

# Wstęp do systemu operacyjnego UNIX

## Laboratorium 2:

### Użytkownicy w systemie UNIX

System operacyjny udostępnia użytkownikom zasoby systemu komputerowego. Przyjmuje się, że użytkownik będzie dążył do maksymalnego ich wykorzystania. Pojawia się zatem konieczność ograniczania dostępu do zasobów, kontrolowania sposobu i intensywności ich wykorzystywania oraz ochrony zasobów stanowiących własność jednego użytkownika przed zakusami innych użytkowników. Zakłada się przy tym, że użytkownik jest maksymalnie „złośliwy” - dąży do nieograniczonego zawłaszczania zasobów oraz całkowitego zniszczenia własności innych użytkowników.

Użytkownik w systemie UNIX jest zasobem abstrakcyjnym. Jądro systemu rozpoznaje go po numerze (liczba typu całkowitego, tzw. *User Identification Number* – UID), co znacznie przyspiesza operacje związane np. z rozstrzyganiem praw własności. W świecie zewnętrznym jest on zdefiniowany przez nazwę (*ang. login name*), która jest łatwa do zapamiętania przez człowieka. Numer identyfikacyjny musi być niepowtarzalny. W systemie nie może istnieć dwóch użytkowników o takim samym numerze identyfikacyjnym. Zasada ta dotyczy również nazwy użytkownika w systemie.

Oprócz nazwy użytkownika konieczne są również dodatkowe poziomy identyfikacji użytkownika. Identyfikacja ta może być oparta na cechach charakterystycznych użytkownika (np. linie papilarne lub obraz żrenicy), cechach charakterystycznych przedmiotów będących własnością użytkownika (np. karta magnetyczna) lub na wiedzy użytkownika (np. hasło). W systemach ogólnego przeznaczenia, ze względu na koszty weryfikacji cech charakterystycznych stosuje się ostatnie rozwiązanie w postaci hasła.

Użytkownicy w systemie nie są równoprawni. O ich możliwościach decyduje przynależność do odpowiedniej grupy. W systemie UNIX istnieją grupy predefiniowane. Grupy są rozróżniane niepowtarzalnym numerem identyfikacyjnym i nazwą na podobnych zasadach jak użytkownicy. Członkostwo w grupie systemowej daje uprawnienia do wykonywania pewnych czynności związanych z konfiguracją systemu. Są one zależne od implementacji systemu. Nowe grupy w systemie może tworzyć użytkownik posiadający określone uprawnienia.

Najważniejszym w systemie jest użytkownik **root**. Jego numer identyfikacyjny wynosi 0, a możliwości są praktycznie nieograniczone. W zasadzie użytkownicy o numerze UID różnym od zera są zwykłymi użytkownikami, jednak wiele konfiguracji systemów typu UNIX rezerwuje numery mniejsze od 100 dla użytkowników systemowych.

Podstawowym plikiem przechowującym w systemie UNIX informacje o jego użytkownikach lokalnych jest plik znajdujący się w katalogu `/etc` o nazwie `passwd`. Jest to plik tekstowy. Każda linijka definiuje jednego użytkownika i składa się z 7 części (kolumn) oddzielonych znakiem „,”. Poniżej przedstawiono przykładowy jego fragment:

```
1 root:x:0:0:root:/root:/bin/bash
2 bin:x:1:1:bin:/bin:/sbin/nologin
3 daemon:x:2:2:daemon:/sbin:/sbin/nologin
4 adm:x:3:4:adm:/var/adm:/sbin/nologin
5 .....
6 pvm:x:24:24:./usr/share/pvm3:/bin/bash
7 test:x:501:501:./home/test:/bin/bash
```

Kolejne kolumny oznaczają:

1. Nazwę użytkownika w systemie – *login*.
2. Pole to ma znaczenie historyczne. Dawniej przechowywane było w tym miejscu hasło w postaci zakodowanej. Dla podniesienia poziomu bezpieczeństwa systemu zostało jednak przeniesione do plików, których prawo odczytu ma jedynie użytkownik **root**. Niektóre systemy wykorzystują to pole do przechowywania informacji o stanie hasła.
3. Numer użytkownika w systemie.
4. Numer grupowy użytkownika. Jest to numer podstawowej grupy użytkownika i służy np. do określania tzw. grupowego właściciela.

