IPv6 Attack Toolkit

Transcribed on July 16, 2025 at 9:55 PM by Minutes AI

Speaker 1 (00:07)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a hablar de algunas herramientas disponibles para trabajar con IPV.

Concretamente vamos a conocer la suite de herramientas de Banhauser conocida como THC IPV Attack Toolkit, o lo que es lo mismo, el kit de herramientas de ataques IPV de THC o de Hacker Choice.

Básicamente se trata de un conjunto de herramientas de código abierto que ofrece una amplia gama de ataques y pruebas de pentesting diseñadas específicamente para redes IPV.

Está desarrollada por el equipo de The Hacker Choice, de ahí el nombre THC, y es que esta herramienta es ampliamente utilizada por profesionales de la seguridad para evaluar la resistencia de las redes IPV y para detectar posibles vulnerabilidades.

Vamos a conocer un poco más sobre ello, así que vamos a movernos a un sistema operativo Kali Linux, donde además de tener las herramientas ya instaladas de serie, vamos a conocer un poco más en detalle sobre estas.

Nos encontramos ya en el sistema operativo Kali Linux y en esta ocasión quiero empezar directamente desde el navegador, ya que aunque tenemos el kit herramienta instalado, quiero que veamos una cosa, y es que si dentro de la página web de GitHub, este repositorio con miles de miles de proyectos de código abierto, hacemos una búsqueda sobre IPV, si queremos saber qué tipo de proyectos o de repositorios tenemos con esta etiqueta.

Y es que encontramos varios que tienen que ver con esta terminología, algunos por supuesto que bastante interesante, pero lo que a nosotros nos interesa es centrarnos de hecho en el primero, pero quiero que conozcáis otros, como puede ser por ejemplo Mam in the Middle 6, que como veis es para hacer ataques en redes IPV a través de redes IPV, un proyecto que está escrito en Python y que por supuesto que os recomiendo echar un vistazo.

Si nos fijamos dentro de esta terminología de búsqueda que nos aparece 6100 resultados, tenemos justamente aquí el de Banhauser THC THC IPV, este sería el nombre del usuario y aquí el nombre del proyecto, que como vemos es ese Attack Toolkit.

Vemos que se trata de un proyecto escrito su mayor parte en C, en código C.

Y si bajamos un poquito más vamos a ver el README, vemos que es cierto que es un repositorio que lleva bastantes años parado, de hecho vemos desde hace nueve años, vemos que sí que hay alguna cosita que se hizo hace ocho meses, pero que en general es un proyecto que se hizo y que no ha tenido mayor desarrollo.

Si bajamos un poco, como estaba indicando, vamos a llegar al readme del proyecto donde vamos a poder leer un poco más sobre las herramientas.

De hecho ya lo primero que nos indican, aparte de esta primera introducción, nos indican también unas limitaciones, es decir, que necesitan un Linux en una versión del kernel 2.6 mínimo y además obviamente Ethernet.

Si bajamos un poco más vemos aquí una sección para ver cómo deberíamos hacer el compilado de estas herramientas.

Pero es que para hacer el compilado necesitamos una serie de dependencias, en este caso el lib pk y además también las librerías lib ssl y libnefilterq.

De hecho aquí vemos que esto es bastante sencillo de instalar si nos encontramos en un sistema operativo como Kali, Debian o Ubuntu, simplemente haciendo uso del gestor de paquetes apt con su apt get install y ahora las herramientas todas en su versión de desarrollo lib pcap, lib ssl y libnefilter queue.

Luego veis que para hacer el compilado utilizaríamos el makell Y por último si quisiéramos instalarlo una vez que se ha hecho el compilado de todas las herramientas, haríamos uso de makeinstall.

Y ahora pasando a hablar de las herramientas, aunque aquí no aparecen todas las que hay, esto sí que es un buen listado de todas las que aparecen, y es que una de las más famosas herramientas que se tienen aquí es el Parasite 6, que esto nos va a permitir hacer el spoofing de vecinos o el envenenamiento de vecinos, es decir, algo muy parecido a lo que sería el envenenamiento de la tabla ARP en redes IPV.

Luego por ejemplo hay otra utilidad llamada Live 6 que nos permite detectar precisamente los vecinos que tenemos cerca en otra ocasión.

Aquí tenemos el DNS div, que básicamente es un DNS para redes IPV, nosotros le vamos a indicar un dominio y la dirección a la que debería redireccionar.

Luego aquí tenemos uno para hacer, por ejemplo, enunciarnos como un router falso.

Aquí otro para redirigir el tráfico.

En definitiva tenemos bastantes.

Aquí tenemos ataques de de denegación de servicio, etcétera.

Un fuzer por aquí.

Luego tenemos varios que tienen que ver con hacer mensajes falsos o anunciarlos de manera falsa en la red, o incluso poder hacer nuestro propio paquete para mandar un paquete pin 6 como nosotros queramos.

