Użytkownicy

Zaraz po zakończeniu instalacji systemu (lub w jej trakcie) powinien zostać utworzony użytkownik inny niż *root*. Administrator powinien to zrobić ze względów bezpieczeństwa, gdyż konto *root* daje zbyt wiele uprawnień i można nawet przez pomyłkę spowodować nieodwracalne zmiany w systemie. Źródłem informacji o użytkownikach jest plik */etc/passwd*.

Plik /etc/passwd

W pliku tym w kolejnych liniach przechowywane są informacje o użytkownikach systemu. Przykład takiej informacji o użytkowniku:

```
et:u34werGek.iN0:500:500:Grzegorz Hryn:/home/et:/bin/sh
\/ \___________/ \_/ \_/ \___________/ \_____/ \____/
 |        |       |   |     |             |       |
 |        |       |   |     |             |       +-------- powłoka
 |        |       |   |     |             +--------- katalog domowy
 |        |       |   |    +--------- rzeczywiste  imię i nazwisko
 |        |       |   +-------------------------- numer grupy (GID)
 |        |       +----------------------- numer użytkownika (UID)
 |        +------------------------------------- zakodowane hasło
 +-------------------------------------nazwa użytkownika (login)
```

Wyjaśnienia wymaga kilka pól. Pole *hasło* jest używane, jeśli nie korzystamy z opcji ukrywania haseł, co zdarza się w dzisiejszych czasach coraz rzadziej. Wynika to z faktu, że prawa do pliku *passwd* ma każdy użytkownik, co umożliwia skopiowanie go, a następnie poddanie procedurze łamania haseł.
Katalog domowy to katalog, w którym znajdują się pliki konfiguracyjne użytkownika, w tym katalogu użytkownik domyślnie rozpoczyna pracę po zalogowaniu.
Powłoka to program odpowiedzialny za interakcję z użytkownikiem, wykonujący jego polecenia itp. Najczęściej używaną w Linuxie powłoką (ang. *shell*) jest *bash*.

Ukrywanie haseł (shadow password)

W celu wzmocnienia bezpieczeństwa w wielu systemach zaimplementowno system *ukrytych haseł* . Jest to metoda przechowywania zakodowanych haseł w pliku */etc/shadow*, do którego dostęp ma tylko użytkownik *root*. Wówczas plik */etc/passwd* zawiera specjalny znacznik (najczęściej znak *x* w polu hasła) oznaczający, że hasło znajduje się gdzieś indziej. Każdy program dokonujący autoryzacji użytkowników musi mieć ustawiony bit *setuid*. Normalne programy, które potrzebują innych pól, działają bez zmian, odczytując je standardowo z pliku */etc/passwd*.
Zmiana hasła, niezależnie od tego, czy użyty jest system haseł ukrytych, jest możliwe za pomocą polecenia *passwd*

Tworzenie użytkowników

W systemie Linux można dodawać użytkowników na kilka sposobów:

1. Wykorzystując programy graficznego pośrednictwa użytkownika (Gnome, KDE itp), ułatwiające pracę administratora
2. Za pomocą polecenia *adduser* lub *useradd* (szczegółowe informacje na temat składni poleceń można znaleźć w dokumentacji, lub wywołując polecenie *man adduser*)
3. Ręcznie modyfikując plik /etc/passwd. Uwaga: przy tej metodzie należy używać polecenia *vipw*, które umożliwia założenie odpowiednich blokad na system plików, co

zabezpiecza przed równoczesną modyfikacją pliku *passwd* i *shadow* przez kilku użytkowników.

Grupy

Służą do organizacji użytkowników mających dostęp do systemu na tych samych zasadach. W zależności od zadań, które mają wykonywać, programów, do których mogą mieć dostęp, administrator przydziela użytkowników do stworzonych uprzednio grup. Przynależność do grup można sprawdzić przy użyciu polecenia *groups*.

