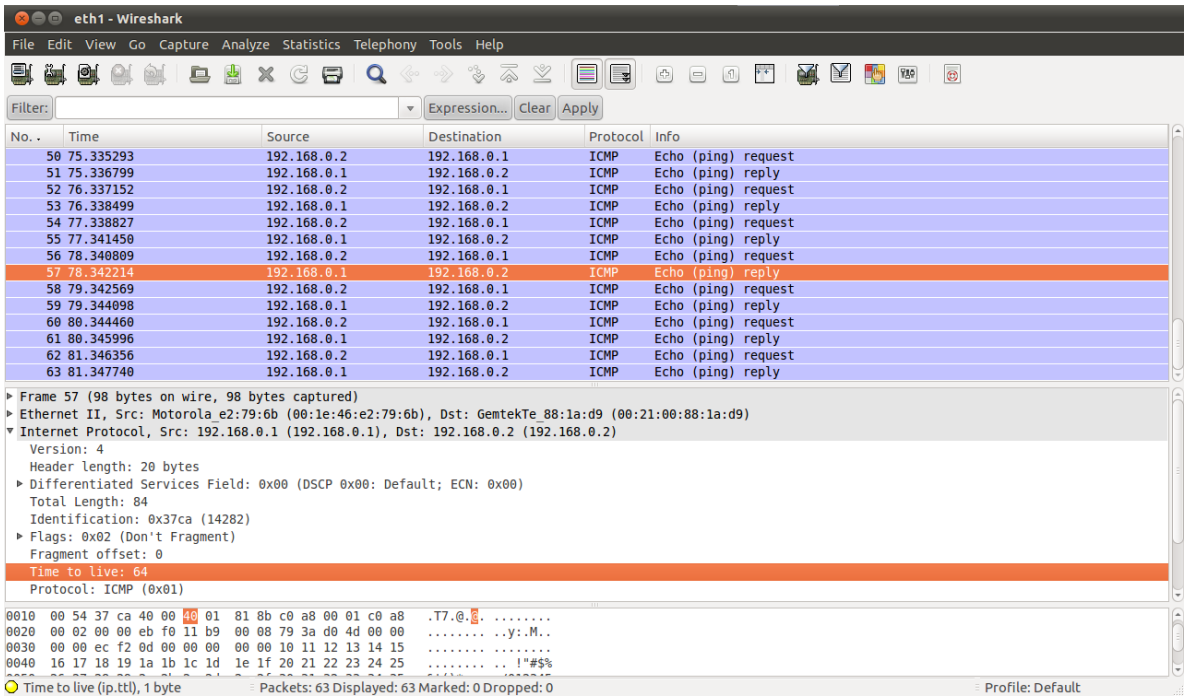


Figura 4.7 Manipulación de paquetes.

Existe una manera de visualizar los paquetes mientras esta activo el proceso de captura esto se logra, seleccionando la opción *Update list packets in real time* desde menú *Edit->Preferentes->Capture*. Adicionalmente, Wireshark permite visualizar el contenido de un paquete seleccionado en el panel de paquetes capturados en una ventana individualmente seleccionando la opción Show Packet in new Windows en menú principal *View*. Esto permite comparar con más facilidad dos o más paquetes.

4.1.3 Función de búsqueda de paquetes

Cuando se inicia la captura de paquetes por lo general se obtiene una gran cantidad de paquetes que cumple con los filtros y/o expresiones definidas, Wireshark permite realizar búsqueda(s) de paquete(s) que tienen cierta característica. Para esto se debe seleccionar la opción *Find Packet* en el menú *Edit* se despliega la siguiente ventana.

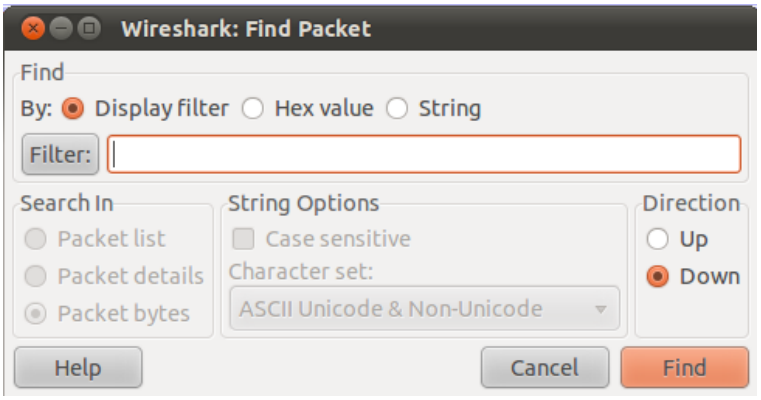


Figura 4.8 Búsqueda de paquetes.

Se rellena el campo *Filter* con el criterio de búsqueda que se desea y el resto de los campos seguidamente se presiona el botón de búsqueda.

Otra opción es realizar la búsqueda del paquete anterior y próximo al que esta seleccionado en el panel de paquetes esto se aplica desde el menú de *Edit* las opciones *Find Next* y *Find Previous*.

Marcado de paquetes

Por lo general el análisis de tráfico es bastante complejo ya que son muchos los paquetes que se obtienen en la captura, Wireshark permite marcar los paquetes para que sean identificados con más facilidad esta marca es aplicar colores a los paquetes en el panel correspondiente.

Existen tres funciones para aplicar el marcado de paquetes:

1. Mark packets (toggle) para marcar el paquete.
2. Mark all packets, aplica la marca a todos los paquetes.
3. Unmark all packets, elimina la marca para todos los paquetes.

4.1.4 Visualización de estadísticas

Wireshark proporciona un rango amplio de estadísticas de red que son accedidas desde el menú *Statistics* que abarcan desde la información general de los paquetes capturados hasta las estadísticas específicas de un protocolo. Se puede distinguir entre cada una de las anteriores:

Estadísticas Generales

- Summary, la cantidad de paquetes capturados.
- Protocol Hierarchy, presenta las estadísticas para cada protocolo de forma jerárquica.

- Conversations, un caso particular es el tráfico entre una IP origen y una IP destino.
- Endpoints, muestra las estadísticas de los paquetes hacia y desde una dirección IP.
- IO Graphs, muestra las estadísticas en grafos.

Estadísticas específicas de los protocolos

Service Response Time entre la solicitud (*request*) y la entrega *(response*) de algún protocolo existente, entre otras.

Es importante tener presente que los números arrojados por estas estadísticas solo tendrán sentido si se tiene un conocimiento previo el protocolo de lo contrario serán un poco compleja de comprender.

4.2 Tcpdump

Es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

La captura se inicia con el comando *Tcpdump –i [interfaz]*, también se puede ejecutar con la opción-w, lo que hace que se guarde el paquete de datos a un archivo para su posterior análisis, y / o con el *r-bandera*, lo que hace que se lea de un archivo guardado de paquetes en lugar de leer los paquetes desde una interfaz de red. En todos los

casos, sólo los paquetes que coinciden con la expresión serán procesados por Tcpdump.

4.2.1 Sinopsis

La siguiente lista describe las opciones más utilizadas en la ejecución de los comandos y se visualiza que tanto se puede obtener del tráfico de la red que se está monitoreando.

- -A: Imprime cada paquete en código ASCII.
- -D: Imprime la lista de interfaces disponibles.
- -n: No convierte las direcciones de salida.
- -p: No utiliza la interfaz especificada en modo promiscuo.
- -t: No imprime la hora de captura de cada trama.
- -x: Imprime cada paquete en hexadecimal.
- -X: Imprime cada paquete en hexadecimal y código ASCII.
- -c count: Cierra el programa tras recibir “count” paquetes.
- -C file_size: Indica el tamaño máximo por archivo de captura almacenado.
- -E algo:secret: Se utiliza para descifrar paquetes IPsec.
- -F file: Se utiliza para filtrar expresiones.
- -i interface: Escucha en la interfaz especificada.
- -M secret: Se utiliza para validación de dígitos de paquetes TCP mediante secreto compartido.
- -r file. Leer los paquetes desde un archivo.

- -s snaplen: Captura el tamaño del paquete en bytes en lugar del valor por default de 65535 bytes.
- -T type: Forza a los paquetes seleccionados por alguna “expresión” ser interpretados por algún tipo en específico.
- -w file: Guarda la salida en el archivo “file”.
- -W file count: Límita el número de archivos creados.
- -y data link type: Establece el modo data link type mediante la captura.
- -Z user: Libera los privilegios de root y establece los del usuario.

Estos comandos son acompañantes en la sinopsis de Tcpdump la cual se presenta a continuación:

```
Tcpdump [AdDefIKlLnNOpqRStuUvxX] [-B buffer_size] [-c count]
[C-file_size][-G rotate_seconds][F-archivo]
[-I interface] [módulo m] [-M secreto]
[R-archivo] [-s snaplen] [tipo T-] [w archivo]
[W-filecount]
[E- spi @ ipaddr algoritmos: secreto, ...]
[Y datalinktype] [-z postrotate-comando] [-Z usuario]
[Expresión]
```

4.2.2 Captura de paquetes

Recordemos que tener conocimientos sobre la línea de comandos en Tcpdump permitirá a la herramienta tener un mejor desempeño.

