AUDITORÍA DE SEGURIDAD LYNIS

Informe de endurecimiento del sistema

Auditoría de seguridad automatizada de la imagen, ejecutada con Lynis sobre una instancia recién provisionada antes de publicarla.

HOST **ip-172-31-83-68**	SISTEMA OPERATIVO **Ubuntu 26.04 LTS**
KERNEL **7.0.0-1011-aws**	ARQUITECTURA **arm64**
VERSIÓN DE LYNIS **3.1.7**	PERFIL **custom.prf**
DURACIÓN **57s**	EJECUTADO POR **root**

Nuestro compromiso de endurecimiento

Todas las imágenes que publica imaxe.cloud van endurecidas de serie, por la seguridad de quien las pone en producción. No entregamos una distribución desnuda: el sistema llega con cortafuegos que deniega por defecto, SSH restringido, kernel y opciones de montaje reforzados, actualizaciones de seguridad desatendidas y las herramientas de integridad de ficheros, rootkits, malware y auditoría instaladas y funcionando.

Este informe es la prueba. Se genera automáticamente sobre una instancia recién construida, antes de publicar la imagen, no se edita nunca a mano y se publica entero, incluido todo lo que la auditoría no puntuó. El endurecimiento es parte del producto, así que la auditoría que lo mide viaja con él.

ÍNDICE DE ENDURECIMIENTO

0
Advertencias
Problemas que conviene corregir

0
Sugerencias
Mejoras a considerar

241
Pruebas realizadas
Comprobaciones de seguridad de Lynis ejecutadas

0
Plugins activos
Plugins adicionales de auditoría

Veredicto
El sistema alcanza un índice de endurecimiento de 100/100: una configuración fuertemente endurecida y lista para producción.

1 Puntuación por categoría

Desglose del resultado de la auditoría por área de seguridad, derivado de las advertencias y sugerencias de cada una.

Kernel y arranque	100
Autenticación	100
Sistema de archivos e integridad	100
Red y cortafuegos	100
SSH	100
Paquetes y herramientas	100

Registro y hora	100
Endurecimiento y malware	100

2 Advertencias

Hallazgos que Lynis marca como advertencias. Se revisan y corrigen antes de cada publicación.

ID DE TEST	DESCRIPCIÓN	SEVERIDAD
Sin advertencias: la auditoría no encontró problemas de este nivel.		

3 Sugerencias

Recomendaciones de Lynis. Algunas no aplican a imágenes cloud o son decisiones de diseño deliberadas.

ID DE TEST	RECOMENDACIÓN	CATEGORÍA
Sin sugerencias.		

4 Comprobaciones omitidas a propósito

La imagen ejecuta Lynis con un perfil que omite 23 comprobaciones. Ninguna es un agujero de endurecimiento: son comprobaciones que no se pueden evaluar en una imagen cloud, que ya cubre otro control, o que dependen de datos que solo existen con la instancia en marcha. Cada una se lista con su motivo para que la omisión sea auditable.

ID DE TEST	MOTIVO POR EL QUE NO APLICA
AUTH-9284	Las cuentas que señala son las de servicio de la base de Ubuntu (daemon, bin, sys…). Vienen sin password válida y sin shell interactiva, que es justo lo que se quiere; el test lee ese estado normal como un hallazgo.
BOOT-5122	No hay password de GRUB porque no hay consola física donde teclearla: una instancia EC2 arranca sola y su consola es una llamada de API protegida por IAM. La password solo sería un estorbo para un rescate.
BOOT-5180	Falso positivo en esta imagen: la comprobación no se puede evaluar aquí y su resultado no reflejaría el estado real del sistema.

