Descripción del Problema de Envenenamiento al Protocolo ARP, Mediante Árboles de Ataque

Chiang, Luis; Abad, Cristina Ms.Sc.
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral
Campus Gustavo Galindo, Km 30.5 vía Perimetral,
Apartado 09-01-5863. Guayaquil-Ecuador
{lchiang,cabad}@fiec.espol.edu.ec

Resumen

El problema del envenenamiento ARP es un problema grave, que compromete la confidencialidad de los datos en nuestras redes de área local. Este problema hasta el momento no tiene una solución ideal. Parte de la razón por la que no se ha podido encontrar una buena solución al problema, es la dificultad de apreciar el alcance del mismo y de enumerar todas las posibles maneras de llevar a cabo este ataque. Los árboles de ataque muestran información de manera ordenada y rápida de comprender. Esta trabajo demuestra diferentes métodos para envenenar la caché ARP de diferentes sistemas operativos, implementados en una herramienta automatizada de pruebas de envenenamiento ARP. A partir de estos resultados se generó árboles de ataque del protocolo ARP de cada sistema. Estos árboles representan un aporte a la comunidad de seguridad informática ya que constituyen un recurso que no existía anteriormente, y además, facilita la evaluación de posibles soluciones al mencionado problema.

Palabras Claves: *protocolo, ARP, switch, árbol de ataque, trama, paquete, dirección MAC, dirección IP, broadcast, Windows 2000 SP4, Windows XP SP3, PCBSD 7.0, MAC OSX 10.5.*

Abstract

The ARP poisoning problem is very serious, as it compromises data confidentiality in local networks. This problem has no ideal solution so far. An important cause of the lack of solution for this problem is the difficulty to study the real length of the problem and to enumerate all the possible ways of completing an attack. The attack trees show information in an organized way, ideal for quick understanding. This work shows different methods to poison ARP's cache under different operating systems. These methods were implemented with an automated testing tool for ARP poisoning. The results obtained from these research were used to build attack trees, which represent a useful resource to the information security community, as they offer before unavailable information. Furthermore, it makes the evaluation if possible solutions for the above mentioned problem an easier task.

1. Introducción

ARP (Address Resolution Protocol), protocolo utilizado en redes Ethernet, sirve para obtener la dirección física de un computador (MAC Address) de la red preguntando a toda la red mediante un mensaje broadcast por el propietario de la dirección IP. Quien tiene esa dirección IP responde directamente a quien hizo la solicitud.

El protocolo ARP es un protocolo sin estado, y no tiene información de cuáles fueron las solicitudes realizadas, ni las respuestas anteriores, cada respuesta nueva sobre escribe a la anterior en la tabla cache ARP.

El funcionamiento estándar de ARP está documentado en el RFC 806 [1], pero pequeños detalles de implementación del protocolo dependen del sistema operativo, los cuales pueden agregar algunos mecanismos sencillos de seguridad.

El problema de los ataques a este protocolo radican en que la respuesta no puede ser autenticada y alguien más que no sea el autentico dueño de esa IP puede enviar una respuesta falsa y hacerse pasar por otra computadora. Para una mayor eficiencia, la asociación IP-MAC recibida en la respuesta ARP se almacena por un cierto tiempo en la tabla cache ARP. En el caso de darse un ataque como el descrito, se dice que la tabla cache del host fue “envenenada”. De esta manera quien hace la solicitud inicial no se comunicara con el computador correcto si no con el falso y le enviara la información que era para el destinatario original.

Un agravante de este problema es que no es necesario ser un hacker experto para montar este tipo de ataques, ya que hay herramientas que uno puede bajarse de Internet para realizarlos. El problema del envenenamiento ARP es un problema grave, que compromete la confidencialidad de los datos enviados en nuestras redes de área local (y desde ahí, hacia Internet), y que hasta el momento no tiene una solución ideal.

Para lograr analiza el problema del protocolo ARP se desarrolló una aplicación que ataque a la pila del protocolo ARP de un sistema para saber si el sistema fue vulnerable los ataques. Esta aplicación permitirá seleccionar cuales pruebas efectuar, los datos con cuales

realizar el ataque, configurar los estados del sistema atacado, entre otras opciones. A partir de las vulnerabilidades encontradas, se creará árboles de ataque, que es una manera estructurada y ordenada de analizar la falla de seguridad.

