Nombre de la Materia: Fundamentos de Telecomunicaciones	Aula
Nombre de la Licenciatura: Ing. Sistemas Computacionales.	
Nombre del Alumno(a): Pool Ramírez Miguel Ángel.	
Número de Control: 18530437.	
Nombre de la Tarea: Examen Wireshark	
Nombre del Profesor(a): Ing. Ismael Jiménez Sánchez Fecha: 17/12/20	

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

- Protocolos soportados
- Todos los rastreadores de paquetes pueden interpretar varios protocolos. La mayoría de los
- sniffers pueden interpretar todos los protocolos más comunes tales como DHCP, IP, y ARP,
- pero no todos pueden interpretar algunos de los protocolos más no tradicional. Al elegir un
- sniffer, asegúrese de que es compatible con los protocolos que va a utilizar.
- Userfriendliness
- Considere el diseño del programa del sniffer del paquete, la facilidad de instalación, y el
- flujo general de las operaciones estándar. El programa que elija debe ajustarse a su nivel de
- experiencia
- Costo
- Apoyo al programa
- Soporte del sistema operativo

2.¿Cómo funcionan los detectores de paquetes?

La detección, rastreo o sniffing de paquetes es la práctica de obtener, recopilar y registrar algunos o todos los paquetes que pasan a través de una red de ordenadores, independientemente de cómo se enruten dichos paquetes.

Un rastreador de paquetes, también llamado a veces analizador de paquetes, se compone de dos partes principales. Primero, un adaptador de red que conecta el rastreador a la red existente. Segundo, un software que proporciona una forma de registrar, ver o analizar los datos recopilados por el dispositivo.

3.Describa el modelo OSI de siete capas.

	Unidad de Datos	**Nivel o Capa**
Capa del Anfitrión	**Dato**	7.- Aplicación: Se compone de los servicios y aplicaciones de comunicación estándar que puede utilizar todo el mundo.
	Dato	6.- Presentación: Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el Sistema.
	Dato	5.- Sesión: Administra las conexiones y terminaciones entre los sistemas que cooperan.

	Segmento	4.- Transporte: Administra la transferencia de datos. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos.
Capas del Medio	**Paquete**	3.- Red: Administra las direcciones de datos y la transferencia entre redes.
	Trama	2.- Enlace de Datos: Administra la transferencia de datos en el medio de red.
	Bit	1.- Físico: Define las características del hardware de red.

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. Los esquemas de gestión del tráfico se adaptan típicamente de tal manera que la calidad del servicio de estos usos seleccionados está garantizada, o al menos priorizada sobre otras clases de tráfico.

Tráfico de mejor esfuerzo

El mejor tráfico de esfuerzo es todos los otros tipos de tráfico no detrimental. 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. En algunas redes, esta definición puede incluir tráfico como VoIP no local.

5. Describa el sniffing alrededor de los hubs

El tráfico enviado a través de un concentrador (hub) se envía a todos los puertos conectados a ese concentrador. Por lo tanto, para analizar un equipo en un concentrador, todo lo que tiene que hacer es conectar un rastreador de paquetes a un puerto vacío en el concentrador, y puede ver toda la comunicación hacia y desde todos los equipos conectados a ese concentrador.

6.Describa el sniffing en un entorno cambiado.

Los conmutadores son el tipo más común de dispositivo de conexión utilizado en entornos de red modernos. Proporcionan una manera eficiente de transportar los datos vía el broadcast, el unicast,

y el tráfico de multidifusión. Como ventaja, los conmutadores permiten la comunicación dúplex completa, lo que significa que las máquinas pueden enviar y recibir datos simultáneamente.

Desafortunadamente para los analistas de paquetes, los switches agregan un nuevo nivel de complejidad. Cuando usted conecta un sniffer con un puerto en un Switch, usted puede ver solamente el tráfico de broadcast y el tráfico transmitido y recibido por su máquina.

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

El ataque de suplantación DE ARP es un tipo de ataque en el que un atacante envía mensajes ARP falsificados (Protocolo de resolución de direcciones) a través de una LAN. Como resultado, el atacante vincula su dirección MAC con la dirección IP de un equipo (o servidor) legítimo en la red. Si el atacante logró vincular su dirección MAC a una dirección IP auténtica, comenzará a recibir cualquier dato al que pueda acceder esa dirección IP. La suplantación de ARP permite a los atacantes malintencionados interceptar, modificar o incluso detener los datos que están en tránsito. Los ataques de suplantación ARP solo pueden ocurrir en redes de área local que utilizan el Protocolo de resolución de direcciones.

