http://revistas.udistrital.edu.co/ojs/index.php/REDES/index

# Alternativas de solución al envenenamiento del Protocolo ARP en entornos LAN

## Alternative solutions to Poisoning the ARP protocol in LAN environments

Oscar Leonardo Cely Granados[1]
Octavio José Salcedo Parra[2]
Jorge E. Salamanca Céspedes[3]



**Resumen**

En el presente artículo se presentan algunos fallos de seguridad del protocolo ARP reflejando su vulnerabilidad a diversos tipos de ataques dando lugar a fugas y/o daños de información, se han presentado diversas soluciones factibles en las cuales se encuentran S-ARP (secure ARP), ES-ARP (Secure and efficient ARP) y como alternativa de solución planteamos la creación de algoritmos que permitan detectar y mitigar ataques mediante el uso de Registros Estáticos en la Tabla ARP, como objetivo queremos resolver algunos fallos en la seguridad de ARP cambiando y mejorando los protocolos originales de este realizando las configuraciones que se creen factibles para mejorar su seguridad, en este artículo se realizará un envenenamiento ARP utilizando las herramientas VMware y GNS3 que nos permiten virtualizar un entorno real con el fin de mostrar la inseguridad que posee el protocolo ARP y así mismo implementar una alternativa económica y eficiente que mejore su seguridad.

**Palabras clave:** fallos de seguridad, Registros Estáticos, envenenamiento ARP, alternativa económica y eficiente.

**Abstract**

The following article represents certain weakness in the safety of the Protocol ARP which leaves a door open to information failures. Therefore, some solutions such as S-ARP (Secure ARP), ES-ARP (Secure and efficient ARP) have been considered, including as an alternative, the creation of algorithms which are able to detect and reduce attacks through the use of static records in the ARP table.

The main goal is address serious shortcomings and weaknesses in the ARP security, changing and improving the original protocols through the necessary settings.

In the following article, the protocol ARP will be poisoned; using resources such as VMware and GNS3 we will be able to visualize a real environment in order to demonstrate the insecurity that belongs to the Protocol to the protocol ARP as well as the introductions of an efficient and economical alternative capable to improve it's security.

**Keywords:** S-ARP (Secure ARP), ES-ARP (Secure and efficient ARP), interaction, economical and efficient alternative.

1 ing.oscar.dba@gmail.com
2 osalcedop@udistrital.edu.co
3 jsalamanca@udistrital.edu.co

## Introducción

Address Resolution Protocol (ARP) parece un protocolo sencillo, aunque los detalles que este presenta hacen que este se complique. "Muchas implementaciones no interpretan la especificación del protocolo y otras suministran enlaces incorrectos debido a que eliminan el tiempo de espera de la cache en un intento de mejorar la eficiencia" *(comer, 2000)*.

Podemos decir que el protocolo ARP funciona principalmente en tres partes, la primera que devuelve un enlace que es empleado por la interfaz de red para encapsular y transmitir el paquete, la segunda un módulo que maneja los paquetes ARP que llegan de la red y actualizan la cache ARP agregando nuevos enlaces, y por último un administrador que implementa la política de sustitución de cache que examina las entradas en la cache y las elimina cuando alcanzan un determinado tiempo. Cuando una respuesta ARP es solicitada, esta se puede cambiar (dirección MAC), por una falsa, y atacando así el sistema, esto se llama envenenamiento ARP. Derivado al envenenamiento se han buscado alternativas que vuelvan el protocolo seguro, una de ellas es S-ARP está basado en una extensión del protocolo ARP y se introduce un conjunto de funcionalidades que permiten una comprobación de autenticidad y la integridad del contenido de las respuestas ARP, usando criptografía asimétrica. También existe ES-ARP que se guía principalmente por el mayor problema de ARP que es el hecho de que esta es totalmente confiable, ya que no diferencia entre los mensajes recibidos y confía en que haya recibido respuestas a ciegas, ya que es un protocolo sin estado y no lleva ninguna información con respecto a las solicitudes que envía o las respuestas que recibe, este "bucle" es aprovechado por los atacantes para enviar respuestas falsificadas para que sean aceptadas por la ARP y terminen envenenado la caché ARP. Estos dos protocolos todavía no han sido implementados, ya que ambos consideran costos sumamente altos ya sean en software como ES-ARP, que al enviar dos mensajes de confirmación de los paquetes de datos, hace que este método de autentificación sea más lento de lo normal, lo que hace que la eficiencia disminuya, de otro lado la implementación de S-ARP, es mucho más cara, si se lleva a cabo en una red con muchos hosts.

## Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) es un protocolo sin estado, es decir, una respuesta puede ser procesada a pesar de que la solicitud correspondiente nunca fue recibida, cuando se recibe una respuesta, se actualiza la entrada correspondiente en la memoria cache, con la dirección lógica IP, y la dirección física MAC en la respuesta. Un ARP es un mensaje enviado por un host que solicita la dirección MAC de su propia dirección IP, esta se envía de una maquina a otra con la misma o diferente red. ARP reside en la capa de red de la suite TCP/IP, donde un host se identifica por su dirección IP de 32 bits, y por la dirección MAC que sigue un esquema de 49 bits.

Cuando la capa de red recibe un mensaje de las capas superiores se comprueba la dirección IP de la máquina de destino. Si la máquina de destino está en la misma red local que el de la maquina fuente, el mensaje puede ser enviado directamente a la máquina de destino, pero por el contrario si no está en una red local el mensaje tiene que ser encaminado a través de un router. Para enviar el mensaje directamente a la máquina de destino, la capa de red necesita saber la dirección MAC de la máquina de destino. ARP asigna dinámicamente la dirección IP de 32 bits de una máquina a su dirección MAC de 48 bits en un espacio de memoria temporal denominada caché ARP. Existen dos tipos de mensajes ARP que pueden ser enviados por el protocolo ARP, uno es solicitud ARP y otro es respuesta ARP.

**Solicitud ARP:** cuando se hace la solicitud ARP mediante un host, se enmarca la dirección IP, dirección MAC, tipo de mensaje ARP y la dirección IP de destino. Donde esta petición se difunde a todos los hosts de la misma LAN que el envío de acogida, el campo de la dirección MAC de destino se deja en blanco para el host con la dirección IP de destino para rellenarla.

**Respuesta ARP:** cuando un host recibe la solicitud ARP que contiene la dirección IP, como la dirección IP de destino, se llena con dirección MAC y el campo de operación se establece en el código de operación de la respuesta ARP, este mensaje es enviado directamente a la maquina solicitante. Cuando la respuesta ARP es recibida por la maquina solicitante actualiza su cache ARP con la dirección MAC solicitada.

| ARP | ES-ARP |
|---|---|
| 1. Mzáquina A desea enviar un paquete a D, pero A sólo conoce la dirección IP de D. | 1. máquina A desea enviar un paquete a D, pero A sólo conoce la dirección IP de D. |
| 2. Máquina A difunde ARP Solicitud con la dirección IP de D. | 2. Máquina A difunde ARP Solicitud con la dirección IP de D. |
| 3. Todas las máquinas de la red local recibe la solicitud ARP que se emite. | 3. Todas las máquinas de la red local reciben la solicitud ARP que se transmitió y actualizan su caché ARP con la dirección MAC de A. |

| | |
|---|---|
| 4. Máquina D responde con su dirección MAC unicast de ARP respuesta y actualiza su caché ARP con la MAC de A. | 4. Máquina D responde con su dirección MAC mediante la difusión de respuesta ARP. |
| 5. Máquina A agrega la dirección MAC de D a su caché ARP. | 5. Todas las máquinas añaden la dirección MAC de D a su caché ARP. |
| 6. Ahora la Máquina A puede ofrecer paquetes directamente a D. | 6. Ahora la Máquina A puede ofrecer paquetes directamente a D. |

Tabla 1: procedimientos de solicitud y respuesta de ARP Y ES-ARP. Fuente Autores.

