Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

“Examen Wireshark”

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

1. - Factors to consider when selecting a packet sniffer:

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.- How Packet Sniffers Work?

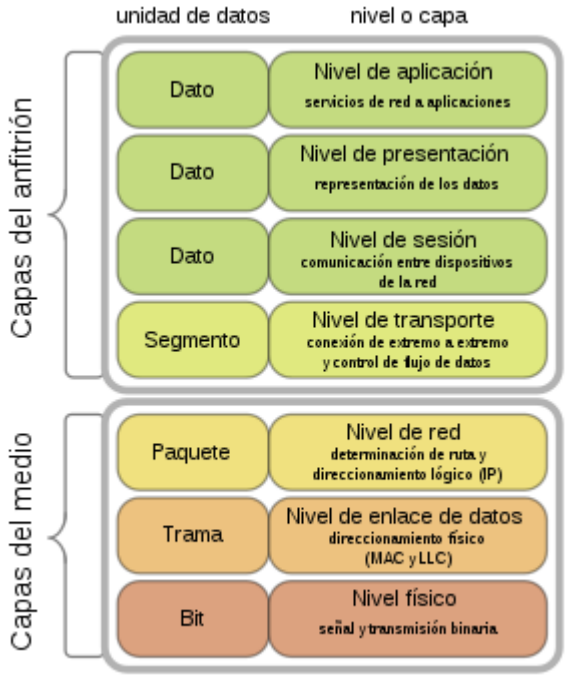
2.- ¿Cómo funcionan los detectores de paquetes?

Los paquetes Sniffer son un programa para monitorizar y analizar el tráfico en una red de computadoras, detectando los cuellos de botella y problemas que existan. También ser utiliza para "captar" los datos que son transmitidos en la red.

3.- Describe The Seven-Layer OSI Model

3.- Describir el modelo OSI de siete capas

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



4.- Describe Traffic Classifications.

4.- Describe las clasificaciones de tráfico.

El tráfico de red se puede dividir en tres clases principales: difusión, multidifusión y unidifusión.

Tráfico de difusión: Es aquel que se envía a todos los puertos de un segmento de red sin importar si este puerto es concentrador o conmutador.

La multidifusión es un medio el cual transmite un paquete desde una única fuente a varios destinos de manera simultánea. Simplifica este proceso mediante el menor ancho de banda posible.

Tráfico de unidifusión Un paquete de unidifusión se transmite de una computadora directamente a otra. Los detalles de las funciones de unidifusión dependen del protocolo que lo utilice.

5.- Describe sniffing around hubs.

El tráfico enviado a través de un "hub" se envía a todos los puertos conectados a ese hub. 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 hacia y desde todas las computadoras conectadas a ese hub.

6.- Describe sniffing in a switched environment

6.- Describe el sniffing en un entorno conmutado

Los conmutadores agregan un nivel completamente nuevo de complejidad al trabajo de un analista de paquetes. 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. - How ARP Cache Poisoning Works?

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 sniffing in a routed environment

