****

**Sniffers**

**(Analizador de paquetes)**

**Integrantes: Pablo Stuardo**

**Fernanda Mateo**

**Oscar Veraguas**

**Profesor: Agustín González**

**Fecha: 23 / 07 / 2012**

**Institución: UTFSM**

**Resumen**

Durante las tareas normales, como navegar en la Web y la mensajería, las computadoras están en constante comunicación con otras máquinas.  Obviamente, el usuario debe ser capaz de ver todo el tráfico que viaja hacia o desde su máquina. Sin embargo, la mayoría de los PCs están en una red de área local (LAN), lo que significa que comparte una conexión con otros equipos. Si la red no es “switcheada” (un Switch es un dispositivo que filtra y reenvía los paquetes entre segmentos de la LAN), el tráfico destinado a cualquier máquina en un segmento se transmite a todas las máquinas en ese segmento. Esto significa que un equipo normalmente ve los datos que viajan desde y hacia cada uno de sus vecinos, pero los ignora, a menos que se indique lo contrario. Debido a esto, un sniffer puede existir y husmear estos datos.

En este informe desarrollaremos las formas en que trabajan estos programas, los usos que se les pueden dar y ciertas formas de protegerse de algunos de ellos, una vez que son utilizados de manera malintencionada ya que esa es la gran desventaja de estos programas.

Al final, los sniffers son herramientas muy poderosas, que permiten seguir avanzando en lo que son las redes de computadores, pero si son mal usados, pueden provocar mucho daño.

Introducción

En este informe hablaremos de los Sniffers o analizadores de paquetes, que son softwares que permiten capturar tramas de la red. Investigaremos y explicaremos más sobre su definición, su funcionamiento o forma de operar, los diferentes tipos de sniffers, usos que se les da, ya sea buenos o malos, como también enseñar formas de evitar que se usen de forma maliciosa contra uno mismo, ya que es una amenaza que cada vez cobra más importancia.

**Sniffers**

**Definición:**

Comenzaremos con explicar que es un “Sniffer” (Sniff: olfatear, rastrear) o “analizador de paquetes”. Un Sniffer es un software que se encarga de capturar paquetes en tránsito (entrada y salida) en una cierta red y analizarlos. En otras palabras, es un programa que puede mirar la información en tránsito en una red y obtener información de esta. Está hecho para recibir información que no está destinada para él, lo que es muy útil, pero a la vez un gran peligro.

Están disponibles para varias plataformas, tanto en las variaciones comerciales como en código abierto. Algunos de los paquetes más simples son muy fáciles de implementar en C o Perl, utilizando una interfaz de línea de comandos y descargando los datos capturados a la pantalla.   
 Los proyectos más complejos utilizan una interfaz gráfica de usuario. Las estadísticas de tráfico de gráficos, realizan un seguimiento de varias sesiones y ofrecen varias opciones de configuración.   
 Los sniffers de red son también los motores para otros programas. Los llamados “Sistemas de Detección de Intrusos” (IDS) utilizan sniffers para localizar paquetes que coincidan con las reglas designadas para marcar algo como malicioso o extraño. La utilización de la red y los programas de vigilancia a menudo los utilizan para recoger los datos necesarios para mediciones y análisis. Las fuerzas de seguridad que necesitan controlar los correos electrónicos durante sus investigaciones, probablemente emplean un sniffer diseñado para capturar tráficos muy específicos. Sabiendo ya que los sniffers simplemente se apoderan de datos de la red, veremos a continuación cómo funcionan.

**Funcionamiento:**

Este programa le ordena a un computador, específicamente a su tarjeta de red (NIC), que deje de ignorar a todo el tráfico dirigido a otros equipos y preste atención a ellos. Para esto, se coloca a la NIC en un estado conocido como “modo promiscuo”, el cual no descarta los paquetes que no son para su dirección MAC, sino que los almacena y lee. Una vez que esto sucede, una máquina puede ver todos los datos transmitidos en ese segmento de red. El programa entonces comienza una lectura constante de toda la información que entra en el PC, a través de la tarjeta de red. Los datos que viajan por la red se presentan como paquetes o ráfagas de bits con formato para protocolos específicos. Debido a este formato estricto, un sniffer puede filtrar las capas de encapsulación y decodificar la información pertinente almacenada en el equipo de origen, equipo de destino, número previsto de puerto, capacidad de carga y, en pocas palabras, en cada pieza de información que se intercambia entre dos equipos.

Esto puede ser muy útil, y a la vez perjudicial, ya que puede usarse como un medio para robar información. Esta forma de operar se considera un “ataque pasivo”, ya que no altera el funcionamiento de la red.

**Usos:**

Los Sniffers son una herramienta útil a la hora de administrar y optimizar redes, ya que con estos puedes ver todos los paquetes en tránsito, sus IPs destino y origen, puertos, direcciones MAC (en algunos), etc. Con esto se puede detectar problemas en la red como loops, problemas de conectividad entre 2 ordenadores, exceso de tráfico y muchas otras cosas.

Pero todo esto tiene un precio, ya que es un arma de doble filo. Los Sniffers pueden ser usados por gente maliciosa e intervenir en una red y robar información como claves mal encriptadas.

