INSTITUTO TECNOLÓGICO DE CANCUN

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES

ALUMNO: LÓPEZ HERNÁNDEZ JAVIER ISAC

PROFESOR: ISMAEL JIMENEZ SÁNCHEZ

CURSO: FUNDAMENTOS DE TELECOMUNICACIONES

PREGUNTAS

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

• 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.- ¿Cómo funcionan los detectores de paquetes?

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 el modelo OSI de siete capas.

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 las clasificaciones de tráfico.

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 cómo hacer sniffing en los 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 el sniffing en un entorno conmutado.

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.- ¿Cómo funciona el envenenamiento de caché ARP?
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.- Describir el rastreo 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.- Describir 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
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.- ¿Cómo configurar wireshark para monitorear los paquetes que pasan a través de un Router?
Primero se elije la interfaz, luego se le hace la captura, Una vez que haya capturado los paquetes, debe empezar a analizarlos. El análisis de paquetes en Wireshark se lleva a cabo a través de los 3 paneles principales, en este punto que está listo para aplicar filtros de captura y visualización. Estos son los dos tipos de filtros que se pueden utilizar en Wireshark.

12.- ¿Se puede configurar wirehark en un router Cisco?
Si se puede, solo que es un procedimiento laborioso.

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

Si se puede abrir wireshark desde la linea de comandos, primero se accede a la carpeta del programa y si necesitamos ayuda ejecutamos *wireshark -h* y para ejecutar el programa con la interfaz ejecutamos *wireshark -i 1*

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 se puede marcar si se reciben los paquetes.

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

Los servidores web HTTP utilizan el puerto TCP 80. Las solicitudes entrantes al servidor web tendrían el número de puerto de destino como 80. Por lo tanto, el filtro tcp.dstport-80.

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

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. ¿Cuales son los dos filtros principales de wireshark?

Los de captura y visualización

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

Colocamos la dirección IP relacionado con los paquetes entrantes para obtenerlo.
(ip.src == * P *).

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

Solo se necesita escribir rdp en el filtro.

20. - ¿Qué filtro de wirehark se puede usar para filtrar paquetes TCP con el indicador SYN configurado?

tcp.flags.syn==1 es el filtro correcto para obtener todos los paquetes con SYN

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

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

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

El filtro es sencillo, es: no arp

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

Http. Para mostrar todo el trafico: tcp.dstport == 80

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

-Para mostrar filtro basado en Telnet use: Telnet
-Para mostrar filtro basado en FTP use: ftp

25. Qué filtro de Wireshark se puede utilizar para filtrar el tráfico de correo electrónico (SMTP, POP o 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"

-Mostrar solo el tráfico basado en POP: pop

-Mostrar sólo el tráfico basado en IMAP: imap

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

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
- IEEE 802.3 (et)
- PPP (Point-to-Point Protocol - Protocolo de punto a punto)
- Red en anillo (tr)

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

Son registros DNS necesarios para entregar correo electrónico a su dirección. Se utiliza un registro MX para indicar al mundo a qué servidores de correo aceptan correo entrante para tu dominio y a dónde deben enrutarse los correos electrónicos enviados a tu dominio. Si sus registros MX no apuntan a la ubicación correcta, no recibirá correo electrónico.

28. Describir el apretón de manos de tres vías TCP

Es un proceso que se utiliza en una red TCP/IP para establecer una conexión entre el servidor y el cliente. Es un proceso de tres pasos que requiere que el cliente y el servidor intercambien paquetes de sincronización y confirmación antes de que se inicie el proceso de comunicación de datos real.

29. Mencione las banderas TCP

SYN: Inicia la conexión entre hosts.

ACK: Reconoce la recepción de un paquete.

FIN: No abrá mas transmisiones.

RST: Resetea y aborta la conexión, por diversos motivos.

PSH: Envía todos los datos almacenados en el buffer, inmediatamente.

URG: Todos los datos contenidos en un paquete, serán procesados urgentemente.

30. Cómo el comando ping puede ayudarnos a identificar el sistema operativo de un control remoto

el comando Ping para conseguir el nombre del sistema operativo. Básicamente Ping es una utilidad de software de administración de red de computadora que se utiliza para encontrar la disponibilidad de cualquier host en la red de protocolo de Internet (IP).