Seguridad y Privacidad en Redes

SNIFFERS

¿Qué son los sniffers?

- Un sniffer es un “capturador” de tráfico de red.
- Pueden utilizarse:
  - Como una herramienta que facilita el mantenimiento de las redes (analizador de protocolos).
  - Con fines de “espionaje”
- Aprovechan:
  - Que las redes de área local utilizan medios compartidos
  - El comportamiento de algunos protocolos de red

Sniffers -Conceptos

- Modo promiscuo:
  - Es un modo de recepción especial que implica que el adaptador recibirá todos las tramas que viajen por el medio y no sólo las que van dirigidas a ese adaptador.
  - Esta funcionalidad es usada por los agentes de monitoreo de tráfico o sniffers.

Conceptos relacionados (cont)

- Modo promiscuo:
  - Algunos drivers permiten habilitar este modo.
  - ¿Cómo detectarlo?
    - En algunos SO UNIX-like (Ifconfig)
    - En un SO Windows (Antisniffers)

Sniffers en redes switcheadas

- En un ambiente no switcheado, cuando un nodo transmite, las tramas viajan por el medio compartido y son “vistas” por todos los nodos que forman parte del segmento
- Un switch divide dominios de colisión: un segmento está conformado por el nodo y el puerto del switch al que dicho nodo está conectado.

¿Es posible sniffear una red switcheada?

Sniffers en redes switcheadas

- Algunas técnicas usadas en redes con switches:
  - Switch Jamming
  - ICMP Redirect
  - ICMP Router Advertisements
  - ARP Spoofing al switch
  - ARP Redirect o Spoofing al cliente
  - Aprovechar el puerto de monitoreo en el switch
  - Cable-taps/Hubs
  - DHCP spoofing

Ejemplos de herramientas

- Algunas herramientas que implementan sniffers:
  - Etherpeek
  - Wireshark (nuevo nombre del proyecto Ethereal)
  - Tcpdump
  - Ettercap

Sniffers-Etherpeek

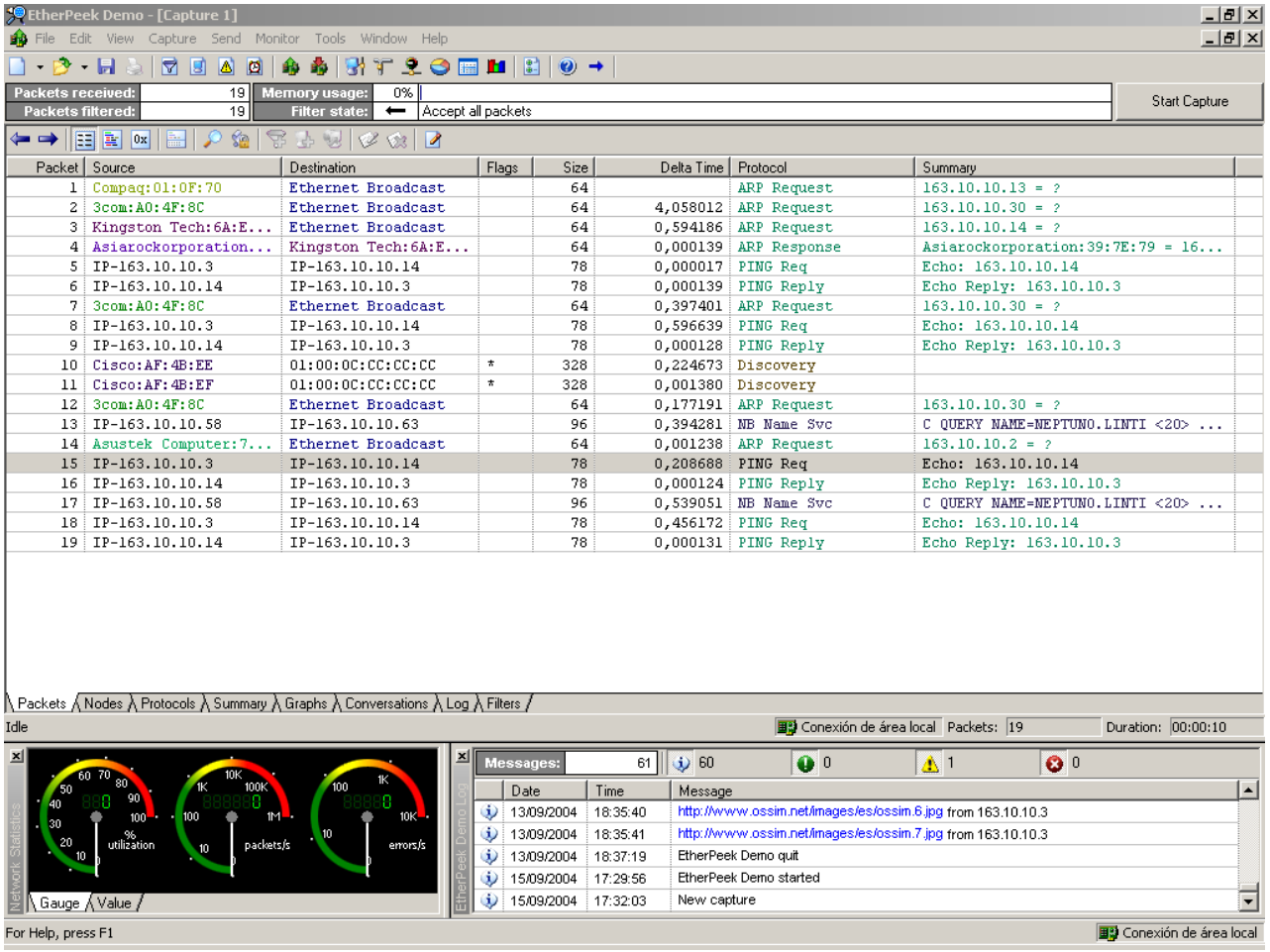
- Analizador de protocolos que constituye una poderosa herramienta de monitoreo y permite decodificar tramas en tiempo real, durante la captura.