Es una herramienta muy potente en manos de quien sabe usarla, por esto es que se crean muchos sistemas de seguridad como los antivirus y anti-spyware, pero también existen métodos de encriptación que cada vez son más avanzados y difíciles de descifrar, lo que dificulta la intervención en la red de estas personas mal intencionadas conocidas como Hackers.

Los sniffers funcionan bien en las redes no conmutadas, ya que en estas, todos los datos son enviados a la red y esta re-envía a todos, si el paquete no era para el pc, este lo descarta. Si implementamos un Sniffer en una red de este estilo, es fácil tener acceso a toda la información ya que basta que un pc tenga su tarjeta de red en “modo promiscuo” para que vea la información que se envía

En las redes de paquetes conmutados no es posible realizar lo anterior, ya que los paquetes enviados, solo los ven los receptores correspondientes y no toda la red. En este caso se emplea una técnica llamada Arp-spoofing, que envía paquetes falsos a la red. Esta técnica generalmente asocia la MAC del atacante con la IP de otro nodo, como por ejemplo, el Gateway. Cualquier dato dirigido a la IP del Gateway, será erróneamente re-dirigido al PC del atacante.

Algunos de estos programas son: Ethereal, Ksniffer, Dsniff, Kismet, Nessus, Sniffit, Cain & Abel, Wireshark, Snort, entre otros.

**Algunos Sniffers:**

Algunos sniffers trabajan sólo con paquetes de TCP/IP, pero hay otros más sofisticados que son capaces de trabajar con un número más amplio de protocolos e incluso en niveles más bajos tal como el de las tramas del Ethernet. Algunos de más utilizados son los siguientes:

**Wireshark** (antiguamente llamado Ethereal): utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

**Ettercap**: es un interceptor sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo, aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing.

**Kismet**: es un sniffer, un husmeador de paquetes, y un sistema de detección de intrusiones para redes inalámbricas 802.11 (Wifi). Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw, y puede rastrear tráfico 802.11b, 802.11a y 802.11g. El programa corre bajo Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X. Se puede operar en Windows, aunque la única fuente entrante de paquetes compatible es otra sonda.

**TCPDUMP:** es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

**Formas de Protegerse:**

Los Sniffers son difíciles de detectar, ya que al ser atacantes pasivos, dejan pocos rastros de su intromisión.

Una forma de identificarlos es ver si existe alguna tarjeta de red en modo promiscuo con la herramienta ifconfig nativa de Linux.

Uno de los métodos más eficaces es el uso de encriptación de los datos, que consiste en cifrar los datos bajo una serie de códigos que solo pueden ser leídos con una llave que solo posee el receptor. Este método es usado en la mayoría de las páginas web donde se requieren datos o contraseñas, ya que estas son de suma importancia y nadie más debe saberlas

También es posible defenderse de estos mismos, usando el mismo programa, ya que con este puedes saber que datos salen de tu pc y a donde van a parar. Si existe algún Sniffer en tu PC, con un mismo Sniffer lograras detectarlo y obtener su dirección IP y MAC para, posteriormente, bloquearlo.

Existen programas para detectar este tipo de intrusos, que utilizan ciertas técnicas para identificarlos y bloquearlos. Algunos de estos programas son: NEPED, Sniffdet, AntiSniff, Sentinel, entre otros.

**Conclusión**

Al investigar sobre estos programas, se puede apreciar de que son herramientas muy potentes al momento de analizar datos en una red, ya sea verificando errores como optimizándola. Pero al ser un programa tan poderoso, su uso puede ser desvirtuado y provocar mucho daño, como por ejemplo, el robo de contraseñas y lectura de mensajes privados. Por suerte, existen programas dedicados a detectar a estos usuarios maliciosos y así, proteger nuestra información para poder hacer uso de las redes de forma más confiable.  
 Estas herramientas permitirán seguir mejorando las redes en el futuro e incluso, quizás, se creen sniffers más avanzados, con más características que nos permitan obtener mayor información de una red, para así, poder realizar mejoras en estas mismas.

Pero al crear este tipo de herramientas, siempre surgen problemas a solucionar, y como siempre, se crearán formas de protección contra este tipo de ataques, quizás un nuevo tipo de encriptación, o programas de detección más avanzados.  
La tecnología avanza rápido, por eso hay que estar siempre actualizándose para poder hacer uso de ésta sin mayores complicaciones y no ser víctima de estafas o robos cibernéticos, ya que la tecnología está cada vez más integrada a nuestra vida diaria.

**Referencias**

**Informe anterior del tema:** <http://www.decom-uv.cl/~mferrand/cursos/redes/sniffers.pdf>

**Sniffers: What They Are and How to Protect Yourself:**

<http://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself>

**¿Qué es un Sniffer?:** <http://www.mundocisco.com/2009/08/que-es-un-sniffer.html>

**Si quieres profundizar más, consulta:**

<http://www.securityfocus.com/infocus/1549>

<http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm>

<http://es.wikipedia.org/wiki/Wireshark>

<http://es.wikipedia.org/wiki/Ettercap>

<http://es.wikipedia.org/wiki/Kismet>

<http://es.wikipedia.org/wiki/Tcpdump>