UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos

TÉLÉMATIQUE

VULNERABILIDAD DEL PROTOCOLO MYSQL EN REDES LAN BAJO PLATAFORMA LINUX

César Augusto Sánchez Pacheco[1]
Universidad Del Zulia. Maracaibo – Venezuela

José R.Fermin[2]
Universidad Del Zulia. Maracaibo – Venezuela

RECIBIDO: diciembre 2008 APROBADO: marzo 2009

RESUMEN

El propósito de la presente investigación es estudiar el nivel de vulnerabilidad del protocolo MySQL en una red LAN bajo plataforma LINUX. Para esto se utilizó la técnica de medición de tráfico mediante un software analizador de redes denominado Wireshark en su versión 1.0.3. El estudio se realizó interconectando un computador de medición en modo promiscuo a un puerto del enrutador, a su vez colocado en modo troncal hacia el servidor Mysql. La data obtenida se observa con claridad que la información de las solicitudes hacia las tablas de la base de datos no tiene ningún tipo de encriptación y se pueden utilizar para ingresar hacia la base de datos y obtener información sin permiso del administrador de la base de datos. El monitoreo del tráfico de datos se realizó durante 15 días continuos en una red LAN de uso administrativo. Este reporte está orientado a adoptar medidas que ayuden a minimizar la vulnerabilidad del protocolo Mysql.

Palabras clave: Seguridad de datos, Tráfico de datos, Mysql

ABSTRACT

The purpose of this investigation is study the level of vulnerability of the MySQL protocol in a local area network under LINUX platform. For this, the technique of traffic monitoring is used, with the help of a commercial tool called Wireshark network analyzer 1.0.3. The study was performed connecting interconnecting a single computer and router in promiscuous mode, which is, at the same time, connected in troncal mode to the MySQL server. From the data it is clearly observed that the information of the requests from the data base is not encrypted, and it can be used to enter into the system without permission. The traffic measurement was performed continuously during 15 days in a LAN for administrative purposes. This report is oriented to adopt strategies for enhancing the network security.

Key words: Data security, traffic measurment, Mysql protocol

[1] **Magister en Telemática. Universidad Del Zulia, Centro de Computación, Maracaibo – Venezuela.**

[2] **Doctor en Física. Universidad del Zulia, Maracaibo, Dpto. de Física, Facultad de Ciencias Maracaibo – Venezuela.**

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

INTRODUCCIÓN

Con el avance de las tecnologías, aplicaciones y tendencias en las comunicaciones, así como el crecimiento y expansión de los entornos de red, se hace evidente la necesidad de contar con mecanismos que permitan al administrador(a) de red, medir y registrar la actividad de los recursos de su red, así como también es indispensable que el administrador(a) de base de datos conozca las debilidades que tiene el manejador de base de datos con respecto a la seguridad.

El manejador de base de datos bajo software libre más utilizado es el denominado MySQL el cual por sus características antes descritas, es utilizado junto con el lenguaje de desarrollo web denominado PHP, esas dos herramientas se llevan la preferencia de uso tanto para los expertos como para los principiantes en el desarrollo de software.

El protocolo MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones a nivel mundial, su fundación data del año 1995 en Suecia por David Axmark, Allan Larrson y Michael Widenius. El objetivo es que MySQL cumpla con las especificaciones o estándares SQL, sin sacrificar velocidad, fiabilidad o usabilidad.

Con respecto a la seguridad sólo se tiene información oficial de cómo modificar el archivo de configuración para bloquear usuarios creados por defecto así como también piden encarecidamente que cambien la contraseña del usuario “root” al momento de instalar MySQL.

En esta investigación se pretende determinar el nivel de vulnerabilidad del protocolo MySQL cuando en una aplicación un usuario intenta autenticar hacia una tabla dentro de una base de datos bajo MySQL, dicha tabla debe contener la información del usuario como el nombre de usuario y la contraseña así como otros parámetros de ingreso especificados por el desarrollador. Para esto se realizó el monitoreo de tráfico de datos de una red local administrativo, utilizando una herramienta comercial conocida como WireShark 1.0.3.