- Algunas de las funcionalidades que el mismo provee:
  - Permite realizar y guardar capturas en distintos formatos.
  - Muestra el contenido de los paquetes de forma tal que resulta sencillo interpretar la información que los mismos transportan
  - Permite definir filtros para realizar la captura.
  - Permite simular el envío de paquetes cuyo contenido puede modificarse.

http://www.wildpackets.com/

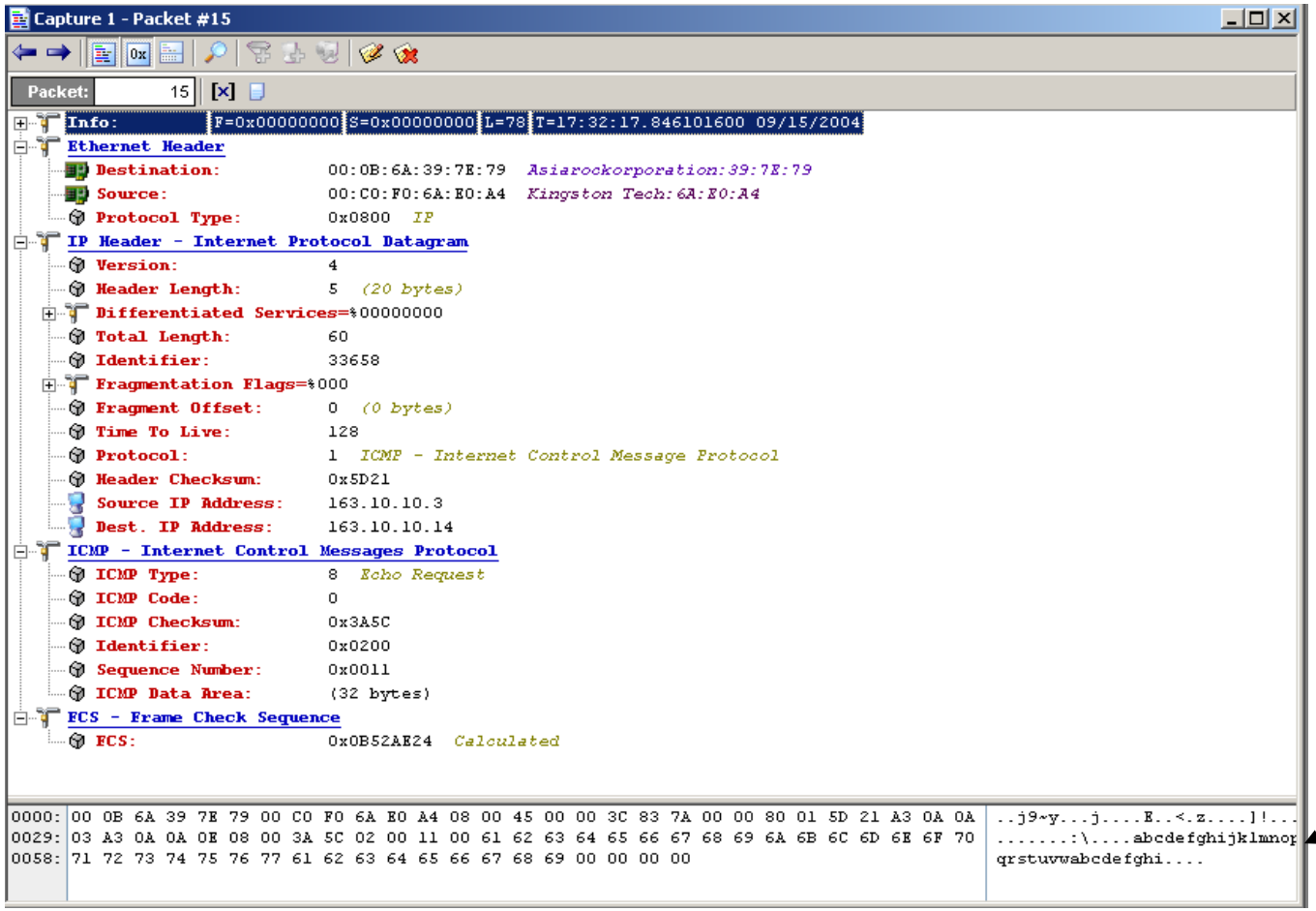
Sniffers-Etherpeek

Interfaz de la herramienta



Paquetes capturados

Sniffers-Etherpeek

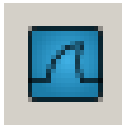


Muestra el contenido separando los encabezados y los datos de cada capa

Muestra el contenido en hexadecimal

Contenido de uno de los paquetes capturados

Muestra el contenido en ASCII



Sniffers – Wireshark

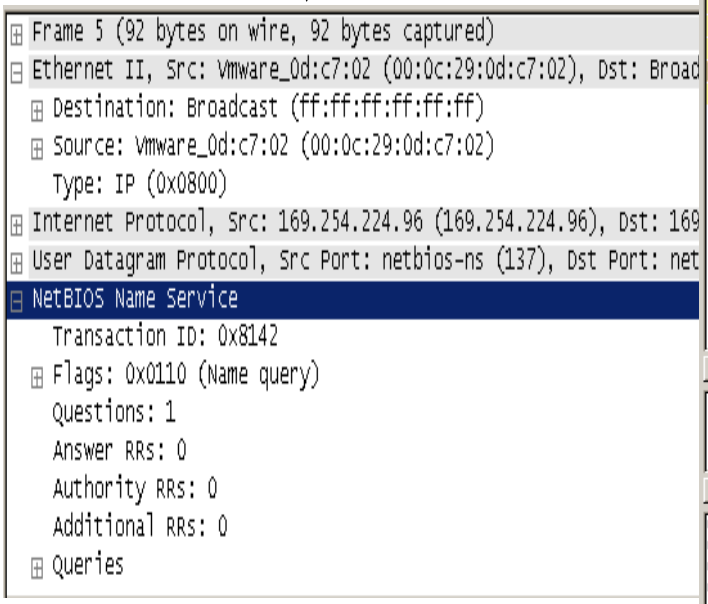
- ✓ Es una herramienta similar al Etherpeek, que corre en plataformas Unix y Windows.
- ✓ Es opensource. Conocido anteriormente como Ethereal.
- ✓ Difiere en la interfaz que provee y en algunos aspectos relacionados con la funcionalidad de la herramienta.

