REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 15. No. 1, enero-abril, 2016, p.62-68 ISSN 1729-3804

DETECCIÓN Y MITIGACIÓN DE ATAQUES ARP EN LA RED CORPORATIVA DE LA DIVISIÓN TERRITORIAL HOLGUÍN, ETECSA.

Dinella Aguilera González, Manuel E. Gutiérrez Pérez,Lester Pérez Bernal

ETECSA, Cuba, Martí 122 Esq. Mártires, Holguín CP 80100
email: dinella.aguilera@etecsa.cu

RESUMEN

El protocolo de resolución de direcciones (ARP) es responsable de convertir las direcciones IP a direcciones de red físicas. Una vulnerabilidad de este protocolo radica en la ausencia de autenticación. La suplantación mediante el protocolo ARP es una técnica "antigua" y aún efectiva hoy día si no se interponen los controles adecuados. Existen varias herramientas de código abierto que permiten ejecutar este tipo de ataque sin necesidad de conocimientos de informática avanzados. Su ejecución afecta gravemente la confidencialidad de la información en la red corporativa, el atacante puede capturar todo el tráfico saliente y entrante (contraseñas, correos electrónicos, mensajería instantánea, etc.) Este trabajo tiene como objetivo la evaluación de la ubicación de controles en la red que permitan detectar la ocurrencia de estos ataques así como implantar medidas que mitiguen la severidad de su ocurrencia.

PALABRAS CLAVE: Protocolo ARP, mitm (man-in-the-middle), redes.

ABSTRACT

The Address Resolution Protocol (ARP) is responsible for translating the IP addresses to physical network addresses. A vulnerability of this protocol is the absence of authentication. ARP spoofing is an "old" technique and yet effective today if proper controls are not stand. There are several free tools to execute such an attack without advanced computer skills. This execution seriously affects the confidentiality of information on the network, the attacker can capture all incoming and outgoing traffic (passwords, email, instant messaging, etc.) This study aims to evaluate the location of controls on a network to detect the occurrence of these attacks and implement measures to mitigate its severity.

KEYWORDS: ARP Protocol, mitm (man-in-the-middle), networks.

INTRODUCCIÓN

El protocolo de resolución de direcciones (ARP) es el responsable de convertir las direcciones IP a direcciones de red físicas. Las especificaciones de ARP en RFC 826 sólo describen su funcionalidad, no su implementación, que depende en gran medida del manejador de dispositivo para el tipo de red correspondiente, que suele estar codificado en el microcódigo del adaptador[1] [2].

Cada equipo conectado a la red tiene un número de identificación de 48 bits. Éste es un número único establecido en la fábrica en el momento de fabricación de la tarjeta. Para que las direcciones físicas se puedan conectar con las direcciones lógicas, el protocolo ARP interroga a los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché. Cuando un equipo debe comunicarse con otro, consulta la tabla de búsqueda. Si la dirección requerida no se encuentra en la tabla, el protocolo ARP envía una solicitud a la red. Todos los equipos en la red comparan esta dirección lógica con la suya. Si alguno de ellos se identifica con esta dirección, el equipo responderá al ARP, que almacenará el par de direcciones en la tabla de búsqueda y a continuación podrá establecerse la comunicación [3]. Si no lo encuentra, descarta el paquete y genera un broadcast de red para una solicitud ARP [1].

La tabla ARP se mantiene dinámicamente. Existen dos maneras en las que un dispositivo puede reunir direcciones MAC. Una es monitorear el tráfico que se produce en el segmento de la red local. A medida que un nodo recibe tramas de los medios, puede registrar las direcciones IP y MAC de origen como mapeos en la tabla ARP. A medida que las tramas se transmiten en la red, el dispositivo completa la tabla ARP con los pares de direcciones. Un dispositivo también puede obtener pares de direcciones mediante el envío de una solicitud de ARP [4] [2].

Las entradas en la tabla ARP tienen una marca de hora similar a la de las entradas de la tabla MAC en los switches. Si un dispositivo no recibe una trama de un dispositivo determinado antes de que caduque la marca horaria, la entrada para ese dispositivo se elimina de la tabla ARP [4]. Además, pueden ingresarse entradas estáticas de asignaciones, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP no caducan con el tiempo y deben eliminarse en forma manual.

El principal problema de seguridad de este protocolo es la ausencia de autenticación. Una máquina modificará su comportamiento acorde con los paquetes ARP recibidos, sin poder determinar de ningún modo la autenticidad de los mismos; y las cachés pueden estar sujetas a alteraciones externas. Es posible modificar los contenidos de una caché ARP tan sólo con construir y enviar una petición o respuesta adecuada. Con la técnica de ARP gratuito, una máquina puede actualizar las cachés ARP del resto en cualquier momento.

