Tecnológico Nacional de México

Instituto Tecnológico de Cancún

Sergio Eleazar Barahona Chulim

Carrera:

Ingeniería en Sistemas Computacionales

Materia:

Fundamentos deTelecomunicaciones

Profesor:

ING ISMAEL JIMÉNEZ

Horario:

5 a 6 PM

PREGUNTAS (ingles)

1.- Factors to consider when selecting a packet sniffer:
Well, the factors to consider would be what protocols are compatible or what protocols can support the other would be to verify the design of the sniffer program, the installation, also check the cost or program support and finally what operating system it can support.

2.- How Packet Sniffers Work?
. R = packet sniffers or packets sniffers are those that are defined with the address of a packet and that this is examined by each network adapter and connected device and this also means the destination that it is directed to.

3.- Describe The Seven-Layer OSI Model.
They are made up of 7 layers and these are the following
• physical layer:
binary transmission.
• Data link layer:
access to the media.
• network layer:
routing and best route
• transport layer:
end-to-end connections.
• session layer:
communication between host.
• presentation layer:
representation of the data.
• application layer:
network processes to applications.

4.- Describe Traffic Classifications.
Sensitive traffic:
Sensitive traffic is traffic that the operator has an expectation of delivering on time. This includes VoIP, online gaming, video conferencing, and web browsing.
Best effort traffic:
This is the traffic that the ISP considers to be not sensitive to quality of service metrics (jitter, packet loss, latency).
Unwanted traffic:
This category is generally limited to delivering spam and traffic created by worms, botnets, and other malicious attacks.
5.- Describe sniffing around hubs.
Well when snooping around a hus it is something interesting because you can see the traffic sent through a hub, this means that it is sent to all the ports connected to said hub. From what you can tell is that in order to scan a machine on a hub, all you have to do is connect a packet sniffer.

6.- Describe sniffing in a switched environment.

It is where one can see the traffic of the switches that can add a new level of complexity. When a sniffer is connected in one of the ports of a Switch, these can only see the traffic of a broadcast and the traffic that can be transmitted in a device.

7.- How ARP Cache Poisoning Works?
Well, what I understood from 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.
What can be understood or described about the routed environment is that the importance in the placement of a sniffer means that when a problem is being solved it can host the segments of a multiple network

9.- Describe the Benefits of wireshark
Wireshark is the de facto standard in network analyzer tools.
Distinguishes yourself as a network analyst
Link to the network's only source of truth - packets.
Find problems before users do.
Wireshark is free
Know what is really happening on your network (at home or at work).

10.- Describe The three panes in the main window in Wireshark
The PDU (or Packet) List panel:
located at the top of the diagram shows a summary of each captured packet.
PDU (or Package) details panel - Located in the middle of the diagram, displays the selected package in the Package List panel in more detail.
The PDU (or Packet) Bytes panel:
Located at the bottom of the diagram, displays the actual data (in hexadecimal numbers representing actual binary) for the selected packet in the Packet List panel and highlights the selected field in the Package Details panel

11.- How would you setup wireshark to monitor packets passing through an internet router
R = It could be through configuring a system on the network the appropriate port of the switch to which the system and the internet router are connected

12.- Can wireshark be setup on a Cisco router?
R = Unable to configure Cisco router as it runs a proprietary operating system where no tools can be installed

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

R = if it is possible to start wireshark through the executable through the system code, the command would be wireshark.exe, this would be to start “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.
The best thing would be to ping icmp this means that it checks if the icmp packets are sent from the system or if it is receiving packets

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

R = this filter is used tcp.dsport == 80

16.- Which wireshark filter can be used to monitor outgoing packets from a specific system on the network?
R = this filter can be used for outgoing packets is the following "ip.src == 192.168.1.2"
17.- Wireshark offers two main types of filters:
R = the types of filters it uses are capture and display.

18.- Which wireshark filter can be used to monitor incoming packets to a specific system on the network?
R = you can create a filter 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?
R = to display you can use the filter "rdp"

20.- Which wireshark filter can be used to filter TCP packets with the SYN flag set
R = with this filters you can use tcp.flags.syn filter.