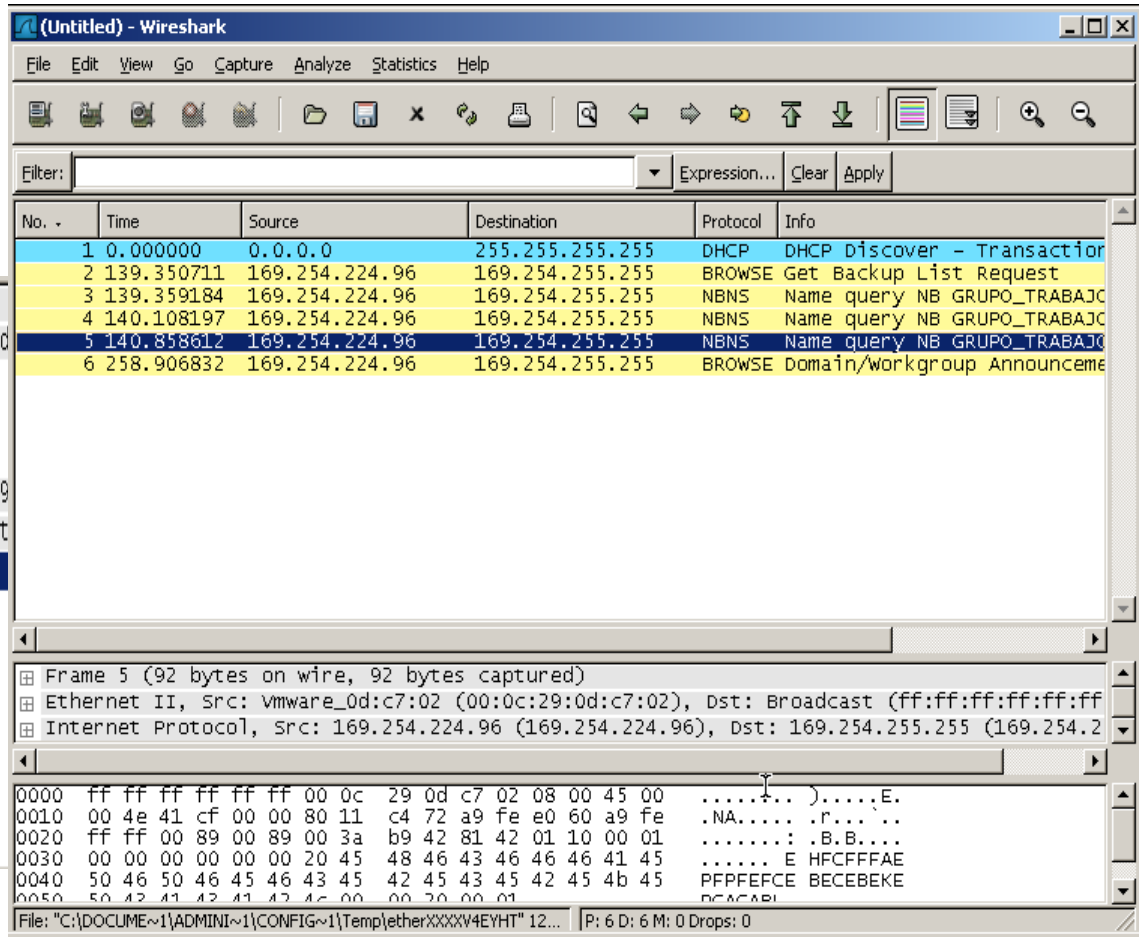
http://www.wireshark.org

Sniffers – Wireshark

Interfaz de la herramienta

Contenido de uno de los paquetes capturados





Sniffers – Wireshark

¿Vemos una DEMO?

Sniffers – Tcpdump

- Es una herramienta de monitoreo de tráfico orientada a comandos que permite especificar expresiones regulares para definir el tráfico a capturar