METODOLOGIA

El estudio se realizó en una red local del tipo esquematizado en la Fig. 1.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

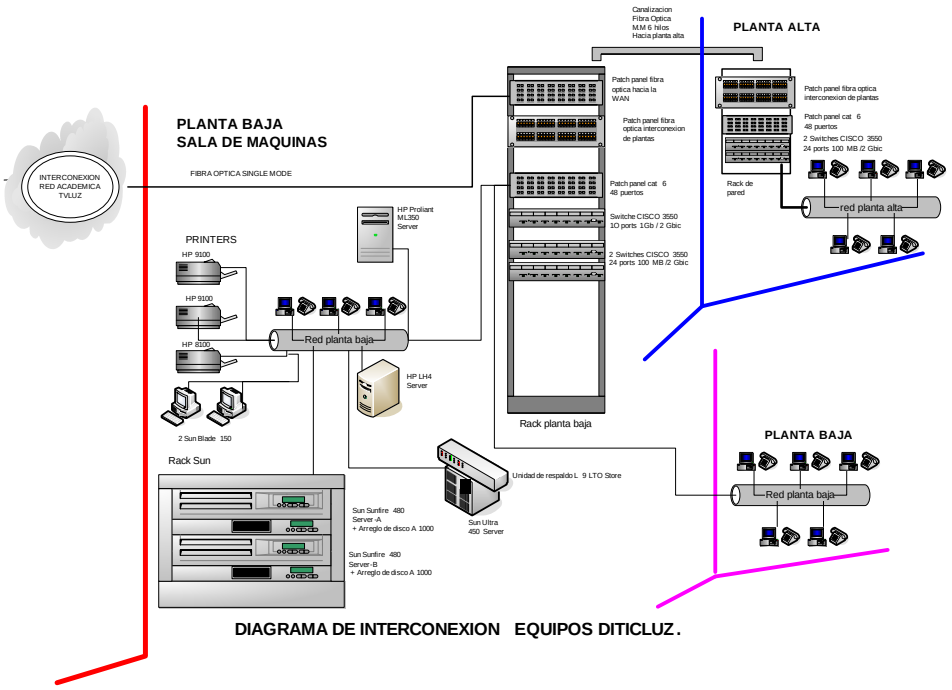

Figura 1. Red local administrativa utilizada en este estudio

Para las captura del tráfico se utilizó la herramienta comercial de uso abierto conocida como WireShark Network Analyzer 1.0.3, instalado en un computador dedicado y conectado a un puerto del router en modo promiscuo, y éste último en modo troncal hacia el servidor MySQL. Cabe mencionar que se experimentó conectando el equipo de captura de datos a un conmutador utilizado de puente entre los clientes y servidores, obteniéndose resultados similares. La captura se realizó durante 15 días continuos.

La configuración en modo promiscuo se realiza en la tarjeta de red del equipo donde está instalado el Wireshark, y es fundamental al igual que el puerto colocado en modo troncal, debido a que ese tipo de configuración permite escuchar toda la información que pasa por todo el conmutador.

RESULTADOS Y ANÁLISIS

En la Figura 2 se muestra la pantalla principal de la herramienta Wireshark. Luego de capturada la información, esta es filtrada para detectar únicamente el protocolo MySQL. Se muestra todo el flujo de tráfico así como la dirección IP de origen y destino, el protocolo utilizado y una descripción de la data que circula por el canal. En la parte inferior se puede apreciar lo que se denomina cadena de información. Aquí se puede observar que el último valor para el protocolo MySQL, específicamente en la petición de la consulta, aparece sin ningún tipo de encriptación.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

Con respecto al protocolo MySQL, el tráfico generado en un día típico consiste de 32 conversaciones enviadas, con un promedio de 149 paquetes para un total fue 2,61 Mbytes. Esta información es fundamental para la seguridad de cualquier manejador de base de datos, lo cual no es conveniente que sea fácilmente capturado