2. Diseño

Para poder crear estos árboles hemos armado una red de pruebas aislada en la que nuestros experimentos no comprometan la seguridad de otros usuarios. En seguridades, a este tipo de experimentos se los llama experimentos en cajas de arena (sandboxes) como se muestra en la **Figura 1**.

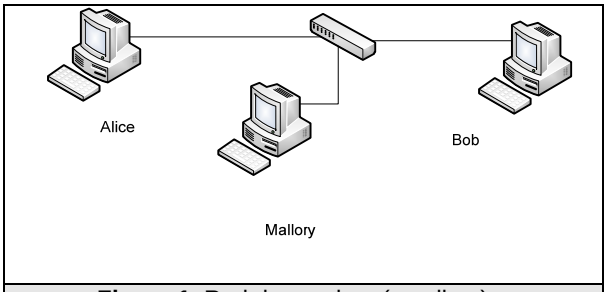

Figura 1. Red de pruebas (sandbox).

El principal objetivo es analizar el comportamiento de la caché ARP en los sistemas operativos: Windows 2000 SP4, Windows XP SP3, PCBSD 7.0, MAC OSX 10.5. Para encontrar sus vulnerabilidades y con esta información construir los árboles de ataque.

La idea básica del mecanismo de evaluar la caché ARP, para realizar árboles de ataque consiste en una máquina atacante trate de envenenar la caché ARP de la otra máquina llamada atacada mediante varias pruebas, y cuando haya terminado una prueba obtener los resultados y pasar a la siguiente.

Además la manera de conocer si una caché se encuentra envenenada es que no se encuentre la relación <MAC, IP> correcta dentro de la caché. Para desarrollar estas pruebas se asume que el sistema operativo usa la caché ARP para cuando necesita enviar paquetes a los otros equipos de la red y los protocolos de comunicación están bien implementados en forma de capas que no permiten que otras capas que no sea la de enlace de datos manipulen las direcciones MAC de destino de los paquetes generados por el sistema operativo y por lo tanto sean otras direcciones de las que están en la caché ARP.

Para que la máquina atacante pueda saber si la caché de la máquina atacada se encuentra envenenada, se usó un mecanismo de comunicación entre ellas que sea independiente de la interfaz de red que está siendo atacada, para por medio de este avisar si el ataque fue exitoso o no. Este mecanismo no debe sufrir de saturación, o algún otro problema relacionado al ataque afectando el funcionamiento de las pruebas, para que por medio de este comunicar información pertinente del ataque.

2.1. Descripción de un árbol de ataque

Un árbol de ataque es una representación formal con la cual se puede sistematizar un grupo de ataques hacia un sistema específico [2]. Los árboles de ataque, como todo árbol, poseen una estructura multi-niveles y constan de nodos padres, nodos hijos y una raíz. La raíz de un árbol de ataque representa el ataque que se quiere llegar a realizar y cada nodo de este representa las condiciones que deben cumplirse o acciones que deben de hacerse para poder lograr el ataque. Es decir que cada nodo hijo representa la condición que se debe de realizar para que su nodo padre se cumpla y una vez que se llegue a la raíz de dicho árbol se ha completado todo el ataque.

Si al final de recorrer todo el árbol de ataques y ninguna ruta permite llegar hasta la raíz del árbol que especifica el ataque a realizar, entonces no se puede realizar ese ataque y se considera un ataque fallido. Es importante mencionar que lo nodos de los árboles de ataque usualmente son colocados a partir de un proceso analítico, el cual no asegura que un árbol sea un herramienta de seguridad perfecta pero si lo bastante ordenada y clara para tener un buen análisis.

3. Implementación

Para la implementación del sistema se divide básicamente entre dos partes la implementación del atacante y la implementación del atacado.

Las funciones de la aplicación atacante es probar sucesivamente ataques, permitir personalizarlos y obtener los resultados de los ataques. El atacante maneja varias opciones las cuales son pasadas al atacado para que trabaje conjuntamente. Primero se deben configurar varios parámetros para realizar las pruebas o ataques. El atacante le informa al atacado cuando inicia un ataque y cuando lo termina, bajo qué condiciones desea realizar las pruebas o sea utilizando entradas estáticas, dinámicas o no usar entradas en la caché, y se encuentra constantemente monitoreando si el atacante le informa que el ataque fue exitoso. Al final muestra el resultado de los ataques en formato XML.

