# 5

# KONTROLOWANIE UPRAWNIEŃ DO PLIKÓW I KATALOGÓW

Nie wszyscy użytkownicy jednego systemu operacyjnego powinni mieć ten sam poziom dostępu do plików i katalogów. Linux, podobnie jak każdy profesjonalny system operacyjny, zwłaszcza przeznaczony dla przedsiębiorstw, umożliwia ograniczanie dostępu do plików i katalogów. System zabezpieczeń pozwala administratorowi – użytkownikowi *root* – lub właścicielowi plików chronić pliki przed nieuprawnionym dostępem lub niedozwoloną modyfikacją. Służą do tego *uprawnienia* do odczytu, zapisu lub wykonywania (uruchamiania) plików. Dla każdego pliku i katalogu można określić poziom uprawnień dla właściciela pliku, konkretnych grup użytkowników oraz wszystkich innych użytkowników. Jest to konieczność w przypadku systemu operacyjnego przeznaczonego dla wielu użytkowników i używanego w przedsiębiorstwie. Alternatywą byłby chaos.

W tym rozdziale zajmiemy się sprawdzaniem i zmienianiem uprawnień wybranych użytkowników w odniesieniu do plików i katalogów, ustawianiem uprawnień domyślnych do plików i katalogów oraz określaniem uprawnień

specjalnych. Na koniec zobaczymy, w jaki sposób znajomość uprawnień przez hakerów może im pomóc eksploatować systemy.

## Różne rodzaje użytkowników

Jak już wiemy, w systemie Linux największe uprawnienia ma użytkownik root. W zasadzie może on wykonywać *wszystko* w systemie. Inni użytkownicy mają bardziej ograniczone możliwości i uprawnienia oraz niemal nigdy nie mają praw dostępu na poziomie użytkownika root.

Ci inni użytkownicy zazwyczaj są organizowani w *grupy*, w których sprawują podobne funkcje. W przedsiębiorstwie mogłyby to być na przykład działy finansów, techniczny, sprzedaży itp. W środowisku IT grupy te mogą obejmować twórców aplikacji, administratorów sieci czy administratorów bazy danych. Idea tego rozwiązania polega na tym, aby osoby o podobnych potrzebach umieścić w grupie, której zostały przypisane odpowiednie uprawnienia dziedziczone przez każdego jej członka. Ma to na celu przede wszystkim ułatwienie administrowania uprawnieniami, a tym samym zwiększenie bezpieczeństwa.

Użytkownik root jest domyślnie członkiem grupy root. Każdy nowy użytkownik systemu musi zostać dodany do grupy, z której odziedziczy uprawnienia.

## Nadawanie uprawnień

Każdy plik i katalog musi mieć przypisany określony poziom uprawnień zezwalających na odpowiednie użytkowanie go przez różne grupy użytkowników. Dostępne są trzy następujące poziomy uprawnień:

**r** Uprawnienie do odczytu. Zezwala ono jedynie na otwarcie pliku i wyświetlenie jego zawartości.

**w** Uprawnienie do zapisu. Zezwala ono na wyświetlenie i edytowanie pliku.

**x** Uprawnienie do wykonania. Zezwala ono na wykonanie (uruchomienie) pliku, ale niekoniecznie na wyświetlenie jego zawartości i jej edytowanie.

W ten sposób użytkownik root może nadawać użytkownikom odpowiednie poziomy uprawnień w zależności od tego, do czego będą tych plików używać. Zazwyczaj, gdy jest tworzony jakiś plik, jego twórca staje się właścicielem pliku, a grupą właścicielską jest grupa, do której ten użytkownik należy. Właściciel pliku może przypisywać różne odnoszące się do tego pliku uprawnienia. Przyjrzyjmy się, w jaki sposób można zmienić uprawnienia w celu przekazania praw własności do poszczególnych użytkowników lub grup.