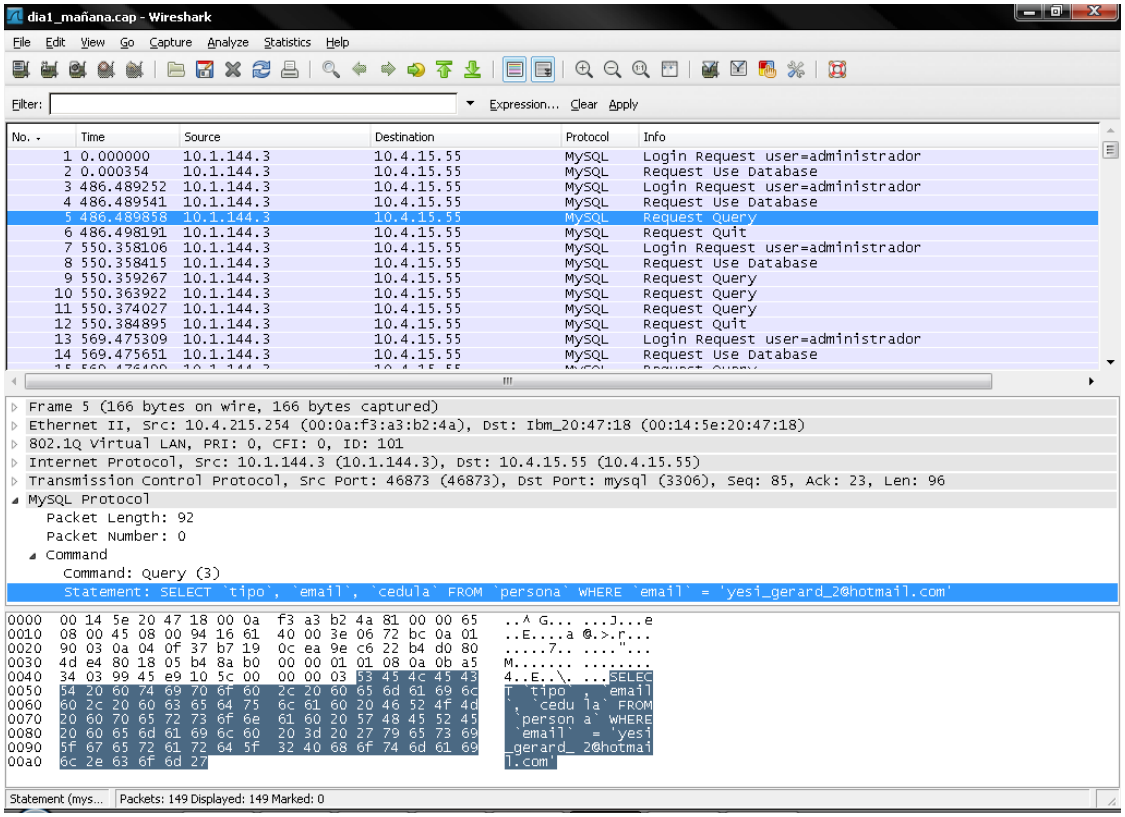

Figura 2. Pantalla principal de Wireshark.

En la Figura 3 se muestra el tráfico para el protocolo MySQL en una sección de un día típico. El flujo de información es uniforme debido a que toda solicitud que se realiza al servidor, siempre debe generar la misma cantidad de tráfico es decir, cuando un equipo cliente solicita cualquier dato al servidor MySQL, este debe tener un canal de permisología para el usuario general, luego ejecuta otra conversación verificando el permiso hacia la base de datos, y seguidamente realiza la consulta para cerrar la comunicación.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

