Departamento de Seguridad Informática MINSAP

Abril 2018

Volumen 1, nº 1

Boletín de Seguridad Informática

Contenido:

ANÁLISIS DE TRÁFICO CON WIRESHARK Parte II

3. DÓNDE REALIZAR LA CAPTURA DE DATOS

El primer paso para poder auditar la red será definir dónde analizar el tráfico. Imaginemos un escenario común. Nos encontramos en un entorno conmutado formado por varios switches, unos cuantos equipos y un servidor de ficheros. El rendimiento de la red ha disminuido en los últimos días y desconocemos la causa.

Carecemos de un IDS que pueda dar la voz de alarma sobre algún ataque o anomalía en la red y sabemos que el servidor de ficheros abastece, en cuanto a tasa de transferencia se refiere, a los equipos de nuestra LAN (Local Area Network) sin problema alguno. Además, nuestros equipos de red no cuentan con protocolos como Netflow para poder analizar tráfico remotamente por lo que decidimos utilizar Wireshark. La primera duda que surge es dónde instalarlo.

A pesar de parecer lógico instalar Wireshark en el propio servidor de ficheros para analizar el tráfico que transita por ese segmento de red, nos encontraremos con situaciones en las cuales no podamos tener acceso físico al servidor o simplemente, por motivos de seguridad, por ejemplo entornos SCADA, no podamos instalar software en el mismo.

En este caso se mostrarán algunas alternativas en el uso de técnicas que permitan llevar a cabo una captura de tráfico sin necesidad de portar Wireshark al propio servidor. La excepción a esta regla la veremos en el último caso, donde se proponen varios métodos de captura remota en los que sí es necesario ejecutar o al menosinstalar aplicaciones en el equipo que se quiere monitorizar.

3.1. UTILIZANDO UN HUB

Si conectásemos un equipo con Wireshark a uno de los puertos del switch, solo veríamos las tramas que transcurren entre el switch y nuestra máquina, y eso no es lo que pretendemos. El switch divide la red en segmentos, creando dominios de colisión separados y eliminando, de esta forma, la necesidad de que cada estación compita por el medio. Únicamente envía las tramas a todos los puertos (pertenecientes a la misma VLAN) cuando se trata de difusiones broadcast (por ejemplo, para saber la dirección física de alguna máquina).

Una de las alternativas que tenemos para alcanzar nuestro propósito es hacer uso de un hub, como se aprecia en la Figura 1- Modos de captura y conectarlo en el mismo segmento de red donde se encuentra nuestro servidor. Al tratarse ahora de un medio compartido, todo el tráfico entre el switch y el servidor podrá analizarse en nuestro equipo.

3.2. PORT MIRRORING O VACL (VLAN -BASED ACLS)

Siempre que tengamos acceso al switch, y soporte esta funcionalidad, será la manera más cómoda para capturar el tráfico de red. Dicho modo de trabajo, denominado modo SPAN en entornos Cisco, permite duplicar el tráfico que transcurre por uno o varios

puertos del switch y replicarlo al puerto que queramos. Hay que tener en cuenta que el puerto configurado como mirroring tiene que ser tan rápido como el puerto/puertos a monitorizar para evitar pérdida de tramas. Este método es empleado por muchos administradores para instalar IDS u otras herramientas de monitorización.

Una ventaja que presentan las VACL frente al Port Mirroring es que permiten una mayor granularidad a la hora de especificar el tráfico que se quiere analizar. Mientras que configurando Port Mirroring es posible redirigir el tráfico de un puerto o VLAN a otro, con VACL es posible especificar ACLs para seleccionar el tipo de tráfico en el que estamos interesados

En el siguiente ejemplo, se define una VLAN Access Map para reenviar y capturar paquetes que coincidan con el tráfico definido en lab_10 y que posteriormente será aplicado a las VLANS 14,15 y 16:

