# Administración de Redes y Seguridad

## Sniffers

Lic. Bruno Zappellini y Lic. Nahuel Defossé

UNPSJB

2018

# Sniffers - Motivación

- Teniendo acceso a una red de la organización es posible:
  - Inspeccionar las comunicaciones
  - Manipular las comunicaciones de los usuarios (MITM)
  - Realizar ataques de DOS a la red, los usuarios y los servicios.
- Para ello pueden usarse:
  - Herramientas de análisis de protocolos (como tcpdump o wireshark)
  - Herramientas de sniffing

# ¿Qué son los sniffers?

- Un sniffer es un “capturador” de tráfico de red.
- Pueden utilizarse:
  - Con fines de “espionaje”
  - Al igual que los analizadores de protocolos, como una herramienta que facilita el mantenimiento de las redes.
- 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 hacerlo?
  - En algunos SO UNIX-like (`#ifconfig eth0 promisc` o `#ip link set dev eth0 promisc on`)
  - En un SO Windows (mediante drivers especializados, software especializado o el protocolo monitor de red).

# 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?

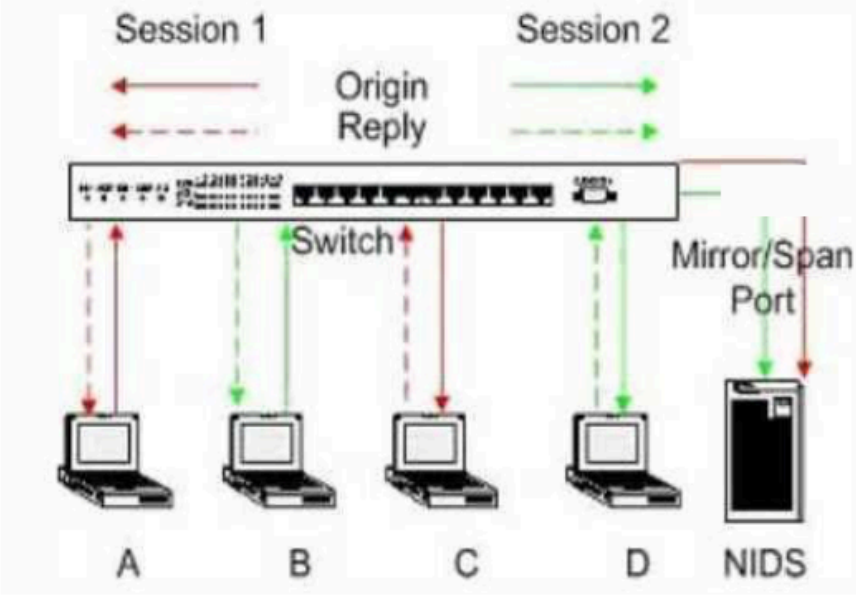
# Sniffers en redes switcheadas

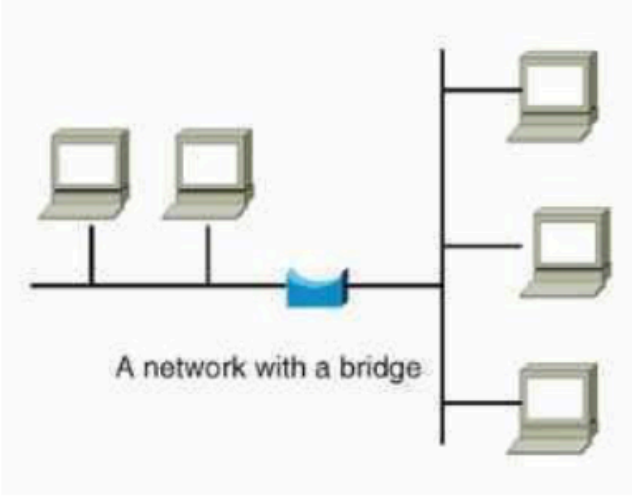
- Si la red está conectada con SWITCHs se pueden realizar los mismos ataques que en una red conectada con HUBs, pero antes es necesario atacar la infraestructura de la red ("manipulando el switch lógica o físicamente" o haciendo MITM).
- Se podría engañar al switch:
  - Saturación del switch (MAC flooding)
  - Spoofing de MACs

# Sniffers en redes switcheadas

Si se tiene acceso físico al Switch:

- Usar el puerto de monitoreo si hay uno configurado (fig.1)
- Usar un HUB para conectar el cable que va al gateway de la red

