INSTITUTO TECNOLÓGICO DE CANCÚN

EXAMEN DE WIRESHARK

MIGUEL ÁNGEL OY CASTRO

ENERO-26- 2021

PROFESOR: ISMAEL JIMÉNEZ SÁNCHEZ

FUNDAMENTOS DE TELECOMUNICACIONES

1.- Factores a considerar a la hora de seleccionar un rastreador de paquetes:

los factores a considerar serian que protocolos son compatibles o que protocolos puede soportar el otro seria verificar el diseño del programa del sniffer la instalación también checar el costo o el apoyo de programa y por ultimo que sistema operativo puede soportar.

2.- ¿Cómo funcionan los Packet Sniffers?

R= los packet sniffers o paquetes de sniffers son aquellos que está definidos con la dirección de un paquete y que esta se examina por cada adaptador de red y dispositivo conectado y esto quiere decir también al destino que va dirigido.

3.- Describe el modelo OSI de siete capas.

Se conforman por medio de 7 capas y estas son las siguientes

- **capa física: transmisión** binaria.
- **capa de enlace de datos:**
  Acceso a los medios.
- **capa de red:**
  Direccionamiento y mejor ruta

capa de transporte: conexiones de extremo a extremo.

- **capa de sesión: comunicación** entre host.
- **capa de presentación:**
  Representación de los datos.
- **capa de aplicación:**
  Procesos de red a aplicaciones.

4.- Describe las clasificaciones de tráfico.

Tráfico sensible:

El tráfico sensible es el tráfico que el operador tiene una expectativa de entregar a tiempo. Esto incluye VoIP, juegosen línea, videoconferenciasy navegación web.

Tráfico de mejor esfuerzo:

Este es el tráfico que el ISP considera que no es sensible a las métricas de calidad de servicio (jitter, pérdida de paquetes, latencia).

Tráfico no deseado:

Esta categoría se limita generalmente a la entrega de spam y tráfico creado por gusanos, botnetsy otros ataques maliciosos.

5.- Describe husmear alrededor de hubs.

Bueno al husmear un hus es algo interesate porque se puede ver el tráfico enviado a través de un hub esto quiere decir que se envía a todos los puertos conectados a dicho hub. Por lo que se puede saber es que para poder analizar un equipo en un concentrador, todo lo que tiene que hacer es conectar un rastreador de paquetes.

6.- Describe el olfateo en un entorno conmutado.

Es aquel en donde uno puede ver el trafico de los switches que pueden agregar un nuevo nivel de complejidad. Cuando se conecta un sniffer en unos de los puertos de un Switch, estos se pueden ver solamente el tráfico de un broadcast y el trafico que puede ser transmitido en un dispositivo.

7.- ¿Cómo funciona el envenenamiento de caché ARP?

Pues lo que le entendí al ARP Spoofing permite a los atacantes maliciosos interceptar, modificar o incluso retener datos que están en tránsito. Los ataques de suplantación ARP ocurren en redes de área local que utilizan protocolo de resolución de direcciones (ARP).

8.- Describe el rastreo en un entorno enrutado

Lo que se pueden entender o describir sobre el entorno enrutado es que la importancia en la colocación de un sniffer esto quiere decir que cuando se este solucionando un problema este pueda albercar los segmentos de un red multiple.

9.- Describe los Beneficios de Wireshark

Wireshark es el estándar de facto en las herramientas de analizador de red.

Se distingue como analista de red

Enlace con la única fuente de la verdad de la red - los paquetes.

Encontrar problemas antes de que lo hagan los usuarios.

Wireshark es gratis

Saber lo que realmente está sucediendo en su red (en casa o en el trabajo).

10.- Describe los tres paneles de la ventana principal de Wireshark

El panel de Lista de PDU (o Paquete): ubicado en la parte superior del diagrama muestra un resumen de cada paquete capturado.
El panel de detalles de PDU (o Paquete): ubicado en el medio del diagrama, muestra más detalladamente el paquete seleccionado en el panel de Lista del paquete.

El panel de bytes de PDU (o paquete): ubicado en la parte inferior del diagrama, muestra los datos reales (en números hexadecimales que representan el binario real) del paquete seleccionado en el panel de Lista del paquete y resalta el campo seleccionado en el panel de Detalles del paquete

11.- ¿Cómo configurarías Wireshark para monitorear los paquetes que pasan a través de un enrutador de Internet?

R=Se podría atraves de configurar un sistema en la red el puerto apropiado del conmutador al que están conectadas al sistema y el enrutador de internet.

