INSTITUTO TECNOLÓGICO DE CANCÚN

ALUMNO: GONGORA JIMENEZ FRANCISCO DAVID.

CARRERA: ING. EN SISTEMAS COMPUTACIONALES.

PROFESOR: ISMAEL JIMÉNEZ SÁNCHEZ.

MATERIA: FUNDAMENTOS DE TELECOMUNICACIONES.

U3 EXAMEN:

RESPONDER EL EXAMEN

HORARIO: 5PM-6PM.

FECHA DE ENTREGA:

17 DE DCIEMBRE DEL 2020

PREGUNTAS DEL EXAMEN (ingles)- EXAM QUESTIONS ENGLISH

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

so I understood first you have to check that it is compatible with the protocols that one will use, hence you should consider the design,
its ease of installation, the cost, the overall flow of operations are either these standards among others.

2.- How Packet Sniffers Work?

It refers to network capture, its function to build data packets in order to obser ve their headers and contents in a structured way,
displaying the field values in an orderly and consistent manner.

3.- Describe The Seven-Layer OSI Model.

Layer 1 Physics: Defines the characteristics of the network hardware.

Layer 2 Data Link: Manages data transfer on the network media.

Layer 3 Network: Manages data addresses and inter-network transfer.

Layer 4 Transport: Manages data transfer,
in which, it ensures that the data received is identical to those transmitted.

Layer 5 session: Manage connections and terminations

Layer 6 presentation:
Ensures that information is transferred to the receiving system in a way that is understandable to the system.

Layer 7 application: It consists of standard communication services and applic ations and is used by the world.

4.- Describe Traffic Classifications.

1. the basic Internet traffic which is described as TCP traffic with destination (output), port 80 or 443 (for HTTPS), and with a size of 512 KB (meaning that it is not a large file transfer).

2. Unwanted traffic: This category is generally limited to the delivery of spam and traffic created by worms, botnets and other malicious attacks.

3. Web traffic is likely to be a large file transfer (more than 512 KB). This traffic is assigned to the «low» class, the idea this traffic is not as sensitive to delay, as Web browsing.

5.- Describe sniffing around hubs.

In it you can see all the network traffic, also the packets are transmitted to all the hosts connected in the same network segment, and the packets are transmitted at the speed of the slowest device in the segment.

6.- Describe sniffing in a switched environment.

It is where one can see only broadcast traffic and traffic transmitted and receiv ed by the machine.

7.- How ARP Cache Poisoning Works?

It works in that the attacker generates a series of ARP (Address Resolution Protocol) packets with false information that alters the ARP tables of the victim hosts.

8.- Describe sniffing in a routed environment

What I can understand a little is that it takes importance to the moment of the sniffer placement when one is solving problems and that problem covers multiple network segments.

9.- Describe the Benefits of wireshark

-Allows you to open and save captured packages. -Capture packets in real time from a network interface. -Examine network security issues. -It allows to detect transmission errors of problems of our network. -It supports different protocols. -It shows information of the captured packets. -Import and export packages of different formats.

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

Data area. this section can display two data sets depending on the actions that have been performed, What these panels display are as follows: The package list: Shows the packets that have been captured showing the package number,

the time it was captured, the source address, the destination address, the package protocol and additional information.

Package Details: Displays the headers and data that make up the selected package in the package list.

Package bits: The same data as in the previous panel, only presented in hexadecimal.

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

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

If you can configure

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

What I researched and understood is that you can't

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

Configuring it to do a network scan and see the problem you are sending to find the solution.

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

From what I researched I understood that http.response is used

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

So investigate you use the host dst

17.- Wireshark offers two main types of filters:

Capture filters (Capture Filter): are those that are set to show only packages of meet the requirements indicated in the filter.

Display filters (Display Filer): set a filter criterion on the captured packets that we are viewing on the main screen of Wireshark.

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

What I understand is that you can use the host filter or you can create a filter to do this.

19.- Which wireshark filter can be used to Filter out RDP traffic?

The rpd filter is used

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

The filter tcp.flags.syn is used

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

only TCP segments are used

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

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

The Capture Filter is used

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

So research uses the SMTP protocol- simple mail transfer protocol

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

5.6.7 Application, session, presentation Application NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP and others.

4 Transport TCP, UDP, SCTP

3 Internet Network IPv4, IPv6, ARP, ICMP

2 Data Link PPP, IEEE 802.2

1 Physical Network Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI and others.

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

address a domain's mail to the servers that host the domain's user accounts.

