




## Bezpieczeństwo systemów informatycznych

### SPRAWOZDANIE Z ĆWICZENIA: Ograniczanie środowiska pracy

Imię Nazwisko: ..... nr albumu: .....

data ćwiczenia: ..... godzina: .....

#### 1. Polityka limitów

 *Uruchom system Linux lokalny czysty*

1. Przeczytaj podręcznik użytkownika dla mechanizmu ulimit.

Wymień, które parametry środowiska systemu operacyjnego możesz ograniczać:

2. Skonfiguruj określony przez prowadzącego rodzaj ograniczeń. Zapisz jak skonfigurować to ograniczenie:

i jak je przetestować:

3. Napisz program, który spowoduje utworzenie zrzutu pamięci (core):

4. Skompiluj stworzony program wraz z symbolami debuggera (gcc -g) i uruchom. Skonfiguruj limity tak, by zrzut został utworzony. Przeanalizuj utworzony zrzut za pomocą gdb. Zapisz czynności:

## 2. Polityka sudo

5. Zapoznaj się w podręczniku ze strukturą pliku `/etc/sudoers` i metodą jego edycji.
6. Skonfiguruj politykę sudo, tak by dowolny użytkownik mógł wykonać polecenie: `fdisk -l`  
Podaj zmiany wprowadzone w pliku konfiguracyjnym `/etc/sudoers`:

Czyje hasło jest wymagane przy uruchomieniu tego polecenia przez sudo?

Czy można ustalić w polityce by pytanie o hasło dotyczyło innego konta. Jakie są możliwe opcje?

7. Sprawdź w jaki sposób można konfigurować ile czasu sudo przechowuje informacje na temat uwierzytelnionych użytkowników. Zapisz zmiany wprowadzone w pliku konfiguracyjnym, by czas przechowywania potwierdzenia uwierzytelnienia wynosił 30 sekund.

8. Skonfiguruj politykę sudo, tak by jeden wybrany użytkownik mógł wykonać wybrane polecenie z uprawnieniami root bez podawania hasła. Zapisz zmiany wprowadzone w pliku konfiguracyjnym:

### 3. Mechanizm SUID i SGID

9. Podaj polecenie, które znajdzie w systemie pliki z ustawionymi flagami SUID lub SGID.

10. Wymień po jednym programie, który posiada odpowiednią flagę i wyjaśnij dlaczego ją posiada:  
SUID

SGID

11. Jakie potencjalne zagrożenie dla systemu stanowią polecenia z flagami SUID lub SGID?