LYNIS سیکیورٹی آڈٹ

سسٹم ہارڈننگ رپورٹ

امیج کا خودکار سیکیورٹی آڈٹ، اشاعت سے پہلے نئے فراہم کردہ انسٹینس پر Lynis کے ذریعے چلایا گیا۔

ہوسٹ **ip-172-31-83-68**	آپریٹنگ سسٹم **Ubuntu 26.04 LTS**
کرنل **7.0.0-1011-aws**	آرکیٹیکچر **arm64**
LYNIS ورژن **3.1.7**	پروفائل **custom.prf**
دورانیہ **57s**	چلایا گیا بذریعہ **root**

ہارڈننگ سے متعلق ہمارا عہد

imaxe.cloud جو بھی امیج شائع کرتی ہے وہ بطورِ ڈیفالٹ ہارڈن شدہ ہوتی ہے، تاکہ اسے چلانے والے کی سلامتی محفوظ رہے۔ ہم کوئی خالی ڈسٹری بیوشن حوالے نہیں کرتے: نظام ڈیفالٹ پر انکار کرنے والے فائروال، محدود SSH، سخت کیے گئے کرنل اور ماؤنٹ آپشنز، خودکار سیکیورٹی اپ ڈیٹس، اور فائل سالمیت، روٹ کٹ، مالویئر اور آڈٹ کے آلات کے ساتھ آتا ہے، جو نصب اور چالو حالت میں ہوتے ہیں۔

یہ رپورٹ ہی ثبوت ہے۔ امیج شائع کرنے سے پہلے، تازہ بنی ہوئی انسٹینس پر یہ خودکار طور پر تیار ہوتی ہے، کبھی ہاتھ سے تبدیل نہیں کی جاتی، اور مکمل شائع کی جاتی ہے — بشمول ہر اُس چیز کے جسے آڈٹ نے نمبر نہیں دیے۔ ہارڈننگ مصنوعات کا حصہ ہے، اس لیے اسے ناپنے والا آڈٹ بھی اسی کے ساتھ سفر کرتا ہے۔

ہارڈننگ انڈیکس

0 انتباہات حل طلب مسائل	**0** تجاویز قابلِ غور بہتریاں
241 انجام شدہ ٹیسٹ چلائی گئیں Lynis سیکیورٹی جانچیں	**0** فعال پلگ اِن اضافی آڈٹ پلگ اِن

نتیجہ

سسٹم 100/100 کا ہارڈننگ انڈیکس حاصل کرتا ہے: پروڈکشن کے لیے تیار، مضبوطی سے محفوظ کردہ ترتیب۔

1 زمرے کے لحاظ سے اسکور

سیکیورٹی شعبے کے لحاظ سے آڈٹ نتائج کی تفصیل، ہر شعبے کے انتباہات اور تجاویز سے اخذ کردہ۔

کرنل اور بوٹ	100
توثیق	100
فائل سسٹم اور سالمیت	100
نیٹ ورک اور فائروال	100
SSH	100
پیکیجز اور اوزار	100
لاگنگ اور وقت	100
ہارڈننگ اور مالویئر	100

2 انتباہات

وہ نتائج جنہیں Lynis انتباہ کے طور پر نشان زد کرتا ہے۔ ہر اجراء سے پہلے ان کا جائزہ اور ازالہ کیا جاتا ہے۔

ٹیسٹ ID	تفصیل	شدت
کوئی انتباہ نہیں — آڈٹ کو اس درجے کا کوئی مسئلہ نہیں ملا۔		

3 تجاویز

Lynis کی سفارشات۔ کچھ کلاؤڈ امیجز پر لاگو نہیں ہوتیں یا دانستہ ڈیزائن فیصلے ہیں۔

ٹیسٹ ID	سفارش	زمرہ
کوئی تجویز نہیں۔		

4 جان بوجھ کر چھوڑی گئی جانچیں

یہ امیج Lynis کو ایسے پروفائل کے ساتھ چلاتی ہے جو 23 جانچیں چھوڑ دیتا ہے۔ ان میں سے کوئی بھی ہارڈننگ کا خلا نہیں: یہ وہ جانچیں ہیں جن کا جائزہ کلاؤڈ امیج پر ممکن نہیں، یا جنہیں کوئی دوسرا کنٹرول پہلے ہی ڈھانپ چکا ہے، یا جو ایسے ڈیٹا پر منحصر ہیں جو انسٹینس چلنے کے بعد ہی وجود میں آتا ہے۔ ہر ایک اپنی وجہ کے ساتھ درج ہے تاکہ یہ چھوٹ بھی جانچی جا سکے۔

