

Konta użytkowników

Przygotował Michał Tracewicz 2019

Spis treści

1. [Historia](#)
 2. [Pliki](#)
 3. [Administracja kontami użytkowników](#)
 4. [Zasoby systemowe](#)
 5. [Quoty](#)
 6. [Bibliografia](#)
-

Historia

System GNU-Linux powstał w roku 1991. Jest on oparty na systemie UNIX (lata 70-te dwudziestego wieku) wywodzącym się z Bell Labs. Co za tym idzie był on od początku projektowany z założeniem, że będzie to system przeznaczony na którym będzie możliwość pracy wielu użytkowników.

Pliki

Uprawnienia do plików

W systemach Linux możemy wyświetlić listę plików za pomocą polecenia ls.

```
ls -la
drwxr-xr-x 1 mtracewicz mtracewicz 4096 Oct  4 09:05 .oh-my-zsh
```

Kolejno od lewej wpis zawiera:

- Typ pliku:
 1. - dla plików zwykłych
 2. **d** dla katalogów
 3. **c** dla plików specjalnych
 4. **b** dla plików specjalnych przypisanych
 5. **l** dla łączy symbolicznych
- **Uprawnienia kolejno dla:**
 1. Użytkownika
 2. Grupy
 3. Innych

Dla każdej z tych kategorii możemy wyróżnić trzy rodzaje uprawnień

(Myślnik '-' oznacza, że dany użytkownik nie posiada danego prawa)

W wypadku gdy jest to plik nie będący katalogiem

- r - oznaczające możliwość czytania
- w - oznaczające możliwość edycji
- x - oznaczające możliwość uruchomienia

W wypadku przeciwnym

- r - oznaczające możliwość czytania plików zawartych w katalogu
- w - oznaczające możliwość tworzenia i usuwania plików w katalogu
- x - oznaczające możliwość dostępu do katalogu

Możemy to interpretować jako:

- r-x prawo dostępu do katalogu
- x prawo dostępu do plików o znanej nazwie

Uprawnienia te możemy również zapisać w postaci trzech liczby w systemie ósemkowym.

Gdzie:

0	---	4	r--
1	--x	5	r-x
2	-w-	6	rw-
3	-wx	7	rwX

- Liczba łączy
- Właściciel
- Grupa
- Objętość
- Data i godzina ostatniej modyfikacji
- Nazwa pliku

Możemy modyfikować uprawnienia dostępu za pomocą polecenia chmod.

Poniżej przykład użycia:

```
#nadajemy użytkownikowi możliwość uruchomienia pliku
chmod u+x exampleFile
#nadajemy grupie prawo edycji pliku
chmod g+w exampleFile
#odbieramy pozostałym użytkownikom możliwość czytania pliku
chmod o-r exampleFile
#odbieramy wszystkim użytkownikom możliwość uruchomienia pliku
chmod a-x exampleFile
#ustawiamy uprawnienia w formacie rwxr-xr-x
chmod 755 exampleFile
```

Mamy możliwość zmiany właściciela pliku oraz grupy za pomocą polecenia chown.

```
#zmieniamy właściciela pliku exampleFile na użytkownika mtracewicz a grupę na student.  
chown mtracewicz:student exampleFile  
#zmieniamy właściciela folderu exampleDir oraz wszystkich zawartych w nim plików na mtracewicz.  
chown -R mtracewicz exampleDir
```

Alternatywnie możemy zmienić grupę pliku za pomocą polecenia chgrp.

```
#zmieniamy grupę pliku example file na student  
chgrp student exampleFile
```

W systemie Linux informacje o użytkownikach znajdują się w plikach:

- /etc/passwd
- /etc/group
- /etc/shadow

Plik /etc/passwd

W tym pliku przechowywane są informacje o użytkownikach.

```
#Wszyscy użytkownicy mają możliwość odczytu pliku, gdybyśmy ją odebrali  
niebylibyśmy w stanie zmienić użytkownika a wiele aplikacji przestało by działać  
poprawnie nie mając dostępu do danych w nim dostępnych(stąd późniejszy podział  
na /etc/passwd i /etc/shadow)  
-rw-r--r-- 1 root root 1594 10-02 21:50 /etc/passwd  
#Przykładowy wpis w pliku /etc/passwd na Manjaro Linux  
mtracewicz:x:1000:1001:Michał Tracewicz:/home/mtracewicz:/bin/bash  
#|---1---|2|-3--|-4--|-----5-----|-----6-----|----7-----  
#Składnia:  
#1 - nazwa użytkownika  
#2 - hasło(zwykle znajdziemy tu x ponieważ aktualnie przechowuje się je w pliku  
/etc/shadow)  
#3 - id użytkownika  
#4 - id grupy  
#5 - komentarz/opis/informacja o użytkowniku  
#6 - folder domowy  
#7 - powłoka domyślna
```

