LYNIS सुरक्षा ऑडिट

सिस्टम हार्डनिंग रिपोर्ट

इमेज का स्वचालित सुरक्षा ऑडिट, प्रकाशन से पहले नए प्रोविज़न किए गए इंस्टेंस पर Lynis से चलाया गया।

होस्ट **ip-172-31-83-68**	ऑपरेटिंग सिस्टम **Ubuntu 26.04 LTS**
कर्नेल **7.0.0-1011-aws**	आर्किटेक्चर **arm64**
LYNIS संस्करण **3.1.7**	प्रोफ़ाइल **custom.prf**
अवधि **57s**	द्वारा चलाया गया **root**

हार्डनिंग को लेकर हमारी प्रतिबद्धता

imaxe.cloud जो भी इमेज प्रकाशित करती है, वह डिफ़ॉल्ट रूप से हार्डन की हुई होती है — उसे चलाने वाले की सुरक्षा के लिए। हम कोई नंगी डिस्ट्रिब्यूशन नहीं सौंपते: सिस्टम डिफ़ॉल्ट रूप से मना करने वाले फ़ायरवॉल, सीमित SSH, कड़े किए गए कर्नेल और माउंट विकल्पों, स्वचालित सुरक्षा अपडेट, तथा फ़ाइल-अखंडता, रूटकिट, मैलवेयर और ऑडिट उपकरणों के साथ आता है, जो स्थापित और चालू रहते हैं।

यह रिपोर्ट ही प्रमाण है। इमेज प्रकाशित करने से पहले, नई बनी इंस्टेंस पर यह स्वतः तैयार होती है, कभी हाथ से संपादित नहीं की जाती, और पूरी की पूरी प्रकाशित होती है — उस सब समेत जिसे ऑडिट ने अंक नहीं दिए। हार्डनिंग उत्पाद का हिस्सा है, इसलिए उसे मापने वाला ऑडिट भी उसके साथ ही चलता है।

हार्डनिंग सूचकांक

0	0
चेतावनियाँ	सुझाव
सुधारने योग्य समस्याएँ	विचार करने योग्य सुधार
241	**0**
किए गए परीक्षण	सक्रिय प्लगइन
चलाई गईं Lynis सुरक्षा जाँचें	अतिरिक्त ऑडिट प्लगइन

निष्कर्ष

सिस्टम 100/100 का हार्डनिंग सूचकांक प्राप्त करता है: उत्पादन के लिए तैयार, अत्यधिक सुदृढ़ कॉन्फ़िगरेशन।

1 श्रेणी के अनुसार स्कोर

सुरक्षा क्षेत्र के अनुसार ऑडिट परिणाम का विवरण, प्रत्येक क्षेत्र की चेतावनियों और सुझावों से व्युत्पन्न।

कर्नेल और बूट	100
प्रमाणीकरण	100
फ़ाइल सिस्टम और अखंडता	100
नेटवर्क और फ़ायरवॉल	100
SSH	100
पैकेज और उपकरण	100
लॉगिंग और समय	100
हार्डनिंग और मैलवेयर	100

2 चेतावनियाँ

वे निष्कर्ष जिन्हें Lynis चेतावनी के रूप में चिह्नित करता है। प्रत्येक रिलीज़ से पहले इनकी समीक्षा और समाधान किया जाता है।

टेस्ट ID	विवरण	गंभीरता
कोई चेतावनी नहीं — ऑडिट को इस स्तर की कोई समस्या नहीं मिली।		

3 सुझाव

Lynis की सिफ़ारिशें। कुछ क्लाउड इमेज पर लागू नहीं होतीं या जानबूझकर लिए गए डिज़ाइन निर्णय हैं।

टेस्ट ID	सिफ़ारिश	श्रेणी
कोई सुझाव नहीं।		

4 जानबूझकर छोड़ी गई जाँचें

यह इमेज Lynis को ऐसे प्रोफ़ाइल के साथ चलाती है जो 23 जाँचें छोड़ देता है। इनमें से कोई भी हार्डनिंग की कमी नहीं है: ये वे जाँचें हैं जिनका मूल्यांकन क्लाउड इमेज पर संभव नहीं, या जिन्हें कोई दूसरा नियंत्रण पहले ही ढक लेता है, या जो ऐसे डेटा पर निर्भर हैं जो इंस्टेंस चलने पर ही बनता है। हर एक अपने कारण के साथ सूचीबद्ध है, ताकि यह छूट भी जाँची जा सके।

