

LYNIS নিরাপত্তা অডিট

সিস্টেম হার্ডেনিং প্রতিবেদন

ইমেজের স্বয়ংক্রিয় নিরাপত্তা অডিট, প্রকাশের আগে সদ্য প্রভিশন করা ইনস্ট্যান্সে Lynis দিয়ে চালানো হয়েছে।

হোস্ট ip-172-31-83-68	অপারেটিং সিস্টেম Ubuntu 26.04 LTS
কার্নেল 7.0.0-1011-aws	আর্কিটেকচার arm64
LYNIS সংস্করণ 3.1.7	প্রোফাইল custom.prf
সময়কাল 57s	চালিয়েছে root

হার্ডেনিং নিয়ে আমাদের অঙ্গীকার

imaxe.cloud যত ইমেজ প্রকাশ করে, প্রতিটিই ডিফল্টভাবে হার্ডেন করা — যিনি এটি প্রোডাকশনে চালাবেন, তাঁর নিরাপত্তার জন্য। আমরা খালি ডিস্ট্রিবিউশন হাতে ধরিয়ে দিই না: সিস্টেম আসে ডিফল্ট প্রত্যাখ্যানকারী ফায়ারওয়াল, সীমিত SSH, কড়া করা কার্নেল ও মাউন্ট অপশন, স্বয়ংক্রিয় নিরাপত্তা আপডেট এবং ফাইল-অখণ্ডতা, রুটকিট, ম্যালওয়্যার ও অডিট সরঞ্জাম ইনস্টল ও চালু অবস্থায়।

এই প্রতিবেদনই তার প্রমাণ। ইমেজ প্রকাশের আগে, সদ্য তৈরি একটি ইনস্ট্যান্সে এটি স্বয়ংক্রিয়ভাবে তৈরি হয়, কখনও হাতে সম্পাদনা করা হয় না, এবং পুরোটাই প্রকাশ করা হয় — অডিট যা কিছুতে নম্বর দেয়নি তা-সহ। হার্ডেনিং পণ্যেরই অংশ, তাই যে অডিট তা মাপে সেটিও পণ্যের সঙ্গেই যায়।



হার্ডেনিং সূচক

0

সতর্কবার্তা

সমাধানযোগ্য সমস্যা

0

পরামর্শ

বিবেচনাযোগ্য উন্নতি

241

সম্পাদিত পরীক্ষা

চালানো Lynis নিরাপত্তা পরীক্ষা

0

সক্রিয় প্লাগইন

অতিরিক্ত অডিট প্লাগইন



সিদ্ধান্ত

সিস্টেমটি 100/100 হার্ডেনিং সূচক অর্জন করেছে: উৎপাদনের জন্য প্রস্তুত, দৃঢ়ভাবে সুরক্ষিত কনফিগারেশন।

1 বিভাগ অনুযায়ী স্কোর

নিরাপত্তা ক্ষেত্র অনুযায়ী অডিট ফলাফলের বিশ্লেষণ, প্রতিটি ক্ষেত্রের সতর্কবার্তা ও পরামর্শ থেকে নির্ণীত।

কার্নেল ও বুট		100
প্রমাণীকরণ		100
ফাইল সিস্টেম ও অখণ্ডতা		100
নেটওয়ার্ক ও ফায়ারওয়াল		100
SSH		100
প্যাকেজ ও সরঞ্জাম		100
লগিং ও সময়		100

2 সতর্কবার্তা

Lynis যেসব বিষয় সতর্কবার্তা হিসেবে চিহ্নিত করে। প্রতিটি প্রকাশের আগে এগুলো পর্যালোচনা ও সমাধান করা হয়।

টেস্ট ID	বিবরণ	গুরুত্ব
কোনও সতর্কবার্তা নেই — অডিটে এই স্তরের কোনও সমস্যা পাওয়া যায়নি।		

3 পরামর্শ

Lynis-এর সুপারিশ। কিছু ক্লাউড ইমেজে প্রযোজ্য নয় বা ইচ্ছাকৃত ডিজাইন সিদ্ধান্ত।

টেস্ট ID	সুপারিশ	বিভাগ
কোনও পরামর্শ নেই।		

4 ইচ্ছাকৃতভাবে বাদ দেওয়া পরীক্ষা

ইমেজটি Lynis চালায় এমন একটি প্রোফাইল দিয়ে, যা 23টি পরীক্ষা বাদ দেয়। এর কোনোটিই হার্ডেনিংয়ের ফাঁক নয়: এগুলো এমন পরীক্ষা যা ক্লাউড ইমেজে মূল্যায়ন করা যায় না, কিংবা অন্য একটি নিয়ন্ত্রণ আগেই ঢেকে দিয়েছে, কিংবা যা এমন তথ্যের উপর নির্ভরশীল যা ইনস্ট্যান্স চালু হলেই কেবল তৈরি হয়। প্রতিটির সঙ্গে কারণ দেওয়া আছে, যাতে বাদ দেওয়াটাও যাচাই করা যায়।

