# PARTE II:

# PARTE EXPERIMENTAL

# CAPITULO 5

# Análisis de un sistema conectado a Internet

En este último capítulo de nuestro trabajo dedicado a la seguridad en las redes IP presentaremos la parte práctica o experimental realizada.

Inicialmente realizaremos una presentación de los objetivos que se persiguen en este experimento (deseamos monitorizar una conexión permanente a Internet durante una semana) así como los requisitos necesarios. A continuación analizaremos las distintas posibilidades que podemos utilizar teniendo en cuenta los requerimientos necesarios para ir centrándonos en la arquitectura propuesta.

Posteriormente realizaremos un análisis detallado de todo el tráfico de red obtenido durante la semana, comentando los distintos resultados obtenidos y desglosándolos por día. También analizaremos los resultados globales desde una perspectiva semanal centrándonos en los aspectos más relevantes.

Finalmente describiremos las conclusiones de este experimento que se obtendrán partir del análisis de los informes anteriores y del tráfico registrado durante la semana.

# 5.1 Objetivos

En los capítulos anteriores de este trabajo hemos ido comentando diferentes sistemas y tecnologías que permitían un incremento de la seguridad en nuestras redes de ordenadores (sistemas de detección de intrusos o IDS, Honeypots…). Cada pocos días vemos noticias referentes a nuevas amenazas en Internet (gusanos, virus, *hackers*…) sin embargo ¿realmente tanta falta de seguridad existe en Internet? ¿Tantas son las fuentes de peligro que justifican cada vez más inversión y mejores sistemas de seguridad?

En la actualidad existen cientos de informes que justifican todas y cada una de las miles de soluciones informáticas de seguridad existentes. Sin embargo, prácticamente siempre estos mismos informes son realizados (o peor aún, financiados) por las mismas empresas que venden esos productos.

La bibliografía y las notas de prensa [Far96][Wei00][Bor03][WWW159][WWW160] [WWW161][WWW163][WWW164] están llenas de referencias y datos que indican siempre un aumento espectacular de la inseguridad en Internet. No obstante, cuando deseamos investigar más a fondo los datos o conclusiones que presenta un informe y planteamos preguntas del tipo ¿dónde se ha realizado? ¿quién exactamente lo ha realizado? ¿cómo se ha realizado? ¿qué criterios de verificación de los datos se han seguido? Nos encontramos sin ninguna respuesta satisfactoria.

En este capítulo realizaremos un estudio consistente en la monitorización de una conexión permanente "común" a Internet durante la semana del 21 al 28 de Agosto de 2003 con el objetivo de extraer nuestras propias conclusiones al respecto.

El objetivo de la realización de este estudio es el de presentar unos datos fiables, contrastables y públicamente accesibles que nos permitan evaluar por nuestros propios métodos la situación actual así como verificar o desmentir la conveniencia de la instalación de más medidas de seguridad en las redes IP.

## 5.2 Red de pruebas

Una vez fijado nuestro objetivo de monitorizar una conexión a Internet de forma permanente durante una semana, debemos elegir las características que determinarán la configuración final de nuestro sistema.

Primero realizaremos una enumeración de los distintos requisitos que debe cumplir la solución propuesta. A continuación daremos forma a las posibles soluciones existentes y finalmente las evaluaremos para escoger aquella que más se ajuste a nuestras necesidades.

### 5.2.1 Requisitos estructurales

El objetivo de la red propuesta es el de permitir un análisis completo y exhaustivo del tráfico que circula por ella. Es por ello que existen diferentes aspectos estructurales que debemos tener en cuenta al diseñarla y que por tanto nos permitirán fijar criterios de selección entre las distintas opciones:

1. **Tipo de conexión a Internet:** Nuestro objetivo es el de monitorizar totalmente un acceso a Internet, de esta forma las características de la conexión (ubicación, acceso administrativo, ancho de banda…) determinarán la posibilidad o no de realizar esta tarea.

   Ya hemos demostrado en el capítulo de sistemas de detección de intrusos (IDS) que la monitorización en tiempo real es un tema difícil y que no siempre es posible. El ancho de banda que deseemos controlar es un factor esencial a tener en cuenta.

   Por otro lado, la monitorización de un sistema conectado a Internet requiere de privilegios de administrador en los sistemas de comunicaciones (*routers*) y los servidores, lo que limita las posibilidades a sistemas controlados por nosotros mismos.

2. **Recursos disponibles**: La disponibilidad de recursos para la realización de este trabajo no es infinita, lo que nos obliga a utilizar únicamente aquellas herramientas de las que disponemos.

   La imposibilidad de disponer de tantos equipos conectados a diferentes puntos de Internet como se desee así como la imposibilidad de pagar licencias de software debe ser tenida siempre en cuenta.

3. **Arquitectura de la red**: Para obtener unos resultados fiables en nuestro estudio debemos por un lado realizar un modelo de red genérico y parecido a la mayoría de los sistemas conectados a Internet. Por otro lado debemos realizar un diseño que nos permita el control total de la red para su monitorización sin afectar al resto de los sistemas conectados.

4. **Elementos de monitorización**: Finalmente debemos realizar un análisis de los aspectos a monitorizar así como de las herramientas existentes en el mercado que nos puedan permitir su control y análisis.

Una vez expuestos los distintos requisitos estructurales pasamos al análisis de las distintas posibilidades y opciones.

Nuestro deseo es monitorizar todo el tráfico existente en el punto de conexión a Internet seleccionado. Tal y como se observa en la figura 3-2 del capítulo de detección de intrusos, una conexión a Internet de 256Kbit puede llegar a generar hasta 2.6Gbytes de información al día, mientras que una conexión de 2Mbit generará hasta 21Gbytes diarios.

Si nuestro objetivo es la monitorización del tráfico generado en toda una semana, tenemos que la única alternativa viable es una conexión de 256Kbit (ver figura 5-1) que nos consumirá un máximo de 18Gbytes.

| Tecnología<br>**T** | Espacio de disco diario<br>**EDD** = (T * 86400 s) / 1 GByte | Espacio en disco semanal<br>**EDS** = EDD * 7 |
|---|---|---|
| ADSL (256Kbits/s) | (32768 Bytes/s * 86400 s) / 1Gbyte = **2,6 Gbytes** | **18 Gbytes** |
| ADSL (2Mbit/s) | **21,09 Gbytes** | **147 Gbytes** |

FIG. 5-1: Anchos de banda y tamaño diario de las redes más comunes.

Por otro lado, la potencia de CPU necesaria[ℜ] para el proceso de la información que circula también nos limita la posibilidad de examinar el tráfico de la red, ya que la limitación de recursos nos permite únicamente utilizar un conjunto mínimo de ordenadores con las características de PCs normales.

También deseamos que la arquitectura propuesta para el experimento sea flexible, económica y representativa de la mayoría de arquitecturas conectadas a Internet. De todas las posibles arquitecturas de conexión, la más típica y utilizada [TH96] se basa en la existencia de un router que se encarga de conectar nuestra red local (LAN) a Internet (ver figura 5-2).

[ℜ] Realmente nos referimos a potencia de procesador (CPU), disco y memoria, ya que nuestro objetivo es guardarnos todas las trazas de tráfico generadas en la red.

No entraremos en la configuración específica de la red local puesto que este aspecto no es fundamental para la realización de nuestro objetivo debido a que deseamos controlar y supervisar de todo el tráfico entre Internet y la red local. De esta forma, todas las interacciones entre elementos locales (LAN) no quedarán registradas y por tanto no afectarán a nuestro estudio.

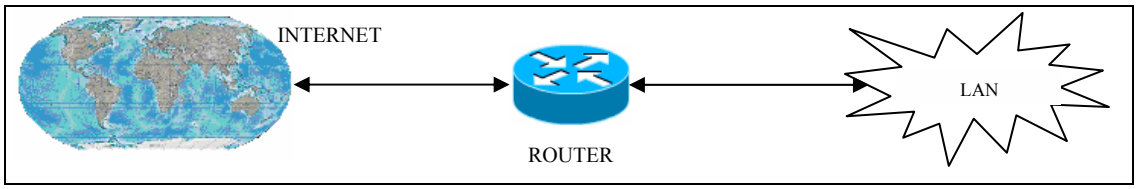


FIG. 5-2: Arquitectura de red propuesta.

## 5.2.2 Arquitectura propuesta

A continuación realizaremos una breve explicación de la implementación del esquema de red realizado teniendo en cuenta los distintos requerimientos funcionales anteriormente citados (ver figura 5-3).

El desglose de los elementos y características básicas de los distintos componentes utilizados en esta prueba es el siguiente:

- **Router**: Es el modelo 3COM 812 y es el encargado de conectar una línea ADSL de 256Kbit y la red local a 10Mbit.

- **HUB**: Es un modelo 3COM Dual Speed 10/100 Office Connect de 8 puertos y se encarga de conectar el router a 10Mbit con el resto de equipos de la red local a 100Mbit.

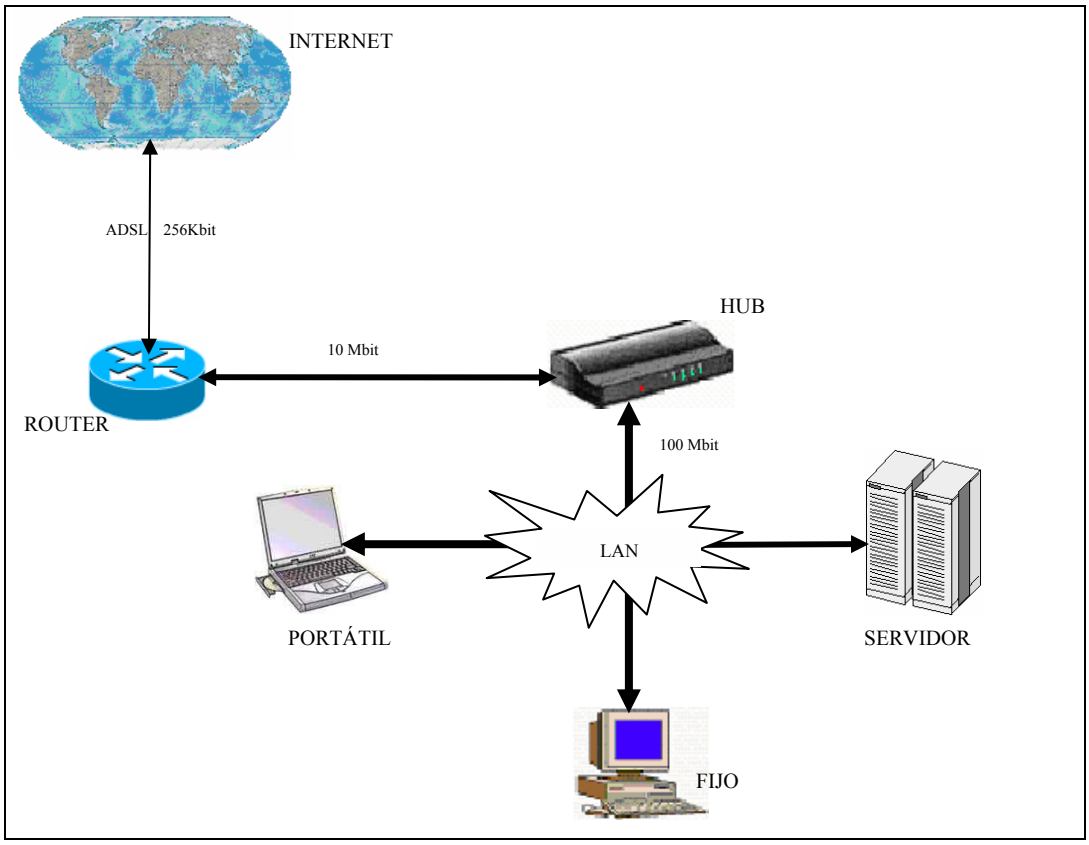


FIG. 5-3: Esquema de la red de pruebas utilizada.

- **SERVIDOR**: Es una máquina Sun Blade 100 con 512MB de RAM y dos discos duros de 120GB en RAID 1 (*mirroring*). Está configurado con el sistema operativo Linux Debian 3.0 testing y es el ordenador encargado de proporcionar los siguientes servicios:

  **Servicio de resolución de nombres** (*Domain Name Server, DNS*[9]): Permite la resolución de nombres y direcciones IP a los usuarios de la red local. También implementa la gestión de un dominio interno para los ordenadores conectados a la LAN.

  **Servicio de compartición de ficheros con Windows** (*SAMBA*[10]): Este servicio permite a los distintos usuarios acceder a los ficheros que poseen en el servidor Unix desde sistemas Windows de una forma transparente.

[9] Para más información ver [Liu02][RFC1034].
[10] Para más información ver [TCE03][WWW157].

**Servicio WWW**: Este servicio implementa distintas funcionalidades accesibles a los usuarios mediante un navegador. Principalmente son servicios de lectura y consulta de correo (Webmail), consulta del estado del servidor de ficheros (SAMBA/SWAT) y visualización del estado de la red.

**Servicio de monitorización de red**: Analiza y almacena todo el tráfico que se registra en nuestra red.

**Servicio de correo**: Permite a los usuarios enviar y recibir correos a Internet (SMTP) así como consultarlos mediante los protocolos IMAP4 y POP3.

**SSH** (*Secure SHell*): Permite la conexión segura de los usuarios al servidor.

- **FIJO**: Es un PC AMD-K6III a 450Mhz con 400MB de RAM y un disco duro de 40GB. Está configurado con un sistema operativo Windows 2000 y se utiliza como puesto de trabajo.

- **PORTÁTIL**: Es un PC portátil con un INTEL PIV a 2.4Ghz con 512MB y 40GB de disco duro. Está configurado con un sistema operativo Windows XP y se utiliza como puesto de trabajo móvil.

## 5.2.3 Configuración

Una vez presentada la arquitectura de red que utilizaremos, pasaremos a pormenorizar los distintos aspectos técnicos de su configuración.

Debido a que el tipo de conexión a Internet utilizado (ADSL) únicamente proporciona una dirección IP pública, se ha tenido que realizar una configuración específica en el router que permita:

1. **Acceso a Internet a todos los ordenadores de la red local (LAN) mediante el uso de técnicas de NAT**[ℜ]: Los ordenadores conectados a la LAN reciben automáticamente direcciones IP del rango 192.168.0.XXX mediante el protocolo DHCP[℘] que implementa el router. De esta forma, todas las direcciones locales tienen acceso a Internet.

2. **Redirección del tráfico de red generado desde y hacia la red local al ordenador encargado de la monitorización del sistema** (servidor): Debido a que deseamos examinar todo el tráfico que llega a nuestra dirección pública, el router ha sido configurado de forma que automáticamente redirija (*bridging*) todo el tráfico de Internet no solicitado por los ordenadores locales al ordenador encargado del análisis.

En la configuración propuesta se utiliza un HUB para la interconexión de los elementos internos de la LAN (router y ordenadores). Esta decisión no es arbitraria, sino que responde a la característica que tienen todos los HUBs de reenviar lo que reciben por un puerto a todos los demás. De esta forma, nos aseguramos que todo el tráfico existente en la red local (vaya o no específicamente al ordenador "servidor") llegará a él.

Las distintas herramientas de monitorización y control del tráfico de red utilizan un modo de trabajo de las tarjetas de red denominado "**modo promiscuo**". El modo de funcionamiento normal de una tarjeta de red consiste en que al recibir un paquete de información, si la dirección de destino no es el la que hay configurada en la tarjeta de red lo ignora. En el modo promiscuo toda la información que llega a la tarjeta de red es accesible.

De esta forma, con la configuración realizada (usando un HUB en lugar de un SWITCH) podemos realmente controlar todo el tráfico existente en nuestra red. Además, durante la semana en la que se realizó este experimento únicamente se mantuvo en funcionamiento el ordenador encargado de la recolección de datos (servidor), de esta forma evitamos cualquier tipo de interferencia que pudieran causar las conexiones de los otros ordenadores locales.

[ℜ] Network Adderss Translation, para más información consultar la bibliografía [Has97].
[℘] Dinamic Host Configuration Protocol, para más información mirar bibliografía [DLD02][WWW156].

Por otro lado, el hecho de mantener un sistema conectado a Internet únicamente "escuchando" y sin generar ningún tipo de tráfico concreto (solamente las respuestas a peticiones iniciadas desde Internet) permite que los resultados obtenidos puedan extrapolarse a cualquier otro sistema conectado a Internet ya que:

- Tenemos un punto de conexión a Internet que no genera tráfico intrínsecamente, lo que nos permite asegurar que si recibimos tráfico externo, cualquier otro nodo conectado a Internet **puede** recibirlo también.

- La elección del periodo de tiempo de análisis (una semana) viene determinada principalmente por tres factores:

    1. **Repetición de los patrones obtenidos:** La observación del tráfico en un día es insuficiente para poder extraer conclusiones plausibles, mientras que la observación en varios días puede permitir la correlación de resultados.

    2. **El tamaño de los datos en disco:** Cada semana se podrían llegar a generar hasta 18Gbytes de información (tope teórico de transmisión), cantidad mas que suficiente para analizar y realizar pruebas.

    3. **Seguridad:** La realización de este experimento requiere de una supervisión constante del sistema ya que cualquier ataque puede resultar exitoso y comprometer nuestro sistema. El esfuerzo de supervisión del sistema por largos períodos de tiempo queda fuera de nuestros recursos.

## 5.3 Herramientas

En este apartado realizaremos una breve explicación de las características principales y rol asumido dentro de este experimento práctico de las diferentes herramientas de software elegidas.

Una vez decidido nuestro objetivo se procedió a la selección de las herramientas necesarias para llevarlo a cabo. Los criterios en los que nos hemos basado para la selección de estos programas son los siguientes:

- **Plataforma de funcionamiento**: Las herramientas elegidas deben funcionar perfectamente en la mayoría de plataformas existentes.

- **Licencia de uso**: La licencia bajo la que se distribuya el software debe permitir su uso de forma libre y sin limitaciones contractuales en nuestro ámbito de estudio (experimento). Herramientas distribuidas bajo licencias GPL, GNU, BSD o similares serán las candidatas.

- **Disponibilidad del código fuente**: Los programas seleccionados deberán estar disponibles en forma de código fuente. Parte de este experimento es la compilación de las herramientas que se van a utilizar. **NO** se utilizarán binarios precompilados en otros sistemas.

- **Continuidad del proyecto**: Siempre que sea posible la elección entre varias herramientas similares, la continuidad del proyecto (existencia de más de un desarrollador, que el software tenga mas de nueve meses de vida…) será una prioridad. Esto nos asegura que la herramienta seleccionada nos permitirá tener soporte de sus creadores en caso de necesidad.

- **Madurez del software**: Se buscan herramientas estables que ya tengan desarrolladas varias versiones. Nuestro objetivo es el de evitar el uso de herramientas en fase de desarrollo o poco probadas que puedan introducir inestabilidad en el sistema.

- **Integración con el sistema Unix**: El software elegido debe ser fácilmente integrable en plataformas Unix (Solaris, Linux, AIX…) y preferiblemente en otros sistemas existentes (Windows…). Análogamente, los prerrequisitos que puedan necesitar las diferentes herramientas deberán de ser lo más standard posible.

# 5.3.1 APACHE

Para las funciones de servidor WWW (principalmente visualización de páginas HTML de los programas instalados) utilizaremos el software **Apache** [WWW166] versión 1.3.27.

Apache el servidor WWW líder con más de un 63% [WWW167] de cuota. Es un proyecto maduro que lleva varios años produciendo un software de calidad y gratuito que funciona perfectamente en casi cualquier sistema operativo existente (desde Windows hasta sistemas Unix).

