# Network Management

Transcribed on July 12, 2025 at 9:50 AM by Minutes AI

Speaker 1 (00:08)

Bienvenidos a esta nueva sesión donde vamos a trabajar con diferentes comandos de red, principales herramientas para el manejo de la red y configuración de esta.

Vamos a comenzar viendo las diferentes herramientas que vamos a tratar, los diferentes comandos.

Vamos a hablar sobre ifconfig, vamos a hablar sobre ip, sobre el comando road, sobre el comando ping, sobre la herramienta fping, una herramienta similar a la anterior, sobre el comando netstat y sobre el comando hpin o sobre la herramienta hpin.

Bueno, tenemos que saber que dentro de la distribución en linux como los sistemas operativos windows, cualquier sistema operativo contiene un conjunto de herramientas que permiten configurar la red, que permiten sacar conexiones, listar puertos abiertos, poder configurar tanto la IP, la máscara de red, los servidores ns que queremos utilizar.

Toda esta configuración de red se puede hacer a través de ciertos comandos, además hay gran cantidad de herramientas que nos permiten hacer otras cosas que vienen en esta sesión.

Todas estas herramientas por supuesto son sencillas de utilizar y nos permiten disponer de un conjunto de funcionalidades importantes a la hora de ver cómo funcionan las redes.

Vamos a comenzar hablando de la herramienta ifconfig o el comando ifconfig.

Este comando se utiliza para configurar principalmente interfaces de red, sistemas Unix, sistemas Linux.

Nos permite ver, modificar, adaptar la configuración de reducción, por ejemplo configurar mi dirección ip, configurar la máscara de la red a la que estoy conectado, me permite listar interfaces activas, me permite deshabilitar interfaces, mostrar incluso estadísticas de transmisión de datos o incluso ver información sobre la dirección física o la dirección marca.

Después haremos una serie de ejemplos con cada una de estas herramientas.

Tenemos también la herramienta IP.

La herramienta IP es similar a la anterior, es una evolución, podemos decirlo así o podemos verlo así, es una utilidad que nos permite, que también son de sistemas Unix y Linux y nos permite mostrar y configurar la información de la red, nos permite poder editar las interfaces red, ver las rutas, las tablas de enrutamiento, ver la caché rp, la tabla rp, incluso reglas del firewall en algunas ocasiones.

También podemos realizar diferentes operaciones de red dentro de esta herramienta.

Otro de los comandos importantes en la configuración de red en el mundo Linux es root.

Esta herramienta nos permite visualizar y manipular o editar la tabla de enrutamiento del kernel.

Esto es importante porque si queremos configurar o manejar bien las redes de ordenadores necesitamos tener conocimiento sobre este comando para poder crear mis rutas, estoy creando una red o estoy diseñando diferentes redes, puedo necesitar este tipo de comandos para poder configurar las tablas de enrutamiento.

Tenemos también la herramienta ping, una herramienta bastante conocida.

La herramienta ping también se utiliza para verificar la conectividad entre máquinas, es decir, sin si yo desde mi máquina puedo tener visibilidad o conectividad con otra máquina, puedo intentar hacer un ping.

Al final lo que hace esta herramienta es lanzar por debajo el protocolo ICMP con el tipo de mensaje eco request y esperamos respuestas del tipo del tipo eco repli.

Al final, como vimos en otras sesiones, aquí los protocolos de red cobran muchísima importancia porque al final las herramientas cuando interactúan con otras lo hacen a través de esos protocolos y podemos descubrir diferentes cosas.

Entonces la herramienta Ping nos va a permitir comprobar si un juego remoto está accesible, está vivo a través de la red, incluso calcular el tiempo de ida y vuelta, incluso calcular a cuántos saltos, gracias al dato del TTL, el time to give del protocolo IP, a cuántos saltos está de nosotros esa máquina, cuánto salto significa, cuántos routers están por delante.

Tenemos también la herramienta fping.

La herramienta fpin, como he comentado anteriormente, es similar a la herramienta ping, permite enviar múltiples paquetes de tipo icmp, del tipo eco request a múltiples host de una red de forma simultánea.

Entonces simplifica un poco el proceso de tener que hacer ping a cada una de las IPs que hay una red, podemos ganar, generar un rango de direcciones ip automáticamente fp nos va a hacer esa solicitud para ver la conectividad con esas máquinas.

Incluso podemos decirle oye, solamente muéstrame las máquinas que estén vivas, que estén despiertas y el resto no me las muestres.

Claro, tener en cuenta que el ping por icmp es muy fácil que esté en muchas ocasiones filtrado, entonces bueno, pues es un mecanismo para poder descubrir máquinas, pero bueno, habrá mecanismos mejores.