Esto para que veáis un poco, para que conozcáis el repositorio, aquí vemos cómo nos hablan un poco más de las librerías.

Si nos vamos al conjunto de herramientas de Kali, en la sección de Kali Tools, aquí podremos hacer una búsqueda para encontrar cómo viene instalado, ya que vamos a ver que cambia un poco y no se ejecuta simplemente con thc, de hecho si busco aquí parasite, al buscar parasite vemos cómo nos aparece ATK para site 6, vemos que esto era un comando, si os habéis fijado nos aparecía ahí la parte de comando, que es este comando que tenemos aquí, pero es que si nos fijamos esto pertenece a un paquete denominado thc ipv, pero es que este paquete dentro nos va a instalar toda esta cantidad de comandos, hay muchos que no estáis viendo, pero esto es lo que si nos ponemos un poquito por encima nos aparecen toda la cantidad de comandos que podemos lanzar y cada uno de ellos hará una acción diferente.

De hecho voy a venir aquí arriba para ver la documentación de las herramientas y vemos cómo nos hacen una serie de ejemplos, en este caso con el comando adress 6, que no es simplemente adress 6 sino atk address sería la manera correcta que lo tendríamos justamente aquí es donde le tenemos, aquí vemos otro con alive 6, otro para detectar nuevas redes y view v y si bajamos un poquito más pues aquí tenemos el ejemplo del DNS Git 6.

Luego ya por supuesto que pasamos a hablar de nuevo de todos los paquetes, de cómo lo podríamos instalar en el caso de estar en otra distribución que no lo tenga instalada o si se ha borrado, pues la manera de instalar todo el conjunto de de herramientas, todo el comando es con sudo apt install thc y pv.

Como veis no es lo mismo que hemos visto antes en el gitcab, porque eso era para hacer el compilado de todas las herramientas, en este caso son ya todas las herramientas compiladas que las vamos a instalar a través del gestor de paquetes de apt.

Y luego bueno, por supuesto como en kalitools pues tenemos todas las ayudas que ya nos vienen aquí para que nos expliquen un poco más, que esto es lo que obtendríamos cuando ejecutamos este comando en la terminal.

Así que lo que quiero hacer simplemente por supuesto que podéis explorar cada una de las herramientas que vienen aquí, pero vamos a probar estas dos que tenemos aquí delante, así que para ello me voy a abrir la terminal, vamos a utilizar, como digo si pongo adress 6 e intento darle al tabulador, pues vemos que no nos sale, de hecho si le doy me dice oye el comando no ha sido encontrado, como digo tenemos que hacer atk address 6, de hecho aquí voy a ejecutar la ayuda para que lo veamos y veis que esta herramienta pues como nos dice aquí en su descripción nos va a permitir convertir una Mac o una dirección IPV en una dirección IPV del modo link local, siempre y cuando no se haya indicado un prefijo.

Entonces vamos a hacer esta pequeña prueba, yo le digo oye pues quiero convertir, bueno quiero más bien obtener la dirección Mac de esta dirección IP v, aquí podemos ver claramente cómo una dirección de link local está basada en gran parte de la dirección Mac, de hecho si empezamos a ver después de tener el FE y que aquí ya sabéis que estos dobles dos puntos van a representar un conjunto de de ceros y vemos como aquí nos pone 76 D, es verdad que no es exactamente igual, bueno de hecho vamos a marcar esto, 76 d 35 no es exactamente igual, pero vemos como sí que el D y el 35 sí que se corresponde con lo mismo que estamos viendo aquí.

Luego vemos cómo nos aparece fff para hacer una separación, pero luego vemos también como los tres últimos octetos o la última parte de la dirección Mac es también la última parte de la dirección IPV y por supuesto que si copiásemos esta dirección y digo oye quiero que me generes de esta dirección, de esta dirección Mac la dirección IPV, si yo pongo aquí el d e c, vamos a ver cómo nos genera exactamente la misma dirección que hemos visto aquí en la parte superior, Veis que ese dato de una herramienta bastante sencillita y que pues dada una dirección Mac, una dirección IPV, una dirección IPV, pues nos sacará la dirección link local de IPV o en el caso de dar la dirección IPV nos va a sacar la dirección Mac.

Vamos ahora también a utilizar esta otra bastante sencillita que es para descubrir los hosts que están vivos y es que si lo utilizamos con el comando de ayuda vamos a ver que tenemos un montón de opciones, vamos a ver que tenemos un montón de opciones disponibles pero que al final hay una cosa que tenemos que indicar seguro que es la interfaz en la cual queremos que se detecten todas esas máquinas o esos host que están disponibles o que podemos ver dentro dentro de nuestra red.