Al forjar una respuesta ARP, un atacante puede cambiar fácilmente la asociación mantenida en la memoria cache ARP de acogida, es decir, puede cambiar la dirección MAC por una falsa(respuesta falsa) enviando mensajes IP encapsulados con esta dirección falsa. De esta manera el atacante podrá recibir todos los marcos originalmente dirigidos a otro host. Una vez los hosts estén envenenados, estos enviaran todo el tráfico al host atacante que podrá leerlos, y si este decide reenviarlos de vuelta los hosts atacados no detectaran que están siendo atacados. Este es un ataque MITM (man in the middle). Otro ataque a esta red es el DoS (denial of service) y es cuando el atacante no reenvía los mensajes después de leerlos, a la máquina de destino y esto se denomina ataque de negación de servicio.



## ES-ARP

ES-ARP se guía principalmente por el mayor problema de ARP que es el hecho de que esta es totalmente confiada, ya que no diferencia entre los mensajes recibidos y confía en que haya recibido respuestas a ciegas, debido a que es un protocolo sin estado y no lleva ninguna información con respecto a las solicitudes que envía o las respuestas que recibe, este "bucle" es aprovechado por los atacantes para enviar respuestas falsificadas para que sean aceptadas por ARP y terminen envenenado la caché ARP.

Así que ES-ARP implementa un método de tal manera que la "respuesta ARP y la solicitud ARP es transmitida, y va almacenando la información de la trama de solicitud en la cache ARP. En este protocolo todos los hosts excepto el host de origen almacenarán las entradas en la caché ARP" *(Md. Atullah, N. Chauhan)*. En la tabla 1 podemos observar los pasos de solicitud y respuesta de ARP y ES-ARP, la cual nos muestra algunas diferencias que se tuvieron en ES-ARP para mejorar la seguridad de los datos que se envían en ARP, como hacer que todas las máquinas de la red local reciban la solicitud ARP que se transmitió y actualizar inmediatamente su cache ARP con la dirección MAC del dispositivo de origen, para comprobarla en su cache ARP y comprobar si la entrada de host de destino esta presento o no, lo que hace que de una vez se guarde la dirección MAC y no permite que la falsifiquen impidiendo así que puedan envenenar la ARP, y esta logre ser más segura, ya que solo la fuente de acogida aceptara la respuesta, de lo contrario será simplemente descartar la trama de respuesta ARP. Este procedimiento actualiza la memoria cache ARP dos veces, es decir, la primera vez que se emite la petición ARP donde se almacenará la IP y la MAC del host de origen, y la segunda vez cuando Respuesta ARP se emite o sea la IP y la MAC del host de destino se almacenaran.

## S-ARP

S-ARP está basado en una extensión del protocolo ARP y se introduce un conjunto de funcionalidades que permiten una comprobación de autenticidad y la integridad del contenido de las respuestas ARP, usando criptografía asimétrica. Además también sigue las mismas especificaciones de ARP, para que sea compatible con esta y solo se inserta un encabezado final de los mensajes estándar de protocolo para llevar la información de autentificación, ósea que S-ARP no aceptara mensajes no autenticados (a menos de que se encuentren en una lista de hosts conocidos). S-ARP lleva en la respuesta ARP un encabezado S-ARP, y las solicitudes ARP no cambian. El encabezado S-ARP contiene la firma digital del remitente, una marca de tiempo, el tipo y la longitud del mensaje, el mensaje se autentifica buscando la dirección IP del remitente y su clave pública correspondiente en su anillo (ya que cada host mantiene un anillo de claves públicas y las direcciones IP correspondientes previamente solicitadas por las AKD (Authorizedkeydealer), si la entrada utiliza el contenido para verificar la firma, de lo contrario, envía una petición a la AKD para la certificación. Una petición al AKD se envía también en caso de que la clave en el anillo local no verifique la firma, puesto que ya no puede ser válida. En este caso, el paquete en cola es una "lista respuestas pendientes". El AKD envía una respuesta firmada con la clave pública solicitada y la corriente de sello de tiempo. Al recibir la respuesta de la AKD, el anfitrión sincroniza el reloj local con el sello de tiempo, si es necesario, almacena la clave pública en su anillo y verifica la firma. En caso de que la clave antigua ya no sea válida, si la nueva clave recibida de la AKD es la misma que la que está en la memoria caché, la respuesta se considera no válida y se deja caer. Si la clave ha cambiado de hecho, el host actualiza su caché y verifica la firma con la nueva clave.