La compilación e instalación de este software es la usual (por defecto) que recomienda el sistema. Las únicas modificaciones que se han tenido que realizar para adecuarlo al resto de programas que hemos utilizado, son la configuración del servidor WWW para que permita servir páginas y ejecución de *scripts* a los usuarios locales del sistema[ℜ] (ver figura 5-4).

Añadir al fichero "**httpd.conf**":

```
#
# UserDir: The name of the directory which is appended onto a user's home
# directory if a ~user request is received.
#

<IfModule mod_userdir.c>
    UserDir public_html
</IfModule>

<Directory /home/*/public_html/cgi-bin>
      Options +ExecCGI -Includes -Indexes
      SetHandler cgi-script
 </Directory>
```

FIG. 5-4: Modificación del archivo de configuración de Apache.

[ℜ] Las expresiones del tipo http://servidor/~usuario acceden a los archivos del usuario situados en /home/usuario/public_html/ análogamente la ejecución de *scripts* http://servidor/~usuario/cgi-bin accede a /home/usuario/public_html/cgi-bin/

# 5.3.2 Ethereal

Para la visualización y manipulación del tráfico de la red capturado utilizaremos el programa **Ethereal** [WWW168] versión 0.9.14.

Este programa goza de gran reputación entre los administradores de red y se ha convertido en una herramienta básica para cualquier análisis de redes. Este software es gratuito y funciona perfectamente tanto en sistemas Unix como Windows.

Entre sus características principales se encuentra la de realizar completos análisis y visualizaciones en tiempo real de todos los protocolos de redes más usuales. También permite la captura del tráfico de red en disco y la aplicación de filtros de selección así como la visualización del contenido de los datagramas, su edición, modificación y selección interactiva en tiempo real (ver figura 5-5).

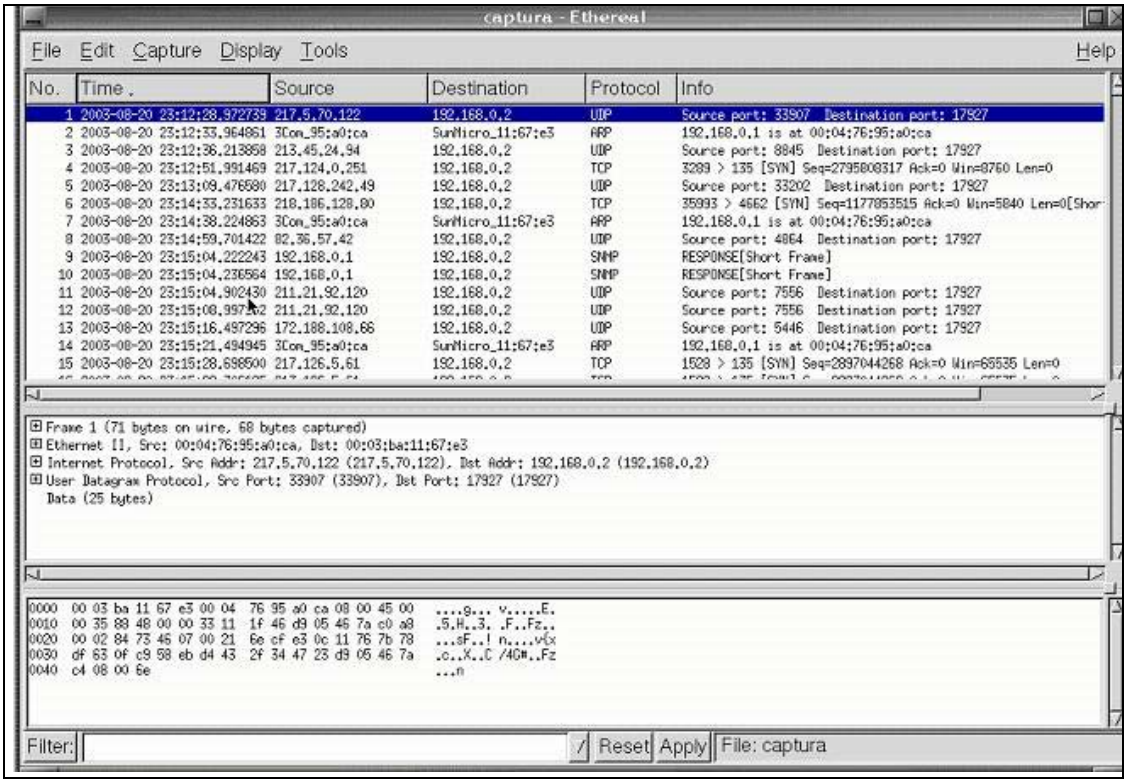


FIG. 5-5: Ethereal.

La compilación e instalación de este software es la que se realiza por defecto. No obstante se han de tener en cuenta los siguientes requisitos:

1. Necesita las librerías GTK+ para su entorno gráfico.

2. Necesita las librerías del sistema GLIB.

3. Necesita las librerías de interface LIBPCAP para su acceso a los dispositivos de red.

4. Para poder utilizar todas sus funcionalidades correctamente debe ser ejecutada como administrador (*root*) del sistema.

Estos requisitos no son excesivos o complicados, ya que usualmente cualquier sistema lleva instaladas estas librerías por defecto. En cuanto a la necesidad de ser administrador de la máquina es debido a que el programa trata directamente con el dispositivo de red configurándolo en modo promiscuo para poder espiar todos los paquetes de información que llegan al dispositivo.

## 5.3.3 IPaudit- IPaudit WEB

Para la visualización y la generación de las gráficas del tráfico recibido en nuestra red utilizaremos el programa **IPaudit** [WWW169]. Este programa dispone de una versión con interface WWW denominada **IPaudit WEB** [WWW170] que será la que se utilizará en su versión 1.0-BETA7.

La elección de IPaudit sobre otras herramientas de monitorización de redes se basa en que cumple perfectamente los requisitos estructurales planteados inicialmente y existe una gran experiencia en su uso por nuestra parte.

Es un proyecto sólido (empezó en 1999) que ha ido evolucionando gradualmente y dispone de un grupo de gente que le proporciona continuidad. Funciona perfectamente en entornos Unix y proporciona una gran flexibilidad de configuración. Además genera una gran variedad de informes útiles que nos permiten conocer el estado real de nuestra red.

También tiene la capacidad de realizar complejas búsquedas (por dirección IP de origen, destino, protocolo…) por los distintos logs que genera. Asimismo almacena y realiza las búsquedas de los datos en formato comprimido (con el programa *gzip* concretamente) lo que permite un gran ahorro de espacio de disco, vital en este tipo de aplicaciones.

Hemos escogido el uso de la versión IPaudit WEB debido principalmente a que la versión "normal" de IPaudit es en modo texto (línea de comandos) lo que dificulta la interpretación de los datos. Por otro lado, la versión WWW nos permite consultar de una forma visual sencilla los diferentes datos y gráficas generadas por el tráfico de red (ver figura 5-6).

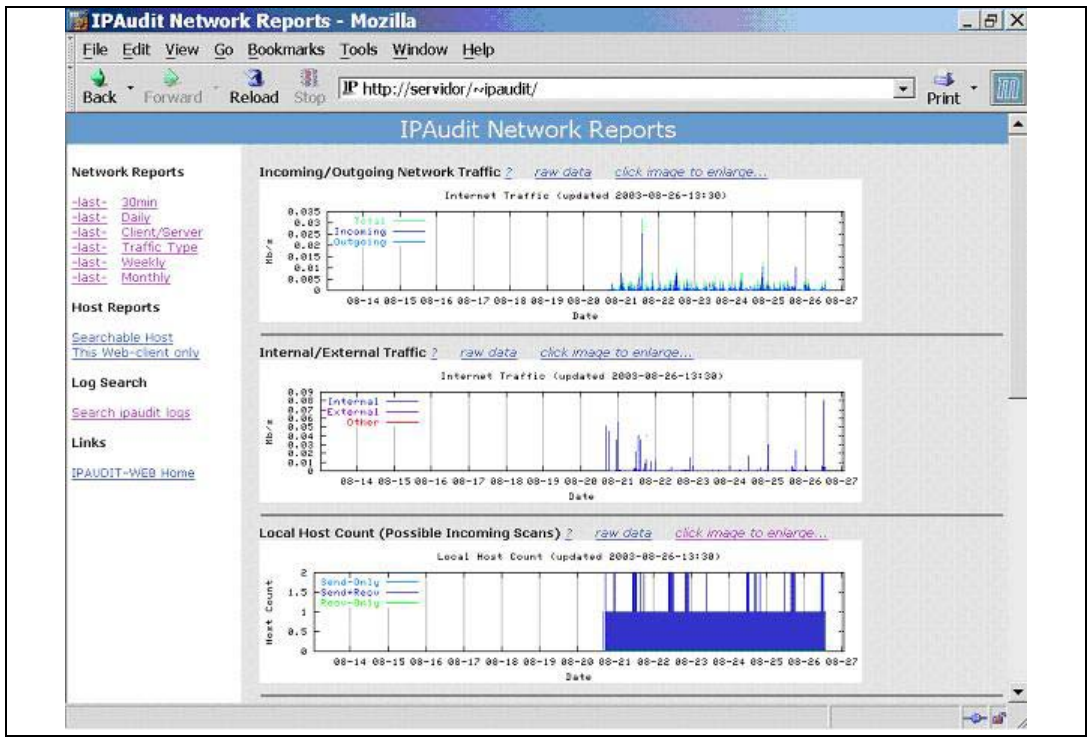


FIG. 5-6: Página inicial de IPaudit WEB.

La versión WEB utiliza procesos CRON que se lanzan cada media hora y que durante treinta minutos se encargan de registrar todo el tráfico generado en la red. De esta forma tenemos que cada 30 minutos se envía una señal de finalización controlada al proceso anterior (que escribe en el fichero de log correspondiente los datos del tráfico pendientes) y se inicia un nuevo proceso de captura de datos.

Esta captura de datos se almacena en disco aplicando un filtro de conversión a un formato más compacto que incluye los campos más relevantes de los paquetes recibidos (ver figura 5-7). De esta forma podemos observar como si bien tenemos todos los datos que determinan la comunicación entre las distintas direcciones IP, no disponemos de los datos transmitidos[9R] (el contenido).

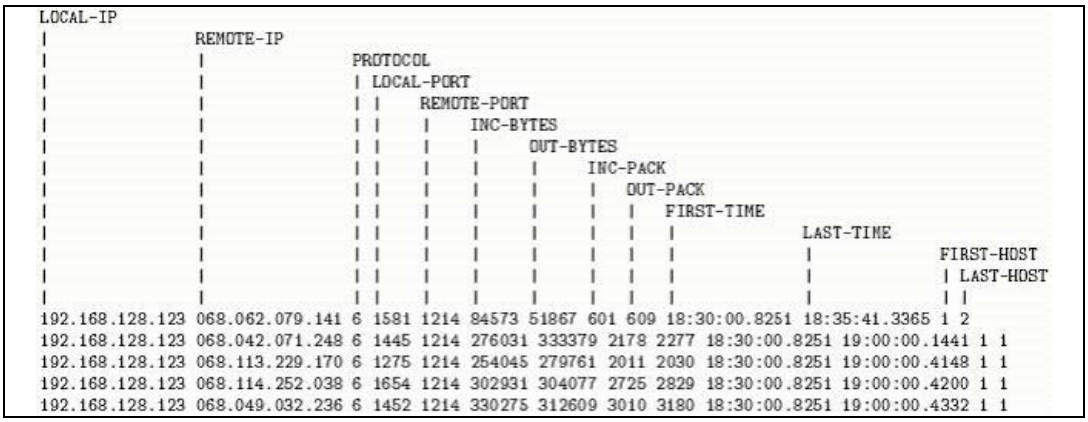


FIG. 5-7: Página inicial de IPaudit WEB.

Una vez finalizado el proceso anterior se generan las gráficas y los informes correspondientes:

- **Informes cada 30 minutos**: En este tipo de informe se muestra el total de bytes enviados y recibidos en nuestra red durante la media hora analizada. Asimismo se muestran las veinte direcciones IP locales y remotas con más tráfico generado, lo que nos permite examinar más a fondo las comunicaciones que nos interesen (ver figura 5-8).

[9R] Para obtener los datos que se intercambian durantes las comunicaciones de red debemos usar otros programas como el Ethereal o el tcpdump.

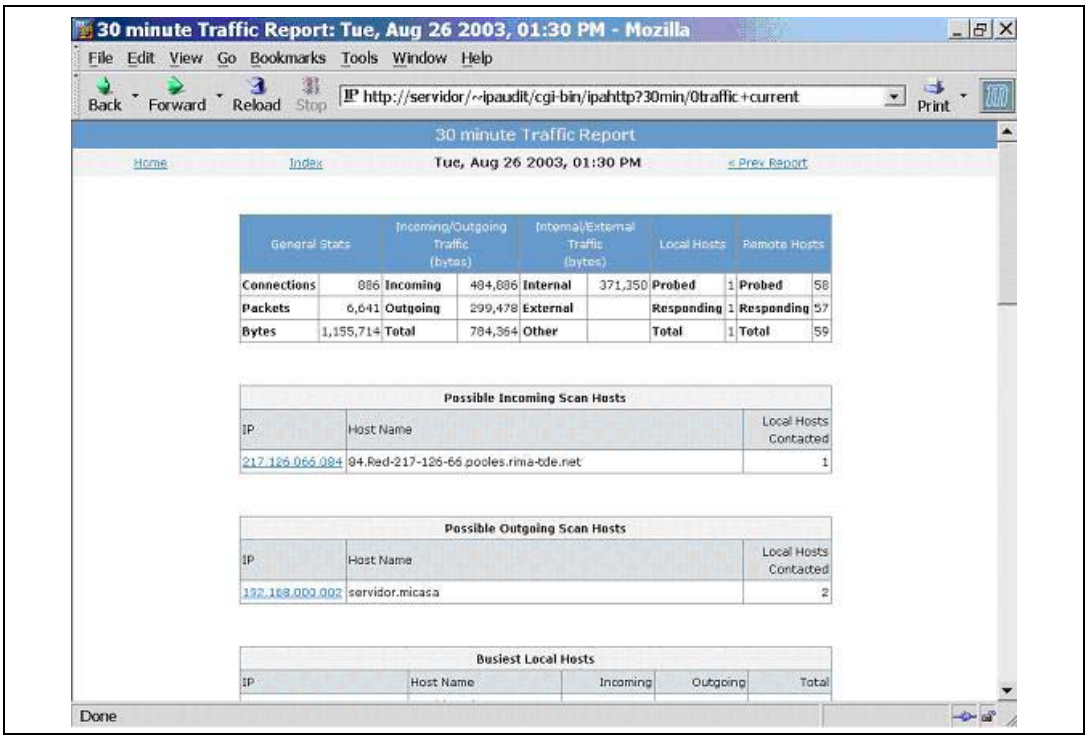


FIG. 5-8: Informe de IPaudit WEB de los 30minutos.

- **Informes diarios**: Estos informes presentan el resumen de la acumulación de todos los informes de media hora realizados durante el día. Visualiza el total de bytes enviados y recibidos en nuestra red así como las veinte direcciones IP locales y remotas que más tráfico han generado o recibido (ver figura 5-9).

- **Informes cliente/servidor** (diario): Este informe se genera diariamente y desglosa todo el tráfico recibido o enviado a los servidores que proporcionan los servicios de Mail, SSH, Telnet, HTTP, HTTPS tanto para servidores o clientes locales como remotos (ver figura 5-10).

- **Informes por tipo de tráfico** (diario): En este informe se realiza una agregación de todo el tráfico generado diariamente y se clasifica según el protocolo (TCP, UDP, ICMP, NetBios, Telnet, FTP…) al que pertenezca (ver figura 5-11).

- **Informes semanales**: Estos informes reflejan la suma total del tráfico generado por la red durante la semana y presentan las 25 direcciones IP que más tráfico han generado o recibido (ver figura 5-12).

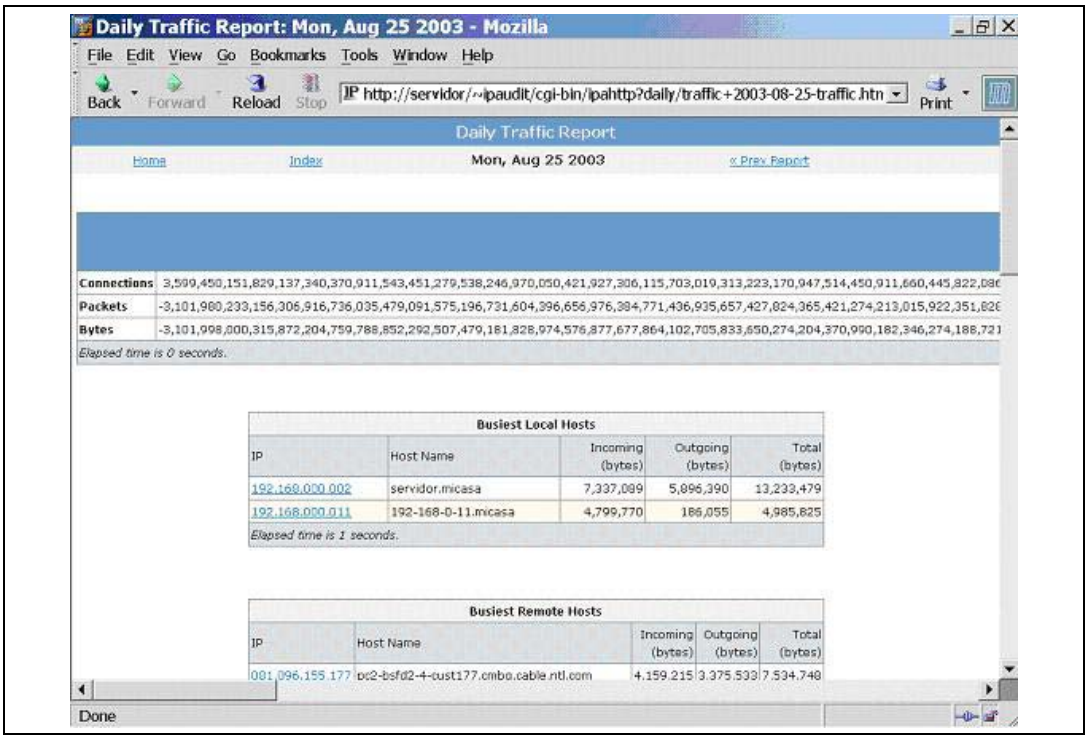


FIG. 5-9: Informe de IPaudit WEB diario.

