INSTITUTO TECNOLOGICO DE CANCUN

LEON QUEB MIGUEL ANGEL

ISMAEL JIMENEZ SANCHEZ

FUND. TELECOMUNICACIONES

HORARIO

17:00 – 18:00

PREGUNTAS EXAMEN

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

• Protocolos soportados

Todos los rastreadores de paquetes pueden interpretar varios protocolos. La mayoría de los sniffers pueden interpretar todos los protocolos más comunes tales como DHCP, IP, y ARP, pero no todos pueden interpretar algunos de los protocolos más no tradicional. Al elegir un sniffer, asegúrese de que es compatible con los protocolos que va a utilizar.

• Userfriendliness

Considere el diseño del programa del sniffer del paquete, la facilidad de instalación, y el flujo general de las operaciones estándar. El programa que elija debe ajustarse a su nivel de experiencia

• Costo

• Apoyo al programa

• Soporte del sistema operativo

2.- How Packet Sniffers Work?

Los rastreadores de paquetes funcionan interceptando y registrando el tráfico de red que pueden ver a través de la interfaz de red cableada o inalámbrica. Una vez que se capturan los datos del paquete sin procesar, el software de sniffing del paquete los analiza y los presenta en forma legible para que la persona que utiliza el software pueda dar sentido a él.

3.- Describe The Seven-Layer OSI Model.

7. Capa de aplicación

6. Capa de presentación

5. Capa de sesión

4. Capa de transporte

3. Capa de red

2. Capa de enlace de datos

1. Capa física

4.- Describe Traffic Classifications.

1. 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.

2. Tráfico de mejor esfuerzo: El mejor tráfico de esfuerzo es todos los otros tipos de tráfico no detrimental. Este es el tráfico que el ISP considera que no es sensible a las métricas de calidad de servicio (jitter, pérdida de paquetes, latencia).

3.Tráfico no deseado: Esta categoría se limita generalmente a la entrega de spam y tráfico creado por gusanos, botnetsy otros ataques maliciosos. En algunas redes, esta definición puede incluir tráfico como VoIP no local (por ejemplo, Skype)o servicios de streaming de vídeo para proteger el mercado de los servicios 'in-house' del mismo tipo.

5.- Describe sniffing around hubs.

Oler en una red que tiene hubs instalados es un sueño para cualquier analista de paquetes. Como aprendió anteriormente, el tráfico enviado a través de un hub se envía a todos los puertos conectados a ese hub. Por lo tanto, para analizar un equipo en un concentrador, todo lo que tiene que hacer es conectar un rastreador de paquetes a un puerto vacío en el hub, y puede ver toda la comunicación hacia y desde todos los equipos conectados a ese hub.

6.- Describe sniffing in a switched environment.

Los switches agregan un nuevo nivel de complejidad. Cuando usted conecta un sniffer con un puerto en un Switch, usted puede ver solamente el tráfico de broadcast y el tráfico transmitido y recibido por su máquina.

7.- How ARP Cache Poisoning Works?

El envenenamiento por ARP se usa generalmente para ataques de intermediario. El atacante genera una serie de paquetes ARP con información falsa que altera las tablas ARP de los hosts víctimas.

Ettercap y Cain and Abel son dos herramientas que pueden usarse para realizar envenenamiento por ARP.

8.- Describe sniffing in a routed environment

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.- Describe the Benefits of 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 The three panes in the main window in Wireshark

1.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.

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

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

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

Se puede configurar y establecer un sistema en la red con Wireshark. El puerto apropiado del conmutador al que están conectados al sistema y el enrutador de Internet se puede configurar para la duplicación de puertos. Todos los paquetes que pasan a través de la interfaz del conmutador al enrutador pueden reflejarse en el sistema en el que está configurado Wireshark.

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

Wireshark es un ejecutable. Se puede configurar en sistemas operativos como Windows y Linux. No se puede configurar en un enrutador Cisco, ya que ejecuta un sistema operativo propio en el que no se pueden instalar herramientas o software adicionales.

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

Sí, es posible comenzar a usar el ejecutable apropiado en Windows que es wirehark.exe

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

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

Los servidores web HTTP usan el puerto TCP 80. Las solicitudes entrantes al servidor web tendrían el número de puerto de destino como 80. Entonces, el filtro tcp.dstport == 80.

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

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:

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

De la misma manera que buscamos los paquetes salientes de un sistema específico en la red. En lugar de escribir la dirección IP relacionada con los paquetes salientes, colocamos la dirección IP relacionada con los paquetes entrantes para obtenerla. (ip.src == * IP *).

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

Wireshark proporciona un filtro visual donde podemos escribir directamente el componente que necesitamos, en este caso solo necesitamos escribir rdp en el filtro.

