



MANAŽMENT POUŽÍVATEĽOV A SKUPÍN

POUŽITIE PRÍKAZOV SU A SUDO



Teoretická časť

Identitu používateľa meníme pomocou programu *su* (substitute user). Ak zmeníme identitu používateľa pomocou *su* s pomlčkou, t. j. príkazom ***su - username***, novému používateľovi sa načítajú aj jeho systémové nastavenia a pracovný priečinok sa zmení na domovský priečinok používateľa. Program *su* môžeme spúšťať s rôznymi prepínačmi, najčastejšie sa používa *-c*, ktorý umožní pod identitou iného používateľa vykonať jednorazovo nejaký príkaz.

Niektoré distribúcie, napr. Ubuntu nepoužívajú superpoužívateľa *root*. Tento používateľ síce v systéme existuje, ale počas inštalácie sa mu nevytvára heslo. V systéme ho zastupuje používateľ, ktorý má právo používať program *sudo* (superuser do). Právo používať program *sudo* môžeme pridať aj ďalším používateľom, nastavuje sa to v súbore */etc/sudoers*. Používateľovi sa nemusia prideliť všetky práva, dá sa vyšpecifikovať, pod koho identitou a aké príkazy môže spúšťať. Súbor je veľmi dobre okomentovaný. Nachádza sa v ňom hlavne nasledujúci riadok:

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

Tento riadok znamená, že používateľ *root* môže na všetkých systémoch pod identitou všetkých používateľov spúšťať všetky príkazy.

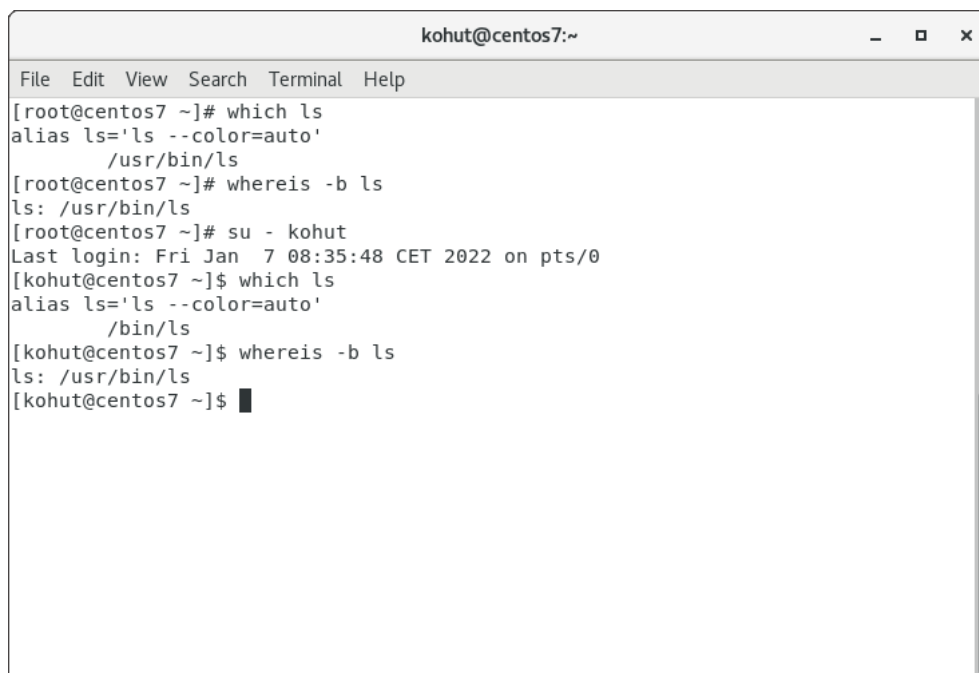
Podobne riadok:

```
straka  myserver=(vrana) /bin/l
```

znamená, že používateľ *straka* môže pomocou programu *sudo* na stroji s názvom *myserver* ako používateľ *vrana* spúšťať príkaz *ls*.

