[[1]](#footnote-1)

**MIM: La inseguridad acechando**

L. F. Cruces Vidal*, Ingenieria de sistemas*

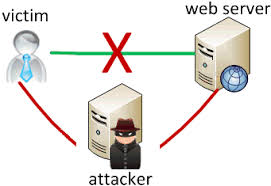
*J. Mejia Trujillo, Ingeniería de sistemas*

*J. D. Colina Echeverry, Ingeniería de sistemas*

***Resumen*— En la actualidad, cuando navegamos o nos comunicamos con otros hosts, estamos expuestos a ciertos tipos de ataques que usan diferentes métodos y técnicas. Man in the middle o Mim es una de ellas. Basada en esta técnica, se desarrollaron diferentes formas para acceder a los paquetes en una transferencia de información, privando la intimidad y privacidad de la comunicación entre hosts. Sin embargo, nunca es tarde para detener estos ataques, usando una metodología adecuada para frenarlos.**

***Abstract*--Currently, when we browse or communicate with other hosts, we are exposed to certain types of attacks that use different methods and techniques. Man in the middle or Mim is one of them. Based on this technique, different ways were developed to access the packets in an information transfer, depriving the privacy and privacy of the communication between hosts. However, it is never too late to stop these attacks, using an adequate methodology to stop them.**

Introducción

Cada vez es más frecuente sentirse más privado de la libertad y seguridad al navegar en la internet. Las vulnerabilidades de los sistemas junto con la astucia e ingenio de los atacantes, la evolución de los dispositivos, hace de las comunicaciones algo difícil de proteger. A lo largo de la historia y conforme llega el desarrollo y avances de la era informática, han aparecido técnicas que buscan vulnerar la

seguridad de las redes para acceder a cierta información y/o realizar la modificación de los recursos que se están transmitiendo para beneficio propio u otro fin. De esto se trata Man in the middle(Mim) o como lo indica su traducción “hombre en el medio”.

En el mundo de las comunicaciones informáticas, Mim se puede definir como una técnica, método o acción por la cual un atacante se coloca en medio de 2 host para capturar el tráfico y el intercambio de paquetes en esa comunicación. La información obtenida puede ser usada por el atacante de diferentes formas. Este tipo de técnicas cada vez se vuelve más comunes para hacer ataques malignos. Para ejemplificar cómo se puede emplear esa técnica, tenemos que contextualizar los siguientes conceptos que operan en la capa de enlace del modelo OSI:

Address Resolution Protocol o ARP es un protocolo que se encarga de encontrar la interfaz o dirección física que le pertenece a una dirección IP específica. También hay que hablar de ARP caché que corresponde a unas tablas en las cuales están mapeadas ciertas direcciones IP con su correspondiente dirección Mac.

Una vez entendido los anteriores conceptos, se puede hablar de un tipo particular de ataque: ARP poisoning o envenenamiento por ARP. Pero, ¿en qué consiste dicho ataque?

El atacante accede a la ARP caché de algún host para modificarla, de tal manera que introduzca una dirección IP falsa con una dirección Mac que no corresponde a ese host, sino al del atacante. De esta manera, cuando el host envía cualquier tipo de dato a otro host, el atacante tendrá acceso a ellos ya que estos paquetes son enviados a su dirección ethernet. Sin embargo, ¿es posible detectar ataques Man in the middle que utilicen ARP poisoning analizando paquetes del tráfico de red?

A continuación, se muestran los objetivos de esta investigación junto con la metodología empleada, los resultados y la conclusión.

1. Objetivos específicos

Con base en la temática del actual proyecto y la hipótesis planteada se seleccionaron algunos objetivos que posteriormente fueron clasificados como alcanzables y no alcanzables.

Por un lado, los objetivos alcanzables son aquellos que dentro del lapso de tiempo destinado para el desarrollo del proyecto y con los conocimientos que el equipo de trabajo poseía se consideraron posibles de realizar, tales objetivos son:

* Aplicar la packet-squirrel para realizar una captura de información. Esto es, utilizar una de las funcionalidades principales de la packet-squirrel para una captura de paquetes de tráfico de red.
* Recolectar muestras de tráfico de red de MiM.
* Analizar las variables del estudio contra una muestra de captura de paquetes o tráfico de red de MiM.
* Describir una metodología para análisis de ciberataques respecto a MiM.