5. Opis użytkownika. Informacja ta nie jest dla systemu istotna. Bywa wykorzystywana przez niektóre aplikacje (np. finger) do podawania cech użytkownika. W niektórych systemach jest podzielona przecinkami na 4 pola (Nazwisko imię, numer pokoju, telefon biurowy, telefon domowy).
6. Ścieżka dostępu do katalogu domowego użytkownika.
7. Ścieżka dostępu do podstawowego interpretera poleceń.

**0. Podłącz się do systemu jako użytkownik root. Zapoznaj się ze stronami manuala dotyczącymi pliku `passwd` (opisy plików znajdują się w rozdziale 5 dokumanetacji systemowej - polecenie: `man 5 passwd`).**

1. Ilu użytkowników jest zdefiniowanych w systemie?
  2. Jak został opisany w systemie użytkownik (5 kolumna pliku `/etc/passwd`), którego numer identyfikacyjny wynosi 14?
  3. Ilu użytkowników posiada numer identyfikacyjny UID większy od 23?
- Dla pytań 1, 2 i 3 podaj postać linii komend.

Dodawanie nowego użytkownika.

Nowego użytkownika w systemie najprościej można zdefiniować korzystając z komendy `useradd` (w niektórych systemach `useradd`). W postaci najprostszej wymaga ona podania jedynie nazwy użytkownika w systemie, a wartości pozostałych zmiennych opisujących użytkownika w systemie komenda nada korzystając z wartości domyślnych:

```
1 [root@thorin root]# useradd user1
```

4. Zapoznaj się ze stronami manuala dotyczącymi komendy `useradd:1`.
5. Załóż w systemie użytkowników o nazwach `test` i `team` określając dla użytkownika `team` numer identyfikacyjny (np. 997). Ustaw hasła dla użytkowników `test` oraz `team`. Jaki numer został nadany użytkownikowi `test`?
6. Korzystając z komendy `su` przełącz się na użytkownika `test`. Utwórz w katalogu `/tmp` plik o nazwie `pliktester`. Wyloguj się. Powtórz to samo dla użytkownika `team` tworząc plik `plikteam`.

W systemie operacyjnym Linux postać zakodowana haseł użytkowników jest przechowywana w pliku `shadow` w katalogu `/etc`. Plik ten jest własnością użytkownika `root` i tylko on ma prawo do jego odczytu i modyfikacji. Plik ten jest plikiem tekstowym. Każda linia opisuje jednego użytkownika systemu i podobnie jak w pliku `passwd` podzielona jest znakiem „,” na kolumny. Fragment pliku zamieszczono poniżej:

```
1 root:$1$FRRwFyfT$11IOfqMrI/MYHhQKeKNOEE0:12091:0:99999:7:::
2 bin:!:11894:0:99999:7:::
3 radvd:!!:11894:0:99999:7:::
4 .....
5 pvm:!!:11894:0:99999:7:::
6 test:RfRj4a7/tqRh/W:12131:0:99999:7:::
```

Kolejne kolumny oznaczają:

1. Nazwa użytkownika (login), to pole musi być zgodne z polem w pliku `/etc/passwd`.
2. Zakodowane hasło.
3. Dni, licząc od 1 stycznia 1970, kiedy hasło było ostatni raz zmienione.
4. Dni przed których upłynięciem niemożliwa jest zmiana hasła.
5. Dni, po których upłynięciu konieczna jest zmiana hasła.
6. Liczba dni, jaka musi dzielić hasło od przedawnienia, by użytkownik był ostrzegany.
7. Liczba dni po przedawnieniu hasła, kiedy konto jest blokowane.

8. Dni od 1 stycznia 1970, kiedy konto jest wyłączane (przedawnione).

9. Pole zarezerwowane.

Wartości dotyczące minimalnego i maksymalnego wieku hasła oraz momentu pojawienia się ostrzeżenia o konieczności zmiany hasła można wpisać ręcznie (będąc użytkownikiem `root`) lub skorzystać z komendy `passwd`. Komenda ta oprócz zmiany hasła umożliwia również ustawienie podstawowych parametrów hasła. Jeśli komenda `passwd` zostanie użyta bez argumentu, zmiana hasła dotyczy użytkownika, który ją wywołał. Użytkownik `root` chcący ustawić hasło dowolnemu użytkownikowi w systemie musi podać jego nazwę jako argument wywołania komendy. Zwróć uwagę, że nie ma możliwości sprawdzenia jakie jest obecne hasło, można je jedynie zmienić.

