System operacyjny Linux

Paweł Rajba

pawel.rajba@continet.pl
http://kursy24.eu/

Zawartość modułu 3

- Zarządzanie użytkownikami
  - Użytkownicy i grupy
  - Katalogi domowe
  - Hasła
  - Pliki konfiguracyjne
  - Polecenia konsolowe
  - Moduł YaST-a
- Łamanie haseł użytkowników

Użytkownicy i grupy

- Kilka uwag wstępnych
  - Każdy użytkownik i grupa ma w systemie swoją nazwę i swój identyfikator
  - Każdy plik w systemie musi mieć właściciela
  - Każdy użytkownik musi należeć do co najmniej jednej grupy (grupa podstawowa)
  - Administratorem jest użytkownik root (id=0)
  - Zwykły użytkownik nie może mieć praw root-a

Użytkownicy i grupy

- Katalogi domowe
  - zalecana osobna partycja
  - zalecany system quota
- Przykłady katalogów domowych
  - `/home/pawel`
  - `/root`
  - `/home/math/steinhaus`

Hasła

- Krótka historia
  - klasyczne podejście: jawny plik z hasłami, szyfrowanie algorytmem DES
  - sposób autoryzacji: zaszyfrować hasło i porównać z szyfrogramem
  - problem: komputery były coraz szybsze
  - ukrycie haseł w pliku shadow
  - obecne rozwiązanie: połączenie md5 i shadow

Hasła

- Kilka uwag o hasłach
  - powinno się składać z co najmniej 6-8 znaków
  - znaki powinny z następujących kategorii: małe litery, wielkie litery, cyfry, znaki interpunkcyjne
  - jeśli hasło już musimy zapisać, to tak, żeby nikt nie mógł tego podglądnąć
  - nie należy się chwalić jakie to fajne hasło udało nam się wymyślić

Hasła

- Kilka uwag o hasłach
  - jeżeli już musimy komuś podać hasło, to należy je zmienić jak najszybciej
  - nie należy korzystać z konta admina systemu do normalnej pracy np. przeglądania internetu
  - hasło należy zmieniać co najmniej raz na 3 miesiące
  - raczej nie należy korzystać z możliwości zapamiętania hasła w aplikacjach

Powłoka i pliki poczty

- Powłoka
  - bash, tcsh, sh
- Pliki poczty
  - **`/var/mail (/var/spool/mail)`**
  - lokalne skrzynki np. **`~/Mail`**
    - zależy od programu pocztowego

Pliki konfiguracyjne

- Dane o użytkownikach – plik **/etc/passwd**
  - Schemat jednego wiersza w pliku:
    - konto – nazwa użytkownika, bez wielkich liter
    - hasło – zakodowane hasło lub znak x
    - UID – id użytkownika
    - GID – id grupy
    - imienazwisko – informacja o użytkowniku
    - katalog – katalog domowy
    - powłoka – program uruchamiany po zalogowaniu
  - Kolejne sekcje oddzielone są znakiem dwukropka

Pliki konfiguracyjne

- Plik z hasłami - **/etc/shadow**
  - Schemat pojedynczego wiersza w pliku
    - nazwa użytkownika
    - zaszyfrowane hasło
    - liczba dni od 1.1.1970 do daty ostatniej zmiany hasła
    - liczba dni od ostatniej zmiany hasła, podczas których nie można zmienić hasła
    - liczba dni od ostatniej zmiany hasła, po których zmiana hasła jest wymagana
    - liczba dni przed wygaśnięciem hasła, podczas których użytkownik będzie informowany o konieczności zmiany hasła

Pliki konfiguracyjne

- Plik z hasłami - **/etc/shadow**
  - Schemat pojedynczego wiersza w pliku c.d.
    - liczba dni licząc od ostatniego dnia kiedy można było zmienić hasło, podczas których użytkownik może jeszcze zmienić hasło
      - po tych dniach konto zostanie zablokowane
      - po zablokowaniu niezbędny jest kontakt z administratorem systemu,
    - liczba dni od 1.1.1970 do momentu, do dnia w którym konto zostało zablokowane,
    - zarezerwowane

