VLASTNÍCTVO A PRÍSTUPOVÉ PRÁVA

ATRIBÚTY, ŠPECIÁLNE PRÍSTUPOVÉ PRÁVA, POUŽÍVATEĽSKÁ MASKA

Teoretická časť

Okrem prístupových práv môže superpoužívateľ *root* nastavovať súborom aj atribúty. Atribúty súboru je možné prezerať pomocou programu *lsattr*, nastavovať pomocou *chattr*. Najčastejšie sa súboru nastavuje atribút *i* – imutable (nezmeniteľný). Takýto súbor nie je možné upravovať ani mazať bez ohľadu na prístupové práva.

Okrem štandardných prístupových práv, existujú aj nasledujúce špeciálne prístupové práva:

a) *SUID* bit – používa sa pre súbory; ak je nastavený a *others* majú právo súbor spúšťať, súbor sa spustí s právami vlastníka. Príkladom súboru, ktorý má nastavený tento bit je napr. program */usr/bin/passwd* pomocou ktorého si môžu používatelia meniť heslo. Hašované heslo sa potom uloží do súboru */etc/shadow*, do ktorého bežní používatelia nemôžu nielen zapisovať, ale ho ani čítať. Vlastníkom programu */usr/bin/passwd* je *root* a keďže má tento súbor nastavený *SUID* bit, bežný používateľ ho spúšťa s právami *roota* a program preto dokáže zapisovať do */etc/shadow.*

b) *SGID* bit – ak sa používa pre súbory, má podobný význam ako *SUID* bit. Ak je nastavený a *others* majú právo súbor spúšťať, súbor sa spustí s právami skupiny, ktorá súbor vlastní. Príkladom môže byť program */usr/bin/wall*, pomocou ktorého môže používateľ napísať správu ostatným prihláseným používateľom. Tento súbor má nastavený *SGID* bit a patrí skupine *tty*, ktorá vlastní všetky terminály. Ak je *SGID* bit nastavený na priečinok, používateľ, ktorý má v ňom právo vytvárať súbory ich vytvorí

tak, že súbor vlastní nie predvolená skupina tohto používateľa ale skupina vlastniaca priečinok. Toto nastavenie potom umožňuje používateľom patriacim do tejto skupiny upravovať ten istý súbor.

c) *Sticky* bit – kedysi sa používal pre súbory. Súbor, ktorý ho mal nastavený zostával po spustení a ukončení v RAM pamäti. Dnes sa používa hlavne pre priečinky. Ak má priečinok nastavené všetky prístupové práva, používatelia v ňom môžu vytvárať súbory a priečinky, ale aj mazať súbory vytvorené inými používateľmi. Ak má ale priečinok nastavený naviac aj *sticky* bit, používatelia môžu mazať a upravovať iba vlastné súbory a priečinky. Príkladom takéhoto priečinka je priečinok */tmp.*

Keď používateľ vytvára nový súbor alebo priečinok, prístupové práva sa priradia odčítaním používateľskej masky od predvolenej hodnoty, ktorá je pre súbory 666 a pre priečinky 777.

Pomôcky

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

Úlohy

1. Zapnite virtuálny stroj s CentOS 7 a prihláste sa do jeho grafického režimu ako superpoužívateľ *root*.
2. V termináli zmeňte svoju identitu na bežného používateľa, nech je to napr. *hruska*.
3. Ako *hruska* sa presuňte do svojho domovského adresára, vytvorte v ňom neprázdny súbor *file1* a odoberte mu všetky prístupové práva.
4. Overte, že ako *hruska* nemôžete upravovať obsah tohto súboru ani si ho prezerať.
5. V termináli sa vráťte k superpoužívateľovi *root* a overte, že máte plný prístup k súboru *file1*, ktorý vytvoril *hruska* (*root* nepatrí medzi ostatných, preto sa ho nastavené prístupové práva netýkajú).

6. Vytvorte ako *root* v priečinku */root* súbor *file2.* Odoberte mu všetky práva a overte, že aj keď je *root* vlastník súboru a nemal by mať práva k tomuto súboru, môže ho aj čítať aj upravovať. Vzhľadom na nastavené prístupové práva pre priečinok */root* môže tento súbor aj mazať. Zmažte ho.
7. Vytvorte ako *root* v jeho domovskom priečinku *file3* a nastavte mu všetky prístupové práva.
8. Ako *root* nastavte súboru *file3* atribút *imutable* príkazom **chattr +i file3**. Nastavené atribúty si prezrite príkazom **lsattr file3**. Overte, že súbor nemôžete upravovať ani pomocou editora *vim.* Overte tiež, že mu nemôžete meniť prístupové práva ani ho zmazať.
9. Ako *root* odoberte súboru *file3* atribút *imutable* príkazom **chattr -i file3** a súbor zmažte.
10. Ako používateľ *hruska* sa presuňte do jeho domovského priečinka. Z predchádzajúcich úloh by tam mal byť súbor *file1*, ktorý nemá nastavené žiadne prístupové práva.
11. Súboru *file1* postupne nastavte *SUID* bit*, SGID* bit a *sticky* bit príkazmi:
    a) **chmod u+s file1**
    b) **chmod g+s file1**
    c) **chmod o+t file1**

