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

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

Debemos de tener en cuenta que tenemos que capturar los paquetes y analizarlos, entonces hay que buscar uno que sea versión libre que este diseñado para este, que tenga interfaz de usuario para que sea mucho mas entendible y podamos trabajar en ello.

2.- How Packet Sniffers Work?

2.- ¿Cómo funcionan los Packtes Sniffers?

Este nos sirve para que estemos monitoreando y también que podamos analizar el trafico en una red de computadora, se detectan problemas y otras cosas.

3.- Describe The Seven-Layer OSI Model.

3.- Describe el modelo OSI de siete capas.

En si este modelo nos ayuda a describir una estructura para las actividades de red. En si las capas representan las operaciones de transferencia de datos comunes a todos los tipos de transferencias de datos entre las redes de cooperación.

N° de capa	Nombre de capa
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Vinculo de datos
1	Fisica

4.- Describe Traffic Classifications.

4.- Describe las clasificaciones de tráfico.

En esta clasificación se cuenta con 3 tipos de trafico que vamos a observar a continuación.

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 sniffing around hubs.

5.- Describe sniffing alrededor de los hubs:

En este tipo de casos, aquí es que podamos ver la comunicación hacia y desde la computadora que estemos analizando, así como también cualquier otro dispositivo que este conectado. Todo esto se ejecuta conectando un rastreador de paquetes a un puerto vacío.

6.- Describe sniffing in a switched environment:

6.- Describe el olfateo en un entorno conmutado:

Aquí nos describe que para poder realizar esta tarea se debe lograr mediante una configuración de un ataque de “intermediario”, entonces en este caso el atacante utiliza variedad de técnicas para que el trafico de red se forcé hacia la víctima y cuando esto es que ocurre ya podemos decir que el atacante puede inspeccionar el trafico de red de la víctima en este caso.

7.- How ARP Cache Poisoning Works?

7.- ¿Cómo funciona el envenenamiento de caché ARP?

De echo el funcionamiento de este es que el atacante envía mensajes que son falsificados tipo (ARP) a una red LAN, entonces se empezaran a recibir datos en los que se puedan acceder mediante la IP y con eso se puede robar información como en caso de empresas que es muy peligroso en estos casos.

8.- Describe sniffing in a routed environment:

8.- Describe el rastreo en un entorno enrutado.

Esto se debe a que se envía tráfico de red a un hub que lo transmite a todos. Conmutado. Las redes son completamente diferentes en la forma en que pueden llegar a funcionar. Los conmutadores funcionan enviando tráfico al host de destino solamente.

9.- Describe the Benefits of wireshark

9.- Describe los Beneficios de Wireshark:

Algunos de los beneficios que se pueden aprovechar de Wireshark podrían ser los siguientes:

Que es gratuito y todos los usuarios podemos aprovechar y usar este software para lo que estemos necesitando.

Nos permite guardar los análisis que hayamos hecho en filtros de búsqueda, ósea en las capturas de datos que hayamos podido capturar.

Nos permite observar desde el protocolo y todo tipo de información que estemos solicitando, además que tiene herramientas muy sencillas de usar y nos ayuda mucho mas en el aprendizaje de esto.

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

10.- Describe los tres paneles de la ventana principal de Wireshark:

Para empezar si nos damos cuenta cuando usamos Wireshark nos damos cuenta que esta contiene 3 ventanas **la lista de paquetes capturados** en donde se ven más a detalle como por ejemplo que vienen en código de colores, porque están enumerados etc**., el panel de detalle del paquete seleccionado** viene mucho más a detalle el contenido del paquete y diversas cosas y, en tercer lugar, el panel de paquetes de bytes convertido en hexadecimal.

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

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

Lo que haría seria cerrar los programas que generen trafico para capturar esos paquetes nadamas, seria ejecutar la aplicación depende si solo lo queremos capturar de una sola aplicacacion o de ya toda la red, abrir el wireshark y empezarlo a capturar y analizar los paquetes.

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

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

Se tiene entendido que sí, pero el router cisco debe de contener algunas características para que pueda funcionar correctamente. Por ejemplo, El sistema debe utilizar un Cisco Catalyst 4500 Series Switch, también debe tener una base Ip etc.