Súbor */etc/sudoers* je v systéme taký dôležitý, že sa nemá editovať bežným textovým editorom, ale pomocou príkazu **visudo**, ktorý kontroluje aj syntax a nedovolí zmeny v súbore v prípade chyby uložiť.

V súbore */etc/sudoers* pridávame používateľom práva na spúšťanie programov pod identitou iných používateľov, pričom do súboru zapisujeme absolútnu cestu k danému programu. V CentOS 7 došlo k zmene vo *FHS* (Filesystem Hierarchy Standard) a napr. */bin* už nie je osobitný priečinok ale iba odkaz na */usr/bin*. Ako je vidieť z Obrázka 1, ani programy *which* a *whereis* nemusia ukázať umiestnenie programu rovnako.



```
kohut@centos7:~  
File Edit View Search Terminal Help  
[root@centos7 ~]# which ls  
alias ls='ls --color=auto'  
/usr/bin/ls  
[root@centos7 ~]# whereis -b ls  
ls: /usr/bin/ls  
[root@centos7 ~]# su - kohut  
Last login: Fri Jan 7 08:35:48 CET 2022 on pts/0  
[kohut@centos7 ~]$ which ls  
alias ls='ls --color=auto'  
/bin/ls  
[kohut@centos7 ~]$ whereis -b ls  
ls: /usr/bin/ls  
[kohut@centos7 ~]$
```

Obrázok 1 Umiestnenie programu *ls* nájdené pomocou programov *which* a *whereis*.



Pomôcky

Virtuálny stroj s CentOS 7 vytvorený vo *VMware vSphere*. Úloha je určená pre jedného žiaka.

Použitie tohto učebného materiálu je určené výhradne pre Duálne vzdelávanie realizované SPŠ elektrotechnickou Košice v spolupráci s Deutsche Telekom IT Solutions Slovakia.

Autor: J. Ploščica
Verzia 3

Predmet: ZIL, 1. ročník
Strana 2 z 6



Úlohy

1. Zapnite virtuálny stroj s CentOS 7 a prihláste sa do jeho grafického režimu ako superpoužívateľ *root*.
2. Zmeňte v termináli svoju identitu na bežného používateľa, ktorého máte v systéme; v prípade používateľa *kohut* použite príkaz **su - kohut**. Ako tento používateľ vyhľadajte umiestnenie programu *ls* pomocou programov *which* a *whereis*. Overte, že na zobrazenie adresárovej štruktúry vášho systému môžete použiť priamo príkaz **ls /**, príkaz obsahujúci absolútnu cestu k programu *ls*, t. j. príkaz **/usr/bin/ls /** ale aj príkaz obsahujúci absolútnu cestu k programu *ls* so symbolickým odkazom, t. j. príkaz **/bin/ls /**.
3. V termináli sa vráťte k superpoužívateľovi *root*. Vytvorte v systéme nových používateľov: *bobrik*, *vydra*, *medved*, *myska*, *kocur*, *husak*, *kacer*. Vytvorte im aj navzájom rôzne heslá.
4. Ako *root* si zobrazte svoju vyhľadávaciu cestu príkazom **echo \$PATH**.
5. Príkazom **su bobrik** zmeňte svoju identitu, príkazmi **pwd** a **echo \$PATH** si overte, že sa stále nachádzate v domovskom priečinku *roota* a že sa vám ani nezmenil obsah premennej *PATH*.
6. Príkazom **exit** sa vráťte k *rootovi* a opäť zmeňte svoju identitu, tento krát príkazom **su - bobrik**. Overte si, že sa nachádzate v domovskom priečinku používateľa *bobrik* a že sa vám zmenil aj obsah premennej *PATH*.
7. Ako *bobrik* si skúste zobraziť obsah domovského priečinka používateľa *vydra* príkazom **ls /home/vydra**.
8. Ako *bobrik* si zobrazte obsah domovského priečinka (aj so skrytými súbormi) používateľa *vydra* tento krát príkazom **su -c "ls -a /home/vydra" vydra**. Musíte samozrejme zadať heslo používateľa *vydra*.
9. Ako *bobrik* vytvorte v domovskom priečinku superpoužívateľa *root* priečinok s názvom *bobdir*. Použite príkaz **su -c "mkdir /root/bobdir"**. Musíte samozrejme zadať heslo superpoužívateľa *root*.
10. Ako *bobrik* si pomocou programu *sudo* skúste prezrieť obsah *rootovho* domovského priečinka. Použite príkaz **sudo ls /root**. Prečítajte si systémové hlásenie, ktoré hovorí, že incident bude reportovaný.