Router(config)# vlan access-map bmf 10

Router(config-access-map)# match ip address lab_10

Router(config-access-map)# action forward capture

Router(config-access-map)# exit

Router(config)# vlan filter bmf vlan-list 14-16

Router# show ip access-lists lab_10

Extended IP access list lab_10

permit ip 10.0.0.0 0.255.255.255 any

Algunos dispositivos Cisco también disponen de una funcionalidad denominada MiniProtocol Analyzer gracias a la cual se puede capturar tráfico desde una sesión SPAN y almacenar los paquetes en un buffer local, pudiendo ser posteriormente exportados en un fichero .cap. Esta funcionalidad también permite especificar opciones de filtrado para limitar la captura de paquetes, por ejemplo, podrían especificarse aquellos paquetes que tengan un EtherType determinado o aquellos declarados en una ACL previamente configurada. Además, utiliza libpcap como formato de captura por lo que puede emplearse Wireshark o cualquier otro analizador de protocolos para un análisis posterior.

3.3. MODO BRIDGE

En caso de no tener acceso al switch, podremos utilizar un equipo con dos tarjetas de red para situarnos entre el switch y el servidor, como se observa en la Figura 1.

Consiste en un MitM (Man in the Middle), a nivel físico, donde tendremos un acceso pasivo a todo el caudal de tráfico.

Tenemos varias alternativas para poner nuestro PC en este modo de funcionamiento,pero destacamos las bridge-utils (paquete de utilidades bridge para Linux) por su facilidad de instalación y configuración. Únicamente tendremos que crear una interfaz de tipo bridge y posteriormente añadir las interfaces físicas que forman parte de dicho puente. Por último, levantaremos la interfaz y ejecutaremos Wireshark. El inconveniente de éste método de captura es la pérdida de tramas durante su instalación, situación que en ciertos escenarios no es asumible. A continuación, se muestra un ejemplo de su configuración:

root@bmerino:~# brctl addbr mybridge

root@bmerino:~# brctl addif mybridge eth1

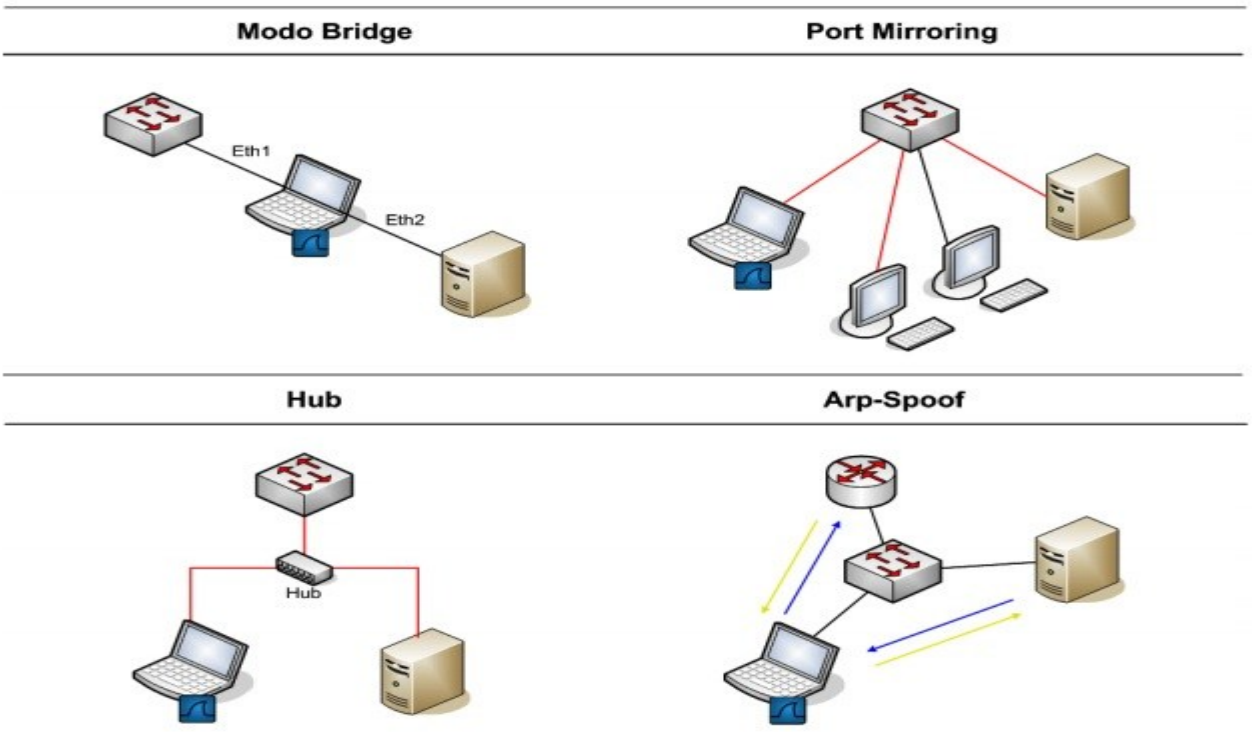
root@bmerino:~# brctl addif mybridge eth0