टेस्ट ID	लागू न होने का कारण
AUTH-9284	यह जिन खातों की ओर इशारा करती है वे Ubuntu आधार के सेवा-खाते हैं (daemon, bin, sys...)। वे बिना वैध पासवर्ड और बिना इंटरैक्टिव शेल के आते हैं, जो ठीक वही है जो चाहिए; जाँच इस सामान्य स्थिति को ही समस्या पढ़ लेती है।
BOOT-5122	GRUB पासवर्ड इसलिए नहीं है कि उसे टाइप करने के लिए कोई भौतिक कंसोल ही नहीं: EC2 इंस्टेंस अपने आप बूट होता है और उसका कंसोल IAM से सुरक्षित एक API कॉल है। पासवर्ड सिर्फ़ बचाव-कार्य में अड़चन बनता।
BOOT-5180	इस इमेज पर ग़लत सकारात्मक: यह जाँच यहाँ मूल्यांकित नहीं की जा सकती और इसका परिणाम सिस्टम की वास्तविक स्थिति नहीं दर्शाएगा।
BOOT-5264	इस इमेज पर ग़लत सकारात्मक: यह जाँच यहाँ मूल्यांकित नहीं की जा सकती और इसका परिणाम सिस्टम की वास्तविक स्थिति नहीं दर्शाएगा।
CRYP-7902	ऐसे डेटा पर निर्भर जो इमेज बनाते समय होता ही नहीं; पहली बूट पर तय होता है।
DEB-0810	apt-listbugs संवादात्मक है: यह अपग्रेड रोककर किसी व्यक्ति से पूछता है। बिना निगरानी वाली इमेज पर यह स्वचालित सुरक्षा अपडेट रोक देता, जो कहीं ज़्यादा ज़रूरी हैं।