11. Vráťte sa k superpoužívateľovi *root*. Incident sa mu zapísal do mailu. Zobrazte si súbor s mailom, t. j. súbor */var/spool/mail/root* a prečítajte si, k akému incidentu došlo.

12. Prezrite si prístupové práva súboru */etc/sudoers* a otvorte si ho príkazom **visudo**.

13. Súbor si preštudujte a pod riadok:

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

pripíšte riadok:

```
vydra   ALL=(ALL)  ALL
```

Najskôr urobte v syntaxe chybu (nenapíšte pravú zátvorku) a overte, že zmeny v editovanom súbore sa nedajú uložiť. Potom ho napíšte správne a zmeny uložte. Pri použití programu *sudo* má používateľ *vydra* rovnaké práva ako *root*.

14. Zmeňte svoju identitu na používateľa *vydra*. Príkazom **sudo mkdir /root/vyddir** vytvorte v *rootovom* domovskom priečinku priečinok *vyddir*. Na spustenie príkazu sa vyžaduje zadať heslo – nie *roota* ale *vydru*.

15. Príkazom **sudo ls /root** si prezrite obsah *rootovho* domovského priečinka. Heslo zadávať nemusíte do uplynutia predvoleného času (5 min) od predošlého zadania hesla.

16. Použitím programu *sudo* používateľ *vydra* spúšťa programy pod identitou *roota*, ale môže ich spúšťať aj pod identitou iného používateľa. Skúste si ako *vydra* zobrazí obsah domovského priečinka používateľa *bobrik* aj so skrytými súbormi postupne príkazmi:

```
ls -a /home/bobrik
```

```
sudo ls -a /home/bobrik
```

```
sudo -u kocur ls -a /home/bobrik
```

```
sudo -u bobrik ls -a /home/bobrik
```

17. Ako *root* otvorte opäť príkazom **visudo** súbor */etc/sudoers* a pridajte riadok:

```
medved  ALL=(kocur) /bin/ls
```

18. Overte, ktorým z nasledujúcich príkazov si môže používateľ *medved* pozrieť obsah domovského priečinka používateľa *kocur*:

```
ls -a /home/kocur
```

```
sudo ls -a /home/kocur
```

```
sudo -u kocur ls -a /home/kocur
```