root@bmerino:~# ifconfig mybridge up

3.4. ARP SPOOF

En contadas ocasiones, y en los casos en los que no podamos utilizar los métodos anteriores, podemos hacer uso de herramientas como Ettercap o similares para llevar a cabo un MitM (Man in the Middle). Es importante entender que se trata de un método bastante ofensivo y que únicamente será útil en entornos no críticos, donde prima cierta necesidad en interceptar tráfico entre varias máquinas.Lo que conseguiremos será que el equipo que se desea monitorizar envíe todas las tramas a través de nuestro PC donde tendremos Wireshark ejecutándose. El proceso se lleva a cabo contaminando la cache de los equipos involucrados con una asociación IP/MAC falsa. Algunos switches disponen de funcionalidades que les permiten detectar este proceso (véase Dynamic Arp Inspection y DHCP Snooping), por lo que es importante deshabilitar dicha funcionalidad en los dispositivos de red si no queremos que nuestro puerto entre en modo shutdown. Para interponernos entre el servidor (10.0.0.100) y el gateway de nuestra LAN (10.0.0.1) bastará con ejecutar Ettercap de la siguiente forma:

root@bmerino:~# ettercap -T -M arp:remote /10.0.0.1/ /10.0.0.100/ &



3.5. REMOTE PACKET CAPTURE

Además de los métodos citados anteriormente, existen varias posibilidades para capturar datos de forma remota. Una de ella es mediante RPCAP (Remote Packet Capture System), aunque en este caso sería necesario ejecutar un programa servidor (rpcapd) junto con las librerías necesarias en el equipo a monitorizar y un programa cliente desde el cual se recuperarán y visualizarán los mismos; en nuestro caso, Wireshark.

Como hemos dicho anteriormente, este método es apropiado para entornos no críticos donde tenemos posibilidad de instalar software en el equipo cuyo tráfico queremos analizar, con el riesgo que ello conlleva para la estabilidad y rendimiento del mismo.

Para la configuración del servidor, únicamente hay que ejecutar rpcapd.exe, incluido en la instalación de WinPcap 4.0 (librerías libpcap en equipos Windows) o superior.

Se puede especificar el puerto de escucha y otras opciones como autenticación, lista de clientes autorizados a conectar al servidor, etc. El modo de funcionamiento puede ser activo o pasivo. En el primer caso el demonio tratará de establecer una conexión hacia el cliente para que éste envíe los comandos adecuados al servidor. Este modo de funcionamiento será útil cuando el demonio esté detrás de un Firewall que no tenga NAT configurado para su conexión desde el exterior. En el segundo caso, será el cliente el que inicie la conexión con el servidor para comenzar a monitorizar datos. (Imagen 1)

El cliente tendrá que especificar dirección, puerto, credenciales (en el caso de que así fuera requerido por el servidor) y la interface desde la cual se desean capturarpaquetes. En Wireshark, esto se realiza desde Capture >> Options y especificando en Interface el tipo Remote: (Imagen 2)

Es importante destacar que, si la captura se realiza en la misma interfaz en la que se está utilizando el propio protocolo RPCAP para transferir los datos entre el demonio y el cliente, dichos paquetes también serán visualizados en Wireshark pudiendocomplicar la interpretación de los mismos. Se puede impedir que estos paquetes interfieran con el resto. Para ello, tendremos que seleccionar la opción "Do not capture own RPCAP traffic" dentro de "Remote Settings".