El atacado espera los parámetros del atacante, cuando el atacante le informa que debe utilizar entradas dinámicas o estáticas en su caché el atacando utiliza los parámetros que son ingresados por pantalla en la máquina atacada. Mientras se realiza el ataque constantemente revisa la tabla ARP para ver si se da la condición de envenenamiento y en el caso que se dé envía un mensaje mediante el puerto serial para informar que fue exitosa esa prueba.

3.1. Los ataques realizados

Se implementaron diferentes tipos de ataques para realizar las pruebas. Estos ataques fueron el fruto del análisis y de investigación de ataques al protocolo ARP con el fin de abarcar la mayor cantidad de

probabilidades para así obtener un árbol lo más completo posible, sin dejar abierta la posibilidad de un nuevo y diferente ataque al protocolo ARP.

Estos ataques tal y como aparecen en la aplicación del atacante fueron:

1) Enviar ARP-Response hasta n.- Este ataque consiste en enviar mensajes ARP-Response con la información del envenenador al atacado. Este mensaje es muy conocido como el ARP Gratuito. Usualmente este ataque logra su objetivo debido a que el equipo atacado no tiene implementados mecanismos de estados y hace cambios en la caché con información nueva.

2) Enviar ARP-Broadcast hasta n.- Los mensajes broadcast en ARP los envía un equipo que quiere conocer la dirección de red de una IP, lo envía a la red pero existe una falla que al hacer el broadcast también en ese paquete ARP se puede poner información falsa, y una mala implementación del protocolo por parte del atacado puede hacer que aprenda la relación <MAC, IP> a partir de esas solicitudes.

3) Esperar ARP-Broadcast, luego enviar ARP-Response hasta n.- Este ataque tiene mucho parecido a un ataque de hombre en el medio. Lo que hace este ataque es husmear el tráfico de la red y cuando detecta que en la red un equipo está solicitando la MAC de la IP del equipo que se desea interceptar comienza a enviar paquetes para tratar de ganarle en responder al equipo interceptado que el también enviara una respuesta al atacado, de esta manera se presiona al atacado en decidir cual respuesta tomar, si la que llega primero, o la mas repetitiva, o cualquiera que sea la implementación del protocolo en esos casos.

4) Enviar ICMP EcoRequest falso, luego esperar ARP-Broadcast, y enviar ARP-Response hasta n.- Sistemas que tienen mejores implementaciones del protocolo ARP, tienen más cuidado en los mensajes ARP no solicitados y los rechazan. Pero se puede forzar al equipo a hacer una solicitud ARP, por ejemplo mediante una respuesta a un ICMP EcoRequest (más conocido como ping), para que el equipo atacado al no tener la información MAC de quien envía el ping utilice el protocolo ARP para obtenerla, o la interprete del paquete recibido. Este ataque está enfocado en que el equipo hace una solicitud ARP por la dirección IP de la cual no se conoce la MAC y ahí es cuando se espera a que el atacado haga un ARP-Broadcast preguntando por el interceptado y la máquina atacante envía paquetes ARP con la información del envenenador.

5) Enviar ICMP EcoRequest falso, luego NO esperar ARP-Broadcast, y enviar ARP-Response hasta n.- Este ataque es muy similar que el anterior solo que no tiene que esperar del ARP-Broadcast para así en el caso que el atacado envié una solicitud ARP-Broadcast se le adelanta al interceptado que espera recibir la solicitud para generar el paquete y enviarlo por la red.

6) Enviar ICMP EcoResponse falso, hasta n.- Esta prueba trata de probar si el equipo atacado no aprende la relación <MAC, IP> a partir de las respuestas ICMP que algún otro equipo le pueda estar enviando, en este caso el atacante envía con información del envenenador paquetes ICMP EcoResponse, que son también conocidos como la respuesta a los ping que puede hace una máquina cuando recibe una solicitud.

7) Enviar ICMP EcoRequest falso, hasta n.- Esta prueba se basa en la prueba anterior, la única diferencia es que el paquete enviado por el atacante ya no es un ICMP EcoResponse sino un ICMP EcoRequest, también conocido como ping.

