Практикалық жұмыс 2. Қол жеткізу құқықтарын ажырата білу
Негізгі теориялық ақпарат

Мақсаты: Ресурстарға қол жеткізуді басқару тетіктерін, қол жеткізу құқықтарын зерттеу. Пайдаланушы мен топ ұғымын түсіну. Консольдық утилиталардың көмегімен пайдаланушыларды басқарудың практикалық дағдыларын игеру. Консольдық утилиталардың көмегімен пайдаланушылардың құқықтарымен және файлдарға, каталогтарға құқықтармен жұмыс істеу дағдыларын игеру.

Теориялық бөлім
Әрбір объектінің (файлдың) оған қол жеткізуге болатын бірегей атауы және процестер сол объектіге қатысты орындай алатын операциялардың соңғы жиынтығы бар. Файл read, write және execute операцияларымен сипатталады.
Қол жеткізу құқығы жоқ объектілерге қол жеткізу процестеріне тыйым салу әдісі қажет екені анық. Сонымен қатар, бұл механизм қажет болған жағдайда процестерді рұқсат етілген операциялардың ішкі жиынтығымен шектеуге мүмкіндік беруі керек. Мысалы, A процесіне F файлынан деректерді оқуға рұқсат берілуі мүмкін, бірақ бұл файлға жазуға рұқсат етілмейді.
Қол **жеткізу құқығы** белгілі бір операцияны (оқу, жазу, орындау)орындауға рұқсатты білдіреді
Пайдаланушы кірген кезде оның қабығы құпия сөз файлындағы жазбасында қамтылған UID және GID (UID пайдаланушы идентификаторы, GID топ идентификаторы) алады және олар оның барлық еншілес процестеріне мұра болады. Кез-келген комбинацияны (UID, GID) ұсына отырып, сіз барлық нысандардың толық тізімін жасай аласыз (файлдар, соның ішінде арнайы файлдар түрінде ұсынылған енгізу-шығару құрылғылары және т.б.), оларға процесс қол жетімділіктің мүмкін түрін көрсете алады (оқу, жазу, орындау).
Бірдей комбинациясы бар екі процесс (UID, GID) бірдей Нысандар жиынтығына бірдей қол жеткізе алады. Әр түрлі мәндері бар процестер (UID, GID) әр түрлі файлдар жиынтығына қол жеткізе алады, бірақ бұл жиынтықтардың айтарлықтай қабаттасуы болуы мүмкін.
SUID (Set User ID)
Орындалатын файлдың атрибуты, оны иесінің құқықтарымен іске қосуға мүмкіндік береді. Linux операциялық жүйелерінде қосымша аталған қосымшаны іске қосқан пайдаланушының құқықтарымен іске қосылады. Бұл қосымша қауіпсіздікті қамтамасыз етеді, өйткені пайдаланушы құқықтары бар процесс маңызды жүйелік файлдарға жазылуға қол жеткізе алмайды, мысалы /etc/passwd, ол Root суперпайдаланушысына тиесілі. Егер орындалатын файлға suid биті орнатылған болса, онда бұл бағдарлама автоматты түрде "тиімді пайдаланушыны" сол файлдың иесі болып табылатын пайдаланушының идентификаторына өзгертеді. Яғни, бұл бағдарламаны кім іске қосқанына қарамастан, ол орындалған кезде осы файлдың хост құқығына ие болады.
SGID (Set Group ID)
SUID-ке ұқсас, бірақ топқа қатысты. Сонымен қатар, егер каталог үшін sgid биті орнатылған болса, онда онда жасалған нысандар пайдаланушыны емес, каталог иесінің тобын алады.
Практикалық мысалдар
Файл/каталог құқықтарын біліңіз

```
sit@ubuntu:~$ ls -l /bin/ls
-rwxr-xr-x 1 root root 129280 Feb 18  2016 /bin/ls
```

Кіру құқықтары үш таңбадан тұрады. Бірінші үштік файл иесінің құқықтарын, екіншісі файл тобының құқықтарын және барлық басқа пайдаланушылардың үшінші құқықтарын білдіреді.
Біздің жағдайда бұл :

* "rwx" - файл иесінің құқықтары
* "r-x" - файл тобының құқықтары
* "r-x" - файлға басқалардың құқықтары.

"R" таңбасы оқуға (файлдағы деректерді көруге) рұқсат етілгенін, "w" жазуға (деректерді өзгертуге, сондай-ақ жоюға) рұқсат етілгенін және "x" орындалуын (бағдарламаны іске қосуға рұқсат етілген) білдіреді.

Осылайша, егер құқықтарға жалпы қарайтын болсақ, біз кез-келген адамға мазмұнды оқуға және осы файлды орындауға рұқсат етілгенін көреміз, бірақ тек иесіне (root) бұл файлды кез-келген түрде өзгертуге рұқсат етіледі. Басқаша айтқанда, қалыпты пайдаланушыларға осы файлдың мазмұнын көшіруге рұқсат етіледі, содан кейін оны тек түбір өзгерте немесе жоя алады.