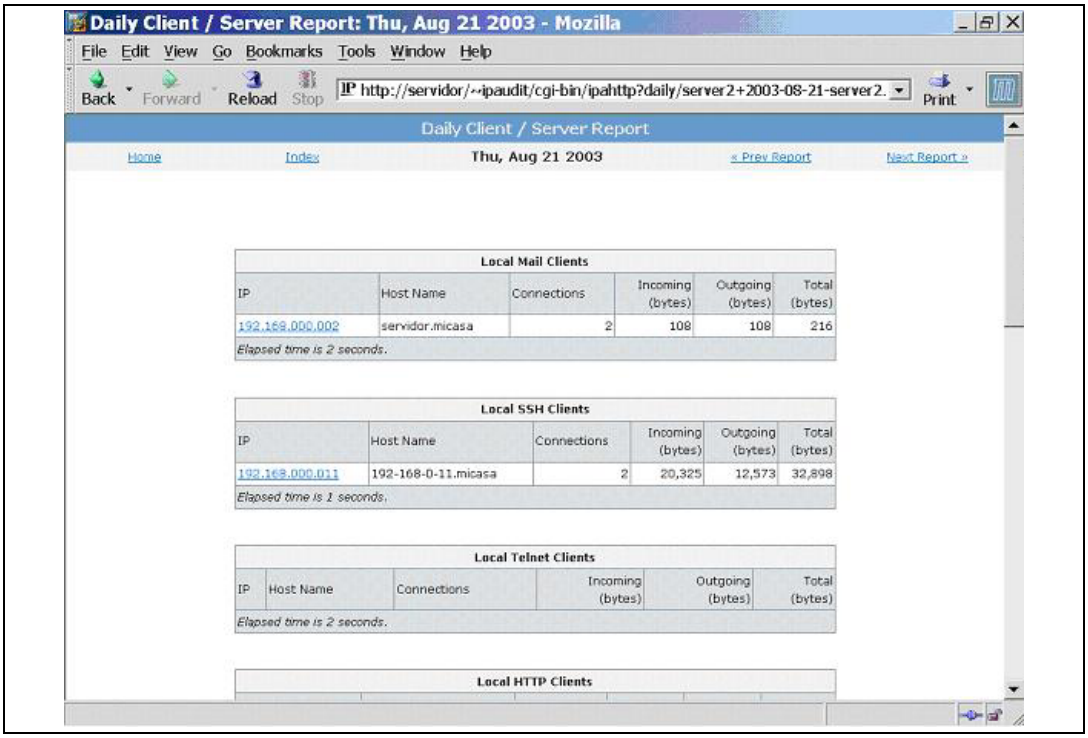


FIG. 5-10: Informe de IPaudit WEB diario cliente/servidor.

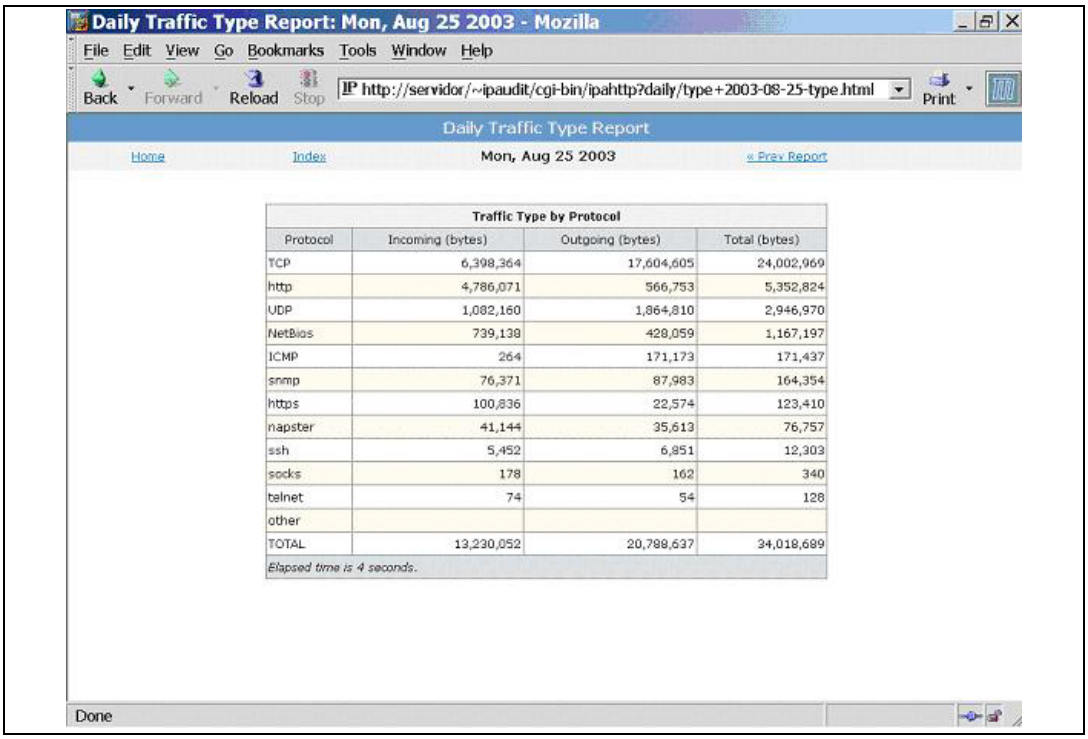


FIG. 5-11: Informe de IPaudit WEB diario por tipo de tráfico.

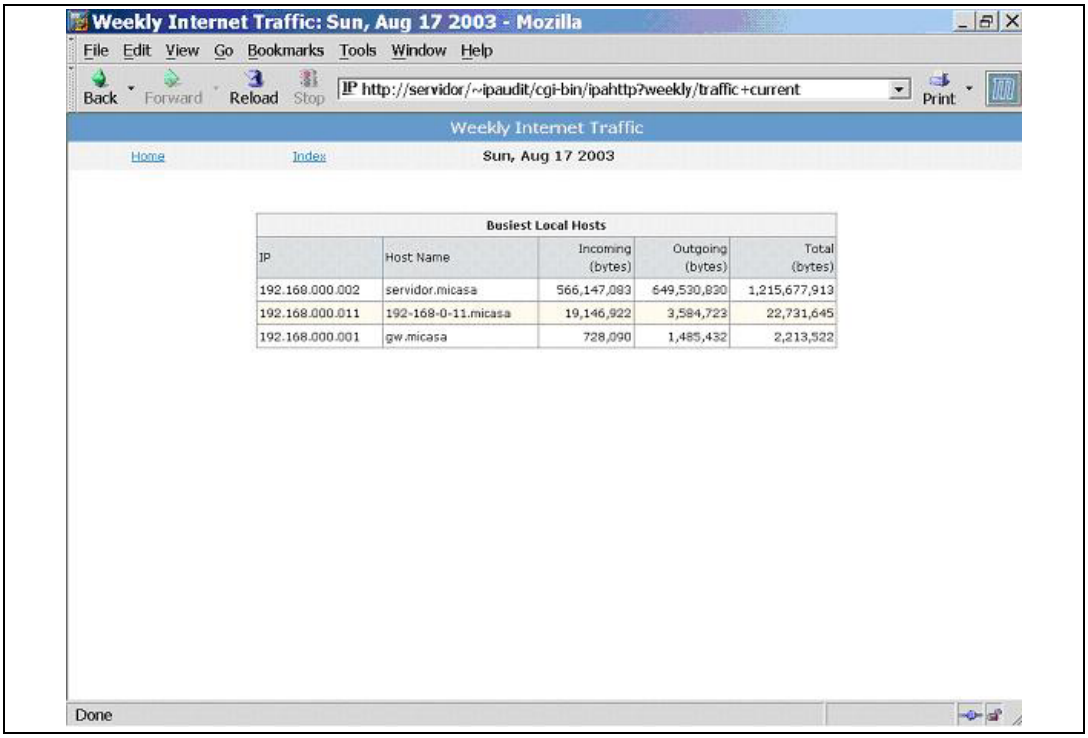


FIG. 5-12: Informe de IPaudit WEB semanal.

- **Informes mensuales**: Este informe es exactamente igual que el informe semanal, pero mostrando el tráfico de las 25 direcciones IP con más tráfico de red durante el mes.

IPaudit WEB también permite la realización de búsquedas en los ficheros de log por una gran cantidad de campos (tipo de protocolo, dirección IP, puerto de origen, puerto de destino…) lo que permite filtrar el tráfico registrado para analizar únicamente las comunicaciones deseadas (ver figura 5-13).

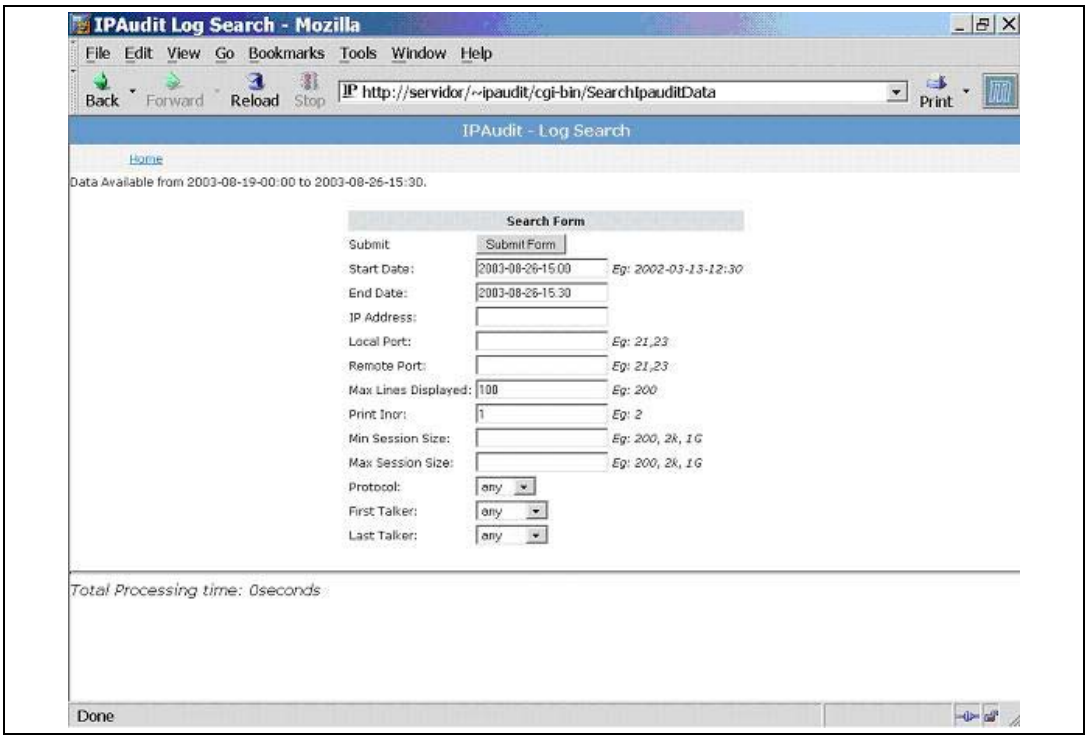


FIG. 5-13: Búsquedas en IPaudit WEB.

La instalación efectuada es la que se recomienda por defecto. Sin embargo se han de tener en cuenta los siguientes requisitos:

1. Necesita las librerías de interface LIBPCAP para su acceso a los dispositivos de red.

2. Necesita la utilidad GNUPLOT para la generación de los gráficos.

3. Es necesario el compilador del lenguaje PERL debido a que IPaudit WEB ejecuta varios *scripts* escritos en este lenguaje.

4. Necesita que se cree un usuario específico en el sistema denominado "*ipaudit*" y privilegios de administrador para realizar la instalación del software.

5. Es necesario un servidor WWW que esté configurado para que permita al usuario ipaudit la visualización de páginas HTML (http://servidor/~ipaudit) y la ejecución de *scripts* (http://servidor/~ipaudit/cgi-bin/) desde su directorio (/home/ipaudit/public_html usualmente).

6. El sistema debe permitir la ejecución planificada (CRON) de *scripts* a los usuarios. Este punto es esencial ya que el programa genera gráficas cada cierto intervalo de tiempo, lo que le obliga a ejecutar determinados comandos cada 30 minutos.

## 5.3.4 MRTG

**MRTG** (*Multi Router Traffic Grapher*) [WWW171] es una herramienta gráfica que permite la monitorización de las conexiones de red mediante la generación de gráficas que reflejan el uso del ancho de banda. Se comunica con los distintos dispositivos mediante el protocolo SNMP[ℜ] y suele utilizarse en la monitorización de equipos de red, principalmente en routers y swiches. La versión que se ha utilizado en este experimento ha sido la 2.9.29.

MRTG es una herramienta gratuita, estable y que funciona prácticamente con cualquier sistema Unix. En nuestro esquema de red este software será el encargado de la monitorización del ancho de banda que circula por el router, tanto del extremo conectado a Internet (ADSL) como del extremo conectado a la red local (LAN).

[ℜ] Simple Network Management Protocol [Ric98-1].

A diferencia de otras herramientas de monitorización como el IPaudit, MRTG simplemente genera una gráfica diaria, semanal, mensual y anual con el total del ancho de banda utilizado en la conexión a Internet (ver figura 5-14). De esta forma, es el complemento perfecto para el IPaudit, ya que nos permite obtener un control exhaustivo de los dos segmentos de la red que conecta el router.

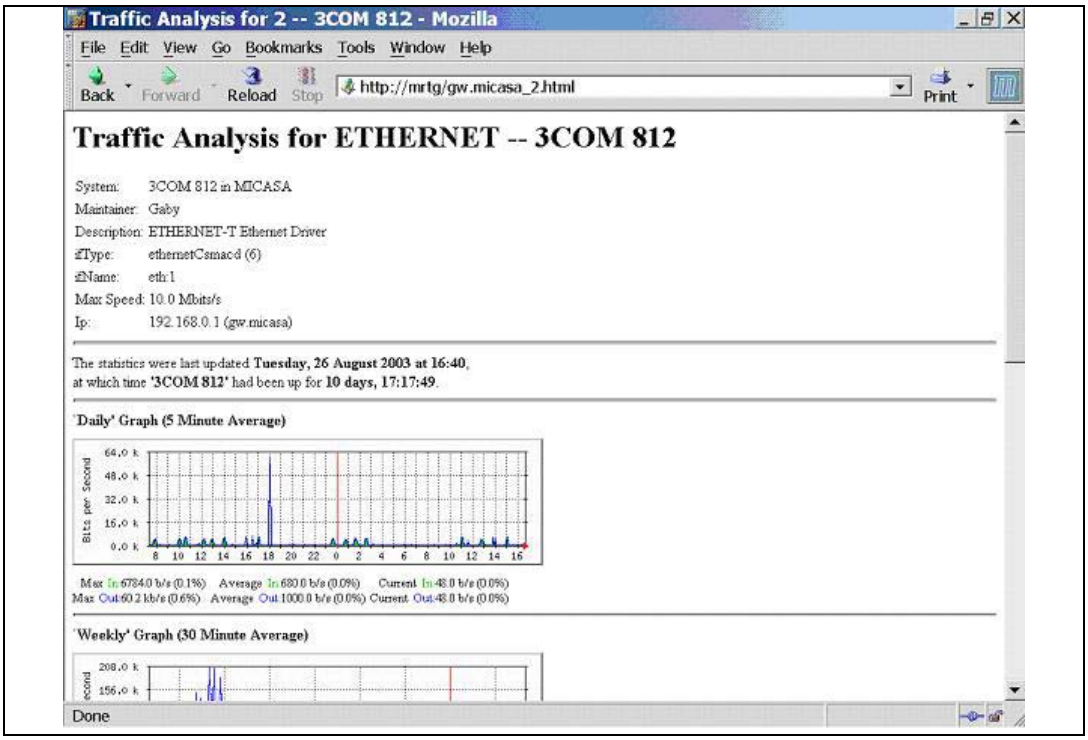


FIG. 5-14: MRTG.

La instalación efectuada es la que se recomienda por defecto. Sin embargo se han de tener en cuenta los siguientes requisitos:

1. Los dispositivos monitorizados con MRTG deben tener activado el protocolo SNMP para que el software pueda conectarse a ellos y leer los datos.

2. Es necesario un servidor WWW.

3. Son necesarias las librerías LIBPNG que permiten la creación y manipulación de imágenes en formato PNG.

4. El sistema debe permitir la ejecución planificada (CRON) de *scripts* a los usuarios. Este punto es esencial ya que el programa genera gráficas cada cierto intervalo de tiempo, lo que le obliga a ejecutar determinados comandos cada 5 minutos.

## 5.3.5 NMAP

**NMAP** (*Network Mapper*) [WWW172] es una herramienta que permite la exploración y la auditoria de redes de ordenadores. Su misión principal consiste en la realización de varios tipos de exámenes de puertos (*port scanning*) para la obtención de los servicios existentes en un ordenador. La versión que se ha utilizado en este experimento ha sido la 3.3.0.

Este software gratuito, muy estable que funciona tanto en sistemas Unix como Windows. Es ampliamente conocido y utilizado por administradores de red y *hackers*.

El objetivo del uso de esta herramienta en nuestra arquitectura es la de verificar los servicios accesibles desde nuestra red hacia Internet. De esta forma, podemos comprobar la eficacia de nuestro sistema de monitorización y asegurarnos que cualquier tipo de tráfico que se genere desde Internet quedará registrado.

Otra característica de NMAP es la de efectuar la detección del sistema operativo existente en el ordenador (*OS fingerprinting*). De esta forma, antes de abrir nuestra red a Internet podemos auditarnos de forma que ya sabremos toda la información que cualquiera podría llegar a extraer de nosotros.

La instalación efectuada es la que se recomienda por defecto. Sin embargo cabe notar que para ejecutar todas las funcionalidades que proporciona esta herramienta se debe tener privilegios de administrador (*root*).

# 5.3.6 TCPdump

**TCPdump** [WWW173][WWW174] es una herramienta que permite la auditoria y la adquisición del tráfico que circula por la red. La versión que se ha utilizado en este experimento ha sido la 3.7.2.

Este software es gratuito y funciona sin problemas tanto en sistemas Unix como Windows. Pertenece a un proyecto estable que lleva varios años desarrollando software de calidad y se le considera como el referente principal en el análisis del tráfico de redes.

TCPdump permite el uso de filtros de tráfico (por protocolo, por dirección IP de origen o destino, por puerto de origen o destino…) así como diferentes opciones de captura tanto de las cabeceras de los paquetes como de los datos que transportan. Precisamente esta característica es la que utilizaremos principalmente.

Otros programas de monitorización de redes capturan en mayor o menor medida el tráfico existente en la red pero únicamente a nivel de cabeceras (como IPaudit) o a nivel de tamaño del paquete (como MRTG). TCPdump nos permite almacenar junto con la cabecera del datagrama los datos que transporta, lo que nos permite la reconstrucción total de las comunicaciones existentes en nuestra red (ver figura 5-15).

- Ejemplo de la captura del tráfico del dispositivo ETH0 de nuestra red en el fichero 'captura.cap':

```
servidor:/home/gaby/tcpdump/sbin# ./tcpdump –i eth0 –ln -w captura.cap
tcpdump: listening on eth0
```

FIG. 5-15: Ejemplo de captura de datos con TCPdump.

Los ficheros de log de salida generados por TCPdump son ficheros binarios que pueden ser visualizados/manipulados por otras herramientas como el Ethereal.

La instalación efectuada es la que se recomienda por defecto. Sin embargo se han de tener en cuenta los siguientes requisitos:

1. Necesita las librerías de interface LIBPCAP para su acceso a los dispositivos de red.

2. Para ejecutar todas las funcionalidades que proporciona esta herramienta se deben tener privilegios de administrador (*root*). Esto es debido principalmente a que accede directamente al dispositivo de red y lo configura en modo promiscuo para la captura de todo el tráfico.

## 5.3.7 TCPreplay

**TCPreplay** [WWW175] es una herramienta que permite "a posteriori" la reproducción del tráfico de red a partir de los logs generados por el programa TCPdump o compatibles. La versión utilizada en las pruebas realizadas es la 1.4.4.

El proyecto TCPreplay es gratuito y está diseñado para funcionar perfectamente en sistemas Unix.

Después de monitorizar y capturar todo el tráfico de nuestra red, puede interesarnos realizar una simulación de algún comportamiento anómalo detectado o que deseemos analizar en profundidad.

Con TCPdump podemos aplicar los filtros deseados a la captura del tráfico de red, mientras que con Ethereal podemos visualizarlo y modificarlo. TCPreplay cierra el círculo permitiéndonos la reproducción de secuencias de tráfico ya capturadas en un entorno controlado. Además nos permite la posibilidad de reproducir estas secuencias tantas veces como queramos y a la velocidad que deseemos, lo que permite simular distintos comportamientos según el ancho de banda configurado.

