Instrukcja laboratoryjna do ćwiczenia:

Konta użytkowników w systemie LINUX

1. Cel ćwiczenia

Celem ćwiczenia jest zapoznanie z administracją kont użytkowników w systemie linux.

2. Wstęp teoretyczny

Administracja kontami użytkowników sprowadza się w zasadzie do (bezpośredniej lub przy użyciu komend i programów) edycji dwóch plików. Konta użytkowników zdefiniowane w pliku **/etc/passwd**, zaś informacje na temat grup, do których użytkownicy przynależą, zawarte są w pliku **/etc/group**. Każdemu użytkownikowi odpowiada jeden wiersz w pliku **/etc/passwd**, składający się z 7 pól oddzielonych dwukropkami, w postaci:

nazwa_użytkownika : hasło : UID : GID : opis_użytkownika : katalog_osobisty : program_powłoki

Ponieważ plik **/etc/passwd** jest plikiem publicznym, pole 2 przechowujące hasło, może być puste lub może zawierać znak „x". Hasła (w postaci zakodowanej) przechowywane są wtedy w osobnym pliku **/etc/shadow**. Pola 3 i 4 zawierają odpowiednio identyfikator użytkownika (User ID) oraz identyfikator grupy podstawowej (Group ID), do której użytkownik należy. W polu 6 przechowywana jest ścieżka dostępu do katalogu domowego, zazwyczaj **/home/nazwa_użytkownika**. W polu 7 przechowywana jest ścieżka dostępu do programu powłoki (interpretera komend). Za jedną z najlepszych uchodzi powłoka **/bin/bash**. Przykładowy wiersz pliku **/etc/passwd** może zatem wyglądać następująco:

ksiegowy1 : x : 100 : 100 : pan Staszek : /home/ksiegowy1 : /bin/bash

Przed zdefiniowaniem użytkownika należy jednak utworzyć grupę, do której użytkownik będzie przynależeć. W tym celu należy dokonać edycji (bezpośredniej lub pośredniej) pliku **/etc/group**. Każdy wiersz pliku składa się z 4 pól oddzielonych dwukropkami:

nazwa_grupy : hasło : GID : lista_użytkowników_należących_do_grupy

Istotnym polem jest pole 4. Dzięki niemu możliwe jest zdefiniowanie dodatkowych użytkowników przynależących do grupy, nawet jeśli ich grupa podstawowa jest inna. Przykładowy wiersz pliku **/etc/group** może zatem wyglądać tak:

ksiegowi : : 100 : pracownik_kadr1

Z powyższych przykładów wynika, że **ksiegowy1** jest członkiem grupy **ksiegowi**. Należy zwrócić uwagę na fakt, że członkiem tej grupy jest też **pracownik_kadr1**, którego grupą podstawową może być np. grupa **kadry**. Użytkownik ten może zatem korzystać z przywilejów obu grup.

Plik **/etc/shadow** zawiera zakodowane hasła oraz opcjonalne informacje na temat wieku hasła. Każdy wiersz pliku składa się z 9 pól oddzielonych dwukropkami:

- nazwa użytkownika,
- zakodowane hasło,
- liczba dni, licząc od 1 stycznia 1970r, kiedy hasło było ostatni raz zmieniane,
- liczba dni, przed których upływem niemożliwa jest zmiana hasła,
- okres ważności hasła, czyli liczba dni, po których upływie konieczna jest zmiana hasła,
- liczba dni, jaka musi dzielić hasło od przedawnienia, by użytkownik był ostrzegany,
- liczba dni po przedawnieniu hasła, po których konto jest blokowane,
- liczba dni od 1 stycznia 1970r określająca datę, kiedy konto jest automatycznie blokowane,
- pole zarezerwowane.

Jeżeli w polu 2 przed zakodowanym hasłem znajdują się dwa wykrzykniki, świadczy to o blokadzie konta. Odblokowanie konta wiąże się z koniecznością edycji pliku i usunięcia wykrzykników. Wpisanie wartości 0 w pole 3 wymusza na użytkowniku zmianę hasła przy najbliższym logowaniu się. Wartość 0 w polu 4 lub 5 oznacza brak limitów związanych z możliwością i koniecznością zmiany hasła. Podanie w polu 4 wartości większej, niż w polu 5 uniemożliwia zmianę hasła. Puste pole 8 oznacza, że konto nie zostanie zablokowane automatycznie. Przykładowy wiersz pliku **/etc/shadow** może wyglądać następująco:

ksiegowy1 : !!skjdfnxsajiwf : 0 : 0 : 30 : 7 : 5 : 14000 :

