

Bezpieczeństwo 2018

Zastrzeżenie

To nie jest przewodnik totalny. Jedynie tłumaczy niektóre slajdy, które wydawały mi się zawikłane i musiałem googlować, lub pamiętałem, że sprawiały mi problemy kiedyś.

Poprawki do ortografii i merytoryki walimy pull requestami: [gitrepo](#)

Użytkownicy w systemie UNIX

Linux jest systemem:

- wielozadaniowym,
- wielo-użytkownikowym

UID w systemie UNIX

UID -> ID użytkownika który **STWORZYŁ** ten proces. Może być zmienione, tylko kiedy proces ma EUID=0.

EUID -> [*effective*] używane do ewaluacji zezwoleń procesu. (Tego używasz do stwierdzenia czy proces coś może czy nie.)

SUID -> [*Saved UID*] Daje użytkownikowi prawo do wystartowania aplikacji, nie jako on, ale osoba zapisana.

GID -> ID grupy użytkowników.

[source1](#)

[source2](#)

Ważne miejsca na /

```
# Ten plik ogranicza dostęp do hashy haseł,  
# dla wszystkich, z wyjątkiem najbardziej uprawnionych.  
/etc/shadow  
# Tekstowa baza danych przechowująca dane logowania  
# oraz informacje kto może się zalogować.  
/etc/passwd  
# Plik tekstowy definiujący przynależność do grup.  
/etc/group
```

/etc/passwd

An example record may be:

```
jsmith:x:1001:1000:Joe Smith,Room 1007,(234)555-8910,(234)555-0044,email:/home/jsmith:/bin/sh
```

The fields, in order from left to right, are:^[1]

1. User name: the string a user would type in when logging into the operating system: the [logname](#). Must be unique across users listed in the file.
2. Information used to validate a user's [password](#); in most modern uses, this field is usually set to "x" (or "*", or some other indicator) with the actual password information being stored in a separate [shadow password](#) file. On [Linux](#) systems, setting this field to an asterisk ("*") is a common way to disable direct logins to an account while still preserving its name, while another possible value is "*NP*" which indicates to use an [NIS](#) server to obtain the password.^[2] Without password shadowing in effect, this field would typically contain a cryptographic hash of the user's password (in combination with a [salt](#)).
3. [user identifier](#) number, used by the operating system for internal purposes. It need not be unique.
4. [group identifier](#) number, which identifies the primary group of the user; all files that are created by this user may initially be accessible to this group.
5. [Gecos field](#), commentary that describes the person or account. Typically, this is a set of comma-separated values including the user's full name and contact details.
6. Path to the user's [home directory](#).
7. Program that is started every time the user logs into the system. For an interactive user, this is usually one of the system's [command line interpreters](#) ([shells](#)).

[source](#)