7. Zapoznaj się ze stronami manuala dotyczącymi komendy `passwd`.

8. Korzystając z odpowiednich opcji komendy `passwd` ustaw dla użytkowników `test` i `team` nowe hasła obowiązujące 14 dni. Użytkownicy ci powinni na dwa dni przed upływem ważności hasła otrzymać stosowny komunikat. Dodatkowo użytkownicy nie powinni zmieniać hasła wcześniej niż po 6-ciu dniach od ostatniej zmiany. Jaki jest sens tego ograniczenia?

9. Zapoznaj się ze składnią pliku `/etc/shadow` (rozdział 5 dokumentacji). Sprawdź, czy stosowne zapisy pojawiły się w pliku `/etc/shadow`. Sprawdź skuteczność wprowadzonych ograniczeń.

Bardziej ogólne zmiany charakterystyki użytkownika możliwe są do przeprowadzenia przy pomocy komendy `usermod`. Dotyczą one głównie informacji zapisanej w pliku `/etc/passwd`.

10. Korzystając z komendy `usermod` zmień opis użytkownika `team` dodając do istniejącego numer telefonu. Sprawdź, czy zmiany zostały zapisane w pliku `/etc/passwd`.

11. Zapoznaj się z manuałem komend `chsh` oraz `chfn`. Korzystając z komendy `chsh`, zmień podstawowy interpreter poleceń użytkownika `test` na `/bin/tcsh`. Zmień opis użytkownika `test`.

Jak widać informacja o konfiguracji użytkownika jest zapisana w kilku plikach (podstawowa w `/etc/passwd` oraz w systemie Linux w `/etc/shadow`). Istnieje zatem potencjalna możliwość, że będzie ona niespójna. Innym problemem są modyfikacje konfiguracji systemu, które mogą spowodować, że informacja zapisana w plikach konfiguracyjnych użytkownika będzie nieaktualna lub błędna. Wszystkie systemy operacyjne z rodziny UNIX oferują kilka programów narzędziowych do sprawdzania spójności i poprawności konfiguracji użytkownika. W systemie Linux podstawowymi są `pwck` oraz `grpck`.

12. Zapoznaj się ze składnią i działaniem komendy `pwck`. Sprawdź poprawność konfiguracji użytkowników w systemie.

13. Skopiuj plik ze strony <http://messy.icsr.agh.edu.pl/sysopy/lab2.tgz>. Zapoznaj się z poleceniem `tar` rozpakuj zawartość archiwum do katalogu `/tmp`. W archiwum znajdują się przykładowe pliki `passwd` oraz `shadow`. Sprawdź poprawność zapisanych w nich danych. Jakie błędy występują w plikach przykładowych?

Jak już wspomniano o uprawnieniach użytkowników w systemie decyduje przynależność do odpowiedniej grupy systemowej. Grupy użytkowników zostały stworzone również dlatego, aby móc w sposób efektywny zarządzać użytkownikami oraz aby użytkownicy mogli łatwiej współdzielić między sobą pliki i katalogi. Ta ostatnia właściwość jest wykorzystywana np. wtedy, gdy pewni użytkownicy systemu pracują nad wspólnym projektem. Tworzy się wówczas nową grupę i przypisuje do niej tych użytkowników. Ograniczenia dotyczące przynależności do grup, które pojawiają się w systemach z rodziny UNIX mówią zazwyczaj, że pojedynczy użytkownik może przynależeć do max. 32 grup i jedna jest jego grupą podstawową, decydującą o prawach własności. Dostępne w systemie grupy użytkowników zostały zdefiniowane w pliku `group` w katalogu `/etc`. Podobnie jak pliki definiujące użytkowników jest to plik tekstowy, w którym jedna linijka opisuje jedną grupę. Linijka jest podzielona na pola (kolumny) znakiem „;”. Poniżej przedstawiono fragment pliku.

```
1 root:x:0:root
2 bin:x:1:root,bin,daemon
3 daemon:x:2:root,bin,daemon
4 sys:x:3:root,bin,adm
5 adm:x:4:root,adm,daemon
6 .....
```

```

7 ident:x:98:
8 radvd:x:75:
9 wine:x:66:
10 pvm:x:24:
11 test:x:501:

```

Kolejne kolumny oznaczają:

1. Nazwa grupy
2. (zaszyfrowane) hasło dostępu do grupy. Pole to ma znaczenie w szczególnych przypadkach.
3. Numer identyfikacyjny grupy tzw.GID – *ang. Group ID*
4. Lista użytkowników zawierająca nazwy lub numery identyfikacyjne wszystkich użytkowników, należących do grupy, oddzielonych przecinkami.

