Daniel Pérez Vélez.

17 de Diciembre de 2020.

1- Factors to consider when selecting a packet sniffer:

Depende de cómo queremos sniffear. Si queremos hacer un sniff en un segmento específico de la red debemos elegir uno de hardware, conectando el sniffer en la red física.

En cambio, si queremos analizar una interfaz de red, debemos usar un sniffer de software que permitirá filtrar todo el tráfico de red que esté pasando en el momento. Todo eso se hace a partir del software que cambia la configuración de la interfaz de red.

2- How packet sniffers works?

El primer paso es elegir la red que analizaremos. Después capturaríamos tráfico navegando por internet para realizar intercambio de paquetes y analizar cada uno, depende de cuánto tiempo capturemos tráfico será el número de paquetes. También podemos filtrar paquetes por protocolos, tiempo, dirección de origen/destino, puerto, longitud de paquetes, etc. Cada uno de esos aspectos nos permiten tener información detallada sobre nuestra red y evaluar la seguridad de ella.

3- Describe the seven-layer OSI model.

- Capa de aplicación (7): Es la capa más cercana al usuario, permite el intercambio de datos entre el usuario y las apps al recibir información de los usuarios.
- Capa de presentación (6): En esta capa se traduce el formato de aplicación al de red y viceversa al cifrar o descifrar datos de transmisión.
- Capa de sesión (5): Habilita la comunicación entre máquinas (computadoras y servidores) al crear una sesión para el proceso.
- Capa de transporte (4): Aquí sucede la transferencia de datos entre usuarios finales y host. Aplican los protocolos TCP y UDP.
- Capa de red (3): Se encarga de enviar paquetes entre host y destino. Influye mucho el router en esta capa, ya que ayuda a elegir el camino óptimo para que los paquetes lleguen correctamente y rápido. Se usan los protocolos IPv4 e IPv6.
- Capa de enlace de datos (2): A diferencia de la capa 4, la capa 2 se encarga de la transferencia de datos de nodo a nodo. Aquí influyen algunos switch al manejar MAC y LLC.

- Capa física (1): Como su nombre lo indica, se engloban todos los aspectos físicos como pines, componentes eléctricos y cables.

4- Describe traffic classifications.

Es un proceso en el cual se clasifica el tráfico bajo distintos parámetros como el número de puerto o protocolo.

Cuando se basa en el número de puerto es la forma más rápida de clasificar y sin involucrar la privacidad del usuario. Con la inspección profunda de packets se requiere un poder de procesamiento alto y detectar aplicaciones y servicios de los packets. Por otro lado, está la clasificación estadística donde se pueden detectar aplicaciones desconocidas y sus tipos.

5- Describe sniffing around hubs.

Cuando el tráfico es enviado a través de un hub se envía a cada uno de los puertos conectados al hub, lo que haces mucho más fácil observar todo el tráfico. Lo único que se necesita hacer es conectar el sniffer a un puerto vacío en el hub, también se obtiene una ventana de visibilidad ilimitada mientras estés conectado a él.

6- Describe sniffing in a switched environment.

Los switches sólo envían paquetes hacia máquinas que realmente tengan como destino la máquina, no se envían paquetes adicionales o algo por el estilo, entonces es más fácil analizar el tráfico enviado y transmitido en un entorno de switches ya que sólo tienen 1 destino los paquetes.

7- How ARP cache poisoning works?

También llamado spoofing, es una técnica en la que una persona mal intencionada envía mensajes con el protocolo ARP dentro de una red LAN. Lo que se busca hacer es que la MAC del atacante sea confundida por la IP de la víctima que se encuentra en la LAN, para así desviar los paquetes que eran para la víctima y ahora lleguen al atacante, robando información u ocasionando otros problemas.

8- Describe sniffing in a router environment.

Es muy similar al entorno de switch, sólo que en un entorno de routers lo que más importante es dónde colocarás el sniffer, pues de ahí depende de qué máquinas estarás analizando el tráfico. Sin embargo, entiendo que se puede obtener más datos fuera de la red del router haciendo un mapeo con direcciones IP y usando un poco la imaginación para realizar un diagrama de los dispositivos y sus redes.

9- Describe the benefits of Wireshark.

Es una interfaz bastante intuitiva, además de que ofrece las herramientas básicas para un análisis de red correcto y con un fácil manejo de ellas. También tiene opciones avanzadas que de igual manera con la práctica se aprenden a usar y mejoran mucho hasta qué punto puedes analizar un tráfico de red, como los filtros de protocolos o direcciones, gráficos de envío de paquetes junto a sus longitudes y cantidad de packets en una captura, incluso permite hacer una gráfica de líneas para expresar la actividad en la red y los tiempos de respuesta en bits o bytes.

De igual manera permite exportar nuestras capturas a formatos como los de excell y así podemos manipular mejor la información obtenida.