21.- Which wireshark filter can be used to filter TCP packets with the RST flag set
R = can not be done can only be using the TCP segment

22.- Which wireshark filter can be used to Clear ARP traffc
A: with this filter it is possible to clear the arp traffic only using this Netflow filter

23.- Which wireshark filter can be used to filter All HTTP traffic
R = with the filter “http.request it is possible to filter an http traffic because I could show us its get and the post

24.- Which wireshark filter can be used to filter Telnet or FTP traffic.
R = With the Capture Filter it is possible to make the network traffic from telnet or from an ftp.

25.- Which wireshark filter can be used to filter Email traffc (SMTP, POP, or IMAP).
R: = It would be the SMTP filter that is in charge of filtering the traffic of an email.

26.- List 3 protocols for each layer in TCP/IP model.
Layer 4 or Application:
equivalent to layers: 5 (session), 6 (presentation) and 7 (application), of the OSI model. It handles aspects of representation, coding and control of information.
Layer 3 or Transport:
similar to layer 4 (transport) of the OSI model. It basically provides a logical connection between the sender and the receiver, segmenting and reassembling the data, together with mechanisms that allow knowing the state of the transmission.
Layer 2 or Internet:
Assimilable to layer 3 (network) of the OSI model. It is responsible for selecting the best route to send packets through the network; it is responsible for providing the data packet (datagram).
Layer 1 or Network Interface:
equivalent to layers 2 (data link) and 1 (physical) of the OSI model. Responsible for placing data packets on the network and receiving them.

27.- What does means MX record type in DNS?
R: = is a record type, a DNS resource. MX records point to the servers to which they send an email, and to which of them it should be sent first, by priority.

28.- Describe the TCP Three Way HandShake
R = because it is the procedure that is done is that two devices can exchange one another in order to establish a section and a synchronization.

29. Mention TCP flags

R = these are some tcp flags that are used
• SYN: Synchronization,
• ACK: Acknowledgment,
• FIN: Finished,
• RST: Reset,
• PSH: Push,
• URG: Urgent,
• ECE,
• CWR: Congestion Windows Reduced,
• NS: Nonce Sum

30.- How ping command can help us to identify the operating system of a remote host?
allows a verification of the status of a specific connection of a local host with at least one remote computer in a TCP / IP type network. It is used 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:

bueno los factores a considerar serian que protocolos son compatibles o que protocolos puede soportar el otro seria verificar el diseño del programa del sniffer la instalación también checar el costo o el apoyo de programa y por ultimo que sistema operativo puede soportar.

2.- ¿Cómo funcionan los Packet Sniffers?

R= los packet sniffers o paquetes de sniffers son aquellos que está definidos con la dirección de un paquete y que esta se examina por cada adaptador de red y dispositivo conectado y esto quiere decir también al destino que va dirigido.

3.- Describe el modelo OSI de siete capas.

Se conforman por medio de 7 capas y estas son las siguientes

- capa física:
  transmision binaria.
- capa de enlace de datos:
  accesso a los medios.
- capa de red:
  direccionamiento y mejor ruta
  - capa de transporte:
    conexiones de extremo a extremo.
  - capa de session:
    comunicaion entre host.
    - capa de presentación:
      representacion de los datos.
  - capa de aplicación:
    procesos de red a aplicaciones.

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.

Tráfico de mejor esfuerzo:

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.

5.- Describe husmear alrededor de hubs.

Bueno al husmear un hus es algo interesate porque se puede ver el tráfico enviado a través de un hub esto quiere decir que se envía a todos los puertos conectados a dicho hub. Por lo que se puede saber es que para poder analizar un equipo en un concentrador, todo lo que tiene que hacer es conectar un rastreador de paquetes.

6.- Describe el olfateo en un entorno conmutado.

Es aquel en donde uno puede ver el trafico de los switches que pueden agregar un nuevo nivel de complejidad. Cuando se conecta un sniffer en unos de los puertos de un Switch, estos se pueden ver solamente el tráfico de un broadcast y el trafico que puede ser transmitido en un dispositivo.

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

Pues lo que le entendí al 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

Lo que se pueden entender o describir sobre el entorno enrutado es que la importancia en la colocación de un sniffer esto quiere decir que cuando se este solucionando un problema este pueda albercar los segmentos de un red multiple.