Podobnie jak w przypadku użytkowników, nazwa grupy i jej numer identyfikacyjny nie mogą się powtarzać. Analogicznie do pliku `/etc/shadow` zawierającego dodatkowe, istotne z punktu widzenia bezpieczeństwa systemu dane o użytkownikach w systemie *Linux* stworzony został plik `/etc/gshadow`, który w zamyśle ma zawierać istotne dane o grupach. Jego znaczenie jest jednak niewielkie. Inne systemy operacyjne, przechowują w plikach - odpowiednikach informacje o limitach nałożonych na grupę.

Nową grupę w systemie może stworzyć użytkownik `root`, a w niektórych systemach typu UNIX użytkownik będący członkiem grupy administratorów. Służy do tego komenda `groupadd`. W najprostszej postaci wymaga ona podania jedynie unikalnej nazwy grupy. Numer identyfikacyjny grupy (GID) zostanie nadany.

**14. Korzystając z rozdziału 5 manuala zapoznaj się ze budową pliku `/etc/group`.**

**15. Zapoznaj się ze składnią komendy `groupadd`.**

**16. Utwórz w systemie grupę o nazwie `projekt`. Zmień charakterystykę użytkownika `test` tak, aby stał się on członkiem nowo utworzonej grupy `projekt`. Nowa grupa ma być jego grupą podstawową.**

Czasami istnieje konieczność zabronienia podłączania się do systemu użytkownikom z powodu np. prowadzonych prac administracyjnych. Za sposób podłączania się do systemu odpowiada konfiguracja programu `login`. Jednym z plików konfiguracyjnych jest plik `/etc/nologin`. Jest to plik tekstowy. Jeśli istnieje, to nikt poza użytkownikiem `root` nie może podłączyć się do systemu. Podczas próby podłączania się do systemu jego zawartość jest wypisywana na ekran.

**17. Będąc zalogowanym jako użytkownik `root` utwórz w katalogu `/etc` plik tekstowy `nologin` zawierający informacje o prowadzonych pracach administracyjnych. Sprawdź, czy nikt poza użytkownikiem `root` nie może podłączyć się do systemu. Usuń plik `/etc/nologin`.**

Nagle i niezapowiedziane zabronienie logowania do systemu spotka się z gwałtownymi reakcjami ze strony użytkowników, którzy planowali właśnie na ten dzień grubsze prace. Wskazane byłoby wcześniejsze powiadomienie użytkowników o przerwach w pracy systemu. System Unix dostarcza taki mechanizm w postaci kolejnego pliku konfiguracyjnego programu `login`. Plik ten nosi nazwę `motd` (*ang. message of the day*) i znajduje się w katalogu `/etc`. Jest to plik tekstowy, którego zawartość jest wypisywana na ekran podczas podłączania się dowolnego użytkownika do systemu. Użytkownik, który nie chce czytać tej informacji umieszcza w swoim katalogu domowym plik o nazwie `.hushlogin` (zawartość dowolna, np. pusty komendą `touch .hushlogin`).

**18. Utwórz w katalogu `/etc` plik o nazwie `motd` zawierający komunikat o ewentualnym, czasowym wyłączeniu komputera z eksploatacji. Sprawdź, czy komunikat pojawia się podczas podłączania się do systemu. Usuń utworzony plik `motd`.**

Z punktu widzenia administratora systemu istotna jest informacja, kto jest aktualnie podłączony do systemu. Podstawowych informacji udziela komenda `who`. Wynik działania przedstawiono poniżej:

```

1 [bory@thorin bory]$ who
2 bory      tty1      Jul 31 04:28
3 bory      pts/1      Jul 31 04:29
4 wacek     pts/0      Jul 31 02:21
5 bory      pts/3      Jul 31 04:29

```

```

6 root pts/5 Jul 31 04:29
7 zdzicho pts/6 Jul 31 07:11
8 bory pts/2 Jul 31 04:29
9 bory pts/4 Jul 31 04:29
10 bory pts/7 Jul 31 04:29
11 bory pts/8 Jul 31 04:29