ٹیسٹ ID	لاگو نہ ہونے کی وجہ
AUTH-9284	جن کھاتوں کی یہ نشاندہی کرتی ہے وہ اُبنٹو بنیاد کے سروس کھاتے ہیں (daemon، bin، sys...)۔ وہ بغیر مؤثر پاس ورڈ اور بغیر تعاملی شیل کے آتے ہیں، جو بالکل مطلوب ہے؛ جانچ اسی معمول کی حالت کو مسئلہ سمجھ لیتی ہے۔
BOOT-5122	GRUB کا پاس ورڈ اس لیے نہیں کہ اسے ٹائپ کرنے کے لیے کوئی طبیعی کنسول ہی نہیں: EC2 انسٹینس خود بخود بوٹ ہوتا ہے اور اس کا کنسول IAM سے محفوظ ایک API کال ہے۔ پاس ورڈ صرف بحالی کے کام میں رکاوٹ بنتا۔
BOOT-5180	اس امیج پر غلط اشارہ: یہ جانچ یہاں پرکھی نہیں جا سکتی اور اس کا نتیجہ نظام کی اصل حالت ظاہر نہیں کرے گا۔
BOOT-5264	اس امیج پر غلط اشارہ: یہ جانچ یہاں پرکھی نہیں جا سکتی اور اس کا نتیجہ نظام کی اصل حالت ظاہر نہیں کرے گا۔
CRYP-7902	ایسے ڈیٹا پر منحصر ہے جو امیج بناتے وقت موجود نہیں ہوتا؛ پہلے بوٹ پر طے ہو جاتا ہے۔
DEB-0810	apt-listbugs تعاملی ہے: یہ اپ گریڈ روک کر کسی انسان سے پوچھتا ہے۔ بغیر نگرانی چلنے والی امیج پر یہ خودکار سیکیورٹی اپ ڈیٹس روک دیتا، جو کہیں زیادہ اہم ہیں۔

