Laboratorium 3 - Użytkownicy, grupy i prawa

1. Teoria

System Linux wywodzi się z rodziny systemów unixowych, których przeznaczeniem było głównie działanie jako systemy serwerowe obsługujące bardzo wielu użytkowników. Z tego powodu w systemie Linux istnieje stosunkowo rozbudowany system zarządzania użytkownikami. Każdy użytkownik rozpoznawany jest po nazwie użytkownika oraz jednocześnie w systemie po specjalnym numerze `UID`, który jest unikalny dla niego. Dodatkowo użytkownicy mogą przypisani być do grup. Grupy także rozpoznawane są za pomocą nazwy oraz specjalnego unikalnego numeru `GID`. Grupa powinny reprezentować pewną wspólna cechę wielu użytkowników. Głównym użytkownikiem systemu jest `root` który ma zawsze `UID` równy `0`. Jest on także członkiem grupy `root`. Nazwy grup i użytkowników mogą się powtarzać, co jest w niektórych dystrybucjach domyślną polityką tworzenia grup dla użytkowników (nazwa grupy taka sama jak login).

1.1. Prawa dostępu do plików

1.1.1. Kategorie

Prawa dostępu do pliku definiujemy dla 3 kategorii:

- **u**ser - użytkownik, czyli właściciel pliku
- **g**roup - grupa przypisana do pliku
- **o**ther - wszyscy pozostali

1.1.2. Rodzaje praw dostępu

Wyróżniamy 3 rodzaje praw:

- **r**ead - odczyt zawartości pliku/katalogu ($4 = 100_2$)
- **w**rite - zapis do pliku/katalogu ($2 = 010_2$)
- e**x**ecute - wykonanie pliku/otwarcie katalogu ($1 = 001_2$)

Polecenie `ls -l` prezentuje prawa w zapisie symbolicznym:

```
-rwxr-xr—x fizyk fizyk 0 kwi 16 13:09 plik
```

Pierwsza kolumna ma format `tuuugggooo`:

- `t` - typ pliku
  - `-` - zwykły plik
  - `d` - katalog

    - `l` - dowiązanie symboliczne
- `u` - uprawnienia użytkownika
- `g` - uprawnienia grupy
- `o` - uprawnienia wszystkich pozostałych

1.1.3. Sposoby reprezentacji praw

Typ zapisu	Odczyt	Zapis	Wykonanie
binarny	2^2	2^1	2^0
liczbowy	4	2	1
symboliczny	r	w	x

1.2. `chmod`

Zmienia prawa dostępu do pliku.

Argument	Opis
prawa ścieżka	zmienia prawa dostępu do podanego pliku
`-R`	rekurencyjnie ustawia prawa wszystkim plikom w podkatalogach

Prawa można podać w zapisie numerycznym lub symbolicznym.

1.2.1. Zapis numeryczny

Przy zapisie numerycznym dodajemy do siebie reprezentację liczbową dla każdej kategorii (osobno dla użytkownika, grupy i pozostałych), co daje nam 3 liczby, np `755`.

1.2.2. Zapis symboliczny

Zapis symboliczny pozwala również na zmianę dotychczasowych praw za pomocą znaków:

- `=` - ustawia podane prawa
- `+` - dodaje podane prawa
- `-` - usuwa podane prawa

Do każdej kategorii odwołujemy się przez odpowiednią literę (`u`,`g` lub `o`) stawiając za nim jeden z powyższych znaków i podając prawa,
np. `u=rwx,g+rw,o-r`.

1.3. `sudo`

Uruchamia polecenie jako administrator.

Argument	Opis
polecenie	uruchamia podane polecenia jako administrator

1.4. whoami

Wypisuje nazwę aktualnego użytkownika.

1.5. id

Wypisuje informacje o użytkowniku i grupach, do których należy.

1.6. adduser, addgroup

Dodaje użytkownika/grupę do systemu. Na podstawie informacji w `/etc/adduser.conf` konfiguracja obejmuje m.in.:

- ustawienie powłoki na Bash
- utworzenie katalogu domowego użytkownika

Argument	Opis
nazwa	dodaje użytkownika/grupę o podanej nazwie
użytkownik grupa	dodaje użytkownika do grupy

1.7. /etc/passwd

`passwd` jest plikiem tekstowym z jednym rekordem na linię, z których każda opisuje jedno konto użytkownika. Każdy rekord (linia) składa się z siedmiu pól oddzielonych dwukropkami. Kolejność rekordów w pliku jest zazwyczaj nieistotna. Przykład: `jsmith:x:1001:1000:Joe Smith, pokój 1007, (234) 555-8910, (234) 555-0044, e-mail:/home/jsmith:/bin/sh`

Kolejne pola w rekordzie oznaczają:

1. Nazwa użytkownika
2. Drugie pole przechowuje informację używaną do sprawdzania hasła użytkownika. W nowych systemach wartość tego pola to "x", gdyż przechowywanie haseł, do których mają dostęp wszyscy użytkownicy nie jest bezpieczne. Obecnie stosuje się plik `/etc/shadow`. Ustawienie tego pola na gwiazdkę "*" wyłącza konto, aby zapobiec jego użyciu.
3. Identyfikator użytkownika `UID`, numer, który system operacyjny używa do celów wewnętrznych.
4. Identyfikator grupy `GID`. Liczba ta określa podstawową grupę użytkownika, wszystkie pliki, które są tworzone przez użytkownika są początkowo dostępne dla tej grupy.
5. Piąte pole, zwane polem GECOS, jest komentarzem, który opisuje osoby lub konta. Zazwyczaj jest to zbiór wartości oddzielonych przecinkami w tym pełnej nazwy użytkownika i dane kontaktowe.
6. Ścieżka do katalogu domowego użytkownika.
7. Domyślna powłoka (shell). Program, który jest uruchamiany przy każdym zalogowaniu do systemu. Dla użytkownika interaktywnego, zazwyczaj jest to jeden z systemu tłumaczy linii komend np. `bash`.