## Arquitectura de red

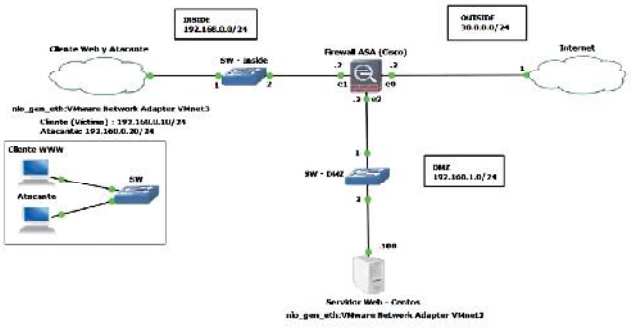


Figura 1. Arquitectura básica de una de red LAN.
Fuente Autores.

## Metodología

En la figura 1, se muestra una arquitectura básica de un entorno de producción, la red está dividida en tres segmentos un segmento INSIDE donde están dos máquinas virtuales una es el host del cliente que utilizara un sistema operativo CENTOS y el host del atacante que estará en una máquina virtual KALI LINUX, ambos conectados a un Switch y al adaptador VMnet3 de VMware, tanto el cliente web como el atacante están conectados a un Switch al que llamamos SW-Inside. Tenemos un segundo segmento al que llamamos DMZ donde encontramos un servidor web con CENTOS y el servidor APACHE 2 este hace uso del adaptador VMnet2 de VMware y conectado al Switch SW-DMZ que será expuesto hacia otras redes y por ultimo nuestro tercer segmento OUTSIDE que se conecta a redes externas, en este caso internet.

En el centro de la arquitectura encontramos un firewall, para la implementación de este firewall usamos la herramienta GNS3 la cual nos permite cargar y configurar la imagen de diferentes equipos de conectividad que encontramos en el mercado con todas sus propiedades y características, cabe resaltar que esta herramienta consume gran cantidad de recursos del equipo anfitrión pero como beneficio obtenemos un equipo de conectividad real con todas sus funciones.

Con base en esta arquitectura de red, la cual virtualiza un entorno real interceptaremos desde el host atacante la comunicación que se establece entre el cliente y el servidor web poniendo en evidencia fallas en la seguridad del protocolo ARP. Posteriormente se implementará un algoritmo de mitigación que genera un registro estático que impida el envenenamiento de ARP.

## Implementación

1. Utilizando la herramienta VMware montamos y configuramos la ISO de nuestra máquina virtual cliente (Centos), atacante (Kali Linux) y servidor web (Centos, apache2) con sus respectivas direcciones IP y direcciones Mac, configuramos nuestro Firewall (Router ASA-Cisco) con GNS3 al igual que los Switch y los Host que interactúan en nuestra red de tal manera que nuestra configuración final sea la mostrada en la figura 1.

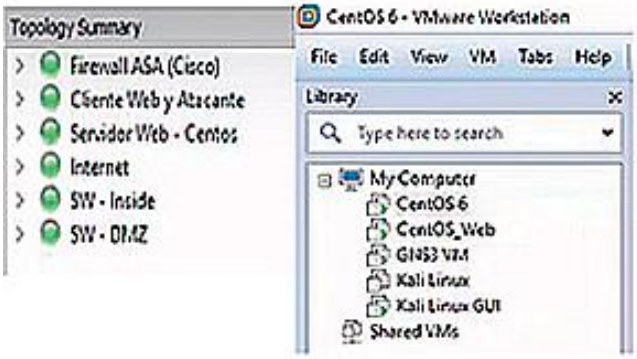


Figura 2. Componentes de Red en GNS3 y VMware necesarios para el ejercicio. Fuente Autores.