19. Overte, že používateľ *medved* nevie spúšťať pod identitou používateľa *kocur* žiadny iný príkaz okrem */bin/ls*. Skúste použiť napr. príkaz: **sudo -u kocur touch /home/kocur/file01**.
20. Ako root pridajte do súboru */etc/sudoers* riadok:
- ```
myska ALL=(root) /bin/su
```
- Overte, že hoci používateľ *myska* môže spúšťať ako *root* len jediný príkaz, v skutočnosti má v systéme rovnaké práva ako *root*, lebo zadáním príkazu **sudo su** a použitím svojho hesla vie zmeniť svoju identitu na *roota*.
21. Overte, že príkazom **sudo su - bobrik** sa vie používateľ *myska* prepnúť bez znalosti jeho hesla aj na používateľa *bobrik*, a teda aj na ľubovoľného iného používateľa.
22. Overte, že používateľ *myska* nevie zmeniť svoju identitu na používateľa *bobrik* príkazom **sudo -u bobrik su - bobrik**.
23. Nastavte, aby používateľ *husak* vedel na všetkých strojoch pod identitou všetkých používateľov spúšťať program *chattr* (spúšťať ho samozrejme bude pod identitou *roota*, lebo bežný používateľ aj tak nemôže nastavovať súborom atribút *i*). Tiež mu nastavte aby mohol bez zadania hesla aktualizovať databázu súborov. Umiestnenie programov *chattr* a *updatedb* si zistíte pomocou programu *which* alebo *whereis*. Potom do */etc/sudoers* pridajte riadok:
- ```
husak ALL=(ALL) /usr/bin/chattr, NOPASSWD: /usr/bin/updatedb
```
24. Zmeňte svoju identitu na používateľa *husak*. Vytvorte v jeho domovskom priečinku súbor *husakovsubor*. Skúste súbor vyhľadať príkazom **locate husakovsubor**.
25. Príkazom **updatedb** skúste ako *husak* aktualizovať databázu súborov. Aktualizujte databázu súborov príkazom **sudo updatedb**. Všimnite si, že príkaz sa vykonal a systém vás nepožiadala o zadanie hesla. Vyhľadajte súbor *husakovsubor* pomocou programu *locate*.
26. Skúste súboru *husakovsubor* pridať atribút *i* (immutable) príkazom **chattr +i husakovsubor**. Skúste to aj príkazom **sudo -u bobrik chattr +i husakovsubor**; tento krát musíte zadať *husakovo* heslo, ale k nastaveniu atribútu nedôjde, lebo používateľ, pod identitou ktorého ste príkaz spustili, na to nemá práva. Nastavte súboru *husakovsubor* atribút *i* príkazom **sudo chattr +i husakovsubor** (heslo

- vás systém nepýta, lebo ste ho zadali pred chvíľou). Príkazom **lsattr husakovsubor** overte, že príslušný súbor má naozaj nastavený atribút *i*.
27. Vráťte sa k superpoužívateľovi *root* a ako tento používateľ sa pokúste zmazať súbor */home/husak/husakovsubor*. Súboru odoberte atribút *i* príkazom **chattr -i /home/husak/husakovsubor** a potom ho zmažte.
28. Vytvorte skupinu s názvom *instalovaci*. Túto skupinu priradíte ako sekundárnu skupinu používateľom *bobrik* a *kacer*.
29. Nastavte, aby používatelia patriaci do skupiny *instalovaci* mohli pod ľubovoľnou identitou spúšťať programy *rpm* a *yum*, ktoré sú určené na inštalovanie softvérových balíčkov. Do súboru */etc/sudoers* pridajte riadok:
- ```
%instalovaci ALL=(ALL) /bin/rpm, /usr/bin/yum
```
30. Zmeňte svoju identitu na používateľa *bobrik* a ako tento používateľ nainštalujte pomocou programu *yum* nejaký nový balíček, napr. *mc* (Midnight Commander) príkazom **sudo yum install mc**.
31. Vráťte sa k superpoužívateľovi *root*, v */etc/sudoers* vytvorte *User\_Alias VYTVARACI* a priradíte k nim používateľov *bobrik* a *husak*, t. j. na vhodné miesto pridajte riadok:
- ```
User_Alias VYTVARACI = bobrik, husak
```
32. V */etc/sudoers* vytvorte alias pre príkaz s názvom *CREATE* a priradíte k nemu programy *touch* a *mkdir*, t. j. na vhodné miesto pridajte riadok:
- ```
Cmnd_Alias CREATE = /bin/touch, /bin/mkdir
```
33. Nastavte, aby používatelia s aliasom *VYTVARACI* mohli pod identitou všetkých používateľov spúšťať príkazy priradené k aliasu *CREATE*. Pridajte do */etc/sudoers* riadok:
- ```
VYTVARACI ALL=(ALL) CREATE
```
34. Zmeňte svoju identitu na používateľa *husak* a v *rootovom* priečinku vytvorte priečinok *husakdir* a prázdny súbor *husakfile*.
35. Vráťte súbor */etc/sudoers* do pôvodného stavu, zmažte súbory a priečinky, ktoré ste vytvorili v domovskom priečinku *roota* a odstráňte všetkých vytvorených používateľov.