La suplantación mediante el protocolo ARP es una técnica “antigua”, pero sigue siendo efectiva hoy día si no se interponen los controles adecuados. Existen varias herramientas libres que permiten ejecutar este tipo de ataque sin necesidad de conocimientos de informática avanzados. Este tipo de ataque modifica el flujo de datos enviado desde la víctima hacia la pasarela (gateway) haciendo un ataque de tipo Hombre en el medio (MITM), de esta forma consigue que este tráfico pase a través de la máquina atacante sin que la víctima se percate de ello.

Su ejecución afecta gravemente la confidencialidad de la información en la red corporativa, el atacante puede capturar todo el tráfico saliente y entrante, esto incluye contraseñas, correos electrónicos, mensajería instantánea y la operatividad de la red puede verse comprometida si por ejemplo el ataque no es detenido y se suprime el equipo atacante, pues todas las cachés ARP continúan envenenadas y el tráfico no logra llegar al router.

Este trabajo tiene como objetivo proponer mecanismos que garanticen la detección y mitigación de ataques de suplantación a partir del protocolo ARP en la red corporativa.

CONTENIDO

ARP utiliza una caché que consiste en una tabla que almacena las asignaciones entre nivel de enlace de datos y las direcciones IP del nivel de red. Para reducir el número de peticiones ARP, cada sistema operativo que implementa el protocolo ARP mantiene una caché en la memoria RAM de todas las recientes asignaciones [5].

Envenenamiento a la caché ARP (ARP Spoofing)

El envenenamiento de tablas ARP, es una técnica de hacking usada para infiltrarse en una red, con el objetivo de husmear los paquetes que pasan por la LAN, modificar el tráfico o incluso provocar una denegación de servicio (DoS). Mediante este tipo de ataques, se puede obtener información sensible de una víctima que esté en la misma red que el atacante, como nombres de usuario, contraseñas, cookies, mensajes de correo, mensajería instantánea, conversaciones VoIP, etcétera.

La cahé ARP se encuentra envenenada cuando las relaciones MAC-IP no contienen valores correctos. Esto puede ocurrir de 2 formas:

- No inducido
- Inducido

En el caso de los no inducidos pueden ser provocados por las asignaciones de direcciones IP de un servidor DHCP y el tiempo de actualización de la caché ARP o cuando la red maneja direcciones IP estáticas y se asigna el mismo IP a varias máquinas [6].

El envenenamiento inducido consiste básicamente en inundar la red con paquetes ARP indicando que la nuestra es la MAC asociada a la IP de nuestra víctima y que nuestra MAC está también asociada a la IP del router de nuestra red. De este modo, todas las máquinas actualizarán sus tablas con esta nueva información maliciosa. Así cada vez que alguien quiera enviar un paquete a través del router, ese paquete no será recogido por el router, sino por nuestra máquina, pues se dirige a nuestra dirección MAC, y cada vez que el router u otra máquina envíe un paquete a nuestra víctima sucederá lo mismo. Como nuestra máquina sabe que “está haciendo trampas” no se autoenvenenará y sí conocerá las MACs reales de todas sus víctimas, por lo que la podremos configurar para que reenvíe esos paquetes a su verdadero destinatario [7].

Herramientas para hacer un Ataque ARP

Existen múltiples herramientas que permiten ejecutar un envenenamiento ARP sin grandes complicaciones.

- Cain y Abel
- Arpspoof
- Ettercap
- Arpoison

El modo de uso es sencillo y consiste básicamente en los pasos mencionados anteriormente. En una prueba realizada con la herramienta Ettercap, fue posible realizar el envenenamiento ARP y capturar más de 50 usuarios y contraseñas de correo electrónico y aplicaciones. En muchos casos las contraseñas de los usuarios coincidían para varios sistemas, lo que hace aún más sensible el tráfico capturado.

Durante la ejecución del ataque, no existían las condiciones idóneas para que las herramientas ubicadas como mecanismos de detección y/o protección funcionaran adecuadamente. El Antivirus Kaspersky detectó el escaneo y bloqueó la IP atacante por 2 horas, sin embargo el ClamAV instalado en las estaciones con Linux no detectó el ataque, por lo que un segmento sustancial de la red quedó desprotegido.

Mecanismos de detección ante un ataque ARP

Arpwatch: Es una herramienta que permite el monitoreo del tráfico de red en busca de paquetes ARP y registra los cambios existentes en la relación MAC-IP. Una vez detectado el cambio envía una alerta que puede ser configurable a través de interfaz gráfica o mediante correo electrónico.

