IPV6 Security

Transcribed on July 29, 2025 at 10:38 AM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a ver algunos de los aspectos de seguridad de IPV y también veremos una filosofía aplicada a la seguridad llamada Zero Trust o Confianza cero.

Bien, no voy a explicaros qué es IPV ni cómo funciona, pero sí quería contaros que cada vez son más habituales encontrar los direccionamientos basados en IPV.

Estas proveen mejoras tanto en el enrutado como en la velocidad de comunicaciones.

Respecto al estándar IPV, por ejemplo, no existe casting como tal.

Es muy habitual que empresas actuales tienen el modelo llamado Dual Stack, es decir, utilizan dos IPV e IPV en la misma infraestructura i y esto es un problema porque es un vector de ataque.

Sobre IPV solo quería contaros que es un estándar que está en evolución continua y cada vez más son las redes que lo están utilizando.

Su finalidad principal es proveer el máximo número de direcciones públicas de Internet y también se centra mucho en el diseño y la securización de redes.

De hecho es muy útil instalarlo en redes empresariales porque nos ofrece una gran cantidad de mejoras en la seguridad.

Como recordatorio, los tipos de direcciones IPV son diferentes a los de IPV, por ese motivo es muy importante conocerlos.

Los tres tipos de direccionamiento a grandes rasgos son el unicast, que son comunicaciones nodo a nodo, el multicast, donde los paquetes entregan a todos los nodos y el anycast, el cual gestiona la ruta más corta entre dos nodos.

Aunque IPV ofrece por defecto algunas características de seguridad de base en su diseño, como por ejemplo IPSec por defecto, esto no quiere decir que por solo aplicar IPV la red sea más segura.

IPV también tiene una característica llamada SLAAC que es Stainless Address Auto Configuration que facilita enormemente como el host configura la red con este protocolo, pero a su vez puede hacer que perdamos el control de la misma.

Para aplicar este SLAAC o slack necesita exponer su dirección Mac, lo que también supone un riesgo de la seguridad.

Para remediar este problema se pueden utilizar técnicas que generen direcciones más por ejemplo aleatorias.

También con IPV es posible que un mismo host tenga varias direcciones, como por ejemplo las suministradas por DHCP v una slack o incluso direcciones IPV.

Para evitar exponer nuestra actual configuración IPV es recomendable seguir al menos tres sencillos consejos a la hora de integrar IPV en una organización.

La primera es comenzar instalando una pequeña infraestructura paralela que asigne direcciones IPV a equipos y usuarios controlados.

Más que nada se hace para irnos acostumbrando un poco a su funcionamiento.

El punto número 2 o fase 2 sería configurar ipv en los elementos de red dentro de la organización, es decir, en router, switches, etc.

Es decir, aplicar un término llamado Dual Stack.

Ahí podéis ver una captura de cómo se hace este Dual Stack desde Windows en la configuración de la tarjeta de red.

Así poco a poco iremos comprobando qué problemas de conexión, de seguridad, etcétera, de aquellos dispositivos que estén bajo esa configuración están teniendo.

Entonces a partir de ahí podemos empezar a tener un listado o tener un feedback de cómo están funcionando con esta doble configuración.

En esta fase es imprescindible revisar qué elementos conectan en la red y además que son compatibles con este protocolo.

Esto es importante.

Y ya una última fase 3 o punto 3 sería establecer por defecto el acceso ya completo a Internet con IBV, el es decir, todos los dispositivos de la infraestructura utilizarán este protocolo para sus comunicaciones tanto privadas como públicas.

Este sería el último escenario, el ideal, donde todo funciona bajo IPV.

Ahora os voy a hablar de Zero Trust o confianza cero, y no es más que una estrategia que asume que ningún usuario ni dispositivo es confiable dentro de mi perímetro de la red, incluso aquellos que ya están por defecto dentro de ella, es decir, los mismos elementos que yo he configurado o que yo tengo dentro.

Gracias a esta técnica es posible limitar al máximo cualquier tipo de acción dentro de los límites de un perímetro que utiliza la estrategia Zero Trust.

De hecho, esta estrategia es la más efectiva para contrarrestar los posibles movimientos laterales en caso de un acceso no autorizado a la red.

La implementación de zerotrass se realiza directamente utilizando técnicas ya conocidas de segmentación.

En definitiva, con este método de protección estamos añadiendo una capa extra, digamos creando microperímetros al segmento de la red que estamos protegiendo.

Quizás el caso más útil o más práctico que pone en práctica el Zero Trust es un caso de amenazas internas, los llamados insider, donde tanto empleados o un atacante que haya podido acceder, si tenemos Zero Trust, estas técnicas podrían mitigar ese ataque y uno de los motivos es por la microsegmentación que antes he comentado, ya que añade una granularidad al diseño, creando pequeños perímetros de seguridad que aíslan al atacante utilizando por ejemplo métodos de autenticación y de autorización.