12.- ¿Se puede configurar wireshark en un router Cisco?

R=no es posible configurar enrutador cisco ya que ejecuta un sistema operativo propietario en el que no se pueden instalar herramientas.

13.- ¿Es posible iniciar Wireshark desde la línea de comandos en Windows?

R= si es posible iniciar wireshark por el ejecutable por medio del código de sistema el comando seria wireshark.exe este seria para iniciar "wireshark -i2 k -f "host 192.168.1.5" -s512"

14.- Un usuario no puede hacer ping a un sistema en la red. ¿Cómo se puede utilizar Wireshark para resolver el problema?

Lo mejor seria hacer un ping en icmp esto quiere decir que comprueba si los paquetes icmp se envían desde el sistema o si esta recibiendo paquetes

15.- ¿Qué filtro Wireshark se puede utilizar para verificar todas las solicitudes entrantes a un servidor web HTTP?

R= se utiliza este filtro tcp.dsport==80

16.- ¿Qué filtro Wireshark se puede usar para monitorear los paquetes salientes de un sistema específico en la red?

R= este filtro se puede usar para paquetes salientes es el el siguiente "ip.src ==192.168.1.2"

17.- Wireshark ofrece dos tipos principales de filtros:

R= los tipos de filtros que usa son los de captura y de visualización.

18.- ¿Qué filtro Wireshark se puede utilizar para monitorear los paquetes entrantes a un sistema específico en la red?

R= se puede crear un filtro para poder monitorear una red especifica o elegir una existente como el filtro "host".

19.- ¿Qué filtro Wireshark se puede utilizar para filtrar el tráfico RDP?

R= para visualizar se puede utilizar el filtro “rdp”

20.- ¿Qué filtro Wireshark se puede utilizar para filtrar paquetes TCP con la bandera SYN configurada?

R=con este filtros puede utilizar para filtrar los paquete tcp.flags.syn.

21.- ¿Qué filtro Wireshark se puede utilizar para filtrar paquetes TCP con la bandera RST configurada?

R= no se puede realizar solo se puede utilizando el segmento de TCP

22.- ¿Qué filtro Wireshark se puede utilizar para despejar el tráfico ARP?

R: con este filtro es posible despejar el trafico arp solo usando este filtro Netflow

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

R=con el filtro “http.request es posible filtrar un trafico http porque nos pude mostrar su get y el post.

24.- ¿Qué filtro Wireshark se puede utilizar para filtrar el tráfico Telnet o FTP?

R=con el Filtro de captura es posible hacer el trafico de red de telnet o de un ftp.

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

R:=seria el filtro SMTP es el que se encarga de filtrar el trafico de un correo electrónico.

26.- Enumere 3 protocolos para cada capa en el modelo TCP / IP Capa

4 o de Aplicación:

equivalente a las capas: 5 (sesión), 6 (presentación) y 7 (aplicación), del modelo OSI. Maneja aspectos de representación, codificación y control de la información.

Capa 3 o de Transporte:

similar a la capa 4 (transporte) del modelo OSI. Proporciona fundamentalmente una conexión lógica entre el emisor y el receptor, segmentando y reensamblando los datos, junto con mecanismos que permiten conocer el estado de la transmisión. **Capa 2 o de Internet**:

asimilable a la capa 3 (red) del modelo OSI. Se encarga de seleccionar la mejor ruta para enviar paquetes a través de la red; es responsable de proporcionar el paquete de datos (datagrama).

Capa 1 o de Interfaz de Red:

equivalente a las capas 2 (enlace de datos) y 1 (física) del modelo OSI. Responsable de la colocación de los paquetes de datos en la red y de la recepción de los mismos.

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

R:=es un tipo de registro, un recurso DNS . Los registros MX apuntan a los servidores a los cuales envían un correo electrónico, y a cuál de ellos debería ser enviado en primer lugar, por prioridad.

28.- Describe el TCP Three Way HandShake

R=pues es aquel procedimiento que se hace es que dos dispositivos puedan intercambiarse unos en si a fin de poder establecer un sección y una sincronización.

29.- Mencionar las banderas de TCP

R= estas son algunas banderas tcp que se utilizan

- SYN: Synchronisation,
- ACK: Acknowledgment,
- FIN: Finished,
- RST: Reset,
- PSH: Push,
- URG: Urgent,
- ECE,
- CWR: Congestion Windows Reduced,
- NS: Nonce Sum

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

Nos permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP. Sirve para determinar si una dirección IP específica o host es accesible desde la red o no