INSTITUTO TECNOLOGICO SUPERIOR DE TANTOYUCA

ING. SISTEMAS COMPUTACIONALES

Administración de Redes.

DOCENTE:

Ing. Edgar Medellín Orta

ALUMNO(A):

Arely Alejandra de Jesús Rendon

"ANALISIS DE PROTOCOLOS, SCANNERS Y SNIFFERS"

INDICE

Introducción.

Una de las actividades más comunes en la administración de una red o administración de seguridad, es la del análisis de tráfico de dicha red. Existen muchas herramientas que pueden sernos muy útiles dependiendo del S.O. y tipo de red, por ejemplo. Una de estas herramientas es un sniffer de red, basada en la librería de captura de paquetes (pcap) y que además funciona en plataformas tanto Windows como GNU/Linux-UNIX, y que hace uso de la librería Winpcap para funcionar correctamente.

Por ello es necesario el control de tráfico en una red a través de herramientas conocidas cono sniffers, necesarios para la detección de problemas y sobre todo para detectar el tráfico no esperado, presencia de puertas traseras, escaneos y cualquier otra intrusión que pudiera inferir en la red.

Contenido.

ANALIZADOR DE PROTOCOLOS

Un analizador de protocolos es un programa que permite a la computadora capturar tramas de la red para, posteriormente o en tiempo real, proceder a su análisis. Por analizar se entiende que el programa puede reconocer que la trama capturada transporta información asociada a un protocolo.

Por analizar se entiende que el programa puede reconocer que la trama capturada pertenece a un protocolo concreto (TCP, ICMP...) y muestra al usuario la información codificada y decodificada. De esta forma, el usuario puede ver todo aquello que en un momento concreto está circulando por la red que se está analizando.

Esto último es muy importante para un programador que esté desarrollando un protocolo, o cualquier programa que transmita y reciba datos en una red, ya que le permite comprobar lo que realmente hace el programa.

Además, estos analizadores son muy útiles a todos aquellos que quieren experimentar o comprobar cómo funcionan ciertos protocolos de red, si bien su estudio puede resultar poco ameno, sobre todo si se limita a la estructura y funcionalidad de las unidades de datos que intercambian. También, gracias a estos analizadores, se puede ver la relación que hay entre diferentes protocolos, para así, comprender mejor su funcionamiento.

Los sniffers o analizadores de protocolo son aplicaciones que operan en la capa de enlace del modelo OSI y permiten capturar todos los paquetes de datos en un proceso de comunicación determinado. Este tipo de herramientas nos permiten, entre otras cosas, entender mejor lo que está ocurriendo en la red.

De manera general, un sniffer ejecuta tres fases:

- Captura: En esta etapa se realiza la recolección de paquetes.
- Conversión: Luego, se toman los datos binarios y se les da formato para facilitar su lectura.
- Análisis: Como su nombre lo indica, en esta fase se analiza la información obtenida.

Existen analizadores de protocolos de tipo software y de tipo hardware.

De tipo hardware *como:*

Los analizadores de protocolos usb.

Los analizadores de protocolos de CAN.

Los analizadores de protocolo de Bluetooth.

Los analizadores de protocolos WiMedia.

Y también existen los analizadores de protocolos **software.**

COMMVIEW.

Un programa para capturar y analizar los paquetes de red.Es un programa para supervisar la actividad de Internet y de la red de área local(LAN) capaz de capturar y analizar los paquetes de red. Recopila información sobrelos datos que pasan a través de tu conexión por línea conmutada o tarjeta Ethernet y descodifica los datos analizados.

YORK.

Registro de todo el tráfico de red.York registra el origen, el destino y el tamaño de los paquetes de todo el tráfico dered en la red y, por supuesto, también el tráfico saliente.Es una aplicación diseñada para saber para qué es utilizada una red, así como para averiguar que paginas son visitadas.

MING CHAT MONITOR HOME.

Supervisa y graba las conversaciones de AOL, MSN, Yahoo!, ICQ, MySpace, etc. en modo oculto.Es una solución de software simple y asequible para los usuarios que desean controlar,supervisar y archivar el tráfico ilimitado de mensajería instantánea en la red de empresa o la reddoméstica, incluyendo: AOL Instant Messenger, MSN Messenger, Yahoo Messenger,ICQ , MySpaceIM, FacebookIM, WarcraftIM y QQ.

TCPMON.

Es un programa analizador de protocolos TCP/IP diseñado e implementado por el departamento

DISCA (Departamento de Informática de Sistemas y Computadores) dela Universidad Politécnica de Valencia para su uso, principalmente, en la docencia delas asignaturas de redes de computadores

Utilidad de un Sniffer

Los programas de sniffers han estado ejecutándose por la red durante mucho tiempo en dos formas. Los programas comerciales de sniffers se usan a menudo para ayudar en el mantenimiento de las redes. Mientras que sniffers “underground” son usados por los crackers para introducirse en los ordenadores ajenos.

Ventajas

Un Sniffer más que una herramienta de ataque en manos de un administrador de red puede ser una valiosa arma para la auditoría de seguridad en la red. Puesto que el acceso a la red externa debe estar limitado a un único punto. Un Sniffer puede ser la herramienta ideal para verificar como se está comportando la red.

