Sniffers

Nina Limachi Lisette Veronica
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas
NINA_LMCH_00@gmail.com

RESUMEN

Una de las principales preocupaciones del hombre es comunicarse, no importa cómo ni cuándo, pero el hecho de mantenerse comunicado a toda hora es sin duda una preocupación que agobia.

Las redes mantienen comunicados simultáneamente a una infinidad de usuarios de manera que se han convertido en una gran prioridad.

Sin duda la conectividad en red presenta diversas ventajas, sin embargo muchas veces el usuario no sabe que mediante la misma también se puede atentar contra la privacidad, como es el caso de los sniffers.

Los sniffers son un arma de doble filo, utilizados para la captura de información en la red (robo de información; como para mejorar la seguridad de las redes (ya que pueden monitorear el tráfico que producen los usuarios de una red).

Por esta razón se fueron desarrollando aplicaciones seguras que utilizan cifrado en la información para que ésta no viaje en texto claro por las redes y de esta manera evitar o retardar la obtención de la información, además de que se asegura de alguna forma la integridad de la misma.

Palabras Claves

Comunicación, Sniffer, Tráfico, Información, Modo Promiscuo, Red, Root .

1. INTRODUCCION

Bien se sabe que una contraseña poderosa, ya sea con más de 15 caracteres y mezclando números, letras, mayúsculas, minúsculas, caracteres fuera del alfabeto, entre otros, no es suficiente sino se cuenta con un buen esquema de seguridad, ya que existen varias formas de burlar estos y todo tipo de seguridad, incluso grandes organizaciones, como los bancos, pueden ser fácilmente interceptados, de manera que se pueda extraer información relevante para la empresa. Entre estos se encuentran los Sniffers que funcionan a nivel de red y son difíciles de detectar, pero no imposibles, es importante saber cómo funcionan para poder enfrentarse a ellos.

En el presente apartado se da un vistazo al funcionamiento de un Sniffer y como podría ser contrarrestado y detectado.

2. ¿QUE ES UN SNIFFER?

Un sniffer es un dispositivo o una aplicación que permite capturar los datos o información que pasan a través de una red, que no precisamente van dirigidos hacia él, por lo tanto es un tráfico de información al que no debería tener acceso.

3. ¿PORQUE SON PELIGROSOS?

Resulta bastante obvio suponer que los Sniffers presentan un riesgo de seguridad tanto en una sola maquina como en una red, debido a la facilidad con la que cuenta para poder capturar información.

Lamentablemente viaja por la red una cantidad innumerable de información confidencial sin contar con ningún tipo de cifrado, entre las que se pueden mencionar: contraseñas,correo confidencial, números de tarjetas de crédito, registros de bases de datos, cookies con información de autenticación, entre otros.

Es de vital importancia realizar una inspección de detección de Sniffers en la red no solo para detectar el daño que pueda causar, sino también para darse cuenta que los niveles de seguridad pueden ser violados y que se deben tomar medidas.

4. FUNCIONAMIENTO GENERAL DE UN SNIFFER

Para poder capturar el tráfico de la red a la que estamos conectados se debe colocar la tarjeta de red en “modo promiscuo”.

El modo promiscuo por definición consiste en que “todos los adaptadores de red reciben los paquetes que son para ellos, (filtran por IP), pero el colocar el adaptador de red en modo promiscuo hace que no filtre, y vea todo el tráfico que está en la red” [2].

El medio en el que un Sniffer es más efectivo es en una red LAN que maneje la topología tipo Bus; otro entorno de los Sniffers es una máquina víctima, en la que será necesario tener acceso a esa máquina para poder instalar el programa correspondiente, de manera que se pueda adquirir toda la información relacionada a las maquinas que habitualmente son accedidas desde esta máquina víctima (Ver Figura 1).

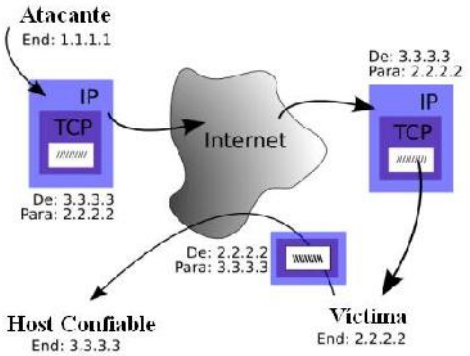

Figura 1. Sniffer en una Máquina Víctima

5. TRAFICO CAPTURADO

Para capturar tráfico hay que ser root (permiso de superusuario). Es poco seguro usar wireshark ("wireshark" es un Sniffer) como root, es preferible capturar con un programa distinto como los que se mencionan a continuación:

- Dumpcap. herramienta de captura derivada de wireshark
- tshark. wireshark en modo texto.
- aidump-ng. Para captura inalámbrica

6. CONCLUSIONES

La lucha contra los Sniffers es un tema de permanente actualidad, debido a que cada vez se desarrollan técnicas más sofisticadas para su detección y a su vez, casi al instante, se crean nuevos modelos de Sniffers que las burlan.

Es de primordial importancia que un administrador de seguridad conozca los programas que pueden ayudarle a detectar sniffers en sus redes, así mismo conocer las técnicas de evasión que un atacante puede utilizar para luchar contra ellos.

7. REFERENCIAS

[24] ¿Cómo Descubrir un Sniffer en la Red? [Disponible en:] http://www.opmsecurity.com/es/articles/contraespionaje-como-descubrir-un-sniffer-en-la-red.html [leído:] 5/04/13.

[25] Fernandez L. Desarrollo de un Analizador de Red. 2006. [Disponible en:] Sahttp://www.google.com.bo/url?q=http://openaccess.uoc.edu/webapps/o2/bitstream/10609/454/1/38443tfc.pdf&sa=U&ei=IrRRUdquF8-50QH4iIH4DA&ved=0CCQQFjAD&usg=AFQjCNF4EV5gn_e8DEXCz5c1alhH2c8z8g. [leído:] 17/04/13.

[26] Hernández J., Sierra J., Ribagorda A., Ramos B. Técnicas de Detección de Sniffers. 2000 [Disponible en:] http://www.google.com.bo/url?q=http://www.revistasic.com/revista42/pdf_42/SIC_42_agora.PDF&sa=U&ei=IrRRUdquF8-50QH4iIH4DA&ved=0CCcQFjAE&usg=AFQjCNFdedXEWYLN0mTJmD7wSTwpLhweKg [leído:] 10/04/13.

[27] Raise. Sniffers, que son y cómo funcionan. [Disponible en:] http://www.govannom.org/index.php/seguridad/16-sniffing/395-sniffers-que-son-y-como-funcionan [leído:] 6/04/13.

Sanders Ch. Sniffers. 2011. [Disponible en:] http://www.google.com.bo/url?q=http://gsyc.es/~mortuno/rom.2011.2012/sniffers.pdf&sa=U&ei=IrRRUdquF8-50QH4iIH4DA&ved=0CBoQFjAA&usg=AFQjCNFw7sQ_81g3Mj3YxrBMWTVosnLmHQ [leído:] 7/04/13