Plik /etc/group

W tym pliku przechowywane są informacje o poszczególnych grupach w systemie. Dla przykładu

```
-rw-r--r-- 1 root root 988 10-03 14:42 /etc/group
#Przykładowy wpis w pliku /etc/group na Manjaro Linux
sys:x:3:bin,mtracewicz
#|1|2|3|-----4-----
#Składnia
#1 - nazwa grupy
#2 - hasło(zwykle puste ale może zawierać zaszyfrowane hasło)
#3 - id grupy
#4 - lista użytkowników należących do grupy
```

Możemy sprawdzić do jakich grup należy dany użytkownik poprzez użycie polecenia groups.

```
#Przykład użycia polecenia groups dla użytkownika mtracewicz
groups mtracewicz
wheel lp sys network power autologin vboxusers mtracewicz
```

Plik /etc/shadow

W tym pliku przechowujemy hasła użytkowników.

```
#Możemy zauważyć, że w przeciwieństwie do poprzednich plików plik /etc/shadow
może być zarówno czytany jak i edytowany przez użytkownika root
-rw----- 1 root root 922 10-02 21:50 /etc/shadow
#Przykładowy wpis w pliku(wzięty z https://www.slashroot.in/how-are-passwords-
stored-linux-understanding-hashing-shadow-utils i delikatnie zmodyfikowany)
testUser:$1$Etg2ExUZ$F9NTP7omafhKI1qabMqng1:15651:0:99999:7:::
#-1-|-----2-----|--3--|4|--5--|6|7|8|9
#1 - nazwa użytkownika
#2 - zaszyfrowane hasło(poniżej przykładu znajduje się informacja o tym jak
wygląda ten proces)
#3 - ile dni minęło od ostatniej zmiany hasła
#4 - ile minimalnie dni jest wymaganych między zmianami hasła(jak często można
zmieniać hasło)
#5 - ile maksymalnie dni jest dopuszczalne między zmianami hasła
#6 - na ile dni przed następną wymaganą zmianą hasła użytkownik dostanie
ostrzeżenie
#7 - ile dni po wygaśnięciu hasła konto będzie wyłączone
#8 - po ilu dniach od 01.01.1970r. konto zostanie wyłączone
#9 - pole jeszcze nie obecnie używane
```

W jaki sposób hasła są zabezpieczane?

Hasło przechowywane w pliku /etc/shadow możemy podzielić na trzy części rozdzielone znakiem '\$'. Przyjmuje ono postać \$ID\$SALT\$HASHED.

Algorytm hashujący - algorytm który z podanych danych tworzy unikatowy ciąg znaków zadanej długości. Jest to funkcja, której nie da się w prosty sposób odwrócić tzn. znając hash nie możemy odzyskać danych wejściowych (To odróżnia algorytm hashujący od szyfrującego, ten drugi jest odwracalny).

ID jest to wartość wskazująca jakiego algorytmu hashującego użyto. Może on przyjąć wartości:

- 1 - oznacza algorytm MD5(Nie jest zalecane jego użycie, obecnie jest łatwy do złamania)

- 2 - oznacza algorytm Blowfish
- 2a - oznacza algorytm eksblowfish
- 5 - oznacza algorytm SHA-256
- 6 - oznacza algorytm SHA-512

Salt jest to losowo wygenerowany ciąg znaków, który jest łączony z hasłem użytkownika w celu zwiększenia bezpieczeństwa.

HASHED jest to wartość wynikowa algorytmu hashującego na hasło użytkownika połączonym z saltem.

Co daje nam salt?

Salt pomaga nam zabezpieczyć nasze hasła przed atakami typu dictionary attack czy rainbow table(więcej o tym w następnym podpunkcie). Dzięki zastosowaniu wartości salt nawet dwa dokładnie te same hasła będą posiadały inny hash. Co za tym idzie nawet jeżeli osobie atakującej udało się złamać jedno hasło nie będzie ona w stanie znaleźć osoby o identycznym hasle ponieważ ich zahaszowana wartość będzie inna.