```

**19. Zapoznaj się ze składnią komendy `who`. Przy jej pomocy określ czas bezczynności zalogowanych użytkowników.**

Znacznie więcej informacji o użytkownikach podłączonych do systemu udziela komenda `w`. Umożliwia ona między innymi określenie wykorzystania procesora przez procesy uruchamiane z określonego terminala (kolumna JCUPU). Istotna jest również informacja o dacie, czasie pracy systemu (up) oraz średnim obciążeniu systemu (*ang. load average*). Poniżej przedstawiono wynik jej działania.

```

1 [bory@thorin bory]$ w
2 04:33:42 up 6 min, 9 users, load average: 0.06, 0.33, 0.20
3 USER TTY LOGIN IDLE JCUPU PCPU WHAT
4 bory tty1 04:28 5:03 0.12s 0.02s /bin/sh /usr/X11R6/bin/startx
5 bory pts/1 04:29 0.00s 0.08s 0.02s w
6 bory pts/0 04:29 4:21 0.00s 0.35s kdeinit: kwrited
7 bory pts/3 04:29 4:20 0.05s 0.05s /bin/bash
8 bory pts/5 04:29 24.00s 0.12s 0.07s /bin/bash
9 bory pts/6 04:29 4:18 0.08s 0.08s /bin/bash
10 bory pts/2 04:29 4:20 0.04s 0.04s /bin/bash
11 bory pts/4 04:29 4:20 0.05s 0.05s /bin/bash
12 bory pts/7 04:29 4:18 0.05s 0.05s /bin/bash
13 bory pts/8 04:29 4:18 0.08s 0.08s /bin/bash

```

**20. Korzystając z komendy `w` określ ile czasu procesora zużyły procesy użytkownika test.**

Każdy system operacyjny z rodziny Unix przechowuje historię połączeń. Niestety nazwa pliku, w którym jest ta informacja przechowywana oraz jego umiejscowienie w systemie plików zależą od implementacji systemu. Należy pamiętać o ciągłym powiększaniu się jego rozmiaru i okresowo go archiwizować. Komenda, która udostępnia informację to `last`. Poniżej fragment.

```

1 bory pts/8 Thu Jul 31 01:05 - down (01:01)
2 bory pts/4 Thu Jul 31 01:05 - 01:38 (00:33)
3 bory pts/7 Thu Jul 31 01:05 - down (01:01)
4 bory pts/1 Thu Jul 31 01:05 - down (01:01)

```

**21. Gdzie w systemie Linux przechowywana jest historia logowań? Zaproponuj postać komendy, która określi ile razy użytkownik test podłączał się do systemu z urządzenia pts/1.**

Równie często co dodawanie nowego użytkownika w systemie przeprowadza się operację usuwania użytkownika. Większość systemów z rodziny Unix posiada programy narzędziowe do tego celu służące. W przypadku systemu Linux komenda usuwająca użytkownika to `userdel`. Komenda ta użyta z opcją `-r` pozwala usunąć zdefiniowanego w systemie użytkownika oraz jego katalog domowy wraz z zawartością. Wskazane jest jednak wykonanie kopii zapasowej katalogu osobistego, gdyż często zdarza się, że użytkownik usunięty po pewnym czasie potrzebuje swoje dane. Należy dodatkowo sprawdzić, czy użytkownik, którego z systemu usuwamy nie posiada plików w katalogach `/tmp` oraz `/var`.

**22. Usuń z systemu użytkowników test oraz team. Skorzystaj z komendy `userdel`.**

Zdarza się również konieczność usunięcia grupy użytkowników w systemie. We wszystkich systemach z rodziny systemów operacyjnych UNIX nie można usunąć grupy, jeśli jest ona grupą podstawową choć jednego użytkownika. W takim wypadku należy przed usunięciem grupy przenieść użytkownika do innej grupy. Po usunięciu grupy należy sprawdzić, czy w systemie nie istnieją pliki, których właścicielem była usunięta grupa.

23. Zapoznaj się ze składnią komendy `groupdel`. Przy jej pomocy usuń z systemu grupę projekt. Sprawdź, czy w odpowiednich plikach konfiguracyjnych znikła informacja o usuniętej grupie.
24. Wyświetl informacje na temat wcześniej utworzonych plików `pliktest` oraz `plikteam`. Kto jest obecnie ich właścicielem.