- Ej: tcpdump –X host 163.10.5.66

  tcpdump –i eth0 port 80

http://www.tcpdump.org

Sniffers – Ettercap

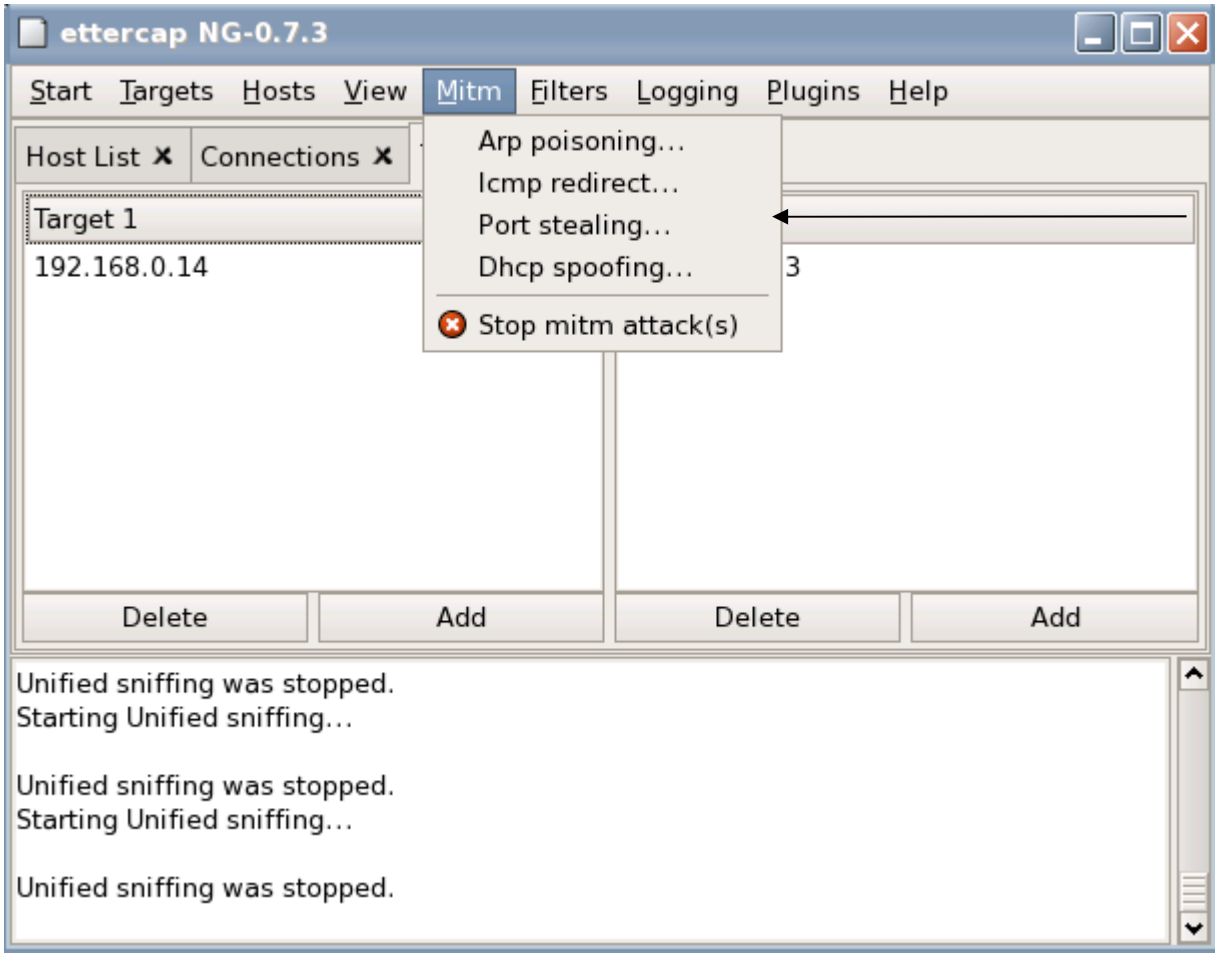
- ✓ Es un sniffer multipropósito que permite realizar ataques de “man in the middle” (Mitm).
- ✓ Es opensource.
- ✓ Corre sobre plataformas Windows y Linux.
- ✓ Permite sniffear en redes switcheadas.

