MOEN AKE GERALDY MARÍA

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

- Protocolos compatibles
- La facilidad de uso
- Costo
- Soporte para el programa
- Soporte del sistema operativo

2.- ¿Cómo funcionan los detectores de paquetes?

Es un programa para monitorizar y analizar el tráfico en una red de computadoras, detectando los cuellos de botella y problemas que existan. También puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red.

3.- Describir el modelo OSI de siete capas

El modelo OSI está conformado por 7 capas o niveles de abstracción.

- Nivel físico
- Nivel de enlace de datos
- Nivel de red
- Nivel de transporte
- Nivel de sesión
- Nivel de presentación
- Nivel de aplicación

4.- Describe las clasificaciones de tráfico.

- **Tráfico de difusión**: Un paquete de difusión es aquel que se envía a todos los puertos de un segmento de red, independientemente de si ese puerto es un concentrador o un conmutador.
- **La multidifusión:** Es un medio de transmitir un paquete desde una única fuente a varios destinos simultáneamente.
- **Tráfico de unidifusión:** Un paquete de unidifusión se transmite de una computadora directamente a otra.

5.- Describe sniffing around hubs.

El tráfico enviado a través de un "hub" se envía a todos los puertos conectados a ese hub. Por lo tanto, para analizar una computadora en un "hub", simplemente conecte un rastreador de paquetes a un puerto vacío en el hub, y permitirá ver todas las comunicaciones hacía y desde todas las computadoras conectadas a ese hub.

6.- Describe el sniffing en un entorno conmutado

En un entorno de red conmutada, los paquetes solo se envían al puerto al que están destinados, de acuerdo con sus direcciones MAC de destino.

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

El envenenamiento de la caché ARP, es el proceso de enviar mensajes ARP a un conmutador o enrutador Ethernet con direcciones MAC falsas para interceptar el tráfico de otra computadora.

8.- Describe el rastreo en un entorno enrutado

El dominio de transmisión de un dispositivo se extiende hasta que llega a un enrutador. En este punto, el tráfico se transfiere al siguiente enrutador ascendente y pierde la comunicación con los paquetes que se transmiten hasta que recibe un acuse de recibo. En situaciones como esta, donde los datos deben atravesar varios enrutadores, es importante analizar el tráfico en todos los lados del enrutador.

9.- Describe los Beneficios de Wireshark

- Protocolos compatibles
- La facilidad de uso
- Costo
- Soporte para el programa
- Soporte del sistema operativo

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

El panel de la lista de paquetes (Arriba), el panel de detalles del paquete (Medio) y el panel de bytes del paquete (Abajo).

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

En el puerto apropiado del switch se puede configurar para la duplicación de puertos. Todos los paquetes que pasan a través de la interfaz del switch al router pueden reflejarse en el sistema en el que está configurado Wireshark.

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

No, Wireshark solo se puede ejecutar en sistemas operativos.

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

Si, si es posible usando el comando Wireshark.exe

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

Dado que ping usa ICMP, Wireshark se puede usar para verificar si los paquetes ICMP se están enviando desde el sistema.

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

Los servidores web HTTP usan el puerto TCP 80. Las solicitudes entrantes al servidor web tendrían el número de puerto de destino como 80. Entonces, el filtro tcp.dstport == 80.

16.- ¿Qué filtro de wireshark se puede utilizar 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. Entonces, asumiendo 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

- Los filtros de captura: se especifican cuando se capturan paquetes y capturarán solo aquellos paquetes que se especifiquen para su inclusión / exclusión en la expresión dada.
- Los filtros de visualización: se aplican a un conjunto existente de paquetes capturados para ocultar los paquetes no deseados o mostrar los paquetes deseados en función de la expresión específica.

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

ip.dst==192.168.1.1

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

Puede filtrar los protocolos RDP durante la captura, ya que siempre se usa tcp port 3389

20.- ¿Qué filtro de wireshark se puede usar para filtrar paquetes TCP con el indicador SYN configurado?

El filtro es tcp.flags.syn==1

21.- ¿Qué filtro wireshark se puede utilizar para filtrar paquetes TCP con el indicador RST establecido

tcp.flags.rst==1

22.- ¿Qué filtro wireshark se puede utilizar para borrar ARP traffc

!arp

23.- ¿Qué filtro 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

tcp.port==23 || tcp.port 21

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

smtp || pop || imap

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

- Capa de acceso a red: Protocolo, ARP
- Capa de red: Protocolo, IP, IPV4
- Capa de transporte: Protocolo, TCP, UDP
- Capa de aplicación: Protocolo, Telnet, HTTP, DNS

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

Intercambio de correo, es principalmente una lista de servidor de intercambio de correo que se debe utilizar para el dominio.

28.- Describa el TCP Three Way HandShake

Es un proceso de tres pasos que requiere que el cliente y el servidor intercambien paquetes de sincronización y confirmación antes de que se inicie el proceso de comunicación de datos real.

29.- Mencione las banderas TCP

CWR: El host emisor establece el indicador de ventana reducida de congestión para indicar que recibió un segmento TCP con el indicador de ECE establecido.

ECE (ECN-Echo): Indica que el par TCP es compatible con ECN durante el protocolo de enlace de 3 vías.

URG: Indica que el campo del puntero URGent es significativo

ACK: Indica que el campo ACKnowledgment es significativo (a veces abreviado por tcpdump como “.”)

PSH: Función de empuje

RST: Restablecer la conexión (visto en conexiones rechazadas)

SYN: Sincronizar números de secuencia (visto en nuevas conexiones)

FIN: No hay más datos del remitente (visto después de que se cierra una conexión)

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

Al ejecutar el comando ping, el protocolo ICMP envía al host un determinado datagrama para solicitar una respuesta. El protocolo ICMP se ocupa de los errores en las redes TCP/IP. Al utilizar ping, se puede saber si el host remoto dispone de conexión