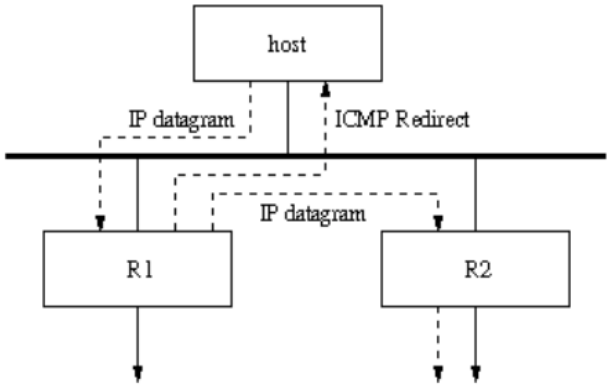


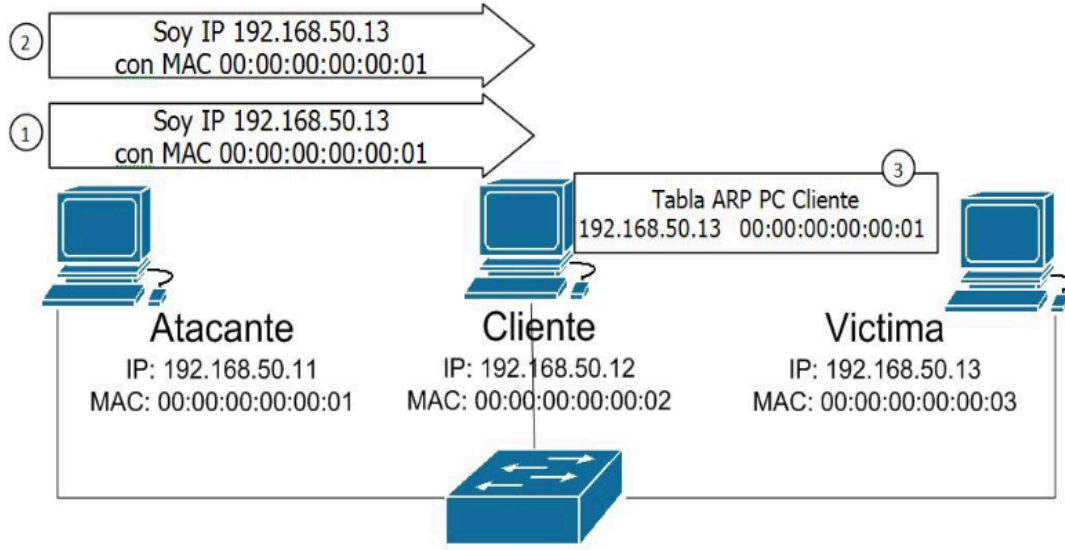



# Sniffers en redes switcheadas

Engaño a estaciones con:

- ICMP Redirect (izquierda)
- ICMP Router
- Advertisements ARP
- Spoofing (derecha)
- DHCP Spoofing



# Ejemplos de herramientas

Algunas herramientas que implementan sniffers:

- Tcpdump
- Omnipeek (Sucesor de Etherpeek+Airopeek)
- Wireshark
- Ettercap

# Sniffers Tcpdump

- Es una herramienta de monitoreo de tráfico orientada a comandos que permite especificar expresiones (soportando regex) para definir el tráfico a capturar (http://www.tcpdump.org)

