

### Polecenie su

- Używane już wcześniej polecenie **su** służy do przełączania użytkowników, można też się przełączyć na użytkownika **root**.
- Opcja **-** (minus) lub **-l** powoduje uruchomienie powłoki w trybie **login shell**.

```
foo@debian:~$ id
uid=1000(foo) gid=1000(foo)
groups=1000(foo),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),102(scanner),106(bluetooth),108(lpadmin)
```

```
foo@debian:~$ su -
```

```
root@debian:~# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@debian:~# logout
```

```
foo@debian:~$ id
uid=1000(foo) gid=1000(foo)
groups=1000(foo),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),102(scanner),106(bluetooth),108(lpadmin)
```

- Aby wykonać pojedynczą komendę, można użyć opcji **-c**.

```
foo@debian:~$ id
uid=1000(foo) gid=1000(foo)
groups=1000(foo),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),102(scanner),106(bluetooth),108(lpadmin)
```

```
foo@debian:~$ grep root /etc/shadow
grep: /etc/shadow: Permission denied
```

```
foo@debian:~$ su - -c "grep root /etc/shadow"
Password:
root:y$j9T$TWb ... 2kn0kt1IC/:20434:0:99999:7:::
```

### Delegowanie uprawnień

- W powyższych przykładach, aby zwykły użytkownik mógł wykonać polecenia z prawami użytkownika **root** musiał podać jego hasło.
- Aby zwykły użytkownik mógł wykonywać polecenie z prawami użytkownika **root** bez znajomości hasła, można wydelegować mu prawa do wydawania poleceń za pomocą programu **sudo**.
- Plik konfiguracyjny **/etc/sudoers** **nie może** być edytowany dowolnym edytorem tylko poleceniem **visudo**, które sprawdza poprawność pliku konfiguracyjnego (zwykle używany jest edytor **vi**, może być też **nano**).
- Składnia linii pliku konfiguracyjnego jest następująca:

**user/groupa host = command1, command2, !command3, ...**

oznacza, że użytkownik **foo** może uruchamiać program **fdisk** (podając swoje hasło) na wszystkich komputerach (**ALL**) wydając polecenie **sudo fdisk**.

- **sudo** pozwala na stosowanie aliasów:

```
User_Alias ADMIN = user, foo
Cmd_Alias PRINT = /usr/sbin/lpc
Cmd_Alias FDISK = /usr/sbin/fdisk
ADMIN ALL = PRINT, FDISK
user ALL = NOPASSWD: /usr/bin/passwd [A-z]*, !/usr/bin/passwd root
```

- W powyższym przykładzie użytkownicy **user** i **foo** mogą używać poleceń **lpc** i **fdisk**, ponadto użytkownik **user** może zmieniać hasła innym użytkownikom (polecenie **passwd** z jednym argumentem) za wyjątkiem użytkownika **root**.
- Zwykły użytkownik (**foo**) nie może uruchamiać polecenia **fdisk**.

```
foo@debian:~$ id
uid=1000(foo) gid=1000(foo)
groups=1000(foo),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),102(scanner),106(bluetooth),108(lpadmin)
```

```
foo@debian:~$ fdisk -l
bash: fdisk: command not found
```

- Przy pomocy **visudo** dopisz następującą linię (użytkownik **foo** nie będzie pytany nawet o swoje hasło).

**foo ALL = (root) NOPASSWD: /usr/sbin/fdisk**

```
root@debian:~# visudo
```

- Po wprowadzeniu zmian, sprawdź zawartość pliku.

```
root@debian:~# grep fdisk /etc/sudoers
foo ALL = (root) NOPASSWD: /usr/sbin/fdisk
```

- Wypróbuj działanie polecenia **fdisk**.

```
foo@debian:~$ sudo fdisk -l
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xb0b6628f

Device      Boot      Start         End      Sectors  Size Id Type
/dev/sda1   *           2048    39061503    39059456   18.6G 83 Linux
/dev/sda2             39061504    41940991     2879488    1.4G 82 Linux swap / Solaris
...
```