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

Podemos usar el mismo filtro visual que nos proporciona Wireshark y configurar el filtro escribiendo tcp.flags.syn para obtener todos los paquetes TCP con las banderas SYN.

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

(tcp.flags.syn == 1) || (tcp.flags.push == 1) || (tcp.flags.reset == 1)

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

not arp

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

http / mostrar todo el tráfico http: tcp.dstport 80

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

telnet

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

Mostrar solo el tráfico basado en SMTP: smtp Muestre solamente el tráfico basado SMTP con el comando "MAIL FROM": smtp.req.parameter contains "FROM"

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

Capa de Aplicación:

Ofrece a las aplicaciones la capacidad de acceder a los servicios de las otras capas y define los protocolos que utilizan las aplicaciones para intercambiar datos.

1.- HTTP (Hypertext Transfer Protocol): se utiliza para transferir archivos que componen las páginas Web de la World Wide Web.

2.- FTP (File Transfer Protocol): se utiliza para la transferencia interactiva de archivos.

3.- DNS (Domain Name System): se utiliza para resolver un nombre de host a una dirección IP.

Capa de Transporte:

La capa de transporte se encarga de establecer una conexión lógica entre el dispositivo transmisor y el receptor.

1.- TCP (Transmission Control Protocol): proporciona un servicio de comunicaciones fiable orientado a la conexión punto a punto.

2.- UDP (User Datagram Protocol): proporciona una conexión, punto a punto, o uno a muchos poco fiable, aunque rápido y con poca carga adicional en la red.

3.- SCTP admite conexiones entre sistema que tienen más de una dirección, o de host múltiple.

Capa de Internet:

La capa de Internet es responsable de las funciones de direccionamiento, empaquetado y enrutamiento.

1.-IP (Internet Protocol): es el protocolo responsable del direccionamiento IP, enrutamiento, fragmentación, y reensamblado de los paquetes de datos entre los dispositivos conectados a una red.

2.- ARP (Address Resolution Protocol): es responsable de la resolución de la dirección de la capa de Internet a la dirección de la capa de interfaz de red.

3.- ICMP (Internet Control Message Protocol): es responsable de proporcionar funciones de diagnóstico y notificación de errores debidos a la entrega sin éxito de paquetes IP.

Capa de Interfaz a Red:

La capa de interfaz de red, también conocida como de acceso de red, es responsable de la colocación y recepción de paquetes en la red

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

Un registro MX es un tipo de registro, un recurso DNS que especifica cómo debe ser encaminado un correo electrónico en internet. 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 the TCP Three Way HandShake

El proceso de "Three-way Handshake" es el procedimiento por el cual dos dispositivos intercambian una serie de mensajes a fin de poder establecer una sesión y sincronizar sus "Sequence Numbers".

29.- Mention the TCP Flags

Synchronization (SYN): Se utiliza en el primer paso de la fase de establecimiento de conexión o el proceso de Three-way Handshake entre los dos hosts.

Acknowledgement (ACK): Se utiliza para reconocer los paquetes que son recibidos con éxito por el host. El indicador se establece si el campo de número de confirmación contiene un número de acuse de recibo válido.

Reset (RST): Se utiliza para terminar la conexión si el remitente RST siente que algo está mal con la conexión TCP o que la conversación no debe existir.

Push (PSH): La capa de transporte de forma predeterminada espera algún tiempo para que la capa de aplicación envíe suficientes datos iguales al tamaño máximo del segmento para que el número de paquetes transmitidos en la red minimice lo que no es deseable por alguna aplicación como aplicaciones interactivas (chat).

Urgent (URG): Los datos dentro de un segmento con el indicador URG 1 se reenvían inmediatamente a la capa de aplicación, incluso si hay más datos que se entregarán a la capa de aplicación. Se utiliza para notificar al receptor para procesar los paquetes urgentes antes de procesar todos los demás paquetes.

Finish (FIN): Se utiliza para solicitar la terminación de la conexión, es decir, cuando no hay más datos del remitente, solicita la terminación de la conexión. Este es el último paquete enviado por el remitente. Libera los recursos reservados y termina correctamente la conexión.

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

El objetivo de un ping es determinar si un host destino, identificado con una determinada IP, es accesible desde otro host.

Para ello, el host origen envía al host destino un paquete de información de 32 bytes mediante el protocolo ICMP y espera una contestación de éste, que debe contener los mismos datos. Si la respuesta llega correctamente, el ping ha sido satisfactorio. Si por el contrario el ping falla, entonces es que o bien la petición del host origen o bien la respuesta del host destino se han perdido por el camino.