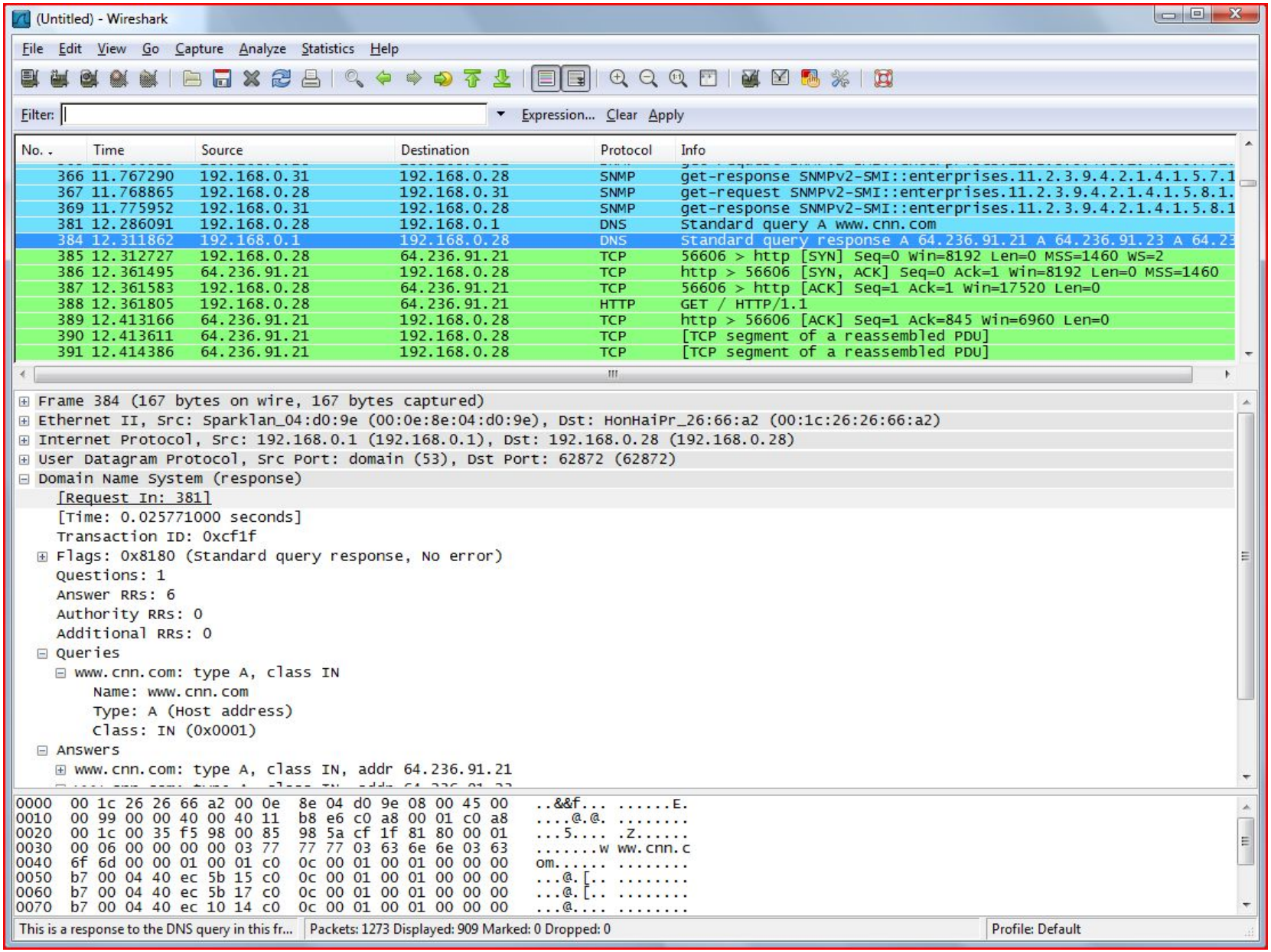
```
tcpdump -X host 163.10.5.66
tcpdump -i eth0 port 80
```

# Sniffers - Wireshark

- Es una herramienta Open Source , que corre en plataformas Unix y Windows.
- Interfase visual
- Conocido anteriormente como Ethereal.
- Captura tráfico, visualiza en timepo real
- Almacena capturas, abre capturas de tcpdump
- Filtros de captura
- Plugins
- Se pueden agregar más protocolos a analizar utilizando disectores.
- http://www.wireshark.org

