

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 todas 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 switchheadado, 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 switchheada?

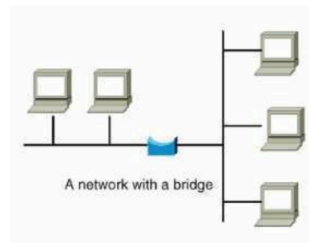
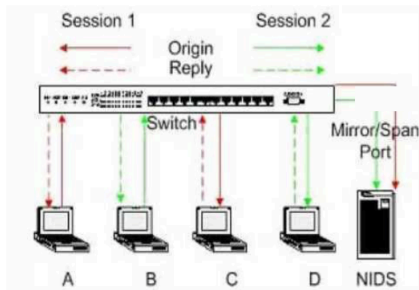
Sniffers en redes switcheadas

- ▶ 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 lógicamente 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:

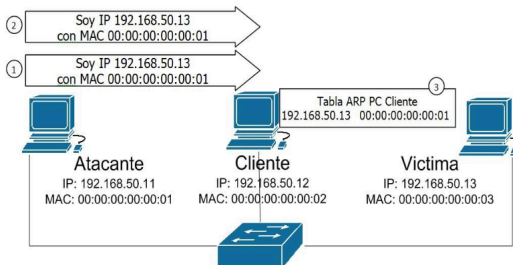
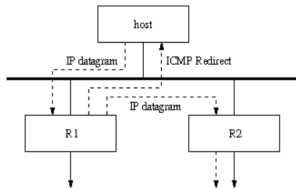
- ▶ Usar el puerto de monitoreo si hay uno configurado (fig.1)
- ▶ Usar un HUB para conectar el cable que va al gateway de la red



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
- ▶ Omnipcap (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 tiempo 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

The screenshot displays the Wireshark interface with a packet capture of network traffic. The main pane shows a list of captured packets, with packet 384 selected. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
366	11.767290	192.168.0.31	192.168.0.28	SNMP	get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
367	11.768865	192.168.0.28	192.168.0.31	SNMP	get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
369	11.775952	192.168.0.31	192.168.0.28	SNMP	get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
381	12.286091	192.168.0.28	192.168.0.1	DNS	Standard query A www.cnn.com
384	12.311862	192.168.0.1	192.168.0.28	DNS	Standard query response A 64.236.91.21 A 64.236.91.23 A 64.236.91.24
385	12.312727	192.168.0.28	64.236.91.21	TCP	56606 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2
386	12.361495	64.236.91.21	192.168.0.28	TCP	http > 56606 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460
387	12.361583	192.168.0.28	64.236.91.21	TCP	56606 > http [ACK] Seq=1 Ack=1 win=17520 Len=0
388	12.361805	192.168.0.28	64.236.91.21	HTTP	GET / HTTP/1.1
389	12.413166	64.236.91.21	192.168.0.28	TCP	http > 56606 [ACK] Seq=1 Ack=845 win=6960 Len=0
390	12.413611	64.236.91.21	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
391	12.414386	64.236.91.21	192.168.0.28	TCP	[TCP segment of a reassembled PDU]

The packet details pane for the selected packet (Frame 384) shows the following structure:

- Frame 384 (167 bytes on wire, 167 bytes captured)
- Ethernet II, Src: sparklan.04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)
- Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)
- User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)
- Domain Name System (response)
 - [Request In: 381]
 - [Time: 0.025771000 seconds]
 - Transaction ID: 0xcfff
 - Flags: 0x8180 (Standard query response, No error)
 - Questions: 1
 - Answer RRs: 6
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.cnn.com: type A, class IN
 - Name: www.cnn.com
 - Type: A (Host address)
 - Class: IN (0x0001)
 - Answers
 - www.cnn.com: type A, class IN, addr 64.236.91.21

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 1c 26 26 66 a2 00 0e 8e 04 d0 9e 08 00 45 00  ..&&f.....E.
0010 00 99 00 00 00 40 00 04 11 b8 e6 c0 a8 00 01 c0 a8  ...@.@.....
0020 00 1c 00 35 f5 98 00 85 98 5a cf 1f 81 80 00 01  ...5....Z.....
0030 00 06 00 00 00 00 00 03 77 77 77 03 63 6e 03 63  ....w ww.cnn.c
0040 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00  om.....
0050 b7 00 04 40 ec 5b 15 c0 0c 00 01 00 01 00 00 00  ...@.....
0060 0c 00 04 40 ec 5b 17 c0 0c 00 01 00 01 00 00 00  ...@.....
0070 b7 00 04 40 ec 10 14 c0 0c 00 01 00 01 00 00 00  ...@.....
```

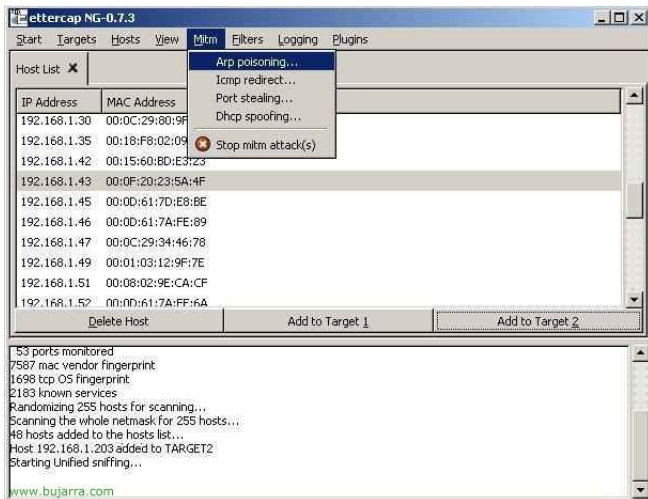
The status bar at the bottom indicates: "This is a response to the DNS query in this fr...", "Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0", and "Profile: Default".

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.aimsniiff.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