Engineer

Three locks on the door, none of them locked

Found and closed three SSH brute-force protections that had never worked: a ban jail watching port 22 while the daemon listened on 1986, a rate limit shadowed by a broader rule above it, and a ban action whose binary never resolved, so no ban had ever applied.

August 2026

three brute-force defences that had never worked

Situation. A hardening review of the production host in August 2026 asked a question that usually gets a confident answer: are the SSH brute-force protections working. All three were configured, all three appeared in every report anyone looked at, and all three had been inert since the day the host was built.

Task. The controls had to be checked against what the kernel actually does with a packet, rather than against the configuration files that describe what should happen to one.

Action. Reading the configuration would have confirmed the wrong answer three times, so the review read the running system instead. The intrusion-banning jail was watching port 22 while the daemon had been moved to 1986 during the initial hardening — every ban it wrote named a port nothing listened on. The firewall's rate limit was worse in a subtler way: the rule existed, and it sat below a broader rule that matched first. Firewall user rules are evaluated top down and the first match wins, so a broad allow above a rate limit makes the limit dead code that still prints in every status listing. The third was the quietest of them: the ban action shells out to a packet-filter binary that the package system only recommends rather than requires, so on a host without it the jail starts, counts and decides, and then fails at the one moment it tries to ban. All three fixes were small. What came out of it was not the fix but two rules that now govern the repository: a security control gets an assertion rather than a comment, and a firewall is verified by rule position rather than by rule presence.

Result. Three protections that had never once fired now do, and the class of defect they belong to — a control whose failure mode is that it keeps reporting healthy — is the class the platform's checks are now built to catch. All three had been inert from bootstrap. All three printed healthy in every place anyone looked, which is the whole reason they lasted.

Bring this experience to your project

Use "Three locks on the door, none of them locked" as a starting point for a similar challenge in your organisation. The services behind this work are available for your project. Monitoring and alerts that speak up while a fault is still small, and the figures that show how often it stays that way.

Explore our services Get in touch →

Look behind the result

Read the situation, decisions and result in this example. We can discuss which parts transfer to your constraints and which need another approach. Three locks on the door, none of them locked — three brute-force defences that had never worked

Explore our services Get in touch →

Sure your intrusion protection actually protects?

Talk through your project with the engineer responsible for delivery. We agree the scope, price basis and handover in writing before work begins.

Role context: Security Engineer. It draws on Infrastructure, Monitoring & Observability, Networking & VPN, Linux & Servers, Security and System Administration. And while you are here, we are rather good at Site Reliability & Monitoring, Networking & VPN Setup, Security & Access Management and AI Agent Security.

Get in touch Explore our services

One piece of **a longer record** — and it is all on this site.

Every entry is written the same way: the situation, the task, what we did and what changed.

See the whole record

Define the improvement you need

Bring the deployment path, the operational risks and the people on call. We can scope a change with checks, a recovery route and clear ownership.

See what it costs Get in touch →

Sure your intrusion protection actually protects?

Ask about the decisions behind “Three locks on the door, none of them locked”. You will speak with the people who can explain the work and assess your own project.

Explore our services

welcome@engineer.company +45 50 10 61 84 Copenhagen, Denmark

Take this page with you

Contact card

Carefully Crafted With Love by D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – present · Engineer ApS · All rights reserved.

Printed from https://engineer.company/portfolio/three-locks-on-the-door-none-of-them-locked/