La instalación efectuada es la que se recomienda por defecto. Sin embargo se han de tener en cuenta los siguientes requisitos:

1. Necesita las librerías de interface LIBPCAP para su acceso a los dispositivos de red.

2. Necesita las librerías de interface LIBNET para su acceso a los dispositivos de red.

3. Para ejecutar todas las funcionalidades que proporciona esta herramienta se deben tener privilegios de administrador (*root*).

## 5.4 Resultados

Los resultados presentados a continuación hacen referencia al tráfico observado durante la semana del 21 al 28 de Agosto de 2003. La presentación de los datos se desglosará en dos bloques.

Inicialmente se realizará una presentación de los datos mediante un informe diario que contendrá los datos más relevantes del día así como su análisis. Después se realizará un resumen semanal que contendrá los datos más importantes del tráfico observado durante la semana analizada.

Dentro del informe diario se realizarán dos presentaciones distintas de los datos obtenidos en nuestra red.

La primera clasificación dividirá en tráfico dirigido según los puertos a los que haga referencia. De esta forma tendremos los inferiores al 1024 denominados conocidos[ЭЯ] (*well-know ports*) desglosados por servicios y la dirigida a puertos iguales o superiores al 1024:

[ЭЯ] Según la clasificación de la IANA [WWW176][WWW177].

1. **MAIL**: En esta categoría se clasificaría todo el tráfico que hiciera referencia a los servicios de correo más usuales (SMTP, POP3 e IMAP). Puertos de conexión 25, 110 y 143.

2. **SSH**: En este grupo se colocarán las peticiones recibidas al servicio de conexión remota segura. Puerto de conexión 22.

3. **TELNET**: Este grupo hará referencia a las peticiones recibidas al servicio de conexión remota. Puerto de conexión 23.

4. **HTTP**: En esta categoría se incluye todo el tráfico destinado al servidor WWW. Puerto de conexión 80.

5. **HTTPS**: En esta categoría se incluye todo el tráfico destinado al servidor WWW seguro. Puerto de conexión 443.

6. **Netbios-ns**: En este grupo se indicarán las peticiones recibidas al servicio de resolución de nombres (*name server*) de *Netbios*. Puerto de conexión 137.

7. **Netbios-dmg**: Este grupo abarca las peticiones recibidas al servicio de datagramas (*datagram service*) de *Netbios*. Puerto de conexión 138.

8. **Netbios-ssn**: Esta categoría referenciará todas las peticiones recibidas al servicio de sesión (*session service*) de *Netbios*. Puerto de conexión 139.

9. **Microsoft-ds**: En este grupo se indicarán las peticiones recibidas al servicio de Microsoft DS. Puerto de conexión 435

10. **Otros (< 1024)**: En esta categoría se incluirá todo el tráfico destinado a otros puertos inferiores al 1024 y que no corresponde a ninguno de los grupos anteriores.

11. **Otros (>= 1024):** En esta última categoría se clasificará todo el tráfico destinado a puertos superiores al 1024 (puertos no standard).

La segunda clasificación agrupará los datagramas recibidos según el tipo de protocolo utilizado para su transmisión. Análogamente los protocolos en los que subdividiremos el tráfico obtenido son los más usuales en Internet:

- **TCP**: Protocolo orientado a conexión y fiable. Lo utilizan servicios como el SSH, TELNET, WWW…
- **UDP**: Protocolo no fiable. Lo utilizan servicios como el DNS, NFS…
- **ICMP**: Protocolo no fiable utilizado para la gestión y el control del flujo de las comunicaciones IP. Lo utilizan servicios como en PING, Traceroute…
- **Otros**: Agrupa el resto de tráfico que no haga referencia a ninguno de los protocolos anteriores.

Para el análisis "fino" de los datos obtenidos con el programa IPaudit WEB se han utilizado herramientas y filtros standard existentes en todos los sistemas Unix (ver figura 5-16):

- **gzip**: Es el compresor de datos standard en sistemas Unix.
- **gunzip**: Es el descompresor de datos generados por gzip. Recordamos que IPaudit WEB almacena los datos obtenidos en formato comprimido (gzip).
- **zcat**: Es una utilidad del sistema que nos permite examinar ficheros comprimidos con gzip redireccionando su salida descomprimida hacia la salida standard (*standard output*).
- **awk**: Es una utilidad para el proceso de ficheros de texto. Este programa tiene un lenguaje de programación que permite la aplicación de complejos filtros a los datos.

- Ejemplo de filtrado manual de los datos del día 21-08-2003:

```
/home/ipaudit/data/30min/# zcat 2003-08-21*
| awk '{ if (substr($2,1,8) != "192.168." && $12 == 2) { print }  }'
| awk '{ if ($4 >= 1024) { print} } '
| wc -l
```

FIG. 5-16: Ejemplo de filtrado fino de datos.

## 5.4.1 Día 21 de Agosto

El día 21 de agosto de 2003 se registraron un total de 19.123 paquetes enviados a nuestra red local. El desglose básico del tráfico clasificado por los principales servicios a los que hace referencia podemos observarlo en la figura 5-17.

| | | |
|---|---|---|
| MAIL | : | 10 |
| SSH | : | 4 |
| TELNET | : | 0 |
| HTTP | : | 8 |
| HTTPS | : | 3 |
| Netbios-ns | : | 233 |
| Netbios-dgm | : | 4 |
| Netbios-ssn | : | 5255 |
| Microsoft-ds | : | 5860 |
| Otros (< 1024) | : | 3571 |
| Otros (>=1024) | : | 4175 |
| **TOTAL** | **:** | **19123** |

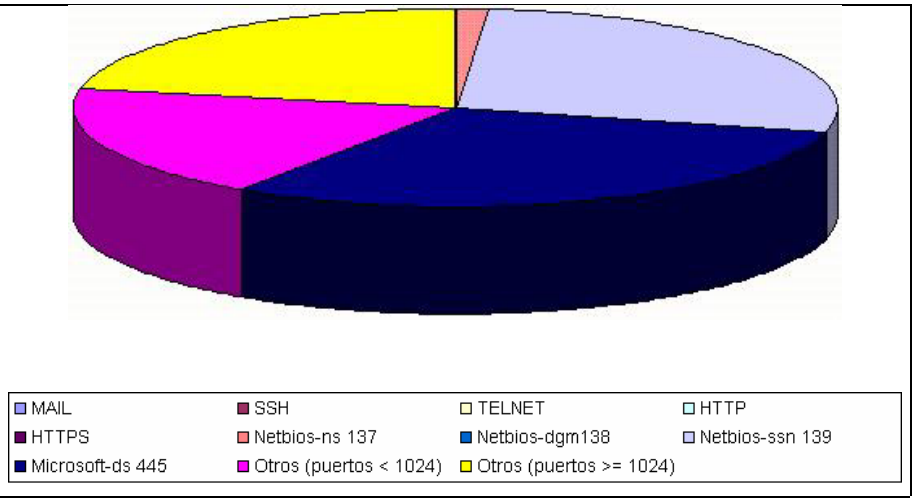


FIG. 5-17: Clasificación del tráfico del día 21/08/2003 por servicio.

Podemos observar en el gráfico de distribución del tráfico por servicios cómo existe una enorme cantidad de datagramas que hacen referencia a los servicios *Netbios/Microsoft-ds*. Este gran porcentaje (casi el 60% del total) nos sorprendió enormemente ya que

durante el resto de la semana este patrón se siguió repitiendo. Después de examinar el tráfico más detalladamente y consultar distinta bibliografía [Alex00][WWW178] [WWW179][WWW181][WWW182] hemos encontrado las siguientes explicaciones:

- Los sistemas basados en Windows (95, 98, NT, 2000, XP…) implementan un protocolo de red denominado **Netbios** y que se sitúa por encima de la pila IP (*IP stack*). Este protocolo "escucha" en diferentes puertos del sistema (137,138…) para proporcionar los distintos servicios de compartición de archivos por red.

- El comportamiento por defecto de los sistemas Windows conectados a una red es el de anunciar su presencia (y por tanto datos como el nombre de la máquina, dominio al que pertenece, recursos compartidos que ofrece…) al resto de máquinas conectadas. Este anuncio se realiza indiscriminadamente a toda la red local y a todos los ordenadores conectados sin ningún mecanismo de seguridad o autenticación.

- Si estos puertos son accesibles desde fuera de la red local[ℜ] (debido a la inexistencia de mecanismos de seguridad en nuestra red o a su una mala configuración), cualquier petición recibida en estos puertos sería contestada automáticamente por el sistema. De esta forma, cualquier problema de seguridad (*bug*) en estos servicios permitiría a un eventual atacante tomar el control del sistema.

- Los sistemas operativos Windows son los más utilizados en el mundo, según el buscador Google [WWW183] en junio de 2003 el 92% de los navegadores utilizados para acceder a su buscador utilizaban este sistema operativo.

- Al igual que cualquier software los sistemas operativos Windows son propensos a presentar fallos de seguridad que son utilizados por *hackers* o *blackhats* con el objetivo de hacerse con el control de la máquina. El envío indiscriminado de peticiones a estos servicios por toda Internet con la esperanza de que llegue a un ordenador con Windows (la mayoría) explica la gran cantidad de peticones registradas.

[ℜ] Para más información ver el capítulo 1 dónde se explican los distintos protocolos de Internet así como su encapsulación.

De esta forma, todo el tráfico *Netbios/Microsoft-ds* recibido hace referencia a peticiones de información de estos servicios. Debido a esta característica y al gran volumen de tráfico que representan, no los comentamos con más detalle en los informes diarios.

En el análisis del día 21 también podemos observar la existencia de 10 intentos de conexión a los protocolos de MAIL.

192.168.000.002 149.083.020.007 6 **110** 54867 108 58 2 1 11:18:29.7280 11:18:29.8747 2 2
192.168.000.002 149.083.020.007 6 **110** 51827 108 58 2 1 11:18:37.0295 11:18:37.1500 2 2
192.168.000.002 149.083.020.007 6 **110** 56729 108 58 2 1 11:21:48.5914 11:21:48.6971 2 2
192.168.000.002 149.083.020.007 6 **110** 35268 108 58 2 1 11:23:40.9491 11:23:41.2797 2 2
192.168.000.002 149.083.020.007 6 **110** 56892 108 58 2 1 11:25:25.7887 11:25:25.9939 2 2

192.168.000.002 149.083.020.007 6 **143** 54867 108 58 2 1 11:18:29.6776 11:18:29.7769 2 2
192.168.000.002 149.083.020.007 6 **143** 51827 108 58 2 1 11:18:37.0442 11:18:37.1566 2 2
192.168.000.002 149.083.020.007 6 **143** 56729 108 58 2 1 11:22:03.8638 11:22:04.2172 2 2
192.168.000.002 149.083.020.007 6 **143** 35268 108 58 2 1 11:23:44.1623 11:23:44.4669 2 2
192.168.000.002 149.083.020.007 6 **143** 56892 108 58 2 1 11:25:31.5112 11:25:31.8420 2 2

Estos intentos de conexión revelan la intención de realizar una comprobación de los puertos (*port scanning*) existentes en nuestro sistema con el objetivo de detectar la existencia de los servicios de lectura de correo (POP3 e IMAP) ya que las peticiones provienen de la misma dirección IP en un corto lapso de tiempo y al observar los logs del sistema no se ha observado ningún otro comportamiento anormal.

Análogamente observamos que las peticiones a los servicios de SSH, HTTP y HTTPS provienen de la misma dirección IP y en el mismo período de tiempo, lo que nos permite concluir que desde la dirección IP 149.083.020.007 nos están sondeando el sistema para adivinar que servicios tenemos accesibles (por ejemplo con la herramienta NMAP).

192.168.000.002 149.083.020.007 6 **22** 51827 108 58 2 1 11:18:37.0474 11:18:37.1597 2 2
192.168.000.002 149.083.020.007 6 **22** 56729 108 58 2 1 11:22:01.6413 11:22:01.8319 2 2
192.168.000.002 149.083.020.007 6 **22** 35268 108 58 2 1 11:23:48.5159 11:23:48.7246 2 2
192.168.000.002 149.083.020.007 6 **22** 56892 108 58 2 1 11:25:29.4515 11:25:29.8100 2 2

192.168.000.002 149.083.020.007 6 **80** 51827 108 58 2 1 11:18:37.0375 11:18:37.1532 2 2
192.168.000.002 149.083.020.007 6 **80** 56729 108 58 2 1 11:21:58.2244 11:21:58.5682 2 2
192.168.000.002 149.083.020.007 6 **80** 35268 108 58 2 1 11:23:48.6333 11:23:48.9217 2 2
192.168.000.002 149.083.020.007 6 **80** 56892 108 58 2 1 11:25:27.4131 11:25:27.6054 2 2

Podemos observar también como recibimos algunas peticiones al servicio HTTP (puerto 80) desde otras direcciones IP. Como son pocas peticiones, aisladas y no se repiten, a priori podríamos concluir que probablemente no son más errores que ha cometido un usuario al teclear la dirección IP en su navegador.

192.168.000.002 081.096.155.177 6 **80** 4493 481 519 6 4 05:03:48.5840 05:04:24.5418 2 2
192.168.000.002 199.035.016.165 6 **80** 5632 108 58 2 1 06:48:57.7993 06:48:58.2571 2 2
192.168.000.002 080.004.006.139 6 **80** 3310 337 524 5 4 08:35:25.7793 08:35:26.5009 2 2
192.168.000.002 146.145.025.067 6 **80** 2146 318 531 5 5 22:42:10.8798 22:42:11.4060 2 2

Sin embargo al observar los logs del servidor WWW para conocer los comandos que se han ejecutado desde estas direcciones IP podemos observar con cierta sorpresa que estamos siendo víctimas de distintos ataques [WWW185].

81.96.155.177 -- [21/Aug/2003:05:03:48 +0200] "OPTIONS / HTTP/1.1" 200 –
146.145.25.67 -- [21/Aug/2003:22:42:11 +0200] "HEAD / HTTP/1.0" 200 0

La bibliografía consultada [PU02][WWW186][WWW187][WWW194] nos indica que muchas aplicaciones de *hackers* o *blackhats* comprueban la posibilidad de utilizar los servidores WWW como sistemas *proxy*[91]. La idea que se esconde tras estas peticiones es la de buscar el anonimato del atacante de forma que pueda utilizar el servidor WWW-*proxy* como lanzadera de peticiones a otros servidores de forma indirecta.

80.4.6.139 -- [21/Aug/2003:08:35:26+0200] "GET/scripts/..%255c%255c../
winnt/system32/cmd.exe?/c+dir"

En esta otra petición el atacante de la dirección 80.4.6.139 busca un sistema Windows que tenga un servidor WWW mal configurado o anticuado (que no se hayan aplicados los distintos parches de seguridad que van saliendo). Su objetivo es la comprobación de la posibilidad de ejecutar comandos arbitrarios en el servidor atacado. En este caso para realizar la comprobación simplemente prueba de ejecutar un simple comando '*dir*'.

En el caso de los accesos HTTPS vemos que hemos recibidos tres peticiones de conexión. Sin embargo como este servicio no está en funcionamiento no puede causarnos mas problemas que el de recibir tráfico no solicitado.

[91] El sistema de *proxy* más famoso actualmente es el SQUID [WWW91].

192.168.000.002 149.083.020.007 6 **443** 56729 54 54 1 1 11:21:58.8044 11:21:58.8044 2 1
192.168.000.002 149.083.020.007 6 **443** 35268 54 54 1 1 11:23:49.3747 11:23:49.3747 2 1
192.168.000.002 149.083.020.007 6 **443** 56892 54 54 1 1 11:25:21.4252 11:25:21.4252 2 1

A continuación realizaremos otro desglose del tráfico de la red local recibido según el tipo de protocolo (TCP, ICMP, UDP y Otros) al que hacen referencia (ver figura 5-18).

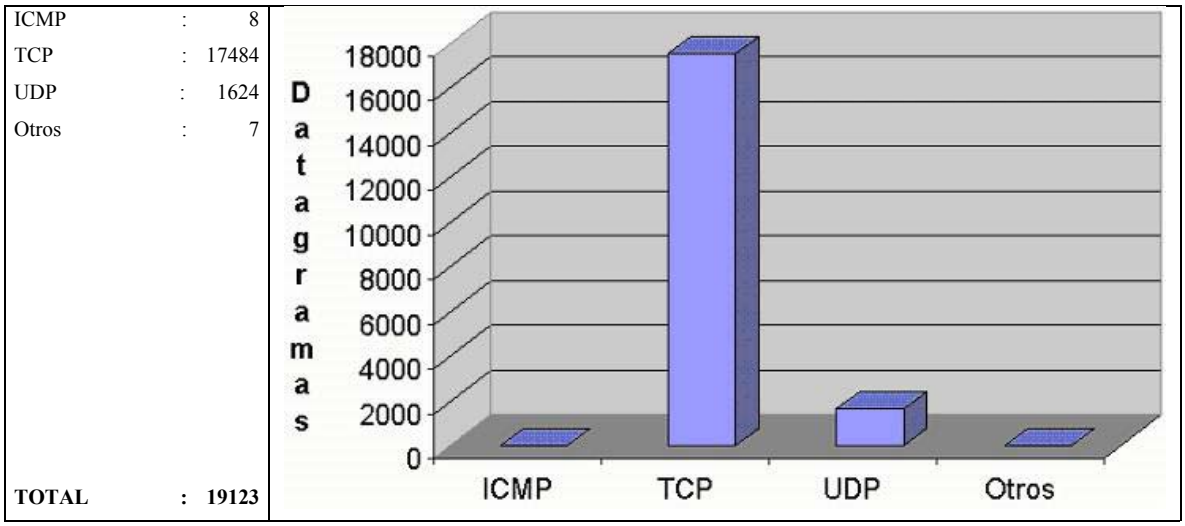


FIG. 5-18: distribución del tráfico del día 21/08/2003 por protocolo.

Lo que realmente nos llamó la atención sobre el tipo de tráfico recibido fueron los siete datagramas clasificados en la categoría de otros:

127.000.000.001 127.000.000.001 **4** 0 0 54 0 1 0 18:34:59.1733 18:34:59.1733 2 2

Este datagrama tiene dirección 127.0.0.1 (dirección local o *loopback* de cualquier ordenador) como origen y destino. Además se identifica como protocolo 4 (inexistente en las especificaciones [Ric98-1]) y se dirige del puerto 0 del ordenador origen al puerto 0 del ordenador destino (los puertos van del 1 al 65535).

Probablemente se trate de un paquete mal construido por algún software de los que tenemos instalado o un *bug* del sistema operativo. En cualquier caso no se ha vuelto a repetir durante el experimento.

000.011.000.000 193.197.192.168 **4** 0 0 7868592 0 3816 0 18:57:42.5740 18:57:53.3571 2 2

Este otro datagrama es también bastante extraño, ya que si bien podemos observar que se identifica perfectamente por la dirección IP de origen (193.197.192.168) no debería haber llegado nunca a nuestra red. Además podemos observar como pertenece a un protocolo inexistente (4) y sus puertos de origen y destino son inválidos.

255.000.000.000 255.255.255.255 **0** 0 0 14 0 1 0 18:57:53.0193 18:57:53.0193 2 2
000.000.000.000 000.000.000.000 **0** 0 0 112 0 8 0 18:57:53.0213 18:58:16.5709 2 2
000.000.000.000 255.255.255.000 **0** 0 0 14 0 1 0 18:57:53.0217 18:57:53.0217 2 2
000.000.000.000 118.118.118.118 **0** 0 0 14 0 1 0 18:57:53.0295 18:57:53.0295 2 2
000.000.000.000 118.118.118.000 **0** 0 0 14 0 1 0 18:57:53.2009 18:57:53.2009 2 2

Análogamente, estos otros datagramas también están construidos de forma anómala. Sin embargo, el hecho de que se registren tan cercanos en el tiempo (entre las 18:57 y las 18:58) y no hayan vuelto a producirse durante la semana, nos hace creer que son paquetes erróneos creados por el *router* o algún software instalado localmente (como por ejemplo el de captura del tráfico).