Pliki konfiguracyjne

- Grupy użytkowników – plik **/etc/group**
  - Schemat wiersza w pliku:
    - nazwa grupy
    - hasło grupy
    - GID
    - lista użytkowników w grupie (np. bea, pawel)

Narzędzia do zarządzania kont

- Omówimy następujące polecenia konsolowe:
  - useradd, userdel, usermod
  - groupadd, groupdel, groupmod
  - passwd, gpasswd, su, sg, newgrp
  - users, last, groups, id, finger, who

Polecenie useradd

- Tworzy nowego użytkownika
- Składnie:
  - useradd [-c komentarz] [-d katalog] [-m] [-g gid] [-G grupa,...] [-s powłoka] [-u uid] nazwauzytkownika
  - useradd --show-defaults
  - useradd --save-defaults [-d katalog] [-f liczba] [-g gid] [-G grupa,...] [-s powłoka]

Polecenie useradd

- Opis opcji:
  - -c komentarz – informacje o użytkowniku
  - -d katalog – katalog domowy
  - -g gid – ID grupy podstawowej
  - -G grupa,... – lista grup dodatkowych, których nowy uzytkownik powinien być członkiem,
    np. dialout,uucp,video,audio

Polecenie useradd

- Opis opcji:
  - -m – zostanie utworzony katalog domowy użytkownika oraz zostanie do niego skopiowana domyślna konfiguracja
  - -s powłoka – powłoka uruchomieniowa
  - -u uid – jawnie podajemy ID użytkownika

Polecenie useradd

- Domyślne ustawienia
  - **/etc/default/useradd** – plik z parametrami domyślnymi
  - **/etc/skel/** – lokalizacja z domyślnymi plikami dla nowo tworzonego użytkownika

Polecenie userdel

- Usuwa użytkownika z systemu
- Składnia:
  - userdel [-r] nazwauzytkownika
- Opcje:
  - -r – usunięcie dodatkowo całego katalogu domowego wraz z zawartością

Polecenie usermod

- Zmienia ustawienia konta
- Składnia:
  - usermod [-c komentarz] [-d katalog [-m]]
    [-f liczba] [-g gid] [-G grupa,...] [-s powłoka] [-u uid]
    [-l login] nazwa_uzytkownika
- Opcje:
  - -d katalog [-m] – tworzy nowy katalog domowy; jeśli dodatkowo jest opcja -m, przenosi zawartość ze starego katalogu domowego do nowego,
  - -l login – nowa nazwa użytkownika
  - pozostałe opcje jak w useradd

Polecenie groupadd

- Tworzy grupę
- Składnia:
  - groupadd [-g gid] [-p hasło] nazwa
- Opcje:
  - -g gid – jawnie podajemy ID grupy,
  - -p hasło – podajemy hasło dla grupy
    - **hasło jest w postaci zaszyfrowanej**

Polecenie groupdel

- Usuwa grupę
- Składnia
  - groupdel nazwagrupy

Polecenie groupmod

- Zmienia ustawienia grupy
- Składnia
  - groupmod [-g gid] [-p haslo] nazwa
- Opcje:
  - -g gid – zmieniamy ID grupy,
  - -p hasło – podajemy nowe hasło dla grupy
    - **hasło jest w postaci zaszyfrowanej**

Polecenie passwd

- 1. Zmienia hasło dla konta
  - Składnia
    - passwd [nazwauzytkownika]
  - Opcje
    - nie podanie nazwy użytkownika powoduje próbę zmiany hasła dla bieżącego użytkownika

Polecenie passwd

- 2. Ustawienie informacji o użytkowniku
  - Składnia
    - passwd -f [nazwauzytkownika]
  - Opcje
    - nie podanie nazwy użytkownika powoduje próbę zmiany hasła dla bieżącego użytkownika

Polecenie passwd

- 3. Konfiguracja konta
  - Składnia:
    - passwd {-l | -u | -d | -e} nazwa
  - Opcje:
    - -l – blokowanie konta,
    - -u – odblokowanie konta,
    - -d – usunięcie hasła,
    - -e – użytkownik będzie musiał zmienić hasło przy kolejnym logowaniu.