Snort: Es un sistema basado en la detección de intrusos, sin embargo, contiene reglas que pueden configurarse de forma tal que se convierta además en un sistema de detección de ataques ARP a pesar de que estos ocurren en la capa 2 del modelo OSI. Sus preprocesadores pueden ser configurados para que cada ARP_REQUEST sea analizado a partir de la dirección de origen de la trama ETHERNET sea igual a la dirección de origen del paquete ARP [8][9]. Por tanto es capaz de detectar y alertar sobre un ataque ARP, aunque debe ser refinado en el tiempo para evitar los falsos positivos.

ARPGuard: Analiza de forma constante el tráfico de red. Controla y protege cada uno de los elementos de red, de forma tal que solo los dispositivos autorizados pueden tener acceso mientras que los desconocidos son tratados según directivas de la organización. Protege además contra ataques en la Capa 2 de tipo MITM [10].

Política de defensa ante un ataque ARP

Switches: Seguridad en la configuración ARP.
La política de defensa ante un ataque debe ser desplegado con prioridad alta en el nodo más cercano a la fuente de ataque para minimizar el impacto y mejorar la eficiencia de defensa. Por esta razón es recomendable iniciar la protección en la configuración de los switches, como posible primer blanco de un atacante. La tecnología de seguridad de la mayoría de los switches actuales para el protocolo ARP

garantiza la seguridad y solidez de los dispositivos de red mediante el filtrado de paquetes ARP que no son de confianza.

Los ataques contra una o varias computadoras de usuarios pueden ser de menos impacto debido al uso de antivirus, aunque no todos actúan de forma efectiva. En comprobaciones realizadas se demostró que si el software antivirus detecta la dirección falsa, limpia la caché local y envía nuevos paquetes ARP, si clasifica como un ataque bloquea la dirección por un lapso de tiempo predefinido. Si el ataque va contra los routers o los switches es un poco más complicado. Debemos tener en cuenta que si el ataque ARP logra tomar el router la red entera podría ser comprometida. Sin embargo, si se aseguran los switches que son los que reenvían los paquetes ARP es posible que el ataque no logre tal magnitud.

Si los switches los permiten, es necesario revisar en su configuración los siguientes aspectos:

- ARP antispoofing
- Defensa a la puerta de enlace
- Supresión de paquetes ARP perdidos basado en la dirección fuente.
- Defensa contra ataques de hombre en el medio
- Fijar límites de velocidad entre paquetes ARP y paquetes ARP perdidos
- Chequeo de la dirección MAC fuente en los paquetes ARP

Para limitar un ataque ARP dentro de las subredes administradas, se realizó un script con el objetivo de fijar las direcciones del gateway correspondiente por cada subred, y los pares IP-MAC de los servicios más importantes (DHCP, DNS, NTP). Este script se pasa como política a cada una de las máquinas. Con esto resulta más complicado la ejecución de un ataque MITM, puesto que es necesario actualizar de forma manual las direcciones IP del gateway u otro servicio que haya sido fijado.

```
@echo off
::Subredes
set netx=192.168.x.


::Mac del router(4503)
set macgw=00-22-92-c4-c1-ff

::macs e IPs de srvdc01->192.168.X.X y srvdc02->192.168.C.C(AD, NTP, File Server, WINS, DNS)
set macdc01=00-45-56-8c-09-05
set ipdc01=192.168.X.Z
set macdc02=00-96-56-96-00-D2
set ipdc02=192.168.X.Y

::----------
ipconfig > _tmpipcfg.txt
FIND "IP Address" _tmpipcfg.txt > _tmpips.txt
for /f "tokens=2 skip=2 delims=:" %%a in (_tmpips.txt) do (call :subroutine1 "%%a")
::pause
for /f "delims=." %%a in ('ver') do @set version=%%a
set short1=%version:~18,2%
set short2=%version:~18,4%
set short3=%version:~27,8%
if %short1%==XP GOTO :Adicionar
if %short2%==2000 GOTO :Adicionar
if %short3%==5.2.3790 GOTO :Adicionar
del _tmpips.txt
del _tmpipcfg.txt
exit
:Adicionar
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v ArpCacheLife /t REG_DWORD /d 0x000000a /f
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v ArpCacheMinReferencedLife /t REG_DWORD /d 0x000000f /f
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v ArpRetryCount /t REG_DWORD /d 0x0000003 /f
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v StrictARPUpdate /t REG_DWORD /d 0x0000001 /f
del _tmpips.txt
del _tmpipcfg.txt
if  %subnet02%==%net15% arp -s %ipdc01% %macdc01% & arp -s %ipdc02% %macdc02%
exit
:subroutine1
set ip=%1
set ip=%ip:~1,-1%
set subnet01=%ip:~1,9%
set subnet02=%ip:~1,11%
set subnet03=%ip:~1,12%
if  %subnet02%==%net95% arp -s 192.168.Z.X %macgw% & GOTO :eof
if  %subnet03%==%net217% arp -s 192.168.W.X %macgw% & GOTO :eof
if  %subnet01%==%netdmz% arp -s 10.30.B.X %macgw% & GOTO :eof
if  %subnet02%==%net15% arp -s 192.168.A.X %macgw% & GOTO :eof
```