28.- Describe the TCP Three Way HandShake

is where two devices exchange messages to be able to set up a session

29.- Mention the TCP Flags

SYN: Synchronisation: a SYN was sent, the SYN bit was marked in that communication and it was the establishment of the connection.

ACK: Acknowledgment: is marked to "thank" the reception, in the 3-way challenge process is what is sent to confirm that we have received the initial SYN.

END: Finished: The END flag indicates that there is no more data from the source, it will be used in the last segment sent by the source.

RST: Reset: This flag is sent from the destination to the source and is sent when the destination receives a segment that is not expected and should not have arrived.

PSH: Push: tells the receiver to process segments as they are received and not to be stored in a buffer.

URG: Urgent: Prioritize those segments marked as urgent over those not marked.

ECE Explicit Congestion Notification [ECN]-Echo: indicates that the TCP peer allows the ECN (Explicit Congestion Notification).

CWR: Congestion Windows Reduced: The sender host sets the CWR flag to indicate that it received a TCP segment with the ECE flag.

NS: Nonce Sum: The NS flag is an experimental flag used against malicious sending by the source.

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

It helps us determine whether the IP address or host is accessible from the network or not.

PREGUNTAS DEL EXAMEN (español)

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

R= por lo que entendí primero hay que checar que sea compatible con los protocolos que uno va a utilizar, de ahí se debe considerar el diseño, su facilidad de instalación, el costo, el flujo general de las operaciones ya sean estas estándar entre otros.

2.- ¿Cómo funcionan los Packet Sniffers?

R= Se refiere a la captura de red, su función la de construir los paquetes de datos para poder observar sus cabeceras y contenidos de forma estructurada, mostrando los valores de campo de forma ordenada y consistente.

3.- Describe el modelo OSI de siete capas.

R= modelo de referencia de Interconexión de Sistemas Abiertos (OSI) son utilizadas para las actividades de red:

capa 1 Física: Define las características del hardware de red.

Capa 2 Vínculo de datos: Administra la transferencia de datos en el medio de red.

Capa 3 Red: Administra las direcciones de datos y la transferencia entre redes

Capa 4 Transporte: Administra la transferencia de datos, en el cual, garantiza que los datos recibidos sean idénticos a los transmitidos.

Capa 5 sesión: Administra las conexiones y terminaciones entre los sistemas que cooperan

Capa 6 presentación: Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el sistema.

Capa 7 aplicación: Se compone de los servicios y aplicaciones de comunicación estándar y es utilizado por el mundo.

4.- Describe las clasificaciones de tráfico.

R= Se clasifican en los siguientes:

1. el tráfico de Internet básico que se describe como el tráfico TCP con el destino (de salida), puerto de 80 o 443 (para HTTPS), y con un tamaño de 512 KB (lo que significa que no es una transferencia de archivos de gran tamaño).
2. Tráfico no deseado: Esta categoría se limita generalmente a la entrega de spam y tráfico creado por gusanos, botnets y otros ataques maliciosos.
3. tráfico web es probable que sea una transferencia de archivos grandes (más de 512 KB). Este tráfico se asigna a la «baja» de clase, la idea este tráfico no es tan sensible al retardo, como la navegación Web.

5.- Describe husmear alrededor de hubs.

R= En él se pude ver todo el tráfico de la red, también los paquetes son transmitidos a todos los hosts conectados en el mismo segmento de red, y se transmiten los paquetes a la velocidad del dispositivo más lento del segmento.

6.- Describir el sniffing en un entorno conmutado.

R= Es en donde uno puede ver solamente el tráfico de broadcast y el tráfico transmitido y recibido por la máquina.

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

R= Funciona en que el atacante genera una serie de paquetes ARP (Protocolo de resolución de direcciones-Address Resolution Protocol) con información falsa que altera las tablas ARP de los hosts víctimas.

8.- Describe el rastreo en un entorno enrutado

R= Por lo que logre entender un poco es que lleva importancia al momento de la colocación del sniffer cuando uno está solucionando problemas y ese problema abarque los segmentos de red múltiples.

9.- Describe los Beneficios de Wireshark

Permite abrir y guardar paquetes capturados.

Captura paquetes en tiempo real desde una interfaz de red.

Examina problemas de seguridad de red.

