Hartowanie Linuksa we wrogich środowiskach sieciowych. Ochrona serwera od TLS po Tor
K. Rankin

Helion, 2018 r.

W dzisiejszym świecie, w którym wiele codziennych aktywności odbywa się przez internet, bardzo dużo zależy od bezpieczeństwa serwerów. Kiedy zwykli ludzie tworzą społeczności, komunikują się i robią zakupy online, hakerzy niestrudzenie przeglądają sieć, poszukując słabych punktów. Atakują różne obiekty: mogą to być agencje rządowe, elektrownie i banki, ale równie dobrze ich celem może się stać jakakolwiek sieć komputerów. Chodzi o uzyskanie wrażliwych informacji, zbiorów danych osobowych czy wreszcie przejęcie kontroli nad systemem.
Co gorsza, agresorzy odnoszą sukcesy nawet w przypadku sieci, w których wdrożono złożone i kosztowne zabezpieczenia.
Dzięki tej książce poznasz sprawdzone i niezbyt skomplikowane procedury, które pozwolą Ci na zahartowanie swoich danych. Najpierw zapoznasz się z ogólnym ujęciem tematyki bezpieczeństwa systemów, w tym stacji roboczych, serwerów i sieci. Następnie dowiesz się, w jaki sposób zahartować specyficzne usługi, takie jak serwery WWW, pocztę elektroniczną, systemy DNS i bazy danych. Na końcu książki znalazł się rozdział poświęcony reagowaniu na incydenty - to również jest wiedza potrzebna każdemu administratorowi.
Zawarte tu treści przedstawiono w sposób bardzo praktyczny, z uwzględnieniem najnowszych osiągnięć w dziedzinie zabezpieczania systemów.

Źródło opisu: helion.pl