Por otro lado, los objetivos no alcanzables se definieron como aquellos que por motivos de tiempo o de recursos (tanto tecnológicos como de conocimiento) no serían posibles de cumplir. Estos objetivos son:

* Desarrollar un algoritmo de extracción de las variables representativas.
* Implementar un sistema para detección de MiM.

1. Metodología

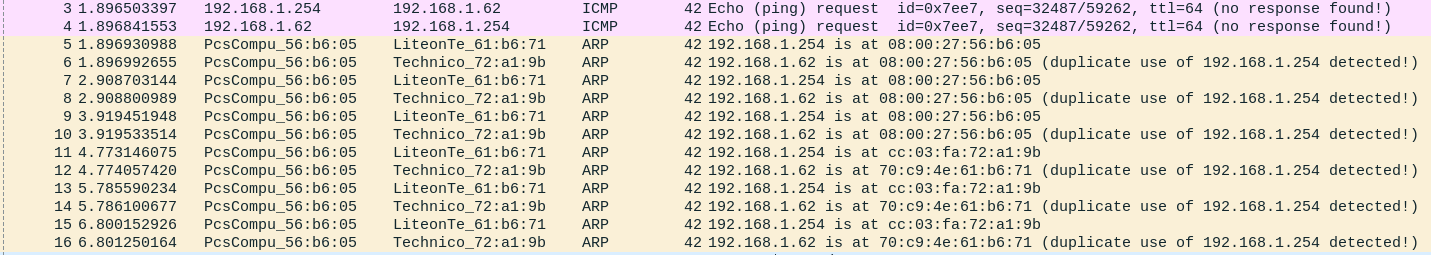
Detectar ese tipo de ataques puede ser complejo. Sin embargo, se desarrolló una posible metodología muy sencilla para detectar el ataque mim. Esta metodología está compuesta de 2 etapas simples que se componen a su vez de pasos para descubrir la actividad. La primera etapa consiste en detectar los hosts que actúan como enrutadores, es decir, aquellos que capturan los paquetes cuando son enviados a su destino, para luego reenviarlos al destino verdadero una vez capturados. Pero, ¿qué es lo que se envía? El primer paso consiste en enviar paquetes trampa usando el protocolo ICMP a todos los host involucrados en la red. Esto es hacer un broadcast o mensaje de difusión masiva de paquetes a través de la red. En el segundo paso de esta etapa, se tiene que contar con un programa que capture los paquetes y haga un análisis de la red para detectar aquellos hosts que habilitan enrutamiento de paquetes ip. Estos host se agruparán en una lista como posibles host malignos.

En la etapa 2, se analiza cada uno de los posibles host malignos utilizando la misma técnica de MIM para evaluar su tráfico. De esta manera se puede detectar si el host tiene acceso al intercambio de paquetes de otros hosts.

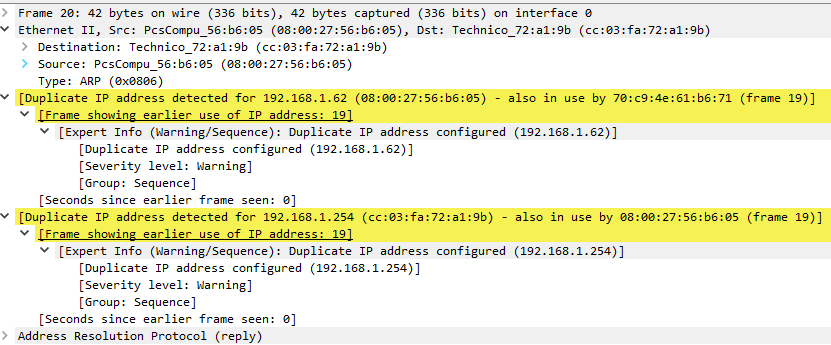
1. Resultados

Después de realizar la captura de tráfico de red del experimento ARP poisoning presentado en este trabajo, se continuó con la fase de análisis de dicha captura. Esta fase de análisis fue realizada considerando principalmente las variables que actúan en el ARP poisoning como son las direcciones IP, la dirección MAC, el protocolo ARP y protocolo ICMP. Además, de esta fase de análisis se obtuvieron los siguientes resultados.