En cuanto a los datagramas ICMP recibidos son datagramas destinados al puerto de destino 0. Este número de puerto es incorrecto ya que las especificaciones formales de IETF e IANA señalan el rango válido del puerto 1 al 65535.

192.168.000.002 064.014.070.082 **1** 0 769 70 0 1 0 00:00:13.3872 00:00:13.3872 2 2
192.168.000.002 064.014.070.082 **1** 0 769 70 0 1 0 00:30:08.9668 00:30:08.9668 2 2
192.168.000.002 068.213.215.242 **1** 0 771 299 0 1 0 01:06:53.2221 01:06:53.2221 2 2
192.168.000.002 212.033.064.003 **1** 0 771 124 0 1 0 01:30:14.9810 01:30:14.9810 2 2
192.168.000.002 203.036.248.001 **1** 0 771 120 0 1 0 03:00:04.7731 03:00:04.7731 2 2
192.168.000.011 149.083.020.012 **1** 0 0 148 0 2 0 16:22:55.7337 16:23:04.2181 2 2
192.168.000.002 200.164.059.251 **1** 0 769 70 0 1 0 21:45:28.1387 21:45:28.1387 2 2
192.168.000.002 212.033.064.003 **1** 0 771 124 0 1 0 22:01:11.4647 22:01:11.4647 2 2

Probablemente estos paquetes sean ejemplos de intentos de adivinación del sistema operativo existente. La herramienta NMAP (como muchas otras) permite la posibilidad de descubrir el sistema operativo remoto enviando datagramas específicamente construidos (*OS fingerprinting*). Las reacciones del sistema a peticiones al puerto 0 del protocolo ICMP es una de las técnicas más utilizadas.

El resto del tráfico TCP y UDP registrado hace referencia a las peticiones *Netbios/Microsoft-ds* por lo que no serán estudiadas con más profundidad en los informes diarios.

## 5.4.2 Día 22 de Agosto

El día 22 de agosto de 2003 se registraron un total de 14.173 paquetes enviados a nuestra red local. El desglose básico del tráfico clasificado por los principales servicios a los que hace referencia podemos observarlo en la figura 5-19.

| | | |
|---|---|---|
| MAIL | : | 0 |
| SSH | : | 0 |
| TELNET | : | 0 |
| HTTP | : | 5 |
| HTTPS | : | 0 |
| Netbios-ns | : | 205 |
| Netbios-dgm | : | 0 |
| Netbios-ssn | : | 5758 |
| Microsoft-ds | : | 6810 |
| Otros (< 1024) | : | 380 |
| Otros (>=1024) | : | 1015 |
| **TOTAL** | **:** | **14173** |

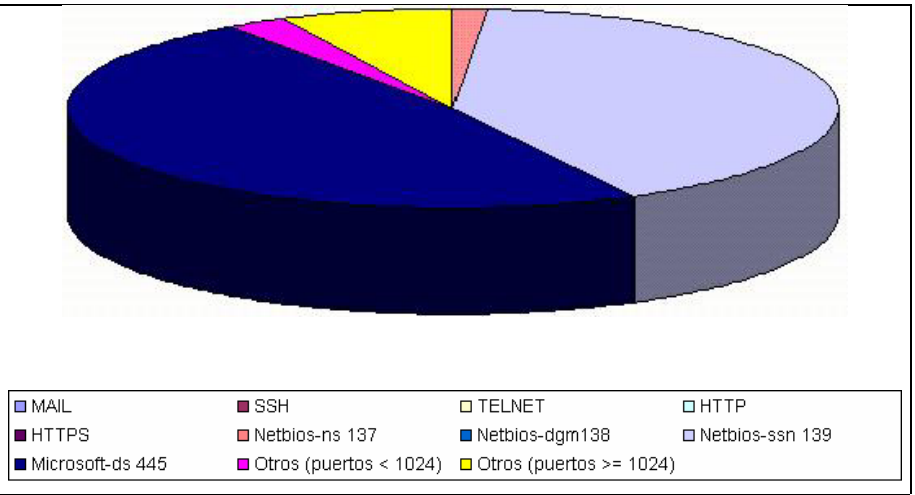


FIG. 5-19: Clasificación del tráfico del día 22/08/2003 por servicio.

Podemos observar nuevamente como el tráfico de los servicios *Netbios/Microsoft-ds* es el gran dominante. También podemos observar la existencia de cinco peticiones realizadas al servicio HTTP:

192.168.000.002 081.096.155.177 6 **80** 4320 427 519 5 4 01:36:19.3746 01:36:36.3773 2 2
192.168.000.002 064.222.171.148 6 **80** 4752 483 458 6 4 01:37:48.3108 01:38:08.2907 2 2
192.168.000.002 195.249.206.242 6 **80** 2852 314 527 5 5 07:09:08.9599 07:09:09.2694 2 2
192.168.000.002 066.183.188.131 6 **80** 1090 300 446 5 5 07:35:45.6170 07:35:46.3324 2 2
192.168.000.002 195.227.096.181 6 **80** 53470 253 503 4 4 23:39:22.6346 23:39:22.9817 2 2

Una vez examinados los logs podemos observar que las peticiones realizadas al servidor WWW se tratan de ataques similares a los registrados el día 21 de Agosto. Vemos que algunas peticiones sondean la existencia de un sistema *proxy* y también ataques a la espera de encontrar un sistema Windows con un servidor Microsoft IIS vulnerable:

```
81.96.155.177    -- [22/Aug/2003:01:36:19 +0200] "OPTIONS / HTTP/1.1" 200 –
195.249.206.242 -- [22/Aug/2003:07:09:09 +0200] "HEAD / HTTP/1.0" 200 0
66.183.188.131   -- [22/Aug/2003:07:35:45 +0200] "OPTIONS * HTTP/1.0" 200 –

195.227.96.181   -- [22/Aug/2003:23:39:22 +0200] "GET /scripts/nsiislog.dll" 404 –
```

Además, al observar el log del servidor WWW vemos una petición nada usual ya que intenta obtener la página principal de http://www.yahoo.com.

```
64.222.171.148   -- [22/Aug/2003:01:37:49 +0200] "GET http://www.yahoo.com/ HTTP/1.1"
```

La idea del atacante es comprobar si existe un servidor WWW mal configurado que permita las referencias a sistemas externos. De esta forma podrían utilizarlo como lanzadera contra otros sitios de Internet.

En la figura 5-20 podemos observar el desglose del tráfico recibido según el tipo de protocolo (TCP, ICMP, UDP y Otros) al que hacen referencia.

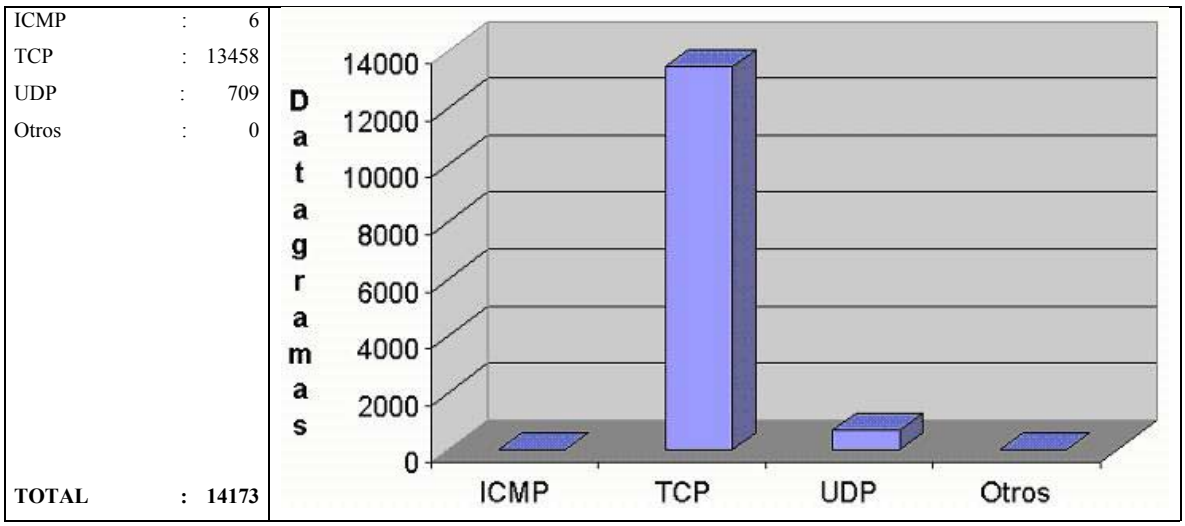


FIG. 5-20: distribución del tráfico del día 22/08/2003 por protocolo.

Observamos que durante el día se han recibido seis datagramas ICMP que presentan dos características comunes inquietantes:

192.168.000.002 193.205.245.008 **1** 0 771 70 0 1 0 01:00:48.9558 01:00:48.9558 2 2
192.168.000.002 212.033.064.003 **1** 0 771 124 0 1 0 03:30:08.6266 03:30:08.6266 2 2
192.168.000.002 200.049.165.248 **1** 0 771 299 0 1 0 10:43:14.0115 10:43:14.0115 2 2
192.168.000.002 080.218.038.007 **1** 0 771 299 0 1 0 17:20:40.2051 17:20:40.2051 2 2
192.168.000.002 209.102.127.086 **1** 0 771 299 0 1 0 23:20:30.3301 23:20:30.3301 2 2
192.168.000.002 200.045.217.105 **1** 0 771 299 0 1 0 23:51:23.0115 23:51:23.0115 2 2

1. Son datagramas ICMP que van destinados al puerto 0 de nuestro servidor local.

2. Todas provienen del mismo puerto de origen (771).

Al igual que parte del tráfico ICMP del día 21, nos encontramos con algunas peticiones que provienen de un mismo puerto [WWW188]. Aunque y que no hemos encontrado en la bibliografía ninguna referencia a posibles ataques, virus o gusanos que presenten estas características, estamos convencidos de que proviene de alguna herramienta específica poco común o no muy extendida actualmente (ya hemos recibido pocas peticiones).

La probabilidad de recibir la misma petición desde dos o más direcciones IP distintas con el mismo puerto de origen es prácticamente nula.

## 5.4.3 Día 23 de Agosto

El día 23 de agosto de 2003 se registraron un total de 10.262 paquetes enviados a nuestra red local. El desglose básico del tráfico clasificado por los principales servicios a los que hace referencia podemos observarlo en la figura 5-21.

Una vez más, el tráfico de los servicios *Netbios/Microsoft-ds* es el más abundante de los registrados. De todo el tráfico recibido destacamos las tres peticiones al servicio HTTP recibidas.

192.168.000.002 217.082.197.149 6 **80** 4900 4154 773 6 6 04:57:33.7074 04:57:34.4797 2 2
192.168.000.002 218.005.066.254 6 **80** 1148 4150 769 6 6 16:43:18.6133 16:43:22.8677 2 2
192.168.000.002 193.115.134.132 6 **80** 4406 307 503 5 4 17:39:39.4002 17:39:39.7001 2 2

Al observar los logs del servidor WWW y ver las peticiones que se han realizado podemos concluir que hemos recibido un ataque en toda regla del virus CodeRed II [WWW184]. Este virus busca servidores WWW de Microsoft para propagarse (*IIS, Internet Information Server*).

217.82.197.149 -- [23/Aug/2003:04:57:34 +0200] "GET /default.ida?XXX……..
218.5.66.254 -- [23/Aug/2003:16:43:21 +0200] "GET /default.ida?XXX……
193.115.134.132 -- [23/Aug/2003:17:39:39 +0200] "GET /scripts/nsiislog.dll" 404 –

| | | |
|---|---|---|
| MAIL | : | 0 |
| SSH | : | 0 |
| TELNET | : | 0 |
| HTTP | : | 3 |
| HTTPS | : | 2 |
| Netbios-ns | : | 186 |
| Netbios-dgm | : | 0 |
| Netbios-ssn | : | 4618 |
| Microsoft-ds | : | 4440 |
| Otros (< 1024) | : | 398 |
| Otros (>=1024) | : | 615 |
| **TOTAL** | **:** | **10262** |

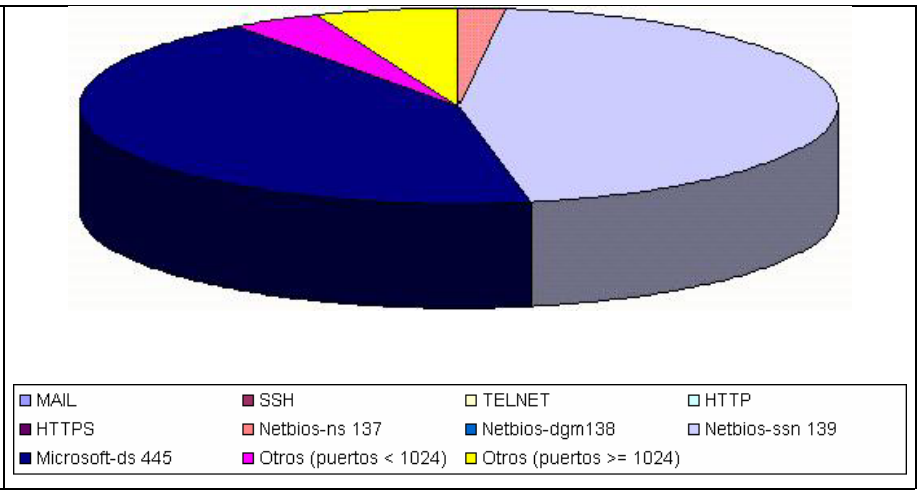


FIG. 5-21: Clasificación del tráfico del día 23/08/2003 por servicio.

En el caso de los accesos al servicio HTTPS vemos que hemos recibidos dos peticiones de conexión. Sin embargo como este servicio no está en funcionamiento no puede causarnos mas problemas que el de recibir tráfico no solicitado.

192.168.000.002 207.044.130.095 6 **443** 34775 74 54 1 1 09:07:30.8778 09:07:30.8780 2 1
192.168.000.002 211.110.012.055 6 **443** 38958 74 54 1 1 09:51:56.5157 09:51:56.5159 2 1

A continuación podemos observar el desglose del tráfico según el tipo de protocolo (TCP, ICMP, UDP y Otros) al que hacen referencia del día 23 en la figura 5-22.

| | | |
|---|---|---|
| ICMP | : | 7 |
| TCP | : | 9706 |
| UDP | : | 549 |
| Otros | : | 0 |
| **TOTAL** | **:** | **10262** |

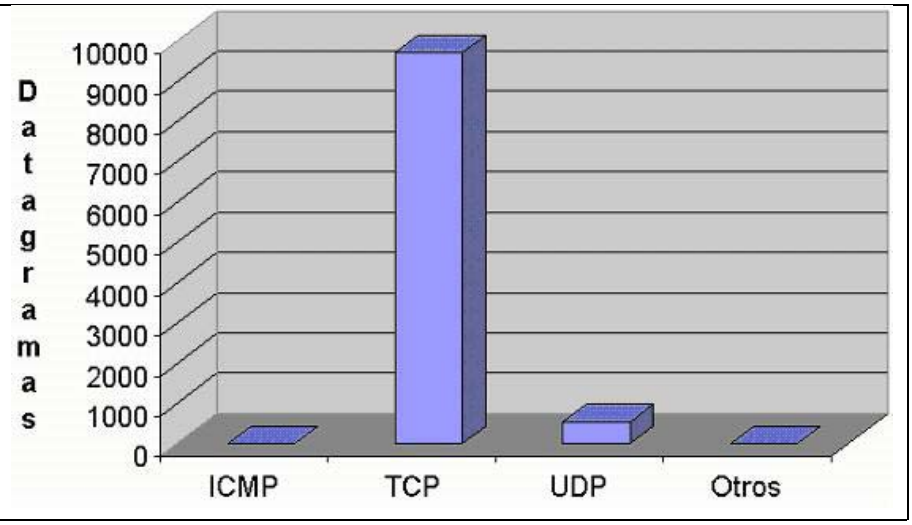


FIG. 5-22: distribución del tráfico del día 23/08/2003 por protocolo.

El día 23 volvemos a observar algunas peticiones ICMP extrañas desde varias direcciones distintas con dos puertos concretos de origen (771 y 781) y con destino el puerto local 0.

192.168.000.002 148.081.027.094 **1** 0 781 70 0 1 0 01:00:49.5464 01:00:49.5464 2 2
192.168.000.002 063.152.127.062 **1** 0 781 350 0 5 0 01:51:18.6785 01:52:49.6403 2 2
192.168.000.002 212.033.064.003 **1** 0 771 123 0 1 0 02:00:14.4856 02:00:14.4856 2 2
192.168.000.002 144.232.018.002 **1** 0 781 70 0 1 0 06:30:14.6294 06:30:14.6294 2 2
192.168.000.002 212.074.093.014 **1** 0 781 70 0 1 0 08:30:25.7445 08:30:25.7445 2 2
192.168.000.002 212.033.064.003 **1** 0 771 124 0 1 0 20:00:14.3016 20:00:14.3016 2 2
192.168.000.002 063.237.032.218 **1** 0 781 140 0 2 0 23:39:01.8081 23:39:04.8241 2 2

## 5.4.4 Día 24 de Agosto

El día 24 de agosto de 2003 se registraron un total de 13.638 paquetes enviados a nuestra red local. El desglose básico del tráfico clasificado por los principales servicios a los que hace referencia podemos observarlo en la figura 5-23.

Como en días anteriores, el tráfico de los servicios *Netbios/Microsoft-ds* es el más abundante de los registrados. También podemos destacar las cinco peticiones al servicio HTTP recibidas:

192.168.000.002 217.162.137.110 6 **80** 1251 4204 1314 7 8 02:47:31.3763 02:47:38.6239 2 1

192.168.000.002 153.109.141.031 6 **80** 1198 311 819 5 4 05:02:45.0445 05:02:45.3621 2 2
192.168.000.002 065.192.064.082 6 **80** 4218 318 531 5 5 09:45:48.9481 09:45:49.4206 2 2
192.168.000.002 217.058.137.120 6 **80** 3632 258 666 4 4 21:19:56.9372 21:19:57.2922 2 2
192.168.000.002 149.099.032.020 6 **80** 3635 309 886 5 4 22:02:02.1511 22:02:02.8126 2 2

Una vez más analizamos los logs del servidor WWW para intentar descubrir el objetivo de estas peticiones. Al igual que en los días anteriores recibimos intentos de ataques a sistemas Windows y servidores IIS así como pruebas de las capacidades *proxy* que podría presentar nuestro servidor.

