Examen Wireshark

UNIDAD III

FECHA: 17 - 12 - 2020

Wilmer Rodríguez Jiménez

Fundamentos de telecomunicaciones

Prof. Ismael Jimenez Sanchez

Periodo Ago – Dic

1-Factores a considerar al seleccionar un rastreador de paquetes:

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 pueda filtrar todo el tráfico de red que esté pasando en el momento.

2- ¿Cómo funcionan los rastreadores de paquetes?

Capturaremos el 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 o destino, puerto, longitud de paquetes.

3- Describe el modelo OSI de siete capas.
Capa física 1: Como su nombre lo indica, se engloban todos los aspectos físicos como pinos, componentes eléctricos y cables.
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 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 transporte 4: Aquí sucede la transferencia de datos entre usuarios finales y host. Aplican los protocolos TCP y UDP.
Capa de sesión 5: Habilita la comunicación entre máquinas (computadoras y servidores) al crear una sesión para el proceso.
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 aplicación 7: Es la capa más cercana al usuario, permite el intercambio de datos entre el usuario y las aplicaciones al recibir información de los usuarios.

4- Describe las clasificaciones de tráfico.

Es un proceso en el cual se clasifica el tráfico bajo parámetros como el número de puerto o protocolo. Cuando se basa en el número de puerto es la forma más rápida de clasificación y sin involucrar la privacidad del usuario. Con la inspección profunda de paquetes se requiere un poder de procesamiento alto y detectar aplicaciones y servicios de los paquetes. Por otro lado, está la clasificación estadística donde se pueden detectar aplicaciones desconocidas y sus tipos.

5- Describe el sniffing alrededor de los 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 estás conectado a él.

6- Describe el sniffing en un entorno conmutado.

Los switches sólo envían paquetes hacia máquinas que realmente tienen como 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 y que sólo tienen 1 destino los paquetes.

7- ¿Cómo funciona el envenenamiento de la caché ARP?
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 llegar al atacante, robando información u ocasionando otros problemas.

8- Describe el rastreo en un entorno de enrutador.
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 los beneficios de Wireshark.
Las opciones avanzadas que contiene 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 paquetes 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.

10- Describe los tres paneles de la ventana principal de Wireshark.
1. Es una vista del tráfico capturado en la que se ve el número de paquete, tiempo, origen, destino y la información, se pueden agregar otras características a mostrar como el protocolo y el DNS, pero requiere otra información.
2. Da una información más detallada de características como marco, ethernet y el protocolo del paquete que tengamos seleccionado, por ejemplo, si es HTTP muestra si tuvo un error y de qué tipo fue (códigos).
3. Permite ver la información, texto o código que contiene el paquete que tenemos seleccionado.

11- ¿Cómo configuraría Wireshark para monitorear los paquetes que pasan a través de un enrutador de Internet?
Utilizando la opción para capturas de tráfico y vería todas las fuentes posibles para hacerlo, de ahí si mi computadora está conectada por cable seleccionaría ethernet, elige la opción donde haya fluctuación de actividad

12- ¿Se puede configurar Wireshark en un enrutador Cisco?
No ya que 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- ¿Es posible iniciar Wireshark desde la línea de comandos en 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- Un usuario no puede hacer ping a un sistema en la red. ¿Cómo se puede utilizar Wireshark para resolver el problema?
Capturando 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- ¿Qué filtro de Wireshark se puede usar para verificar todas las solicitudes entrantes a un servidor web HTTP? tcp.dstport==80

16- ¿Qué filtro Wireshark se puede usar para monitorear paquetes salientes de un sistema específico en la red?
ip.src==xxx.xxx.xxx.xxx, donde las x reemplazan nuestra dirección ip o de quien queramos analizar.

17- Wireshark ofrece dos tipos principales de filtros.
Filtros de captura.
Filtros de visualización.

18- ¿Qué filtro de Wireshark se puede usar para monitorear los paquetes entrantes a un sistema específico en la red?
ip.dst==xxx.xxx.xxx.xxx donde las x reemplazan nuestra dirección ip o de quien queramos analizar.

19- ¿Qué filtro de Wireshark se puede utilizar para filtrar el tráfico RDP?
not tcp.port==3389

20- ¿Qué filtro Wireshark se puede usar para filtrar paquetes TCP con el indicador SYN configurado? tcp.flags.syn==1

21- ¿Qué filtro de Wireshark se puede usar para filtrar paquetes TCP con el indicador RST configurado? tcp.flags.reset==1

22- ¿Qué filtro de Wireshark se puede usar para filtrar paquetes TCP con el indicador RST configurado? arp -d

23- ¿Qué filtro de Wireshark se puede utilizar para filtrar todo el tráfico HTTP? http

24- ¿Qué filtro Wireshark se puede utilizar para filtrar el tráfico Telnet o FTP?
“Telnet o ftp” o también “telnet || ftp ”

25- ¿Qué filtro de Wireshark se puede utilizar para filtrar el tráfico de correo electrónico (SMTP, POP o IMAP)? smtp pop imap

26- Enumere 3 protocolos para cada capa en el modelo TCP / IP.
-Capa 1 (Física): Ethernet (802.3), Token ring, FDDI.
-Capa 2 (Vínculo de datos): PPP, IEEE 802.2
-Capa 3 (Internet): IPv4, IPv6, ARP.
-Capa 4 (Transporte): UDP, TCP, DCCP
-Capa 5 (Aplicación): SMTP FTP, DNS

27- ¿Qué significa el tipo de registro MX en DNS?

MX significa Mail Exchange por lo que MX record indica cómo los correos electrónicos son enrutados o se encuentran el dominio del servidor destino en relación al protocolo SMTP.

28- Describe el protocolo de enlace de tres vías de TCP.
Un cliente y servidor realizan un proceso, donde entran las banderas de SYN y ACK.
El cliente manda un SYN al servidor para avisarle que quiere establecer una conexión.
El servidor respondió al cliente con un SYN-ACK para indicarle que recibió el mensaje y acepta la conexión.

29- Menciona las banderas de TCP.
-Reiniciar (RST).
-Sincronización (SYN).
-Urgente (URG).
-Finalizar (FIN).
-Reconocimiento (ACK).
-Presione (PSH).

30- ¿Cómo nos puede ayudar el comando ping a identificar el sistema operativo de un host remoto?

Para que nosotros logremos saber su dirección IP y enviar paquetes nos muestra cuántos fueron recibidos y cuántos fallaron, y así determinar si nuestro host se encuentra disponible.