Engineer

Три замки на дверях, і жоден не замкнений

Знайшла й виправила три механізми захисту SSH від перебору паролів, які ніколи не працювали: jail блокування, що стежив за портом 22, тоді як демон слухав порт 1986; обмеження частоти, яке перекривало ширше правило, розташоване вище; і дію блокування, бінарний файл якої так і не знаходився, тож жодне блокування жодного разу не спрацювало.

серпень 2026

три захисти від перебору, що ніколи не працювали

Ситуація. Перевірка захищеності продакшн-хоста в серпні 2026 року поставила питання, на яке зазвичай відповідають упевнено: чи працює захист SSH від перебору паролів. Усі три засоби захисту було налаштовано, усі три фігурували в кожному звіті, який хтось переглядав, — і всі три не діяли від того самого дня, коли хост було створено.

Завдання. Засоби контролю треба було перевірити за тим, що ядро насправді робить із пакетом, а не за файлами налаштувань, які описують, що з ним мало б статися.

Дія. Читання налаштувань тричі підтвердило б хибну відповідь, тому перевірка дивилася натомість на систему в роботі. Jail системи блокування зловмисників стежив за портом 22, хоча сам демон ще під час початкового посилення захисту перенесли на порт 1986, — кожне блокування, яке він записував, стосувалося порту, на якому ніщо не слухало. З обмеженням частоти на брандмауері все було гірше, хоч і менш помітно: правило існувало, але стояло нижче ширшого правила, яке спрацьовувало першим. Користувацькі правила брандмауера перевіряються згори вниз, і застосовується перше, що збіглося, тож широкий дозвіл над обмеженням частоти перетворює це обмеження на мертвий код, який і далі з’являється в кожному виводі стану. Третя проблема була найнепомітнішою: дія блокування викликає через командну оболонку бінарний файл фільтра

пакетів, який система керування пакетами лише рекомендує, а не вимагає, тож на хості без нього jail запускається, рахує, ухвалює рішення — і дає збій саме тієї миті, коли намагається заблокувати. Усі три виправлення були дрібними. Головним підсумком стали не вони, а два правила, яких тепер дотримується весь репозиторій: засіб безпеки отримує перевірку (assert), а не коментар, а брандмауер перевіряють за тим, де стоїть правило, а не за тим, чи воно є.

Результат. Три засоби захисту, які досі жодного разу не спрацювали, тепер працюють, а клас дефектів, до якого вони належать, — засіб контролю, що, відмовивши, і далі звітує про справність, — саме той клас, на виявлення якого тепер розраховані перевірки платформи. Усі три не діяли від першого розгортання. Усі три показували «справний» скрізь, куди хтось дивився, — і саме тому так довго протрималися.

Застосуйте цей досвід у своєму проєкті

Використайте «Три замки на дверях, і жоден не замкнений» як відправну точку для схожого завдання у вашій організації. Послуги, що стоять за цією роботою, доступні й для вашого проєкту. Моніторинг і сповіщення, які попереджають, поки збій ще малий, і цифри, що показують, як часто так і залишається.

Переглянути наші послуги Зв'язатися з нами →

Дізнайтеся, що привело до результату

Прочитайте про ситуацію, рішення та результат цього прикладу. Ми можемо обговорити, що відповідає вашим умовам, а що потребує іншого підходу. Три замки на дверях, і жоден не замкнений — три захисти від перебору, що ніколи не працювали

Переглянути наші послуги Зв'язатися з нами →

Упевнені, що ваш захист від вторгнень справді захищає?

Обговоріть свій проєкт з інженером, відповідальним за виконання. Обсяг, основу розрахунку вартості та передачу результатів узгоджуємо письмово до початку робіт.

Роль у цій роботі: Інженер з безпеки. Тут задіяні Інфраструктура, Моніторинг і спостережуваність, Мережі та VPN, Linux та сервери, Безпека та Системне адміністрування. І, до речі, ми добре вміємо Надійність та моніторинг (SRE), Налаштування мереж та VPN, Безпека та керування доступом та Безпека ШІ-агентів.

Зв'язатися з нами Ознайомтеся з нашими послугами

Одна частина **довшого переліку** — і він увесь на цьому сайті.

Кожен запис написано однаково: ситуація, завдання, що ми зробили і що змінилося.

Переглянути весь перелік

Визначте потрібне покращення

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Упевнені, що ваш захист від вторгнень справді захищає?

Запитайте про рішення в роботі «Три замки на дверях, і жоден не замкнений». Ви говоритимете з людьми, які можуть пояснити роботу й оцінити ваш проєкт.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

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

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/portfolio/three-locks-on-the-door-none-of-them-locked/