- Para imprimir todos los paquetes destino u origen de la tarde:

```
tcpdump host sundown
```

- Para imprimir el trafico excluyendo el origen y destino de los host locales.

```
tcpdump ip and not net localnet
```

- Para imprimir los paquetes de inicio y fin (paquetes SIN y FIN).

```
tcpdump 'tcp port 80 and (((ip[2:2] -
((ip[0]&0xf)<<2))-((tcp[12]&0xf0)>>2)) ¡=0)'
```

- Para imprimir los paquetes IP que pesan más de 576bytes y son enviados por el gateway.

```
tcpdump 'gateway snup and ip[2:2]>576'
```

- Para imprimir los paquetes broadcast o multicast que no fueron enviados a través de Ethernet.

```
tcpdump 'ether[0] &1=0 and ip[16]>224'
```

- Para imprimir todos los paquetes ICMP que no generar eco de las peticiones.

```
tcpdump 'icmp[icmptype] != icmp-echo and
icmp[icmptupe] !=icmp-echoreply'
```

4.2.3 Formatos de salida

La salida de Tcpdump depende del protocolo. A continuación se presenta una breve descripción y ejemplos de la mayoría de los formatos.

Si tcpdum no es ejecutado con la bandera *-c,* continúa con la captura de paquetes hasta que es interrumpido por una señal (generada, por ejemplo, al escribir su carácter de interrupción que por lo general es Ctrl-C), si se ejecuta con la opción *–c*, se capturarán paquetes hasta que sea interrumpido por una señal o porque han sido procesados el número especificado.

Una vez que termina la captura de paquetes, tcpdump dará un informe de:

- Paquetes capturados. Es el número de paquetes que tcpdump ha recibido y procesado.

- Paquetes recibidos mediante filtro. Esto depende del SO en que sea ejecutado tcpdump y como se encuentre configurado, si un filtro es especificado en la línea de comandos, algunos sistemas operativos cuentan paquetes independientemente de si corresponde con la expresión de filtro y otros SO cuentan sólo paquetes que corresponde con la expresión de filtro y se procesaron mediante tcpdump.
- Paquetes perdidos por Kernel. Este es el número de paquetes que fueron perdidos por la falta de espacio en el buffer, debido al mecanismo de captura de paquetes en el sistema operativo en que tcpdump se está ejecutando, siempre que el sistema operativo lo reporte de lo contrario es reportado con un '0'.

Es preciso recordar que la lectura de los paquetes de una interfaz de red puede requerir de privilegios especiales. La lectura de un archivo de paquetes guardados no requiere privilegios especiales.

Los paquetes TCP

El formato general de una línea de protocolos TCP es el siguiente:

```
src > dst: flags data-seqno ack window urgent options
```

Src y dst son las direcciones IP (origen destino) y los puertos. Las banderas pueden ser una combinación de: S (SYN), F (FIN), P (PUSH), R (RST), W (ECN CWR) o E (ECN eco), o puede denotarse como '.' (sin bandera).

Cuando hablamos de los datos *seqno* nos referimos a aquellos datos que describen la parte secuencial cubierta por la información de este paquete. ACK es el número de secuencias del próximo dato esperado por otra dirección en la misma conexión. *Window* es el número de bytes de espacio disponible para recepción en buffer en la misma conexión (conexión actual). *Urg* indica que es de tipo urgente los datos en el paquete.

Src, sdt las *banderas (flags)* deben estar siempre presentes. Los otros campos dependen de los contenidos de la cabecera del paquete del protocolo TCP y se emiten sólo si es necesario.

Los paquetes UDP

El formato UDP se ilustra a continuación:

```
actinide.who>broadcast.who: udp 84
```

Esto dice que el puerto en un host *'actínidos'* envía un datagrama UDP al puerto del host broadcast. El paquete contiene 84 bytes de datos e usuario.

Algunos de los servicios UDP son reconocidos (de la fuente o el número de puerto de destino) y se imprime la información de protocolo de nivel superior. En particular, las solicitudes de servicio Nombre de Dominio (RFC-1034/1035) y Sun llamadas RPC (RFC-1050) para NFS.

Fragmentación IP

Los datagramas fragmentados de internet se muestran como:

```
frag id:size@offset+
frag id:size@offset
```

(La primera forma indica que hay más fragmentos. La segunda indica que ese es el último fragmento).

Id se refiere al identificador del fragmento. Size es el tamaño del fragmento (en bytes) excluyendo la cabecera IP. Offset es el fragmento de offset (en bytes) del datagrama original.

La información del fragment es la salida para cada fragment. El primer fragmento contiene la cabecera del protocolo de más alto nivel y la información del fragmento es mostrada después de la información de protocolo. Los fragmentos después del primero no contienen información de

cabecera del protocolo más alto y la información del fragmento de muestra después de las direcciones fuente y destino. Por ejemplo, aquí se muestra parte de un ftp de arizona.edu to lbl-rtsg.arpa sobre una conexión CSNET la cual no parece manejar datagramas de 576 bytes.

```
arizona.ftp-data > rtsg.1170: . 1024:1332(308) ack 1 win
4096 (frag 595a:328@0+)
arizona > rtsg: (frag 595a:204@328)
rtsg.1170 > arizona.ftp-data: . ack 1536 win 2560
```

Hay un par de cosas que deben de notarse: La primera, la dirección en la 2da línea no incluye números de puertos. Esto es debido a que la información del protocolo TCP está en el primer fragmento y no se tiene idea de que puertos o secuencias son cuando se muestran los fragmentos siguientes. Segundo, la información TCP de secuencia en la primera línea es mostrada como si fueran 308 bytes de información de usuario cuando, de hecho, hay 512 bytes (308 en el primer fragmento y 204 en el segundo). Si usted está buscando por huecos en el espacio de secuencia o intenta relacional ACKs con paquetes, esto lo puede confundir.

Un paquete con la bandera IP *no fragmentada* es marcada al final con DF (don’t fragmented).

Marcas de tiempo

Por default, todas las líneas de salida están precedidas por una marca de tiempo. La marca de tiempo es la hora actual del reloj con la forma:

hh:mm:ss.frac

y es tan acertada como el reloj del kernel. La marca de tiempo refleja el tiempo en el que el kernel vío el paquete por primera vez. No intenta hacer la cuenta del tiempo que transcurre de cuando la interfaz Ethernet toma el paquete del cable y cuando al kernel se le interrumpe con el “nuevo paquete”.

4.3 Ntop

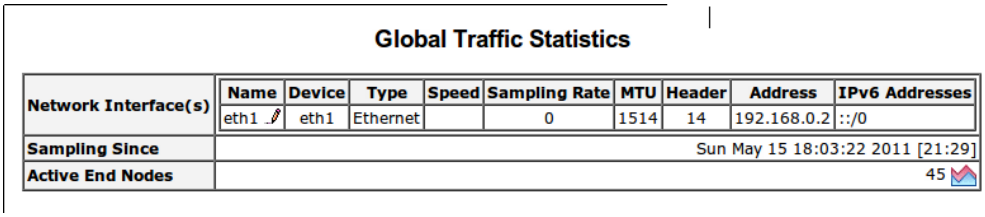
Es una herramienta que permite monitorizar en tiempo real una red. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y para ayudarnos a detectar malas configuraciones de algún equipo, o a nivel de servicio.

Para realizar una captura utilizando Ntop, se debe de ingresar a la consola de administración mediante protocolo http, por lo que se deberá de abrir algún navegador (Internet Explorer, Opera, Chrome, Firefox, etc.) y se deberá de escribir la siguiente dirección en la barra de direcciones: http://localhost:3000.

En caso de que se haya cambiado el puerto en el cual trabaja Ntop (por defecto 300) se deberá de colocar en lugar del puerto por default en la dirección http.

4.3.1 Interfaz

Aquí se muestran algunas pantallas sencillas de la interfaz que maneja Ntop. La figura 4.9 muestra el nombre, tipo, velocidad, direcciones IPv4 e IPv6 de la interfaz de red. También muestra la hora de inicio de la muestra y los nodos activos.



Global Traffic Statistics

	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
Network Interface(s)	eth1	eth1	Ethernet		0	1514	14	192.168.0.2	::/0
Sampling Since	Sun May 15 18:03:22 2011 [21:29]								
Active End Nodes	45								

Figura 4.9 Reporte de tráfico.

Ntop permite visualizar estadísticas mediante gráficos donde se muestra la información agrupada por tipo de tráfico, tiempo de vida de los paquetes, distribución de paquetes por protocolo, carga de tráfico en la red y estadísticas históricas de tráfico como se muestra en las figuras 4.10 y 4.11.

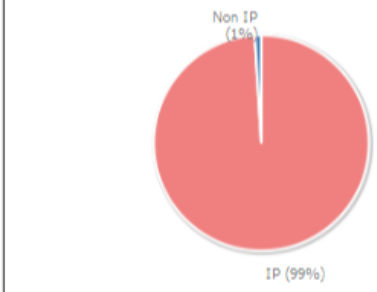
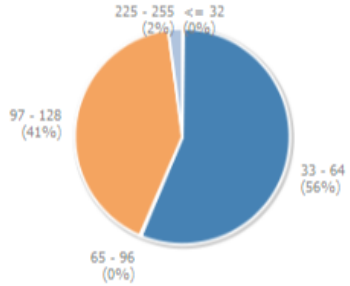
Traffic	**Total**	1.2 GBytes [1,818,361 Pkts]	
	IPv4 Traffic	1.2 GBytes [1,818,175 Pkts]	
	Fragmented IPv4 Traffic	0 [0.0%]	
	Non IPv4 Traffic	2.5 MBytes	
			
	Average TTL		78
	TTL <= 32	0.2%	2,877
	32 < TTL <= 64	56.1%	1,020,225
	64 < TTL <= 96	0.2%	3,267
	96 < TTL <= 128	41.4%	752,903
	128 < TTL <= 160	0.0%	2
	160 < TTL <= 192	0.0%	107
	192 < TTL <= 224	0.0%	0
	224 < TTL <= 256	2.0%	37,253
			

Figura 4.10 Gráficas de tráfico.

