1.- FACTORS TO CONSIDER WHEN SELECTING A PACKET SNIFFER:

Qué elemento de un analizador de protocolo se requiere para capturar paquetes de unidifusión enviados

2.- HOW PACKET SNIFFERS WORK?

Los rastreadores de paquetes funcionan interceptando y registrando el tráfico de red que pueden ver a través de la interfaz de red cableada o inalámbrica a la que tiene acceso el software de rastreo de paquetes en su computadora host. En una red cableada, la información que se puede capturar depende de la estructura de la red.

3.- DESCRIBE THE SEVEN-LAYER OSI MODEL.

7 Aplicación.- Se compone de los servicios y aplicaciones de comunicación estándar que puede utilizar todo el mundo.

6 Presentación.- Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el sistema.

5 Sesión.- Administra las conexiones y terminaciones entre los sistemas que cooperan.

4 Transporte.- Administra la transferencia de datos. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos.

3 Red.- Administra las direcciones de datos y la transferencia entre redes.

2 Vínculo de datos.- Administra la transferencia de datos en el medio de red.

1 Física.- Define las características del hardware de red.

4.- DESCRIBE TRAFFIC CLASSIFICATIONS.

Las clasificaciones de tráfico permiten clasificar variables de tráfico (props). Las clasificaciones de tráfico solo pueden usar clasificaciones de texto.

5.- DESCRIBE SNIFFING AROUND HUBS.

Es un proceso de monitoreo y captura de todos los paquetes de datos que pasan por una red determinada. Los rastreadores son utilizados por el administrador de red / sistema para monitorear y solucionar problemas de tráfico de red. Los atacantes utilizan rastreadores para capturar paquetes de datos que contienen información confidencial como contraseña, información de cuenta, etc.

El rastreo de paquetes es la práctica de recopilar, recopilar y registrar algunos o todos los paquetes que pasan por una red informática.

6.- DESCRIBE SNIFFING IN A SWITCHED ENVIRONMENT.

Se logra mediante la configuración de un ataque de "intermediario". El atacante utiliza una variedad de técnicas para forzar el tráfico de red hacia / desde la víctima para ir a la máquina del atacante. Cuando esto ocurre, el atacante puede inspeccionar (o incluso modificar) el tráfico de red de la víctima.

7.- HOW ARP CACHE POISONING WORKS?

El envenenamiento de caché de ARP pone al atacante en posición de interceptar las comunicaciones entre las dos computadoras. La computadora A cree que se está comunicando con la computadora B, pero debido a la tabla ARP envenenada, la comunicación en realidad va a la computadora del atacante. El atacante puede entonces responder a la Computadora A (pretendiendo ser la Computadora B), o simplemente reenviar los paquetes a su destino previsto.

8.- DESCRIBE SNIFFING IN A ROUTED ENVIRONMENT

Hay dos tipos básicos de entornos Ethernet y la forma en que funcionan los rastreadores en ambos casos es... paquetes de un host a otro. El conmutador tiene... ARP Watch: como se describió anteriormente, un método para rastrear una red conmutada es ARP.

9.- DESCRIBE THE BENEFITS OF WIRESHARK

Este software gratuito le permite analizar el tráfico de la red en tiempo real y, a menudo, es la mejor herramienta para solucionar problemas en su red. Los problemas comunes que Wireshark puede ayudar a solucionar incluyen paquetes caídos, problemas de latencia y actividad maliciosa en su red.

- Los administradores de red lo utilizan para solucionar problemas de red.
- Los ingenieros de seguridad de redes lo utilizan para examinar problemas de seguridad.
- Los ingenieros de control de calidad lo utilizan para verificar aplicaciones de red.
- Los desarrolladores lo utilizan para depurar implementaciones de protocolos.

10.- DESCRIBE THE THREE PANES IN THE MAIN WINDOW IN WIRESHARK

La lista de paquetes capturados, el panel de detalle del paquete seleccionado y, en tercer lugar, el panel de paquetes de bytes en hexadecimal.

11.- HOW WOULD YOU SETUP WIRESHARK TO MONITOR PACKETS PASSING THROUGH AN INTERNET ROUTER

- Cerrar todos los programas que generen tráfico de red, el cual no queremos capturar
- Asegurarnos de que el firewall se encuentra desactivado, ya que podría bloquear cierto tráfico y no aparecerá en Wireshark, o solamente aparecerá parte del tráfico generado.

- Si queremos capturar un cierto tráfico de datos que genere una aplicación, es recomendable esperar 1 segundo antes de iniciarlo y que capture tráfico de red del equipo, a continuación, ejecutamos esa aplicación, y por último, cerramos la aplicación y esperamos 1 segundo antes de detener la captura de tráfico.

12.- CAN WIRESHARK BE SETUP ON A CISCO ROUTER?

Un enrutador Cisco tiene un procesador y un software operativo diseñados para ejecutar aspectos de una red. No es un sistema operativo (SO) de propósito general. 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?

Para iniciar Wireshark usando el cuadro de comando Ejecutar:

1. Abra el menú Inicio o presione la tecla Windows + R.
2. Escriba Wireshark en el cuadro de comando Ejecutar.
3. Presione Entrar.