A partir de los resultados obtenidos de las pruebas, variando los estados de la caché del atacante y de la cantidad de paquetes enviados en cada ataques, se crearon los árboles ataque que tratan de representar todo el universo conocido hasta el momento.

4. Pruebas y resultados

Después de analizar las pruebas y el alcance de ellas, se prosiguió a crear un árbol muy general donde estén mostradas todas las combinaciones de envenenamiento a una caché ARP, para solo marcar las hojas que son vulnerables a un ataque y detectar si se puede llegar a cumplir la raíz del árbol. Se colocó de color verde a las hojas o acciones que son vulnerables a ataques a la caché ARP y de color rojo a las que no, para una mejor apreciación del árbol.

El objetivo de estos árboles de ataque es envenenar la caché del atacado, por tal motivo es el nodo raíz del árbol. En los árboles se colocó que se debe conocer las relaciones <MAC, IP> del equipo que quiere ser atacado y del suplantado, también colocando una rama que se cumple si alguien tiene acceso físico a al equipo atacado y agrega entradas estáticas.

Los árboles de ataque obtenidos a partir de las evaluaciones son: Figura 2: Árbol de ataque ARP en Windows 2000 SP 4, Figura 3: Árbol de ataque ARP en Windows XP SP 3, Figura 4: Árbol de ataque ARP en Fedora 8, Figura 5: Árbol de ataque ARP en PCBSD 7.0, Figura 5: Árbol de ataque ARP en MAC OSX 10.5.5

5. Caminos críticos de los árboles

La intención de los caminos críticos, es mostrar cuales son las condiciones de mayor relevancia en el momento de enfrentar un ataque que pueda comprometer la seguridad del sistema si llega hasta la raíz del árbol.

A continuación se describe desde los caminos más comunes encontrados en los árboles, hasta los caminos más particulares.

El camino más crítico fue el encontrado a partir de la prueba “Enviar ICMP EcoRequest falso, luego NO esperar ARP-Broadcast, y enviar ARP-Response hasta n” este camino hace vulnerable a casi todos los sistemas, Fedora 8 es el único que no es vulnerable. Y su peligrosidad es aún mayor debido a que hace el cambio de entradas que ya se encuentran en la caché ingresadas de manera dinámica que es la manera más común con la cual trabajan la mayoría de las redes y a la vez genera mayor costo tratar de resolverlo.

Cuando la caché ARP del atacado se encuentra vacía es cuando el atacante tiene mayor probabilidad de cumplir su objetivo, debido a que el equipo está predispuesto a aprender la MAC de las IP que no conoce. Esto se puede ver en cuatro de los árboles, del cual el único que tiene una pequeña protección es Windows XP que no acepta ARP-Response cuando no las ha solicitado.

Los siguientes ataques más efectivos son ARP-Response y ARP-Broadcast, pero cuando ya existe una entrada en la caché y por medio de muchos mensajes el equipo atacado acepta el cambio falso en la caché ARP. El único sistema que no fue afectado por este mecanismo de ataque fue Fedora 8.

Los árboles de PCBSD y MAC OS X son iguales, debido a que descienden de BSD y su implementación en el protocolo muy poco ha cambiado, lo que se puede apreciar es que PCBSD es más rápido de vulnerar ante un ataque que MAC OSX.

6. Conclusiones

Se logró implementar correctamente una aplicación que permite evaluar diferentes posibles soluciones al protocolo ARP, y que funciona en diferentes sistemas operativos y con facilidad de portarlo a otros sistemas.

Como resultado de los análisis se logro conocer los árboles de ataque al protocolo ARP de sistemas operativos representativos de la actualidad. Estos resultados pueden ser usados como base para la investigación de futuras posibles soluciones permitiendo conocer cuáles son los aspectos que afectan a la caché ARP.

Al conocer los árboles de ataque, se tiene información valiosa sobre qué tan vulnerable es un sistema a los ataques efectuados, qué tan rápida es su convergencia y una pequeña comparación que sirve como factor de decisión en el momento de seleccionar el sistema operativo a utilizar.