Las ventajas en las que más se destacan los sniffers son:

- Control del Tráfico en la Red Administrada.
- Verificar el comportamiento de los usuarios de acuerdo a la normativa de la Red.
- Observar el uso indebido de un recurso que dañe el normal tráfico de la Red.
- Obtención de estadísticas de Tráfico.
- Se puede analizar qué servicios son los más utilizados en la Red.
- En base a esta información, se pueden definir políticas de adquisición de Software y Hardware.
- Suponiendo que se es un Atacante, ver las falencias y las fortalezas de ésta.
- Verificar que tráficos de paquetes realiza un proceso en particular.

Ejemplos de sniffers.

Ethereal o Wireshark

ETHEREAL es una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. (WireShark.com, 2012)

Ethereal permite analizar los paquetes de datos en una red activa como también desde un archivo de lectura previamente generado, un caso particular es generar un archivo con TCPDUMP y luego analizarlo con Ethereal.

A partir del año 2006 Ethereal es conocido como Wireshark y hoy en día está categorizado como uno de los TOP 10 como sniffer junto a Nessus y Snort ocupando el segundo lugar entre estos.

Fig 1. Sniffer Ethereal

Capsa packet Sniffer

Capsa es un analizador de red de paquetes para los administradores de red, puede supervisar, diagnosticar y solucionar problemas en la red y es lo suficientemente buena para uso doméstico, así como su uso en la pequeña empresa.

El Paquete de software libre Capsa Sniffer le permite monitorear y capturar 50 direcciones IP de red de datos de tráfico juntos y análisis de redes eficaces en tiempo real para los paquetes de red sniffing, y analizarlos.

Características del succionador de paquete:

- Detalle Supervisor de tráfico de todos los equipos
- El control de ancho de banda (para encontrar los equipos que están viendo vídeos en línea)
- Diagnóstico de Red para identificar problemas en la red
- La actividad Netwok registro (para la grabación de mensajería instantánea y correo web)
- Red de monitoreo del comportamiento.

Fig 2. Sniffer Capsa

SniffPass

SniffPass es un succionador de tráfico del paquete único, que se centra en la captura de contraseñas de tráfico de la red. Cada vez que se activa rastreadores contraseña SniffPass, se mantiene sobre el control de tráfico de red y tan pronto como se intercepta una contraseña, que inmediatamente pone de manifiesto que en la pantalla. Esta es una gran manera de encontrar las contraseñas olvidadas de sitios web.

SniffPass es muy fácil en su uso, y proporciona una agradable interfaz gráfica de usuario para controlar todas las contraseñas capturadas.

SniffPass es compatible con la mayoría de los protocolos de redes, tales como: POP3, IMAP4, SMTP, FTP y HTTP.

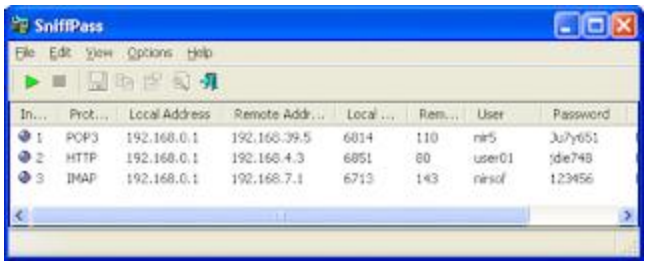

Fig 3. Sniffer SniffPass

Conclusión.

La información que circula por nuestra red puede ser fácilmente capturada por personas ajenas y la encriptación de datos es un método eficaz para evitar el uso de estos programas. Además, al crear un programa o sistema que utilice algún protocolo de red, se debe de tener en cuenta utilizar solo puertos y protocolos que va a utilizar evitando crear puertos innecesarios ya que esto puede generar filtrado de información no deseada.

En nuestro caso en nuestro utilizaremos el **software de monitoreo Cactus**, y este posee soporte incorporado para el analizador de protocolo SNMP, además que posee con interfaces graficas para el usuario facilitando así, su uso, viendo que nuestro software es de licencia publica general se abren un cumulo de posibilidades para su manejo y seguridad.

Bibliografía.

Las 5 Mejores herramientas Analizadoras de red y Sniffers. (22 de febrero de 2011). Obtenido de https://underc0de.org/foro/pentest/las-5-mejores-herramientas-analizadoras-de-red-y-sniffers!/?action=printpage;PHPSESSID=q9jespjudnd71oqab12vvcbot3

Argandoña, A. (2004). Sniffer ventajas y desventajas para administradores y atacantes. Chile: LOM Ediciones.

Rosas, A. R. (18 de noviembre de 2016). UNIDAD III y IV ANALISIS Y MONITOREO Y SEGURIDAD BASICA : 3.3 Analizadores de protocolos (scanners y sniffers).:. Obtenido de http://administracionderedesdeba.blogspot.mx/2016/11/33-analizadores-de-protocolos-scanners.html

Sotelo, A. H. (11 de enero de 2008). Seguridad y redes. Obtenido de Analizando la Red con WinDump / TCPDump.: https://seguridadyredes.wordpress.com/2008/01/11/analizando-la-red-con-windump-tcpdump-i-parte/

WireShark.com. (2012). Manual de usuario WireShark. USA.