14.- A USER IS UNABLE TO PING A SYSTEM ON THE NETWORK. HOW CAN WIRESHARK BE USED TO SOLVE THE PROBLEM.

Ping usa ICMP. Wireshark se puede utilizar para comprobar si los paquetes ICMP se envían desde el sistema.

15.- WHICH WIRESHARK FILTER CAN BE USED TO CHECK ALL INCOMING REQUESTS TO A HTTP WEB SERVER?

Para ver solo el tráfico HTTP, escriba http (minúsculas) en el cuadro Filtro y presione Entrar.

16.- WHICH WIRESHARK FILTER CAN BE USED TO MONITOR OUTGOING PACKETS FROM A SPECIFIC SYSTEM ON THE NETWORK?

Ping usa ICMP. Wireshark se puede utilizar para comprobar si los paquetes ICMP se envían desde el sistema. Si se envía a cabo, se puede también comprobar si los paquetes se reciben.

17.- WIRESHARK OFFERS TWO MAIN TYPES OF FILTERS:

-Los filtros de captura (como el puerto tcp 80) no se deben confundir con los filtros de visualización (como tcp.port == 80).

-tráfico DNS (puerto 53):

18.- WHICH WIRESHARK FILTER CAN BE USED TO MONITOR INCOMING PACKETS TO A SPECIFIC SYSTEM ON THE NETWORK?

Capturar solo el tráfico que está destinado a la IP de su host

19.- WHICH WIRESHARK FILTER CAN BE USED TO FILTER OUT RDP TRAFFIC?

Se usa el puerto TCP 3389

20.- WHICH WIRESHARK FILTER CAN BE USED TO FILTER TCP PACKETS WITH THE SYN FLAG SET

fin == 1 es el filtro correcto para obtener todos los paquetes con los indicadores SYN y FIN establecidos

21.- WHICH WIRESHARK FILTER CAN BE USED TO FILTER TCP PACKETS WITH THE RST FLAG SET

Una forma de crear un filtro como ese es mirar la sección Banderas de un fragmento de TCP y luego, para cada bit que le interese, haga clic con el botón derecho en el campo de ese bit y seleccione "Preparar como filtro " y luego seleccione "... o Seleccionado". (Es posible que deba cambiar el valor de lo que viene después del signo igual).

22.- WHICH WIRESHARK FILTER CAN BE USED TO CLEAR ARP TRAFFIC

Utilice arp -d para borrar la caché ARP.

23.- WHICH WIRESHARK FILTER CAN BE USED TO FILTER ALL HTTP TRAFFIC

Servidores web HTTP utilizan el puerto TCP 80. Las solicitudes entrantes al servidor web tendrían el número de puerto de destino como 80. Por lo tanto, el filtro tcp.dstport == 80.

24.- WHICH WIRESHARK FILTER CAN BE USED TO FILTER TELNET OR FTP TRAFFIC

Escriba Telnet en el campo Nombre del filtro y puerto 23 en el campo Cadena de filtro.

25.- WHICH WIRESHARK FILTER CAN BE USED TO FILTER EMAIL TRAFFC (SMTP, POP, OR IMAP)

- SMTP (envío, sin cifrado) - puerto 25
- SMTP (envío, con cifrado) - puerto 587
- POP3 (recuperando, sin cifrado) - puerto 110
- POP3 (recuperación, con cifrado) - puerto 995
- IMAP (recuperando, sin cifrado) - puerto 143
- IMAP (recuperación, con cifrado) - puerto 993

26.- LIST 3 PROTOCOLS FOR EACH LAYER IN TCP/IP MODEL

5,6,7	Application, Session, Presentation	Application	NFS, NIS+, DNS, `telnet`, `ftp`, `rlogin`, `rsh`, `rcp`, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP, ARP, ICMP
2	Data Link	Data Link	PPP, IEEE 802.2
1	Physical	Physical Network	Ethernet (IEEE 802.3) Token Ring, RS-232, others

27.- WHAT DOES MEANS MX RECORD TYPE IN DNS?

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). Al igual que los registros CNAME , un registro MX siempre debe apuntar a otro dominio.

Un registro de 'intercambio de correo' (MX) de DNS dirige el correo electrónico a un servidor de correo.

28.- DESCRIBE THE TCP THREE WAY HANDSHAKE

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

1ra Bandera - Puntero Urgente. El primer indicador es la urgente puntero indicador , como se muestra en la captura de pantalla anterior. ...

2da bandera - reconocimiento. La bandera de acuse de recibo se utiliza para reconocer la recepción exitosa de paquetes. ...

3ra Bandera - PUSH. ...

4ª Bandera - Reset (RST) Bandera . ...

5ta Bandera - Bandera de sincronización . ...

6a Bandera - Bandera FIN . ...

30.- HOW PING COMMAND CAN HELP US TO IDENTIFY THE OPERATING SYSTEM OF A REMOTE HOST?

Cuando se trata de “ mesa de ping ” de un host remoto , sus máquinas inicia el envío de eco ICMP peticiones y espera para una respuesta. Si la conexión está establecida, se recibe una respuesta de eco para cada petición. La salida para el comando ping contiene la cantidad de tiempo que toma para cada paquete para llegar a su destino y retorno.

Alan Gerardo Gijon Agosto