W powyższym przykładzie okres ważności hasła użytkownika **ksiegowy1** wynosi 30 dni (pole 5). Pierwsza zmiana hasła możliwa jest natychmiast od momentu założenia konta (pole 4). Komunikaty o konieczności zmiany hasła zaczną się pojawiać na 7 dni (pole 6) przed upływem okresu ważności hasła. Jeżeli użytkownik w po okresie 5 dni (pole 7) nie zmieni hasła, konto zostanie automatycznie zablokowane. Wartość „0” w polu 3 oznacza, że użytkownik musi zmienić hasło przy następnym logowaniu do systemu. Pole 8 informuje o tym, że konto wygasa po upływie 14000 dni od dnia 1 stycznia 1970r, czyli dnia 1 maja 2008r. W polu 2 znajduje się hasło użytkownika w postaci zakodowanej. Dwa wykrzykniki na początku tego pola świadczą o tym, że konto jest aktualnie zablokowane.

Jeżeli konto użytkownika założone jest poprawnie, nowo utworzony użytkownik może się zalogować i wylogować z systemu przy użyciu odpowiednich poleceń **login**, **logout**.

Podsumowując, w celu utworzenia konta użytkownika, należy kolejno wykonać poniższe działania:

1. Utworzyć grupę użytkowników (edycja pliku **/etc/group**).
2. Utworzyć użytkownika (edycja pliku **/etc/passwd**).
3. Określić reguły dotyczące hasła użytkownika (edycja pliku **/etc/shadow**, pozostawiając puste pole 2).
4. Zmienić hasło nowo utworzonego użytkownika (polecenie **passwd nazwa_użytkownika** – pole 2 pliku **/etc/shadow** zostanie zapisane).

5. Utworzyć katalog domowy użytkownika, odpowiednio zmienić jego właściciela, przypisać mu odpowiednią grupę i określić uprawnienia dostępu (polecenia **chown**, **chmod**, **chgrp**).

3. Zadania do wykonania

W pewnej firmie planuje się zinformatyzowanie dwóch działów: księgowości oraz kadr. W tym celu zakupiono dwa moduły, finansowo-księgowy (FK) i kadrowo-płacowy (KP), pracujące pod systemem operacyjnym linux.

Należy utworzyć konto dla każdego użytkownika systemu komputerowego oraz przydzielić mu prawa do użytkowania katalogów z oprogramowaniem tak, aby:

1. Pracownik miał pełne prawa do dostępu do wszystkich plików z danymi aplikacji oraz z prawami tylko do wykonania dla plików wykonywalnych aplikacji.
2. Każdy pracownik miał własny prywatny katalog z pełnymi prawami

Pracowników należy podzielić na 2 grupy,

a) Tylko z dostępem do FK – pracownicy finansów i księgowości,
b) Tylko z dostępem do KP – pracownicy działu kadr.

Należy również utworzyć konto dla właściciela firmy. Właściciel musi mieć pełne prawo dostępu zarówno do FK jak i KP. W trakcie pierwszego logowania należy wymusić zmianę hasła przez każdego użytkownika. Dodatkowo należy utworzyć konto studentowi zatrudnionemu na okres wakacji, któremu wraz zakończeniem stażu (dnia 30.09) konto wygaśnie. Student powinien mieć uprawnienia pracownika finansów i księgowości.

4. Przydatne wskazówki

Zakładamy, że moduł finansowo-księgowy znajduje się w katalogu **/FK**. Należy utworzyć ten katalog, utworzyć wewnątrz niego kilka podkatalogów oraz kilka przykładowych plików. Analogicznie należy postąpić przy tworzeniu katalogu **/KP**. W każdym z katalogów powinien znajdować się przynajmniej jeden program wykonywalny.

Sprawdzenia poprawności utworzonych kont można dokonać przy użyciu menedżera użytkowników dostępnym w **kmenu / system**. Uruchomienie menedżera wiąże się z koniecznością zmiany hasła użytkownika **root**.

UWAGA! Kategorycznie zabrania się zapisywania jakichkolwiek danych na dyskach twardych komputerów! Zapis jakichkolwiek danych do podkatalogów zaczynających się nazwą **hd** w katalogu **/mnt** może prowadzić do uszkodzenia zawartych tam danych.