# Sniffers - Wireshark

## Análisis de tráfico con Wireshark

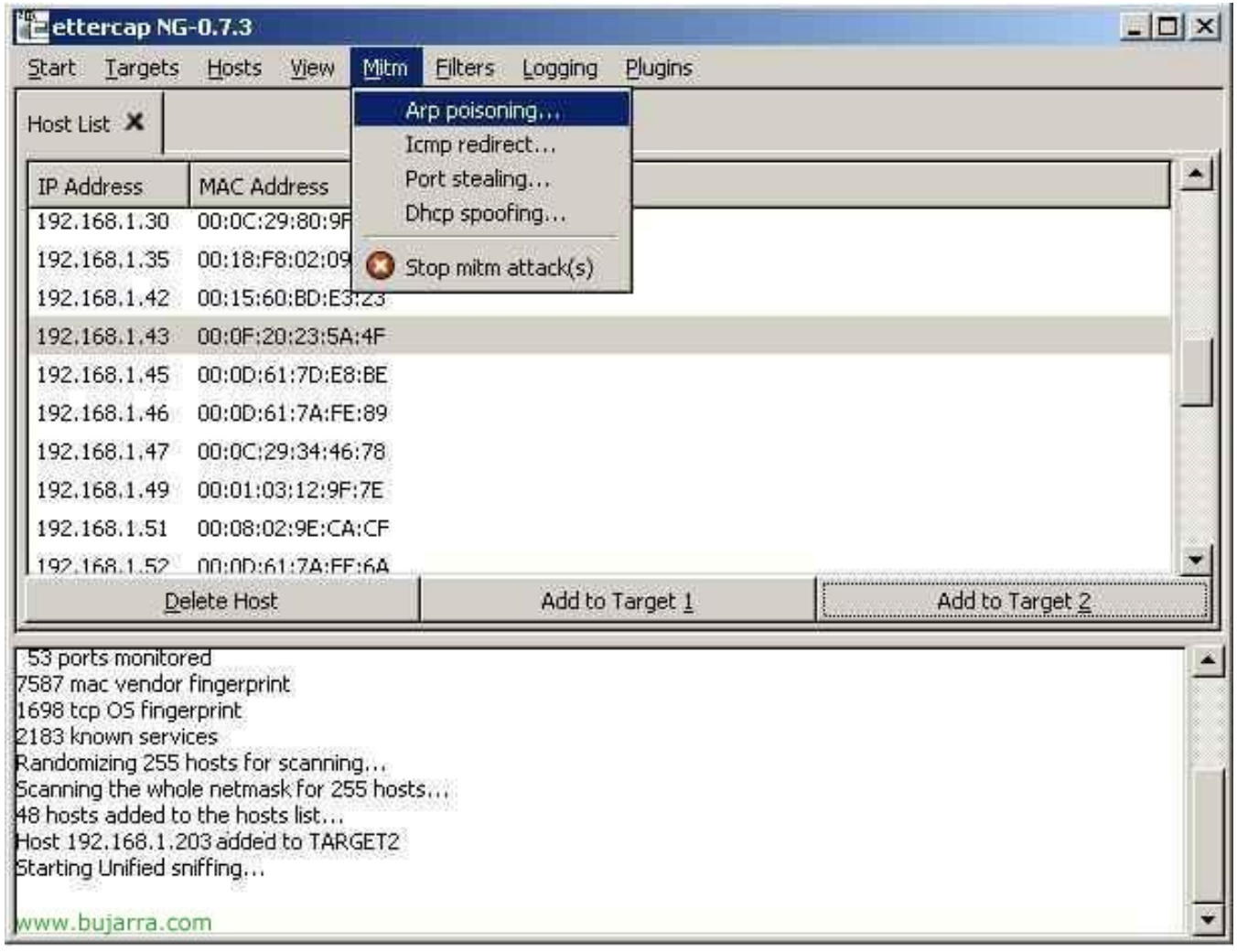


# Sniffers - Ettercap

- 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/

# Ettercap

Interfaz gráfica de la herramienta



# Sniffers de propósitos específicos

- Hay sniffers de propósito específicos que permiten:
  - Mostrar imágenes que circulan en el tráfico capturado
  - Mostrar usuarios y contraseñas de conexiones capturadas de protocolos “inseguros”
  - Mostrar comunicaciones de mensajería instantánea

# Sinffer de propósitos específico

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

# 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/]

# Detección de Sniffers

- ¿Como se detectan?
- Si bien trabajan de modo pasivo:
  - Con acceso al HOST ifconfig (Unix), Antisniffers (Windows)

# Métodos de detección de Sniffers

- Sin acceso al host o a través de la red:
  - PING test
  - ARP test
  - DNS test
  - Medición de latencia
  - Decoy method (tipo honeypot)

# 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.
- A través de herramientas que detecten “tráfico sospechoso” generado por los sniffers que usan técnicas de MITM

# Métodos de detección de sniffers - Herramientas

- PromiSCA
  http://www.securityfriday.com/products/promiscan.html
- Sniffdet http://sniffdet.sourceforge.net/index.html
- Packit http://sourceforge.net/projects/packitgui/
- Nemesis (generador de paquetes)
  http://nemesis.sourceforge.net/
- Arpwatch

# Otras formas de obtener Información

- Keyloggers
  - Software
    - PC Spy Keyloggers
    - PyKeyLogger
  - 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 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