টেস্ট ID	প্রযোজ্য না হওয়ার কারণ
AUTH-9284	এটি যেসব অ্যাকাউন্টের কথা বলে সেগুলো Ubuntu ভিত্তির সেবা-অ্যাকাউন্ট (daemon, bin, sys...)। বৈধ পাসওয়ার্ড ছাড়া আর ইন্টারঅ্যাকটিভ শেল ছাড়াই সেগুলো আসে, যা ঠিক কাম্য; পরীক্ষাটি এই স্বাভাবিক অবস্থাকেই সমস্যা ধরে নেয়।
B00T-5122	GRUB পাসওয়ার্ড নেই, কারণ তা টাইপ করার মতো কোনো ভৌত কনসোলই নেই: EC2 ইনস্ট্যান্স নিজে নিজেই বুট করে, আর তার কনসোল হলো IAM-সুরক্ষিত একটি API কল। পাসওয়ার্ড কেবল উদ্ধারকাজে বাধা হতো।
B00T-5180	এই ইমেজে ভুল শনাক্তকরণ: পরীক্ষাটি এখানে মূল্যায়নযোগ্য নয় এবং এর ফল সিস্টেমের প্রকৃত অবস্থা তুলে ধরবে না।
B00T-5264	এই ইমেজে ভুল শনাক্তকরণ: পরীক্ষাটি এখানে মূল্যায়নযোগ্য নয় এবং এর ফল সিস্টেমের প্রকৃত অবস্থা তুলে ধরবে না।

টেস্ট ID	প্রযোজ্য না হওয়ার কারণ
CRYP-7902	এমন তথ্যের উপর নির্ভরশীল যা ইমেজ তৈরির সময় থাকে না; প্রথম বুটেই তা নির্ধারিত হয়।
DEB-0810	apt-listbugs ইন্টারঅ্যাকটিভ: আপগ্রেড থামিয়ে মানুষকে প্রশ্ন করে। তত্ত্বাবধানহীন ইমেজে এটি স্বয়ংক্রিয় নিরাপত্তা হালনাগাদ আটকে দিত, যা অনেক বেশি জরুরি।
FILE-6310	ইমেজ একটিমাত্র রুট ভলিউম ব্যবহার করে — ক্লাউড ইনস্ট্যান্স এভাবেই বড় করা হয় ও স্ল্যাপশট নেওয়া হয়। এই পরীক্ষা আসলে যা চায় — /tmp, /dev/shm আর /run যেন বাইনারি চালাতে বা ডিভাইস রাখতে না পারে — এখানে তা কড়া মাউন্ট অপশন দিয়েই অর্জিত।
FILE-7524	অনুমতিগুলো এই পণ্যের প্রয়োজন মেনেই দেওয়া এবং প্রতিটি বিল্ডে আমাদের নিজস্ব টেস্ট-সেট তা যাচাই করে; সাধারণ পরীক্ষাটি অ্যান্লিকেশনের বৈধ ফাইলকেই ভুল বলে চিহ্নিত করে।
FIRE-4512	এই পরীক্ষা iptables-এর নিয়ম গোনে আর ছোট তালিকাকে «ফাঁকা» বলে ধরে নেয়। এখানে প্রথম ছাঁকনি ইনস্ট্যান্সের বাইরে AWS-এর সিকিউরিটি গ্রুপ, আর বাকি সব ufw ডিফল্টেই বন্ধ রাখে: সুরক্ষা আছে, কেবল সেটি সেখানে লেখা নেই যেখানে এই পরীক্ষা তাকায়।
FIRE-4513	যে নিয়মের প্যাকেট-গণনা শূন্য, এই পরীক্ষা তাকেই «অব্যবহৃত» বলে চিহ্নিত করে। সদ্য চালু হওয়া ইনস্ট্যান্সে সব গণনাই শূন্য, কারণ এখনও কোনো ট্রাফিক আসেনি। Lynis নিজেই সতর্ক করে: না-চলা নিয়মও দিব্যি ব্যবহারে থাকতে পারে।
HRDN-7220	DKMS ও কার্নেল মডিউলের জন্য ইমেজে কম্পাইলার দরকার, তাই সরানো যায় না। বদলে 0750 অনুমতি দিয়ে সেগুলো কেবল root-এর জন্য সীমিত রাখা হয় — এটিই যাচাই করে সহোদর পরীক্ষা HRDN-7222, আর সেটি উতরে যায়।
HTTP-6710	এমন তথ্যের উপর নির্ভরশীল যা ইমেজ তৈরির সময় থাকে না; প্রথম বুটেই তা নির্ধারিত হয়।
KRNL-6000	এই পরীক্ষা sysctl মানগুলো মেলায় এমন একটি নির্দিষ্ট তালিকার সঙ্গে, যা আসল যন্ত্রপাতি ধরে নিয়ে বানানো। এই ইমেজ নিজের কড়া মান বসায়, আর কিছু ঠিক করে দেয় AWS-এর কার্নেল; যে পার্থক্য এটি জানায় তা আমাদের সিদ্ধান্ত, ভুলে যাওয়া নয়।
LOGG-2154	কোনো বাহ্যিক লগ সার্ভার ইমেজে বসানো হয় না, কারণ লগ কোথায় যাবে তা ক্রেতার সিদ্ধান্ত, আমাদের নয়। লগ সম্পূর্ণ ও স্থানীয়ভাবে রাখা, যেখানে খুশি পাঠানোর জন্য প্রস্তুত।
LOGG-2190	রোটেশন ডিস্ট্রিবিউশন যেভাবে দেয় সেভাবেই রাখা হয় এবং সেবা ধরে ধরে দেখা হয়; পরীক্ষাটি একটি নির্দিষ্ট বিন্যাস আশা করে, যা কেনার পরে নতুন করে সাজানোর জন্য বানানো ইমেজে খাটে না।
MALW-3280	এই পরীক্ষা কেবল বাণিজ্যিক অ্যান্টিভাইরাস পণ্যকেই নম্বর দেয়। ইমেজে ClamAV আছে, যার সিগনেচার আপনাআপনি হালনাগাদ হয়, আর সেটির নম্বর দেয় আলাদা একটি পরীক্ষা — একটি নম্বরের জন্য আমরা তৃতীয় পক্ষের সশুল্ক সফটওয়্যার জুড়ে দেব না।
NAME-4028	DNS ডোমেন ইমেজে বসানো হয় না, কারণ ইনস্ট্যান্স সেটি ক্রেতার VPC থেকে DHCP-র মাধ্যমে পায়। এখানে যা-ই লিখতাম, প্রথম বুটেই তা মুছে যেত।
NAME-4404	এমন তথ্যের উপর নির্ভরশীল যা ইমেজ তৈরির সময় থাকে না; প্রথম বুটেই তা নির্ধারিত হয়।