    Po vykonaní každého jednotlivého príkazu si overte zmenu prístupových práv pomocou príkazu **ls -l**.
12. Nastavte súboru *file1* prístupové práva príkazom **chmod a+rwx file1**. Všimnite si, ako sa zmenilo označenie špeciálnych prístupových práv.
13. Odoberte špeciálne práva súboru *file1* príkazom **chmod ug-s,o-t file1**.
14. Nastavujte súboru *file1* prístupové práva pomocou číselných hodnôt *0777*, *1777*, *2777*, *3777*, *4777*, *5777*, *6777*, *7777*. Zmeny si vždy overte pomocou **ls -l**.
15. Ako *hruska* zmažte súbor *file1* z jeho domovského priečinka.
16. Ako *hruska* vyhľadajte umiestnenie programu *passwd* a potom si zobrazte jeho prístupové práva. Všimnite si, že má nastavený *SUID* bit.
17. Ako *hruska* si zobrazte prístupové práva súboru */etc/shadow.*

18. Ako *hruska* sa pokúste programom *cat* zobraziť obsah súboru */etc/shadow.* Potom sa pokúste otvoriť tento súbor v editore *vim.* Na prezeranie ani úpravu tohto súboru nemajú bežní používatelia práva.
19. Ako *root* si v inom pseudoterminál zobrazte obsah súboru */etc/shadow.*
20. Ako *hruska* si príkazom **passwd** zmeňte heslo. Najskôr musíte zadať aktuálne heslo, potom nové a pre kontrolu zadať nové ešte raz. Pre silu hesiel platia isté pravidlá; ak mení používateľské heslo *root*, systém ho na to, že je heslo slabé iba upozorní, bežnému používateľovi nedovolí takéto heslo nastaviť.
21. Ako *root* si v pseudoterminál opäť zobrazte obsah súboru */etc/shadow.* Overte si, že sa hašované heslo u používateľa *hruska* zmenilo.
22. Vyhľadajte umiestnenie programu *vim*, prezrite si jeho vlastníka a ako *root* mu pridajte *SUID* bit.
23. Otvorte ako *hruska* súbor */etc/shadow* pomocou *vim* a u superpoužívateľa *root* zmažte hašované heslo umiestnené medzi v poradí prvou a druhou dvojbodkou. Súbor uložte.
24. Ako *hruska* zmeňte svoju identitu na superpoužívateľa *root*. Všimnite si, že nemusíte zadávať heslo.
25. Ako *root* si spustením príkazu **passwd** nastavte nové heslo a programu *vim* odstráňte *SUID* bit.
26. Pomocou programu *find* ako *root* vyhľadajte všetky súbory alebo priečinky, ktoré majú nastavený *SUID* bit. Použite príkaz: **find / -perm -4000 2> /dev/null**.
27. Vyhľadajte umiestnenie programu *wall* a prezrite si jeho prístupové práva. Overte, že patrí skupine *tty* a má nastavený *SGID* bit.
28. V jednom pseudoterminál nech je prihlásený *root*, v druhom *hruska*. Stlačte kombináciu klávesov *Ctrl+Alt+F2*, prihláste sa do otvoreného terminálu ako *jahoda.* Príkazom **tty** si overte, že *jahoda* je prihlásený v terminál */dev/tty2.*
29. Stlačením kombinácie klávesov *Ctrl+Alt+F1* sa prepnite naspäť do grafického režimu a ako *root* aj ako *hruska* si príkazom **tty** overte, že sa nachádzate v termináloch */dev/pts/0* a */dev/pts/1.*
30. Prezrite si vlastníctvo súborov */dev/tty2*, *dev/pts/0* a */dev/pts/1*, overte si, že patria skupine *tty.*