La captura del experimento relevo diversas anomalías con respecto al intercambio de paquetes entre el hots usado como víctima y el enrutador. Estas anomalías toman forma en la captura de tráfico de red como dos direcciones MAC asociadas a la misma dirección IP del host víctima, y son representadas por la alerta “(duplicate use of 192.168.1.254 detected)”. La figura 1 representa algunas de estas anomalías.

Fig. 2 Captura de tráfico de red

Al observar individualmente estas anomalías se encontró que la dirección MAC 70:c9:4e:61:71 que aparece en la captura de tráfico de red pertenece al host víctima, el cual es quien realiza las solicitudes de salida a internet por medio del enrutador y la dirección IP 192.168.1.62. Por otro lado, se observa que la otra dirección MAC 08:00:27:56:b6:05 pertenece al host que fue utilizado para realizar el ataque de ARP Poising. Y, además dicha dirección MAC también está asociada a la dirección IP 192.168.1.62. La figura 2 muestra el resultado en detalle de una de estas anomalías.

Fig. 3 Análisis detallado de un paquete de datos.

Otro punto importante observado en la captura es la posición de las direcciones MAC. Esto es importante porque representa el inicio y fin del ARP poisoning; pues en algunas anomalías la dirección MAC del host que realiza el ataque está entre paréntesis y la dirección MAC del host víctima se muestra después del anuncio “also is use by”. A su vez, hay otras anomalías en las cuales pasa todo lo contrario; la dirección MAC del host víctima está entre paréntesis y la dirección MAC del host que realiza el ataque se muestra después del mismo anuncio.

1. Conclusiones y trabajos futuros

Considerando la sección IV, y teniendo en cuenta que para obtener dichos resultados se utilizaron capturas de tráfico de red por medio de la herramienta WireShark; es posible afirmar que gracias a las capturas de tráfico de red se puede detectar el ataque Man in the Middle. Lo anterior está respaldado por el hecho de una IP con dos direcciones MAC asociadas a ella implica que los hosts correspondientes a esas direcciones MAC, tendrán acceso a el intercambio de paquetes que se realice por medio de la ya mencionada dirección IP.

También se puede concluir que los ataques de ARP poisoning tienen la característica de que una vez finalizado el ataque las direcciones MAC regresan a su estado inicial. Es decir, la dirección MAC del host que realiza el ataque no seguirá asociada a la dirección IP del host víctima. Por ende, el host víctima volverá a tener únicamente su dirección MAC correspondiente, y esto disminuye la probabilidad de que el ataque sea detectado.

Además, se puede decir que la captura de tráfico de red facilita la detección de ataque Man in the Middle. Pues, en la captura saltan alarmas indicando que una dirección IP tiene asociada dos direcciones MAC. Sin mencionar que, dependiendo de la herramienta utilizada se podrá observar específicamente cuales son las direcciones MAC, y distinguir cual de ella está realizando el ataque.

Referencias

1. G. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” *Phil. Trans. Roy. Soc. London,* vol. A247, pp. 529-551, April 1955.
2. J. Clerk Maxwell, *A Treatise on Electricity and Magnetism,* 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
3. I.S. Jacobs and C.P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
4. K. Elissa, “Title of paper if known,” no puplicado.
5. R. Nicole, “Title of paper with only first word capitalized,” *J. Name Stand. Abbrev.,* en impresión.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” *IEEE Transl. J. Magn. Japan*, vol. 2, pp. 740-741, August 1987 [*Digests 9th Annual Conf. Magnetics Japan,* p. 301, 1982].
7. M. Young, *The Technical Writer’s Handbook.* Mill Valley, CA: University Science, 1989.

1. Fig. 1, tomada de: http://www.martinezmartinez.eu/wp-content/uploads/2013/11/min.png [↑](#footnote-ref-1)