http://ettercap.sourceforge.net/

Sniffers – Ettercap

Interfaz de la herramienta

Hosts a sniffear →



Técnicas para sniffear en redes switcheadas

Sniffers – Ettercap

¿Vemos una DEMO?

Sniffers de propósitos específicos

- Para sniffear mensajería instantánea:
  - Aimsniff [http://www.aimsniff.com/]
  - Imsniff []
- Para sniffear imágenes
  - Driftnet [http://sourceforge.net/projects/im-snif/]
- Tráfico SSL:
  - SSLSniff [http://www.thoughtcrime.org/software/sslsniff/]
- Tráfico Wireless:
  - Kismet [http://www.kismetwireless.net]
  - AirPcap [http://www.wireshark.org]

Sniffers – Más herramientas y urls

Otras herramientas

- ✓ Cain and Abel [http://www.oxidit.it/cain.html]
- ✓ Dsniff [http://www.monkey.org/~dugsong/dsniff/]
- ✓ Ngrep [http://www.packetfactory.net/projects/ngrep/]
- ✓ Snoop [http://www.spitzner.net/snoop.html]

DETECCIÓN DE SNIFFERS

¿Cómo se detectan los Sniffers?

- ✓ Si bien en teoría se dice que es imposible detectarlos, debido a que son pasivos (sólo monitorean el tráfico, no transmiten nada), a veces en la práctica es posible detectarlos.

- ✓ Existe una serie de métodos que hacen posible la detección de los sniffers.

Métodos de detección de sniffers

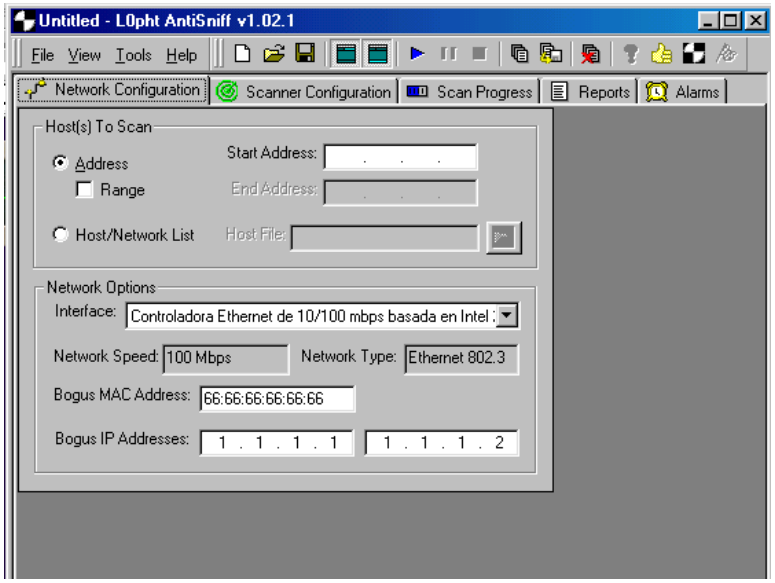
- ✓ Ping method
- ✓ ARP method
- ✓ DNS method
- ✓ Decoy method
- ✓ Host method
- ✓ Latency method

Métodos de detección de sniffers

- ✓ Existen herramientas que realizan esta tarea basándose en los métodos anteriormente mencionados.
- ✓ Otras herramientas permiten generar paquetes de modo tal de permitirnos poner en marcha alguno de los métodos en cuestión.