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

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

Si es posible, y este tiene algunos comandos básicos para que nosotros lo podamos ocupar. -i interface -k iniciar de inmediato la captura (usaremos esta opción siempre) -f filtro de captura -s snaplen

Por ejemplo, si queremos arrancar Wireshark estableciendo como interface de captura la establecida como número 2, como filtro de captura “host 192.168.1.5”, y estableciendo un snaplen = 512:

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

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

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.- Which wireshark filter can be used to check all incoming requests to a HTTP Web server?

15.- ¿Qué filtro Wireshark se puede utilizar para verificar todas las solicitudes entrantes a un servidor web HTTP?

http contains pues este filtro visualiza el trafico origen y destino, además visualiza los paquetes que contienen en el protocolo htttp.

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

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

dst net net que este nos sirve para capturar todo el trafico de destino de la red.

17.- Wireshark offers two main types of filters:

17.- Wireshark ofrece dos tipos principales de filtros:

Filtros de captura: son los que se establecen para mostrar solo los paquetes de cumplan los requisitos indicados en el filtro.

Filtros de visualización: establecen un criterio de filtro sobre los paquetes capturados y que estamos visualizando en la pantalla principal de Wireshark. Estos filtros son más flexibles y potentes.

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

18.- ¿Qué filtro de wireshark se puede usar para monitorear los paquetes entrantes a un sistema específico en la red?

Con el frame contains, ya que con este filtro capturamos todos los paquetes de origen

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

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

"not tcp port 3389" asumiendo que el RPD se este ejecutando en este caso.

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

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

En el siguiente ejemplo se capturo los paquetes tcp con origen y destino puerto 80 y con el flag TCP SYN activado. (Quitamos de las opciones el -q para deshabilitar la salida rápida y obervar la notación S que indica SYN).

windump -i1 -tn tcp and port 80 and “tcp[tcpflags] & tcp-syn !=0”

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

21.- ¿Qué filtro Wireshark se puede utilizar para filtrar paquetes TCP con la bandera RST activada?

En este caso para filtrar esos paquetes debemos de hacer coincidir solo los paquetes TCP con el indicador SYN establecido, necesita para usar tcp.flags.syn == 1. ... filtrar ya que cerrar una conexión puede asociarse con paquetes FIN o RST.

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

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

ether proto \arp, aunque se usa muy rara vez en estos casos.

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

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

Para poder mostrar todo el tráfico utilizaremos el filtro http.request.method == “POST”. Este filtro nos mostrará todo el tráfico en la red que sea HTTP.

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

24.- ¿Qué filtro Wireshark se puede usar para filtrar el tráfico Telnet o FTP?

En una terminal usamos el comando ftp 192.168.1.103 para conectarnos por ftp a metasploitable, ponemos las credenciales msfadmin, detenemos la captura en wireshark en el filtro ponemos "ftp", en cualquier linea de ftp damos clic derecho y seleccionamos Follow TCP Stream.

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

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

Para filtrar ese trafico se deben de ocupar lo siguiente:

smtp (filtro para protocolo SMTP ó correo electrónico). Con esto nos filtrara ese tipo de tráfico.

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

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

La capa de aplicación: HTTP, FTP, SMTP.

La capa de transporte: UDP, SCTP,

La capa de red: ICMP, IPv4, ICMPv6.

La capa física: ARP, DSL, ISDN.

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

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

Significa “Registro de intercambio de correo” y esta en si viene un tipo de registro y que usa el recurso DSN que se encamina un correo electrónico en red.

28.- Describe the TCP Three Way HandShake:

28.- Describe el TCP Three Way HandShake:

es un proceso que se utiliza en una red TCP / IP para establecer una conexión entre el servidor y el cliente, es un proceso de tres pasos que requiere que tanto el cliente como el servidor intercambien paquetes de sincronización y reconocimiento antes de que comience el proceso de comunicación de datos reales. (SYN, SYN-ACK, ACK).

29.- Mention the TCP Flags:

29.- Mencionar las banderas de TCP:

Estas banderas que se emplean para establecer el mantenimiento y la terminación de una conexión.

SYN: Inicia la conexión entre hosts.

ACK: Reconoce la recepción de un paquete.

FIN: No habrá más transmisiones.

RST: Resetea y aborta la conexión, por diversos motivos.

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

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

Nos sirve para que el host remoto recibe el paquete y envía una respuesta de eco ICMP a cambio, comprobando ... El uso del comando ping nos sirve para la detección de fallos y otras cosas mas.