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 the Benefits of wireshark

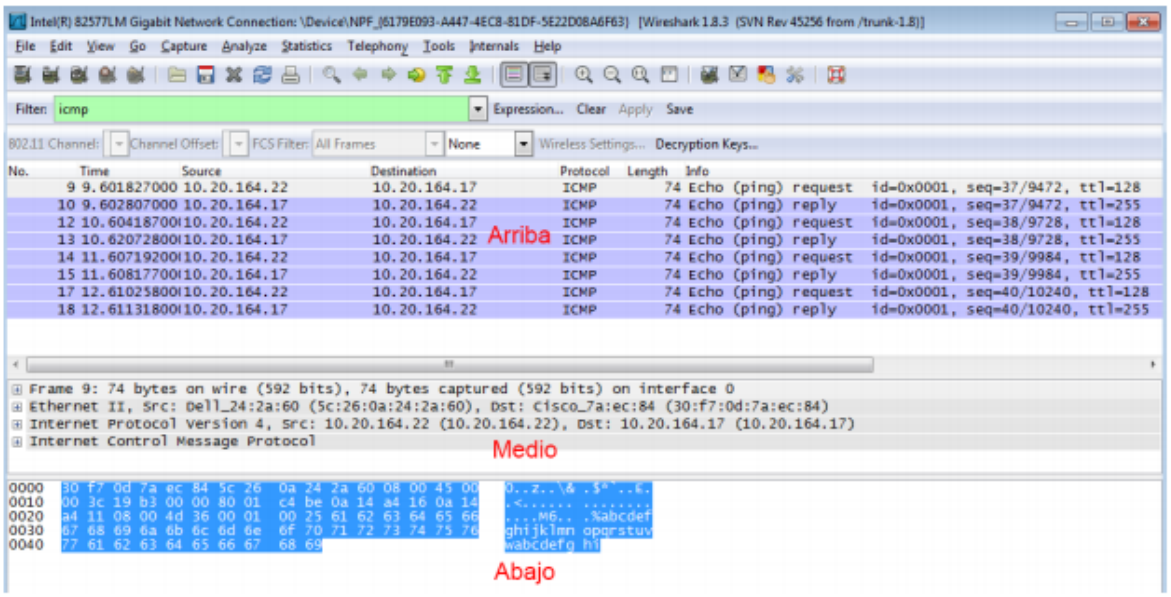
9. - Describe los Beneficios de Wireshark

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

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

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. How would you setup wireshark to monitor packets passing through an internet router?

¿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. Can wireshark be setup on a Cisco router?

¿Se puede configurar wireshark en un router Cisco?

No porque Wireshark es un programa ejecutable y solo se puede ejecutar en sistemas operativos.

13. Is it possible to start wireshark from command line on Windows?

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

Si, si es posible usando el comando Wireshark.exe

14. A user is unable to ping a system on the network. How can wireshark be used to solve the problem?

Un usuario no puede hacer ping a un sistema en la red. ¿Cómo se puede utilizar Wirehark 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. Si se envía, también se puede comprobar si se están recibiendo los paquetes.

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

¿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, el filtro tcp.dstport == 80.

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

¿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 offers two main types of filters

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. Which wireshark filter can be used to monitor incoming packets from a specific system on the network?

¿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. Which Wireshark filter can be used to filter out RDP traffic?

¿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. Which wireshark filter can be used to Filter TCP packets with SYN flag set?

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

El filtro es tcp.flags.syn==1

21.- Which wireshark filter can be used to filter TCP packets with the RST flag set

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

tcp.flags.rst==1

22.- Which wireshark filter can be used to Clear ARP traffc

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

!arp

23.- Which wireshark filter can be used to filter All HTTP traffic

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

http

24.- Which wireshark filter can be used to filter Telnet or FTP traffic

- ¿Qué filtro wireshark se puede utilizar para filtrar el tráfico Telnet o FTP

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

25.- Which wireshark filter can be used to filter Email traffc (SMTP, POP, or IMAP)

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

smtp || pop || imap

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

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

1° capa de acceso a red: Protocolo, ARP

2° Capa de red: Protocolo IP, IPv4

3° Capa de transporte: Protocolo TCP, UDP

4° Capa de aplicación: Protocolo, Telnet, HTTP, DNS

27. - What does means MX record type in DNS?

- ¿Qué significa tipo de registro MX en DNS?

El registro "MX" o intercambio de correo es principalmente una lista de servidor de intercambio de correo que se debe utilizar para el dominio.

28. - Describe the TCP Three Way HandShake

- 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.

El proceso de apretón de manos de tres vías está diseñado de tal manera que ambos extremos le ayudan a iniciar, negociar y separar las conexiones de socket TCP al mismo tiempo. Le permite transferir varias conexiones de socket TCP en ambas direcciones al mismo tiempo.

29.- Mention the TCP Flags

- Mencione las banderas TCP

CWR: el host emisor establece el indicador de ventana reducida de congestión (CWR) 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. - How ping command can help us to identify the operating system of a remote host?

- ¿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