टेस्ट ID	लागू न होने का कारण
FILE-6310	इमेज एक ही रूट वॉल्यूम पर चलती है — क्लाउड इंस्टेंस इसी रूप में बड़ा किया जाता और स्नैपशॉट लिया जाता है। यह जाँच असल में जो चाहती है — कि /tmp, /dev/shm और /run न बाइनरी चला सकें, न डिवाइस रख सकें — वह यहाँ कड़े माउंट विकल्पों से हासिल है।
FILE-7524	अनुमतियाँ वही हैं जो इस उत्पाद को चाहिए और हर बिल्ड पर हमारी अपनी टेस्ट-श्रृंखला उन्हें जाँचती है; सामान्य जाँच अनुप्रयोग की वैध फ़ाइलों को ही ग़लती मान लेती है।
FIRE-4512	यह जाँच iptables के नियम गिनती है और छोटी सूची को «खाली» कह देती है। यहाँ पहली छननी इंस्टेंस के बाहर AWS का सिक्योरिटी ग्रुप है, और बाकी सब कुछ ufw डिफ़ॉल्ट रूप से बंद रखता है: सुरक्षा मौजूद है, बस वहाँ लिखी नहीं जहाँ यह जाँच देखती है।
FIRE-4513	यह जाँच हर उस नियम को «अप्रयुक्त» बता देती है जिसका पैकेट काउंटर शून्य हो। अभी-अभी चालू हुए इंस्टेंस पर सभी काउंटर शून्य ही होते हैं, क्योंकि ट्रैफ़िक आया ही नहीं। ख़ुद Lynis चेताता है: जो नियम चला नहीं, वह भी पूरी तरह प्रयोग में हो सकता है।
HRDN-7220	कंपाइलर इमेज में DKMS और कर्नेल मॉड्यूल के लिए चाहिए, इसलिए हटाए नहीं जा सकते। उन्हें 0750 अनुमतियों के साथ केवल root तक सीमित किया जाता है — यही इसकी सहोदर जाँच HRDN-7222 परखती है, और वह पास होती है।
HTTP-6710	ऐसे डेटा पर निर्भर जो इमेज बनाते समय होता ही नहीं; पहली बूट पर तय होता है।
KRNL-6000	यह जाँच sysctl मानों की तुलना एक तयशुदा सूची से करती है, जो असली हार्डवेयर मानकर बनी है। यह इमेज अपने कड़े मान ख़ुद तय करती है और कुछ AWS का कर्नेल तय करता है; जो अंतर यह बताती है वे हमारे निर्णय हैं, चूक नहीं।
LOGG-2154	कोई बाहरी लॉग सर्वर इमेज में नहीं पकाया जाता, क्योंकि लॉग कहाँ जाएँ यह खरीदार तय करता है, हम नहीं। लॉग पूरे और स्थानीय हैं, जहाँ चाहें वहाँ भेजने को तैयार।
LOGG-2190	रोटेशन वैसा ही रहता है जैसा वितरण देता है और सेवा-दर-सेवा जाँचा जाता है; यह जाँच एक ख़ास ढाँचे की अपेक्षा करती है जो ख़रीद के बाद दोबारा कॉन्फ़िगर होने वाली इमेज पर फिट नहीं बैठता।
MALW-3280	यह जाँच केवल व्यावसायिक एंटीवायरस उत्पादों को अंक देती है। इमेज में ClamAV है, जिसके सिग्नेचर अपने आप अपडेट होते हैं, और उसे अलग जाँच अंक देती है — एक अंक के लिए हम तीसरे पक्ष का सशुल्क सॉफ़्टवेयर साथ नहीं बाँधेंगे।
NAME-4028	DNS डोमेन इमेज में नहीं पकाया जाता, क्योंकि इंस्टेंस उसे खरीदार की VPC से DHCP द्वारा पाता है। यहाँ हम जो भी लिखते, पहले बूट पर ही मिट जाता।
NAME-4404	ऐसे डेटा पर निर्भर जो इमेज बनाते समय होता ही नहीं; पहली बूट पर तय होता है।
SSH-7408	SSH पोर्ट 22 पर ही रहता है, क्योंकि EC2 Instance Connect और कंसोल उपकरण यही अपेक्षा करते हैं। पोर्ट बदलने से स्कैनर से कुछ नहीं छिपता; ब्रूट-फ़ोर्स को कुंजी प्रमाणीकरण और fail2ban रोकते हैं।
SSH-7440	SSH अनुमत उपयोगकर्ताओं की कोई निश्चित सूची तय नहीं करता: खरीदार इस इमेज के ऊपर अपने खाते बनाता है, और हमारी सूची उसी को बाहर कर देती। पहुँच पहले से ही केवल-कुंजी प्रमाणीकरण, रूट लॉगिन पर रोक और fail2ban से सीमित है।

टेस्ट ID	लागू न होने का कारण
TOOL-5002	कोई कॉन्फ़िगरेशन-प्रबंधन एजेंट जानबूझकर स्थापित नहीं किया जाता: इमेज SSH के ज़रिये Ansible से बनती है, जो बाद में कुछ भी चलता हुआ नहीं छोड़ता। एक डेमॉन कम यानी एक हमला-सतह कम।
USB-1000	क्लाउड इंस्टेंस के ढाँचे पर लागू नहीं: यह जिसकी जाँच करता है वह यहाँ है ही नहीं, या उसे प्रदाता का बुनियादी ढाँचा सँभालता है।
USB-3000	क्लाउड इंस्टेंस के ढाँचे पर लागू नहीं: यह जिसकी जाँच करता है वह यहाँ है ही नहीं, या उसे प्रदाता का बुनियादी ढाँचा सँभालता है।

यह सूची इमेज के भीतर ही पकाए गए Lynis प्रोफ़ाइल से पढ़ी जाती है, हाथ से रखे किसी दस्तावेज़ से नहीं: यहाँ जो दिख रहा है, ऑडिट ने ठीक वही लागू किया था।