



Bezpieczeństwo systemów informatycznych

SPRAWOZDANIE Z ĆWICZENIA: Ograniczanie środowiska pracy

Imię Nazwisko: nr albumu:

data ćwiczenia: godzina:

1. Mechanizm 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. Mechanizm sudo

5. Zapoznaj się w podręczniku z budową pliku `/etc/sudoers` i sposobem jego modyfikacji.
6. Skonfiguruj mechanizm sudo, aby 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:

7. Skonfiguruj mechanizm sudo, aby jeden wybrany użytkownik mógł wykonać wybrane polecenie z uprawnieniami root bez podawania hasła. Zapisz zmiany wprowadzone w pliku konfiguracyjnym:

8. 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.

3. Mechanizm SUID i SGID

9. Zapoznaj się z podręcznikiem użytkownika na temat praw określanych flagami SUID i SGID.
10. Podaj polecenie, które znajdzie w systemie pliki z ustawionymi flagami SUID lub SGID.

11. Wymień kilka programów, które muszą posiadać odpowiednią flagę i wyjaśnij dlaczego:

SUID

SGID

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