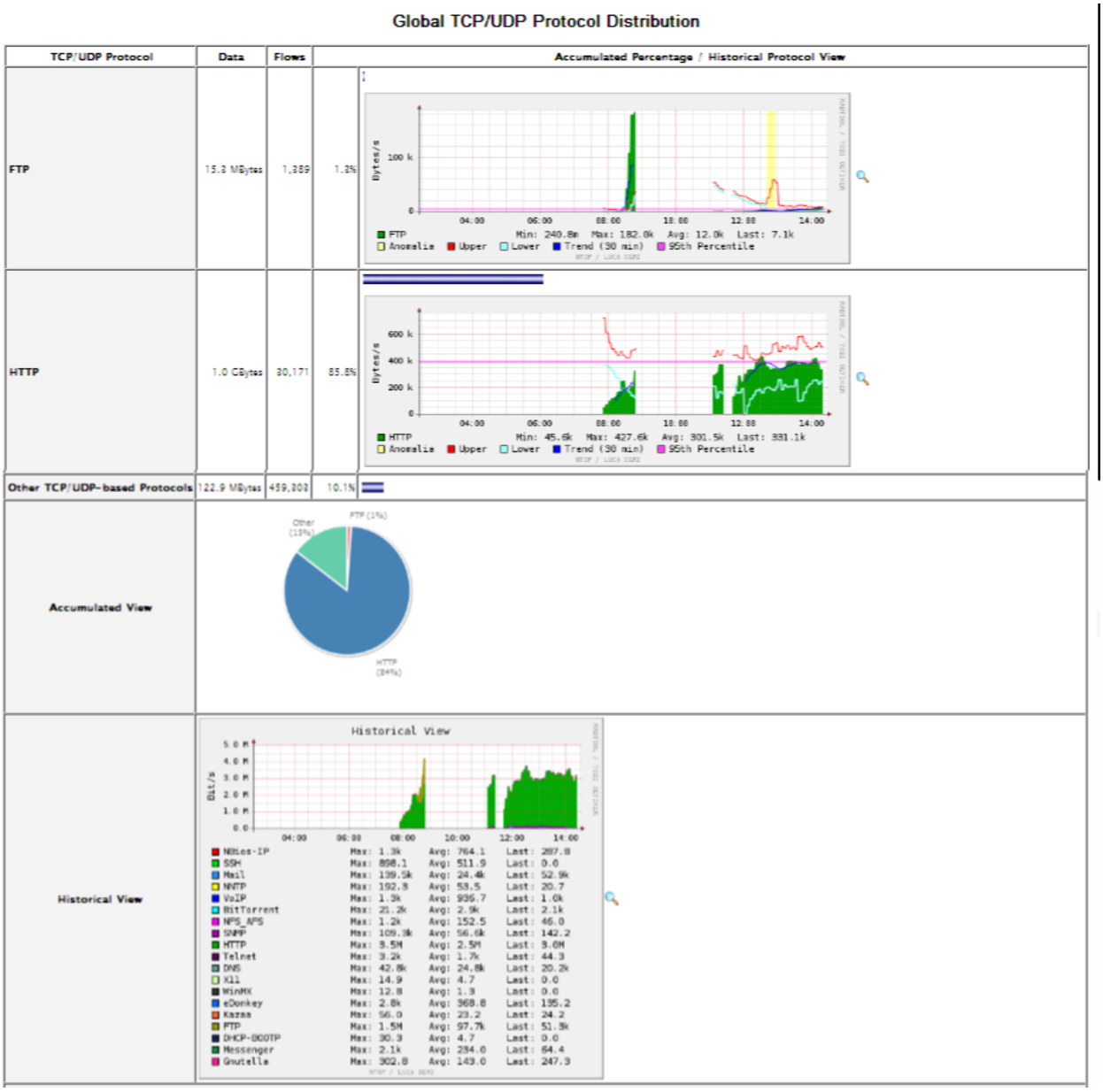


Figura 4.11 TCP / UDP Protocolo de Distribución Global.

La presentación estadística de tráfico de red permite la interpretación de fallas en la red. Esta información se presenta en cuatro graficas que presentan el tráfico de los últimos 10 minutos, la ultima hora, el día actual y el último mes.

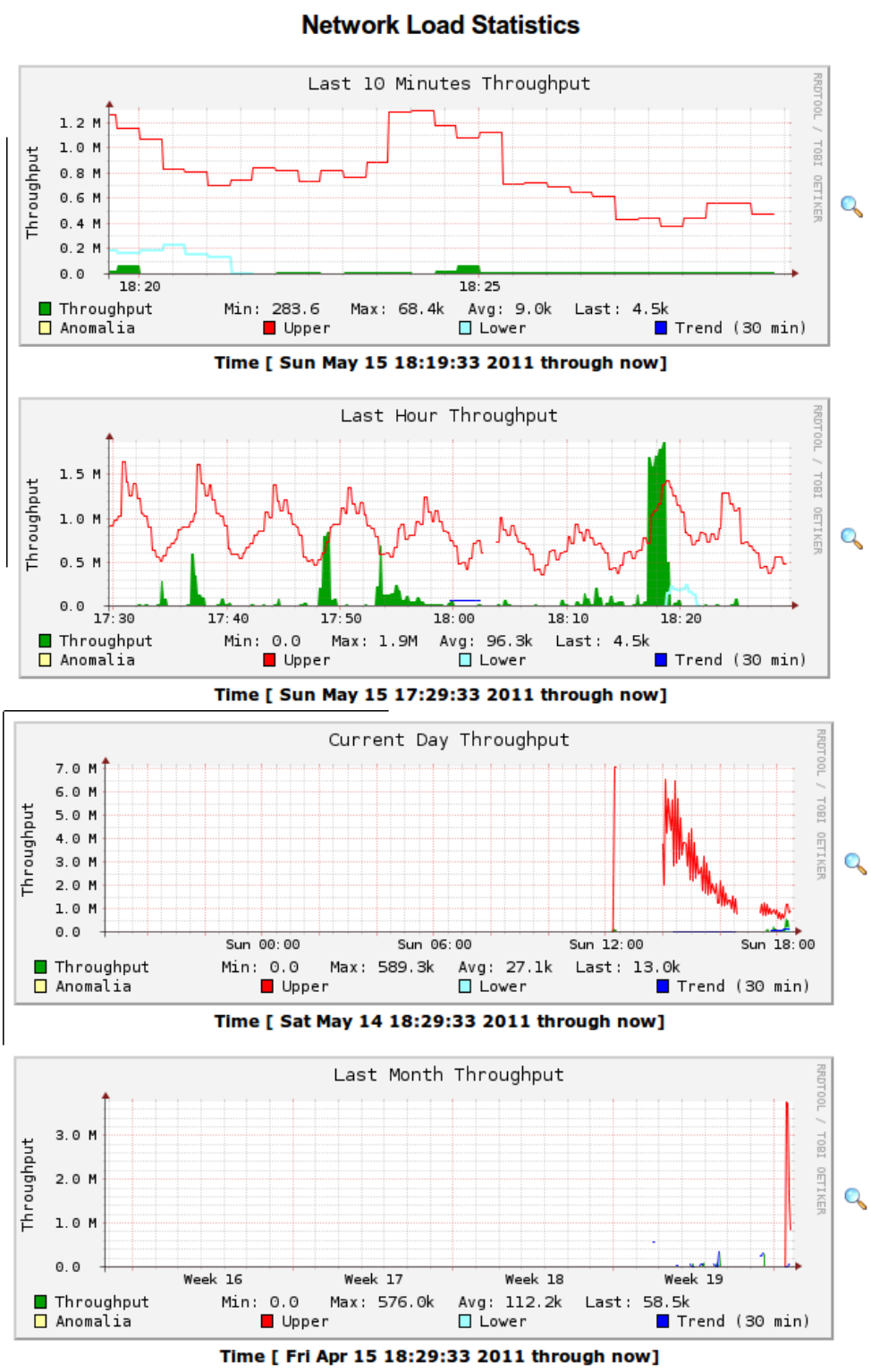


Figura 4.12 Estadísticas de red.

Dentro de la tabla de información de host encontraremos información relacionada sobre los dispositivos conectados donde se muestran las direcciones físicas y lógicas, sitios visitados, ancho de banda, información sobre el dominio, distancia de saltos, tiempo transfiriendo datos e inactividad. Algunos campos como el nombre de dispositivo y nombre del proveedor de servicios se muestran si están disponibles.