Debido a que ninguna implementación del protocolo ARP logró evadir todos los ataques, esto muestra la complejidad del problema aún no solucionado por los fabricantes de sistemas operativos, y el requerimiento de un mayor esfuerzo por parte de los administradores de red de proteger la privacidad de sus usuarios.

7. Agradecimientos

Este trabajo ha sido posible gracias al financiamiento del programa VLIR-ESPOL [3] y a la donación de equipos de la FIEC. Especialmente gracias al apoyo y orientación de la Ing. Cristina Abad.

8. Referencias

[1] “RFC 826”, <http://www.ietf.org/rfc/rfc826.txt> [Consulta: Viernes, 20 de febrero de 2009].

[2] Bruce Scheneier “Attack Trees” <http://www.schneier.com/paper-attacktrees-ddj-ft.html> [Consulta: Viernes, 20 de febrero de 2009]

[3] “Proyecto VLIR – Espol”, <http://www.vlir.espol.edu.ec> [Consulta: Viernes, 20 de febrero de 2009]

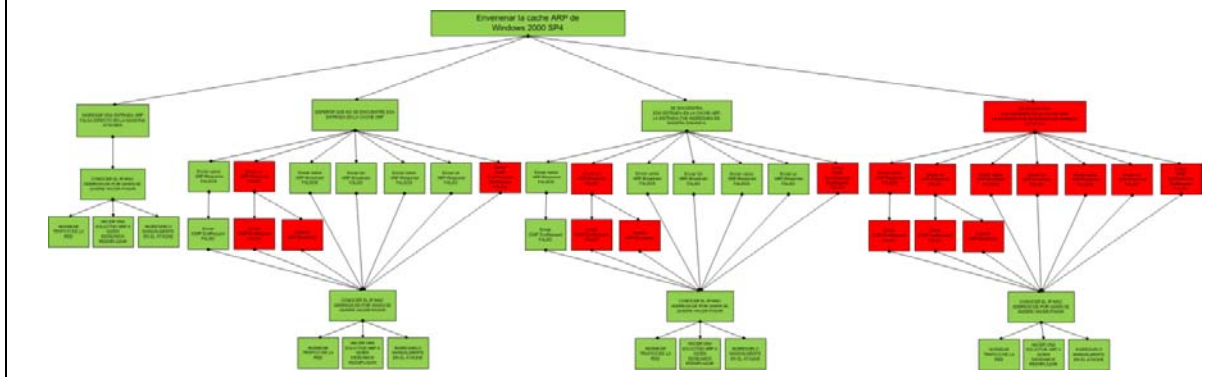

Figura 2. Árbol de ataque ARP en Windows 2000 SP 4.

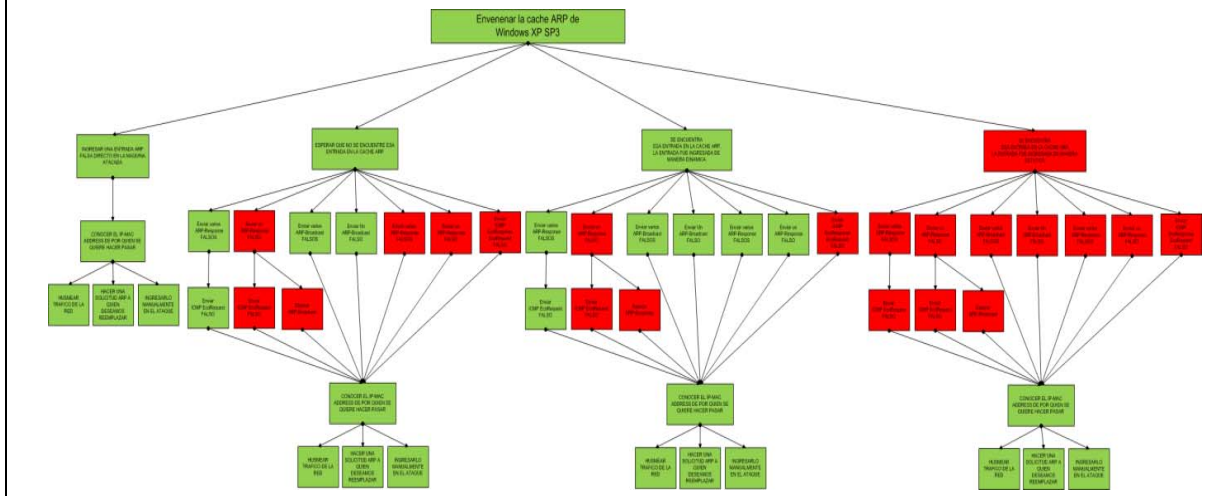

Figura 3. Árbol de ataque ARP en Windows XP SP 3.

