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 inforamcje 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 poszczegulnych 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 popszednich 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$F9NTP7omafhKIlqaBMqng1:15651:0:99999:7:::
#-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 hasło
#4 - ile minimalnie dni jest wymaganych miedzy zmianami hasła(jak często można
zmieniać hasło)
#5 - ile maksymalnie dni jest dopuszczalne między zmianami hasła
#6 - na ile dni przed następną wymaganą zmiany 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 jesze nie obecnie używane
```

W jaki sposób hasła są zabezpieczane?

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

Algorytm hasujący - algorytm który z podanych danych tworzy unikatowy ciąg znaków zadanej długości. Jest to funkcja, której nie da się 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 wartośći:

- 1 - oznacza algorytm MD5
- 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 haśle użytkonika połączonym z saltem.

Co daje nam salt?

Salt pomaga nam zabezpieczyć nasze hasła przed atakami typu dictionary atack 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 haśle ponieważ ich zahaszowana wartość będzie inna.

Jak można łamać hasła?

Najprostszym sposobem łamania haseł są tak zwany dictionary atack 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 liery 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 wktórej najpopularniejsze hasła są już zahaszowa wraz z informacjąo tym jaki algorytm został użyty. Następnie sprawdzamy czy, któryś z posiadanych przez nas hashy znajduję 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 = haslo123!) nie znajdzie się w żadnej z rainbow tables. W przypadku dictionary atack dodanie wartości salt masywnie 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 wilkie 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 jake znaki dopuszczamy jako znaki specjalne).

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

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

Administracja kontami użytkowników

Wyświetlanie listy aktywnych użytkowników

Wyświetlanie ostatnich logowań użytkowników

Zasoby systemowe

Quoty

Bibliografia

Polecenie last(wyświetlenie ostatnich loginów użytkownika)

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

Polecenie users(wyświetlenie aktywnych użytkowników)

- 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 kont użytkowników i edycja haseł

- https://www.lifewire.com/create-users-useradd-command-3572157

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