Sniffers

Departamento de Sistemas Telemáticos y Computación (GSyC)

gsyc-profes (arroba) gsyc.es

Diciembre de 2012

Sniffers

Un *sniffer*, aka analizador de paquetes, aka analizador de protocolos es un dispositivo o una aplicación capaz de interterceptar y registrar el tráfico que circula por una red de datos digital, para su posterior análisis

- El sniffer más popular (y libre) es wireshark. Hasta 2006 se llamaba ethereal. Hay otros, comerciales, como OmniPeek

Ubicación del sniffer

El sniffer debemos ubicarlo en el lugar adecuado, o no capturaremos ningún tráfico

1. Redes cableadas
   - En un concentrador
   - Mediante replicado de puertos (*port mirroring*)
   - En un *Network Tap*
2. Redes inalámbricas
   - En una máquina con interfaz en modo monitor
3. Ambos tipos de redes
   - En una máquina que realice envenamiento de cache ARP (*ARP cache poisonig*)

Sniffer en un concentrador

- En un verdadero concentrador todas las máquinas están en el mismo dominio de colisión. Un sniffer en cualquier *boca* recibirá todo el tráfico
- Pero hace tiempo que no se fabrican, hay que conseguir uno antiguo, tal vez comprarlo usado en eBay
- Con cuidado, porque *hub* (concentrador) vs *switch* (conmutador) son palabras con los que el marketing no es riguroso.
  En un conmutador, solo la boca origen y la boca destino tienen acceso a una trama

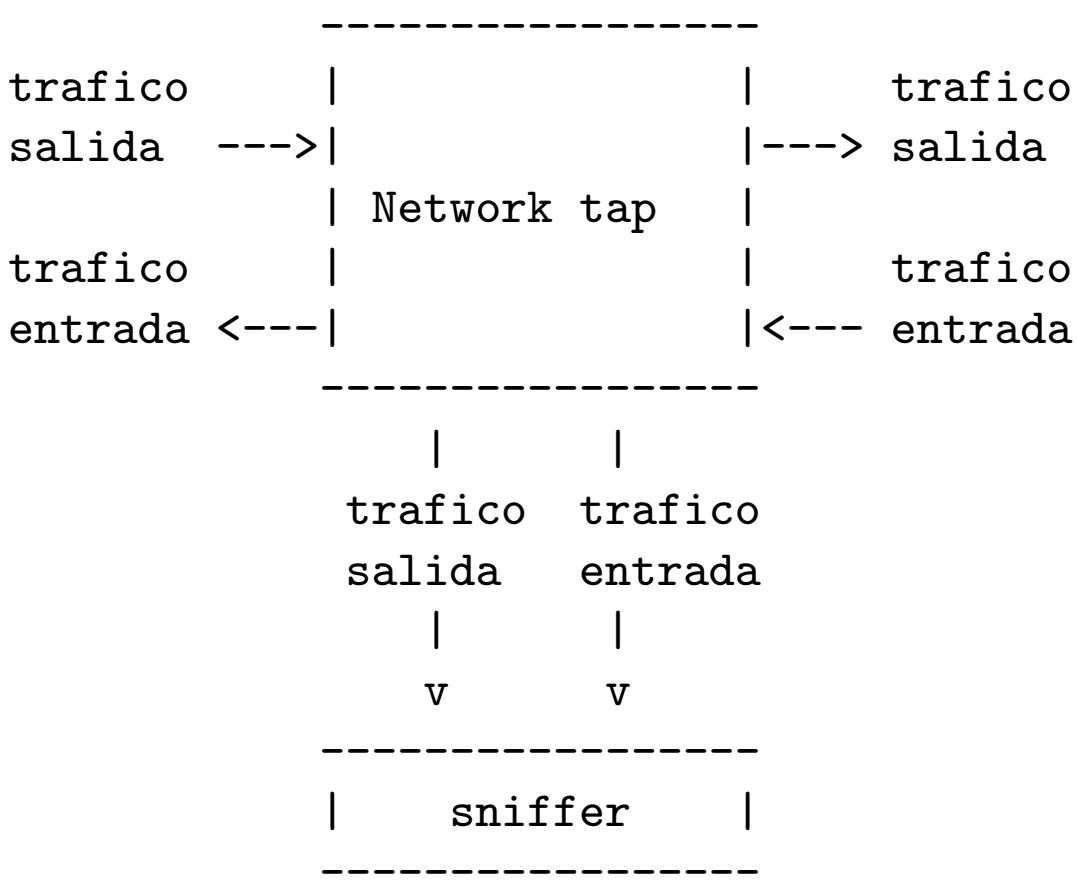
Replicado de puertos / port mirroring

Los conmutadores de uso corporativo son capaces de replicar en cierta boca el tráfico de otras bocas
Observaciones:

- En este contexto, *puerto* no es un puerto de nivel de transporte, sino una *boca*
- Si se replican varias bocas sobre otra, esta puede ser incapaz de asumir todo el tráfico
- Todo el conmutador irá más lento
- Los errores de nivel 1 no se perciben

Network TAP

- Dispositivo similar a un conmutador con replicado de puertos, pero cuyo único propósito es enviar todo el tráfico que pasa por el cable a un analizador



Interfaz inalámbrico en modo monitor

- Es difícil recibir todas las tramas
  - Hay que saber en qué canal escuchar
  - O monitorizar los 14 canales
  - Y aún así, es muy normal que se nos *escapen* tramas.
  - Una buena antena y proximidad a la fuente mejoran el resultado
- Hay que capturar el tráfico con una herramienta orientada a tráfico inalámbrico (como airodump-ng, parte de aircrack-ng) Capturando con el wireshark ordinario, el tráfico 802.11 se vería como si fuera ethernet

Envenenamiento de caché ARP

- Una máquina responde *mintiendo* a las preguntas de ARP y consigue tramas dirigidas a otra máquina
- Monitores activos pueden detectar e impedir esto
- Una herramienta muy popular es Cain & Abel

Captura de tráfico

Para capturar tráfico hay que ser root. Es poco seguro usar wireshark como root, es preferible capturar con un programa distinto, como programa distinto para la captura:

- tcpdump
  Herramienta tradicional de captura de paquetes
- dumpcap
  Similar a tcpdump, derivada de wireshark
- pcapdump
  Similar a tcpdump
  `pcapdump -i eth0 -a duration:30 -w captura01.pcap`
- tshark
  wireshark en modo texto
- aidump-ng
  Para captura inalámbrica, forma parte de aircrack-ng

captura con airodump-ng

- Puesta del interfaz en modo monitor. Supondiendo que sea wlan0 (puede ser p.e. wlan1)

```
ifconfig wlan0 down
iwconfig wlan0 mode monitor
ifconfig wlan0 up
```

  Esto crea un nuevo interfaz, wlan0mon

- Hay que ponerlo en el mismo canal que la máquina a monitorizar. P.e.

```
iwconfig wlan0 channel 11 # Atencion! A este canal a
                          # veces se le llama 12.
                          # Fijarse en la frecuencia.
```

- Captura

```
airodump-ng -o pcap -w <nombre_fich> --channel <canal> <interfaz>
```

  p.e.

```
airodump-ng -o pcap -w nombre_fichero --channel 11 wlan0mon
```

Referencias

- Chris Sanders, Practical Packet Analysis
  Ed. No Starch Press