ID DE TEST	MOTIVO POR EL QUE NO APLICA
BOOT-5264	Falso positivo en esta imagen: la comprobación no se puede evaluar aquí y su resultado no reflejaría el estado real del sistema.
CRYP-7902	Depende de datos que no existen mientras se construye la imagen; se resuelve en el primer arranque.
DEB-0810	apt-listbugs es interactivo: para la actualización para preguntar a una persona. En una imagen desatendida bloquearía las actualizaciones automáticas de seguridad, que importan mucho más.
FILE-6310	La imagen usa un único volumen raíz, que es como se redimensiona y se snapshotea una instancia cloud. Lo que esa comprobación busca de verdad —que /tmp, /dev/shm y /run no puedan ejecutar binarios ni contener dispositivos— aquí se consigue con opciones de montaje endurecidas.
FILE-7524	Los permisos son los que necesita este producto y se verifican en cada build con nuestra propia batería de tests; la comprobación genérica marca como error ficheros legítimos de la aplicación.
FIRE-4512	La comprobación cuenta reglas de iptables y llama «vacío» a una lista corta. Aquí la primera capa de filtrado es el Security Group de AWS, fuera de la instancia, y ufw cierra por defecto todo lo demás: la protección existe, solo que no está escrita donde este test mira.
FIRE-4513	El test marca como «sin usar» toda regla cuyo contador de paquetes esté a cero. En una instancia recién arrancada están todos a cero porque aún no ha llegado tráfico. El propio Lynis avisa de esto: una regla que no se ha disparado puede estar perfectamente en uso.
HRDN-7220	Los compiladores hacen falta en la imagen para DKMS y módulos del kernel, así que no se pueden quitar. Lo que se hace es restringirlos a root con permisos 0750, que es lo que verifica su comprobación hermana HRDN-7222, y esa sí pasa.
HTTP-6710	Depende de datos que no existen mientras se construye la imagen; se resuelve en el primer arranque.
KRNL-6000	La comprobación compara los sysctl contra una lista fija pensada para hierro. Esta imagen fija sus propios valores endurecidos y el kernel de AWS condiciona otros; las diferencias que reporta son decisiones nuestras, no descuidos.
LOGG-2154	No se hornea ningún servidor de logs externo porque el destino de los logs lo elige el comprador, no nosotros. Los registros están completos y en local, listos para enviarse a donde quiera.
LOGG-2190	La rotación se deja como la trae la distribución y se revisa servicio a servicio; la comprobación espera una disposición concreta que no encaja en una imagen pensada para reconfigurarse después de comprarla.

ID DE TEST	MOTIVO POR EL QUE NO APLICA
MALW-3280	Esta comprobación solo puntúa antivirus comerciales. La imagen lleva ClamAV, con firmas actualizadas automáticamente, y eso lo puntúa otra comprobación aparte: no vamos a empaquetar software de pago de terceros para ganar un punto.
NAME-4028	El dominio DNS no se hornea porque la instancia lo recibe por DHCP de la VPC del comprador. Lo que escribiéramos aquí se sobrescribiría en el primer arranque.
NAME-4404	Depende de datos que no existen mientras se construye la imagen; se resuelve en el primer arranque.
SSH-7408	SSH se queda en el puerto 22 porque es el que esperan EC2 Instance Connect y las herramientas de consola. Cambiarlo no esconde nada de un escáner; la fuerza bruta la paran la autenticación por clave y fail2ban.
SSH-7440	SSH no fija una lista explícita de usuarios permitidos: el comprador crea sus propias cuentas sobre esta imagen, y nuestra lista lo dejaría fuera. El acceso ya está restringido por autenticación solo con clave, sin login de root y con fail2ban.
TOOL-5002	No se instala ningún agente de gestión de configuración a propósito: la imagen se construye con Ansible por SSH, que no deja nada corriendo después. Un demonio menos es una superficie de ataque menos.
USB-1000	No aplica al modelo de una instancia cloud: lo que comprueba no existe aquí o lo cubre la infraestructura del proveedor.
USB-3000	No aplica al modelo de una instancia cloud: lo que comprueba no existe aquí o lo cubre la infraestructura del proveedor.

La lista se lee del perfil de Lynis horneado en la propia imagen, no de un documento mantenido a mano: lo que aparece aquí es exactamente lo que aplicó la auditoría.