El comando netstat, tenemos una versión de windows, tenemos una versión de Linux, en este caso hacemos eco del comando en Linux.

La herramienta netstat nos detalla, nos muestra información sobre las conexiones de red, sobre las tablas de enrutamiento de la máquina, nos muestra incluso estadísticas de de la propia red, interfaz y otro tipo de datos relacionados.

Además podemos ver conexiones activas, puertos abiertos, qué procesos están en esos puertos, las conexiones que están establecidas, tipo de protocolo de transporte tcp, udp, etc.

La verdad que la herramienta netstat tiene bastantes, bastantes usos.

Y la última herramienta que queremos enumerar es la herramienta hpin.

Ahora iremos haciendo un ejemplo en cada una de ellas.

Herramienta hp es una utilidad bastante avanzada de red que permite hacer muchísimas cosas, es decir, nos permite enviar paquetes tcp, nos permite enviar paquetes IP, nos permite enviar paquetes con diferentes protocolos en la red con el objetivo múltiple de descubrir máquinas o de poder verificar si un puerto está abierto en una máquina o cualquier acción que se nos pueda ocurrir.

Este tipo de herramienta viene muy bien en la parte de escaneos, enumeración, esa fase un de todo OpenTesting que nos permite descubrir máquinas, que nos permite identificar qué servicios, qué puertos, qué tipo de aplicaciones, si existe algún tipo de firewall delante de las máquinas.

Hpin tres nos permite gestionar o controlar esto de manera rápida.

Así que como digo se puede utilizar para muchas cosas.

Es una pequeña navaja suiza de red donde podemos generar tráfico de manera muy rápida y muy sencilla sin necesidad de ponernos a programar con Scapi en Python, que bueno, también es otra posibilidad hacernos nosotros nuestras propias mini herramientas con Scapi en Python, pero hp ya nos lo proporciona.

Bien, ahora vamos a pasar, vamos a pasar a la máquina Kali.

Tenemos aquí en esta máquina, vamos a ir jugando un poco con las diferentes herramientas que hemos ido viendo.

Bien, aquí por ejemplo tenemos la herramienta, hemos hablado de ifconfig, si nosotros listamos o queremos estar las interfaces con ifconfig nos vale.

Con ifconfig podemos ver aquí interfaz de red, esta máquina tiene tres interfaces de red, tiene la interfaz de red de loopback, la local, en localhost tenemos la interfaz de red ETH y la interfaz de red ETHAn.

Vemos que aquí tenemos configurada la dirección ip, aquí tenemos otra dirección ip, diferentes redes, aquí tenemos la máscara de red y aquí tenemos otra máscara de red, sus direcciones de broadcast asociadas y además tenemos aquí información sobre su dirección física, su dirección ipv y lo mismo, dirección física y dirección ipv.

En este caso el th no tiene.

Bien, con ifconfig podemos configurar fácilmente por ejemplo una dirección ip, podemos asociar una dirección ip a mano, manualmente, indicando por ejemplo en eth la red uno 0.0, .024, pues voy a decirle 10 puntos, aquí podemos indicarle la máscara de red en este formato, imaginaos que fueran ocho, como si fuera ocho sería un barra 24, que sería así.

Otra opción que tenemos la de prefijo, de esta forma necesitaríamos ser sudo, tenemos que meter el sudo para poder ejecutar la acción.

Vamos a ir ahora al comando ip, es un comando bastante amplio respecto a lo que ifconfig nos proporciona.

Ifconfig proporciona ciertas funcionalidades, pero ip amplía las funcionalidades y engloba varios comandos de red en uno.

Bueno, primero vamos a probar iPad Show, podemos ver que hay tres interfaces, incluso tiene varias o puede tener varias direcciones ip, podrían estar ahí.

Esto nos muestra un poco el resumen de la configuración de red, de los diferentes adaptadores de red.

Si nosotros quisiéramos por ejemplo crear o añadir una nueva ip lo podríamos hacer por ejemplo de la siguiente manera Indicando aquí esto, lógicamente podemos añadir, como veis, varios lo pasa no tiene mucho sentido, tendríamos que dejarlo en uno principal y el resto pues quedaría ahí.

Añadir es sencillo, eliminar también, simplemente tenemos que cambiar el add por el del y eliminaríamos la configuración de esa ip en ese adaptador de red, en este caso nth.

Tenemos también la posibilidad de ver desde este comando la tabla de enrutamiento que tiene esta máquina.