Ағымдағы пайдаланушыны және оны құрайтын топтарды анықтау

Файлға тиесілі иесін немесе тобын өзгертпес бұрын, ағымдағы пайдаланушыны және ол тиесілі топты анықтай білу керек. Қай пайдаланушымен жұмыс істеп жатқаныңызды білу үшін whoami деп теріңіз:

```
sit@ubuntu:~$ whoami
sit
```

Sit пайдаланушысы қандай топтарда екенін анықтау үшін groups командасын пайдалану керек:

```
sit@ubuntu:~$ groups
sit adm cdrom sudo dip plugdev lxd lpadmin sambashare
```

Бұл мысалдан seat пайдаланушысы set, adm, CD rom, sudo, IP, plugdev, lsd, lpadmin, sambashare топтарынан тұратындығын көруге болады. Егер сіз басқа Пайдаланушының қандай топтарда екенін көргіңіз келсе, оның атын дәлел ретінде беріңіз.

```
sit@ubuntu:~$ groups root
root : root
```

Пайдаланушы мен иесінің тобын өзгерту

Файлдың (немесе басқа нысанның) иесін немесе тобын өзгерту үшін сәйкесінше chown немесе chgrp командалары қолданылады. Алдымен сіз топтың немесе иесінің атын, содан кейін файлдар тізімін беруіңіз керек.

```
chown sit /home/sit/itmo.txt
chgrp sit /home/sit/itmo.txt
```

Сондай ақ chown пәрменін басқа пішінде пайдалану кезінде пайдаланушы мен топты бір уақытта өзгертуге болады:

```
chown sit:sit /home/sit/itmo.txt
```

Ескерту

Сіз chown пәрменін супер пайдаланушы құқығынсыз пайдалана алмайсыз, бірақ chgrp файл иесінің тобын олар тиесілі топқа өзгерту үшін барлығы пайдалана алады.

Chmod-пен танысу

chown және chgrp файлдық жүйенің иесі мен объект тобын өзгерту үшін қолданылады, бірақ олардан басқа chmod деп аталатын басқа бағдарлама бар, ол ls-l командасының шығысында көретін оқу, жазу және орындау рұқсаттарын өзгерту үшін қолданылады. кіру құқықтарын келесі файл атауымен немесе осы өзгертулерді қолдану қажет файлдар тізімімен өзгерту қажет:

```
chmod +x /home/sit/itmo.sh
```

Пайдаланушы, топ және басқалар арасындағы бөлу

Бір уақытта тек бір немесе екі кіру құқығын өзгерту ыңғайлы. Мұны істеу үшін оның алдында "+"" немесе "—" белгісімен өзгертілуі керек кіру құқықтарының жиынтығын

көрсету үшін арнайы таңбаны пайдалану қажет. Пайдаланушы үшін "u", топ үшін "g" және қалған пайдаланушылар үшін "o" таңбасы.

```
chmod go-w /home/sit/itmo.sh
```

Бұл мысал топқа және барлық басқа пайдаланушыларға жазу құқығын жояды, бірақ иесінің құқықтарын бұзбайды.

Сандық режимдер

Құқықтарды көрсетудің тағы бір кең таралған әдісі бар: төрт таңбалы сегіздік сандарды қолдану. Бұл синтаксис қол жетімділіктің сандық синтаксисі деп аталады, мұнда әр Сан үш рұқсатты білдіреді. Мысалы, 0777, 777-де иесіне, тобына және басқа пайдаланушыларға жалаушалар орнатылады. Төменде көрсетілген кесте сандық мәндерге қол жеткізу құқықтары қалай аударылады.

```
Режим   Число
rwx     7
rw-     6
r-x     5
r--     4
-wx     3
-w-     2
--x     1
---     0
```

umask

Процесс жаңа файлды жасаған кезде, ол берілген файл үшін қандай рұқсаттарды орнату керектігін көрсетеді. Көбінесе 0666 құқықтары сұралады (барлығы оқиды және жазады), бұл көп жағдайда қажет болғаннан көп рұқсат береді. Бақытымызға орай, Linux жүйесінде жаңа файл жасалған сайын жүйе umask деп аталатын параметрге қол жеткізеді. Жүйе қолданады umask мәні ақылға қонымды және қауіпсіз нәрсеге бастапқы берілген рұқсаттарды төмендету. Пәрмен жолына umask теру арқылы ағымдағы umask параметрлерін көруге болады:

```
sit@ubuntu:~$ umask
0002
```

Linux жүйелерінде umask үшін әдепкі мән 0022 болып табылады, бұл басқаларға сіздің жаңа файлдарыңызды оқуға мүмкіндік береді (егер олар оларға жете алса), бірақ оларды өзгертпейді. Жасалған файлдар үшін қауіпсіздіктің үлкен деңгейін автоматты түрде қамтамасыз ету үшін umask параметрлерін өзгертуге болады:

```
sit@ubuntu:~$ umask 0077
```

Бұл umask мәні топтың және басқалардың барлық жаңадан жасалған файлдарға мүлдем қол жеткізу құқығына ие болмауына әкеледі.