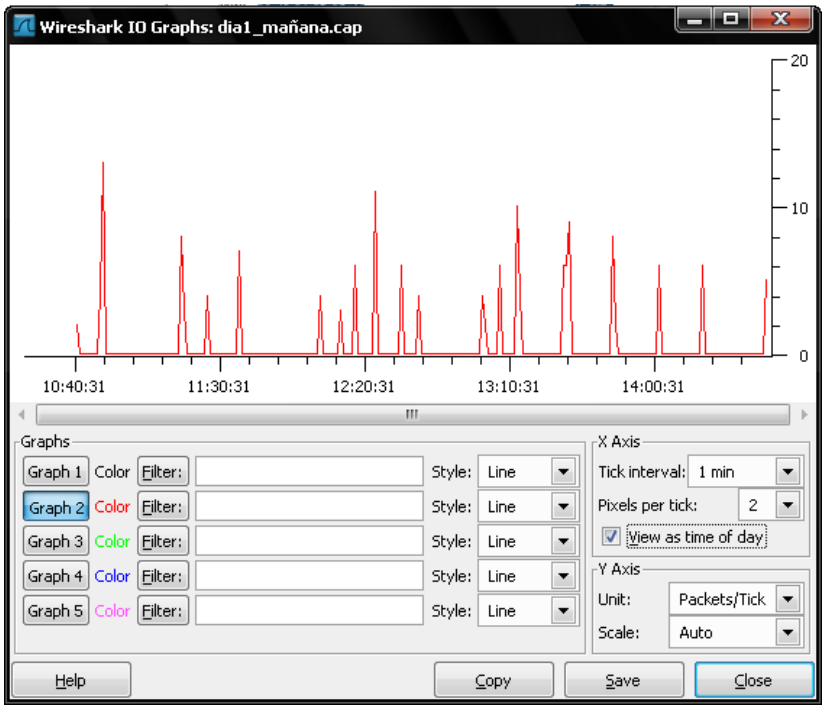

Figura 3. Flujo de datos para el protocolo MySQL, en un día típico.

En la Figura 4 se puede apreciar que la conversación entre el cliente y el servidor utilizando un usuario Administrador, tiene la permisología para ejecutar cualquier consulta dentro del servidor de base de datos. Además en la información de la trama se puede observar el campo denominado “password” el cual muestra la contraseña del usuario. A pesar de estar encriptada la contraseña, este campo es claramente detectado, permitiendo violaciones a la base de datos una vez el “administrador intruso” decodifique el algoritmo. Debido a que el protocolo MySQL es el manejador de datos mas utilizado a nivel mundial, estos resultados son de gran importancia para los administradores de redes locales bajo LINUX.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

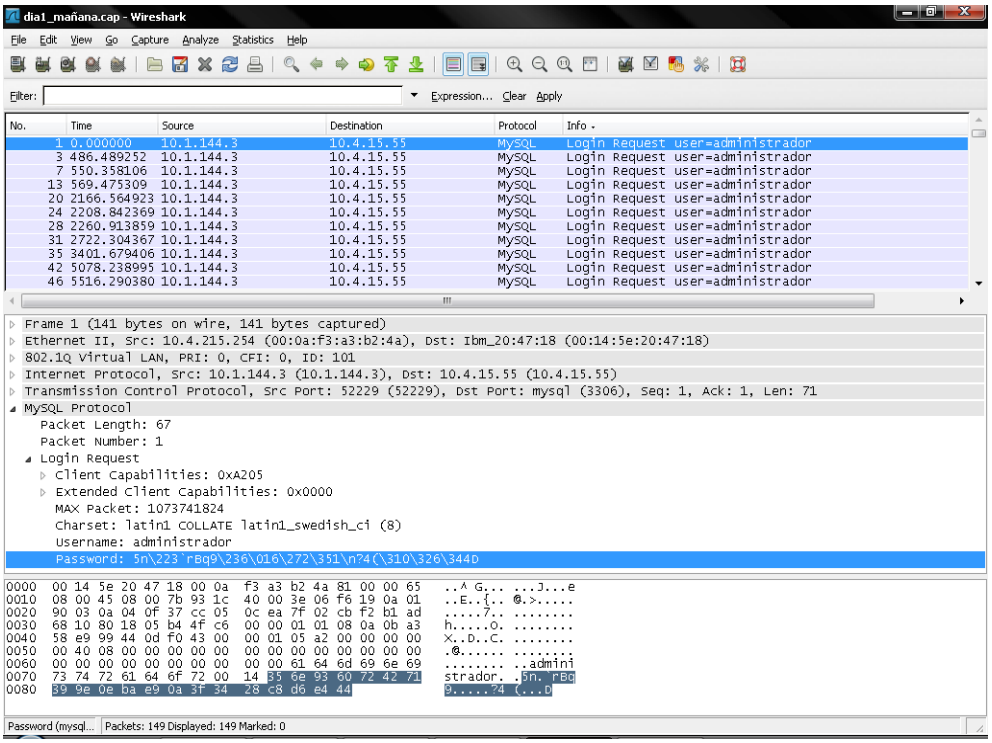

Figura 4. Captura de usuario que administra el MySQL.