La tabla de enrutamiento de esta máquina, aquí la podemos ver, diferentes adaptadores en función de hacia donde quiera enviar el paquete o el tráfico de red, pues irá por un adaptador o por otro, irá a una dirección ip o a otra.

Tenemos también la posibilidad de añadir redes, por ejemplo, si yo quiero decir oye, para ir a la red 11 lo haremos vía la 1000, imaginaos que estuviera la 1001, que fuera un gateway, que fuera un router y oye, a esta máquina para ir a la red 11 yo tengo que enviar el tráfico a la 1,001.

Yo creo esta regla, cuando en la máquina se envíe tráfico hacia una hipotética red 11, 11 24, cualquier dispositivo que se encuentre en esa red, nosotros enviaremos el paquete al 10001, que es un supuesto router, podría ser un router, y le enviamos eso y el router lo acabaría enrutando hacia donde fuera.

Para hacer la operación contraria, es decir, para eliminar una red, haríamos lo mismo, lo único que simplemente tendríamos que indicar la opción del, no haría falta indicar la vía, lógicamente, porque simplemente quiero eliminar que me estoy en la tabla de enrutamiento para que lo olvidemos como máquina, que la olvidemos.

Bien, esta parte del comando ip es muy interesante porque el comando route, que es el tercero que hemos visto, comando road, realmente nos permite hacer un poco lo mismo.

N podemos ver la tabla de enrutamiento, inclusive con netstat también podemos ver tabla de enrutamiento, nos permite ver la tabla de enrutamiento y nos permite luego este comando nos permite ir añadiendo, por ejemplo, entradas a la tabla de enrutamiento con el comando ip particularmente a mí me parece más intuitivo, pero para el comando router también podemos añadir Oye, yo quiero llegar a red máscara de red que es 24 y quiero hacerlo a través del Gateway 1000.

Si os fijáis, esta instrucción es equivalente a la instrucción que hemos utilizado aquí, son formas de hay una red 11 y para llegar a esa red 11 tengo que hacerlo a través de la dirección ip.

Bien, para hacer la eliminación de esta regla lo único que tenemos que hacer es cambiar el add por end.

¿Bien, qué ocurre?

Como vemos aquí, vemos aquí que está la entrada por defecto que se llama es decir, si el tráfico que voy a enviar no va dirigido a la red 10 y va redirigido a la red 172, 17240, significa que lo tengo que enviar por aquí.

Esto es lo que se llama entrada por defecto.

La entrada por defecto crea utilizando el comando route add default ew y la IP a la que queremos enviarle el tráfico que yo no sepa enrutar a ninguna red por otra forma.

Si os fijáis, la ruta por defecto que tiene esta máquina ahora es cualquier paquete que no vaya a esta red de aquí o a esta red de aquí, lo vamos a enviar por este gateway, por esta ip, que puede ser un router, puede ser una maquia, se lo entregamos a él y a la o ya sabrá cómo hacer para que llegue.

Nosotros podríamos añadir un gateway, una ruta por defecto de esta forma y para eliminar la que está ya creada, por ejemplo, tendríamos que hacerlo de la siguiente manera.

Aquí ya podríamos así diríamos quiero eliminar esta y añadir la que hemos puesto antes.

Bueno, este es el comando route, es un comando bastante importante, como veis el comando ip hace algo parecido.

Y ahora vamos a trabajar con el comando ping.

El comando ping es un comando muy sencillo, tenemos muchas, muchas cosas que comentar de este comando, pero por ejemplo el 10 cero cero 20 es una ip que tengo yo ahí levantada y vamos a hacer ping a esa máquina.

Me marca ttl, ttl me puede dar mucha información sobre el tipo de sitio operativo, me puede también dar información sobre el número de saltos, número de rutas que hay entre el destino y la máquina origen, bueno, me puede dar cierta información.

Bueno, aquí tenemos el comando ping.

El comando ping además, como hemos dicho antes, utiliza el protocolo ICMP con el eco y el concepto le correplico y tienen que contestar.

Podemos también indicar el número de paquetes que queremos enviar, por ejemplo queremos enviar dos paquetes con el menos c y luego podemos también indicar el tipo de intervalo, el número de intervalo entre paquetes, bueno, podemos jugar un poco con ellos.

Además fijaros que nos da el tiempo, lo que tarda el paquete en ir y volver.

Tenemos un comando un poco más avanzado o más vitaminado a veces decimos así, que es el fpink.

Aquí el fping nosotros podemos hablar de ello como diciendo bueno, entre el 10001 y el 10000, bueno no entre, sino 1000-1000 2010-0010 ahora mismo 10 no está activa, me tendrá que saber que no se activa, la 10 20 sí y la 10.10 si está activa entonces ahora está arriba y la otra está dando inalcanzable.

