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. AlmaLinux na vykonávanie systémových zmien používajú predvolene účet superpoužívateľa *root*, v iných ako je napr. Ubuntu, *roota* zastupuje používateľ, ktorý má právo používať program *sudo* (superuser do). V Ubuntu účet *roota* síce existuje, ale počas inštalácie sa mu nevytvára heslo.

Právo používať program *sudo* môžeme pridať aj ďalším používateľom; dá sa to nastaviť v súbore */etc/sudoers* alebo v osobitnom súbore, ktorý je potrebné vytvoriť v priečinku */etc/sudoers.d*. Používateľovi sa nemusia prideliť všetky práva; dá sa vyšpecifikovať, pod koho identitou a aké príkazy môže spúšťať. Riadky s nastavením môžu vyzerať napr. takto (v popise je vysvetlený ich význam):

a) *straka ALL=(ALL) ALL*
   Používateľ *straka* môže na všetkých systémoch pod identitou všetkých používateľov spúšťať všetky príkazy.

b) *vrana ALL=(ALL:ALL) ALL*
   Používateľ *vrana* môže na všetkých systémoch pod identitou všetkých používateľov a všetkých skupín spúšťať všetky príkazy.

c) *vrabec ALL=(stehlik:spevavce) ALL*
   Používateľ *vrabec* môže na všetkých systémoch pod identitou používateľa *stehlik* a pod identitou členov skupiny *spevavce* spúšťať všetky príkazy.

d) *sykora myserver=(root) /usr/bin/ls*

Používateľ *sykora* môže na počítači s hostiteľským menom *myserver* pod identitou používateľa *root* spúšťať príkaz */usr/bin/ls*.

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

Pomôcky

Počítač s OS Windows, na ktorom je nainštalovaný *Oracle VM VirtualBox* a v ňom vytvorený virtuálny stroj s Ubuntu. Úloha je určená pre jedného žiaka.

Úlohy

1. Zapnite virtuálny stroj s Ubuntu, prihláste sa do jeho grafického režimu ako používateľ so *sudo* právami; v tomto materiáli to bude používateľ *Milan Kohut.*
2. Otvorte si terminál, vytvorte v ňom troch nových používateľov *husak*, *kacer* a *moriak.* Vytvorte im aj heslá.
3. Zmeňte v termináli svoju identitu na používateľa *husak* príkazom **su - husak**.
4. Ako *husak* si skúste zobraziť obsah domovského priečinka superpoužívateľa *root* príkazom **ls /root**. Príkaz sa skončí chybou, lebo ako používateľ *husak* nemáte práva prezerať si obsah priečinka */root*.
5. Ako *husak* si skúste zobraziť obsah domovského priečinka superpoužívateľa *root* príkazom **su -c "ls root" kacer**. Musíte pritom zadať heslo používateľa *kacer*. Príkaz sa skončí chybou, lebo ani používateľ *kacer* nemá práva prezerať si obsah priečinka */root*.
6. Ako *husak* si zobrazte obsah domovského priečinka superpoužívateľa *root* príkazom **su -c "ls root"**. Musíte pritom zadať heslo superpoužívateľa *root.*
7. Ako *husak* si pomocou programu *sudo* skúste prezrieť obsah *rootovho* domovského priečinka príkazom **sudo ls /root**. Musíte pritom zadať heslo používateľa *husak*. Príkaz sa nevykoná, ale neskončí sa ani chybou. Do terminálu sa však vypíše systémová hláška:

   husak is not in the sudoers file. This incident will be reported.