Plik /etc/group

W pliku tym w kolejnych liniach przechowywane są informacje o grupach w systemie. Przykład takiej informacji o grupie *users*:

```
users::100:et,gregh,adamm,testuser
\___/  \_/  \____________________/
 |   |  |           |
 |   |  |           +-------- Członkowie grupy
 |   |  +-------------------- Identyfikator grupy (GID)
 |   +----------------------- Zakodowane hasło
 |                             (puste pole)
 +--------------------------- Nazwa grupy
```

W celu edycji pliku *group* należy użyć narzędzia *vigr*, z tych samych powodów, dla jakich nie należy bezpośrednio edytować pliku */etc/passwd*.

Tworzenie grup

Do tworzenia, usuwania i modyfikacji grup służą odpowiednio polecenia: *groupadd, groupdel* i *groupmod*. Należy pamiętać, że dodawanie użytkownika do grupy odbywa się w pliku */etc/group*. Jedna z grup, do których należy użytkownik jest jego grupą domyślną (np. przy tworzeniu nowego pliku taki atrybut grupy otrzyma plik). Do chwilowej zmiany grupy domyślnej służy polecenie *newgrp*.

Prawa

System Linux, podobnie jak inne systemy z rodziny Unix, wiąże plik (lub katalog) z prawami właściciela tego pliku oraz grupy. Oto wynik polecenia *ls –l* dla pewnego pliku:

```
-rw-r--r--    1 root     root        20754 May 18 04:53 install.log
\________/    \/\__/     \__/        \___/ \__________/ \_________/
   |          |   |        |           |         |          |
   |          |   |        |           |         |          +-nazwa
   |          |   |        |           |         +--data i godzina
   |          |   |        |           |            modyfikacji
   |          |   |        |           +------------rozmiar pliku
   |          |   |        +----------------------------------grupa
   |          |   +-----------------------użytkownik (właściciel)
   |          +-------------------------------------liczba dowiązań
   +-----------------------------------------------------------prawa
```

Prawa określane są w następujący sposób:

- pierwszy znak określa, czy jest to plik (znak -), czy katalog(litera *d*)
- następne trzy określają prawo, jakie ma właściciel pliku
- kolejne trzy – prawo przysługujące grupie

- ostatnie trzy – prawo przysługujące pozostałym użytkownikom w systemie

W powyższym przykładzie do pliku *install.log* właściciel (użytkownik *root*) ma prawo odczytu i zapisu, grupa *root* prawo do odczytu, podobnie jak inni użytkownicy.
Jedynymi użytkownikami, którzy mogą modyfikować prawa do pliku są jego właściciel oraz użytkownik *root*.
Prawa mogą być przedstawione literowo, jak w powyższym przykładzie (np.: *rwx* to prawa do odczytu, zapisu i wykonania), lub cyfrowo, gdzie wspomagamy się reprezentacją bitową. Trójce *rwx* przypisujemy odpowiednio wartości 2^2, 2^1 i 2^0 a następnie, w zależności czy dany bit jest ustawiony czy nie, mnożymy przez 1 lub 0.
Zatem *rwx* odpowiada $2^2*1+2^1*1+2^0*1 = 7$, *rw* odpowiada 6 itp.
Przedstawiając prawa cyfrowo, podajemy trójkę cyfr, odpowiednio dla właściciela, grupy i pozostałych użytkowników, dla przykładu prawa pliku *install.log* określilibyśmy jako 644.
Należy zwrócić uwagę, że do pewnych operacji na plikach potrzebne są prawa do katalogu, na przykład aby skasować dany plik, do katalogu, w którym on się znajduje, musimy mieć prawo zapisu (*w*).

Polecenia chmod, chgrp i chown

Do zmiany praw dostępu służy polecenie *chmod*. Jako parametry można podać prawa zarówno w postaci symbolicznej (litery *rwx*), jak i cyfrowej. Postać cyfrowa określa wynikowe prawa, natomiast w postaci symbolicznej możemy określić tylko zmianę, np.:
chmod 755 plik
oznacza to, że właściciel będzie miał do pliku wszystkie prawa, natomias grupa i pozostali użytkownicy prawo *rx*. W postaci symbolicznej zapisalibyśmy to samo jako:
chmod u=rwx,g=rx,o=rx plik
Jeśli chcielibyśmy wszystkim (właścicielowi, grupie i innym) dodać prawo do zapisu dla jakiegoś pliku, zapisalibyśmy to następująco:
chmod a+w plik2
Litery użyte w poleceniu *chmod* oznaczają odpowiednio: ***u**ser, **g**roup, **o**ther, **a**ll*.
Do zmiany właściciela pliku służy polecenie *chown*, natomiast do zmiany grupy polecenie *chgrp*.