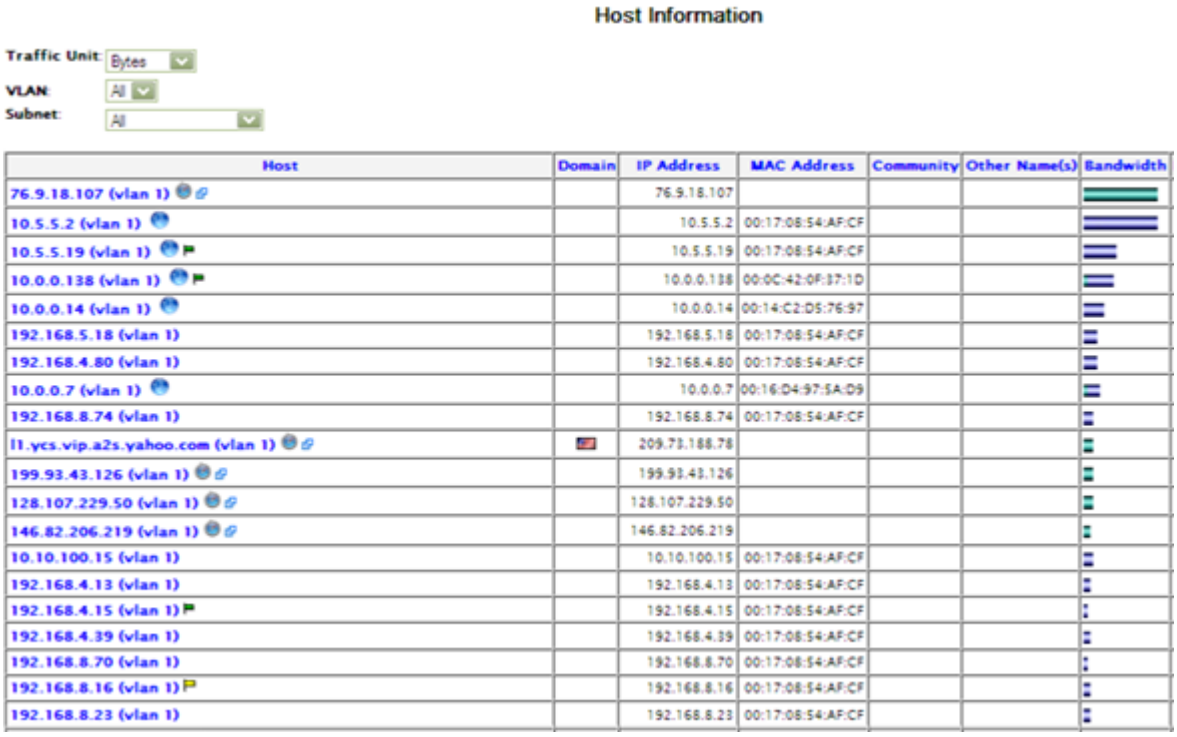


Figura 4.13 Información de Host.

4.3.2 Monitoreo de Usuarios

El consumo del ancho de banda varía dependiendo de los servicios y aplicaciones que utilizan los usuarios de una red.

Debido a la forma de trabajar de la mayoría de quienes navegan vía web, se puede deducir que el tráfico es por lo general entrante de Internet [texto, imágenes, sonido, vídeo], en respuesta a muy poco que está saliendo [como las solicitudes HTTP GET y otros comandos]. Se considera la posibilidad de que un usuario que descarga archivos de gran tamaño [películas piratas, fotos, porno, las imágenes ISO, etc.], pueden enviar una pequeña petición durante un intervalo de 20 minutos que se traduce en la transferencia de 650 MB de datos de entrada a él. Por lo tanto, el ancho de banda crítica es de gran interés aquí: el ancho de banda que cada host de la red local recibe. Para ver los consumos de ancho de banda mayor, se hace lo siguiente:

1. En el menú de opciones, seleccionar todos los protocolos.
2. En el cuadro de lista desplegable de los Ejércitos, seleccionar Sólo local.
3. En el cuadro de lista desplegable de datos, seleccionar sólo recibido.
4. Hacer clic en la VLAN que está interesado o ALL (todas) para ver el tráfico de todas las VLAN.
5. Hacer clic en el nombre de la columna de datos para ordenar los datos y el porcentaje.

Si un host de la red está enviando más tráfico de lo que está recibiendo, entonces ese host ofrece servicios de alguna clase por ejemplo un servidor web, un host P2P que comparte datos y otros los descargan de ellos, un servidor FTP, etc.

Otra forma en que se puede dar una valiosa información específica para el protocolo IP, son las Direcciones de Tráfico de IP Locales a la opción Remota del menú que tabula para cada anfitrión local, la cantidad de tráfico enviado y/o recibido de ubicaciones remotas:

Last Contacted Peers

Sent To	IP Address	Received From	IP Address
91.187.115.253 (vlan 1)	91.187.115.253	sb.google.com (vlan 1)	66.249.89.91
www.fig.net (vlan 1)	131.165.67.2	cds219.lon.llnw.net (vlan 1)	87.248.211.149
amontpellier-157-1-162-57.w90-14.abo.wanadoo.fr (vlan 1)	90.14.185.57	118.100.213.243 (vlan 1) [IP]	118.100.213.243
74.13.153.226 (vlan 1)	74.13.153.226	69.253.109.3 (vlan 1)	69.253.109.3
69.253.109.3 (vlan 1)	69.253.109.3	cellbioed.highwire.org (vlan 1)	171.66.124.194
cellbioed.highwire.org (vlan 1)	171.66.124.194	hs.imesh.com (vlan 1)	192.114.71.235
sb.google.com (vlan 1)	66.249.89.91	au.download.windowsupdate.com (vlan 1)	204.160.107.126
cds219.lon.llnw.net (vlan 1)	87.248.211.149	guru.grisoft.com (vlan 1)	193.86.3.36
Total Contacts	18621	**Total Contacts**	16507

Figura 4.14 Últimos dispositivos conectados.

Otra tabla, justo debajo de la anterior, identifica las aplicaciones del host en cuestión que se están utilizando.

TCP/UDP Service/Port Usage

IP Service	Port	≠ Client Sess.	Last Client Peer	≠ Server Sess.	Last Server Peer
telnet	23	42/7.2 KBytes	76.13.15.40 (vlan 1)		
domain	53	1138/107.2 KBytes	10.0.0.1 (vlan 1) [IP]		
www	80	26468/29.6 MBytes	sb.google.com (vlan 1)		
ntp	123	2/96	clock.via.net (vlan 1)		
netbios-ns	137	3/150	bpcrfectchoice1.com (vlan 1)		
snmp	161	8/616	172.24.194.57 (vlan 1)		
https	443	1207/785.8 KBytes	voipa.sip.yahoo.com (vlan 1)		

Figura 4.15 Aplicaciones de host.

4.3.3 Monitoreo de Tráfico de sitios Web

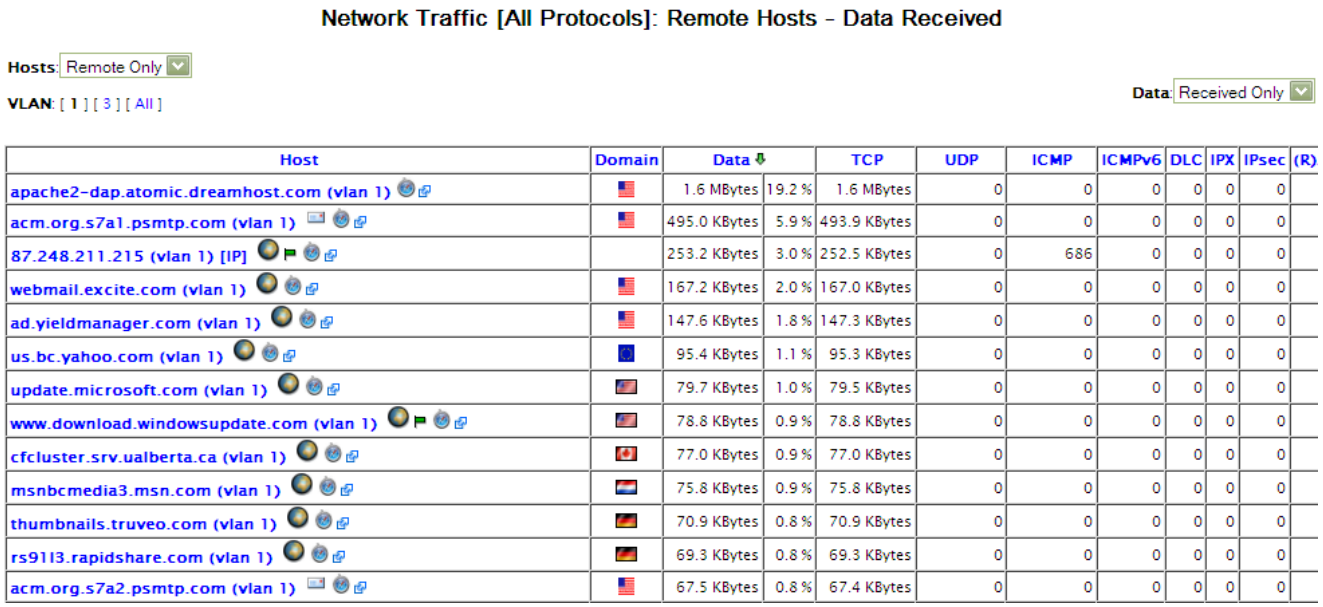
El tráfico de la red se dirige a sitios específicos y resulta importante el conocer las páginas web que más peticiones de nuestros usuarios reciben.

Siguiendo la lógica antes mencionada los sitios web más populares son los que reciben las mayores cantidades de datos de usuarios locales. Hay que tener en cuenta que un host remoto podría haber enviado una mayor cantidad de datos en la red, pero todo puede ser debido a las peticiones de un [único host por ejemplo, solicitando para el streaming de audio / vídeo]. A modo de ejemplo, suponiendo que todo el mundo entra en la oficina de registros llegan a Google para verificar el correo electrónico, la dirección IP o direcciones que alojan Gmail recibirán muchas peticiones.

