Fundamentos de telecomunicaciones

Arturo alexander felipe lopez
Diciembre 2020
Profesor: ING. Ismael Jiménez

Instituto tecnológico de Cancún
Ing. En sistemas computacionales
Examen

PREGUNTAS (ingles)

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

Supported protocols, user friendliness, cost and operating system support must be taken into account

2.- How Packet Sniffers Work?

R = packet sniffers, these are defined with the address of a packet that is examined by each network adapter and connected device to determine to which node that packet is destined in other words if a node sees that a packet is not directed to him, the node ignores that packet and its data.

3.- Describe The Seven-Layer OSI Model.

7 Application Consists of standard communication services and applications that can be used by everyone.
6 Presentation Ensures that information is transferred to the receiving system in a way that the system can understand.
5 Session Manages connections and terminations between cooperating systems.
4 Transportation Manages data transfer. It also guarantees that the data received is identical to that transmitted.
3 Network Manages data addresses and transfer between networks.
2 Data link Manages data transfer on the network medium.
1 Physical Defines the characteristics of the network hardware.

4.- Describe Traffic Classifications.

-There are best effort traffics which are all types of non-detrimental traffic
-the traffic we want, which are generally limited to the delivery of spam and traffic that is created by worms, botnets and other malicious attacks

5.- Describe sniffing around hubs.

The operation of a concentrator is given by the repetition of the same data packet in all its ports, so that all the points access the same information at the same time. The hub is essential for the type of star networks.

6.- Describe sniffing in a switched environment.

a sniffer is connected to a port on a switch only the broadcast traffic and the traffic transmitted and received by the machine can be seen

7.- How ARP Cache Poisoning Works?

ARP Spoofing is a kind of attack in which an attacker sends spoofed ARP (Address Resolution Protocol) messages to a LAN. As a result, the attacker links his MAC address with the IP address of a legitimate computer (or server) on the network.
If the attacker managed to link his MAC address to a genuine IP address, he will start to receive any data that can be accessed using the IP address.

ARP Spoofing allows malicious attackers to intercept, modify, or even retain data that is in transit. ARP spoofing attacks occur on local area networks that use Address Resolution Protocol (ARP).

8.- Describe sniffing in a routed environment

The STRCMNTRC command starts a communications trace for the specified line, network interface description, or network server description. Communications trace continues until one of the following occurs:

- The system runs the End Communications Trace (ENDCMNTRC) command.
- Tracing ends due to a physical problem on the line.
- The communications trace function of the STRSST command ends the trace.
- The * STOPTRC parameter has been specified and the buffer is filled.

9.- Describe the Benefits of wireshark

It is surely the most popular free application that works on both Unix as well as Windows and capable of capturing network packets in real time.

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

Wireshark displays three panels in its main window: the list of captured packets, the detail panel of the selected packet, and third, the hexadecimal byte packets panel.

The package list is our reference point. The packages are marked with a color code that differs from each other depending on the type of package. In addition, they are numbered in order of capture. The rest of the information shown in each column corresponds to the moment of capture, the source IP address, the destination address of the packet, the protocol used (TCP, TLS, ICMP, ARP ...), the size of the packet in bytes and, finally, additional information, such as what the captured packet consists of.

The rest of the information that we are interested in knowing about each package is in the central panel, which we can open in an external window by double clicking on the list of packages. In turn, the information displayed can be displayed.

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

what I would do to configure it would be installing a program that is similar to wireshark to be able to analyze the packet.

12.- Can wireshark be setup on a Cisco router?

It is possible to configure a cisco router in wireshark and configuring the router and wireshark.

13.- Is it possible to start wireshark from command line on Windows?
It is possible to start wireshark through the system code. The command would be this "wireshark -i2 -k -f" host 192.168.1.5 "-s512"

14.- A user is unable to ping a system on the network. How can wireshark be used to solve the problem.
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 packages are being received

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

16.- Which wireshark filter can be used to monitor outgoing packets from a specific system on the network?
It can be used for outgoing packets is the following "dst host"

17.- Wireshark offers two main types of filters:
They are the capture and display filters.

18.- Which wireshark filter can be used to monitor incoming packets to a specific system on the network?
A filter is created to be able to monitor a specific network or choose an existing one as the “host” filter.

19.- Which wireshark filter can be used to Filter out RDP traffic?
The “rdp” filter is used

20.- Which wireshark filter can be used to filter TCP packets with the SYN flag set
With the tcp.flags.syn package.

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

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

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

The http.request filter is used to obtain the get and post that were made during the capture period

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

The capture filter

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

The SMTP protocol

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

1 physical, 2 data link, 4 network

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

It is a type of record that specifies how an email should be routed on the internet, An MX record (Mail eXchange record, in Spanish "mail exchange record")

28.- Describe the TCP Three Way HandShake

TCP connections are made up of three stages: connection establishment, data transfer, and connection end. To establish the connection, the procedure called 3-way handshake is used.

29.- Mention the TCP Flags

SYN. Request connection
ACK. Acknowledge the connection
END. Terminate the connection
RST. Abort a connection, for various reasons

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

This allows the verification of the status of a certain connection of a local host with at least one remote computer contemplating a network type tcp / ip and this serves to determine if a specific IP address or host is accessible from the network or not

PREGUNTAS (español)

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

Se debe tener en cuenta los protocolos soportados, los userfriendliness, el costo y el soporte del sistema operativo

2.- ¿Cómo funcionan los Packet Sniffers?

los packet sniffers, estos están definidos con la dirección de un paquete que esta es examinada por cada adaptador de red y dispositivo conectado para determinar a que nodo esta destinado ese paquete en otras palabras si un nodo ve que un paquete no está dirigido a él, el nodo ignora ese paquete y sus datos.

