ARP Spoofing

Transcribed on August 2, 2025 at 9:56 AM by Minutes AI

Speaker 1 (00:01)

Bienvenidos a esta nueva sesión.

En esta nueva sesión vamos a tratar el tema de los ataques basados en IPV y en esta primera parte veremos un tipo de ataque llamado ARP Spoofing.

El ataque ARP Spoofing, también conocido como ARP Poisoning o envenenamiento, es es una técnica de hacking que se emplea para enviar mensajes ARP falsificados a una red.

Estos mensajes están diseñados para engañar a los dispositivos dentro de la red haciendo que asocien la dirección IP de un host legítimo con la dirección Mac de un atacante.

De esta manera el atacante puede interceptar, modificar o incluso bloquear el tráfico destinado al host legítimo, ya que los dispositivos de la red envían el tráfico al atacante pensando que es el destino legítimo.

Este tipo de ataque explota la manera en la que las redes locales, las LAN, utilizan el protocolo ARP para mapear las direcciones IP a las direcciones Mac, lo que permite al atacante manipular el tráfico de la red sin ser detectado fácilmente.

El esquema que veis en la diapositiva intenta mostrar cómo es la secuencia de ataque de un ARP Spoofing.

Bien, el Swoofing también es un ataque de un man in the middle o de un hombre en medio, que lo que hace es lo que hemos comentado antes, explotar el protocolo ARP que es esencial en las comunicaciones LAN, y eso es justo lo que hemos simulado aquí.

Tenemos dos máquinas virtuales, cada una con su propia IP y veremos cómo actuar o cómo ejecutar un ataque ARP Spoofing.

Bien, pues esta va a ser la máquina servidor que tiene la dirección IP que podéis ver aquí, la 10.211.55.5, y será la que va a ser atacada todo el tráfico que esta red genere en conexión con el gateway es la que vamos a interceptar desde el ataque con ARP Spoofing desde la otra máquina.

Recordemos que ARP lo que hace es traducir las direcciones IP en direcciones Mac, lo que permite la comunicación dispositivos en la misma LAN.

En este ataque, el adversario, el atacante, envía mensajes a ERP falsificados para asociar su dirección Mac con la dirección IP de otro host, que normalmente suele ser el gateway de la red, y esto le permite al atacante interceptar, modificar o incluso bloquear el tráfico destinado a la dirección IP suplantada, lo que es un gran problema de confidencialidad, integridad y disponibilidad de los datos que tiene la dirección IP que veremos ahora que

Lo primero, como siempre vamos a verificar la conectividad, haremos un pin, Correcto, hay conectividad.

Bien, ahora usaremos el comando arp para comprobar cuáles son las máquinas que se pueden comunicar dentro de la red e identificar la máquina que va a ser nuestro objetivo, en este caso será la Mac del gateway.

Entonces lo que miraremos es utilizar el comando arp, que si no lo tenemos instalado podemos instalarlo con apt install nettools Ya lo tenemos, arp, perfecto, Vale, pues haremos el comando arp a Bien, pues ARP ya nos ha ofrecido una información muy importante y muy relevante que es la dirección Mac del gateway, que podéis ver aquí.

Esta es la IP asociada al gateway y aquí tenemos la dirección Mac.

Bien, pues ahora tenemos que habilitar el IP forwarding y esto es para permitir que los paquetes de datos fluyan correctamente entre la víctima y el keyway real mientras el atacante intercepta el tráfico.

Y para eso hay que habilitarlo de la siguiente forma.

Haremos eco, haremos un pipe, sudo a ti y ahora ponemos la junta.

Ahora os cuento lo que hace ese comando IP forward.

Bueno, no hace falta, hasta aquí estaría bien.

Esto lo que hace que echo lo que hace es generar por ejemplo el valor que queremos escribir en el archivo, el pipe lo pasa como entrada y el sudo t con la dirección IP forward es la elevación de privilegios con el comando t para que podamos escribir el 1 en el archivo especificado, en este caso el ip forward y así ya directamente lo habilitamos.

Bien, pues ahora sí que vamos a ejecutar el ataque arp spoofing y para eso utilizaremos la herramienta arpspoof.

Pues bien, ya podemos proceder a ejecutar el ataque arp spoofing, pues con la herramienta arp spoof comenzaremos el envío de respuestas ARP falsificadas para asociar nuestra dirección Mac con la dirección IP del gateway en la tabla ARP de la víctima.

Y el comando sería el siguiente, subo delante ARPSPUF, le pondríamos guión T para asignar la tarjeta de acción y después T para, perdón, sería I T y ahora pondríamos la dirección 55.5, la dirección que queremos atacar y después el gateway 111 55.1 Bien, pues de momento está empezando a funcionar.