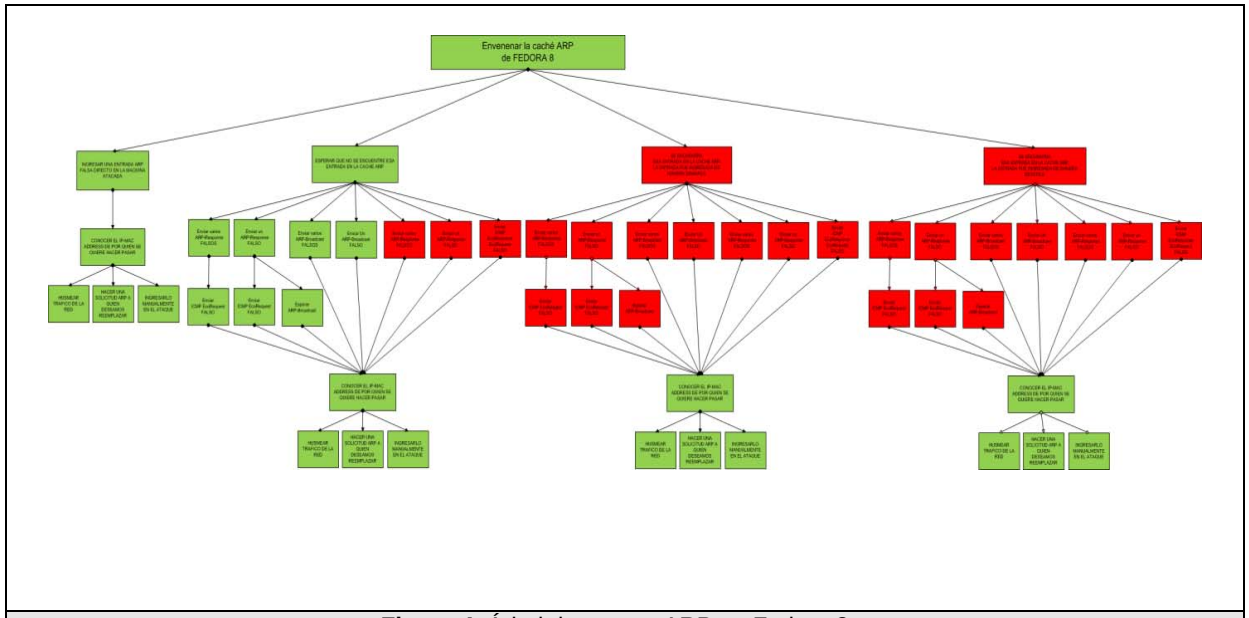

Figura 4. Árbol de ataque ARP en Fedora 8.

