LYNIS-SICHERHEITSAUDIT

Bericht zur Systemhärtung

Automatisiertes Sicherheitsaudit des Images, mit Lynis auf einer frisch provisionierten Instanz vor der Veröffentlichung ausgeführt.

HOST **ip-172-31-83-68**	BETRIEBSSYSTEM **Ubuntu 26.04 LTS**
KERNEL **7.0.0-1011-aws**	ARCHITEKTUR **arm64**
LYNIS-VERSION **3.1.7**	PROFIL **custom.prf**
DAUER **57s**	AUSGEFÜHRT VON **root**

Unsere Verpflichtung zur Härtung

Jedes von imaxe.cloud veröffentlichte Image ist standardmäßig gehärtet – zur Sicherheit derjenigen, die es produktiv einsetzen. Wir liefern keine nackte Distribution: Das System kommt mit einer Firewall, die standardmäßig blockiert, eingeschränktem SSH, gehärtetem Kernel und gehärteten Mount-Optionen, unbeaufsichtigten Sicherheitsupdates sowie installierten und laufenden Werkzeugen für Dateiintegrität, Rootkits, Malware und Auditing.

Dieser Bericht ist der Nachweis. Er wird automatisch auf einer frisch gebauten Instanz erzeugt, bevor das Image veröffentlicht wird, niemals von Hand bearbeitet und vollständig veröffentlicht – einschließlich allem, was das Audit nicht bewertet hat. Härtung ist Teil des Produkts, also reist das Audit, das sie misst, mit ihm.

HÄRTUNGSINDEX

0 Warnungen Zu behebende Probleme	**0** Vorschläge Erwägenswerte Verbesserungen
241 Durchgeführte Tests Ausgeführte Lynis-Sicherheitsprüfungen	**0** Aktive Plugins Zusätzliche Audit-Plugins

Fazit

Das System erreicht einen Härtungsindex von 100/100: eine stark gehärtete, produktionsreife Konfiguration.

1 Bewertung nach Kategorie

Aufschlüsselung des Audit-Ergebnisses nach Sicherheitsbereich, abgeleitet aus den Warnungen und Vorschlägen der jeweiligen Kategorie.

Kernel & Boot	100
Authentifizierung	100
Dateisystem & Integrität	100
Netzwerk & Firewall	100
SSH	100
Pakete & Werkzeuge	100

2 Warnungen

Befunde, die Lynis als Warnungen einstuft. Sie werden vor jeder Veröffentlichung geprüft und behoben.

TEST-ID	BESCHREIBUNG	SCHWEREGRAD
Keine Warnungen — das Audit fand keine Probleme dieser Stufe.		

3 Vorschläge

Empfehlungen von Lynis. Einige treffen auf Cloud-Images nicht zu oder sind bewusste Designentscheidungen.

TEST-ID	EMPFEHLUNG	KATEGORIE
Keine Vorschläge.		

4 Bewusst übersprungene Prüfungen

Das Image führt Lynis mit einem Profil aus, das 23 Prüfungen überspringt. Keine davon ist eine Härtungslücke: Es sind Prüfungen, die sich auf einem Cloud-Image nicht bewerten lassen, die bereits durch eine andere Maßnahme abgedeckt sind oder die von Daten abhängen, die erst mit laufender Instanz existieren. Jede wird mit ihrem Grund aufgeführt, damit die Auslassung nachprüfbar ist.

TEST-ID	GRUND, WARUM ES NICHT ZUTRIFFT
AUTH-9284	Die bemängelten Konten sind die Dienstkonten der Ubuntu-Basis (daemon, bin, sys…). Sie kommen ohne gültiges Passwort und ohne interaktive Shell — genau so soll es sein; die Prüfung liest diesen Normalzustand als Befund.
BOOT-5122	Es gibt kein GRUB-Passwort, weil es keine physische Konsole gibt, an der man es eingeben könnte: Eine EC2-Instanz startet unbeaufsichtigt, und ihre Konsole ist ein per IAM geschützter API-Aufruf. Das Passwort wäre nur ein Hindernis bei einer Rettung.
BOOT-5180	Fehlalarm bei diesem Image: Die Prüfung lässt sich hier nicht bewerten und ihr Ergebnis würde den tatsächlichen Systemzustand nicht widerspiegeln.