Dowiązania (links)

W systemie Linux istnieją dodatkowe możliwości odniesienia się do pliku w systemie plików. Są to tak zwane dowiązania. Uzyskujemy je za pomocą polecenia *ln*, lub też polecenia *ln –s*. Pierwsze z tych poleceń tworzy tzw. dowiązanie twarde (ang. *hard link*), które powoduje, że ten sam plik jest widziany również w innym miejscu, innymi słowy jest to ten sam plik, chociaż może być widoczny pod inną nazwą.
Dowiązanie symboliczne jest natomiast jak gdyby wskazaniem na plik lub katalog, jest to wyraźnie przedstawione po wydaniu polecenia *ls –l*.

Prawa specjalne

W systemie Linux istnieją również tzw. prawa specjalne umożliwiające pewne niestandardowe działania. Są to:

- *sticky bit* – powoduje, że po zakończeniu działania program wykonywalny pozostaje w pamięci w celu przyspieszenia kolejnych jego wywołań. Praktycznie teraz nie używany,
- *sUID* – prawo pozwalające programowi lub skryptowi wykonywać się na prawach właściciela. Przykładem takiego programu jest *passwd*, ponieważ zwykły użytkownik

nie ma dostępu do pliku */etc/shadow/* przechowującego hasła, jedyną możliwością jest wykonanie tego programu na prawach użytkownika *root*.

- *gUID* – prawo pozwalające wykonywania z uprawnieniami grupy.

Nadawanie tych praw odbywa się za pomocą programu *chmod* przy czym podając liczbowo prawa, dodajemy dodatkową cyfrę na początku: dla *sticky bit* 1, dla *sUID* 4 a dla *gUID* 2. Przykładowo aby wszystkim nadać prawa do odczytu i wykonania oraz ustawić *sUID*, należy wydać polecenie:
chmod 4555 plik

Literatura

[1] Obowiązkowo: dokumentacja systemu Linux – *man*. Polecenia *adduser, usermod, passwd, chmod, chown, chgrp, newgrp, umask, chsh, ls, ln, find*
[2] Dokumentacja w internecie, np.: *www.jtz.org.pl, www.linuxpl.org, www.redhat.com*
[3] Harold Davis „Po prostu Red Hat Linux 7.2", ISBN: 83-7197-752-2
[4] Mohammed J. Kabir „Red Hat Linux Administrator's Handbook", ISBN: 0764546376
[5] Tim Parker „Linux. Księga eksperta", ISBN: 83-7197-075-7
[6] Tomasz Rak „SuSe Linux 7.2. Czarna księga administratora", ISBN: 83-7197-556-2
[7] Adam Podstawczyński „Linux. Praktyczne rozwiązania", ISBN: 83-7197-326-8

Zadania do wykonania

1. Utworzyć użytkownika za pomocą polecenia *adduser* i ręcznie poprzez modyfikację pliku */etc/passwd*. Wskazówka: należy pamiętać o założeniu katalogu domowego, nadaniu odpowiednich praw i skopiowaniu szablonu z plikami konfiguracyjnymi z katalogu */etc/skel*
2. Przeprowadzić eksperymenty z tworzeniem grup i dodawaniem użytkowników do grup
3. Sprawdzić działanie systemu praw w Linuksie, ze szczególnym naciskiem na zachowanie grup (nadawanie praw do pliku dla grupy), zachowanie praw do plików podczas przenoszenia i kopiowania plików do różnych katalogów (będących własnością różnych użytkowników i mających różne prawa) oraz zachowaniem praw w dowiązaniach do pliku.
4. Sprawdzić działanie poleceń *newgrp* oraz *umask* (szczegóły w dokumentacji *man*)
5. Zapoznanie z działaniem prawa *sUID*