2.En nuestra máquina virtual atacante (Kali Linux) se instalará una herramienta llamada Bettercap la cual permite realizar ataques de tipo ARP SPOOF es decir que al realizar el ataque podremos observar todo el tráfico que se genera entre el servidor web y el cliente. Dado que hemos configurado un servidor web apache en el cual se alojaran un conjunto de páginas web cuando.

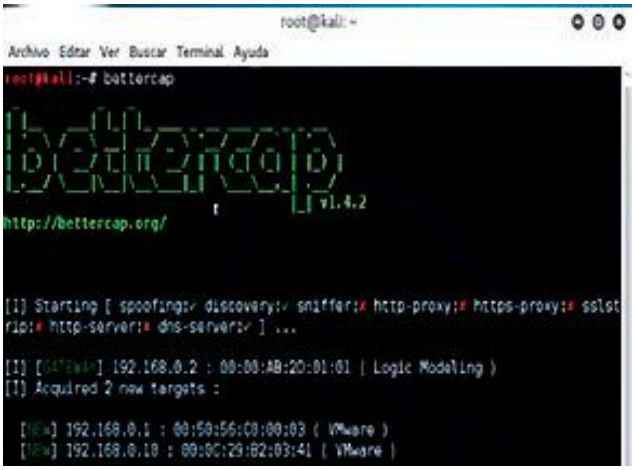


Figura 3 Herramienta Bettercap. Fuente Autores.

El cliente haga una petición al servidor web este le presentara las páginas web alojadas en él.

3. Si en nuestra terminal Linux se ejecuta únicamente el comando bettercap este empezará a capturar todo el tráfico que exista en la red, ahora dadas las condiciones se va a filtrar nuestro ataque especificando que capture solo el tráfico de tipo http que se está generando por el puerto 80 entre la dirección IP del cliente 192.168.0.10 y el servidor web y que lo guarde en un directorio al que se llamará trafico.pcap, para eso ejecutamos la siguiente sentencia:

```
root@kali:~# bettercap --sniffer -sniffer-pcap=trafico.pcap -sniffer-filter "tcp and dts port 80" -T 192.168.0.10
```

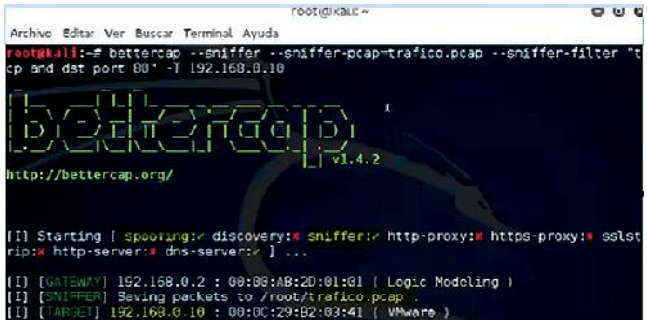


Figura 4. Ejecución del bettercap especificando nuestra victima. Fuente Autores



Como se refleja en la figura 4 vemos que al ejecutar la sentencia se activa el modo spoofing el modo sniffer y el modo dns-server. Lo primero que la aplicación realiza es capturar el Gateway de la red segundo el Sniffer guarda los paquetes que viajan por la red en el archivo trafico.pcap y por último el target confirma el cliente que vamos a atacar.

En este estado la aplicación ya realizo el ataque de tipo ARP SPOOF, es decir ya duplico la dirección MAC para que todo el tráfico que cruce entre el cliente y el servidor se replique hacia el atacante. Para el cliente un ataque de tipo ARP SPOOF es transparente a diferencia de un ataque de denegación de servicio en donde se puede ver claramente que los recursos empiezan a consumirse rápidamente, en pocas palabras el ataque tuvo éxito y en el cliente todo sigue funcionando normalmente.

