Współczesne systemy komputerowe

Polecenia jako **root**

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),1
        08(netdev),114(bluetooth),115(lpadmin),119(scanner)
```

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

```
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),1
        08(netdev),114(bluetooth),115(lpadmin),119(scanner)
```

- 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),1
        08(netdev),114(bluetooth),115(lpadmin),119(scanner)
```

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

```
foo@debian:~$ su - -c "grep root /etc/shadow"
Password:
root:$6$CbQp89a     ...     OjjUwGrzZ.:17506:0:99999:7:::
```

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**)
- W pliku **`/etc/sudoers` musi** znajdować się lini:

```
root ALL=(ALL) ALL
```

- Składnia pliku konfiguracyjnego jest następująca:

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

- Linia:

  ```
  foo ALL = /sbin/shutdown
  ```

  oznacza, że użytkownik *foo* może uruchamiać program **shutdown** (podając swoje hasło) na wszystkich komputerach (**ALL**) wydając polecenie **sudo shutdown ...**
- **sudo** pozwala na stosowanie aliasów

  ```
  User_Alias ADMIN = user, foo
  Cmnd_Alias PRINT    = /usr/bin/lpc, /usr/bin/lprm
  Cmnd_Alias SHUTDOWN = /sbin/shutdown
  ADMIN ALL = PRINT, SHUTDOWN
  user  ALL = NOPASSWD: /usr/bin/passwd [A-z]*, !/usr/bin/passwd root
  ```

- Ponadto w powyższym przykładzie 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),1
       08(netdev),114(bluetooth),115(lpadmin),119(scanner)
```

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

- Zainstaluj program **sudo**

```
root@debian:~# apt install sudo
Reading package lists... Done
Building dependency tree
Reading state information... Done

...
```

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

  ```
  user ALL = (root) NOPASSWD: /sbin/fdisk
  ```

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

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

- Wypróbuj działanie polecenia

```
foo@debian:~$ sudo fdisk -l
Disk /dev/sda: 10 GiB, 10737418240 bytes, 20971520 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: 0x717aa925

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 18946047 18944000    9G 83 Linux
/dev/sda2       18946048 20969471  2023424  988M 82 Linux swap / Solaris

...
```