AUDIT DI SICUREZZA LYNIS

Rapporto di hardening del sistema

Audit di sicurezza automatizzato dell'immagine, eseguito con Lynis su un'istanza appena provisionata prima della pubblicazione.

HOST **ip-172-31-83-68**	SISTEMA OPERATIVO **Ubuntu 26.04 LTS**
KERNEL **7.0.0-1011-aws**	ARCHITETTURA **arm64**
VERSIONE DI LYNIS **3.1.7**	PROFILO **custom.prf**
DURATA **57s**	ESEGUITO DA **root**

Il nostro impegno sull'hardening

Tutte le immagini pubblicate da imaxe.cloud sono rafforzate di serie, per la sicurezza di chi le mette in produzione. Non consegniamo una distribuzione nuda: il sistema arriva con un firewall che nega per impostazione predefinita, SSH ristretto, kernel e opzioni di mount rafforzati, aggiornamenti di sicurezza automatici e gli strumenti di integrità dei file, rootkit, malware e audit installati e in funzione.

Questo report è la prova. Viene generato automaticamente su un'istanza appena costruita, prima di pubblicare l'immagine, non viene mai modificato a mano e viene pubblicato per intero, compreso tutto ciò che l'audit non ha valutato. L'hardening fa parte del prodotto, quindi l'audit che lo misura viaggia con esso.

INDICE DI HARDENING

0
Avvisi
Problemi da correggere

0
Suggerimenti
Miglioramenti da valutare

241
Test eseguiti
Controlli di sicurezza Lynis eseguiti

0
Plugin attivi
Plugin di audit aggiuntivi

Verdetto
Il sistema raggiunge un indice di hardening di 100/100: una configurazione fortemente irrobustita e pronta per la produzione.

1 Punteggio per categoria

Suddivisione del risultato dell'audit per area di sicurezza, derivata dagli avvisi e dai suggerimenti di ciascuna.

Kernel e avvio	100
Autenticazione	100
File system e integrità	100
Rete e firewall	100
SSH	100
Pacchetti e strumenti	100
Log e orario	100

2 Avvisi

Rilievi che Lynis segnala come avvisi. Vengono esaminati e corretti prima di ogni pubblicazione.

ID DEL TEST	DESCRIZIONE	GRAVITÀ
Nessun avviso — l'audit non ha trovato problemi di questo livello.		

3 Suggerimenti

Raccomandazioni di Lynis. Alcune non si applicano alle immagini cloud o sono scelte progettuali deliberate.

ID DEL TEST	RACCOMANDAZIONE	CATEGORIA
Nessun suggerimento.		

4 Controlli omessi di proposito

L'immagine esegue Lynis con un profilo che omette 23 controlli. Nessuno di essi è una falla di hardening: sono controlli che non si possono valutare su un'immagine cloud, già coperti da un'altra misura, oppure che dipendono da dati che esistono solo a istanza avviata. Ognuno è elencato con il suo motivo, perché l'omissione sia verificabile.

ID DEL TEST	MOTIVO PER CUI NON SI APPLICA
AUTH-9284	Gli account segnalati sono quelli di servizio della base Ubuntu (daemon, bin, sys...). Arrivano senza password valida e senza shell interattiva, che è esattamente ciò che si vuole; il test legge questo stato normale come un rilievo.
BOOT-5122	Non c'è password di GRUB perché non c'è una console fisica su cui digitarla: un'istanza EC2 si avvia da sola e la sua console è una chiamata API protetta da IAM. La password sarebbe solo un intralcio in un ripristino.
BOOT-5180	Falso positivo su questa immagine: il controllo non è valutabile qui e il suo esito non rifletterebbe lo stato reale del sistema.