217.58.137.120 -- [24/Aug/2003:21:19:57 +0200] "GET /msadc/msadcs.dll HTTP/1.0" 404 275
217.162.137.110 -- [24/Aug/2003:02:47:35 +0200] "GET /default.ida?XXX%u9090%u6858%ucbd3
%u7801%u9090%u6858%ucbd3%u7801%u9090%u
6858%ucbd3%u7801%u9090%u9090%u8190%u00
c3%u0003%u8b00%u531b%u53ff%u0078%u0000
%u00=a HTTP/1.0" 404 270

153.109.141.31 -- [24/Aug/2003:05:02:45 +0200] "CONNECT 1.3.3.7:1337 HTTP/1.0" 405 296
65.192.64.82 -- [24/Aug/2003:09:45:49 +0200] "HEAD / HTTP/1.0" 200 0
149.99.32.20 -- [24/Aug/2003:22:02:02 +0200] "SEARCH / HTTP/1.1" 501 331

| | | |
|---|---|---|
| MAIL | : | 0 |
| SSH | : | 0 |
| TELNET | : | 0 |
| HTTP | : | 5 |
| HTTPS | : | 2 |
| Netbios-ns | : | 153 |
| Netbios-dgm | : | 0 |
| Netbios-ssn | : | 6222 |
| Microsoft-ds | : | 6167 |
| Otros (< 1024) | : | 457 |
| Otros (>=1024) | : | 632 |
| **TOTAL** | **:** | **13638** |

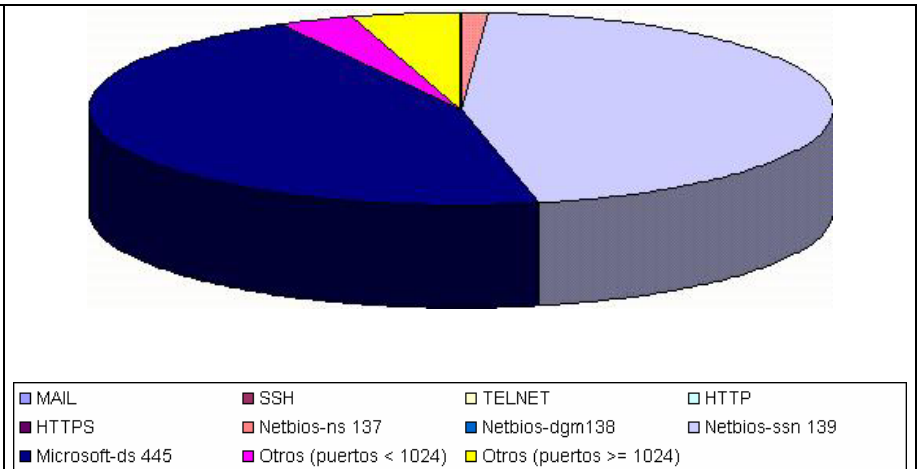


FIG. 5-23: Clasificación del tráfico del día 24/08/2003 por servicio.

A continuación en la figura 5-24 realizaremos un el desglose de todo el tráfico recibido durante el día según el tipo de protocolo (TCP, ICMP, UDP y Otros) al que hacen referencia.

| | | |
|---|---|---|
| ICMP | : | 6 |
| TCP | : | 12988 |
| UDP | : | 644 |
| Otros | : | 0 |
| **TOTAL** | **:** | **13638** |

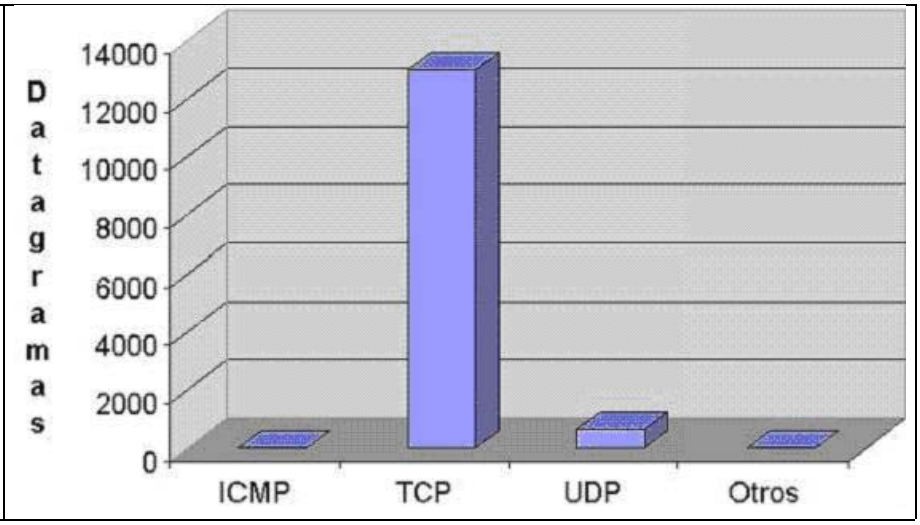


FIG. 5-24: distribución del tráfico del día 24/08/2003 por protocolo.

Al igual que en los días anteriores registramos algunas peticiones ICMP extrañas desde varias direcciones distintas con el puerto de origen 771 y con destino el puerto local 0.

192.168.000.002 198.005.241.058 **1** 0 771 234 0 2 0 04:01:06.8198 04:01:06.8295 2 2
192.168.000.002 212.033.064.003 **1** 0 771 124 0 1 0 05:30:20.7972 05:30:20.7972 2 2
192.168.000.002 217.096.223.189 **1** 0 771 299 0 1 0 05:57:56.3417 05:57:56.3417 2 2
192.168.000.002 211.158.093.040 **1** 0 771 299 0 1 0 11:21:30.9523 11:21:30.9523 2 2
192.168.000.002 212.033.064.003 **1** 0 771 124 0 1 0 13:30:14.9085 13:30:14.9085 2 2
192.168.000.002 203.148.128.017 **1** 0 771 299 0 1 0 23:12:22.1506 23:12:22.1506 2 2

## 5.4.5 Día 25 de Agosto

El día 25 de agosto de 2003 se registraron un total de 10.566 paquetes enviados a nuestra red local. El desglose básico del tráfico clasificado por los principales servicios a los que hace referencia podemos observarlo en la figura 5-25.

Como en días anteriores, el tráfico de los servicios *Netbios/Microsoft-ds* es el más abundante de los registrados. Podemos observar la existencia de varias peticiones externas "simultáneas" al servicio SSH de nuestra red local desde una dirección IP idéntica:

| | | |
|---|---|---|
| MAIL | : | 0 |
| SSH | : | 3 |
| TELNET | : | 0 |
| HTTP | : | 1 |
| HTTPS | : | 0 |
| Netbios-ns | : | 230 |
| Netbios-dgm | : | 0 |
| Netbios-ssn | : | 4544 |
| Microsoft-ds | : | 4549 |
| Otros (< 1024) | : | 534 |
| Otros (>=1024) | : | 705 |
| **TOTAL** | **:** | **10566** |

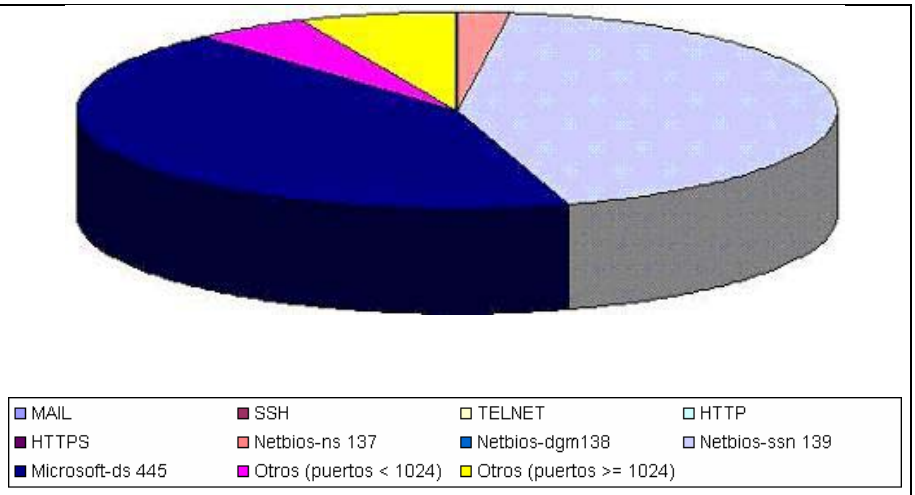


FIG. 5-25: Clasificación del tráfico del día 25/08/2003 por servicio.

192.168.000.002 213.201.169.102 6 22 29311 350 183 5 2 19:50:38.5318 19:50:42.0202 2 2
192.168.000.002 213.201.169.102 6 22 29455 2518 3371 18 20 19:50:41.9192 19:51:58.1431 2 2
192.168.000.002 213.201.169.102 6 22 29542 2584 3297 19 19 19:50:45.1521 19:51:59.7611 2 2

Tras analizar detenidamente el flujo de las conexiones (ver figura 5-26) observamos que las peticiones realizan conexiones (SYN) y desconexiones (RST) rápidamente sin realizar ningún intercambio de datos (Len=0) por lo que probablemente el atacante buscaba un servidor SSH vulnerable a este ataque.

También podemos observar como se ha recibido una única petición al servicio HTTP durante todo el día.

192.168.000.002 209.157.068.242 6 **80** 1380 307 503 5 4 14:47:55.3717 14:47:56.0154 2 2

209.157.68.242 - - [25/Aug/2003:14:47:55 +0200] "GET /scripts/nsiislog.dll" 404 -

Una vez más el análisis de los logs del servidor nos revela que se trataba de un ataque en busca de un sistema operativo Windows mal configurado o no actualizado con IIS como servidor WWW.

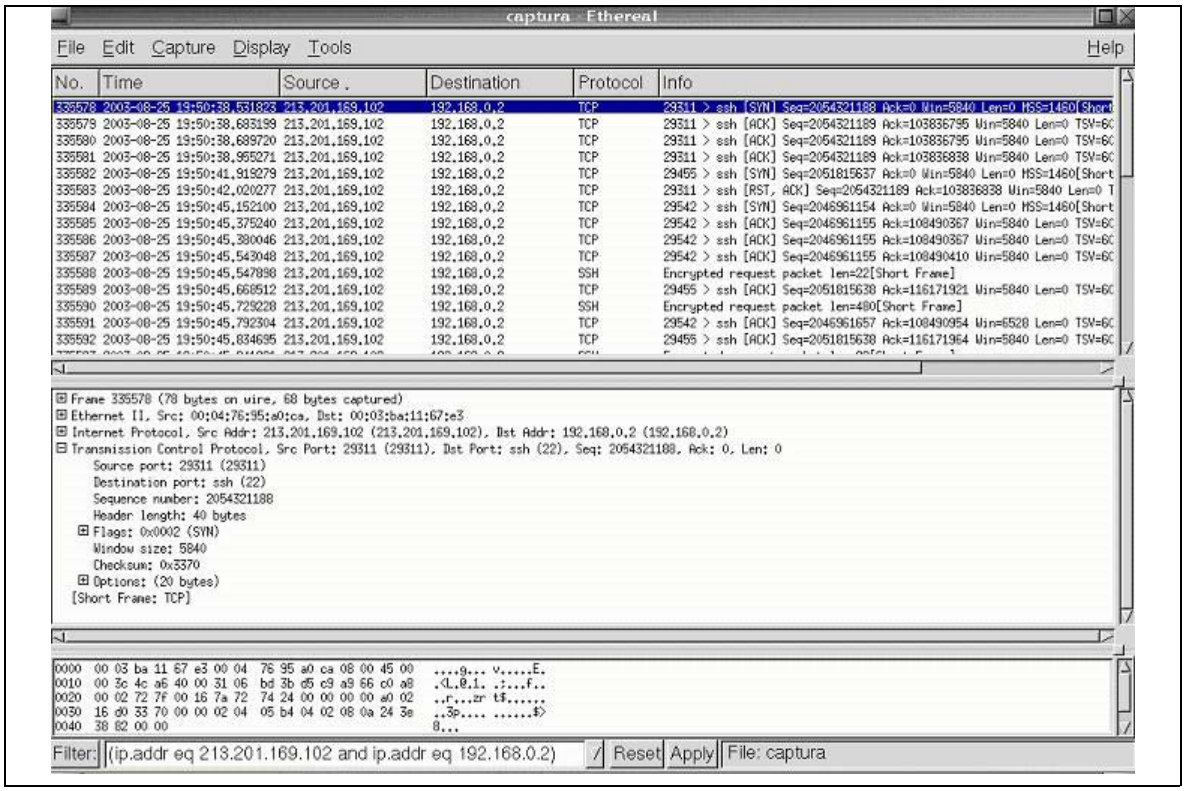


FIG. 5-26: Análisis del tráfico SSH recibido el día 25/08/2003.

A continuación podemos observar el desglose del tráfico del día 25 según el tipo de protocolo (TCP, ICMP, UDP y Otros) al que hacen referencia en la figura 5-27.

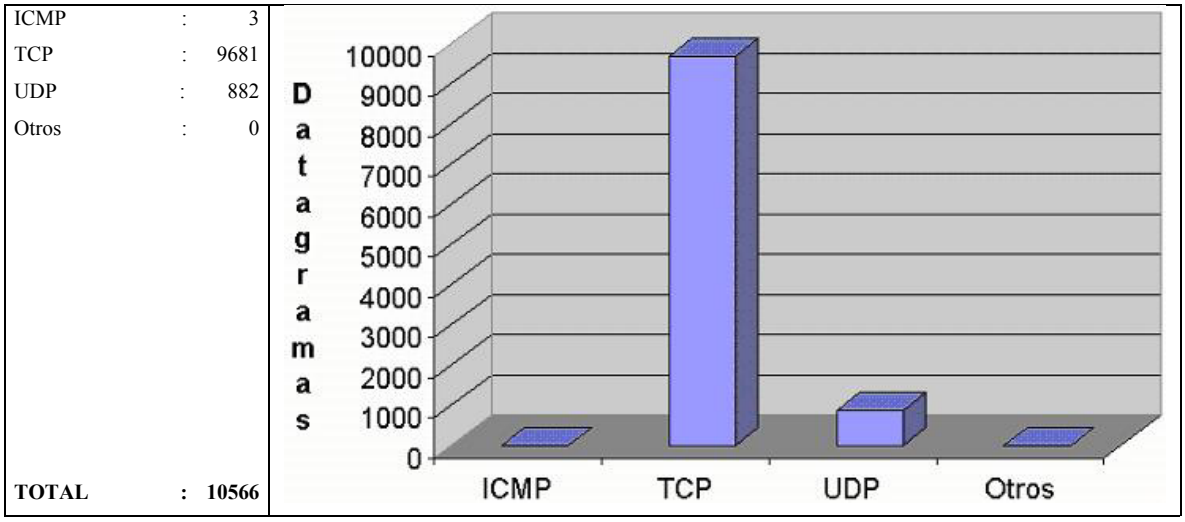


FIG. 5-27: distribución del tráfico del día 25/08/2003 por protocolo.

Como en los días precedentes registramos algunas peticiones ICMP extrañas desde varias direcciones distintas con el puerto de origen 769, 771 o 781 y con destino el puerto 0.

192.168.000.002 196.025.249.070 **1** 0 781 70 0 1 0 13:00:17.5611 13:00:17.5611 2 2
192.168.000.002 080.058.036.083 **1** 0 769 70 0 1 0 14:30:40.7625 14:30:40.7625 2 2
192.168.000.002 212.033.064.003 **1** 0 771 124 0 1 0 17:30:19.8907 17:30:19.8907 2 2

## 5.4.6 Día 26 de Agosto

El día 26 de agosto de 2003 se registraron un total de 7.904 paquetes enviados a nuestra red local. El desglose básico del tráfico clasificado por los principales servicios a los que hace referencia podemos observarlo en la figura 5-28.

| | | |
|---|---|---|
| MAIL | : | 1 |
| SSH | : | 0 |
| TELNET | : | 0 |
| HTTP | : | 9 |
| HTTPS | : | 0 |
| Netbios-ns | : | 236 |
| Netbios-dgm | : | 0 |
| Netbios-ssn | : | 3517 |
| Microsoft-ds | : | 3232 |
| Otros (< 1024) | : | 532 |
| Otros (>=1024) | : | 377 |
| **TOTAL** | **:** | **7904** |

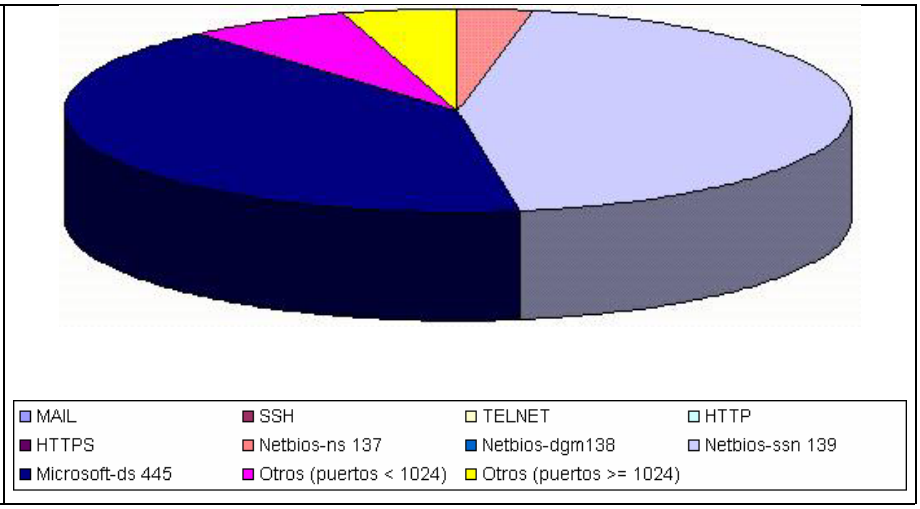


FIG. 5-28: Clasificación del tráfico del día 26/08/2003 por servicio.

Como en días anteriores, el tráfico de los servicios *Netbios/Microsoft-ds* es el más abundante de los registrados. Se ha recibido una única petición de conexión al servicio de MAIL:

192.168.000.002 211.213.123.254 6 **25** 1969 601 624 9 9 22:18:26.2661 22:18:29.8132 2 1

Tras realizar un análisis exhaustivo de los logs del sistema, comprobamos con estupor (ver figura 5-29) cómo el objetivo de esta comunicación es el de comprobar si nuestro sistema de MAIL permite el envío de correos electrónicos a cualquier dirección sin restricciones (*open relaying*). Este tipo de búsquedas persiguen encontrar servidores SMTP mal configurados de forma que puedan ser aprovechados para el envío de correo basura (*spam*).

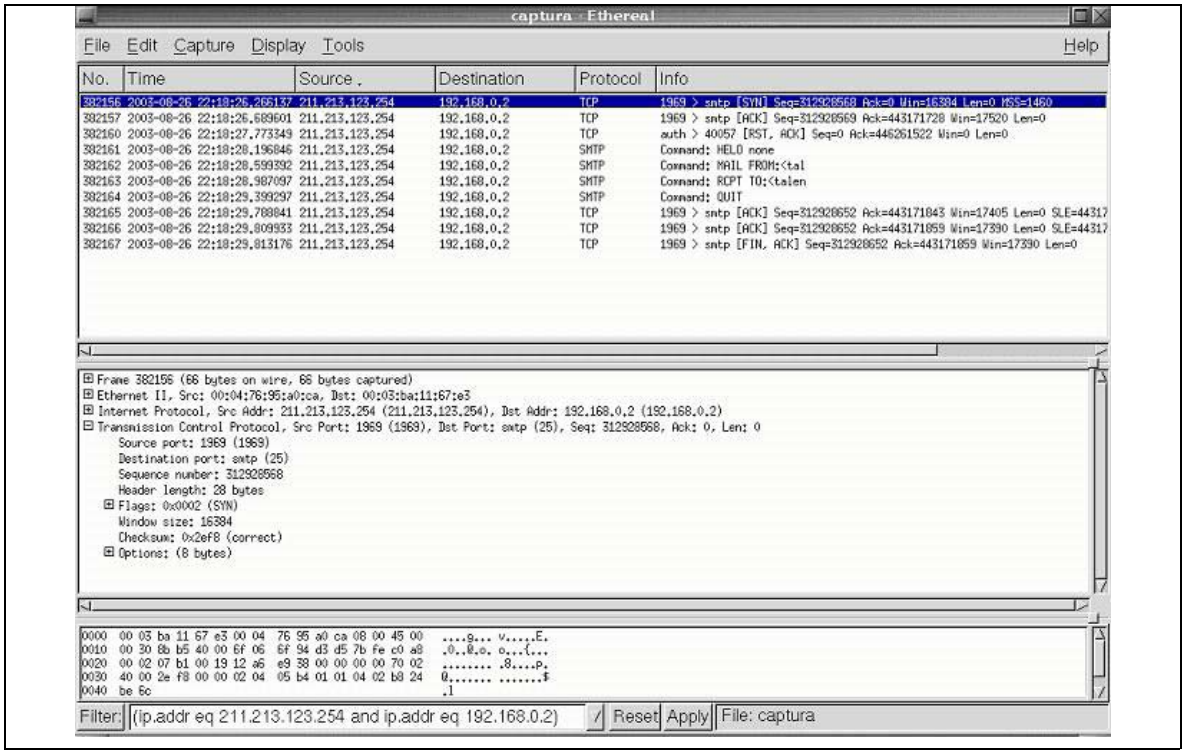


FIG. 5-29: Conexión al servicio MAIL del día 26/08/2003.