Otra alternativa aparte de RPCAP para la captura remota de datos es redirigir la salida de tcpdump desde una conexión ssh. Lógicamente, en este caso el equipo a monitorizar necesita disponer de acceso ssh y tener tcpdump instalado (Imagen 3)

Una vez configurada nuestra máquina, haciendo uso de cualquiera de los métodosanteriores, podemos lanzar Wireshark como root/administrador. Para iniciar la capturaseleccionamos la interfaz en el menú Capture >> Interfaces (en el caso de optar por el uso del modo bridge, podemos utilizar cualquiera de las dos). (Imagen 4)

A continuación, describimos brevemente las áreas más interesantes que nos muestra Wireshark según comienza la toma de datos (Figura 5- Áreas de Wireshark):

La zona 1 es el área de definición de filtros y, como veremos más adelante,

permite definir patrones de búsqueda para visualizar aquellos paquetes o

protocolos que nos interesen.

La zona 2 se corresponde con la lista de visualización de todos los paquetes

que se están capturando en tiempo real. Saber interpretar correctamente los datos proporcionados en esta zona (tipo de protocolo, números de secuencia, flags, marcas de tiempo, puertos, etc.) nos va a permitir, en ciertas ocasiones,deducir el problema sin tener que realizar una auditoría minuciosa.

La zona 3 permite desglosar por capas cada una de las cabeceras de los paquetes seleccionados en la zona 2 y nos facilitará movernos por cada uno de los campos de las mismas. Por último, la zona 4 representa, en formato hexadecimal, el paquete en bruto, es decir, tal y como fue capturado por nuestra tarjeta de red.

Imagen 1: Captura de datos con rpcapd

```
C:\Program Files\WinPcap>rpcapd.exe -n  -p 8080
Press CTRL + C to stop the server...
```

Imagen 2: Conexión a servidor rpcapd

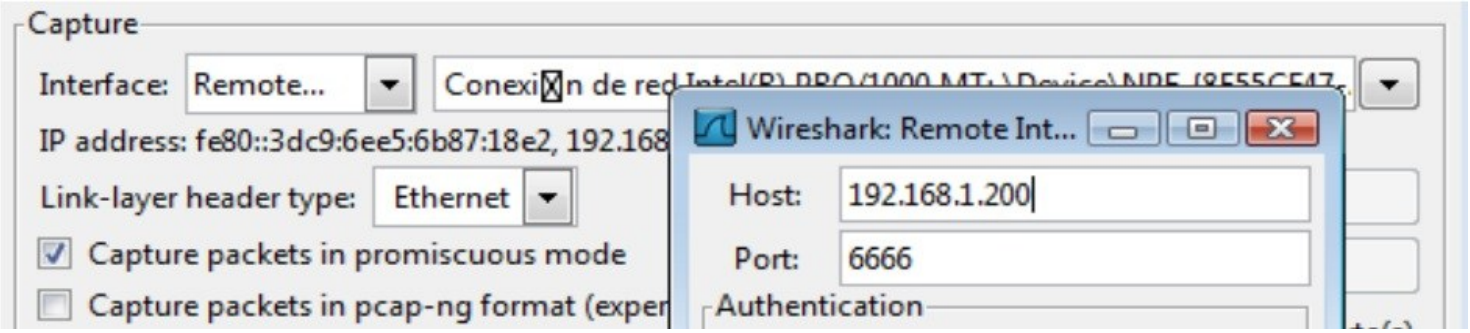


Imagen 3: tcpdump

```
root@borjaBT:~# ssh root@192.168.254.211 tcpdump -w - 'port !22' | wireshark -k -i -
root@192.168.254.211's password:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

Imagen 4: Áreas de Wireshark