



## Eskalacja uprawnień – przykłady

- ▶ Wykonanie zewnętrznego programu z uprawnieniami *root*
  - ▶ *sendmail* v.8.8.5
    - ▶ możliwość wystartowania przez dowolnego użytkownika
    - ▶ brak odłączenia się od grupy procesów
    - ▶ „standardowy” sposób przeładowywania programu przez *kill -HUP*
  - ▶ *Apache* – skrypty CGI
  - ▶ Błędy typu „code injection” (np. *bind* v.4.x – buffer overflows)
- ▶ Wykorzystanie uprawnień istniejącego programu systemowego
  - ▶ błędna (celowo?) konfiguracja
  - ▶ nieprawidłowe dane wejściowe
  - ▶ błędy w sposobie dostępu do plików tymczasowych – wyścig (race condition)
  - ▶ błędy systemowe sprzętu (np. błędy obsługi cache procesora – błędy typu Spectre)