En cuanto a las nueve peticiones recibidas al servicio HTTP podemos desglosarlas en dos grupos según su objetivo. En el primer grupo encontramos las peticiones típicas que hacen referencia a la búsqueda de sistemas operativos Windows con servidores IIS mal configurados o no actualizados así como sondeos en búsqueda de capacidades *proxy* de nuestro servidor WWW.

192.168.000.002 217.132.036.071 6 **80** 2824 4150 769 6 6 02:05:07.9312 02:05:13.9552 2 2
192.168.000.002 065.204.029.059 6 **80** 4014 307 503 5 4 04:44:29.1234 04:44:29.7457 2 2
192.168.000.002 204.210.077.240 6 **80** 4395 307 503 5 4 08:14:24.1462 08:14:24.7506 2 2
192.168.000.002 062.255.181.048 6 **80** 18996 307 503 5 4 10:52:30.4965 10:52:32.0998 2 2
192.168.000.002 081.096.155.177 6 **80** 4336 481 519 6 4 12:41:45.7628 12:43:02.1234 2 2
192.168.000.002 081.096.155.177 6 **80** 4545 481 519 6 4 12:49:03.4079 12:50:22.3072 2 2

```
217.132.36.71    -- [26/Aug/2003:02:05:11 +0200] "GET /default.ida?XXX%u9090%u6858%ucbd3
                                                 %u7801%u9090%u6858%ucbd3%u7801%u9090%u
                                                 6858%ucbd3%u7801%u9090%u9090%u8190%u00
                                                 c3%u0003%u8b00%u531b%u53ff%u0078%u0000
                                                 %u00=a  HTTP/1.0" 404 270
65.204.29.59     -- [26/Aug/2003:04:44:29 +0200] "GET /scripts/nsiislog.dll" 404 –
204.210.77.240   -- [26/Aug/2003:08:14:24 +0200] "GET /scripts/nsiislog.dll" 404 –
62.255.181.48    -- [26/Aug/2003:10:52:31 +0200] "GET /scripts/nsiislog.dll" 404 –

81.96.155.177    -- [26/Aug/2003:12:41:45 +0200] "OPTIONS / HTTP/1.1" 200 -
```

En el segundo grupo podemos encontrar unas peticiones con direcciones de origen y destino que no se corresponden a nuestra red local. Incomprensiblemente estas peticiones han llegado a nosotros.

```
064.028.067.150 216.027.178.155 6 80 32771 18396 428911 210 315 19:09:30.1146 19:10:09.8144 2 2
064.028.067.114 216.027.178.155 6 80 32772 5929 3906 35 28 19:09:34.8245 19:10:10.4744 2 1
064.028.067.057 216.027.178.155 6 80 32773 5460 22176 28 28 19:09:34.8250 19:10:10.3946 2 2
```

Después de verificar la integridad del servidor tres veces así como comprobar toda la arquitectura desplegada, no hemos podido dar una respuesta satisfactoria a este fenómeno. Podríamos especular asumiendo que de alguna forma desconocida un atacante ha logrado utilizar nuestro servidor WWW como sistema *proxy* y ha lanzado algunas peticiones hacia otras máquinas conectadas a Internet. Sin embargo este punto no es demostrable ya que los logs del servidor WWW no reflejan este comportamiento.

El tráfico recibido por nuestra red el día 26 según el tipo de protocolo (TCP, ICMP, UDP y Otros) al que hacen referencia se puede observar en la figura 5-30.

Como en los días precedentes registramos algunas peticiones ICMP extrañas desde varias direcciones distintas con los puertos de origen 769, 771 o 781 y con destino el puerto local 0.

```
192.168.000.002 063.147.015.158 1 0 781 210 0 3 0 01:00:08.3430 01:00:29.5400 2 2
192.168.000.002 212.033.064.003 1 0 771 124 0 1 0 03:30:52.5577 03:30:52.5577 2 2
192.168.000.002 211.128.153.100 1 0 771 299 0 1 0 18:36:30.7620 18:36:30.7620 2 2
192.168.000.002 064.014.070.082 1 0 769 70 0 1 0 19:00:07.2113 19:00:07.2113 2 2
192.168.000.002 064.014.070.082 1 0 769 70 0 1 0 19:30:29.2648 19:30:29.2648 2 2
```

| | | |
|---|---|---|
| ICMP | : | 5 |
| TCP | : | 7377 |
| UDP | : | 522 |
| Otros | : | 0 |
| **TOTAL** | **:** | **7904** |

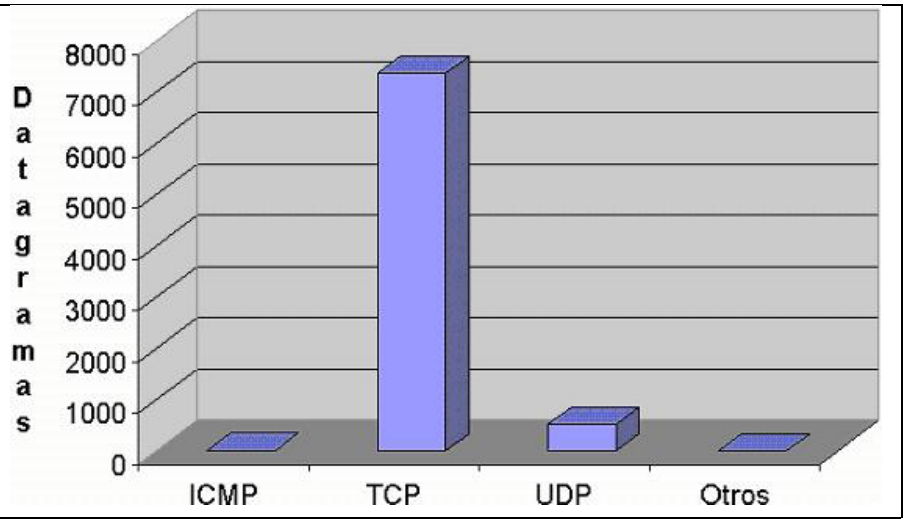


FIG. 5-30: distribución del tráfico del día 26/08/2003 por protocolo.

## 5.4.7 Día 27 de Agosto

El último día del estudio (27 de agosto de 2003) se registraron un total de 10.016 paquetes enviados a nuestra red local. El desglose básico del tráfico clasificado por los principales servicios a los que hace referencia podemos observarlo en la figura 5-31.

| | | |
|---|---|---|
| MAIL | : | 1 |
| SSH | : | 0 |
| TELNET | : | 0 |
| HTTP | : | 22 |
| HTTPS | : | 206 |
| Netbios-ns | : | 0 |
| Netbios-dgm | : | 0 |
| Netbios-ssn | : | 4468 |
| Microsoft-ds | : | 4528 |
| Otros (< 1024) | : | 516 |
| Otros (>=1024) | : | 275 |
| **TOTAL** | **:** | **10016** |

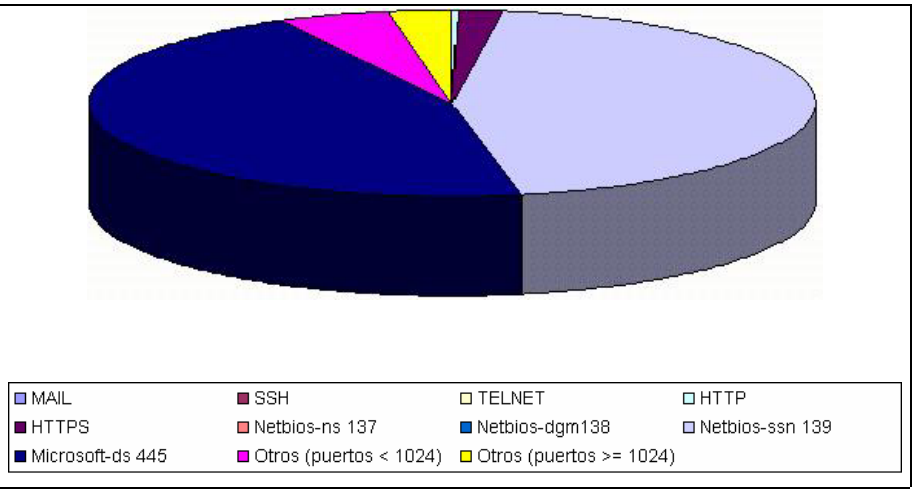


FIG. 5-31: Clasificación del tráfico del día 27/08/2003 por servicio.

Como a lo largo de la semana, el tráfico de los servicios *Netbios/Microsoft-ds* es el más abundante de los registrados. Se ha recibido una petición de conexión al servicio de MAIL al igual que el día 26.

192.168.000.002 218.187.145.024 6 **25** 4681 524 624 8 9 23:28:42.0097 23:28:48.3334 2 1

En análisis de los logs del sistema (ver figura 5-32) nos revela otro intento de búsqueda de un servidor SMTP mal configurado para enviar correo basura.

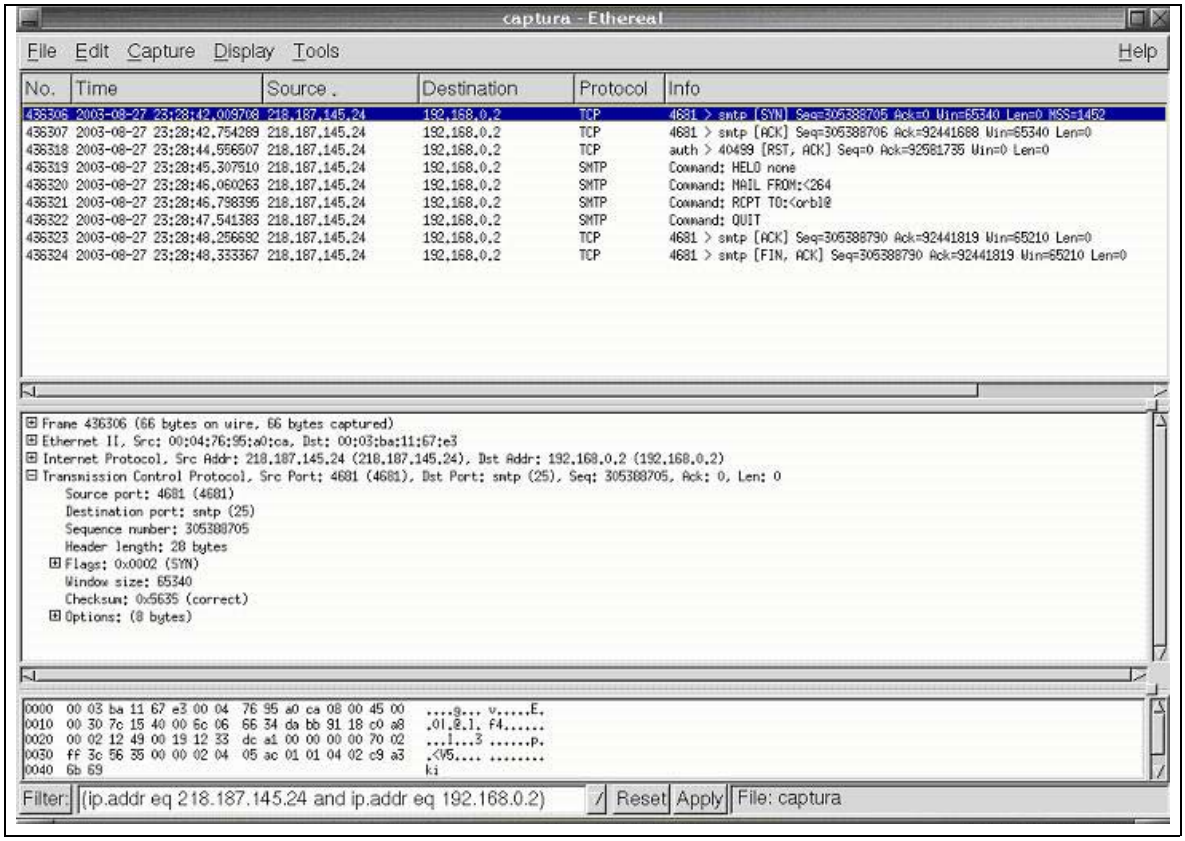


FIG. 5-32: Conexión al servicio MAIL del día 27/08/2003.

En cuanto a las veintidós peticiones recibidas al servicio HTTP podemos desglosarlas en dos grupos según su objetivo. En el primer grupo encontramos las peticiones típicas que hacen referencia a la búsqueda de sistemas operativos Windows con servidores IIS mal configurados o no actualizados y la búsqueda de capacidades *proxy* en nuestro servidor WWW.

192.168.000.002 193.109.252.040 6 **80** 14195 307 503 5 4 10:21:56.9267 10:21:57.6223 2 2
192.168.000.002 217.219.176.067 6 **80** 2455 4150 1260 6 7 15:46:50.3296 15:46:59.3141 2 2
192.168.000.002 066.061.120.188 6 **80** 2504 481 519 6 4 21:00:29.8647 21:01:06.1925 2 2
192.168.000.002 066.061.120.188 6 **80** 2673 481 519 6 4 21:01:32.7518 21:01:59.8359 2 2
192.168.000.002 066.061.120.188 6 **80** 2777 481 519 6 4 21:02:38.3551 21:03:18.9421 2 2
192.168.000.002 066.061.120.188 6 **80** 2837 481 519 6 4 21:03:40.2760 21:04:22.1193 2 2
192.168.000.002 066.061.120.188 6 **80** 2926 481 519 6 4 21:04:43.8393 21:05:04.2428 2 2
192.168.000.002 066.061.120.188 6 **80** 3139 481 519 6 4 21:05:48.5335 21:06:07.8909 2 2
192.168.000.002 066.061.120.188 6 **80** 3362 481 519 6 4 21:06:55.7435 21:07:15.3924 2 2
192.168.000.002 066.061.120.188 6 **80** 3494 481 519 6 4 21:07:59.0118 21:08:22.0239 2 2
192.168.000.002 066.061.120.188 6 **80** 3613 481 519 6 4 21:09:04.2583 21:09:25.8365 2 2
192.168.000.002 066.061.120.188 6 **80** 3804 481 519 6 4 21:10:09.8095 21:10:29.9816 2 2
192.168.000.002 066.061.120.188 6 **80** 4016 481 519 6 4 21:11:17.3926 21:11:53.2347 2 2
192.168.000.002 066.061.120.188 6 **80** 4203 481 519 6 4 21:12:21.0080 21:12:59.1493 2 2
192.168.000.002 066.061.120.188 6 **80** 4317 481 519 6 4 21:13:27.6786 21:13:55.3460 2 2
192.168.000.002 066.061.120.188 6 **80** 4424 481 519 6 4 21:14:30.2513 21:14:48.3605 2 2

193.109.252.40 -- [27/Aug/2003:10:21:57 +0200] "GET /scripts/nsiislog.dll" 404 –

217.219.176.67 -- [27/Aug/2003:15:46:55 +0200] "GET /default.ida?XXX%u9090%u6858
%ucbd3%u7801%u9090%u6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9
090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a
HTTP/1.0" 404 270

66.61.120.188 - - [27/Aug/2003:21:00:30 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:01:32 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:02:38 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:03:40 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:04:44 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:05:48 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:06:55 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:07:59 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:09:04 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:10:10 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:11:17 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:12:21 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:13:27 +0200] "OPTIONS / HTTP/1.1" 200 -
66.61.120.188 - - [27/Aug/2003:21:14:30 +0200] "OPTIONS / HTTP/1.1" 200 -

En el segundo grupo podemos encontrar una serie de peticiones encargadas de comprobar la existencia de soporte PHP[91] en nuestro servidor WWW. De esta manera suponemos que el atacante buscaba los ficheros típicos de ejemplo (*test.php* o *index.php*) con el objetivo de utilizar algún fallo de seguridad en el PHP para conseguir en control del servidor.

192.168.000.002 217.005.080.066 6 **80** 3878 296 531 5 5 15:16:50.6699 15:16:51.6214 2 2
192.168.000.002 217.005.080.066 6 **80** 3968 358 713 5 5 15:16:55.2389 15:16:55.9981 2 2
192.168.000.002 217.005.080.066 6 **80** 3969 116 124 2 2 15:16:55.2420 15:16:59.3987 2 2
192.168.000.002 217.005.080.066 6 **80** 3970 360 715 5 5 15:16:55.2469 15:16:56.0469 2 2
192.168.000.002 217.005.080.066 6 **80** 3971 357 712 5 5 15:16:55.2551 15:16:56.0941 2 1
192.168.000.002 217.005.080.066 6 **80** 3972 359 714 5 5 15:16:55.2599 15:16:56.1463 2 2

[91] Para más información consultar la bibliografía [WW196].

```
217.5.80.66 - - [27/Aug/2003:15:16:51 +0200] "GET / HTTP/1.0" 200 0
217.5.80.66 - - [27/Aug/2003:15:16:55 +0200] "GET /index.php HTTP/1.0" 404 268
217.5.80.66 - - [27/Aug/2003:15:16:55 +0200] "GET /phpinfo.php HTTP/1.0" 404 270
217.5.80.66 - - [27/Aug/2003:15:16:55 +0200] "GET /test.php HTTP/1.0" 404 267
217.5.80.66 - - [27/Aug/2003:15:16:55 +0200] "GET /index.php3 HTTP/1.0" 404 269
```

A continuación podemos observar el desglose del tráfico del día 27 según el tipo de protocolo (TCP, ICMP, UDP y Otros) al que hacen referencia en la figura 5-33.

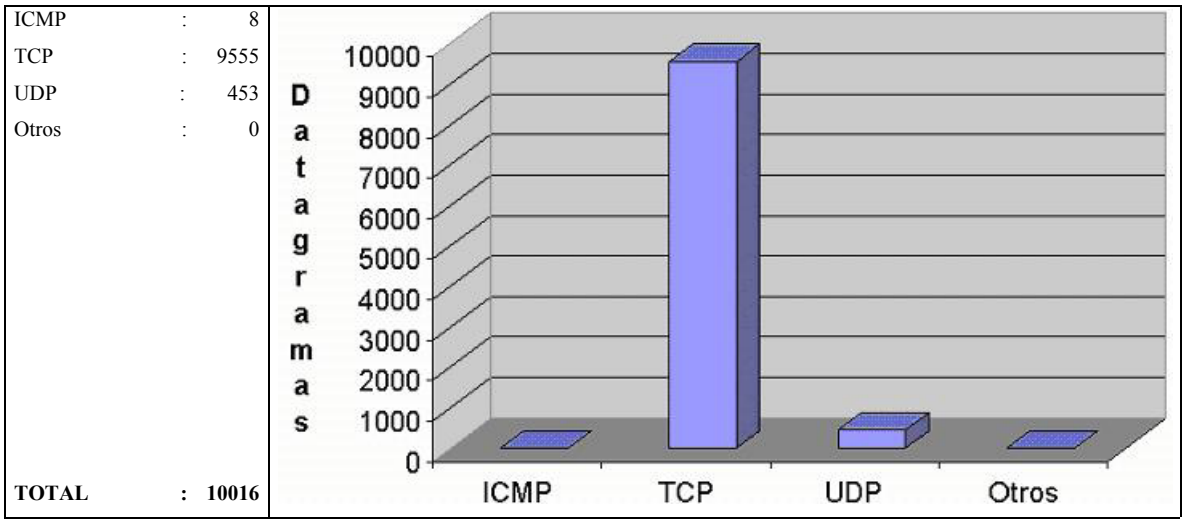


FIG. 5-33: distribución del tráfico del día 27/08/2003 por protocolo.

