INSTITUTO TECNOLÓGICO DE CANCÚN

INGENIERÍA EN
SISTEMAS COMPUTACIONALES

MATERIA:
FUNDAMENTOS DE TELECOMUNICACIONES

TAREA:
EXAMEN DE WIRESHARK.

NUMERO DE CONTROL Y NOMBRE DEL ALUMNO:
18530369 CRUZ GÓNGORA FERNANDO JÓSE

HORARIO:
LUNES A JUEVES
17:00 PM – 18:00 PM

MAESTRO:
ING. ISMAEL JIMÉNEZ SÁNCHEZ

1.- Factors to consider when selecting a package tracker:

For this the factors should take into account would be which protocols are supported or which protocols can support the other would be to verify the design of the sniffer program.

2.- How do package trackers work?

For this, packet trackers work so that those packets are defined with the address of a packet that is examined by each network adapter and connected device to determine which node in that packet it is destined to.

3.- Describe the seven-layer OSI model.

Physical layer: binary transmission.

Data binding layer: media access.

Network layer: addressing and better route

Transport layer: end-to-end connections.

Session layer: Host-to-host communication.

Presentation layer: Representation of the data.

Application layer: Network processes to applications.

4.- Describe traffic classifications.

1. **SENSITIVE TRAFFIC:** This traffic can be sensitive with traffic that the operator has the expectation of delivering on time.
2. **BEST EFFORT TRAFFIC:** This is the best effort traffic is all other non-detrimental traffic types.
3. **UNWANTED TRAFFIC:** This category is usually limited to the delivery of spam and traffic created by worms, botnets and other malicious attacks. type.

5.- Describe the tracking around the centers.

The color on a network that has hubs installed is a packet analyst's dream. Traffic sent through a hub is sent to all ports connected to that hub.

6.- Describe sniffing in a switched environment.

Switches add a new level of complexity this do so when the scheduler connects a sniffer to a port on a switch and can see only broadcast traffic and traffic transmitted and received by its machine.

7.- How does ARP cache poisoning work?

ARP poisoning is usually used for man attacks in the middle. This is why the attacker generates a series of ARP packets with false information that alters the ARP tables of the victim's hosts.

8.- Describe sniffing in a routed environment

The only important consideration when dealing with routed environments is the importance of sniffer placement when you are troubleshooting an issue that spans multiple network segments.

9.- Describe the benefits of Wireshark

1. The Wireshark is the de facto standard in network analysis tools. He distinguishes as a network analyst
2. It is a link to the only real source of the network - packets. Find problems before users.
3. Wireshark is free
4. Know what is actually happening on your network (at home or at work).

10.- Describe the three panels in the main window in Wireshark

THE PACKET LIST: This shows packets that have been captured showing the packet number, the time it was captured, the source address, destination address, packet protocol, and additional information.

PACKAGE DETAILS: This shows us the headers and data that make up the package selected in the package list.

PACKAGE BITS: This is ours the same data as in the previous panel, only presented in hexadecimal.

11.- How would you configure Wireshark to monitor packets passing through an Internet router?

The first thing I would do would be to configure it and then it would be to install a program that is similar to Wireshark to be able to analyze packages.

12.- Can Wireshark be configured on a Cisco router?

If it is possible to configure a Cisco router on wireshark it can be done by configuring the router and wireshark what cannot be configured to the Cisco router while running a proprietary operating system where tools cannot be installed

13.- Is it possible to start wireshark from the command line in Windows?

If you can only start wireshark through system code, the command would be this host "wireshark -i2 -k -f" 192.168.1.5 "-s512"

14.- A user cannot ping a system on the network. How can I use wireshark to resolve the issue?

Ping uses ICMP. Wireshark can be used to check if ICMP packets are being sent from the system. If sent, you can also check if the packets are being received.

15.- What wireshark filter can be used to check all incoming requests to an HTTP Web server?

It's the **http.response filter**

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

This is a filter that is used for outgoing packets is the following "dst host"

17.- Wireshark offers two main types of filters:

The 2 types offered by Wireshark would be:

Capture

Show filters

18.- What wireshark filter can be used to monitor incoming packets to a specific system on the network?

You can create a filter so that you can monitor a specific network or choose an existing one as the "host" filter.

19.- Which Wireshark filter can be used to filter RDP traffic?

To display you can use the filter "rdp"

20.- Which wireshark filter can be used to filter TCP packets with the SYN flag set

These filters are used in **tcp.flags.syn packets in** order to filter.

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

The only ones are the TCP segments

22.- What wireshark filter can be used to delete ARP traffc?

It's the Netflow Filter

23.- What wireshark filter can be used to filter all HTTP traffic?

It's the "http" filter. request" it is possible to get all the http

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

It's the Capture Filter

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

It's the SMTP protocol

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

They would be the protocols of:

4 transports

3 Internet

1 data link

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

It is a type is a type of record, which is a DNS resource that specifies how an email should be routed on the Internet

28.- Describe TCP Three Way HandShake

This is a procedure by which two devices exchange a series of messages to establish a session and synchronize their "sequence numbers".

29.- Mention TCP flags

1. **SYN:** Synchronization
2. **ACK:** Recognition
3. **END: Finished,**
4. **RST:** Reset
5. **PSH:** Push
6. **URG:** Urgent
7. **ECE**
8. **CWR:** Reduced Windows Congestion
9. **NS:** Nonce Sum

30.- How can the ping command help us identify the operating system of a remote host?