Algunos ejemplos

- ✓ Antisniff



- ✓ PMD: promiscuos mode detector
- ✓ Etherpeek, Nemesis u otra herramienta para generar paquetes
- ✓ Sniffdet [http://sniffdet.sourceforge.net/index.html]

Otras formas de obtener Información

Keyloggers

Registran las pulsaciones de teclado realizadas por un usuario, guardándolas en un archivo o enviándolas a través de Internet, por ejemplo por email.

Pueden ser:

- ✓ De software (PC Spy Keylogger, Pykeylogger, etc)
- ✓ De hardware

Otras formas de obtener Información

Keyloggers de software:

Extienden el concepto, permiten no sólo almacenar las teclas pulsadas por el usuario, sino también tomar imágenes de pantallas, eventos del mouse, etc.

¿Cómo se distribuyen?

- ✓ A través de un troyano o como parte de un virus informático o gusano informático.
- ✓ En general se puede decir que pueden adjuntarse a un archivo cualquiera.

¿Cómo se evitan o previenen?

- ✓ Antivirus actualizados constantemente
- ✓ Firewalls personales configurados advirtiendo tráfico saliente

Keyloggers

¿Vemos una DEMO?

Otras formas de obtener Información

Mucho más importante que antivirus y firewalls

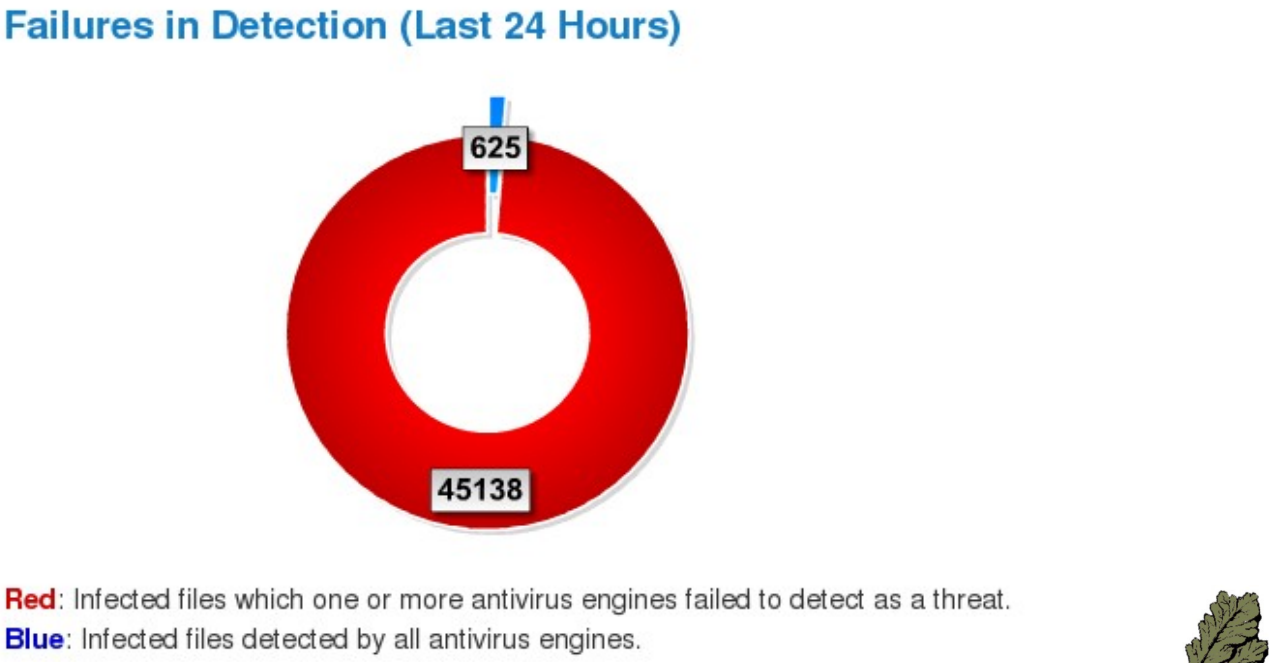
Concientización del Usuario

- Evitar abrir sobre adjuntos u archivos no solicitados o esperados, sobre todo nunca utilizando usuarios permisos de administrador o super usuario.

- Evitar utilizar el equipo como super usuario, restringirlo a los casos necesarios únicamente .

