INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Examen

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

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

- Depende para que lo vas a usar y mediante que método, se tiene que ver en que usuario se va instalar la tarjeta y para que motivos si es para que checar el trafico para de red en una empresa de manera ética ósea que tu eres trabajador o otros motivos no tan legales y obviamente que programa vas a usar

2.- ¿Cómo funcionan los detectores de paquetes?

- se configura una tarjeta de red mediante un software, esta tarjeta se pone en un modo “promiscuo” que siempre checa los paquetes que no son para su dirección Mac , sino que los almacena y los lee, entonces el programa comienza una lectura de toda la información a través de la tarjeta de red

3.- Describe el modelo OSI

- El modelo OSI se describe mediante 7 capas los cuales sirven de cómo fue la transmisión de un paquete en la red mediante distintas capas para saber cómo fue el establecimiento de comunicación, el enrutamiento y el envió
- Capa 1 física: se encarga de las conexiones físicas mediante cables de pares trenzados, cable coaxial, ondas y fibra óptica y maneja las señales y transmite el flujo de bits
- Capa 2 Enlace: de datos En esta capa se encarga de dar los medios funcionales para establecer la comunicación de elementos físicos lo cual usa los direccionamientos físicos
- Capa 3 red: En esta capa se encarga de la identificación del enrutamiento entre dos o mas redes conectadas con esto hace que los datos lleguen desde el transmisor al receptor siendo capaz de hacer las conmutaciones y encaminamientos
- Capa 4 Transporte: Realizar el transporte de los datos desde el origen usando diferentes protocolos como UDP orientado al envío sin conexión o segmento, si trabaja con el protocolo TCP orientada
- Capa 5 Sesión: En esta capa se podrá controlar y mantener activo el enlace entre las maquinas
- Capa 6 presentación: Aquí se encarga de la presentación de la información transmitida
- Capa 7: aplicación: Aquí permite a los usuarios ejecutar acciones y comandos en las aplicaciones como en sus propias aplicaciones

4.- Describe las clasificaciones de tráfico de red.

Sensitive traffic: Es el tráfico que el operador espera entregar a tiempo. Como juegos en línea, videoconferencias etc.

Best-effort traffic: Este es el tráfico que se llega a considerar que no es sensible a las métricas de calidad de servicio (jitter, pérdida de paquetes, latencia).

Undesired traffic: Esta categoría generalmente se limita a la entrega de correo no deseado y tráfico creado por gusanos, botnets y otros ataques maliciosos.

5.- Describe la captura de tráfico en un hub

- Trata sobre el tráfico en un hub sobre todos los puertos que están conectados, para analizar el trafico solo necesita un equipo con un sniffing al hub y empezar a capturar todos los datos con solo conectar a un conector en l hub se podrá ver todos los paquetes de todos los equipos que estén conectados a ese equipo

6.- Describa la captura de tráfico en switches

- La forma de captura es casi idéntica a la de las hub dentro del switch se conecta un sniffing y se empieza a trabajar como si fuera otro equipo simplemente configurando ya que este nunca recibirá trafico al menos que a su dirección Mac se le asigne ese trabajo para eso se usa la tecnología mirroring lo cual la información se transmite hacia y desde los equipos que quieren analizar

7.- Como Funciona ARP Cache Poisoning?

- R: Altera las tablas ARP de destino para la redirección del tráfico local a través de otro host; se usa normalmente se usa para ataques man-in-the-middle

8.- Describe el rastreo en un entorno enrutado.

