

Лабораторная работа №2.

Дискреционноеразграничение прав в Linux. Основные атрибуты

Абакумова О.М., НКАбд-01-22

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux .

Задание

Поэтапно выполнить все пункты лабораторной работы(15)

Теоретическое введение

Дискреционное управление доступом - права доступа состоят из трех компонентов: владелец файла, группа владельца и остальные пользователи. Каждому компоненту присваивается разрешение на чтение (r), запись (w) и выполнение (x). Для управления правами доступа в Linux используются команды `chmod`, `chown` и `chgrp`.

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора): `useradd guest`

2. Задаем пароль для пользователя guest (используя учётную запись администратора): `passwd guest`

```
root@omabakumova:~  
[omabakumova@omabakumova ~]$ sudo mount -o remount,rw /  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for omabakumova:  
[omabakumova@omabakumova ~]$ useradd guest  
useradd: Permission denied.  
useradd: cannot lock /etc/passwd; try again later.  
[omabakumova@omabakumova ~]$ mount -o remount,rw /  
mount: /: must be superuser to use mount.  
[omabakumova@omabakumova ~]$ su -  
Password:  
[root@omabakumova ~]# useradd guest  
[root@omabakumova ~]# passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@omabakumova ~]#
```

en

Wired Connected

Balanced

Settings

Lock

Power Off / Log Out

Suspend






Restart...

Power Off...





Log Out

Switch User...

3.Входим в систему от имени guest.

 guest@omabakumova:~   
[guest@omabakumova ~]\$ 

4. Определяем директорию, в которой находимся, командой `pwd`.

 guest@omabakumova:~   
[guest@omabakumova ~]\$ pwd
/home/guest
[guest@omabakumova ~]\$

5. Уточняем имя пользователя командой whoami.

```
guest@omabakumova:~  
[guest@omabakumova ~]$ pwd  
/home/guest  
[guest@omabakumova ~]$ whoami  
guest  
[guest@omabakumova ~]$
```

6. Уточняем имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запоминаем.

```
guest@omabakumova:~  
[guest@omabakumova ~]$ pwd  
/home/guest  
[guest@omabakumova ~]$ whoami  
guest  
[guest@omabakumova ~]$ id  
uid=1002(guest) gid=1002(guest) groups=1002(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@omabakumova ~]$
```

7. Просматриваем файл `/etc/passwd` командой `cat /etc/passwd`. Дополнительно используем команду `cat /etc/passwd | grep guest` в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания

```
ed_r:unconfined_t:s0-s0:c0.c1023
[guest@omabakumova ~]$ groups
guest
[guest@omabakumova ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996>User for polkitd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:997:993:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
sssd:x:996:992>User for sssd:/:/sbin/nologin
```



```
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/:usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/:usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/:usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/:sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
design:x:981:980:Group for the design signing daemon:/run/design:/sbin/nologin
gnome-initial-setup:x:980:979:/:run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:sbin/nologin
omabakumova:x:1000:1000:omabakumova:/home/omabakumova:/bin/bash
omabakumovaa:x:1001:1001:omabakumovaa:/home/omabakumovaa:/bin/bash
guest:x:1002:1002:/:home/guest:/bin/bash
[guest@omabakumova ~]$
```

8.Grep

```
guest@1002:1002 ~$ cat /etc/passwd | grep guest
guest:x:1002:1002:~/home/guest:/bin/bash
[guest@omabakumova ~]$
```

Определяем существующие в системе директории
командой `ls -l /home/`

```
guest@omabakumova:~  
flatpak:x:985:984:User for flatpak system helper:/:/sbin/nologin  
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin  
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis  
:/usr/sbin/nologin  
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr  
/sbin/nologin  
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin  
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin  
gnome-initial-setup:x:980:979:/:/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin  
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin  
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin  
tcpdump:x:72:72:/:/sbin/nologin  
omabakumova:x:1000:1000:omabakumova:/home/omabakumova:/bin/bash  
omabakumovaa:x:1001:1001:omabakumova :/home/omabakumovaa:/bin/bash  
guest:x:1002:1002:/:/home/guest:/bin/bash  
[guest@omabakumova ~]$ cat /etc/passwd | grep guest  
guest:x:1002:1002:/:/home/guest:/bin/bash  
[guest@omabakumova ~]$ ls -l /home/  
total 8  
drwx-----. 14 guest      guest      4096 Mar  1 17:45 guest  
drwx-----. 14 omabakumova omabakumova 4096 Mar  1 17:22 omabakumova  
drwx-----.  3 omabakumovaa omabakumovaa 78 Mar  1 17:21 omabakumovaa  
[guest@omabakumova ~]$
```

10. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`

```
guest@omabakumova:~  
r/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin  
gnome-initial-setup:x:980:979::/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin  
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin  
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin  
tcpdump:x:72:72:::/sbin/nologin  
omabakumova:x:1000:1000:omabakumova:/home/omabakumova:/bin/bash  
omabakumovaa:x:1001:1001:omabakumova :/home/omabakumovaa:/bin/bash  
guest:x:1002:1002::/home/guest:/bin/bash  
[guest@omabakumova ~]$ cat /etc/passwd | grep guest  
guest:x:1002:1002::/home/guest:/bin/bash  
[guest@omabakumova ~]$ ls -l /home/  
total 8  
drwx-----. 14 guest      guest      4096 Mar  1 17:45 guest  
drwx-----. 14 omabakumova omabakumova 4096 Mar  1 17:22 omabakumova  
drwx-----.  3 omabakumovaa omabakumovaa  78 Mar  1 17:21 omabakumovaa  
[guest@omabakumova ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/omabakumova  
lsattr: Permission denied While reading flags on /home/omabakumovaa  
----- /home/guest  
[guest@omabakumova ~]$ mkdir dir1  
[guest@omabakumova ~]$
```

11. Создаем в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определяем командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.

```

/home/guest
[guest@omabakumova ~]$ mkdir dir1
[guest@omabakumova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Desktop
drwxr-xr-x. 2 guest guest 6 Mar  1 17:55 dir1
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Documents
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Downloads
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Music
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Pictures
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Public
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Templates
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Videos
[guest@omabakumova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@omabakumova ~]$
```


12. Снимаем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверяем с её помощью правильность выполнения команды `ls -l`.

```
guest@omabakumova:~  
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Templates  
drwxr-xr-x. 2 guest guest 6 Mar  1 17:45 Videos  
[guest@omabakumova ~]$ lsattr  
----- ./Desktop  
----- ./Downloads  
----- ./Templates  
----- ./Public  
----- ./Documents  
----- ./Music  
----- ./Pictures  
----- ./Videos  
----- ./dir1  
[guest@omabakumova ~]$ chmod 000 dir1  
[guest@omabakumova ~]$ ls -l  
Desktop  
dir1  
Documents  
Downloads  
Music  
Pictures  
Public  
Templates  
Videos  
[guest@omabakumova ~]$
```

13. Попытка создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`.

```
[guest@omabakumova ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Permission denied
```

Мы получили отказ в связи с тем, что сняли все атрибуты с этой директории в прошлом пункте. Проверка командой `ls -l /home/guest/dir1`

```
[guest@omabakumova ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@omabakumova ~]$
```

14. Заполняем таблицу «Установленные права и разрешённые действия»(см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет.Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-».

Таблица получилась очень большой,не было смысла ее дробить,поэтому она есть в полном размере в отчете.

Пример таблицы

Таблица 2.1

Установленные права и разрешённые действия

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d (000)	(000)	-	-	-	-	-	-	-	-
d--x----- (100)	(000)	-	-	-	-	+	-	-	+
drwx----- (700)	- rwx----- (700)	+	+	+	+	+	+	+	+

15. На основании заполненной таблицы определяем те или иные минимально необходимые права для выполнения операций внутри директории dir1.

Пример таблицы

Таблица 2.2

Минимальные права для совершения операций

Операция	Минимальные права на директо- рию	Минимальные права на файл
Создание файла		
Удаление файла		
Чтение файла		
Запись в файл		
Переименование файла		
Создание поддиректории		
Удаление поддиректории		


```
| | | | | |
|-|-|-|-|-|
|Операция|Минимальные права на директорию|Минимальные права на файл|
|Создание файла| |d(300)| |(000)|
|Удаление файла| |d(300)| |(000)|
|Чтение файла| |d(100)| |(400)|
|Запись в файл| |d(100)| |(200)|
|Переименование файла| |d(300)| |(000)|
|Создание поддиректории| |d(300)| |(000)|
|Удаление поддиректории| |d(300)| |(000)|
```

8

Выводы

Выполняя данную лабораторную работу, мы получили практические навыки работы в консоли с атрибутами файлов и закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

#1.О правах доступа в ОС

(<https://vk.com/away.php?utf=1&to=https%3A%2F%2Fhabr.com%2Fru%2Farticles%2F469667%2F>)

2.Подробнее о дискреционном разграничении прав

(<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjnvnGINSExUmLhAIHY2AD5wQFnoECA0QAw&url=https%3A%2F%2Fitcloud-edu.ru%2Finfo%2Farticles%2Fupravlenie-dostupom-v-gnu-linux%2F&usg=AOvVaw0AZKOfJmBKY3JGoaVnzpqQ&opi=89978449>)

Спасибо за внимание!