INSTITUTO TECNOLOGICO DE CANCUN

ASIGNATURA: FUNDAMENTOS DE TELECOMM

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES

PROFESOR: ISMAEL JIMENEZ SANCHEZ

ALUMNO: FERNANDO FLORES PRADO

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

Tamaño de la red
Conexiones importantes
El tipo de paquetes que vamos a necesitar visualizar
Si requerimos de un analizador de tráfico

2.- How Packet Sniffers Work?

Cuando un remitente transmite paquetes de datos, los paquetes pasan a través de varios nodos en una red. Cada adaptador de red y el dispositivo conectado examinan la información de control de un paquete para ver hacia qué nodo se dirige el paquete. En circunstancias normales, si un nodo encuentra que el paquete está dirigido a otro nodo, descarta o ignora el paquete. Sin embargo, en el rastreo de paquetes, ciertos nodos están programados para no seguir esta práctica estándar y recolectar todos o una muestra definida de paquetes, independientemente de su dirección de destino. Los rastreadores de paquetes utilizan estos paquetes para el análisis de una red.

3.- Describe The Seven-Layer OSI Model.

las comunicaciones entre un sistema informático se dividen en siete capas de abstracción diferentes: física, enlace de datos, red, transporte, sesión, presentación y aplicación.

4.- Describe Traffic Classifications.

Los paquetes se clasifican para que el programador de la red los procese de manera diferente. Al clasificar un flujo de tráfico utilizando un protocolo en particular, se le puede aplicar una política predeterminada y otros flujos para garantizar una cierta calidad (como con VoIP o servicio de transmisión de medios) o para proporcionar la mejor entrega. Esto se puede aplicar en el punto de entrada (el punto en el que el tráfico ingresa a la red) con una granularidad que permite que los mecanismos de gestión del tráfico separen el tráfico en flujos individuales y pongan en cola, controlen y moldeen de manera diferente.

5.- Describe sniffing around hubs.

El sniffing en una red con hubs proporciona una ventana de visibilidad ilimitada. La ventaja de un entorno conmutado es que a los dispositivos solo se les envían paquetes que están destinados a ellos, lo que significa que los dispositivos promiscuos no pueden detectar ningún paquete adicional.

6.- Describe sniffing in a switched environment.

Cuando el sniffer está conectado a un puerto en un switch, permitirá ver sólo el tráfico de transmisión y el tráfico transmitido y recibido por esa máquina

7.- How ARP Cache Poisoning Works?

Es cuando un atacante envía mensajes ARP falsificados a través de una red de área local (LAN) para vincular la dirección MAC del atacante con la dirección IP de una computadora o servidor legítimo en la red. Una vez que la dirección MAC del atacante está vinculada a una dirección IP auténtica, el atacante puede recibir cualquier mensaje dirigido a la dirección MAC legítima. Como resultado, el atacante puede interceptar, modificar o bloquear comunicaciones a la dirección MAC legítima.

8.- Describe sniffing in a routed environment

> Depende de la marca del router para poder establecer el sniffer ya que no todos permiten la captura de paquetes.

9.- Describe the Benefits of wireshark

- Soporta más de 480 protocolos distintos, además de la posibilidad de trabajar tanto con datos capturados desde una red durante una sesión con paquetes previamente capturados que hayan sido almacenados en el disco duro.

- Wireshark soporta el formato estándar de archivos tcpdump, es capaz de reconstruir sesiones TCP, y está apoyado en una completa interfaz gráfica que facilita enormemente su uso.

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

1.- La lista de paquetes capturados
2.- Los detalles del paquete seleccionado. Muestra los protocolos y campos de protocolo del paquete seleccionado
3.- Los detalles en bytes. Muestra un volcado hexadecimal canónico de los datos del paquete. Cada línea contiene el desplazamiento de datos, dieciséis bytes hexadecimales y dieciséis bytes ASCII. Los bytes no imprimibles se reemplazan con un punto.

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

Primero se tiene que habilitar el mirroring de los puertos que vamos a analizar en la configuración del Router. Si se quisiera hacer por la WAN se tienen que usar softwares terceros para lograr esto, y seguido se usa el Wireshark para analizar los paquetes de la red LAN

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

No ejecutará Wireshark. Carece de un entorno gráfico y otras funciones del sistema operativo que Wireshark necesita para funcionar. Una computadora que ejecute Wireshark en Linux o Windows PUEDE conectarse a uno de los puertos de un enrutador Cisco para capturar el tráfico de la red.

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

Sí, entrando a la ruta de la carpeta donde está instalado Wireshark desde el cmd e ingresar el comando *wireshark -h*

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?

http en la sección de filtros

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

Para capturar el tráfico Ethernet que no sea el tráfico Unicast hacia y desde el host en el que está ejecutando Wireshark, tráfico Multicast y tráfico Broadcast, el adaptador deberá ponerse en modo promiscuo, de modo que el filtro mencionado anteriormente esté apagado. y todos los paquetes recibidos se entregan al host

17.- Wireshark offers two main types of filters:

Filtros de captura y filtros de display. Los filtros de captura se utilizan para filtrar al capturar paquetes y se comentan. Los filtros de visualización se utilizan para filtrar qué paquetes se muestran y se describen a continuación.

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

dst host <your Ip>

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

not tcp port 3389 asumiendo que está ejecutando RDP en el puerto estándar. Si se conecta al servidor a través de RDP y luego ejecuta Wireshark en el servidor, Wireshark debería aplicar automáticamente ese filtro de captura en el servidor.

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

tcp.flags.syn==1

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

tcp.flags.reset == 1

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

arp

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

tcp port 80

http

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

tcp port 23

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

smtp
tcp port pop3 -- Captura
 imap

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

1.- Física - Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI
2.- Vínculo de datos - PPP, IEEE 802.2
3.- Internet - IPv4, IPv6, ARP, ICMP
4.- Transport - TCP, UDP, SCTP
5.- Aplicación - NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros.

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

Mail exchange dirige el correo electrónico a un servidor de correo. El registro MX indica cómo se deben enrutar los mensajes de correo electrónico de acuerdo con el Protocolo simple de transferencia de correo (SMTP, el protocolo estándar para todos los correos electrónicos).

28.- Describe the TCP Three Way HandShake

TCP utiliza un protocolo de enlace de tres vías para establecer una conexión confiable. La conexión es full duplex, y ambos lados se sincronizan (SYN) y se reconocen (ACK) entre sí. El intercambio de estos cuatro indicadores se realiza en tres pasos: SYN, SYN-ACK y ACK

29.- Mention the TCP Flags

- 1st **Flag** - Urgent Pointer.
- 2nd **Flag** - ACKnowledgement.
- 3rd **Flag** - PUSH. ...
- 4th **Flag** - Reset (RST)
- 5th **Flag** - SYNchronisation **Flag**. ...
- 6th **Flag** - FIN **Flag**

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

Porque usan un valor llamado TTL o Time To Live, que indica el tiempo que tiene para llegar a su destino antes de que expire. Este valor es el indicador del sistema operativo, ya que cada sistema operativo tiene su propio TTL.