Se envía trafico de red a u un hub que los transmite a todos el routers. Las redes son completamente diferentes en la forma en que pueden llegar funcionar

9.- Describa los beneficios de Wireshark

- Licencia libre
- Muy fácil de aprender a usar
- Basando en la librería de Pcap
- Gran capacidad de filtrado
- Es compatible con más de 480 protocolos

10.- Describa los tres paneles de la ventana principal en Wireshark

- Panel de captura: muestra los paquetes capturado en orden, aquí divide entre columnas y filas la información importante
- Panel de detalle del paquete: al selecciona un paquete de datos se muestra detalladamente el paquete selecciona sobre los protocolos que usa
- Panel de bytes del paquete: debajo del panel de paquete se muestra el panel de bytes lo cual representa la información a un formato actual lo cual es la secuencia de bytes del flujo

11.- ¿Cómo configuraría Wireshark para monitorear los paquetes que pasan a través de un enrutador de Internet?

- Instalaría un sniffer por software en mi equipo lo cual crearía una tarjeta virtual de red un ejemplo de ello sería acrylic wi-fi sniffer con eso usaría wireshark lo cual en lugar de analizar los paquetes de red, analizaría mediante la nueva tarjeta de red

12.- ¿Se puede configurar wireshark en un router Cisco?

- Si es posible mediante la configuración router del cisco junto con wireshark con Windows o linux

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

- Si se puede con diferentes conmandos se puede usar wireshark desde capturar paquetes hasta personalizar el interfaz para iniciar una captura de paquetes seria
- -a <capture autostop condition>, --autostop <capture autostop condition>

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 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 de wirehark se puede usar para verificar todas las solicitudes entrantes a un servidor web HTTP?

- http.request.method == “GET”

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

- dst net net

17.- Wireshark ofrece dos tipos principales de filtros:

- Captura y visualización

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

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

- Not por 3389

20.- ¿Qué filtro wireshark se puede utilizar para filtrar los paquetes TCP con el indicador SYN establecido

- tcp.flags.syn==1 && tcp.flags.ack==0

21.- Qué filtro wireshark se puede utilizar para filtrar los paquetes TCP con el indicador RST establecido

tcp.flags.syn

== 1. ... filtrar ya que cerrar una conexión puede asociarse con paquetes FIN o

RST

22.- Qué filtro wireshark se puede utilizar para borrar el tráfico ARP

- Port not arp
- Arp -d

23.- Qué filtro wireshark se puede utilizar para filtrar todo el tráfico HTTP

- http

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

- telnet or port 21

25.- Qué filtro wireshark se puede utilizar para filtrar el tráfico de correo electrónico (SMTP, POP o IMAP)

- tcp.port eq 25

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

- Física: ethernet (IEEE 802.3), Token Ring, RS-232, FDDI
- Acceso a red: PPP, IEEE 802.2
- Red: IPv4, IPv6, ARP, ICMP
- Transportes: TCP, UDP, SCTP
- Aplicación: NFS, NIS, DNS

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

- Mail Exchange lo cual sirve para saber el registro de Dns en el cual el cliente en que dominio se encuentra el servidor de correo electrónico adecuado

28.- Describa el TCP Three Way HandShakeha

- Se comienza una conexión en una ellas , una abre el socket en un puerto tcp y se queda a la espera de una nueva conexión a esto se le conoce como apertura pasiva y determina el lado servidor de una conexion lo cual realiza una apertura activa de un puerto enviado en un paquete SYN se inicia al servidor como parte del triple hand shake, en el servidor se comprueba un puerto abierto pues se checa que el dispositivo tenga este servicio activo y este aceptando las peticiones en el numero de puerto, en caso de no estarlo se envía al cliente un paquete de respuesta con el bit RST activado, lo que significa el rechazo del intento de conexión. En caso de que sí se encuentre abierto el puerto, el lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un ACK, completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de conexión.

29.- Mention the TCP Flags

- SYN. Solicita la conexión
- ACK. Reconoce (Acknowledge) la conexión
- FIN. Finaliza la conexión
- RST. Aborta una conexión, por motivos diversos

30.- ¿Cómo el comando ping puede ayudarnos a identificar el sistema operativo de un host remoto?

Funciona como que el host remoto reciba el paquete y envía una respuesta de vuelta de icmp a cambio y probando con esto nos sirve para la detección de fallos y otras cosas