Para producir una lista de sitios web se puede hacer lo siguiente.

1. En el menú de opciones seleccionar “todos los protocolos”.

2. En el cuadro de lista desplegable de Hosts, seleccionar Sólo remoto.
3. En el cuadro de lista desplegable de datos, seleccionar sólo recibido.
4. Hacer clic en la VLAN de interés o ALL (todas) para ver el tráfico de todas las VLAN.
5. Hacer clic en el nombre de la columna de datos para ordenar los datos y porcentajes.



Network Traffic [All Protocols]: Remote Hosts - Data Received

Hosts: Remote Only

VLAN: [1] [3] [All]

Data: Received Only

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)
apache2-dap.atomic.dreamhost.com (vlan 1)		1.6 MBytes	19.2 %	1.6 MBytes	0	0	0	0	0	0	
acm.org.s7a1.psmtp.com (vlan 1)		495.0 KBytes	5.9 %	493.9 KBytes	0	0	0	0	0	0	
87.248.211.215 (vlan 1) [IP]		253.2 KBytes	3.0 %	252.5 KBytes	0	686	0	0	0	0	
webmail.excite.com (vlan 1)		167.2 KBytes	2.0 %	167.0 KBytes	0	0	0	0	0	0	
ad.yieldmanager.com (vlan 1)		147.6 KBytes	1.8 %	147.3 KBytes	0	0	0	0	0	0	
us.bc.yahoo.com (vlan 1)		95.4 KBytes	1.1 %	95.3 KBytes	0	0	0	0	0	0	
update.microsoft.com (vlan 1)		79.7 KBytes	1.0 %	79.5 KBytes	0	0	0	0	0	0	
www.download.windowsupdate.com (vlan 1)		78.8 KBytes	0.9 %	78.8 KBytes	0	0	0	0	0	0	
cfcluster.srv.ualberta.ca (vlan 1)		77.0 KBytes	0.9 %	77.0 KBytes	0	0	0	0	0	0	
msnbcmedia3.msn.com (vlan 1)		75.8 KBytes	0.9 %	75.8 KBytes	0	0	0	0	0	0	
thumbnails.truveo.com (vlan 1)		70.9 KBytes	0.8 %	70.9 KBytes	0	0	0	0	0	0	
rs911l3.rapidshare.com (vlan 1)		69.3 KBytes	0.8 %	69.3 KBytes	0	0	0	0	0	0	
acm.org.s7a2.psmtp.com (vlan 1)		67.5 KBytes	0.8 %	67.4 KBytes	0	0	0	0	0	0	

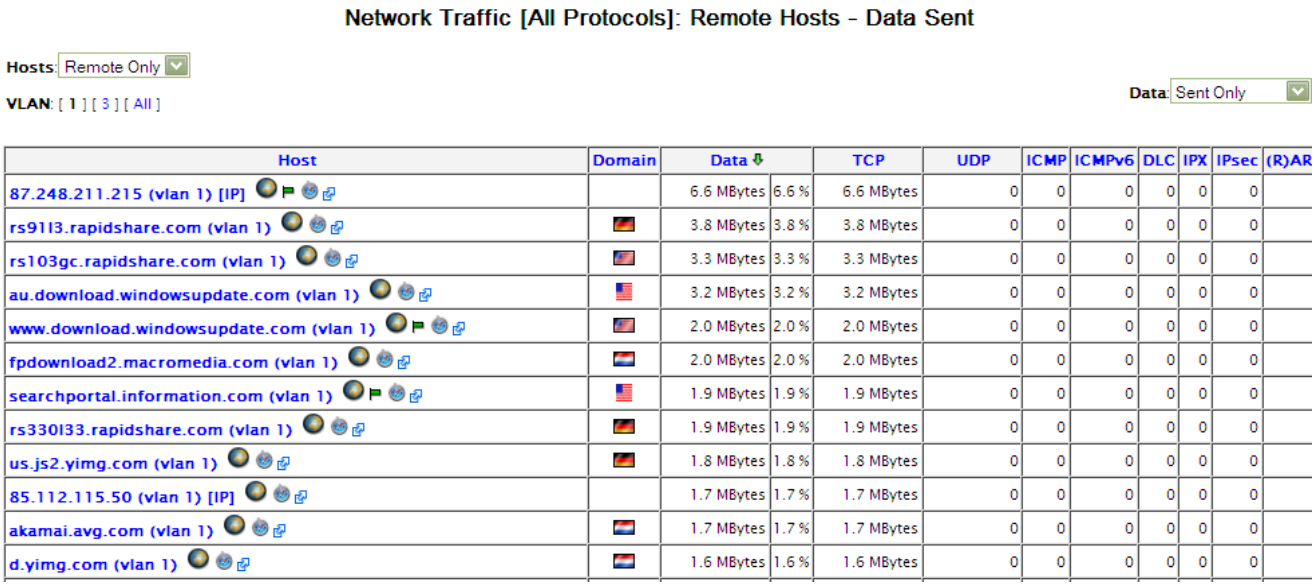
Figura 4.16 Trafico de la red (todos los protocolos).

4.3.4 Monitoreo de Sitios Web

Para dar respuesta a esta incógnita se requiere la información para la aplicación de almacenamiento en caché automático en el servidor proxy o para bloquear destinos populares que desperdician el ancho de banda como

los sitios de descarga. Lo interesante es la cantidad de datos del host remoto enviado.

1. En el menú de opciones seleccionar “todos los protocolos”.
2. En el cuadro de lista desplegable de Hosts, seleccionar Sólo remoto.
3. En el cuadro de lista desplegable de datos, seleccionar Sólo Enviado.
4. Hacer clic en la VLAN que está interesado o ALL (todos) para ver el tráfico de todas las VLAN.
5. Hacer clic en el nombre de la columna de datos para ordenar los datos y el porcentaje.



Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)AR
87.248.211.215 (vlan 1) [IP]		6.6 MBytes	6.6 %	6.6 MBytes	0	0	0	0	0	0	
rs911l3.rapidshare.com (vlan 1)		3.8 MBytes	3.8 %	3.8 MBytes	0	0	0	0	0	0	
rs103gc.rapidshare.com (vlan 1)		3.3 MBytes	3.3 %	3.3 MBytes	0	0	0	0	0	0	
au.download.windowsupdate.com (vlan 1)		3.2 MBytes	3.2 %	3.2 MBytes	0	0	0	0	0	0	
www.download.windowsupdate.com (vlan 1)		2.0 MBytes	2.0 %	2.0 MBytes	0	0	0	0	0	0	
fpdownload2.macromedia.com (vlan 1)		2.0 MBytes	2.0 %	2.0 MBytes	0	0	0	0	0	0	
searchportal.information.com (vlan 1)		1.9 MBytes	1.9 %	1.9 MBytes	0	0	0	0	0	0	
rs330l33.rapidshare.com (vlan 1)		1.9 MBytes	1.9 %	1.9 MBytes	0	0	0	0	0	0	
us.js2.yimg.com (vlan 1)		1.8 MBytes	1.8 %	1.8 MBytes	0	0	0	0	0	0	
85.112.115.50 (vlan 1) [IP]		1.7 MBytes	1.7 %	1.7 MBytes	0	0	0	0	0	0	
akamai.avg.com (vlan 1)		1.7 MBytes	1.7 %	1.7 MBytes	0	0	0	0	0	0	
d.yimg.com (vlan 1)		1.6 MBytes	1.6 %	1.6 MBytes	0	0	0	0	0	0	

Figura 4.17 Tráfico de Red: Host remoto – Datos enviados.

El tráfico de direcciones remotas IPs a locales y la clasificación por datos enviados o recibidos. En la siguiente captura de pantalla se muestra un ejemplo donde hay tres sitios con las direcciones IP: 68.178.228.187, 85.17.230.66, 76.9.18.120 y son responsables del consumo de más de 50%de ancho de banda de descarga.