This allows us to check the status of a specific connection from a local host with at least one remote computer on a TCP/IP type network. It is typically used to determine whether a specific IP address or host is accessible from the network or not

PREGUNTAS (español)

1.- Factores a tener en cuenta al seleccionar un rastreador de paquetes:

Para esto los factores deben de tener en cuenta serían qué protocolos son compatibles o qué protocolos pueden soportar el otro sería verificar el diseño del programa sniffer.

2.- ¿Cómo funcionan los rastreadores de paquetes?

Para esto los rastreadores de paquetes funcionan de manera de que esos paquetes se definen con la dirección de un paquete que es examinada por cada adaptador de red y dispositivo conectado para determinar a qué nodo de ese paquete está destinado.

3.- Describa el modelo OSI de siete capas.

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.- Describir clasificaciones de tráfico.

1. **TRÁFICO SENSIBLE:** Este tráfico puede ser sensible con el tráfico que el operador tiene la expectativa de entregar a tiempo.
2. **MEJOR TRAFFIC DE EFFORT:** Este es el mejor tráfico de esfuerzo es todos los otros tipos de tráfico no detrimental.
3. **TRAFFIC NO DESEADO:** Esta categoría se limita generalmente a la entrega de spam y tráfico creado por gusanos, botnets y otros ataques maliciosos. tipo.

5.- Describa el rastreo alrededor de los centros.

El color en una red que tiene concentradores instalados es el sueño de un analista de paquetes. El tráfico enviado a través de un concentrador se envía a todos los puertos conectados a ese concentrador.

6.- Describa el olfateo en un entorno conmutado.

Los conmutadores añaden un nuevo nivel de complejidad esto lo hacen cuando el programador se conecta un sniffer con un puerto en un Switch y puede ver solamente el tráfico de broadcast y el tráfico transmitido y recibido por su máquina.

7.- ¿Cómo funciona la intoxicación por caché ARP?

La intoxicación por ARP por lo normal se utiliza para ataques de hombre en el medio. Por esto el atacante genera una serie de paquetes ARP con información falsa que altera las tablas ARP de los hosts de la víctima.

8.- Describa el olfateo en un entorno enrutado

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.

9.- Describa los beneficios de Wireshark

1. El Wireshark es el estándar de facto en las herramientas de análisis de red. Se distingue como analista de red

2. Es un Enlace a la única fuente de verdad de la red - paquetes. Encuentre problemas antes que los usuarios.
3. Wireshark es gratis
4. Saber lo que realmente está sucediendo en su red (en casa o en el trabajo).

10.- Describa los tres paneles en la ventana principal en Wireshark

THE PACKET LIST: Esta muestra los paquetes que se han capturado mostrando el número de paquete, la hora en que se capturó, la dirección de origen, la dirección de destino, el protocolo de paquetes e información adicional.

DETALLES DEL PAQUETE: Este nos muestra los encabezados y los datos que componen el paquete seleccionado en la lista de paquetes.

BITS DEL PAQUETE: Este los nuestros los mismos datos que en el panel anterior, solo presentados en hexadecimal.

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

Lo primero que haría seria configurarlo y luego sería instalar un programa que es similar a Wireshark para poder analizar paquetes.

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

Si es posible configurar un router Cisco en wireshark se puede hacer configurando el router y el wireshark lo que no se puede es configurar al router Cisco mientras se ejecuta un sistema operativo propietario donde no se pueden instalar herramientas

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

Si se puede solamente es iniciar el wireshark a través del código del sistema, el comando sería este host "wireshark -i2 -k -f" 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?

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

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

Es el filtro **http.response**

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

Este es un filtro que se utiliza para los paquetes salientes es el siguiente "dst host"

17.- Wireshark ofrece dos tipos principales de filtros:

Los 2 tipos que ofrece Wireshark serian:

Capturar

Mostrar filtros

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

Se pueden crear un filtro para poder supervisar una red específica o elegir una existente como filtro de "host".

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

Para mostrar puede utilizar el filtro "rdp"

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

Estos filtros sirven para utilizar en los paquetes **tcp.flags.syn** para poder filtrar.

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

Los únicos son los segmentos de TCP

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

Es el Filtro Netflow

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

Es el filtro "http. request" es posible obtener todos los http

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

Es el Filtro de captura

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

Es el protocolo SMTP

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

Serían los protocolos de:

4 transportes

3 Internet

1 enlace de datos

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

Es un tipo es un tipo de registro, que es un recurso DNS que especifica cómo se debe enrutar un correo electrónico en Internet

28.- Describa el TCP Three Way HandShake

Este es un procedimiento que por el cual dos dispositivos intercambian una serie de mensajes para establecer una sesión y sincronizar sus "números de secuencia".

29.- Mencione las banderas TCP

1. **SYN:** Sincronización
2. **ACK:** Reconocimiento
3. **FIN:** Terminado,
4. **RST:** Restablecer
5. **PSH:** Empuje
6. **URG:** Urgente
7. **ECE**
8. **CWR:** Congestión de Windows Reducido
9. **NS:** Nonce Sum

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

Esto nos permite una verificación del estado de una conexión específica de un host local con al menos un equipo remoto en una red de tipo TCP / IP. Normalmente se utiliza para determinar si una dirección IP o host específico es accesible desde la red o no