## Detección de ataques Arp Spoof

Detección Manual. Para esto se puede abrir la consola del cliente con la sentencia arp–n, se abre la tabla ARP y se puede observar que existe una dirección duplicada, la del Gatway y la del atacante, y cómo se puede observar ambas tienen la misma dirección MAC, con esto todo el tráfico que devuelve el servidor se replica tanto al cliente como al atacante. Es un método que a pesar de ser bastante efectivo para ver si estamos sometidos a un ataque ARP SPOOF no sería lo óptimo ya que tendríamos que estar ejecutando el comando arp –n con regularidad.

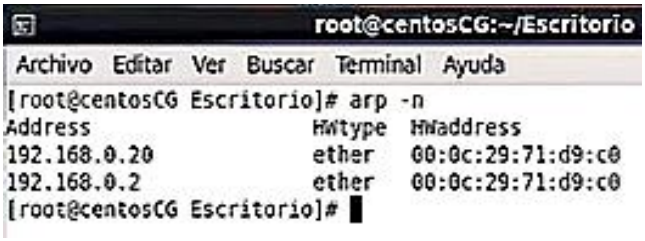


Figura 5. Tabla ARP Fuente Autores

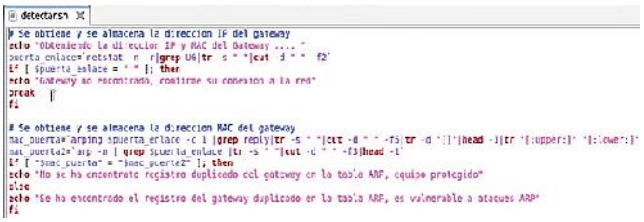

Figura 6. Algoritmo Detectar.sh (Código libre). Fuente Autores.

Detección Automática mediante la ejecución del algoritmo detectar.sh. El algoritmo primero obtiene tanto la dirección IP del Gatway como de la puerta de enlace, para esto se usa el comando netstat el cual arroja la tabla de enrutamiento y allí el algoritmo identifica la dirección IP del Gateway y la selecciona si no encuentra nada arroja un mensaje que pide que confirme su conexión de red. Luego con el comando aprping obtenemos la dirección MAC asociada a la dirección ip del Gatway que obtuvimos en el paso anterior. Por último el algoritmo verifica si existe duplicidad de esos registros en la tabla ARP, si existe arroja el mensaje de alerta diciéndome que el registro del Gatway esta duplicado por lo tanto se encuentra sometido a un ataque ARP SPOOF y si no está duplicado el equipo está protegido.

## Mitigación como alternativa de solución al envenenamiento del protocolo ARP

Esta práctica de seguridad tiene como objetivo evitar que terceros tengan acceso a la información que viaja en el trafico establecido en una comunicación, para esto se desarrolló un script en Linux basado en el principio de creación de registros estáticos en la tabla ARP. Cuando se crea un registro estático lo que se hace es especificar quien va a ser nuestro Gatway y a pesar de que se creen nuevos registros para engañar al cliente la información siempre va a ir únicamente al Gatway del cliente.

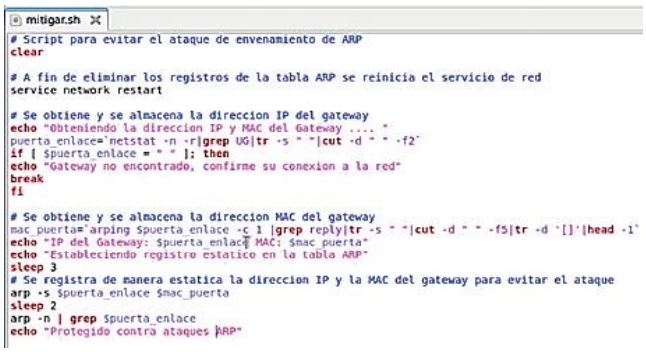


Figura 7. Algoritmo Mitigar.sh Fuente Autores (Código libre)