Polecenie passwd

- 4. Konfiguracja konta
  - Składnia:
    - passwd [-n min] [-x max] [-w liczba] [-i liczba] nazwa
  - Opcje:
    - -n min – ilość dni, podczas których nie można zmienić hasła,
    - -x max – ilość dni, po których zmiana hasła jest wymagana
    - -w liczba – ilość dni przed wygaśnięciem hasła, podczas których użytkownik będzie informowany o konieczności zmiany hasła,
    - -i liczba – ilość dni, które pozostały użytkownikowi do zmiany hasła zanim jego konto zostanie zablokowane.

Polecenie passwd

- 5. Pobieranie informacji o kontach
  - Składnia:
    - passwd -S [-a | nazwa]
  - Opcje:
    - nazwa – informacja koncie nazwa
    - -a – informacja o wszystkich kontach

Polecenie gpasswd

- Zarządza hasłem grupy
  - Składnia:
    - gpasswd [-r] grupa
  - Opcje:
    - -r – podanie tej opcji powoduje usunięcie hasła; niepodanie tej opcji spowoduje ustawienie hasła

Polecenie su

- Zmienia UID i GID bieżącego użytkownika
- Składnia
  - su [-c polecenie] [-] [uzytkownik]
- Opcje
  - - – sprawia, że powłoka będzie powłoką logowania,
  - -c polecenia – zamiast przełączyć się na użytkownika, wykonamy jako ten użytkownik polecenie

Polecenie su

- Uwagi
  - nie podając nazwy użytkownika przełączamy się na użytkownika root
  - root może się przełączyć na dowolnego użytkownika bez podania hasła

Polecenie sudo

- Pozwala na wykonanie polecenia jako inny użytkownik
- Składnia
  - sudo [-u użytkownik] polecenie
  - sudoedit [-u użytkownik] ścieżka-do-pliku
  - sudo { -v | -k }
- Opcje
  - -v – powoduje przedłużenie zapamiętania hasła
  - -k – powoduje natychmiastowe zapomnienie hasła

Polecenie sudo

- Uwagi:
  - Po wykonaniu polecenie jako ktoś inny hasło jest zapamiętywane (domyślnie na 5 minut, można to zmienić w pliku konfiguracyjnym)
  - Polecenie sudoedit służy do edycji plików
    - jest wtedy tworzony plik tymczasowy na prawach uruchamiającego sudoedit
  - Plikiem konfiguracyjnym polecenia sudo jest plik
    - /etc/sudoers

Polecenie sudo

- Plik /etc/sudoers
  - Aliasy
    - User_Alias WEBMASTERS = pawel, michal
    - Host_Alias SERVERS = dc, www, ftp, mail, ns
    - Host_Alias LAB31 = 10.2.31.0/24
    - Cmnd_Alias KILL = /usr/bin/kill
    - Cmnd_Alias HALT = /usr/sbin/halt
    - Cmnd_Alias PRINTING = /usr/sbin/lpc, /usr/bin/lprm

Polecenie sudo

- Plik /etc/sudoers
  - Wartości domyślne
    - Defaults
    - Defaults:użytkownik
    - Defaluts@Host
  - Przykłady
    - Defaults syslog=auth
    - Defaults passprompt="Witaj %u - podaj swoje hasło:"
    - Defaults:pawel timestamp_timeout=-1
    - Defaults:enemy timestamp_timeout=0

Polecenie sudo

- Plik /etc/sudoers
  - Składnia nadawania uprawnień
    - user komputer=(jakokto) polecenia
  - Przykłady
    - root ALL=(ALL) ALL
    - pawel localhost=(root) NOPASSWD: KILL
    - pawel cassiopeia=(root) NOPASSWD: /usr/sbin/useradd,
    - pawel cassiopeia=(root) PASSWD: /usr/sbin/userdel
    - pawel cassiopeia=(ala,basia) NOPASSWD: /bin/ls