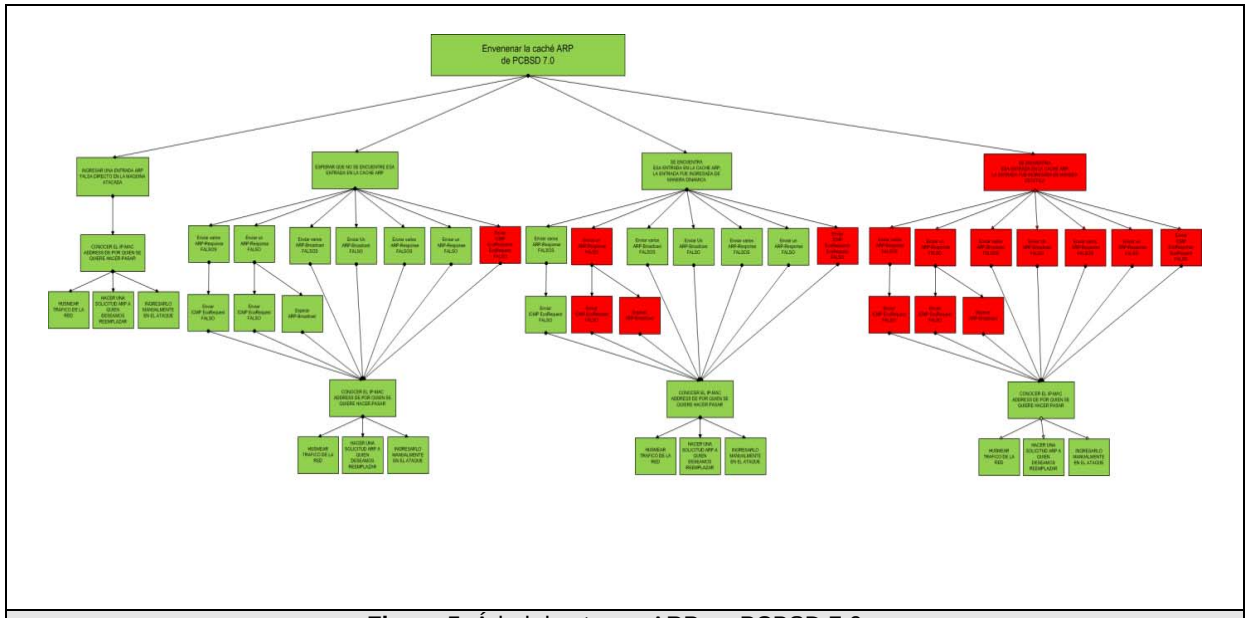

Figura 5. Árbol de ataque ARP en PCBSD 7.0.

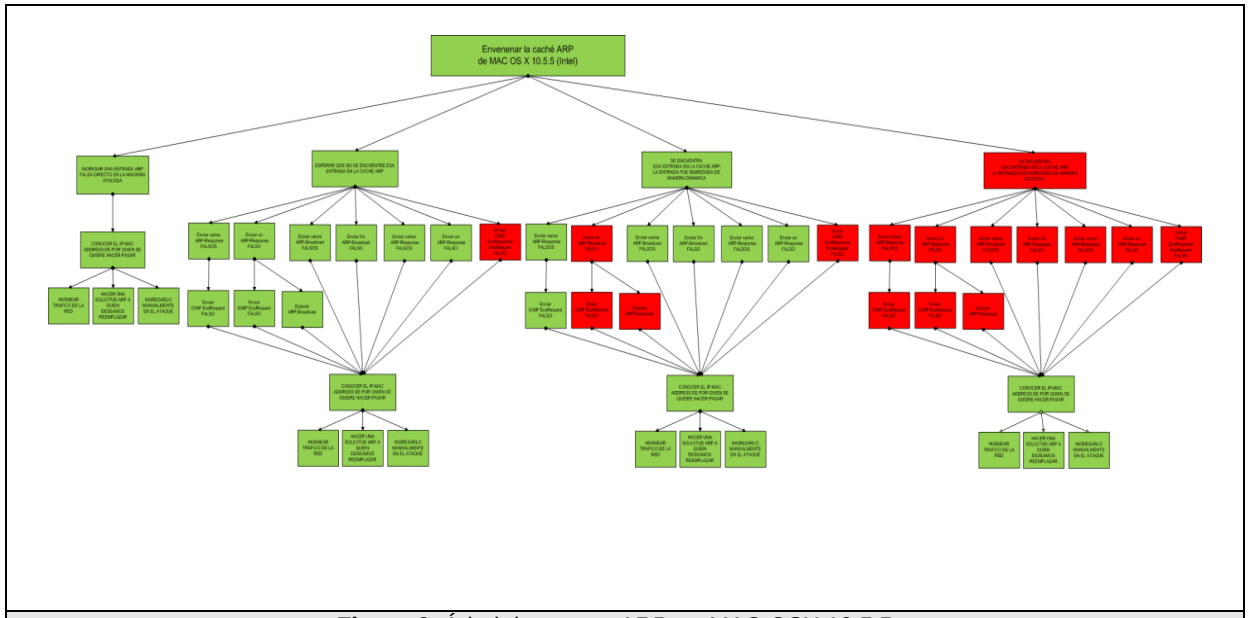

Figura 6. Árbol de ataque ARP en MAC OSX 10.5.5.