8. V termináli sa príkazom **exit** vráťte k používateľovi *kohut.* Príkazom **sudo tail /var/log/auth.log** si zobrazte posledné riadky súboru */var/log/auth.log* a vo výpise nájdite, aký príkaz sa pomocou *sudo* pokúšal spustiť používateľ *husak.*
9. Prezrite si prístupové práva súboru */etc/sudoers* potom si príkazom **sudo head /etc/sudoers** zobrazte prvé riadky tohto súboru. Všimnite si pritom, že sa príkaz vykoná bez toho, aby ste museli zadať heslo používateľa *kohut* (predtým ste už úspešne použili *sudo* a nasledujúcich 5 minút ho môžete používať bez potreby zadávania hesla). Z výpisu vyplýva:
    a) Vzhľadom na vlastníctvo (*root, root*) a prístupové práva (*r--r*-----), ktoré má súbor */etc/sudoers* je problém robiť v ňom zmeny. Je potrebné editovať ho ako *root* príkazom **visudo**.
    b) Tento súbor sa nemusí editovať; potrebné zmeny je možné robiť v osobitných súboroch, ktoré treba vytvoriť v priečinku */etc/sudoers.d* (pri použití tejto možnosti sa ale nekontroluje syntax a prípadná chyba môže spôsobiť, že príkaz *sudo* prestane fungovať).
10. Používateľovi *husak* nastavte, aby mohol pod identitou ľubovoľného používateľa spúšťať pomocou *sudo* akýkoľvek príkaz. Overte si aj funkčnosť zmeny, ktorú ste vykonali. Postupujte podľa nasledujúcich pokynov:
    a) Ako *kohut* príkazom **sudo visudo** otvorte súbor */etc/sudoers* (príkaz je trochu zavádzajúci, súbor by sa mal otvoriť v editore *vi*, ale v Ubuntu je ako predvolený editor nastavené *nano*). Pod riadok:

        root ALL=(ALL:ALL) ALL

        pripíšte riadok:

        husak ALL=(ALL) ALL

        Najskôr urobte v syntaxe chybu (nenapíšte pravú zátvorku) a overte, že zmeny v editovanom súbore sa nedajú uložiť (po vypísaní chyby stlačte *Enter* a potom si pomocou *e* zvoľte, že chcete pokračovať v editovaní súboru). Po oprave zmeny uložte a ukončite editor *nano.*
    b) Zmeňte svoju identitu na používateľa *husak* príkazom **su - husak**. Príkazom **sudo su -** zmeňte pomocou hesla používateľa *husak* svoju identitu na superpoužívateľa *root*. Potom sa príkazom **exit** vráťte k používateľovi *husak*.
    c) Príkazom **sudo touch /home/kacer/file01** vytvorte v domovskom priečinku používateľa *kacer* súbor *file01.* Príkazom **sudo ls -l ~kacer** si

zobrazte podrobný obsah priečinka */home/kacer*; mal by obsahovať súbor *file01*, ktorého vlastníkom je *root* a patrí skupine *root.*

d) Použitím programu *sudo* je možné spúšťať programy nielen pod identitou *roota*, ale aj pod identitou iného používateľa. Skúste vytvoriť v domovskom priečinku používateľa *kacer* súbor *file02*; použite postupne príkazy:

touch /home/kacer/file02

sudo -u kohut touch /home/kacer/file02

sudo -u kacer touch /home/kacer/file02

Úspešný bude len v poradí tretí príkaz. Príkazom **sudo ls -l ~kacer** si zobrazte podrobný obsah priečinka */home/kacer*; porovnajte vlastníctvo súborov *file01* a *file02.*

e) Príkazom **exit** sa v termináli vráťte k používateľovi *kohut.*

11. Používateľovi *kacer* nastavte, aby mohol pod identitou ľubovoľného používateľa spúšťať pomocou *sudo* akýkoľvek príkaz. Overte si aj funkčnosť zmeny, ktorú ste vykonali. Postupujte podľa nasledujúcich pokynov:

a) Príkazom **sudo nano /etc/sudoers.d/pouzivatelia** otvorte v editore *nano* doteraz neexistujúci súbor *pouzivatelia* a vložte doňho riadok:

kacer ALL=(ALL) ALL

Zmenu v súbore uložte a ukončite editor.

b) V termináli príkazom **su - kacer** zmeňte svoju identitu na používateľa *kacer* a ako *kacer* pomocou príkazu **sudo passwd root** zmeňte *rootovi* heslo.

c) Príkazom **exit** sa vráťte k používateľovi *kohut*.

12. Používateľ *kohut* môže používať príkaz *sudo* rovnakým spôsobom ako používatelia *husak* a *kacer*, pritom riadok:

kohut ALL=(ALL) ALL

sa nenachádza ani priamo v súbore */etc/sudoers* ani v žiadnom súbore v priečinku */etc/sudoers.d.* Overte si túto skutočnosť.

13. Príkazom **sudo cat /etc/sudoers** si vypíšte obsah súboru */etc/sudoers*; výpis obsahuje aj nasledujúce riadky:

 # Allow members of group sudo to execute any command

%sudo ALL=(ALL:ALL) ALL

Príkazom **grep sudo /etc/group** si overte, že skupina s názvom *sudo* naozaj existuje a používateľ *kohut* je jej členom.