1.8. `/etc/group`

`group` jest to plik, w którym przechowywane są informacje o grupach. Tak jak w przypadku pliku `passwd` jeden rekord stanowi jedna linia rozdzielana znakiem dwukropka. Przykład: `cdrom:x:24:joe,admins,kate`

Poszczególne pola w rekordzie oznaczają:

1. Nazwa grupy
2. Pole hasła, przeważnie nie używane. Umożliwia tworzenie specjalnych uprzywilejowanych grup.
3. Identyfikator grupy `GID`.
4. Lista użytkowników grupy rozdzielona przecinkami. Wszyscy użytkownicy wymienieni w tym polu należą do danej grupy i zyskują jej uprawnienia.

1.9. `su`

Zmienia użytkownika, na którego jesteśmy zalogowani.

Argument	Opis
login	loguje się na podanego użytkownika

1.10. `chgrp`

Zmienia grupę, do której przypisany jest plik. Pozwala na zmianę grupy, na taką, do której należy użytkownik.

Argument	Opis
grupa ścieżka	przypisuje grupę do podanego pliku/katalogu

1.11. `chown`

Zmienia użytkownika i grupę, do której przypisany jest plik. Zazwyczaj tylko administrator ma prawa do użycia tej komendy.

Argument	Opis
[użytkownik][:grupa] ścieżka	przypisuje grupę/użytkownika do podanego pliku/katalogu

1.12. `deluser, delgroup`

Usuwa użytkownika/grupę.

Argument	Opis
nazwa	usuwa użytkownika/grupę o podanej nazwie
--remove-home użytkownik	usuwa użytkownika wraz z jego katalogiem domowym

1.13. `passwd`

Zmienia hasło użytkownika.

Argument	Opis
brak	zmienia hasło aktualnego użytkownika
login	zmienia hasło użytkownika o podanym loginie

2. Praktyka

2.1. Zadanie

Zapoznaj się z ideą wirtualizacji oraz narzędziem VirtualBox.

2.2. Zadanie

Pobierz i uruchom w VirtualBox lub VMWare obraz systemu Ubuntu.
VirtualBox

VMWare

Obraz Ubuntu

2.3. Zadanie

`sudo`, `whoami`

Uzyskaj prawa użytkownika root wykonując np. polecenie `sudo bash`. Hasło użytkownika `ubuntu` to `ubunu`, sprawdź poleceniem `whoami` czy posiadasz dostęp jako użytkownik `root`.

2.4. Zadanie

`adduser`

Utwórz w systemie użytkowników: `marek`, `ania`, `jurek`.

2.5. Zadanie

Sprawdź jak zmienił się plik `/etc/passwd`.

2.6. Zadanie

`addgroup`

Utwórz w systemie grupy: `marketing`, `zarzad`.

2.7. Zadanie

Sprawdź jak zmienił się plik `/etc/group`.

2.8. Zadanie

Dodaj do grupy `marketing` użytkowników `marek` i `ania`, a do grupy `zarzad` tylko użytkownika `ania`.

2.9. Zadanie

`su`

Jako użytkownik `marek` utwórz katalog `~/projekt` a w nim plik tekstowy z dowolną treścią o nazwie `~/projekt/zalozenia`.

2.10. Zadanie

`chmod`, `chgrp`

Ustaw takie prawa dostępu do tego pliku aby mogły go odczytać wszystkie osoby ale edytować tylko z grupy `marketing`. Sprawdź, logując się jako `marek` lub `ania`, czy możesz wyświetlić plik i go zmodyfikować, a jako `jurek` możesz tylko wyświetlić.

2.11. Zadanie

Ustaw takie prawa dla katalogu `projekt`, aby wyświetlić jego zawartość mogła tylko osoba z grupy `zarzad` (czyli tylko `ania`) - pozostałe prawa pozostają niezmienione. Sprawdź czy jako `marek` znając pełną ścieżkę pliku nadal możesz edytować plik `~/projekt/zalozenia`.

2.12. Zadanie

Ustaw takie prawa do katalogu projekt, aby wejść do katalogu mogła tylko osoba z grupy `zarzad`. Sprawdź czy jako `marek` nadal możesz edytować plik?

2.13. Zadanie

Dodaj kolejne pliki i katalogi do katalogu projekt (przynajmniej 2 poziomy). Spróbuj ustawić dowolne prawa dostępu rekurencyjnie wszystkim plikom i podkatalogom dla `~/projekt`. Np. prawa `666`.

2.14. Zadanie

`deluser`, `delgroup`

Usuń grupy i użytkowników w systemie.