Como ha ido sucediendo durante toda la semana, volvemos a registrar algunas peticiones ICMP extrañas desde varias direcciones distintas con el puerto de origen 771 o 781 y con destino el puerto 0.

```
192.168.000.002 212.033.064.003 1 0 771 124 0 1 0 00:00:43.0555 00:00:43.0555 2 2
192.168.000.002 207.217.120.013 1 0 771 126 0 1 0 01:00:45.2312 01:00:45.2312 2 2
192.168.000.002 212.074.093.014 1 0 781 140 0 2 0 02:30:04.7845 02:30:06.7920 2 2
192.168.000.002 212.033.064.003 1 0 771 124 0 1 0 10:31:24.2288 10:31:24.2288 2 2
192.168.000.002 063.152.126.150 1 0 781 210 0 3 0 17:01:36.9837 17:02:19.1822 2 2
192.168.000.002 198.067.128.010 1 0 771 70 0 1 0 18:00:34.0981 18:00:34.0981 2 2
192.168.000.002 209.042.047.067 1 0 771 70 0 1 0 18:00:55.8393 18:00:55.8393 2 2
192.168.000.002 200.088.008.230 1 0 771 70 0 1 0 22:27:37.3687 22:27:37.3687 2 2
```

## 5.4.8 Resumen semanal

Una vez realizado el estudio pormenorizado del tráfico recibido cada día de la semana, pasaremos a presentar el informe resumido de toda la semana dónde destacaremos los elementos más importantes.

En la figura 5-34 podemos apreciar la evolución de la distribución del tráfico que se ha generado durante toda la semana. Podemos observar cómo desde el primer día del experimento el tráfico se ha reducido hasta estabilizarse en unas 11.000 peticiones diarias de media.

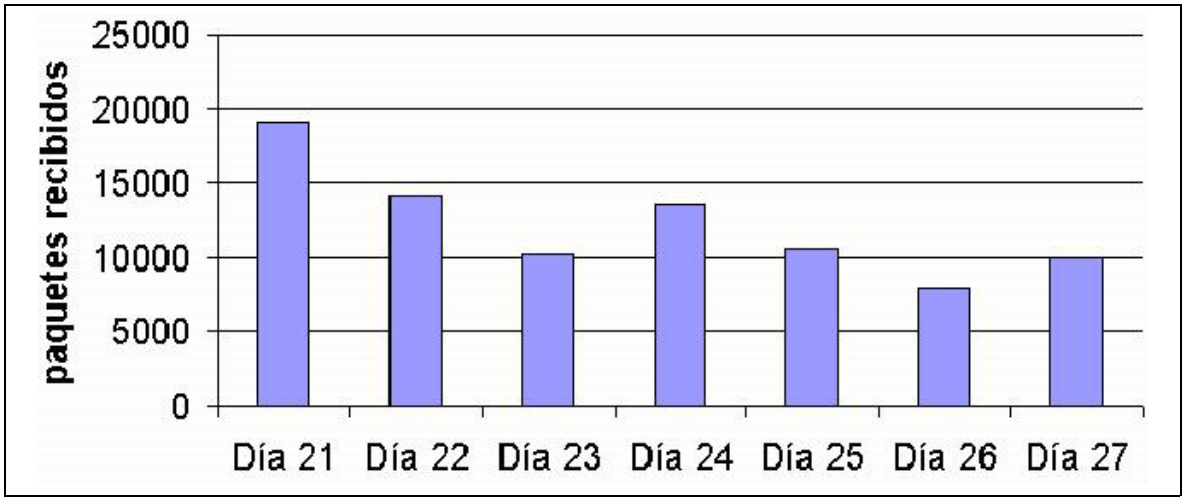


FIG. 5-34: Evolución del tráfico semanal.

El número de peticiones recibidas el día 21 es muy superior (casi el doble) que la media de peticiones semanal. Podemos explicar este hecho basándonos en que prácticamente todas las conexiones existentes en nuestra red de pruebas fueron interrumpidas bruscamente el día 21 para iniciar este experimento. Consecuentemente, los otros extremos de la comunicación enviaban peticiones de servicio durante un tiempo hasta que abandonaban.

En la figura 5-35 podemos observar la distribución semanal de todo el tráfico registrado (85.682 paquetes) por servicio al que hacen referencia.

| | | |
|---|---|---|
| MAIL | : | 12 |
| SSH | : | 7 |
| TELNET | : | 0 |
| HTTP | : | 53 |
| HTTPS | : | 213 |
| Netbios-ns | : | 1243 |
| Netbios-dgm | : | 4 |
| Netbios-ssn | : | 34382 |
| Microsoft-ds | : | 35586 |
| Otros (< 1024) | : | 6388 |
| Otros (>=1024) | : | 7794 |
| **TOTAL** | **:** | **85682** |

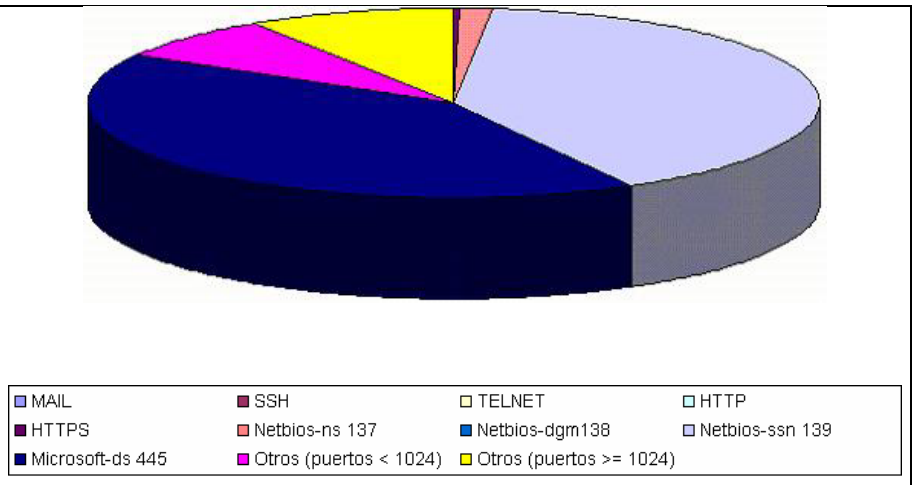


FIG. 5-35: Clasificación semanal del tráfico por servicio.

Podemos observar como las peticiones a los servicios *Netbios/Microsoft-ds* acaparan más del 83% del tráfico registrado. El resto del tráfico se distribuye entre peticiones a puertos distintos de los servicios típicos existentes en el sistema (16%) y minoritariamente (1%) en peticiones y ataques a los servicios de red.

En cuanto a la distribución del tráfico por protocolo (ver figura 5-36), observamos que la mayoría es TCP (93%) y UDP (6%) que mayoritariamente referencia peticiones *Netbios/Microsoft-ds*. El resto corresponde a peticiones anómalas (como las de ICMP).

| | | |
|---|---|---|
| ICMP | : | 43 |
| TCP | : | 80249 |
| UDP | : | 5383 |
| Otros | : | 7 |
| **TOTAL** | **:** | **85682** |

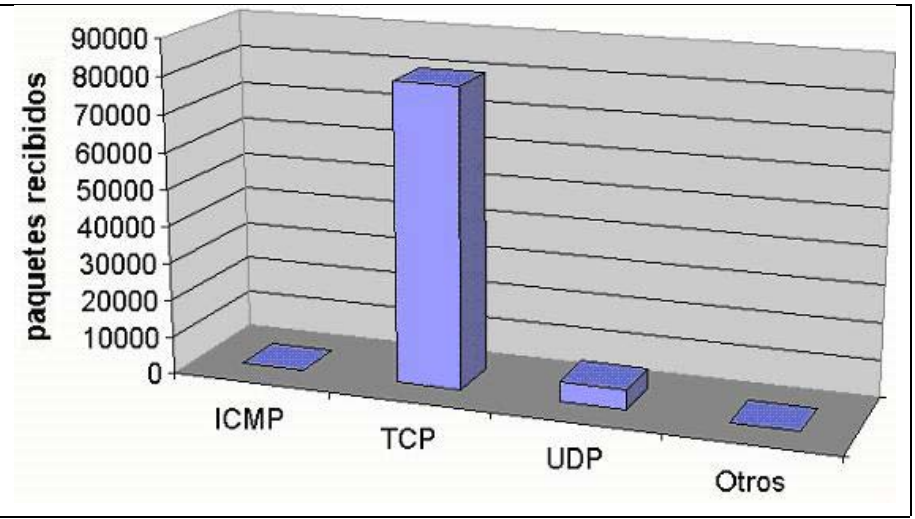


FIG. 5-36: distribución del tráfico semanal por protocolo.

Finalmente en las figuras 5-37 y 5-38 visualizamos una partición del tráfico que ha circulado por nuestra red local (en bytes) según el protocolo al que hace referencia (TCP, UDP, ICMP y otros) y a la dirección de la transmisión que llevaba (si era de entrada hacia nuestra red local o era de salida hacia Internet).

Así mismo podemos observar que la cantidad total de tráfico que ha circulado durante la semana por nuestra red local es de casi 90Mbytes (92.754.552 bytes), lo que realmente es una cantidad de información a tener en cuenta.

| TCP out | UDP in | UDP out | ICMP in | ICMP out | Otros in | Otros out | TOTAL |
|---|---|---|---|---|---|---|---|
| 6784084 | 351798 | 62059 | 1025 | 0 | 168 | 0 | 15064488 |
| 7727861 | 243888 | 68292 | 1390 | 0 | 0 | 0 | 17178892 |
| 5053918 | 69870 | 50406 | 947 | 0 | 0 | 0 | 11312049 |
| 7229306 | 100823 | 68834 | 1379 | 0 | 0 | 0 | 15787368 |
| 5259042 | 138265 | 62059 | 264 | 0 | 0 | 0 | 13671205 |
| 4179911 | 63446 | 68282 | 773 | 0 | 0 | 0 | 8846844 |
| 4929469 | 58604 | 67750 | 934 | 0 | 0 | 0 | 10893706 |
| | | | | | | | |
| | | | | | | | **92.754.552** |

FIG. 5-37: Cantidad de bytes que han circulado en la LAN por protocolo.

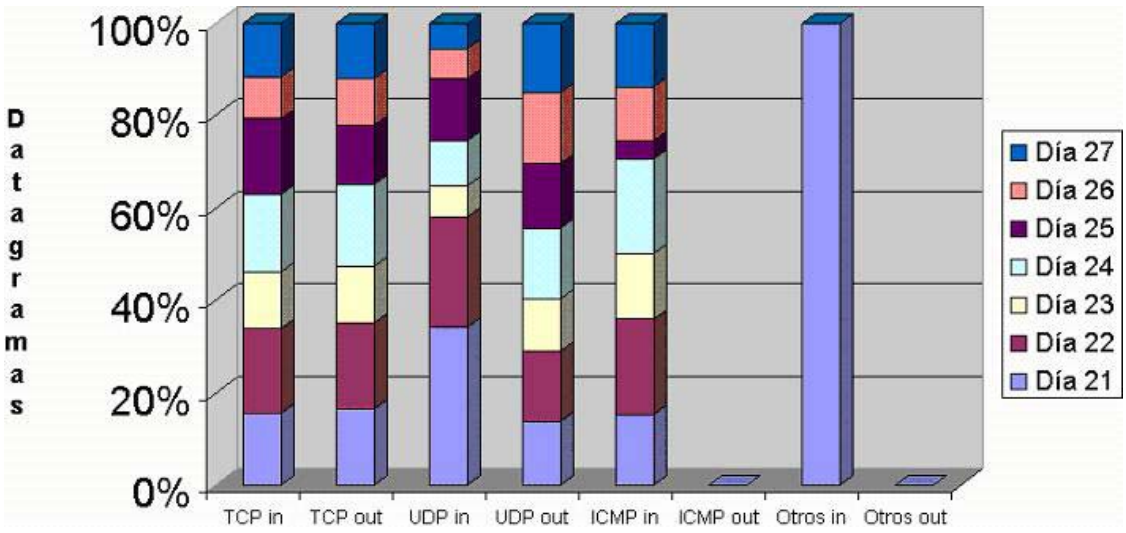


FIG. 5-38: distribución porcentual del tráfico semanal por protocolo.

Del análisis de figura 5-38 podemos deducir rápidamente que generalmente durante toda la semana el tráfico TCP de entrada registrado es prácticamente el mismo que el de salida hacía Internet. Así mismo, el tráfico UDP de entrada suele ser más voluminoso que el de salida, con la excepción de los días 23, 26 y 27 dónde se registra un tráfico de salida muy superior al de entrada.

Prácticamente todo este tráfico (TCP y UDP) registrado hace referencia a interacciones del exterior con los puertos *Netbios/Microsoft-ds* (SAMBA). Coincidiendo con las fechas en las que se realizó este experimento, el virus **W32/BLASTER** tuvo los días de máxima expansión por Internet [WWW197][WWW198][WWW199].

Este virus se caracteriza por aprovechar un fallo (*bug*) del software que controla los servicios de red de Windows, se conecta al puerto TCP/135 (servicio RPC) de los sistemas Microsoft y aprovecha esta vulnerabilidad. Nuestro sistema registró un total de 3086 peticiones al puerto 135.

Finalmente vemos como todo el tráfico ICMP y el clasificado como "Otros" que se ha registrado durante la semana ha sido de volumen similar, con la excepción del día 25 de Agosto dónde el número de peticiones fue netamente inferior a la media. Otro rasgo a comentar es que este tráfico ha sido únicamente de entrada, cosa normal puesto que el análisis de los datagramas nos ha mostrado su naturaleza anómala y por lo tanto carente de respuesta por parte del sistema.

## 5.5 Conclusiones

Una vez finalizado el experimento y realizado el análisis del tráfico obtenido durante la semana, podemos observar que pese a ser una cantidad a tener en cuenta (casi 90Mbytes) este no representa ni el 5‰ del total teórico semanal. Por otro lado, también es cierto que con una simple petición que tenga éxito por parte de un atacante nuestro sistema puede verse comprometido o utilizado como lanzadera contra otros ordenadores.

En cuanto al análisis del tráfico registrado durante esta semana, cabe destacar la impresionante cantidad de peticiones de los protocolos *Netbios/Microsoft-ds* recibidas, de hecho prácticamente todo el tráfico no deseado registrado pertenecía a esta clase (casi un 83%).

Los protocolos de compartición de recursos de red que utilizan los productos basados en Windows responden de forma automática (sin verificar o autenticar el origen) a cualquier petición realizada. Esta característica lleva a que *hackers* o *blackhats* envíen miles de peticiones indiscriminadas por Internet con el objetivo de conseguir alguna respuesta positiva.

La premisa básica es que la mayoría de sistemas funciona con productos Microsoft, de esta forma la mayoría de peticiones llegará a sistemas Windows (siempre y cuando no exista un firewall o sistema de seguridad de red bien instalado). Por otro lado tenemos que la existencia de fallos (bugs) en el software existente es bastante amplia, lo que permite la existencia de múltiples programas que intentan aprovecharse de sistemas anticuados o no actualizados (como ejemplo tenemos las peticiones en busca de sistemas IIS).

En cuanto al riesgo de ataques directos a nuestra red, hemos podido observar cómo efectivamente si que existen. Los ataques basados en fallos existentes en la implementación de los distintos servicios (SSH, HTTP) han podido ser observados varias veces en nuestro sistema durante la semana.

También hemos recibidos exámenes externos sobre la configuración de nuestros servicios de red (MAIL, HTTP) con el objetivo de utilizarlos como puente de acceso hacia otros ordenadores, ya sea como un *proxy* que permita un acceso anónimo al atacante, un virus o gusano (como en el caso de CodeRed II) o como un foco de propagación de mail no deseado (*spam*).

También hemos recibidos peticiones anómalas y que no hemos podido entender como los datagramas pertenecientes a protocolos desconocidos (ver informe del día 21) o los sospechosos paquetes ICMP dirigidos al puerto 0. Aunque que ciertamente este tráfico es mínimo, existe, lo que puede llegarlo a convertir en un foco de problemas.

Curiosamente no se ha detectado ningún intento de conexión al servicio TELNET, lo que nos lleva a concluir que las conexiones remotas a ordenadores han sido felizmente substituidas por el protocolo SSH.

Hay dos factores fundamentales que han contribuido enormemente al aumento de la inseguridad en Internet:

1. Las conexiones a Internet se han abaratado espectacularmente (podemos conseguir una conexión las 24 horas del día por menos de 40€/mensuales) lo que permite que la cantidad de ordenadores permanentemente conectados sea cada vez mayor.

2. El ancho de banda disponible también ha ido aumentando permitiendo a posibles atacantes el lanzamiento de procesos que sondeen rangos enteros de direcciones de IP en períodos razonablemente cortos de tiempo.

Si bien la cantidad y el éxito de los ataques registrados en nuestra red no han sido preocupantes, sí que debemos concluir este trabajo recomendando la adopción de medidas de seguridad para cualquier red local. Esta recomendación se hace extensible también a los ordenadores personales conectados directamente a Internet (usualmente en el domicilio).

La adopción de algún sistema básico de filtrado de tráfico o puertos[ℜ] debe ser el umbral mínimo de seguridad exigible para cualquier conexión a Internet. Además debemos recomendar la existencia de una estricta política de actualizaciones de software debido a la gran facilidad que tienen actualmente los atacantes para utilizar herramientas automáticas que busquen ordenadores con software "anticuado".

La complejidad de las medidas de seguridad a adoptar depende directamente del tamaño de nuestra red local. El número de ordenadores y servidores existente, la variedad de servicios que ofrezcamos y la cantidad de usuarios del sistema deben guiar nuestra política de seguridad.

[ℜ] Existen cientos de herramientas gratuitas que pueden realizar esta función, por ejemplo los firewall.

Finalmente recordar que **es necesario que la seguridad siempre esté en manos de profesionales**. No hay mayor peligro que un sistema de seguridad mal configurado, ya que crea una falsa sensación de seguridad que será aprovechada por un atacante antes o después.

# 5.6 RESUMEN

En este último capítulo hemos presentado la parte experimental o práctica de este trabajo. Se ha optado por la realización de un estudio pormenorizado de una conexión permanente a Internet durante siete días.

Inicialmente hemos presentado y analizado los distintos requerimientos funcionales y de estructura que planteaba la monitorización de la red local escogida. Se ha comentado la arquitectura seleccionada para esta prueba, basada en el modelo más representativo de una conexión a Internet. También hemos explicado los distintos servicios que tendríamos funcionando en nuestra red (MAIL, SSH, HTTP…).

Posteriormente se presentaron las diferentes herramientas de monitorización seleccionadas (Apache, Ethereal, IPaudit, MRTG…) que nos permitirán la realización de un estudio efectivo de todo el tráfico que se genere en nuestro sistema.

Finalmente se han presentado y comentado los informes diarios con los resultados e incidencias obtenidas así como un resumen semanal en el que se engloba todo el tráfico registrado durante la semana. Al final del capítulo se realiza una exposición de las conclusiones obtenidas tras la realización de este experimento.