El algoritmo se basa en el anterior descrito algoritmo de detección es decir inicia obteniendo tanto la dirección ip de la puerta de enlace como la MAC de la puerta de enlace y simplemente lo que hace es tomar esas dos variables y ejecutar el comando arp -s que establece registros estáticos y como variables asigna la dirección ip de la puerta de enlace y la dirección Mac. Con ello crearemos el registro estático y evitaremos los ataques de ARP SPOOF


Figura 8. Ejecución del algoritmo mitigar.sh. Fuente Autores

El algoritmo de mitigación reinicia la interfaz de red para borrar la tabla ARP obtiene la dirección IP y la Mac del Gatway establece un registro estático y da como salida la creación de este registro en la figura 8 podemos ver que al ejecutar arp –n se ha eliminado la duplicidad del registro y que solamente aparece la dirección del cliente y una Flags Mask tipo CM lo que significa que es un registro manual, por ultimo nos arroja un mensaje informándonos que estamos protegidos contra ataques ARP.

## Otras alternativas de seguridad a los ataques ARP

Hay diferentes maneras de hacer más seguro el protocolo ARP, además de los citados anteriormente, existen múltiples programas como la herramienta "ArpON (Arp handler inspectiON) es una herramienta que permite manipular algunos aspectos del protocolo ARP. Una de sus cualidades destacadas es hacer que el protocolo ARP sea más seguro. Implementa dos técnicas de defensa contra ataques de envenenamiento ARP (ARP spoofing):

SARPI "Static Arp Inspection": Static ARP inspection, Redes sin DHCP, utiliza una lista estática de entradas y no permite modificaciones se asemeja al registro estático.

DARPI "Dynamic Arp Inspection": Dynamic ARP inspection, Redes con DHCP, controla peticiones ARP entrantes y salientes, guarda las salientes y fija un timeout para la respuesta entrante.

Además de detectar y bloquear ataques derivados más complejos del estilo de DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking y SSL/TLS Hijacking, está pensado para funcionar como Daemon, y actualmente está adaptado para sistemas GNU/Linux, Mac OS X, FreeBSD, NetBSD y OpenBSD" (GLOBALIP S.A.C, 2011)

## Evaluación

ES-ARP funciona de tal manera que la "respuesta ARP y la solicitud ARP es transmitida, y va almacenando la información de la trama de solicitud en la cache ARP. Lo que hace que el rendimiento no disminuya. S-ARP funciona con criptografía asimétrica lo que significa que usa una par de claves para el envío de mensajes (una clave pública y otra privada del mismo host), lo que hace que el tiempo de ejecución está dominado por la verificación de la firma y generación de firmas, este tiempo de verificación depende de la longitud de la clave. La creación de la firma lleva mucho tiempo debido al cálculo exponencial pero se puede mejorar calculando todo por separado, pero aun así no mejora significativamente el rendimiento. La implementación de Mitigación como alternativa de solución es bastante efectiva y económica en entornos pequeños pues en una red con bastantes hosts su configuración puede ser bastante dispendiosa y demorada. La defensa de ES-ARP contra el envenenamiento es mediante el almacenamiento de la información en la trama de solicitud ARP, lo que reduce las posibilidades de los distintos tipos de ataques. La retransmisión de la respuesta de la trama ARP proporciona seguridad contra el envenenamiento de caché ARP, como si cualquier atacante enviara una falsa respuesta ARP, entonces esta respuesta también recibida por el anfitrión objetivo, cuya dirección IP se utiliza para mapear la dirección MAC del atacante. Así que este host detecta que esta respuesta ARP sea falsa por el atacante. En cambio S-ARP y Mitigación utilizan entradas estáticas en la cache ARP, estas no se pueden actualizar y solo pueden cambiarse

manualmente por el administrador del sistema, nuevamente no es viable para redes con cientos de hosts porque las entradas se deben introducir de manera manual en cada host. Otra opción de seguridad sugerida de S-ARP es la seguridad de puerto que es una característica presente en muchos switches modernos que permite que el conmutador reconoce solo una dirección MAC en un puerto físico, aun no es una protección eficaz contra el envenenamiento ARP, ya que si al atacante no falsifica su propia dirección MAC, puede envenenar la cache de las dos víctimas sin dejar que el switch interfiera en el proceso