Remote to Local IP Traffic

Host	IP Address	Data Sent		Data Rcvd	
ip-68-178-228-187.ip.secureserver.net (vlan 1)	68.178.228.187	78.3 MBytes	28.1 %	613.4 KBytes	5.0 %
76.9.18.120 (vlan 1)	76.9.18.120	48.8 MBytes	17.5 %	253.4 KBytes	2.1 %
w17.easy-share.com (vlan 1)	85.17.230.66	40.3 MBytes	14.4 %	196.1 KBytes	1.6 %
80.239.137.33 (vlan 1)	80.239.137.33	24.7 MBytes	8.9 %	309.4 KBytes	2.5 %
208.48.186.86 (vlan 1)	208.48.186.86	17.8 MBytes	6.4 %	145.8 KBytes	1.2 %
80.70.172.78 (vlan 1)	80.70.172.78	9.3 MBytes	3.3 %	6.1 KBytes	0.1 %
assessment-prod-nv.cisco.com (vlan 1)	128.107.229.51	8.4 MBytes	3.0 %	900.4 KBytes	7.3 %
38.96.182.20 (vlan 1)	38.96.182.20	6.0 MBytes	2.2 %	662.5 KBytes	5.4 %
cna-prod-nv.cisco.com (vlan 1)	128.107.229.50	5.4 MBytes	1.9 %	870.2 KBytes	7.1 %
64.215.158.132 (vlan 1)	64.215.158.132	4.8 MBytes	1.7 %	9.8 KBytes	0.1 %
66.90.103.49 (vlan 1)	66.90.103.49	4.0 MBytes	1.4 %	191.3 KBytes	1.6 %
205.128.73.126 (vlan 1)	205.128.73.126	2.8 MBytes	1.0 %	129.8 KBytes	1.1 %
67.199.128.41 (vlan 1)	67.199.128.41	2.2 MBytes	0.8 %	1.0 MBytes	8.5 %
xmlrpc.rhn.redhat.com (vlan 1)	209.132.177.100	1.6 MBytes	0.6 %	743.6 KBytes	6.1 %
cortona.webhosters.no (vlan 1)	63.247.138.183	1.5 MBytes	0.6 %	17.3 KBytes	0.1 %
66.48.78.209 (vlan 1)	66.48.78.209	1.4 MBytes	0.5 %	481.2 KBytes	3.9 %
67.199.128.42 (vlan 1)	67.199.128.42	1.3 MBytes	0.5 %	465.8 KBytes	3.8 %
l1.ycs.vip.a2s.yahoo.com (vlan 1)	209.73.188.78	1.3 MBytes	0.5 %	100.7 KBytes	0.8 %
87.104.113.106 (vlan 1)	87.104.113.106	1.0 MBytes	0.4 %	258.6 KBytes	2.1 %
76.9.18.128 (vlan 1)	76.9.18.128	1.0 MBytes	0.4 %	123.4 KBytes	1.0 %
unassigned-66.147.227.189.hrwebservices.net (vlan 1)	66.147.227.189	965.2 KBytes	0.3 %	84.2 KBytes	0.7 %
76.9.18.115 (vlan 1)	76.9.18.115	874.3 KBytes	0.3 %	124.1 KBytes	1.0 %
ns1.globalconnex.net (vlan 1)	80.255.35.180	788.5 KBytes	0.3 %	328.8 KBytes	2.7 %
f1.www.vip.re1.yahoo.com (vlan 1)	69.147.76.15	771.6 KBytes	0.3 %	96.8 KBytes	0.8 %
74.54.144.163 (vlan 1)	74.54.144.163	641.9 KBytes	0.2 %	76.1 KBytes	0.6 %
194.129.79.44 (vlan 1)	194.129.79.44	471.7 KBytes	0.2 %	169.5 KBytes	1.4 %
64.236.22.63 (vlan 1)	64.236.22.63	26.3 KBytes	0.0 %	12.4 KBytes	0.1 %
www4.cnn.com (vlan 1)	64.236.16.52	24.4 KBytes	0.0 %	5.8 KBytes	0.0 %
66.218.161.133 (vlan 1)	66.218.161.133	24.1 KBytes	0.0 %	7.8 KBytes	0.1 %

Figura 4.18 Tráfico IP remoto-local.

4.3.5 Monitoreo de Aplicaciones

Aplicaciones en este contexto se refiere a aplicaciones de red y es esencial que sea identificado por los puertos que cada aplicación utiliza. El DNS por ejemplo, es una aplicación cuyo componente de servidor siempre escucha en el puerto UDP 53. Aunque la mayoría de los programas peer-to-peer de forma predeterminada usa un rango específico de los puertos, también puede utilizar los puertos de otros protocolos conocido como http [80]; para Ntop depende de la información de encabezado para la detección de programas p2p.

El protocolo global de distribución TCP / UDP, puede ser accedido desde la página de resumen que muestra los gráficos de tráfico de las aplicaciones más populares que se ven desde que Ntop se inicia.

Acumula vistas históricas en la parte inferior de la página Resumen de tráfico así como un gráfico agradable de la utilización de ancho de banda por intervalo de tiempo, de cada una de las aplicaciones (protocolos).

TCP / UDP: Protocolo de uso local que se accede desde la IP Local en la opción del menú Puertos utilizados, esto mostrará una lista de las aplicaciones que son utilizadas por los host locales. Para cada solicitud, las direcciones IP o los nombres de los clientes locales se encuentran en la máquina local que está cumpliendo la solicitud.

4.3.6 Monitoreo de Datos

Esta información sólo es posible para los hosts locales que están en el mismo dominio de broadcast en una interfaz física de la máquina que contiene Ntop.

Así, sí está usando NetFlow (protocolo de red desarrollado por CISCO) en una subred que no es local a una de las interfaces del servidor Ntop, debe obtener información acerca de los pares de los host locales en el intercambio de tráfico. Para ver el tráfico local de la matriz, hacer clic en IP Local Organizador Local de la matriz. Una captura de pantalla de esta página se muestra en la figura 4.19.

IP Subnet Traffic Matrix

From \ To	10.0.0.1	10.0.0.2	10.0.0.3	10.0.0.7	10.0.0.10	10.0.0.13	10.0.0.17	10.0.0.18	10.0.0.19	10.0.0.22	10.0.0.25	ftp	nis-portal	10.0.0.29
10.0.0.1		220	219	4.1 KB	10.0 KB	130.4 KB	58.1 KB	124.9 KB	279.1 KB	1.0 MB	3.5 MB	90.9 KB	1.1 MB	3.4 MB
10.0.0.2	220													
10.0.0.3	219													
10.0.0.7	4.1 KB													
10.0.0.10	10.0 KB													
10.0.0.13	130.4 KB													
10.0.0.17	58.1 KB													
10.0.0.18	124.9 KB													
10.0.0.19	279.1 KB													
10.0.0.22	1.0 MB													
10.0.0.25	3.5 MB													
ftp	90.9 KB													
nis-portal	1.1 MB													
10.0.0.29	3.4 MB													

Figura 4.19 Matriz de tráfico de subred IP.

4.3.7 Monitoreo por Tiempo

Para resolver esta pregunta hay que ver la página de resumen de carga de red, en concreto el último gráfico del día.

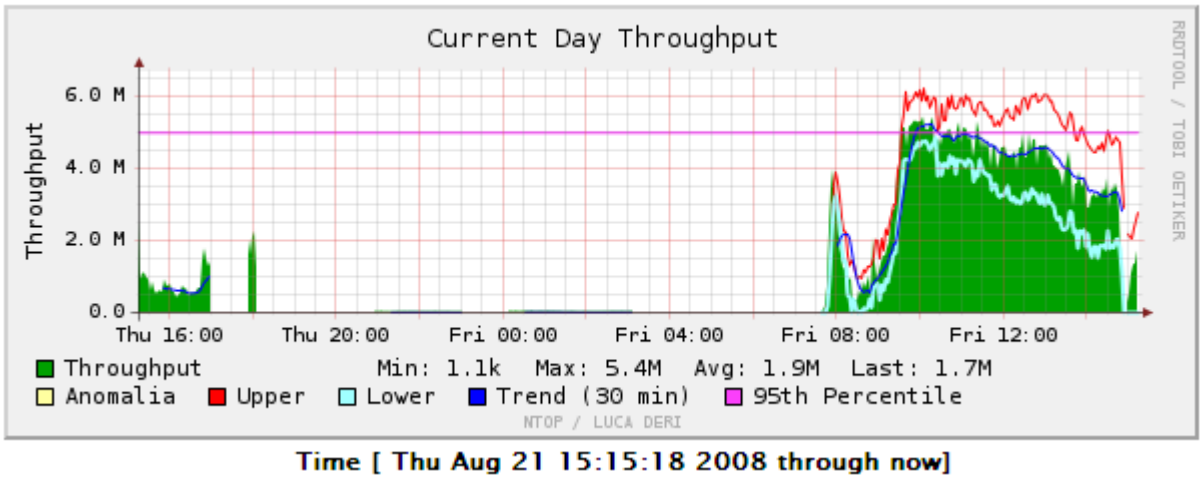


Figura 4.20 Último gráfico del día.

En la imagen del ejemplo anterior, se puede deducir que el viernes, por alguna razón falla de la red (Utilización de otros aparatos, Corte de energía, Usuarios, etc.), se comenzó a tratar de acceder a la web alrededor de las 7:45 de la mañana y el tráfico pico ocurrió alrededor de las 10 horas. También se puede deducir que hubo algún tipo de interrupción sobre 14:00. Al observar gráficos como este se puede establecer una tendencia de uso de tráfico y así ser capaz de detectar algún comportamiento anómalo.

4.3.8 Inventario de redes.

En caso de querer saber cuáles dispositivos ejecutan cuales servicios de red, cuales están en el servidor DHCP, DNS, servidores web, cuales contienen Routers, etc. La indicación para obtenerlo es ir a la página de Caracterización de Hosts Locales y acceder desde Caracterización IP Hosts Local como se muestra en la figura 4.21.

Local Hosts Characterization

Host	Unhealthy Host	L2 Switch Bridge	Gateway	VoIP Host	Printer	NTP/DNS Server	SMTP/POP/IMAP Server	Directory/FTP/HTTP Server	DHCP/WINS Server	DHCP Client	P2P
192.168.4.80 (vlan 1)	X										
10.0.0.1 (vlan 1)	X					X					
10.0.0.7 (vlan 1)						X					
10.0.0.13 (vlan 1)						X					
10.0.0.18 (vlan 1)						X					
10.0.0.19 (vlan 1)	X					X					
bigbrother (vlan 1)	X					X					
egroupware (vlan 1)	X					X					
10.0.0.29 (vlan 1)	X					X					
10.0.0.193 (vlan 1)						X					
10.0.0.194 (vlan 1)	X					X					
10.10.100.20 (vlan 1)	X										
10.10.100.14 (vlan 1)	X										
Total	9 [40.9 %]				10						

Figura 4.21 Caracterización de Host Locales.