ID DEL TEST	MOTIVO PER CUI NON SI APPLICA
BOOT-5264	Falso positivo su questa immagine: il controllo non è valutabile qui e il suo esito non rifletterebbe lo stato reale del sistema.
CRYP-7902	Dipende da dati che non esistono mentre l'immagine viene costruita; si risolve al primo avvio.
DEB-0810	apt-listbugs è interattivo: ferma l'aggiornamento per chiedere a una persona. Su un'immagine non presidiata bloccherebbe gli aggiornamenti di sicurezza automatici, che contano molto di più.
FILE-6310	L'immagine usa un unico volume di root, la forma con cui un'istanza cloud si ridimensiona e si copia. Ciò che questo controllo vuole davvero — che /tmp, /dev/shm e /run non possano eseguire binari né contenere dispositivi — qui si ottiene con opzioni di mount rafforzate.
FILE-7524	I permessi sono quelli che questo prodotto richiede e vengono verificati a ogni build dalla nostra suite di test; il controllo generico segnala come errori file applicativi legittimi.
FIRE-4512	Il controllo conta le regole di iptables e definisce «vuoto» un elenco breve. Qui il primo livello di filtraggio è il Security Group di AWS, fuori dall'istanza, e ufw chiude per impostazione predefinita tutto il resto: la protezione c'è, solo non è scritta dove guarda questo test.
FIRE-4513	Il controllo segna come inutilizzata ogni regola con il contatore di pacchetti a zero. Su un'istanza appena avviata sono tutti a zero perché non è ancora arrivato traffico. Lo avverte lo stesso Lynis: una regola non scattata può benissimo essere in uso.
HRDN-7220	I compilatori servono nell'immagine per DKMS e per i moduli del kernel, quindi non si possono rimuovere. Si limitano invece a root con permessi 0750, che è ciò che verifica il controllo gemello HRDN-7222, e quello passa.
HTTP-6710	Dipende da dati che non esistono mentre l'immagine viene costruita; si risolve al primo avvio.
KRNL-6000	Il controllo confronta i sysctl con un elenco fisso pensato per il ferro. Questa immagine imposta i propri valori rafforzati e il kernel di AWS ne vincola altri; le differenze segnalate sono nostre decisioni, non dimenticanze.
LOGG-2154	Nessun server di log esterno viene incorporato, perché la destinazione dei log la sceglie l'acquirente, non noi. I log sono completi e locali, pronti a essere inviati dove preferisce.
LOGG-2190	La rotazione resta quella fornita dalla distribuzione ed è rivista servizio per servizio; il controllo si aspetta una disposizione precisa che non si adatta a un'immagine pensata per essere riconfigurata dopo l'acquisto.

ID DEL TEST	MOTIVO PER CUI NON SI APPLICA
MALW-3280	Questo controllo assegna punti solo agli antivirus commerciali. L'immagine include ClamAV, con firme aggiornate automaticamente, e ciò viene valutato da un controllo a parte: non impacchettiamo software commerciale di terzi solo per guadagnare un punto.
NAME-4028	Il dominio DNS non viene incorporato perché l'istanza lo riceve via DHCP dalla VPC dell'acquirente. Quello che scrivessimo qui verrebbe sovrascritto al primo avvio.
NAME-4404	Dipende da dati che non esistono mentre l'immagine viene costruita; si risolve al primo avvio.
SSH-7408	SSH resta sulla porta 22 perché è quella che si aspettano EC2 Instance Connect e gli strumenti di console. Cambiare porta non nasconde nulla a uno scanner; il brute force lo fermano l'autenticazione a chiave e fail2ban.
SSH-7440	SSH non fissa un elenco esplicito di utenti ammessi: l'acquirente crea i propri account su questa immagine e il nostro elenco lo lascerebbe fuori. L'accesso è già ristretto da autenticazione solo con chiave, nessun login di root e fail2ban.
TOOL-5002	Nessun agente di gestione della configurazione viene installato, di proposito: l'immagine è costruita con Ansible via SSH, che non lascia nulla in esecuzione dopo. Un demone in meno è una superficie d'attacco in meno.
USB-1000	Non si applica al modello di un'istanza cloud: ciò che verifica non esiste qui oppure è coperto dall'infrastruttura del provider.
USB-3000	Non si applica al modello di un'istanza cloud: ciò che verifica non esiste qui oppure è coperto dall'infrastruttura del provider.

L'elenco viene letto dal profilo Lynis incorporato nell'immagine stessa, non da un documento mantenuto a mano: quello che vedete qui è esattamente ciò che l'audit ha applicato.