Y hablando de autorización, otro punto importante es que también se añade la identificación del usuario.

Zero Trust considera a todos los usuarios no confiables, por este motivo si alguno intenta realizar alguna tarea sospechosa éste estará controlado en todo momento.

Y esto se hace con un control de accesos, ya que es un método para aplicar los menos privilegios posibles dentro del Zero Trust.

Es decir, con Zero Trust un usuario empezaría con el menor de los privilegios y se le iría añadiendo en función que lo fuera solicitando o le fuera necesario dentro de su trabajo habitual.

Pues bien, vamos a ver ahora un ejemplo práctico de cómo aplicar el Zero Trust y para ello utilizaremos una herramienta llamada Fail to ban.

Free to ban es una herramienta de prevención de intrusos que escanea los archivos de registro del sistema y banea aquellas IP que muestran signos maliciosos o demasiados intentos de inicio de sesión fallidos.

Esto de las sesiones fallidas suele ser normalmente utilizada por scripts de fuerza bruta para intentar acceder a una ubicación.

Bien, pues lo primero que vamos a hacer es instalar fail toban.

Hacemos un update como siempre antes de hacer la instalación y ahora procederemos a la instalación final.

Decimos que yes y cuando acabe ya tendremos la aplicación.

Ya tenemos operativa.

Bien, pues una vez instalado fail toban ya debería de estar operativo, pero es mejor trabajar con una copia del archivo de configuración.

Lo primero que vamos a hacer es vamos a copiar el fichero de configuración, utilizamos sudo porque está en una carpeta de sistemas que utilizamos ahora ponemos fail to ban, buscamos el fichero que es yale conf, pero aquí utilizaremos las llaves para conf local.

De esta forma hemos copiado el fichero yale conf a yails local y así ya podremos hacer cualquier tipo de personalización.

Vale, pues vamos a editar el fichero yail conf, entonces hacemos su to nano y lo cargamos y le llamamos yail local.

Vale, aquí tenemos ya el fichero de configuración y la aplicación que vamos a monitorizar va a ser ssh, así que aquí buscaremos entre las páginas la sección que habla de SSHD debe estar por aquí bastante cerca, aquí está, ya la vemos aquí abajo y aquí haremos una serie de modificaciones.

Pondremos la primera debe de ser enable le pondremos que true, la siguiente el port, decimos ssh, añadimos una que sea filter en el que pondremos ese HD ahora es contarle que es cada cosa, después pondremos logpath, podemos hacerlo ahí, vale, dejamos ese, no pasa nada, podemos dejar que viene por defecto en los logs y hacemos max retree, le ponemos bueno un número 5 por ejemplo y band time será 600.

Bien, pues estos valores lo que significan es que el servicio está activo, con lo cual va a monitorizar el puerto SSH estándar y utilizará el filtro SSHD que hemos definido en el SSHD conf irá a ese fichero que se basa en un archivo de registro que es el varlockauthu log max retry es el número de intentos fallidos permitidos antes de banear la IP y bantime es el tiempo en segundos en la que la IP será baneada.

Lo que sí vamos a hacer para que funcione mejor es cambiar esta línea y utilizar el que he comentado, el auth log, funcionará mejor con esa opción, ponemos var, ponemos log y ponemos auth log Bien, pues en este punto ya tenemos los cambios, vamos a grabar, almacenamos el fichero y ya podemos reiniciar el servicio.

Sudo systemml y restart fail to banner Bien, vamos a verificar que está todo OK, vamos a hacer un fail Toban client status pues vemos que en la salida número of jail, el número de jaulas, tenemos que hay una y y está asociada al servicio SSHD, con lo cual está correcto.

Bien, vamos a comprobar nuestra dirección IP para después conectar la otra máquina aquí vemos que está aquí la 10.

211.5514 Bien, pues ya estoy en la otra máquina, vamos a ver qué IP tiene esta máquina diferente, esta acaba en la 15, recordemos que la anterior era la 14, así que vamos a hacer un pin a ver si todo va bien y tenemos visibilidad con la otra máquina.

Bien, ahí está, podemos comprobar que hay conectividad, pues lo siguiente que haremos será una conexión SSH.

Bien, pues ponemos ssh, ponemos usuario ficticio 5 5 14 nos pide una contraseña, ponemos cualquier cosa y otra cualquier cosa también está todo erróneo, el usuario de la contraseña otra vez otra contraseña, pusimos 5 ¿Verdad?

Pues fijaros, se ha parado en el cuarto.