Otras formas de obtener Información

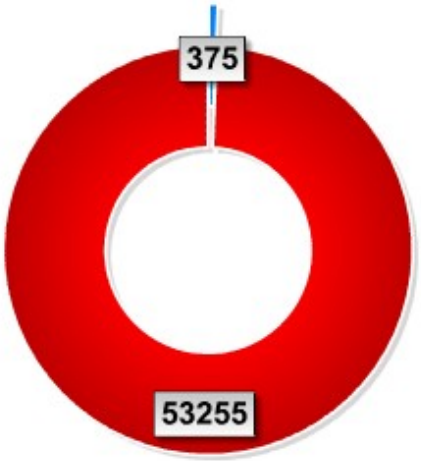
¿Porqué no confiar plenamente en mi antivirus?
Según Virus Total el 24/10/08 a las 00:40 hs :



Otras formas de obtener Información

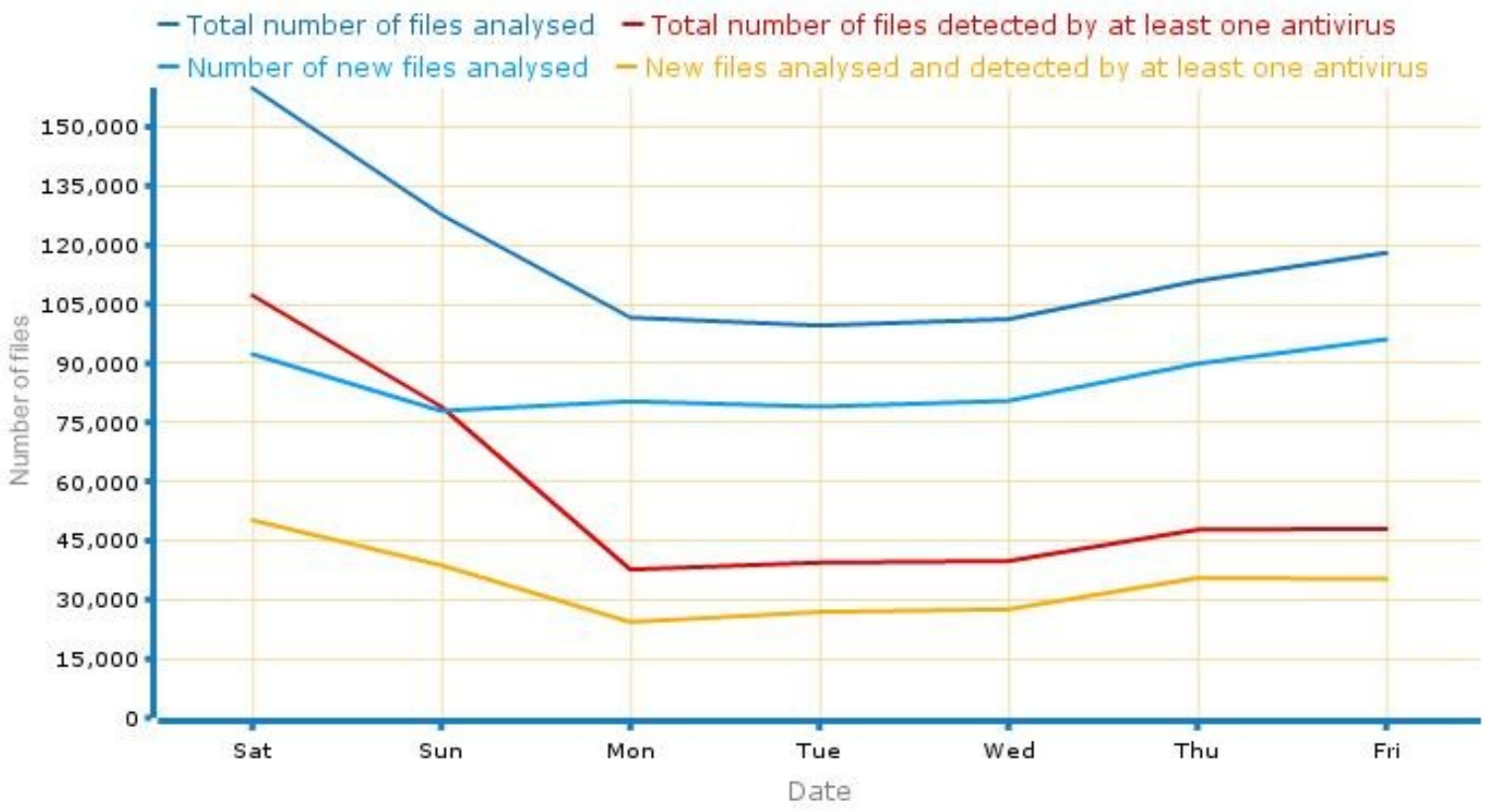
Datos publicados al 20-10-09...

Red: Infected files which one or more antivirus engines failed to detect as a threat.
Blue: Infected files detected by all antivirus engines.



