# Envenenamiento IPV

Transcribed on July 16, 2025 at 10:27 PM by Minutes AI

Speaker 1 (00:01)

Bienvenidos a esta nueva sesión.

En esta sesión se va a proponer un ejercicio para trabajar con el protocolo de descubrimiento de vecinos en redes IPV.

Se trata de un ejercicio bastante completo, ya que contempla desde el montaje de un escenario hasta trabajar con el concepto de envenenamiento de vecinos en redes IPV y por supuesto también para aprender cómo realizar esto de manera práctica y sobre todo con las herramientas adecuadas.

Vamos a ver en detalle un poco más sobre este ejercicio.

Y es que como estaba comentando, este ejercicio va a simular un escenario donde tenemos dos dispositivos en la misma red IPV.

Uno de estos dispositivos va a ser el denominado atacante y el otro o los otros dos serán la víctima.

Realmente uno de los dos será la víctima, pero vamos a establecer un enlace local entre dos máquinas.

Una de ellas será la víctima y luego tendremos nuestra máquina atacante, que será la que se coloque en el medio utilizando el kit de herramientas THC y PIOV.

Nuestro objetivo va a ser el de realizar un ataque de envenenamiento de vecinos para engañar a la víctima y para redirigir su tráfico a través de nuestro dispositivo.

Pero ahora vamos a ver en detalle exactamente qué deberíamos realizar.

En primer lugar, y como vengo comentando, deberíamos preparar un entorno virtual.

En este caso se puede trabajar con el hipervisor con el que se sienta más cómodo, pero sí que sería bastante útil tener al menos dos máquinas, aunque lo recomendable serían tres.

Una de esas máquinas debería ser Kali Linux, otra o bien un Windows o Ubuntu y la otra pues también podría ser un Ubuntu.

Al final, en estas dos máquinas, como he comentado, van a tener comunicación IPV entre ellas y será nuestra máquina Kali la que se encuentre en el medio.

Y como digo, también recomiendo la máquina Kali, ya que tiene instaladas por defecto las herramientas para trabajar, que es el 15 herramientas THC IPV.

Sin embargo, también sería posible instalar estas herramientas en cualquier otro sistema Linux, como es el caso de las máquinas con Ubuntu.

Y es que además del montaje de estas máquinas en el entorno virtual, tendremos que asegurarnos de que la comunicación de red entre ambas máquinas es buena y que también están configuradas para trabajar con IPV.

Y es que de nuevo, dependiendo del hipervisor con el que trabajemos, lo tendremos que configurar de una manera u otra, pero es importante que se consiga la comunicación entre ambas máquinas mediante la red EPV.

Por supuesto que para validar esto deberemos realizar una prueba de conexión entre ambas máquinas, y por supuesto también que lo más sencillo es hacerlo con el comando ping.

Vamos a probar que ambas máquinas tienen conectividad entre ellas, incluso también nuestra máquina Kali, que será la que se coloca en el medio, tiene que tener comunicación entre ellas y lo hacemos mediante un ping.

Eso sí, tendremos que asegurarnos de que ambas máquinas pueden responder a estos paquetes ICMP, que por defecto en los sistemas Linux no suele haber problemas, pero atención con las máquinas Windows, porque por defecto pueden tener bloqueado este tipo de tráfico y por tanto no responder a nuestra comunicación y podemos pensar que no tienen comunicación entre ellas, pero sin embargo puede estar todo correcto y sí que la pueden tener, así que mucho ojo con eso.

Y vamos a hacer la prueba de conexión para asegurarnos de que está todo correctamente instalado y todo correctamente conectado.

Y ahora sí pasaríamos a lo que sería la parte de la identificación del objetivo, que va básicamente sería localizar la dirección IPV de la máquina víctima.

Claro, esto es muy sencillo porque lo podemos hacer directamente observando la configuración de la propia máquina o bien podemos explorar alguna de las herramientas que vienen en el kit Herramientas de THCV para poder descubrir los distintos vecinos, como puede ser por ejemplo la herramienta Alair 6, que por supuesto recomiendo probarla y conocerla.

Y ahora sí, con todo preparado se puede pasar a explorar la herramienta Parasite 6.

Esta herramienta permite falsificar mensajes de descubrimiento de vecinos, como son el caso de los mensajeros, y de esta manera podemos engañar a los dispositivos y redirigir el tráfico a través de un dispositivo controlado en este caso por el atacante, es decir, por la máquina Kali que va a ser la que ejecute este comando.

Y ya por último y para finalizar tendremos que comprobar que el tráfico está pasando por nuestra máquina, y para ello podemos repetir el ping anterior entre las máquinas Windows, Ubuntu o el entorno que hayamos montado, y es que si lo revisamos con Wireshark podemos ver que el PIN que se están haciendo entre ambas máquinas está pasando por nosotros.

Si conseguimos ver el tráfico IPV que pasa por nosotros, esos paquetes ICMP V que están pasando cuando hacemos el ping, habremos conseguido correctamente el envenenamiento de vecinos.

Y es que si observamos la terminal en la que se ejecuta la herramienta o el comando de Parasite 6, vamos a ver cómo nos empieza a indicar distintos mensajes de que se están mandando paquetes escucheados indicando que efectivamente se está realizando el envenenamiento de vecinos.

Con este ejercicio vamos a tener la oportunidad de probar el kit de herramientas DHT IPV en un entorno práctico controlado y también de explorar los desafíos y los riesgos asociados con el envenenamiento de vecinos en redes IPVC.

Y hasta aquí con esta propuesta de trabajo.

Os esperamos en el siguiente vídeo.