ٹیسٹ ID	لاگو نہ ہونے کی وجہ
FILE-6310	امیج ایک ہی روٹ والیوم استعمال کرتی ہے — کلاؤڈ انسٹینس اسی شکل میں بڑھائی اور اس کا سنیپ شاٹ لیا جاتا ہے۔ یہ جانچ اصل میں جو چاہتی ہے — کہ /dev/shm، tmp اور /run نہ بائنری چلا سکیں نہ ڈیوائسز رکھ سکیں — وہ یہاں سخت ماؤنٹ آپشنز سے حاصل ہے۔
FILE-7524	اجازتیں وہی ہیں جو اس مصنوعات کو درکار ہیں اور ہر بلڈ پر ہماری اپنی جانچوں سے پرکھی جاتی ہیں؛ عمومی جانچ ایپلیکیشن کی جائز فائلوں کو ہی غلطی سمجھ لیتی ہے۔
FIRE-4512	یہ جانچ iptables کے قواعد گنتی ہے اور مختصر فہرست کو «خالی» کہہ دیتی ہے۔ یہاں پہلی چھلنی انسٹینس سے باہر AWS کا سیکیورٹی گروپ ہے، اور باقی سب کچھ ufw بطورِ ڈیفالٹ بند رکھتا ہے: تحفظ موجود ہے، بس وہاں لکھا نہیں جہاں یہ جانچ دیکھتی ہے۔
FIRE-4513	یہ جانچ ہر اُس قاعدے کو «غیر استعمال شدہ» قرار دیتی ہے جس کا پیکٹ شمار صفر ہو۔ ابھی ابھی چلنے والے انسٹینس پر سب شمار صفر ہی ہوتے ہیں، کیونکہ ٹریفک آیا ہی نہیں۔ خود Lynis خبردار کرتا ہے: جو قاعدہ چلا نہیں، وہ بھی بخوبی زیرِ استعمال ہو سکتا ہے۔
HRDN-7220	امیج میں DKMS اور کرنل ماڈیولز کے لیے کمپائلر درکار ہیں، سو انہیں ہٹایا نہیں جا سکتا۔ اس کے بجائے 0750 اجازتوں کے ساتھ انہیں صرف root تک محدود کیا جاتا ہے — یہی اس کی ہم جولی جانچ HRDN-7222 پرکھتی ہے، اور وہ کامیاب ہوتی ہے۔
HTTP-6710	ایسے ڈیٹا پر منحصر ہے جو امیج بناتے وقت موجود نہیں ہوتا؛ پہلے بوٹ پر طے ہو جاتا ہے۔
KRNL-6000	یہ جانچ sysctl اقدار کا موازنہ ایک مقررہ فہرست سے کرتی ہے جو اصل ہارڈ ویئر کو ذہن میں رکھ کر بنی ہے۔ یہ امیج اپنی سخت اقدار خود طے کرتی ہے اور کچھ AWS کا کرنل طے کرتا ہے؛ جو فرق یہ بتاتی ہے وہ ہمارے فیصلے ہیں، بھول نہیں۔
LOGG-2154	کوئی بیرونی لاگ سرور امیج میں شامل نہیں کیا جاتا، کیونکہ لاگ کہاں جائیں یہ خریدار طے کرتا ہے، ہم نہیں۔ لاگ مکمل اور مقامی ہیں، جہاں چاہے بھیجنے کے لیے تیار۔
LOGG-2190	روٹیشن ویسی ہی رہتی ہے جیسی تقسیم فراہم کرتی ہے اور ہر سروس کے لحاظ سے دیکھی جاتی ہے؛ جانچ ایک مخصوص ترتیب کی توقع رکھتی ہے جو خریداری کے بعد دوبارہ ترتیب دی جانے والی امیج پر پوری نہیں اترتی۔
MALW-3280	یہ جانچ صرف تجارتی اینٹی وائرس مصنوعات کو نمبر دیتی ہے۔ امیج میں ClamAV موجود ہے، جس کے دستخط خودکار طور پر تازہ ہوتے ہیں، اور اسے ایک الگ جانچ نمبر دیتی ہے: ایک نمبر کے لیے ہم فریقِ ثالث کا معاوضہ والا سافٹ ویئر ساتھ نہیں باندھیں گے۔
NAME-4028	DNS ڈومین امیج میں شامل نہیں کیا جاتا، کیونکہ انسٹینس اسے خریدار کی VPC سے DHCP کے ذریعے پاتا ہے۔ ہم یہاں جو بھی لکھتے، پہلے بوٹ پر مٹ جاتا۔
NAME-4404	ایسے ڈیٹا پر منحصر ہے جو امیج بناتے وقت موجود نہیں ہوتا؛ پہلے بوٹ پر طے ہو جاتا ہے۔
SSH-7408	SSH پورٹ 22 پر ہی رہتا ہے، کیونکہ EC2 Instance Connect اور کنسول کے آلات اسی کی توقع رکھتے ہیں۔ پورٹ بدلنے سے اسکینر سے کچھ نہیں چھپتا؛ بلا امتیاز حملوں کو کلید سے تصدیق اور fail2ban روکتے ہیں۔
SSH-7440	SSH اجازت یافتہ صارفین کی کوئی متعین فہرست طے نہیں کرتا: خریدار اس امیج پر اپنے کھاتے بناتا ہے، اور ہماری فہرست اسی کو باہر کر دیتی۔ رسائی پہلے ہی صرف کلید سے تصدیق، روٹ لاگ اِن کی ممانعت اور fail2ban سے محدود ہے۔

ٹیسٹ ID	لاگو نہ ہونے کی وجہ
TOOL-5002	کوئی کنفیگریشن مینجمنٹ ایجنٹ جان بوجھ کر نصب نہیں کیا جاتا: امیج SSH کے ذریعے Ansible سے بنتی ہے، جو بعد میں کچھ بھی چلتا ہوا نہیں چھوڑتا۔ ایک ڈیمن کم یعنی ایک حملہ سطح کم۔
USB-1000	کلاؤڈ انسٹینس کے ماڈل پر لاگو نہیں: یہ جس چیز کو جانچتا ہے وہ یہاں موجود ہی نہیں، یا اسے فراہم کنندہ کا بنیادی ڈھانچہ سنبھالتا ہے۔
USB-3000	کلاؤڈ انسٹینس کے ماڈل پر لاگو نہیں: یہ جس چیز کو جانچتا ہے وہ یہاں موجود ہی نہیں، یا اسے فراہم کنندہ کا بنیادی ڈھانچہ سنبھالتا ہے۔

یہ فہرست خود امیج کے اندر پکائے گئے Lynis پروفائل سے پڑھی جاتی ہے، ہاتھ سے رکھی کسی دستاویز سے نہیں:
یہاں جو نظر آ رہا ہے، آڈٹ نے بالکل وہی لاگو کیا تھا۔