14. Používateľovi *moriak* nastavte, aby mohol pod identitou ľubovoľného používateľa spúšťať pomocou *sudo* akýkoľvek príkaz. Overte si aj funkčnosť zmeny, ktorú ste vykonali. Postupujte podľa nasledujúcich pokynov:
    a) Príkazom **sudo usermod -G sudo moriak** pridajte používateľa *moriak* do skupiny s názvom *sudo.*
    b) Príkazom **su - moriak** zmeňte svoju identitu na používateľa *moriak*.
    c) Príkazom **sudo useradd kocur** vytvorte nového používateľa *kocur*, pomocou **sudo passwd kocur** mu vytvorte aj heslo.
    d) Príkazom **sudo nano /etc/sudoers.d/pouzivatelia** zeditujte súbor */etc/sudoers.d/pouzivatelia* v editore *nano* a pridajte doňho nasledujúci riadok:

        kocur ALL=(kacer) /usr/bin/mkdir

        Zmenu uložte a editor zavrite
    e) Príkazom **exit** sa vráťte k používateľovi *kohut.*
15. V termináli zmeňte svoju identitu na používateľa *kocur* a overte si, čo môže tento používateľ robiť pomocou príkazu *sudo*. Postupujte podľa nasledujúcich pokynov:
    a) Skúste vytvoriť v domovskom priečinku používateľa *kacer* priečinok *dir01* príkazom **sudo mkdir ~kacer/dir01**. Príkaz sa nevykoná; používateľ *kocur* má síce právo spúšťať pomocou *sudo* príkaz */usr/bin/mkdir* ale iba ako používateľ *kacer.* Keďže ste nešpecifikovali používateľa príkaz sa spustil pod identitou *roota*.
    b) Vytvorte v domovskom priečinku používateľa *kacer* priečinok *dir01* príkazom **sudo -u kacer mkdir ~kacer/dir01**. Príkaz sa tento krát úspešne vykoná.
    c) Skúste príkazom **sudo -u kacer mkdir ~husak/dir01** vytvoriť priečinok *dir01* v domovskom priečinku používateľa *husak*. Príkaz sa nevykoná, lebo používateľ *kacer*, pod identitou ktorého ste príkaz spustili nemá práva vytvárať priečinky v priečinku */home/husak.*
    d) Skúste príkazom **sudo -u kacer touch ~kacer/file03** vytvoriť v domovskom priečinku používateľa *kacer* súbor *file03*. Príkaz sa nevykoná, lebo používateľ *kocur* nemá právo pomocou *sudo* spúšťať iný príkaz ako */usr/bin/mkdir.*
    e) Príkazom **exit** sa v termináli vráťte k používateľovi *kohut*.

16. Vytvorte nového používateľa *vydra*, vytvorte mu aj heslo.
17. S využitím *sudo* zeditujte súbor */etc/sudoers.d/pouzivatelia a* riadok týkajúci sa používateľa *kocur* upravte nasledovne:

    kocur ALL=(root) /usr/bin/su
18. Zmeňte v termináli príkazom **su - kocur** svoju identitu na používateľa *kocur*. Overte, že hoci používateľ *kocur* môže spúšťať ako *root* len jediný príkaz, v skutočnosti má v systéme rovnaké práva ako *root*, lebo zadaním príkazu **sudo su -** a použitím svojho hesla vie zmeniť svoju identitu na *roota.* Po úspešnej zmene identity sa v termináli vráťte späť k používateľovi *kocur*.
19. Overte, že príkazom **sudo su - vydra** sa vie používateľ *kocur* prepnúť bez znalosti jeho hesla aj na používateľa *vydra*, a teda aj na ľubovoľného iného používateľa (*root* pri zmene identity na iného používateľa nemusí zadávať žiadne heslo).
20. V termináli sa vráťte k používateľovi *kohut.*
21. Príkazom **which locate** vyhľadajte absolútnu cestu k programu *locate.* Ak je výpis prázdny, znamená to, že program nemáte nainštalovaný; nainštalujte si ho príkazom **sudo apt install plocate**.
22. Nastavte, aby používateľ *vydra* 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. Potrebnú zmenu urobte v súbore */etc/sudoers.d/pouzivatelia*; pridajte doňho riadok:

    vydra ALL=(ALL) /usr/bin/chattr, NOPASSWD: /usr/bin/updatedb
23. Zmeňte v termináli príkazom **su - vydra** svoju identitu na používateľa *vydra.* V jeho domovskom priečinku vytvorte príkazom **touch vydrovsubor** súbor *vydrovvsubor.* Skúste súbor vyhľadať príkazom **locate vydrovsubor**.
24. Príkazom **updatedb** skúste ako *vydra* aktualizovať databázu súborov. Aktualizujte databázu súborov príkazom **sudo updatedb**. Všimnite si, že príkaz sa vykonal a systém vás nepožiadal o zadanie hesla. Vyhľadajte súbor *vydrovsubor* pomocou programu *locate.*
25. Skúste súboru *vydrovsubor* pridať atribút *i* (immutable) príkazom **chattr +i vydrovsubor**. Nastavte súboru *vydrovsubor* atribút *i* príkazom **sudo chattr +i**

vydrovsubor, tentokrát musíte zadať aj heslo používateľa *vydra.* Príkazom **lsattr vydrovsubor** overte, že príslušný súbor má naozaj nastavený atribút *i*.

26. V termináli sa vráťte k používateľovi *kohut* a ako tento používateľ sa pokúste zmazať súbor */home/vydra/vydrovsubor* najskôr príkazom **rm ~vydra/vydrovsubor**, potom príkazom **sudo rm ~vydra/vydrovsubor** . Súboru odoberte atribút *i* príkazom **sudo chattr -i ~vydra/vydrovsubor** a potom ho zmažte pomocou **sudo rm ~vydra/vydrovsubor**.
27. Vytvorte troch ďalších používateľov *medved*, *vlk* a *liska*. Vytvorte im aj heslá.
28. Vytvorte skupinu s názvom *instalovaci*. Túto skupinu priraďte ako sekundárnu skupinu používateľom *medved* a *vlk.*
29. Nastavte, aby používatelia patriaci do skupiny *instalovaci* mohli pod ľubovoľnou identitou spúšťať programy na inštalovanie balíčkov *dpkg* a *apt.* Vytvorte kvôli tomu v */etc/sudoers.d* súbor *skupiny* a pridajte doňho nasledujúci riadok:

    %instalovaci ALL=(ALL) /usr/bin/dpkg, */usr/bin/apt*
30. Zmeňte v termináli svoju identitu na používateľa *medved* a ako tento používateľ nainštalujte pomocou programu *apt* nejaký nový balíček, napr. *mc* (Midnight Commander) príkazom **sudo apt install mc**.
31. V termináli sa vráťte k používateľovi *kohut.* V */etc/sudoers.d* vytvorte súbor a*liasy* a vložte doňho obsah podľa nasledujúcich pokynov:
    a) Vytvorte *User_Alias VYTVARACI* a priraďte k nim používateľov *vlk* a *liska*, t. j. pridajte do súboru riadok:

        User_Alias VYTVARACI = vlk, liska
    b) Vytvorte alias pre príkaz s názvom *CREATE* a priraďte k nemu programy *touch* a *mkdir*, t. j. pridajte do súboru riadok:

        Cmnd_Alias CREATE = /usr/bin/touch, /usr/bin/mkdir
    c) Nastavte, aby používatelia s aliasom *VYTVARACI* mohli pod identitou všetkých používateľov spúšťať príkazy priradené k aliasu *CREATE*, t. j. pridajte do súboru riadok:

        VYTVARACI ALL=(ALL) CREATE
32. Zmeňte v termináli svoju identitu na používateľa *liska* a v *rootovom* domovskom priečinku vytvorte s využitím *sudo* priečinok *liskadir* a prázdny súbor *liskafile.*
33. V termináli sa vráťte používateľovi *kohut.* Odstráňte postupne všetko, čo ste počas práce na tomto materiáli vytvorili. Postupujte podľa nasledujúcich pokynov:
    a) Zmažte všetky súbory, ktoré ste vytvorili v priečinku */etc/sudoers.d.*

b) Vráťte súbor */etc/sudoers* do pôvodného stavu.

c) Zmažte súbory a priečinky, ktoré ste vytvorili v domovskom priečinku *roota*.

d) Odstráňte skupinu *instalovaci.*

e) Odstráňte všetkých vytvorených používateľov.