En la Figura 5 se muestra otro ejemplo de cómo hacer un seguimiento del flujo de información. Podemos ver en la trama el campo “statement” o sentencia en español, el cual como su nombre lo indica, presenta la sentencia SQL ó consulta hacia la base de datos MySQL, pudiéndose extraer la definición de las tablas que comprenden la consulta. Si por ejemplo, se hace una consulta hacia una tabla de usuario solicitando la información de ingreso, pudiéramos ver con facilidad el usuario y contraseña requeridos para el ingreso hacia el sistema al cual se le solicita la consulta.

Una vez instalada la base de datos MySQL, y establecida la contraseña del usuario “root”, de forma predeterminada MySQL tiene dos usuarios definidos y una base de datos 'test'. Los usuarios no tienen predefinida ninguna contraseña y las tablas de la base de datos, que comienzan por 'test', tienen permisos de escritura para todo el mundo. Para deshabilitar estos usuarios y eliminar las tablas mencionadas se recomienda escribir: DELETE FROM user WHERE User = ''; DELETE FROM db WHERE Host = '%'.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

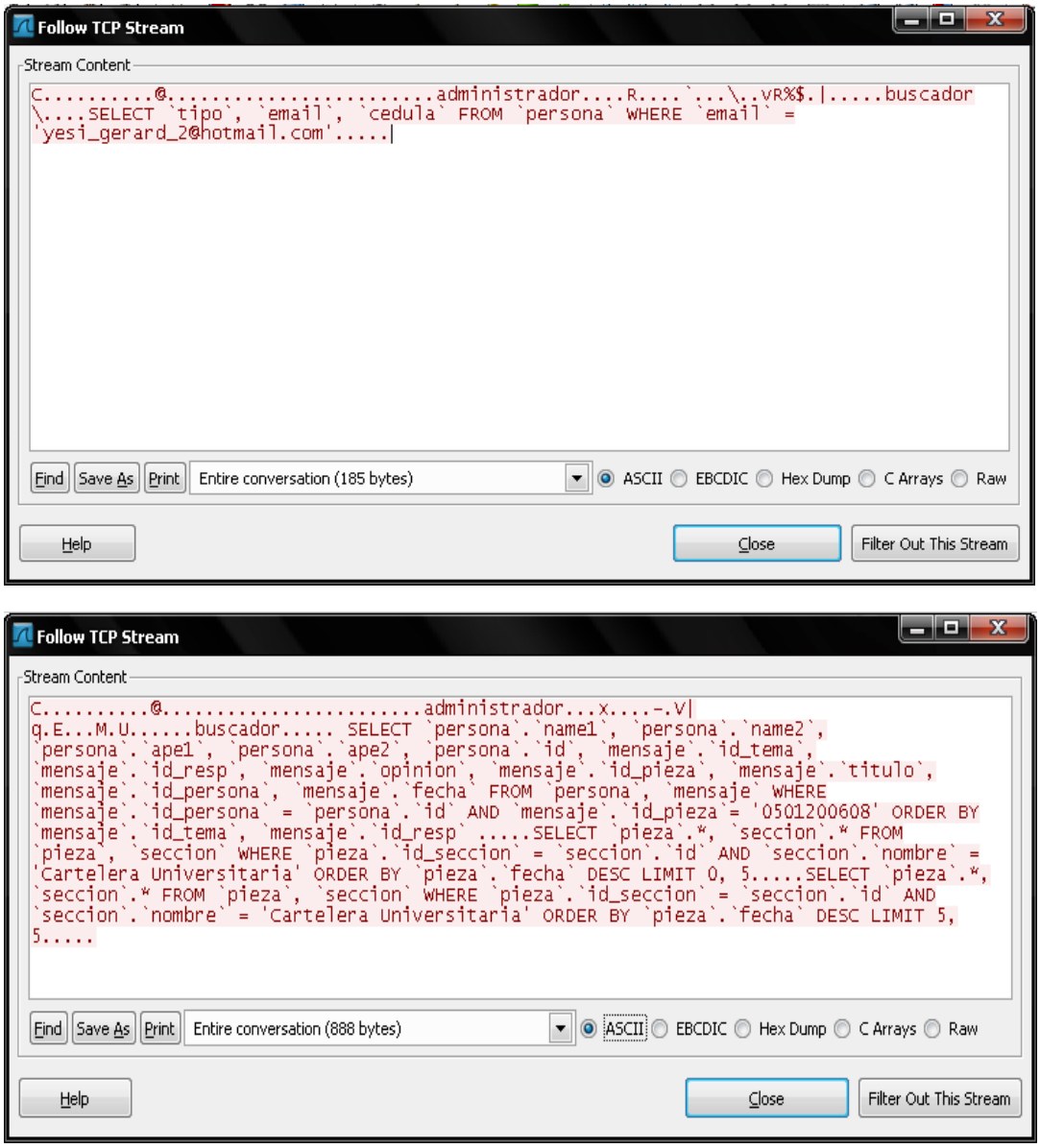

Figura 5. Conversaciones del tipo consulta hacia un servidor MySQL.

Por otro lado, para prevenir la sobre-escritura de archivos del sistema mediante una escalada de privilegios, se recomienda iniciar MySQL con el parámetro “--skip-symlink”. Para prevenir un ataque por 'denegación de servicio' se debería restringir las conexiones a un único usuario, estableciendo la variable “max_user_connections”. Pueden comprobarse los valores actuales de las variables con el comando “SHOW VARIABLES”, y pueden establecerse mediante el comando “SET”.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

Los accesos no autorizados en modo lectura a los ficheros locales, se puede prevenir deshabilitando el comando LOAD DATA LOCAL INFILE. Para ello se debe agregar el siguiente parámetro al fichero de configuración de MySQL: “my.cnf”: set-variable-local-infile=0.