Polecenie sg, newgrp

- Zmienia GID bieżącego użytkownika
- Składnia
  - sg [-l | -c command] group
- Opcje
  - -l – odtwarza zmienne środowiskowe, uruchomiona będzie powłoka logowania
  - -c command – uruchomione zostanie polecenie na prawach podanej grupy

Polecenie sg, newgrp

- Działanie
  - tworzy nową powłokę, w której efektywnym ID grupy jest ID grupy podanej jako parametr
    ALBO
    uruchamia polecenie w nowej powłoce, w której efektywnym ID grupy jest ID grupy podanej jako parametr
  - można wybrać tę grupę, do której użytkownik już należy lub tę, do której zna hasło

Polecenie users

- Wyświetla nazwy aktualnie zalogowanych użytkowników
- Składnia:
  - users

Polecenie last

- Wyświetla historię logowań
- Składnia
  - last [-liczba | -num liczba] [-a] [uzytkownik]
- Opis opcji
  - -liczba, -num liczba – ilość wyświetlanych wierszy
  - -a – nazwa hosta będzie jako ostatnia kolumna
  - podanie użytkownika filtruje wpisy na dotyczące tego użytkownika

Polecenie groups

- Wyświetla grupy do których należy bieżący lub inny użytkownik
- Składnia
  - groups [nazwa_uzytkownika]

Polecenie id

- Wyświetla informacje o identyfikatorach i nazwach użytkowników
- Składnia:
  - id [-u | -g | -G] [-n] [nazwa]
- Opcje:
  - -u – wyświetla ID użytkownika
  - -g – wyświetla ID grupy podstawowej użytkownika
  - -G – wyświetla ID wszystkich grup, do których należy użytkownik
  - -n – zamiast ID będą wyświetlane nazwy

Polecenie finger

- Wyświetla informacje o użytkowniku
- Składnia:
  - finger [-l] [użytkownik]
- Opcje:
  - -l – wyświetla pełne informacje
- Plik .plan

Polecenie who

- Wyświetla informacje o aktualnie zalogowanych użytkownikach
- Składnia:
  - who [-HT]
- Opcje:
  - -H — drukuje listę z nagłówekiem
  - -T — do listy dołącza dodatkową informację, czy do użytkownika można wysyłać komunikaty:
    - + : można
    - - : nie można)
    - ? : nie znaleziono terminala

Polecenie who

- Wyświetla informacje o aktualnie zalogowanych użytkownikach
- Składnia:
  - who -q
- Opis wyniku
  - w pierwszym wierszu drukuję listę zalogowanych użytkowników
  - w drugim wierszu podaje ilość zalogowanych użytkowników

Polecenie who

- Podaje bieżący poziom pracy
- Składnia:
  - who -r

Moduł YaST-a

- Prezentacja modułu YaST do zarządzania kontami i grupami użytkowników

Łamanie haseł

- Będziemy do tego używać programu John the Ripper
- Program jest dostępny na stronie
  - http://www.openwall.com/john/
- No to zaczynamy!
  - Pobieramy źródła znajdujące się pod adresem:
    - http://www.openwall.com/john/f/john-1.7.0.2.tar.gz
  - Przenosimy do /usr/src
  - Kompilujemy (make linux-x86-mmx)

Łamanie haseł

- Cd.
  - Teraz możemy przenieść całość jakieś ustronne miejsce (np. do katalogu root)
  - W katalogu run mamy program,
    a w katalogu doc – dokumentację
  - Poleceniem unshadow przygotowuje plik do łamania
    - unshadow /etc/passwd /etc/shadow > /root/mypasswd
  - Uruchamiamy poleceniem john /root/mypasswd
  - Możemy jeszcze użyć opcji --wordlist

Łamanie haseł

- Cd.
  - Możemy jeszcze użyć opcji
    - --wordlist – jeśli chcemy podać inny niż domyślny słownik
    - --users – ,,testować" wybranych użytkowników
    - --show – zobaczyć złamane hasła
  - Mamy też możliwość tworzenia sesji
    - ale to przećwiczymy na laboratorium