Jak można łamać hasła?

Najprostszym sposobem łamania haseł są tak zwany dictionary attack i rainbow table.

Pierwszy z nich to atak oparty na prostej metodzie siłowej gdzie znając algorytm hashujący próbujemy użyć go na wszystkich prawdopodobnych hasłach(najczęściej robi się to sprawdzając listę najczęstszych haseł oraz dodając do niej te same hasła tylko ze zmienioną wielkością liter czy podmieniając litery na cyfr np. 'A' -> 4, 'O' -> 0 itp.) i znaleźć takie, które zgadza się z jednym z tych które pozyskaliśmy.

Drugi sposób to pozyskanie bazy w której najpopularniejsze hasła są już zahaszowane wraz z informacją tym jaki algorytm został użyty. Następnie sprawdzamy czy, któryś z posiadanych przez nas hashy znajduje się w tej bazie i odczytujemy z niej hasło.

W pierwszym przypadku zużywamy niewiele pamięci jednak bardzo dużo mocy obliczeniowej, w drugi ataku jest dokładnie odwrotnie. Przed oboma tymi atakami pomaga nam bronić się wartość salt. Dzięki generowaniu losowej wartości do naszych haseł mamy niemal pewność, że hash, który uzyskamy(nawet jeżeli użytkownik ustawi sobie hasło = hasło123!) nie znajdzie się w żadnej z rainbow tables. W przypadku dictionary attack dodanie wartości salt masowo zwiększa ilość możliwości, które atakujący musi sprawdzić a co za tymi idzie zwiększamy czas, który musi poświęcić na próbę złamania każdego z haseł.

Czym jest silne hasło?

Silne hasło to takie które zawiera minimum osiem znaków, zarówno wielkie jak i małe litery, znaki specjalne i cyfry.

Jeżeli nasze hasło zawiera tylko 8 małych liter to jest ich możliwie 26^8 , natomiast w wypadku bezpiecznego hasła jest ich minimum 56^8 (liczba ta jest większa zależnie od tego jakie znaki dopuszczamy jako znaki specjalne).

Dodatkowo należy pamiętać, że długość hasła ma istotny wpływ na jego bezpieczeństwo. Jak już pokazaliśmy ośmioznakowych haseł jest $\sim 56^8$ natomiast dodanie np. czterech znaków znacząco zwiększa ilość możliwości 56^{12} . Pokazuje to, że każdy kolejny znak zwiększa ilość obliczeń, którą musi wykonać ktoś, kto próbuje zgadnąć nasze hasło.

Warto także pamiętać o tym, że hasło nie powinno zawierać żadnych danych z nami związanych takich jak imię, nazwisko czy rok urodzenia.

Administracja kontami użytkowników

Wyświetlanie listy aktywnych użytkowników

W systemie Linux możemy wyświetlić listę aktywnych użytkowników za pomocą polecenia `users`.

```
users
#W normalnym systemie wynikiem tego polecenia jest lista aktualnie zalogowanych
użytkowników
test testUser exampleUser
```

Polecenie to nie zawiera żadnych opcji.

Wyświetlanie ostatnich logowań użytkowników

W systemie Linux możemy wyświetlić listę ostatnich logowań użytkowników za pomocą polecenia `last`.

```
#polecenie wyświetli logowania użytkownika mtraciewicz w kolejności od
najstarszych do najnowszych możemy także wyświetlić dla konkretnego tty/host
last mtraciewicz
#przykładowy wpis
mtraciewicz pts/9      188.147.44.127.nat.umn.pl  4 paź 09:15 - 09:18  (00:02)
#----1----|--2-----|-----3-----|-----4-----|
#1 - nazwa użytkownika
#2 - tty(nazwa terminalu)
#3 - host z którego użytkownik się loguje/miejsce dostępu
#4 - data początku - końca logowania i w nawiasie czas trwania
```