8.Describa el snnifiing en un entorno enrutado

Todas las técnicas para aprovechar el cable en una red conmutada también están disponibles en redes enrutadas. La única consideración importante al tratar con los entornos ruteados es la importancia de la colocación del sniffer cuando usted está solucionando problemas un problema que abarque los segmentos de red múltiples.

El dominio de broadcast de un dispositivo se extiende hasta que alcanza un router. En este momento el tráfico se entrega al router ascendente siguiente y usted pierde la comunicación con los paquetes que se transmiten hasta que usted reciba un acuse de recibo. En situaciones como esta donde los datos deben atravesar a los routeres múltiples, es importante analizar el tráfico en todos los lados del router.

9.Describa los beneficios de wireshark

Wireshark es un software que analiza paquetes enviados a través de una red. Mostrará cada paquete y los detalles dentro del paquete. Los administradores de red lo utilizan para analizar la red y solucionar un problema si ven un problema.

10. Los tres paneles de la ventana principal de Wireshark

- El panel de lista de paquetes muestra un resumen de cada paquete capturado. Al hacer clic en los paquetes de este panel, puede controlar lo que se muestra en los otros dos paneles.
- El panel de detalles del paquete muestra el paquete seleccionado en el panel de lista de paquetes con más detalle.
- El panel de bytes de paquetes muestra los datos del paquete seleccionado en el panel de lista de paquetes y resalta el campo seleccionado en el panel de detalles del paquete.

11.- ¿Cómo configurarías wireshark para monitorear los paquetes que pasan por un enrutador de internet

Un sistema en la red se puede configurar y configurar con wireshark. El puerto apropiado en el Switch con el cual el sistema y el router de Internet está conectado se pueden configurar para la duplicación del puerto. Todos los paquetes que pasan a través de la interfaz del switch al router se pueden reflejar en el sistema en el cual se configura wireshark.

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

Wireshark es un ejecutable. Se puede configurar en sistemas operativos como Windows y Linux. No se puede configurar en un router Cisco, ya que funciona con un sistema operativo propietario en el que no se pueden instalar herramientas o software adicionales.

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

Sí, es posible empezar a usar el ejecutable adecuado en Windows que es wireshark.exe

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

Ping utiliza ICMP. Wireshark se puede utilizar para marcar si los paquetes ICMP se están enviando desde el sistema. Si se envía, también se puede marcar si se reciben los paquetes.

15.- ¿Qué filtro de wireshark se puede utilizar para comprobar todas las peticiones entrantes a un servidor web HTTP?

Los servidores web HTTP utilizan el puerto TCP 80. Las solicitudes entrantes al servidor web tendrían el número de puerto de destino como 80. Por lo tanto, el filtro tcp.dstport-80.

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

Los paquetes salientes contendrían la dirección IP del sistema como su dirección de origen. Así que suponiendo que la dirección IP del sistema es 192.168.1.2, el filtro sería ip.src-192.168.1.2

17.- Wireshark ofrece dos tipos principales de filtros:

Filtro de captura

Puede establecer un filtro de captura antes de comenzar a analizar una red. Cuando usted fija un filtro de la captura, captura solamente los paquetes que hacen juego el filtro de la captura.
Por ejemplo, si usted necesita solamente escuchar los paquetes que se envían y reciben de una dirección IP, usted puede fijar un filtro de la captura como sigue.
host 192.168.0.1

Filtros de pantalla

Los filtros de visualización se aplican a los paquetes de captura. Por ejemplo, si desea mostrar solo las solicitudes que se originan a partir de una ip determinada, puede aplicar un filtro de visualización de la siguiente manera:
ip.src==192.168.0.1

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

Los paquetes salientes contendrían la dirección IP del sistema como su dirección de origen. Así que suponiendo que la dirección IP del sistema es 192.168.1.2, el filtro sería ip.src-192.168.1.2

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

!tcp.port-3389

20.- ¿Qué filtro wirehark se puede utilizar para filtrar los paquetes TCP con el conjunto de banderas SYN

(tcp.flags.syn == 1)

21. ¿Qué filtro "Wireshark" se puede usar para filtrar los paquetes TCP con la bandera RST puesta?