10- Describe the three panes in the main window in Wireshark.

El primer panel es una vista del tráfico capturado en la que se ve el número de paquete, tiempo, origen, destino y la información, se le pueden agregar otras características a mostrar como el protocolo y el DNS, pero requiere otra información.

El segundo panel muestra una información más detallada de características como frame, ethernet y el protocolo del packet que tengamos seleccionado, por ejemplo, si es HTTP muestra si tuvo un error y de qué tipo fue (codes).

El tercer panel permite ver la información, texto o código que contiene el packet que tenemos seleccionado.

11- How would you setup Wireshark to monitor packets passing through an internet router?

Comenzaría abriendo la opción para capturas tráfico y vería todas las posibles fuentes para hacerlo, de ahí si mi computadora está conectada por cable seleccionaría “Ethernet”, y si no, elegiría la opción donde haya fluctuación de actividad.

12- Can Wireshark be setup on a Cisco router?

No directamente porque los routers de Cisco no tienen un entorno gráfico y otras características que Wireshark necesita para que se pueda inicializar, sin embargo, Wireshark se puede correr en una computadora y puede conectarse a uno de los puertos del router de Cisco para capturar tráfico.

13- Is it posible to start Wireshark from command line on Windows?

Sí, lo único que se tiene que hacer es iniciar la línea de comandos y abriremos la ruta donde tenemos la carpeta de Wireshark, después simplemente se escribe “wireshark” y el programa se iniciará si ya lo tenemos instalado.

14- A user is unable to ping a system on the network. How can Wireshark be used to solve the problema.

Yo recomendaría que empezáramos a capturar el tráfico del usuario y que él haga ping. En Wireshark apreciaremos el historial de sus packets y es ahí donde veremos el error, sólo sería cuestión de analizar el paquete y ver si es un error de protocolo o si es algo físico.

15- Which Wireshark filter can be used to check all incoming requests to a HTTP Web server?

tcp.dstport==80

16- Which Wireshark filter can be used to monitor outgoing packets from a specific system on the network?

ip.src==xxx.xxx.xxx.xxx, donde las x reemplazan nuestra dirección ip o de quien queramos analizar, que en sí es la dirección que envía los packets.

17- Wireshark offers two main types of filters.

Los filtros de captura y los filtros de visualización.

18- Which Wireshark filter can be used to monitor incoming packets to a specific system on the network?

ip.dst==xxx.xxx.xxx.xxx donde las x reemplazan nuestra dirección ip o de quien queramos analizar, que en sí es la dirección que recibe los packets.

19- Which Wireshark filter can be used to filter out RDP traffic?

not tcp.port==3389

20- Which Wireshark filter can be used to filter TCP packets with the SYN flag set?

tcp.flags.syn==1

21- Which Wireshark filter can be used to filter TCP packets with the RST flag set?

tcp.flags.reset==1

22- Which Wireshark filter can be used to clear ARP traffic?

arp -d

23- Which Wireshark filter can be used to filter all HTTP traffic?

http

24- Which Wireshark filter can be used to filter Telnet or FTP traffic?

“telnet or ftp” o también “telnet || ftp”

25- Which Wireshark filter can be used to filter Email traffic (SMTP, POP or IMAP)?

smtp || pop || imap

26- List 3 protocols for each layer in TCP/IP model.

- Capa 5 (Aplicación): FTP, DNS, SMTP.
- Capa 4 (Transporte): TCP, UDP, DCCP.
- Capa 3 (Internet): IPv4, IPv6, ARP.
- Capa 2 (Vínculo de datos): PPP, IEEE 802.2
- Capa 1 (Física): Ethernet (802.3), Token ring, FDDI.

27- What does means MX record type in DNS?

“MX” significa “Mail Exchange”, por lo que MX record indica cómo los mails son routeados o encuentran el dominio del servidor destino en relación al protocolo SMTP.

28- Describe the TCP three way handshake.

Es un proceso que hace un cliente y servidor, donde entran las flags de SYN y ACK.

Primero, el cliente manda un SYN al servidor para avisarle que quiere establecer una conexión.

Después, el servidor le responde al cliente con un SYN-ACK para indicarle que recibió el mensaje y acepta la conexión.

Por último, el cliente envía un ACK, asemejándose a un “ok”, que está enterado y así ambos establecen la conexión.

29- Mention the TCP flags.

- Synchronization (SYN).
- Acknowledgement (ACK).
- Finish (FIN).
- Reset (RST).
- Push (PSH).
- Urgent (URG).

30- How ping command can help us to identify the operating System of a remote host?

Gracias al comando podemos saber su dirección IP y al enviar paquetes nos muestra cuántos fueron recibidos y cuántos fallaron, por lo que nos indica también si el host se encuentra disponible.