Bien, pues aquí ha pasado una cosa, fijaros aquí no se ha activado el fade to ban, Aquí lo que se ha parado ha sido ssh, Ha sido ssh quien ha cortado la conectividad al cuarto intento, porque ssh también tiene una forma de evitar que tú hagas muchas conexiones contra el servicio que está en su configuración.

También en un fichero muy parecido al que hemos visto de fail to ban.

¿Por qué ha pasado?

Pues porque en el fail to ban hemos puesto, si os acordáis que eran cinco intentos, con lo cual ese ha sido el problema, se ha activado antes el ssh que el fail to ban.

Realmente lo he dejado así para que vierais que hay dos formas de hacerlo, una directamente contra el servicio que es short y otra con fail toban.

La ventaja que tiene fail to ban es que lo podemos hacer con más servicio, no sólo con ssh, con lo cual bueno, vamos a ir para atrás y vamos a cambiar ese valor por 3 para ver cómo se activa failband en vez de ssh.

Bien, pues si os acordáis era editar un fichero que se llama etc, acordáis que era este fichero y aquí bajamos y buscamos la parte de aquí y cambiamos de 5 a 3.

Grabamos.

Bien, pues vamos a reiniciar el servicio con un Systemctl Starter Fail to Pan Inicia servicio, vamos a ver cómo está el estado.

Bien, pues de vuelta aquí otra vez vamos a hacer la misma operación, vamos a conectar de nuevo.

Bien pues contraseña una, ahora debería de pararse en el número 3.

Justo ahora es cuando se debería de aplicar la política del fail to ban en vez de ssh.

Esto se quedará así un buen rato porque lo que está haciendo es esperando una respuesta del servidor que no tiene.

Así que vamos a ir al servidor y a ver cómo está el estado de fail to ban y si aparece algo nuevo deberíamos de ver una dirección IP bloqueada que es la que tiene este equipo, que es la que acaba en 15, la 10211 55 15 para verlo hacemos sudo fail to ban, ponemos client y le decimos status id servicio que es el dhd.

¿Bien, pues ahí lo podéis ver, actualmente hay una IP baneada que es justamente la 15 y en total sólo hay una IP que se ha baneado, veis?

Esta es la IP que tenemos en la otra máquina, que es la que ha intentado hacer esos tres intentos, con lo cual ya a partir de ahora la otra máquina no va a conectar nunca y estará permanentemente baneada de este servidor.

Si quisiéramos volver a darle acceso, pues hacemos sudo fail to ban otra vez client set sshd y le decimos unban ip y ahora la dirección ip que sería la 10.211.55 15 esto quitaría ese baneo y volvería a autorizar la conexión.

Ya si volvemos a hacer esa conexión y ponemos la contraseña correcta pues nos dejaría conectar.

Si ahora mostramos otra vez el status vemos que ya no aparece como IP baneada, con lo cual nos tiene que autorizar el acceso en la próxima conexión.

Pues bien, este ejercicio que es bastante simple pero nos sirve para comprender de una forma muy básica cómo failban puede proteger tus servicios frente a ataques de fuerza bruta.

Porque ese es el objetivo.

El objetivo de limitar el número de accesos a un servicio o un servidor es evitar sobre todo ataques de fuerza bruta o evitar que haya muchas peticiones a la vez que provoquen una denegación de servicio, por ejemplo.

Y estos componentes son un buen ejemplo de lo que es una arquitectura cero trust.

Confianza cero no voy a dejar que nadie, ni siquiera IPs que son dentro de mi sistema o están dentro de mi intranet o dentro de mi control, no todas van a tener un límite de acceso y si lo superas esa dirección IP se va a banear.

También podemos mirar el fichero log haciendo un tail f al fichero log que tiene el mismo fade toban que está en var log fadeban log Ahí veremos un poco lo que ha ido pasando.

Aquí veis que es la restauración y el unban de la dirección IP.

Como conclusión, IPV representa un avance significativo en la seguridad de redes gracias a características como IPsec integrado y los encabezados de paquetes simplificados, que ofrece una mayor protección contra ataques y algún tipo de violación de nuestros datos.

Sin embargo, para garantizar una seguridad completa de toda la información es fundamental implementar una filosofía de Zero Trust o confianza cero.

Este enfoque implica, como antes he comentado, que ninguna entidad, ya sea interna o externa a la red, debe ser confiada por defecto, requiriendo una verificación continua de identidad y autorización para acceder a recursos de red.

Al adoptar los principios de Zero Trust, las organizaciones pueden mitigar eficazmente amenazas internas y externas, reducir el riesgo de brechas de seguridad y proteger los datos sensibles frente a posibles ataques.

Llegamos.