



Eskałacja uprawnień

- ▶ Uprawnienia użytkowników w systemie
 - ▶ „Zwykły” użytkownik i administrator systemu
 - ▶ UID i efektywny UID (**eu**id)
 - ▶ Uprawnienia procesów związane z **uid/euid**
 - ▶ Procesy set-user-id i set-group-id
 - ▶ Kontrola dostępu/uprawnień w dużej mierze odbywa się poprzez system plików (programy, urządzenia specjalne, mechanizmy komunikacji)
- ▶ Aplikacje systemowe
 - ▶ „demony” systemowe (system daemons)
 - ▶ serwery sieciowe
 - ▶ z reguły działają z uprawnieniami użytkownika **root**
 - ▶ błędy w oprogramowaniu mogą prowadzić do eskalacji uprawnień
 - ▶ „dziury bezpieczeństwa” – nieprzewidziane przez twórców działanie programu prowadzące do eskalacji uprawnień lub innych naruszeń bezpieczeństwa
- ▶ „Nietypowe” metody lub błędy konfiguracji systemu
 - ▶ Dostęp przez urządzenia specjalne – np. zmodyfikowane prawa dostępu do **/dev/kmem** lub bezpośrednio do urządzeń dyskowych (np. **/dev/sda** itp.)
 - ▶ Pseudo-system plików **/proc**