31. Ako *hruska* použite príkaz **wall Zdravim vsetkych prihlasenych pouzivatelov pocitaca** a overte, že sa správa zobrazila aj *rootovi* aj *jahodovi.*
32. Ako *root* vytvorte v priečinku */home* priečinok *project.* Nastavte mu prístupové práva na hodnotu *770.*
33. Ako *root* vytvorte novú skupinu s názvom *team* príkazom **groupadd team**.
34. Priečinku */home/project* nastavte skupinu na *team.*
35. Príkazmi **usermod -G team hruska** a **usermod -G team jahoda** nastavte týmto používateľom skupinu *team* ako sekundárnu skupinu.
36. Ako *root* si zobrazte obsah súboru */etc/group* a overte, že používatelia *hruska* a *jahoda* patria do skupiny *team.* Overte si to tiež príkazmi **id hruska** a **id jahoda**.
37. Overte, že používatelia *hruska* a *jahoda* majú prístup do priečinka */home/project* a používateľ *cernica* tam prístup nemá.
38. Ako *hruska* vytvorte v priečinku */home/project* súbor s názvom *navrh* a pridajte doňho nejaký text. Zobrazte si jeho prístupové práva a overte, že patrí vlastníkovi *hruska* a skupine *hruska.*
39. Ako *jahoda* otvorte súbor */home/project/navrh* v editore *vim* a pridajte doňho nejaký text. Overte, že súbor sa nedá uložiť kombináciou klávesov *wq.* Potom ho uložte stlačením kombinácie *wq!.* Overte, že súbor */home/project/navrh* patrí vlastníkovi *jahoda* a skupine *jahoda.*
40. Ako *root* nastavte priečinku */home/project SGID* bit.
41. Ako *hruska* otvorte súbor */home/project/navrh* v editore *vim* a pridajte doňho nejaký text. Overte, že súbor sa dá uložiť kombináciou klávesov *wq.* Overte, že vlastníkom súboru zostal používateľ *jahoda*, ale patrí skupine *team*, a teda všetci členovia tejto skupiny ho majú právo upravovať.
42. Ako *root* zmažte priečinok */home/project.* Ako *root* odstráňte skupinu *team* príkazom **groupdel team**.
43. Pomocou programu *find* ako *root* vyhľadajte všetky súbory alebo priečinky, ktoré majú nastavený *SGID* bit. Použite príkaz: **find / -perm -2000 2> /dev/null**.
44. Prezrite si prístupové práva priečinka */tmp* a overte, že má nastavený *sticky* bit.
45. Ako *root* vytvorte priečinok */home/docasny* a nastavte mu prístupové práva s hodnotou *777*.

46. Ako *hruska* sa presuňte do priečinka */home/docasny* a vytvorte tam priečinok *hrdir1* a neprázdny súbor *hrfil1*.
47. Ako *cernica* sa presuňte do priečinka */home/docasny* a vytvorte tam priečinok *cerdir1* a neprázdny súbor *cerfil1*.
48. Ako *cernica* z priečinka */home/docasny* zmažte priečinok *hrdir1* a súbor *hrfil1*.
49. Ako *root* nastavte priečinku */home/docasny sticky* bit.
50. Ako *hruska* si naspäť vytvorte priečinok *hrdir1* a neprázdny súbor *hrfil1*.
51. Ako *hruska* sa pokúste zmazať priečinok *cerdir1* a zmazať alebo upraviť obsah súboru *cerfil1.*
52. Ako *root* zmažte priečinok */home/docasny.*
53. Pomocou programu *find* ako *root* vyhľadajte všetky súbory alebo priečinky, ktoré majú nastavený *sticky* bit. Použite príkaz: **find / -perm -1000 2> /dev/null**.
54. Ako *hruska* v jeho domovskom priečinku vytvorte súbor *hfile1* a priečinok *hdir1*, všimnite si, s akými prístupovými právami sa vytvárajú.
55. Ako *root* v jeho domovskom priečinku vytvorte súbor *rfile* a priečinok *rdir*, všimnite si, s akými prístupovými právami sa vytvárajú a porovnajte to s prístupovými právami, s akými vytvára súbory a priečinky *hruska.*
56. Príkazom **umask** spusteným pod identitou používateľov *hruska* a *root* si zobrazte predvolenú masku používateľov a porovnajte ju s prístupovými právami, s ktorými predvolene vytvárajú súbory a priečinky.
57. Zmeňte si ako používateľ *hruska* predvolenú masku na hodnotu *0026* príkazom **umask 0026**. Vytvorte v jeho domovskom priečinku súbor *hfile2* a priečinok *hdir2*. Porovnajte ich prístupové práva s predtým vytvoreným priečinkom a súborom.
58. Nastavte používateľovi *hruska* masku na pôvodnú hodnotu *0002.* Zmažte z jeho domovského priečinka súbory a priečinky *hfile1*, *hfile2*, *hdir1* a *hdir2*.
59. Ako *root* zmažte z *rootovho* domovského priečinka súbor *rfil* a priečinok *rdir*,