

Szukamy oznak ataku sieciowego

# ZABAWA W KOTKA I MYSZKĘ

Jeżeli wydaje Ci się, że twoje systemy są zbyt dziwaczne, aby stanowiły obiekt ataków sieciowych, zastanów się nad tym jeszcze raz. Dziś atakujący zadowolą się każdą ofiarą.

JOE CASAD

**C**zy wszystkie wejścia są zamknięte? Czy twoje dane są bezpieczne? Na początku pierwsi intruzi sieciowi włąmywali się dla zabawy: tylko po to, aby udowodnić, że jest to możliwe. Traktowali to jak wyzwanie intelektualne albo może szansę poczucia dreszczyku emocji – jak autor graffiti czy dziecko kradnące cukierki ze sklepu.

Czasy się jednak zmieniły, a jeśli troszczysz się o bezpieczeństwo, lepiej będzie, jeżeli także się zmienisz. Dzisiejsze systemy zawierają kluczowe informacje o wartości bezpośrednio przeliczalnej na pieniądze: numery kart kredytowych, dane medyczne, adresy e-mail. Poza tym sam system może stać się narzędziem dla atakującego. Cyberprzestępcy wykorzystują zaawansowane techniki, aby zmusić zupełnie zwykłe komputery do przekazywania spamu i uruchamiania ataków typu *denial of service* (odmowa usługi). A nastoletni chuligani? Nadal mają się dobrze. Aby trzymać się od nich wszystkich z daleka, musisz wiedzieć to, co oni – i wiedzieć, jak szukać ich śladów. To właśnie jest tematem niniejszego numeru.

Intruz, który łamie zabezpieczenia sieciowe, zawsze chce stworzyć ukrytą furtkę, którym będzie mógł wrócić. Takie tajne przejścia, zwane „tylnymi wejściami” (*backdoors*), są zwykle zamaskowane. Temat numeru w tym miesiącu rozpoczyna się od przeglądu niektórych popularnych technik tworzenia takich „tylnych wejść”. Następnie omawiamy program iWatch – obiecujące narzędzie,

które wykorzystuje interfejs Inotify jądra Linuksa do monitorowania katalogów i wysyłania w czasie rzeczywistym ostrzeżeń o niepożądanym dostępie. Pokazujemy także, jak szukać oznak ataku za pomocą uniwersalnego narzędzia administracyjnego Isof. W ostatnim artykule z tematu numeru przedstawiamy zaś system BackTrack, dys-

trybucję Linuksa typu live, wyposażoną we wspaniały zbiór narzędzi do symulowania ataku sieciowego.

Jeżeli więc chcesz nauczyć się myśleć jak atakujący albo tylko szukasz prostych technik samoobrony, zapoznaj się z naszymi specjalistycznymi radami dotyczącymi ataków sieciowych. Miłej lektury!