(tcp.flags.reset == 1)

22.- ¿Qué filtro Wireshark puede ser usado para limpiar el tráfico de ARP

not arp

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

http / mostrar todo el tráfico http: tcp.dstport 80

24.- ¿Qué filtro wireshark puede ser usado para filtrar el tráfico de Telnet o FTP

telnet

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

Mostrar solo el tráfico basado en SMTP:

smtp

Muestre solamente el tráfico basado SMTP con el comando "MAIL FROM":

smtp.req.parameter contains "FROM"

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

Capa de Aplicación:

Ofrece a las aplicaciones la capacidad de acceder a los servicios de las otras capas y define los protocolos que utilizan las aplicaciones para intercambiar datos.

1.- HTTP (Hypertext Transfer Protocol): se utiliza para transferir archivos que componen las páginas Web de la World Wide Web.

2.- FTP (File Transfer Protocol): se utiliza para la transferencia interactiva de archivos.

3.- DNS (Domain Name System): se utiliza para resolver un nombre de host a una dirección IP.

Capa de Transporte:

La capa de transporte se encarga de establecer una conexión lógica entre el dispositivo transmisor y el receptor.

1.- TCP (Transmission Control Protocol): proporciona un servicio de comunicaciones fiable orientado a la conexión punto a punto.

2.- UDP (User Datagram Protocol): proporciona una conexión, punto a punto, o uno a muchos poco fiable, aunque rápido y con poca carga adicional en la red.

3.- SCTP admite conexiones entre sistema que tienen más de una dirección, o de host múltiple.

Capa de Internet:

La capa de Internet es responsable de las funciones de direccionamiento, empaquetado y enrutamiento.

1.-IP (Internet Protocol): es el protocolo responsable del direccionamiento IP, enrutamiento, fragmentación, y reensamblado de los paquetes de datos entre los dispositivos conectados a una red.

2.- ARP (Address Resolution Protocol): es responsable de la resolución de la dirección de la capa de Internet a la dirección de la capa de interfaz de red.

3.- ICMP (Internet Control Message Protocol): es responsable de proporcionar funciones de diagnóstico y notificación de errores debidos a la entrega sin éxito de paquetes IP.

Capa de Interfaz a Red

La capa de interfaz de red, también conocida como de acceso de red, es responsable de la colocación y recepción de paquetes en la red

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

Un registro MX es un tipo de registro, un recurso DNS que especifica cómo debe ser encaminado un correo electrónico en internet. 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.- Describa el TCP Three Way HandShake

El proceso de "Three-way Handshake" es el procedimiento por el cual dos dispositivos intercambian una serie de mensajes a fin de poder establecer una sesión y sincronizar sus "Sequence Numbers".

29.- Mencionar las banderas del TCP

Synchronization (SYN): Se utiliza en el primer paso de la fase de establecimiento de conexión o el proceso de Three-way Handshake entre los dos hosts.

Acknowledgement (ACK): Se utiliza para reconocer los paquetes que son recibidos con éxito por el host. El indicador se establece si el campo de número de confirmación contiene un número de acuse de recibo válido.

Reset (RST): Se utiliza para terminar la conexión si el remitente RST siente que algo está mal con la conexión TCP o que la conversación no debe existir.

Push (PSH): La capa de transporte de forma predeterminada espera algún tiempo para que la capa de aplicación envíe suficientes datos iguales al tamaño máximo del segmento para que el número de paquetes transmitidos en la red minimice lo que no es deseable por alguna aplicación como aplicaciones interactivas (chat).

Urgent (URG): Los datos dentro de un segmento con el indicador URG 1 se reenvían inmediatamente a la capa de aplicación, incluso si hay más datos que se entregarán a la capa de aplicación. Se utiliza para notificar al receptor para procesar los paquetes urgentes antes de procesar todos los demás paquetes.

Finish (FIN): Se utiliza para solicitar la terminación de la conexión, es decir, cuando no hay más datos del remitente, solicita la terminación de la conexión. Este es el último paquete enviado por el remitente. Libera los recursos reservados y termina correctamente la conexión.

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

El objetivo de un ping es determinar si un host destino, identificado con una determinada IP, es accesible desde otro host.

Para ello, el host origen envía al host destino un paquete de información de 32 bytes mediante el protocolo ICMP y espera una contestación de éste, que debe contener los mismos datos. Si la respuesta llega correctamente, el ping ha sido satisfactorio. Si por el contrario el ping falla, entonces es que o bien la petición del host origen o bien la respuesta del host destino se han perdido por el camino