Laury del Rosario Mex Martin 16/Diciembre/2020

1. Factors to consider when selecting a packet sniffer:

Que pueda interpretar los protocolos comunes de Red los cuales pueden ser: ICMP, TCP, UDP, DNS y HTTP

Facilidad de uso del rastreador de paquetes, fácil instalación, diseño del programa.

2. How Packet Sniffers Work?

Recopilan información (paquetes) de todo un tráfico de red a través de la interfaz de red física

3. Describe The Seven-Layer OSI Model.

- **Capa 1. Física** es la representación física del sistema.
- **Capa 2. Enlace de datos** Proporciona transferencia de datos de un nodo a otro nodo
- **Capa 3. Red** es responsable del reenvío de paquetes a través de diferentes enrutadores.
- **Capa 4 Transporte** Se ocupa de la transferencia de datos.
- **Capa 5 Sesión** Cuando dos dispositivos ya sea computadora o servidores quieren entablar una conversación entre ellos.
- **Capa 6 Presentación** cuando se hace el cifrado y descifrado de datos para una transmisión segura
- **Capa 7 Aplicación** Es lo que el usuario ve como por ejemplo un navegador web (Google Chrome, Firefox, Safari, etc.)

4. Describe Traffic Classifications

- **Tráfico Broadcast:** Un usuario envía paquetes o mensajes a todos.
- **Tráfico Multidifusión**: Un usuario envía paquetes o mensajes a un grupo en especifico
- **Tráfico Unicast:** Un usuario envia paquetes o mensajes a otro usuario

5. Describe sniffing around hubs

Para realizar esto la computadora debe estar conectada directamente al hub a través de un puerto vacío que tenga para comenzar a capturar el tráfico y poder analizarlo de cualquier dispositivo conectado al hub

6. Describe sniffing in a switched environment.

La persona que está conectada al conmutador solo puede ver el trafico que se envía a su máquina ya que en un entorno conmutado solo se le puede enviar mensajes a los dispositivos

7. How ARP Cache Poisoning Works?

El atacante envia mensajes falsos ARP para llenar la tabla de direccionamiento de una LAN, para poder vincular su dirección MAC a una dirección IP y cuando lo logra, el ya puede comenzar a recibir cualquier tipo de dato mediante esa dirección IP

8. Describe sniffing in a routed environment

Para hacer el sniffing es importante ubicarnos en la red conmutada correctamente ya que los paquetes pueden perderse de una red a otra

9. Describe the Benefits of wireshark

- Es gratis
- Conteo una interfaz grafica
- Soportar más de 480 protocolos distintos
- Trabajar tanto con datos capturados desde una red durante una sesión con otros guardados.

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

- Panel de lista de paquetes
- Panel de detalles de paquetes
- Panel de paquetes de bytes

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

Primero debemos estar conectados directamente del Router de Internet y en opciones de captura seleccionamos la entrada en donde está conectado, iniciamos la captura y ya estaremos viendo el tráfico.

12. Can wireshark be setup on a Cisco router?

No se puede configurar en un enrutador Cisco, ya que ejecuta un sistema operativo

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

Sí, es posible comenzar a usar el ejecutable apropiado en Windows utilizando el comando wirehark.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 comprobar si los paquetes ICMP se envían desde el sistema y 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?

el filtro es tcp.dstport == 80. Porque HTTP usa ese puerto

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

Considerando que la dirección IP del sistema es 192.168.128.2, el filtro sería ip.src == 192.168.128.2

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?

dst host host

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

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.reset 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

tcp.port 80

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)

smtp, pop o imap

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

Aplicación

- 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?

Dirige el correo electrónico a un servidor de correo e indica como se deben de enrutar los mensajes de correo mediante SMTP

28. Describe the TCP Three Way HandShake

Es un proceso de 3 Pasos

SYN que es donde el cliente hace una petición al servidor

SYN/ACK donde el servidor aprueba la solicitud del cliente

ACK el servidor le da respuesta al cliente para establecer la comunicación

29.- Mention the TCP Flags

SYN: Inicia la conexión

ACK: Reconoce la recepción de un paquete.

FIN: No habrá más transmisiones.

RST: Resetea y aborta la conexión.

PSH: Envía dato almacenados al buffer.

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

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

Esto es a través del TTL que es un valor que almacena en cache y al final de un comando Tracer nos aparece un numero al final que son los saltos que hizo, sumamos los valores que nos da del TTL y del numero de saltos, el resultado que nos da lo vamos a verificar en la tabla de los valores determinados de TTL de un sistema operativo.