TEST-ID	GRUND, WARUM ES NICHT ZUTRIFFT
BOOT-5264	Fehlalarm bei diesem Image: Die Prüfung lässt sich hier nicht bewerten und ihr Ergebnis würde den tatsächlichen Systemzustand nicht widerspiegeln.
CRYP-7902	Hängt von Daten ab, die es beim Bau des Images noch nicht gibt; wird beim ersten Start aufgelöst.
DEB-0810	apt-listbugs ist interaktiv: Es hält ein Upgrade an, um einen Menschen zu fragen. Auf einem unbeaufsichtigten Image würde es die automatischen Sicherheitsupdates blockieren, die weit wichtiger sind.
FILE-6310	Das Image nutzt ein einziges Root-Volume — so werden Cloud-Instanzen vergrößert und gesichert. Was diese Prüfung wirklich will (dass /tmp, /dev/shm und /run keine Binärdateien ausführen und keine Geräte enthalten können), wird hier über gehärtete Mount-Optionen erreicht.
FILE-7524	Die Rechte entsprechen dem, was dieses Produkt braucht, und werden bei jedem Build von unserer eigenen Testsuite geprüft; die generische Prüfung markiert legitime Anwendungsdateien als Fehler.
FIRE-4512	Die Prüfung zählt iptables-Regeln und nennt eine kurze Liste "leer". Hier ist die erste Filterebene die AWS Security Group außerhalb der Instanz, und ufw sperrt alles Übrige standardmäßig — der Schutz existiert, er steht nur nicht dort, wo diese Prüfung nachsieht.
FIRE-4513	Die Prüfung markiert jede Regel mit Paketzähler null als ungenutzt. Auf einer frisch gestarteten Instanz sind alle Zähler null, weil noch kein Verkehr angekommen ist. Lynis selbst weist darauf hin: Nicht ausgelöste Regeln können sehr wohl in Gebrauch sein.
HRDN-7220	Compiler werden im Image für DKMS und Kernelmodule gebraucht und lassen sich nicht entfernen. Stattdessen sind sie mit 0750 auf root beschränkt — genau das prüft die Schwesterprüfung HRDN-7222, und die besteht.
HTTP-6710	Hängt von Daten ab, die es beim Bau des Images noch nicht gibt; wird beim ersten Start aufgelöst.
KRNL-6000	Die Prüfung vergleicht sysctl-Werte mit einer festen Liste, die von Bare Metal ausgeht. Dieses Image setzt eigene gehärtete Werte, andere gibt der AWS-Kernel vor; die gemeldeten Abweichungen sind unsere Entscheidungen, keine Versäumnisse.
LOGG-2154	Es wird kein externer Log-Server eingebacken, denn das Ziel der Logs wählt der Käufer, nicht wir. Die Protokolle sind vollständig und lokal, bereit zum Versand wohin auch immer.
LOGG-2190	Die Rotation bleibt so, wie die Distribution sie ausliefert, und wird dienstweise geprüft; die Prüfung erwartet ein bestimmtes Layout, das nicht zu einem Image passt, das nach dem Kauf umkonfiguriert werden soll.

TEST-ID	GRUND, WARUM ES NICHT ZUTRIFFT
MALW-3280	Diese Prüfung bewertet ausschließlich kommerzielle Antivirenprodukte. Das Image bringt ClamAV mit automatisch aktualisierten Signaturen mit, und das bewertet eine eigene Prüfung — wir bündeln keine kostenpflichtige Fremdsoftware, nur um einen Punkt zu gewinnen.
NAME-4028	Der DNS-Domainname wird nicht eingebacken, weil die Instanz ihn per DHCP aus der VPC des Käufers erhält. Was wir hier einträgen, würde beim ersten Start überschrieben.
NAME-4404	Hängt von Daten ab, die es beim Bau des Images noch nicht gibt; wird beim ersten Start aufgelöst.
SSH-7408	SSH bleibt auf Port 22, denn den erwarten EC2 Instance Connect und die Konsolenwerkzeuge. Ein anderer Port verbirgt vor einem Scanner nichts; Brute Force stoppen Schlüsselanmeldung und fail2ban.
SSH-7440	SSH legt keine feste Liste erlaubter Benutzer fest: Der Käufer legt auf diesem Image eigene Konten an, und unsere Liste würde ihn aussperren. Der Zugang ist bereits durch reine Schlüsselanmeldung, kein Root-Login und fail2ban beschränkt.
TOOL-5002	Es wird bewusst kein Konfigurationsmanagement-Agent installiert: Das Image wird mit Ansible über SSH gebaut, das danach nichts laufen lässt. Ein Dienst weniger ist eine Angriffsfläche weniger.
USB-1000	Trifft auf das Modell einer Cloud-Instanz nicht zu: Was geprüft wird, existiert hier nicht oder wird von der Infrastruktur des Anbieters übernommen.
USB-3000	Trifft auf das Modell einer Cloud-Instanz nicht zu: Was geprüft wird, existiert hier nicht oder wird von der Infrastruktur des Anbieters übernommen.

Diese Liste wird aus dem im Image selbst hinterlegten Lynis-Profil gelesen, nicht aus einem von Hand gepflegten Dokument: Was hier steht, ist genau das, was das Audit angewendet hat.