Engineer

Tres cerraduras en la puerta, ninguna cerrada

Detecté y corregí tres protecciones contra fuerza bruta SSH que nunca habían funcionado: una jail de bloqueo que vigilaba el puerto 22 mientras el demonio escuchaba en el 1986, un límite de tasa oculto bajo una regla más amplia y una acción de bloqueo cuyo binario nunca se encontraba, por lo que no se había aplicado ningún bloqueo.

agosto 2026

tres defensas contra fuerza bruta que nunca habían funcionado

Situación. Una revisión del endurecimiento del host de producción en agosto de 2026 planteó una pregunta que suele recibir una respuesta segura: si las protecciones frente a ataques de fuerza bruta por SSH estaban funcionando. Las tres estaban configuradas, las tres aparecían en cada informe que alguien consultaba y las tres habían permanecido inertes desde el día en que se creó el host.

Tarea. Los controles debían comprobarse frente a lo que el kernel hace realmente con un paquete, en lugar de frente a los archivos de configuración que describen lo que debería ocurrirle.

Acción. Leer la configuración habría confirmado la respuesta equivocada tres veces, así que la revisión examinó el sistema en ejecución. La jaula del servicio de bloqueo de intrusiones vigilaba el puerto 22 mientras que el demonio se había trasladado al 1986 durante el endurecimiento inicial — cada bloqueo que escribía señalaba un puerto en el que no escuchaba nada. La limitación de frecuencia del cortafuegos era peor de una forma más sutil: la regla existía y estaba situada debajo de una regla más amplia que coincidía primero. Las reglas de usuario del cortafuegos se evalúan de arriba abajo y gana la primera coincidencia, por lo que un permiso amplio por encima de una limitación de frecuencia convierte esa limitación en código muerto que sigue apareciendo en todos los listados de estado. La tercera era la más silenciosa: la acción de bloqueo invoca un ejecutable de filtrado de paquetes que el sistema de paquetes solo

recomienda, sin exigirlo, por lo que en un host que carece de él la jaula arranca, cuenta y decide, y luego falla justo en el momento en que intenta bloquear. Las tres correcciones fueron pequeñas. Lo que surgió de aquello no fue la corrección, sino dos reglas que ahora rigen el repositorio: un control de seguridad recibe una aserción en lugar de un comentario, y un cortafuegos se verifica por la posición de las reglas en lugar de por su presencia.

Resultado. Tres protecciones que nunca se habían activado lo hacen ahora, y la clase de defecto a la que pertenecen — un control cuyo modo de fallo consiste en seguir indicando que funciona correctamente — es la que las comprobaciones de la plataforma están diseñadas ahora para detectar. Las tres habían estado inertes desde el arranque inicial. Las tres aparecían como correctas en todos los lugares que alguien consultaba, y esa es precisamente la razón por la que perduraron.

Aplique esta experiencia a su proyecto

Utilice «Tres cerraduras en la puerta, ninguna cerrada» como punto de partida para un reto similar en su organización. Los servicios que respaldan este trabajo están disponibles para su proyecto. Monitorización y alertas que avisan cuando un fallo aún es pequeño, y cifras que muestran con qué frecuencia se mantiene así.

Explore nuestros servicios Póngase en contacto →

Mire más allá del resultado

Lea la situación, las decisiones y el resultado de este ejemplo. Podemos hablar de qué partes se adaptan a sus restricciones y cuáles necesitan otro enfoque. Tres cerraduras en la puerta, ninguna cerrada — tres defensas contra fuerza bruta que nunca habían funcionado

Explore nuestros servicios Póngase en contacto →

¿Sabe si su protección contra intrusiones protege de verdad?

Converse sobre su proyecto con la ingeniera responsable de la entrega. Acordamos por escrito el alcance, la base del precio y el traspaso antes de empezar a trabajar.

Contexto de la función: Ingeniera de seguridad. Se apoya en Infraestructura, Monitorización y observabilidad, Redes y VPN, Linux y servidores, Seguridad y Administración de sistemas. Y ya que está aquí, también se nos da bien Fiabilidad de sistemas y monitorización, Configuración de redes y VPN, Seguridad y gestión de accesos y Seguridad de agentes de IA.

Póngase en contacto Explore nuestros servicios

Una parte de **una trayectoria más amplia** — y toda ella está en este sitio.

Cada entrada sigue la misma estructura: la situación, la tarea, lo que hicimos y lo que cambió.

Vea la trayectoria completa

Defina la mejora que necesita

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

¿Sabe si su protección contra intrusiones protege de verdad?

Pregunte por las decisiones detrás de «Tres cerraduras en la puerta, ninguna cerrada». Hablará con las personas que pueden explicar el trabajo y valorar su propio proyecto.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/portfolio/three-locks-on-the-door-none-of-them-locked/