Cuando hemos iniciado este comando, lo que comienza es el envío de paquetes ERP falsificados, lo que va a hacer que la víctima envíe su tráfico de red al atacante en lugar del gateway real, y esto permite que nosotros, los atacantes, interceptemos, inspeccionemos o modifiquemos el tráfico de la red entre la víctima y el gateway.

Bien, aquí el ataque sigue su curso, está funcionando y para comprobar que todo está correctamente vamos a ir ahora a la máquina víctima para comprobar que al hacer un arp a, la dirección de gateway que tiene que aparecer como Mac, tiene que ser esta dirección que acaba en e y que no es la primera que tendría que tener, que era la que estaba asociada realmente al gateway.

Bien, de vuelta a la máquina 1, si hacemos un ARP A, veremos que la dirección 1 está apuntando a esta, que es justamente la dirección Mac nuestra, la que hemos puesto en el ataque arp y que podéis comprobar aquí mismo en la captura, acababa en e e, pues justamente la Mac que estamos usando para hacer el ARP spoofing.

De hecho la dirección Mac que debería de salir es esta, si aquí abrimos una ventana nueva y ponemos asp a, esta es la dirección Mac que debería de aparecer como gateway cuando está apareciendo la nuestra en vez de la es la e e, como podéis ver aquí.

Bien, pues a partir de este momento esta máquina ya está comprometida, cualquier tráfico de red lo podemos monitorizar desde la máquina atacante porque todo se va a redirig hacia la máquina número 2, hacia la máquina que está atacando.

Bien, he vuelto a la máquina atacante, he dejado en otra ventana el ARP spoofing y en esta ventana nueva lo que voy a levantar es un TCP dump, que ya conocemos cómo funciona, pero bueno, aquí vemos que es lo que está diciendo, es que va a capturar todo el tráfico que sea ARP o IP.

Pues levantamos este comando y ahora lo dejamos en ejecución para que vaya capturando toda la información.

Como veis la máquina atacante está por un lado haciendo el TCP dump por aquí y por otro lado ejecutando el ataque httpspuffing, así que a partir de ahora toda esa información la tenemos ya almacenada aquí, pero claro, el tráfico HTTPs está cifrado, por lo tanto no veremos a qué URL se ha conectado.

Yo antes he hecho la conexión a Google y ésta no se verá reflejado aquí, pero sí veremos todo el REST de información, por ejemplo, si enviar algún tipo de archivo sin cifrar o cualquier cosa que no tenga ningún tipo de cifrado va a estar siempre a merced de nuestra máquina que está snifando todo el tráfico.

Antes tendría que haber ejecutado el comando aquí voy a parar un momento antes de pena para volcarlo a un fichero, os acordáis que habría que ponerle al final kion W y el fichero de captura sería aquí en W captura pcap y ahí ya lo almacenaríamos para después gestionarlo.

Pero bueno, en este caso sólo quería mostraros cómo se ejecuta un ataque ARP y cómo se captura la información.

Y a partir de aquí, si la queréis analizar sólo tenéis que utilizar de nuevo TCP DAN tal y como lo hemos explicado en otros módulos, sin ningún tipo de cambio, es exactamente igual.

Bien, pues ahora vamos a ver cómo podemos mitigar muy por encima un ataque ATP Spooning.

Lo primero es aplicar algún tipo de autenticación.

Hay que implementar soluciones de seguridad basadas en autenticación como el IEEX, lo que nos permite verificar a dispositivos y usuarios antes de darle acceso a la red y así nos aseguramos que sólo los autorizados se puedan conectar.

Después tenemos que utilizar herramientas de monitorización de red que puedan detectar y alertar sobre cambios inusuales, es decir, anómalos, que se hagan sobre todo en la tabla ARP.

Después tenemos que configurar reglas en los dispositivos de red para bloquear o filtrar el tráfico ARP que sea sospechoso, o sea que tenga algún tipo de comportamiento inusual, como respuestas ARP que provienen de múltiples direcciones Mac para una misma dirección IP.

Y también tenemos una que está asociada con la segmentación, que es la implementación de VLAN.

Se puede implementar una VLAN para segmentar la red y esto reduce la superficie de ataque y limita la propagación de paquetes ARP maliciosos a través de la red.

Pues bien, el ARP Spoofing es una técnica de ataque que sigue siendo una amenaza significativa para la seguridad de redes sociales.

Este método de manipulación de las tablas de direcciones ARP puede permitir a los atacantes interceptar, redirigir o modificar el tráfico de red, y esto compromete toda la información.

Las consecuencias del ARP spoofing pueden ser muy graves, ya que los atacantes pueden realizar actividades maliciosas como el robo de información confidencial, la suplantación de identidad o la interrupción de los servicios de red.

Para mitigar el riesgo de ATP spoofing es fundamental implementar medidas de seguridad muy robustas como la autentica monitorización de ARP, el filtrado, etc.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.