Permite detectar errores de transmisión de problemas de nuestra red.

Soporta protocolos distintos.

Muestra información de los paquetes capturados.

Importa y exporta paquetes de diferentes formatos.

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

R= Área de datos.

esta sección puede desplegar dos conjuntos de datos dependiendo de las acciones que se hallan realizado, Lo que estos paneles despliegan son los siguientes:

La lista de paquetes: Muestra los paquetes que han sido capturados mostrando el número de paquete, el momento en que fue capturado, la dirección fuente, la dirección destino, el protocolo del paquete e información adicional.

Detalles del paquete: Muestra las cabeceras y datos que componen el paquete seleccionado en la lista de paquetes.

Bits del paquete: Los mismos datos que en el panel anterior, solo que presentados en hexadecimal.

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

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

R= Si se puede configurar

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

R= Por lo que investigué y entendí es que no se puede

14.- Un usuario no puede hacer ping a un sistema en la red. ¿Cómo se puede utilizar Wireshark para resolver el problema? Configurándolo para hacer un escaneo de red y ver el problema que le esta mandando para buscar la solución.

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

R= **Por lo que investigue entendí que se utiliza el http.response**

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

R= **Por lo que investigue se utiliza el dst host**

17.- Wireshark ofrece dos tipos principales de filtros:

R=

Los filtros de captura (Capture Filter): son los que se establecen para mostrar solo los paquetes de cumplan los requisitos indicados en el filtro.

Los filtros de visualización (Display Filer): establecen un criterio de filtro sobre los paquetes capturados y que estamos visualizando en la pantalla principal de Wireshark.

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

R= Por lo que llegue a entender es que se puede usar el filtro host o se puede crear un filtro para realizar esto.

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

R= Se utiliza el filtro rpd

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

R= Se utiliza el filtro tcp.flags.syn

21.- ¿Qué filtro Wireshark se puede utilizar para filtrar paquetes TCP con la bandera RST configurada? R: solo se utilizan los segmentos TCP

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

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

R: Se utiliza el filtro http.request

24.- ¿Qué filtro Wireshark se puede utilizar para filtrar el tráfico Telnet o FTP?
R: Se utiliza el Filtro de captura

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

R: Por lo que investigue se utiliza el protocolo SMTP- protocolo simple de transferencia de correo

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

Ref. OSI Nº de capa	Equivalente de capa OSI	Capa TCP/IP	Ejemplos de protocolos TCP/IP
5,6,7	Aplicación, sesión, presentación	Aplicación	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros.
4	Transporte	Transporte	TCP, UDP, SCTP
3	Red	Internet	IPv4, IPv6, ARP, ICMP
2	Vínculo de datos	Vínculo de datos	PPP, IEEE 802.2
1	Física	Red física	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros.

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

R: dirigen el correo de un dominio a los servidores que alojan las cuentas de usuario del dominio.

28.- Describe el TCP Three Way HandShake

R: es donde dos dispositivos intercambian mensajes para poder establecer una sesión

29.- Mencionar las banderas de TCP

SYN: Synchronisation: se enviaba un SYN, se marcaba el bit de SYN en esa comunicación y era el establecimiento de la conexión.

ACK: Acknowledgment: se marca para “agradecer” la recepción, en el proceso de desafío en 3 vías es lo que se envía para confirmar que hemos recibido el SYN inicial.

FIN: Finished: El flag FIN indica que ya no hay más datos desde el origen, se utilizará en el último segmento enviado por el origen.

RST: Reset: Este flag se envía desde el destino al origen y se envía en el momento en el que el destino recibe un segmento que no se espera y que no debería de haber llegado.

PSH: Push: indica al receptor que tiene que procesar los segmentos a medida que son recibidos y que no se deben de almacenar en un buffer.

URG: Urgent: prioriza aquellos segmentos marcados como urgente sobre los no marcados.

ECE Explicit Congestion Notification [ECN]-Echo:

indica que el peer de TCP permite el ECN (Explicit Congestion Notification).

CWR: Congestion Windows Reduced: El host emisor establece el flag CWR para indicar que recibió un segmento TCP con el flag ECE.

NS: Nonce Sum: El flag NS es un flag experimental que se utiliza contra envíos maliciosos por parte del origen.

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

R= Nos ayuda a determinar si la dirección IP o host es accesible desde la red o no es accesible a la red.