A pesar de existir estas opciones, solo nos permiten proteger el servidor MySLQ mas no proteger la base de datos de las consultas.

CONCLUSIONES

El análisis de tráfico de datos es utilizado por los administradores de redes para diagnosticar un problema específico en un momento dado por medio de parámetros que le permiten llegar a conclusiones rápidamente. En el caso de esta investigación, se utilizó el monitoreo de tráfico de datos para determinar la vulnerabilidad de un protocolo específico, como lo es el del protocolo MySQL, el cual contiene información no encriptada para usuarios que puedan estar utilizando herramientas de monitoreo de redes como Wireshark. Esta herramienta es de uso libre y por ende instalable fácilmente en cualquier equipo.

En relación a la vulnerabilidad del protocolo Mysql se encontró que es vulnerable ante las consultas a la base de datos, tales como por ejemplo, información acerca del usuario administrador y su contraseña.

Las consultas realizadas al servidor deben estar encriptadas para así evitar que cualquier “administrador intruso” tenga acceso directo a la información. Este es un punto débil de los ambientes LINUX con relación aunque al nivel de seguridad del protocolo MySQL. Pueden establecerse algunas estrategias para disminuir probabilidad de intrusiones al servidor, mas una vez dentro del sistema, la base de datos queda vulnerable.

REFERENCIAS

Aguilar Sindes, Luis. **Midiendo redes.** Guía sobre el análisis de tráfico de datos. Consultora especializada en gestión de redes de datos. Argentina (2002).

Henrik Abrahamson, Traffic measurement and analysis, SICS Technical Report, **99**, 05 (1999)

Paul Benford, Seffery Kline, David Plonka and Amos Ron, A signal analysis of network traffic anomalies, Proc. Of ACM Sigcomm instrument meas. Workshop, 1 (2002)

Andrew Tanenbaum, Computer Networks, 4ta Ed., 2001

Sergey A. Krashakov and Lev N. Shchur, Active measurement (experiments) of the internet traffic using cache-mesh, Int. J. Mod. Phys, **12**, 549 (2001)

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009