Podemos generar también un rango g le digo entre la un y la 20, todas las que están entre la un y la 20.

Entonces fijaros como dice, oye, la 12 está viva, la 20 está viva, el resto inalcanzable, inalcanzable es algo bastante interesante.

Y luego también hay un pequeño filtro, dime cuáles son las que están vivas.

Al final es muy similar a lo que hemos visto antes, saca el mensaje, no me dice que es inalcanzable y me devuelve esto, que están vivas con el parámetro que nos da, lógicamente Fp.

Muy interesante que echemos un ojo y que veamos las opciones que tiene.

Tiene bastantes opciones dentro de personalizar lo que queremos hacer con el protocolo ICMP.

Vale, pasamos a la siguiente.

La siguiente es netstat.

Netstat es una herramienta para ver principalmente las conexiones de red.

Por ejemplo, con la opción n nosotros podemos visualizar todas las conexiones de red en formato numérico y es un poco locura a veces.

Luego con la opción p tenemos para ver todas las conexiones de red y los procesos asociados.

Sigue siendo un poco locura porque vemos ahí todo.

¿Si juntamos np, hemos visto, bueno, saca un poco lo mismo que hemos visto en la última conexión con el p, qué ocurre?

Con el t le saca las conexiones tcp, con el u saca las conexiones udp, ahí vemos que hay establecido la conexión por udp, capa de transporte udp.

Y con el l me muestra todos los procesos que están a la escucha.

Fijaos esta parte, aquí vemos también conexiones de Internet, mejor dicho, procesos que están a la escucha.

Entonces yo puedo añadir, yo quiero saber o listar, oye, pues también procesos que tienen algo a la escucha pero que sean de Tcp o de Udp Ltu.

Aquí me saca, oye, pues tienes el puerto 22, por ejemplo, el ssh, tienes aquí el formato numérico, lo podemos decir, oye, muéstrame un formato numérico con el menos n, en vez de sacarme aquí el protocolo, fijaos como me mete aquí el sacha que dice, por tanto con el n estoy diciendo dámelo en un formato numérico, no me lo pongas el protocolo.

Y es una herramienta bastante interesante para saber qué servicios tenemos, qué procesos están con servicios a la escucha dentro de las máquinas.

Y bueno, desde el punto de vista de pentestre, cuando accede a las máquinas también es interesante conocer este tipo de comandos porque puede ver cosas de las máquinas.

Y por último tenemos el hpin tres.

Este comando es muy grande, simplemente quería mostraros un poco, es un comando, una herramienta muy potente con muchas funcionalidades, muchos parámetros, pero fijaos en este estamos diciendo que queremos enviar un paquete, la cantidad de paquetes que mandamos por segundo, pues hay fast, está faster, hay diferentes modos, fast creo que son como 10 paquetes por segundo, el s mayúscula que es que queremos mandar un paquete tcp con el flag de sim y el parámetro scan que es el puerto 20 al 500, queremos enviar a ese rango de puerto.

Entonces a la máquina 10 20, por ejemplo, lanzamos esto con el comando sudo, fijaos como aquí me está sacando el puerto de antiguos habilitado y puerto 80 y ahí lo tenemos.

Opciones del resto de puertos, entre el 20 y 500 hay 481 puertos, hay dos abiertos, 479 cerrados, algo así, no tira, está generando 481 puertos, no está yendo muy rápido.

Si lo ponemos en Faster creo que son 100 paquetes por segundo, 80, muy rápido, es mucho más rápido.

Hpin, ya digo, es una herramienta que posiblemente sale en otras partes del módulo o de otros módulos porque tiene muchísimas posibilidades, como veis aquí, muchísimas capas donde configurar a nivel de IP, a nivel de ICMP, a nivel de transporte, tanto UDP como TCP.

Podéis hacer escaneos para identificar puertos abiertos, para identificar si hay puertos filtrados, escaneos también para identificar ciertos servicios, se puede saber muchas cosas con hpin tres, es una herramienta bastante potente, bastante flexible.

Bien, con esto ahora sí llegamos a la parte final.

Como conclusiones hemos estado viendo un conjunto de herramientas de red importante, comandos de red importante y luego hemos estado viendo también algunos ejemplos de uso ya sobre la máquina kali.

Bien, recordar siempre, importante hacer las pruebas sobre vuestro laboratorio, con vuestras máquinas y todo con vuestra propiedad.

Bien, pues con esto finalizamos, nos vemos en la siguiente sesión.