টেস্ট ID	প্রযোজ্য না হওয়ার কারণ
SSH-7408	SSH ২২ পোর্টেই থাকে, কারণ EC2 Instance Connect ও কনসোল সরঞ্জাম সেটিই প্রত্যাশা করে। পোর্ট বদলালে স্ক্যানারের কাছে কিছুই লুকোয় না; ব্রুট ফোর্স ঠেকায় কি-প্রমাণীকরণ ও fail2ban।
SSH-7440	SSH অনুমোদিত ব্যবহারকারীর কোনো নির্দিষ্ট তালিকা বেঁধে দেয় না: ক্রেতা এই ইমেজের উপর নিজের অ্যাকাউন্ট বানান, আর আমাদের তালিকা তাঁকেই বাইরে রেখে দিত। প্রবেশাধিকার এমনিতেই কেবল-কি প্রমাণীকরণ, root লগইন নিষিদ্ধ ও fail2ban দিয়ে সীমিত।
TOOL-5002	ইচ্ছে করেই কোনো কনফিগারেশন-ব্যবস্থাপনা এজেন্ট বসানো হয় না: ইমেজ তৈরি হয় SSH-এর মাধ্যমে Ansible দিয়ে, যা পরে কিছুই চালু রেখে যায় না। একটি ডিমেন কম মানে একটি আক্রমণ-পৃষ্ঠ কম।
USB-1000	ক্লাউড ইনস্ট্যান্সের কাঠামোয় প্রযোজ্য নয়: এটি যা পরীক্ষা করে তা এখানে নেই, কিংবা সেটি সরবরাহকারীর অবকাঠামোই সামলায়।
USB-3000	ক্লাউড ইনস্ট্যান্সের কাঠামোয় প্রযোজ্য নয়: এটি যা পরীক্ষা করে তা এখানে নেই, কিংবা সেটি সরবরাহকারীর অবকাঠামোই সামলায়।

এই তালিকা পড়া হয় ইমেজের ভেতরেই বসানো Lynis প্রোফাইল থেকে, হাতে রাখা কোনো নথি থেকে নয়: এখানে যা দেখছেন, অভিন্ন ঠিক সেটিই প্রয়োগ করেছে।