## Conclusión

Si se desea implementar alguna de las opciones de seguridad que se expusieron en este artículo debemos saber para qué tipo de redes podemos adaptarlas ya que por ejemplo los métodos S-ARP y Mitigación serian tediosos de implementar en una red con cientos de hosts, ya que las entradas se deben introducir manualmente en cada host, en cambio en ES-ARP esta característica no se adopta y es similar a la de ARP. ES-ARP tiene un mejor rendimiento lo que la hace más eficiente.



Las tres soluciones tienen un problema, si la respuesta ARP envenenada se envía antes de la real y se pone en la memoria caché, la victima almacena la respuesta equivocada en la cache y descarta la real. Cuando se envía la primera solicitud ARP, la víctima y el atacante reciben el mensaje. El primero que llegue se pondrá en la cache ARP de la víctima. Además, el atacante también podría suplantar un mensaje de solicitud de eco ICMP y enviar inmediatamente después de que una respuesta ARP falsa. Cuando la víctima recibe la solicitud de eco ICMP, realiza una petición ARP, pero la respuesta falsa ya está en la cola del paquete recibido, por lo que la acepta una.

Si se instala un Antídoto, el host puede suplantar la dirección MAC del remitente y forzar una serie para prohibir otro host.

## De los autores

**Jorge Enrique Salmanca Céspedes:** Ingeniero Electrónico – Universidad Distrital Francisco José de Caldas – Colombia. Especialista en telecomunicaciones móviles y Magister en teleinformática Universidad Distrital Francisco José de Caldas, Estudiante Doctorado en educación, DIE Universidad Distrital Francisco José de Caldas. Docente de planta asociado, adscrito al proyecto curricular de Ingeniería Electrónica, Facultad de ingeniería Universidad Distrital Francisco José de Caldas. jsalamanca@udistrital.edu.co, y adicional a esto.

**Ing. Octavio José Salcedo Parra.** PhD. Doctor en Estudios Políticos – Universidad Externado de Colombia. Doctor en Ingeniería Informática - Universidad Pontificia de Salamanca, Campus de Madrid. DEA Universidad Pontificia de Salamanca, Campus de Madrid. Magister en Economía - Universidad de los Andes. Magister en Teleinformática - Universidad Distrital "Francisco José de Caldas". Ingeniero de Sistemas – Universidad Autónoma de Colombia. Profesor de Planta, Universidad Distrital "Francisco José de Caldas" - Bogotá D.C. Profesor de Planta, Universidad Nacional de Colombia, sede Bogotá D.C. Investigador Senior Colciencias. Director Grupo de Investigación "Internet Inteligente", Clasificado Colciencias A.

## Referencias

[1] Md. Atullah, N. Chauhan, ES-ARP: an Efficient and Secure Address Resolution Protocol, SCEECS 2012.

[2] D. Bruschi, A. Ornagui,E. Rosti S-ARP: a Secure Address Resolution Protocol, ACSAC 200).

[3] D.Comer, D.Stevens interconectividad de redes con TCP/IP vol 11

[4] F. Gutiérrez, laboratorio virtualizado de seguridad informática con Kali Linux.

[5] GLOBALIP S.A.C., "ArpOn" - Un buen aliado contra los ataques AR. 2011. Activo 1 de diciembre de 2014.

http://globalip.blogspot.com/2011/05/arpon-un-buen-aliado-contra-los-ataques.html

[6] Dug Song, "ARP Spoof", http://arpspoof.sourceforge.net.

[7] Peter Burkholder, "SSL Man-in-the-Middle Attacks", www.sans.org/reading_room/whitepapers/threats/480.php.

[8] Thawatchai Chomsiri, "Sniffing Packets on LAN without ARPSpoofing", 11-13 Nov.008.