Dodawanie użytkowników

W systemie Linux możemy dodać użytkownika za pomocą polecenia `useradd`.

```
#polecenie, które doda do systemu użytkownika test, pobierze domyślne wartości z
pliku /etc/default/useradd może zostać wykonane tylko przez użytkownika root lub
użytkownik posiadający uprawnienia do polecenia sudo
useradd test
#jeżeli chcemy utworzyć katalog domowy użytkownikowi musimy użyć opcji -m
useradd -m test
#jeżeli użyjemy opcji -d możemy utworzyć katalog domowy w miejscu innym niż
domyślne
#jeżeli chcemy dodać użytkownika do grup użyjemy opcji -G
useradd test -G student,inf
#w tym wypadku utworzymy użytkownika test i dodamy go do grup student i inf
#jeżeli chcemy ustawić np. po ilu dniach wygasa hasło użyjemy opcji -K
useradd test -K PASS_MAX_DAYS = 3
#jeżeli chcemy dodać komentarz jak np. imię i nazwisko to użyjemy opcji -c
useradd test -c "Jan Kowalski"
```

Usuwanie użytkowników

W systemie Linux możemy usunąć użytkownika za pomocą polecenia `userdel`

```
#tym poleceniem usuniemy użytkownika test, może zostać wywołane tylko przez
użytkownika root lub użytkownik posiadający uprawnienia do polecenia sudo
userdel test
#jeżeli chcemy usunąć także katalog domowy użytkownika użyjemy opcji -r
userdel -r test
```

Modyfikacja użytkowników

W systemie Linux możemy modyfikować użytkownika za pomocą polecenia usermod.

```
#tym poleceniem zmienimy katalog domowy użytkownika test na katalog /test
usermod -d /test test
#jeżeli chcemy wraz ze zmianą katalogu domowego przenieść do niego pliki ze
starego używamy opcji -m
usermod -d /test -m test
#tym poleceniem zmienimy login użytkownika test na jankowalski
usermod -l test jankowalski
#tym poleceniem zmienimy id użytkownika test na 1000
usermod -u 1000 test
#tym poleceniem zmienimy główną grupę użytkownika test na pracownik(grupa musi
już istnieć)
usermod -g pracownik test
#tym poleceniem dodamy wiele grup(student,informatyka) dla użytkownika test.
Opcja -a sprawia, że użytkownik nie utraci obecnie przypisanych grup
usermod -a -G student,informatyka test
#tym poleceniem zmienimy datę wygaśnięcia konta użytkownika test na pierwszy
stycznia 2020. Data musi być w formacie YYYY-MM-DD
usermod -e 2020-01-01 test
#tym poleceniem zmienimy powłokę użytkownika test na zsh
usermod -s /bin/zsh test
```

Zmiany hała

W systemie Linux możemy modyfikować hasło użytkownika za pomocą polecenia passwd.

```
#Każdy użytkownik może zmienić własne hasło
passwd
#Wyświetli nam się taki komunikat
Changing password for mtracewicz.
#Zostaniemy poproszeni o aktualne hasło
Current password:
#Następnie o nowe hasło
New password:
#Oraz powtórzenie w celu potwierdzenia
Retype new password:
#Użytkownik root może zmodyfikować hasło dowolnego użytkownika. Tym poleceniem
zmienimy hasło użytkownika test(jako root nie zostaniemy zapytani o poprzednie
hasło)
passwd test
#Polecenie passwd pozwala nam też usunąć hasło opcją -d
passwd -d test
```

Jak wymusić zmianę hasła?

Aby wymusić zmianę hasła możemy użyć wcześniej wspomnianego polecenia `passwd` lub dedykowanego polecenia `change`.

```
# Aby wymusić zmianę hasła przy pierwszym logowaniu hasłem nadanym przez root-a
możemy użyć opcji -e
passwd -e test
# Polecenie change służy do zarządzania wygasaniem haseł. Możemy użyć polecenia
change do wyświetlenia aktualnych informacji o danych związanych z hasłem
użytkownika w ten sposób:
change -l mtracewicz
# Możemy zmienić maksymalną ilość dni między zmianami hasła z opcją -M. W tym
przykładzie ustawimy, że użytkownik mtracewicz musi zmienić hasło co maksymalnie
5 dni
change -M 5 mtracewicz
# Jeżeli nie chcemy aby użytkownik zmieniał hasło codziennie możemy użyć opcji -
m. W tym przykładzie zmienimy, że użytkownik mtracewicz będzie mógł zmienić hasło
najczęściej co dwa dni.
change -m 2 mtracewicz
```

Blokowanie / odblokowanie konta

Wcześniej wymienionym poleceniem `usermod` możemy zablokować lub odblokować użytkownika.

```
# tym poleceniem blokujemy użytkownika
usermod -L test
# tym poleceniem odblokujemy użytkownika
usermod -U test
```

Zmiana tożsamości użytkownika

W systemie Linux mamy dwa polecenia służące do zmiany tożsamości: `sudo`, `su`.

