TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

“EXAMEN”

UNIDAD 3

1) Factores a considerar a la hora de seleccionar un rastreador de paquete;

R= **Userfriendliness**

el diseño del programa del sniffer del paquete la facilidad de instalación y lo que elijamos debe acomodarse a :

-Costo

-Apoyo al programa

-Soporte del sistema operativo

Protocolos soportados

Todos los rastreadores de paquetes pueden interpretar varios protocolos se 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.

2) ¿Cómo funcionan los Packet Sniffers?

R= Estos están definidos con la dirección de un paquete que esta es examinada por cada adaptador de red y dispositivo conectado para determinar a qué nodo es el destino también si el nodo detecta que el paquete no es para el de plano lo ignora y deja pasar el paquete

3) Describe el modelo OSI de siete capas.

R= 1- capa física

2- capa de enlace de datos

3- capa de red

4- capa de transporte

5- capa de sesión

6- capa de presentación

7- capa de aplicación

4) Describe las clasificaciones de tráfico

R=

1. Tráfico sensible: El tráfico sensible es el tráfico que el operador tiene una expectativa de entregar a tiempo.

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

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

5) Describe husmear alrededor de hubs.

R= una red que tiene hubs instalados, 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 prácticamente seria como administrador donde no permitiría ver a tiempo real lo que se envía o recibe o etc.

6) Describe el olfateo en un entorno conmutado.

R= 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 es decir que para hacer un entorno conmutado necesitamos un sniffer para mas bien monitorear.

7) ¿Cómo funciona el envenenamiento de caché ARP?

R= 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. Es decir que tenemos que tener cuidado y estar al pendiente de este tipo de ataque ARP

8) Describe el rastreo en un entorno enrutado

R= la importancia de la colocación del sniffer cuando usted está solucionando problemas

9) Describe los Beneficios de Wireshark

R= Pues más bien Wireshark es una herramienta que le podemos sacar mucho potencial en el mundo de capturamiento y seguimientos de datos de red de los paquetes. Se pueden Encontrar problemas y podemos ver que enviamos y recibimos en cuestión de paquete es decir que podemos ver a tiempo real que hace nuestra computadora, antes de que lo hagan los usuarios. Estándar.

10) Describe los tres paneles de la ventana principal de Wireshark

R=La ventana principal de Wireshark se divide en tres secciones: el panel Packet List en la parte superior, el panel Packet Details (Detalles del paquete) en la parte central y el panel Packet Bytes (Bytes del paquete) en la parte inferior

La lista de paquetes: Muestra los paquetes que han sido capturados mostrando el numero 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?

R= seria cerrando los programas que pudiera genera interferencia y seria ejecutando Wireshark y configuramos el Wireshark que paquetes queremos capturar

12) ¿Se puede configurar Wireshark en un router Cisco?

R Si se puede configurar Wireshark se adapta a la mayoría de módems y o dispositivos que transmite datos

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

R si primero tenemos que abrir el comando de sistema como administrador y escribimos el siguiente comando "Wireshark i2-k-f " "host 192.168.0.5(o la ip de nuestro equipo)"-s512"

14) Un usuario no puede hacer ping a un sistema en la red. ¿Cómo se puede utilizar Wireshark para resolver el problema?

R Para empezar, debemos de saber que ping usa ICMP. En estos casos el 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?

R http.repose

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

R "dst host"

17) Wireshark ofrece dos tipos principales de filtros

R de captura y la visualización

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

R Host

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

R "rdb"

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

R tcp.flags.syn

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

R no solo los segmento TCP

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

R filtro Netflow

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

R "http.request" es posible obtener todos los datos de GET y POST

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

R Filtro de captura

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

R el protocolo SMTP

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

R Aplicación
Transporte
Internet

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

Res un tipo de registro, un recurso DNS que especifica cómo debe ser encaminado un correo electrónico en internet

28) Describe el TCP Three Way HandShake

R dos dispositivos intercambian una serie de mensajes a fin de poder establecer una sesión y sincronizar sus "Sequence Numbers".

29) Mencionar las banderas de TCP

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?

Pues podemos poner la ip del destino y nos dará como esta la conexión de tal nos puede ayudar a verificar si esta funcionando bien en nuestra red o hay algún tipo de conflicto y TCP/IP. Sirve para determinar si una dirección IP específica o host es accesible desde la red o no