Файлға кіру құқығының" қалыпты " тағайындалуынан айырмашылығы, umask орнатады қандай кіру құқықтары өшірілуі керек. Мәндердің сандардың және әдістердің сәйкестік кестесін қайтадан қарастырайық:

```
Режим   Число
rwx     7
rw-     6
r-x     5
r--     4
-wx     3
-w-     2
--x     1
---     0
```

Осы кестені қолдана отырып, біз 0077 —дегі соңғы үш белгі-rwxrwx екенін көреміз. umask жүйеге қандай кіру рұқсаттарын өшіру керектігін көрсетеді. Бірінші және екіншісін біріктіре отырып, топқа және қалған пайдаланушыларға арналған Барлық құқықтар өшірілетіні көрінеді, ал иесінің құқықтары өзгеріссіз қалады.
Suid және sgid өзгерту
Suid және sgid биттерін орнату және жою әдісі өте қарапайым. Suid битін орнату үшін:

```
chmod u+s /home/sit/itmo.sh
```

Sgid битін орнату үшін:

```
chmod g+s /home/sit/itmo/
```

Қол жеткізу құқығының бірінші белгісін анықтау
Ол sticky, suid және sgid биттерін кіру құқықтарымен бірге орнату үшін қолданылады:

```
suid   sgid   sticky  режим
on     on     on     7
on     on     off    6
on     off    on     5
on     off    off    4
off    on     on     3
off    on     off    2
off    off    on     1
off    off    off    0
```

Төменде каталогқа кіру құқығын орнату үшін төрт таңбалы режимді қалай пайдалану керектігі туралы мысал келтірілген.

```
sit@ubuntu:~$ chmod 4775 /home/sit/itmo
sit@ubuntu:~$ ls -l /home/sit/itmo
-rwsrwxr-x 1 sit sit 0 Sep  9 12:42 /home/sit/itmo
```

Консоль командалары:
* id <пайдаланушы идентификаторын басып шығару>
* chgrp < файл тобын өзгерту>
* chown <файл иесі мен тобын өзгерту>
* chmod <файл рұқсаттарын өзгерту>
* usermod <пайдаланушы тіркелгісінің параметрлерін өзгерту>
* useradd <жаңа пайдаланушыны құру>
* userdel <пайдаланушыны жою>
* whoami <ағымдағы пайдаланушының анықтамасы>
* umask <жаңадан жасалған файлдарға кіру құқығының маскасын анықтау немесе орнату>
* sudo su < супер пайдаланушы құқығын алу>
* groups <пайдаланушы қандай топтарға жататынын анықтау>

Зертханалық жұмыстарға арналған тапсырмалар
* Екі терминалды ашыңыз (Linux серверінде терминалдар арасында ауысу үшін (tty) әдетте alt+F[1-5] пернелер тіркесімі қолданылады). Олардың бірінде sudo su пәрменін пайдаланып суперпайдаланушы құқықтарын алыңыз:
* Man анықтамалық құжаттамасынан useradd пәрменін пайдаланып үй каталогы бар пайдаланушыны қалай құруға болатынын біліңіз
* Useradd көмегімен "sit2" үй каталогымен "sit2" пайдаланушысын жасаңыз.
* Passwd sit2 пәрменін пайдаланып жаңа "sit2" пайдаланушысының құпия сөзін орнатыңыз
* Exit пәрменімен суперпайдаланушыдан шығыңыз
* Бірінші терминал астында "sit" пайдаланушысына, екіншісінде "sit2" пайдаланушысына кіріңіз.

* Id пәрменін пайдаланып "sit" пайдаланушысы мен "sit2" пайдаланушысы қандай идентификатор алғанын қараңыз
* Ls пәрменін пайдаланып "sit" және "sit2" пайдаланушыларының үй каталогына кіру құқығын қараңыз
* Umask көмегімен 0077 маскасы бар "sit2" пайдаланушысының астында файл жасаңыз
* Cat пәрменін пайдаланып, оның мазмұнын "sit" пайдаланушысының астында оқып көріңіз
* Файлға кіру құқығын "sit" пайдаланушысы файлға жаза алатындай етіп өзгертіңіз, бірақ оны оқымаңыз.
* Мәтіндік ақпаратты "sit" пайдаланушысының астындағы файлға VI немесе Nano консольдік мәтіндік редакторын пайдаланып жазыңыз
* Файл құқықтарын тексеріңіз және оның мазмұнын "sit2"пайдаланушысының астынан оқыңыз
* "Sit2"пайдаланушысының астынан каталог жасаңыз
* Осы каталогқа пайдаланушылар тобы үшін жазу құқықтарын орнатыңыз
* Usermod пәрменін пайдаланып "sit2" тобына " sit " пайдаланушысын қосыңыз
* "Sit"пайдаланушысы қандай топтарға кіретінін тексеріңіз
* "Sit2" пайдаланушысы жасаған каталогта "sit" пайдаланушысының астынан бірнеше файл жасаңыз.
* Анықтамалық құжаттамадан пайдаланушыны үй каталогының мазмұнымен бірге қалай жою керектігін қараңыз
* "Sit2" пайдаланушысын үй каталогымен бірге жойыңыз.