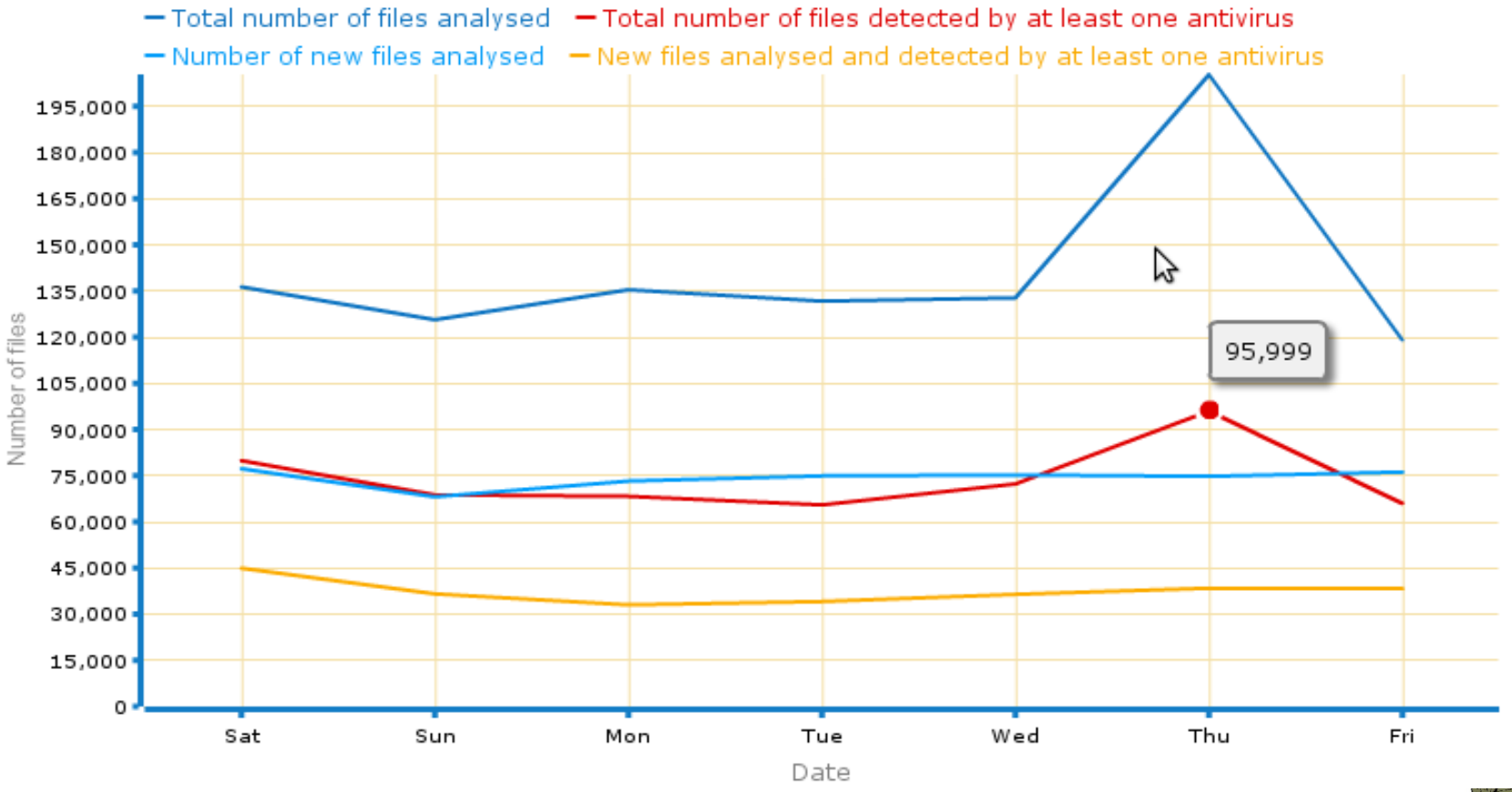
Otras formas de obtener Información

En octubre del 2010



Otras formas de obtener Información

En la actualidad.....el 1-10-2011...



Otras formas de obtener Información

¿Quiero ver un adjunto pero dudo de mi software antivirus?

- Virus total: http://www.virustotal.com
- No Virus Thanks: http://www.novirusthanks.org
- Scanner-virus: http://www.scanner.virus.org

Otras formas de obtener Información

Keyloggers

¿Cómo se evitan o previenen a nivel de red?

- ✓ Instalando filtros de spyware a nivel de host
- ✓ Instalar un aplicación de gateway con filtro de contenidos.
- ✓ Monitoreando los logs del sistema de detección de intruso (IDS) y manteniéndolo actualizado.
- ✓ Previniendo la instalación de software bajado por los usuarios.