4.3.9 Exportación de datos

Es posible que se requiera o desee exportar los datos actuales que Ntop tiene en las estructuras de memoria, para que pueda aplicar otras herramientas de análisis de la misma. Para ello, se debe hacer clic en Utilidades de datos de

descarga para que aparezca la pantalla que se muestra en la figura 4.22. Así se podrán exportar los datos de los hosts, subredes, host de matriz y por interfaz. También se pueden exportar los datos en varios formatos que se pueden seleccionar de la lista desplegable.

Report Type	Description	Action
Hosts	Dump information about known hosts	**Format:** text **Attributes List:** Long Dump Data
Hosts Matrix	Dump local hosts traffic matrix	**Format:** text **Attributes List:** Long Dump Data
Network Interfaces	Dump per-interface information	**Format:** text **Attributes List:** Long Dump Data
Network Flows	Dump traffic information of the configured network flows	**Format:** text **Attributes List:** Long Dump Data

Figura 4.22 Exportación Datos.

CAPÍTULO V. COMPARACIÓN DE HERRAMIENTAS DE MONITOREO

De acuerdo a referencias de manuales y a la implementación que se realizó se pueden determinar los siguientes parámetros con los cuales se realizará la comparación.

Configuración

El proceso para realizar la instalación de una herramienta de monitoreo puede variar de tal modo que algunas herramientas requieran que el usuario se encargue de instalar distintas aplicaciones antes de realizar la instalación de la herramienta en el servidor para que esta funcione correctamente, algunas otras incluyen la instalación y ejecución de aplicaciones de terceros en sus propios procesos de instalación, haciendo de este proceso algo oculto para el usuario final.

Interfaz / Gráficos

Una interfaz gráfica es cualquier medio por el cual uno puede interactuar con una computadora a través de algún tipo de software gráfico. Comúnmente, esto se consigue a través del control mediante el teclado y el mouse de cursores, menús, ventanas, íconos y cajas de diálogo, pero puede tomar cualquier forma imaginable.

Algunas de las funciones de las interfaces son:

- Puesta en marcha y apagado.
- Control de las funciones manipulables del equipo.
- Manipulación de archivos y directorios.
- Herramientas de desarrollo de aplicaciones.
- Comunicación con otros sistemas.
- Información de estado.
- Configuración de la propia interfaz y entorno.
- Intercambio de datos entre aplicaciones.
- Control de acceso.
- Sistema de ayuda interactivo.

Estadísticas

Representa la información que presenta la herramienta después de realizar la captura del tráfico de datos que le permiten al usuario recopilar información que le facilitará el

análisis de los eventos ocurridos en la red. Estas estadísticas suelen presentarse en forma de tablas o gráficos lo que le facilita al usuario la interpretación de la información procesada por la herramienta. Algunas herramientas permiten configurar la forma en la que se generan las estadísticas para obtener datos específicos.

Rendimiento

Se refiere a la cantidad de recursos del servidor que utiliza la herramienta de monitoreo mientras se ejecuta para realizar la captura de tráfico de red.

Autodescubrimiento

El software permite descubrir todos los equipos o estaciones conectadas a la red local, adquieren los nombres y las direcciones de los equipos. Estos equipos se representan en forma de tabla o lista. Normalmente se permite añadir a esta lista equipos, borrar equipos de la misma y realizar consultas SNMP de las mismas a las variables MIB.

Agentes

Algunas aplicaciones basadas en SNMP requieren de la instalación de un agente propio de la herramienta en los clientes que se encuentran conectados en la red para recopilar información mediante mensajes enviados hacia el agente del cliente el cual regresa información que la herramienta es capaz de interpretar y presentar al usuario.

SNMP

Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver los problemas así como planear el crecimiento mediante el envío y recepción de peticiones y respuestas entre los administradores y los agentes.

Syslog

Es un estándar de facto para el envío de mensajes de registro en una red informática IP. Mediante syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro el cual suele tener información sobre los eventos del sistema. Junto con cada mensaje se incluye la fecha y hora del envío el cual genera un historial de eventos.

Scripts Externos

Las herramientas de monitoreo cuentan con sus propias plantillas (predefinidas) para realizar el análisis del tráfico de red y puede darse el caso de que en algunas ocasiones estas plantillas no cuenten con los recursos necesarios para monitorear un servicio determinado. Es posible incorporar scripts implementados por otras personas o desarrollados por el mismo usuario.

Componentes (Plugins)

Permite la incorporación de complementos de otras herramientas para añadir una característica o servicio para mejorar el desempeño de las herramientas de monitoreo.

Creación de complementos

Permite que el usuario genere sus propios complementos para adicionar características al software de monitoreo ya sea para mejorar su funcionamiento, para que el software actúe de forma personalizada por el usuario o para extender las capacidades del producto.

Alertas

Las alertas son reglas para detectar si el estado del sistema cumple con las especificaciones del usuario.

Aplicación web

La herramienta de monitoreo le permite al usuario acceder a la aplicación ya sea mediante la conexión a un servidor web a través de internet o de una intranet mediante un navegador el cual se puede usar para ver las gráficas, el estado del sistema y, eventualmente, editar parámetros como los equipos monitorizados, las alertas, las reglas, etc.

Monitorización distribuida

Capacidad de realizar análisis de tráfico de red ya sea en distintos segmentos de la red, distintos dominios o conjunto de equipos integrando la información capturada por los administradores distribuidos en un servidor de monitoreo central.

Método de almacenaje de datos

Se refiere a la forma en la que se almacenan los datos obtenidos en las capturas, normalmente se hace uso de bases de datos como SQL, MySQL y Oracle. Algunas otras aplicaciones almacenan la información en texto plano.

Licencia

Las licencias de software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, modificar el software y distribuirlo modificado. Suele estar disponible gratuitamente o al precio de costo de la distribución a través de otros medios.

Mapas

La representación gráfica de los componentes monitorizados le muestra al usuario la información recopilada después de que la herramienta realiza y ejecuta el autodescubrimiento de la red con lo que se obtiene un mapa de la topología que se está analizando y la interacción entre equipos por medio de los paquetes enviados y recibidos.

Seguridad

La seguridad es la capacidad para monitorizar de forma segura a través de varios niveles basados en una contraseña u otro dispositivo de seguridad. Note que aunque la aplicación no soporte ninguna seguridad, el servidor Apache aún puede bloquear páginas específicas.

Eventos

Los eventos son la capacidad de notificar y guardar acciones.

Sistemas Operativos

Identifica los sistemas operativos que soportan la instalación y ejecución de las aplicaciones de monitoreo.

Tabla comparativa

De acuerdo a las pruebas realizadas se muestran los resultados obtenidos para la evaluación de cada uno de los parámetros estudiados.

Tabla 5.1 Comparación de Herramientas de monitoreo.

Herramienta / Característica	Wireshark	Tcpdump	Ntop
Configuración	Media, Se apoya en la librería de captura pcap, pero brinda diversas opciones para captura desde la ventana de captura.	Compleja, Se realiza a través del comando tcpdump y distintos argumentos apoyándose en la librería de captura pcap, se requiere de amplia experiencia en manejo de expresiones regulares e interpretación.	Sencilla, Se requiere conocer la paquetería extra a instalar para evitar errores de visualización. Hace uso de la librería pcap.
Interfaz / Gráficos	✓ Ventana con 3 paneles.	✗ Texto Plano.	✓ Diversas interfaces.
Estadísticas	✓ Se obtienen a través del menú Statistics.	Solamente se muestra el total de paquetes capturados,	✓ Muestra tráfico unicast, o multicast, la longitud de los

		recibidos por el filtro y omitidos por el kernel.	paquetes, TTL y tipo de tráfico.
Eventos	✓ Permite habilitar la detección de eventos TCP.	✗ No permite almacenar eventos.	✓ Guarda información en SQL y RDD de estadísticas de tráfico.
Autoconfiguración	Solo mediante la ejecución de scripts.	✗	✓ Obtiene información del mapa de red.
Rendimiento	Al realizar la captura de tráfico utiliza aproximadamente 40 MB de memoria entre sus procesos.	El consumo de memoria se aproxima a 9 MB al realizar la captura.	Oscila entre unos pocos MB (20-30MB) en una LAN, a 100 MB para una WAN. Consume alta cantidad de recursos en escaneo constante.
Agentes	✗	✗	✗
SNMP	✓	✗	✓
Syslog	✓	✓	✓
Scripts Externos	✓	✗	✓
Complementos (Plugins)	✓ Puede incorporar Tcpdump para realizar capturas directamente al disco para análisis posterior.	✓ Incorpora otras herramientas para complementar el análisis de tráfico de tcpdump, por ejemplo se puede abrir la captura pcap tomada en tcpdump en wireshark.	✓ Incorpora información de tráfico de IP (IP Traffic), brinda opciones de Administración y muestran protocolos que no se encuentran en la versión estándar.
Creación de complementos	✓ Permite obtener el código para realizar parches.	✗	✓ Ntop permite registrar modificaciones permitiendo compilarlas en nuevas versiones.