3.- Describe el modelo OSI de siete capas.

7	Aplicación	Se compone de los servicios y aplicaciones de comunicación estándar que puede utilizar todo el mundo.
6	Presentación	Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el sistema.
5	Sesión	Administra las conexiones y terminaciones entre los sistemas que cooperan.
4	Transporte	Administra la transferencia de datos. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos.
3	Red	Administra las direcciones de datos y la transferencia entre redes.
2	Vínculo de datos	Administra la transferencia de datos en el medio de red.
1	Física	Define las características del hardware de red.

4.- Describe las clasificaciones de tráfico.

-Están los tráficos de mejor esfuerzo que son todos los tipos de tráfico no detrimental

-los tráficos nos deseados que son los que generalmente se limitan generalmente a la entrega de spam y trafico que es creado por gusanos, botnets y otros ataques maliciosos

5.- Describe husmear alrededor de hubs.

El funcionamiento de un concentrador está dado por la repetición de un mismo paquete de datos en todos sus puertos, de manera que todos los puntos accedan a la misma información al mismo tiempo. El hub es fundamental para el tipo de redes en estrella.

6.- Describe el olfateo en un entorno conmutado.

se conecta un sniffer con un puerto en un switch solo se puede ver el trafico de broadcast y el tráfico transmitido y recibido por la maquina

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

Un ARP Spoofing es una especie de ataque en el que un atacante envía mensajes falsificados ARP (Address Resolution Protocol) a una LAN. Como resultado, el atacante vincula su dirección MAC con la dirección IP de un equipo legítimo (o servidor) en la red.

Si el atacante logró vincular su dirección MAC a una dirección IP auténtica, va a empezar a recibir cualquier dato que se puede acceder mediante la dirección IP.

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

El mandato STRCMNTRC inicia un rastreo de comunicaciones para la línea, la descripción de interfaz de red o la descripción de servidor de red especificada. El rastreo de comunicaciones continúa hasta que se produce una de las situaciones siguientes:

- El sistema ejecuta el mandato Finalizar rastreo de comunicaciones (ENDCMNTRC).
- El rastreo finaliza debido a un problema físico de la línea.
- La función de rastreo de comunicaciones del mandato STRSST finaliza el rastreo.
- Se ha especificado el parámetro *STOPTRC y se llena el almacenamiento intermedio.

9.- Describe los Beneficios de Wireshark

Es seguramente la aplicación gratuita más popular que funciona tanto en Unix, así como en Windows y capaz de capturar paquetes de red en tiempo real.

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

Wireshark muestra tres paneles en su ventana principal: la lista de paquetes capturados, el panel de detalle del paquete seleccionado y, en tercer lugar, el panel de paquetes de bytes en hexadecimal.

La lista de paquetes es nuestro punto de referencia. Los paquetes aparecen marcados con un código de colores que diferencia unos de otros según el tipo de paquete. Además, aparecen numerados en orden de captura. El resto de la información mostrada en cada columna corresponde al momento de captura, la dirección IP de origen, la dirección de destino del paquete, el protocolo empleado (TCP, TLS, ICMP, ARP…), el tamaño del paquete en bytes y, finalmente, información adicional, como por ejemplo en qué consiste el paquete capturado.

El resto de la información que nos interesa conocer de cada paquete se encuentra en el panel central, que podemos abrir en una ventana externa haciendo doble clic en la lista de paquetes. A su vez, la información mostrada se puede desplegar.

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

lo que haría para configurar seria instalando un programa que sea parecido a wireshark para poder analizar paquete.

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

Es posible configurar un router cisco en wireshark y se configurando el router y el wireshark.

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

Es posible iniciar wireshark por medio del código de sistema el comando seria este “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?

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

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

http.respose

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

Se puede usar para paquetes salientes es el el siguiente “dst host”

17.- Wireshark ofrece dos tipos principales de filtros:

Son los filtros de captura y de visualización.

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

Se crea 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?

Se utiliza el filtro “rdp”

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

Con el paquete tcp.flags.syn.

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

Solo los segmentos TCP.

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

El filtro netflow

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

Se usa el filtro http.request para obtener los get y post que fueron realizados durante el periodo de captura

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

El filtro de captura

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

El protocolo SMTP

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

1 física, 2 vinculo de datos, 4 red

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

Es un tipo de registro que especifica como debe ser encaminado un correo electrónico en internet, Un registro MX (del inglés Mail eXchange record, en español "registro de intercambio de correo")

28.- Describe el TCP Three Way HandShake

Las conexiones TCP se componen de tres etapas: establecimiento de conexión, transferencia de datos y fin de la conexión. Para establecer la conexión se usa el procedimiento llamado negociación en tres pasos (3-way handshake).

29.- Mencionar las banderas de TCP

SYN. Solicita la conexión
ACK. Reconoce (Acknowledge) la conexión
FIN. Finaliza la conexión
RST. Aborta una conexión, por motivos diversos

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

esta permite hacer la verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplando una red tipo tcp/ip y esta sirve para determinar si una dirección IP especifica o host es accesible desde la red o no