Así que es lo que vamos a hacer, vamos a utilizar en vez de el H voy a indicar mi dirección y atención, perdón, voy a indicar mi interfaz y atención porque si lo ejecuto así no me va a dejar, me va a dar un error y es que esta serie de herramientas que trabajan con la red en muchas ocasiones es necesario tener los permisos de administrador como es el caso.

Así que nada, aquí lo damos, vemos como esto ha mandado los paquetes IGMP que de hecho esto lo podemos ver cómo funciona si abrimos por ejemplo el Wireshark, lo vamos a abrir, vamos a poner aquí un filtro solamente para redes IPV, vamos a empezar a capturar en la interfaz eth y vamos a volver a lanzar este comando para que veamos y para que analicemos aquí qué es lo que se está mandando y es que en este caso como podéis ver y como se indica aquí el eco reply básicamente lo que estamos haciendo es si abrimos este, veis que lo estamos mandando al FF, es decir, le estaríamos mandando a todas las partes para que intente responder la parte de los routers y es que luego empezamos a obtener respuesta desde distintas direcciones, de hecho fijaos que aquí abajo tenemos un paquete NS y un paquete na, vamos a ver esto porque es bastante interesante y es que en este caso como es un.

Bueno aquí tenemos primero los que mandamos nosotros que sería el eco request y es que si abrimos aquí en el protocolo de control de mensajes de Internet versión 6 vamos a ver que el tipo es 128 que se corresponde precisamente con ese echo request y luego pues por supuesto que una de las partes que podemos ver aquí es por ejemplo la dirección de origen y la dirección de destino, que eso también lo vamos a ver ahora cuando se manden por ejemplo el NS y el na, esto lo comento ahora mismo.

Por otro lado tendríamos la respuesta, lo que sería el reply, que vemos como en vez de ser el tipo 128 como es el request, pues en este caso lo tenemos aquí el 129 y como digo este caso el NS, los tipos de mensaje NS y NA, que veis que también va sobre el protocolo ICMPV y que sirve para hacer el descubrimiento de vecinos.

De hecho fijaos que aquí se está preguntando por la dirección, en este caso se le está solicitando esta, vamos a abrir aquí un pelín más, vemos como esta dirección está preguntando en este caso a mí, porque si recordamos cuál es nuestra dirección vemos que mi dirección termina en bea.

Entonces si nos venimos de lo vaquí al wiresark, nosotros somos el destino, nos están preguntando, y es que en este caso nos estarían preguntando para asociar nuestra dirección de IPV con una dirección Mac y nosotros pues vemos como aquí estaríamos haciendo esa respuesta.

Algunas cosas que podemos ver aquí es que en esta opción de dice mpv se estaría mandando la dirección, como vemos la dirección Mac, que la vemos aquí, la podemos también ver y claro podemos ver hacia quién va, cuál es la dirección target y aquí en esta capa podríamos ver las dos cosas, tanto la dirección de origen como la dirección del destino, pero la parte interesante en este caso el mensaje NS se está produciendo aquí y luego por el otro lado tendríamos la dirección, o sea la respuesta precisamente a esta solicitud, esta sería la respuesta en el cual sería el tipo 136.

Aquí podemos ver las flag que se estarían mandando, la dirección objetivo, la dirección target y por supuesto aquí en la capa anterior pues también vemos la dirección de origen y la dirección de destino.

Como veis esto es un poco lo que estaría pasando en este caso cuando se está utilizando el comando atk alive por debajo.

Por último sí que quiero enseñar que cuando nosotros lanzamos el ATK y damos al tabulador, todos estos comandos van dentro de la suite de THC y PIOV y que por supuesto, como ya he dicho cada uno es distinto y cada uno va a tener su manera de ejecutarse, sus opciones y va a tener su propia utilidad.

Así que os animo a todos a que investiguéis sobre todas estas herramientas orientadas a las redes libv, sobre todo teniendo en cuenta que uno de los más importantes sería el de Parasite 6, este que vemos aquí, que como digo esto sería algo equivalente a la ERP Spoofer en redes IPV.

Esto lo dejo para que lo investiguéis un poquito más.

Por último y para finalizar con esta sesión, hemos visto un poco más sobre esta herramienta THC IPV Attack Toolkit o el kit de herramientas de THC IPV y también el papel fundamental que tiene para una evaluación y una mejora de seguridad en las redes IPV.

Hemos visto como este kit de herramientas puede ser utilizado para realizar una gran variedad de técnicas y ataques como son el descubrimiento de vecinos, trabajar con las direcciones IPV y ver sus direcciones Mac equivalentes, trabajar por ejemplo el spoofing de vecinos e incluso las denegaciones de servicio, ya que si hacemos una suplantación de identidad pero no estamos permitiendo el paso de los paquetes, estaríamos causando una denegación de servicio.

Además de otras herramientas y otras técnicas que tenemos en THC y PV Attack Toolkit que van a permitir realizar este tipo de técnicas.

Así que con esto llegamos al final de la sesión y os esperamos en el siguiente vídeo.