PREGUNTAS Y RESPUESTAS

Guía de estudio telecomunicaciones

ALUMNO: MANUEL ALFONSO ALONZO CHI

17 DE DICIEMBRE DE 2020

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

How Packet Sniffers Work?

Funcionan de tal manera que capturan y almacena los paquetes que se envían o reciben desde la computadora siempre y cuando estos paquetes ingresen o atraviesen el router.

3.- Describe The Seven-Layer OSI Model.

Es una estructura de siete capas para las actividades de la red, cada una de las capas tiene asociada varios protocolos. Estas capas representan operaciones de transferencia de datos.

Lo que hace el modelo OSI es enumerar las capas de los protocolos dese la superior hasta la inferior quedando de la siguiente forma

7-Aplicación

6-Presentacion

5-sesion

4-Transporte

3-Red

2-Enlace de Datos

1-Fisica

Cada una de estas capas tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta llegar al destino.

4.- Describe Traffic Classifications.

Broadcast, multidifusion, unicast

5.- Describe sniffing around hubs.

Los hub son dispositivos que simplemente reenvían los bits que llegan a un puerto del hub a todos los demás puertos del hub.

para analizar el tráfico que se ejecuta a través de una computadora conectada a un hub, todo lo que necesita hacer es conectar un sniffer a un puerto vacío en el hub. Podrá ver todas las comunicaciones hacia y desde esa computadora, así como todas las comunicaciones entre cualquier otro dispositivo conectado a ese hub.

6.- Describe sniffing in a switched environment

En un entorno de conmutación, la expansión de puertos se utiliza para configurar un conmutador para enviar una copia del tráfico de cualquier puerto a un puerto de monitor, el puerto al que se conectaría un sistema Wireshark. Este método de análisis de redes conmutadas solo se puede utilizar si el conmutador admite esta funcionalidad.

7.- How ARP Cache Poisoning Works?

un atacante envía mensajes falsificados ARP a una LAN. Como resultado, el atacante vincula su dirección MAC con la dirección IP de un equipo legítimo (o servidor) en la red. Si el atacante logró vincular su dirección MAC a una dirección IP auténtica, va a empezar a recibir cualquier dato que se puede acceder mediante la dirección IP.

8.- Describe sniffing in a routed environment

los datos deben atravesar varios enrutadores, es importante analizar el tráfico en todos los lados del enrutador.

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.

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

El panel de la lista de paquetes (Arriba), El panel de detalles del paquete (Medio) El panel de bytes del paquete (Abajo).

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

Estar conectados al router y elegimos el puerto en el que se está conectado y se inicia la captura

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

No, solo en sistemas operativos

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

Si, si es posible usando el comando Wireshark.exe

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

Wireshark se puede usar para verificar si los paquetes se están enviando 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?

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?

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:

Filtros de captura y filtros de visualización

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

ip.dst==ip

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

protocolos RDP

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.rst==1

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

No arp

23.- Which wireshark filter can be used to filter All HTTP traffic 24.- Which wireshark filter can be used to filter Telnet or FTP traffi

http

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

tcp.port==20

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

pop o imap

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

Aplicacion- ssh-dhcp-dns

Transporte- tcp-udp-sctp

Internet-ipv4-ipv6-icmp

Acceso a la red-arp-ppp-ethernet

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

o es principalmente una lista de servidor de intercambio de correo que se debe utilizar para el dominio.

28.- Describe the TCP Three Way HandShake

Syn peticion al servidor, syn/ack aprueba la solicitud del cliente, ack establece la comunicación.

29.- Mention the TCP Flags

SYN, ACK, FIN, RST, PSH, URG

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

Ping es una utilidad de línea de comandos, disponible en prácticamente cualquier sistema operativo con conectividad de red, que actúa como una prueba para ver si se puede acceder a un dispositivo en red. El comando ping envía una solicitud a través de la red a un dispositivo específico