Dobre praktyki

Dodawanie grup

W systemie Linux możemy dodać grupę za pomocą polecenia `useradd`.

```
# Tym poleceniem dodamy grupę testGroup
groupadd testGroup
# Z opcją -g możemy sami wybrać id grupy (musi być unikatowe i nie ujemne)
groupadd -g 999 testGroup
```

Usuwanie grup

W systemie Linux możemy usunąć grupę za pomocą polecenia `groupdel`.

```
# Tym poleceniem usuniemy grupę testGroup, grupa musi istnieć i my jako
administratorzy musimy zadbać aby grupa, która usuwamy nie była główną grupą
dla żadnego z użytkowników
groupdel testGroup
```

Modyfikacja grup

W systemie Linux możemy zmodyfikować grupę za pomocą groupmod.

```
#Możemy zmodyfikować id grupy przy użyciu opcji -g
groupmod -g 999 testGroup
#Możemy też zmodyfikować nazwę grupy za pomocą opcji -n. W tym przykładzie
zminimy nazwę grupy testGroup na myGroup
groupmod -n myGroup testGroup
```

Zasoby systemowe

Quoty

Bibliografia

Polecenie last

- <https://www.golinuxhub.com/2014/05/how-to-check-last-login-time-for-users.html>
- man last

Polecenie users

- man users

Sudo

- <https://www.lifewire.com/what-to-know-sudo-command-3576779>

Dostęp do plików

- <http://www.penguintutor.com/linux/file-permissions-reference>
- <http://mediologia.pl/katalogi-i-pliki-linux/2-4-atrybuty-plikow-uzywanych-w-systemie-linux-polecenie-ls>
- <https://www.hostingadvice.com/how-to/change-file-ownershipgroups-linux/>

Pliki z informacjami o użytkownikach/grupach

- <https://www.cyberciti.biz/faq/understanding-etcgroup-file/>
- <http://www.yourownlinux.com/2015/07/etc-passwd-file-format-in-linux-explained.html>

Hasła użytkowników

- <https://www.cyberciti.biz/faq/understanding-etcshadow-file/>
- <https://www.slashroot.in/how-are-passwords-stored-linux-understanding-hashing-shadow-utils>
- <https://blog.jscrambler.com/hashing-algorithms/>

Tworzenie, usuwanie i modyfikacja kont użytkowników

- <https://www.lifewire.com/create-users-useradd-command-3572157>
- <https://www.linuxnix.com/delete-user-account-linux/>
- <https://www.itzgeek.com/how-tos/linux/how-to-modify-user-accounts-in-linux-using-usermod-command.html>

Blokowanie użytkowników

- <https://www.linuxnix.com/lock-user-account-linux/>
- <https://www.2daygeek.com/lock-unlock-disable-enable-user-account-linux/>

Procesy

- <https://linux.101hacks.com/unix/fuser/>
- <https://linux.101hacks.com/unix/top/>
- <https://linux.101hacks.com/monitoring-performance/ps-command-examples/>

Zasoby

- <https://ss64.com/bash/ulimit.html>

Quoty

- <https://www.linux.com/tutorials/step-step-using-user-quotas-linux/>
- <https://www.looklinux.com/how-to-manage-disk-quota-in-linux/>
- https://docs.fedoraproject.org/en-US/Fedora/14/html/Storage_Administration_Guide/ch-disk-quotas.html
- <https://www.howtoforge.com/tutorial/linux-quota-ubuntu-debian/>
- https://wiki.archlinux.org/index.php/Disk_quota
- <https://www.itworld.com/article/2811509/storage-quotas---hard-vs--soft---explained.html>
- https://en.wikipedia.org/wiki/Disk_quota#Common_Unix_disk_quota_utilities

Linux

- <https://en.wikipedia.org/wiki/Linux>
- [The Complete History of Linux \(Abridged\) -Bryan Lunduke](#)