Figura 1: Script para fijar direcciones en las tablas ARP en estaciones de trabajo con sistema operativo Windows (XP, 2000, 2003)

```
#! /bin/bash

NIC=(ls /proc/sys/net/ipv4/neigh/)

#15 min
TIME=900

ROUTERMAC="00:00:00:00:00:00"

for net in $NIC
do
    if [ "$net" != "lo"]
      then
        sysctl -w net.ipv4.neigh.$net.gc_stale_time=$TIME
    fi
done

IPLIST=$(ifconfig | grep -Eo 'inet (?) (addr)? (:)? [0-9]*\.){3}(0-9)*)'
| grep -Eo ' ([0-9]) *\.) {3} (0-9)*' | grep -v '127.0.0.1')

for i in $IPLIST
do
    if [[ $i == xx.xx.xx.*]]
    then
      router=$(echo $i | sed -r 's/[0-9]+$/1/')
      arp -s $router $ROUTERMAC
    fi

done
exit 0

```

Figura 2: Script para fijar direcciones en las tablas ARP en estaciones de trabajo con sistema operativo Linux (Probado en Fedora 23 o superior, Ubuntu, Debian y Centos)

En el caso de las estaciones de trabajo con Windows se manipulan parámetros tales como el tiempo de vida de la caché ARP, ArpCacheMinReferencedLife que determina que cantidad de entradas deben existir en la caché ARP antes de que pueda ser borrada, ArpRetryCount (ARP gratuito) y StrictARPUpdate. Es importante resaltar que esta es una protección funciona de forma efectiva si se protegen ambos extremos (router y PC).

CONCLUSIONES.

Existen vulnerabilidades en el funcionamiento del protocolo debido entre otros factores, a la ausencia de mecanismos que permitan determinar la autenticidad de las tramas ARP recibidas. Sin embargo se puede proteger la red implementando mecanismos de detección que permitan monitorizar el tráfico ARP en una subred. Si unido a ello se aseguran los elementos de conectividad en la medida de lo posible (switches y routers), así como las computadoras la ejecución de un ataque MITM usando el protocolo ARP resulta más complicado y casi deriva en resultados nulos. El uso de la herramienta snort unido a la distribución de los scripts que modifican el comportamiento por defecto de las tablas ARP y el aseguramiento de la característica antispoofing en los switches y routers garantizan un mecanismo de defensa óptimo.

REFERENCIAS.

1. Neo, Networking and emerging Optimization Group, “Herramientas web para la enseñanza de protocolos de comunicación.” [Online]. Available: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/arp.html.

2. Network Working Group David C. Plumer, “RFC 826.”

3. MORENO P'EREZ, JUAN CARLOS; SANTOS GONZALEZ, MANUEL; Sistemas informáticos y redes locales, España, EDITORIA RA-MA 2012, ISBN 978-84-9964-159-1

4. Tecnológico Nacional de México, cursos online, “Protocolo de resolución de direcciones.”

5. Ecured, “Gestion de la tabla ARP.”

6. CHIANG GUERRERO, L.D.; “Descripción del problema del envenenamiento del protocolo ARP mediante árboles de ataque, usando un mecanismo automatizado para encontrar las vulnerabilidades.,” Escuela Superior Politécnica del Litoral.

7. ELÍAS RM, “ARP Spoofing”. http://linuxgnublog.org/envenamiento-de-las-tablas-arp-arp-spoofing/ Consultado en línea el 19 de mayo de 2016.

8. SNORT TEAM HOMEPAGE, Snort - the de facto standard for intrusion detection_prevention. http://www.snort.org

9. NORT TEAM HOMEPAGE, “Snort Users Manual”. http://www.snort.org

10. ISL ARPGUARD HOMEPAGE, https://www.arp-guard.com/en/home.html