Alertas	✗	✗	✓
Aplicación WEB	✗	✗	✓
Monitorización distribuida	Requiere de aplicaciones distintas para accesar mediante un intérprete de línea de comandos.	✗	✓
Almacenamiento de datos	Utiliza el repositorio de la librería Pcap para el almacenamiento de los datos.	Utiliza el repositorio de la librería Pcap para el almacenamiento de los datos.	SQL.
Licencia	Gratuita.	Gratuita.	Gratuita, licencia GPLv3 (derecho a versiones y correcciones gratuitas).
Mapas	Permite generar mapas que muestren la ubicación geográfica mediante el uso de GeoIP.	✗	✓
Seguridad	✓	✓	✓
Sistemas Operativos	Windows y Unix.	Unix, existe una adaptación para Windows (WinDump).	Windows y Unix.

CONCLUSIONES

Con base en la implementación de las herramientas de monitoreo de redes LAN, que se realizó en un ambiente laboral real y el análisis posterior a los resultados arrojados, se puede decir que en la actualidad las herramientas de software libre han venido produciendo cambios muy fuertes en las empresas, dejando impactos económicos y operativos en las organizaciones que se han animado a utilizarlas.

El área de informática así como el de seguridad de la información, empiezan a ser parte estratégica de cualquier organización; quién no cuenta con ellas sencillamente va un paso atrás de las demás. Invertir en su seguridad y específicamente en el monitoreo de datos dentro de la red, la cual maneja información crucial y confidencial, es un punto que no puede dejarse de lado.

Las herramientas analizadas en el presente trabajo nos brindan diversas opciones de monitoreo y definen sus ventajas y desventajas a partir del entorno o ambiente en el cual se aplican. Wireshark es la más conocida de las herramientas analizadas, representa una muy buena aplicación si el conocimiento sobre análisis de tráfico es limitado. Suele utilizarse como herramienta de aprendizaje en universidades y brinda numerosas funcionalidades aunado a una interfaz muy amigable que permite realizar configuraciones para obtener capturas que se adaptan a los requerimientos de los administradores de red.

Al ser Wireshark la herramienta más utilizada por su sencillez para efectuar análisis de tráfico de red, las mejoras e integraciones de nuevas funcionalidades se realizan frecuentemente. Gran cantidad de manuales permiten al usuario documentarse y dominar la herramienta lo que posteriormente facilitará hacer uso de distintas herramientas que cuentan con funcionalidades que Wireshark no tiene.

Respecto a Tcpdump, concluimos que para nuestro ambiente es la herramienta más limitada puesto que requiere de conocimiento avanzado sobre el manejo de la línea de comandos y especialmente de expresiones regulares para obtener información que le sea relevante al administrador.

Fuera de este entorno Tcpdump es una muy poderosa herramienta especialmente en redes amplias donde la cantidad de usuarios sea elevada y los anchos de banda sean del orden de los gigabytes. Realizar una captura con Wireshark o Ntop para estos anchos de banda y cantidades de tráfico elevadas puede resultar en problemas de memoria e incluso podría no realizar el almacenamiento de las capturas al superar el tamaño del archivo de captura el espacio disponible en disco duro.

Ntop es una herramienta imprescindible para la administración de una red LAN, si lo que se busca es un impacto positivo en la optimización, respecto a usuarios finales, rendimiento y porque no impactos económicos a nivel organizacional.

Puede proveer de información muy valiosa dedicando el tiempo necesario para el correcto análisis y esto conllevaría a cualquier organización que mediante métodos

de seguridad establecidos, optimicen de forma considerable la actual red de cualquier organización y por consiguiente sus procesos.

Contar con la herramienta no lo es todo, Ntop es una herramienta poderosa respecto a información que arroja, por lo que sabiendo cómo interpretarla y mediante un buen análisis, se pueden lograr muchas mejoras en una red LAN.

Se considera que se puede sacar el mayor provecho en aquellas redes LAN de organizaciones pequeñas con personal no mayor de 200 personas, aunque la interfaz gráfica siempre ayudara a la interpretación de datos. Ntop es una herramienta muy noble que se puede adaptar a una LAN de forma exitosa, pese a la topología que esta utilice.

En general las tres herramientas de monitoreo son buenas y la eficiencia de estas dependerá también de los conocimientos que el administrador de red tenga acerca de su funcionamiento y la habilidad de interpretar los datos mostrados.

ANEXOS

1.- Instalación de Wireshark

El instalador y los archivos binarios de Wireshark pueden ser descargados en http://www.Wireshark.org/download.html. Adicional a esto en http://wiki.Wireshark.org podrás obtener una amplia cantidad de información relacionada con la aplicación, listas de correo tanto para usuarios finales como desarrolladores.

Wireshark soporta múltiples plataforma entre ellas UNIX, LINUX y Windows, a continuación se describe la instalación para cada uno de estos sistemas operativos.

Instalación LINUX

Para iniciar la instalación se debe contar con las siguientes utilidades instaladas:

- GTK+, GIMP Tool Kit y Glib (puede obtener en el siguiente site: www.gtk.org)
- libpcap (puede obtener en el siguiente site: www.tcpdump.org)

La instalación en Ubuntu se realiza mediante el comando.

```
$ sudo apt-getinstallWireshark
```

Si es el caso de obtener los archivos fuentes los siguientes pasos describen el proceso para descomprimir los archivos y generar el ejecutable:

1. Según la distribución de LINUX, se aplica el comando correspondiente para descomprimir el archivo obtenido.

    - En versiones de LINUX con GNU tar.

```
$ tar zxvf Wireshark-1.0.0-tar.gz
```

    - En caso contrario se deberá ejecutar los siguientes comandos.

```
$ tar xvf Wireshark-1.0.0-tar

$ gzip –d Wireshark-1.0.0-tar.gz
```

2. Configuración de los archivos fuentes con el objetivo de asegurar el buen funcionamiento en la versión de LINUX correspondiente.

```
$ ./configure
```

3. Para generar el archivo ejecutable se debe aplicar el siguiente comando.

```
$ make
```

4. Finalmente para culminar la instalación de la aplicación se ejecuta el comando.

```
$ makeinstall
```

Otros métodos son aplicados para la instalación según las distribuciones de LINUX todos estos disponibles en la siguiente URL.

http://www.Wireshark.org/docs/wsug_html_chunked/ChBuildInstallUnixInstallBins.html particularmente para el caso de DEBIAN se aplica el siguiente comando para hacer uso de la interfaz gráfica para APT:

```
$ aptitudeinstallWireshark
```

2.- Instalación de Tcpdump y libpcap

En sistemas basados en Debian, se hará mediante este llamada a los repositorios (instalará libpcap y Tcpdump).

```
$ sudo apt-get install Tcpdump libpcap0.8
```

Se puede también instalarlo bajando y compilando el código fuente de libpcap y Tcpdump.

http://projects/libpcap/

http://sourceforge.net/projects/Tcpdump/

Se inicia con libpcap. Se descomprime la carpeta.

```
$ tarzxvf libpcap-0.8.1.tar.gz
```

Se ingresa en el directorio.

```
$ cd libpcap-0.8.1
```

Se crea el makefile adecuado al sistema operativo y se instala.

```
$ ./configure
$  make
$  sudo makeinstall
```

Ahora el Tcpdump. Se descomprime con.

```
$ tarzxvf Tcpdump-3.8.1.tar.gz
```

Se accede en el directorio y se realiza el mismo proceso que para el lipbcap.

```
$ cd Tcpdump-3.8.1
$ ./configure
$ make
$ sudo make install
```

3.- Instalación de Ntop

Antes de instalar Ntop, se deberá tener instalado: la base de datos mysql así como el servidor de http (para poder ver la aplicación).

Para ello, en la maquina a instalar se escribirá el siguiente comando.

```
$ sudo apt-get install apache2
```

Y para MySQL.

```
$ sudo apt-getinstallmysql
```

Pedirá nombre de usuario y contraseña, la cual se deberá recordar para acceder a la base de datos, si es que se realiza; mientras que MySQL preguntará que servidor utilizar, se le indicará que Apache2.

Una vez completado esto, se procede a la instalación de NTOP.

Para contar en el equipo con esta aplicación se debe instalar el paquete NTOP, mediante el comando.

```
$ sudo apt-getinstallNtop
```

Una vez instalado y antes de iniciar el servicio, de debe establecer la contraseña del usuario administrador.

```
$ sudo Ntop --set-admin-password
```

Por defecto se recopilará información del interfaz de red eth0, de modo que si se requiere usar otra interfaz se deberá cambiar dicha configuración en el fichero '/var/lib/Ntop/init.cfg' mediante el siguiente comando.

```
$ sudo gedit /var/lib/Ntop/init.cfg
```

Es necesario iniciar todos los servicios, los cual se logran con los siguientes comandos.

```
$ sudo /etc/init.d/apache2 start
$ sudo /etc/init.d/mysql start
$ sudo /etc/init.d/Ntop start
```

Para poder crear el mapa gráfico, Ntop se apoya en la herramienta 'dot', la cual se encuentra en el paquete graphviz y la se puede descargar con el siguiente comando.

```
$ sudo apt-getinstallgraphviz
```

Puede que se presente el siguiente error al intentar crear el mapa de tráfico local de la red.

```
Error: fontconfig: Didn't find expected font family. Perhaps
URW Type 1 fonts need installing? : Helvetica
```

Este error se soluciona instalando el paquete gsfonts-x11.

```
$ sudo apt-get install gsfonts-x11
```

Finalmente es necesario reiniciar el servicio, lo cual se logra con el siguiente comando.

```
$ sudo /etc/init.d/Ntoprestart
```

Para acceder a las estadísticas de red se tiene que navegar en la dirección.

http://localhost:3000