9.- Describe los Beneficios de Wireshark

Wireshark es el estándar de facto en las herramientas de analizador de red.

Se distingue como analista de red

Enlace con la única fuente de la verdad de la red - los paquetes.

Encontrar problemas antes de que lo hagan los usuarios.

Wireshark es gratis

Saber lo que realmente está sucediendo en su red (en casa o en el trabajo).

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

El panel de Lista de PDU (o Paquete): ubicado en la parte superior del diagrama muestra un resumen de cada paquete capturado.

El panel de detalles de PDU (o Paquete): ubicado en el medio del diagrama, muestra más detalladamente el paquete seleccionado en el panel de Lista del paquete.

El panel de bytes de PDU (o paquete): ubicado en la parte inferior del diagrama, muestra los datos reales (en números hexadecimales que representan el binario real) del paquete seleccionado en el panel de Lista del paquete y resalta el campo seleccionado en el panel de Detalles del paquete

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

R=Se podría atraves de configurar un sistema en la red el puerto apropiado del conmutador al que están conectadas al sistema y el enrutador de internet.

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

R=no es posible configurar enrutador cisco ya que ejecuta un sistema operativo propietario en el que no se pueden instalar herramientas.

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

R= si es posible iniciar wireshark por el ejecutable por medio del código de sistema el comando seria wireshark.exe este seria para iniciar "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?

Lo mejor seria hacer un ping en icmp esto quiere decir que comprueba si los paquetes icmp se envían desde el sistema o si esta recibiendo paquetes

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

R= se utiliza este filtro tcp.dsport==80

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

R= este filtro se puede usar para paquetes salientes es el el siguiente "ip.src ==192.168.1.2"

17.- Wireshark ofrece dos tipos principales de filtros:

R= los tipos de filtros que usa son los de captura y de visualización.

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

R= se puede crear 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?

R= para visualizar se puede utilizar el filtro “rdp”

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

R=con este filtros puede utilizar para filtrar los paquete tcp.flags.syn.

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

R= no se puede realizar solo se puede utilizando el segmento de TCP

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

R: con este filtro es posible despejar el trafico arp solo usando este filtro Netflow

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

R=con el filtro “http.request es posible filtrar un trafico http porque nos pude mostrar su get y el post.

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

R=con el Filtro de captura es posible hacer el trafico de red de telnet o de un ftp.

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

R:=seria el filtro SMTP es el que se encarga de filtrar el trafico de un correo electrónico.

26.- Enumere 3 protocolos para cada capa en el modelo TCP / IP Capa 4 o de Aplicación:

equivalente a las capas: 5 (sesión), 6 (presentación) y 7 (aplicación), del modelo OSI. Maneja aspectos de representación, codificación y control de la información.

Capa 3 o de Transporte:

similar a la capa 4 (transporte) del modelo OSI. Proporciona fundamentalmente una conexión lógica entre el emisor y el receptor, segmentando y reensamblando

los datos, junto con mecanismos que permiten conocer el estado de la transmisión.

Capa 2 o de Internet:

asimilable a la capa 3 (red) del modelo OSI. Se encarga de seleccionar la mejor ruta para enviar paquetes a través de la red; es responsable de proporcionar el paquete de datos (datagrama).

Capa 1 o de Interfaz de Red:

equivalente a las capas 2 (enlace de datos) y 1 (física) del modelo OSI. Responsable de la colocación de los paquetes de datos en la red y de la recepción de los mismos.

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

R:=es un tipo de registro, un recurso DNS . 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.- Describe el TCP Three Way HandShake

R=pues es aquel procedimiento que se hace es que dos dispositivos puedan intercambiarse unos en si a fin de poder establecer un sección y una sincronización.

29.- Mencionar las banderas de TCP

R= estas son algunas banderas tcp que se utilizan

- SYN: Synchronisation,
- ACK: Acknowledgment,
- FIN: Finished,
- RST: Reset,
- PSH: Push,
- URG: Urgent,
- ECE,
- CWR: Congestion Windows Reduced,
- NS: Nonce Sum

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

Nos permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP. Sirve para determinar si una dirección IP específica o host es accesible desde la red o no