

Отчёт по лабораторной работе №2

Информационная безопасность

Дискреционное разграничение прав в Linux. Основные атрибуты

Хусаинова Динара Айратовна,
НПИбд-02-21, 1032212283

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
Атрибуты файлов	6
Заполнение таблицы 2.1	10
Заполнение таблицы 2.2	12
Вывод	14
Список литературы. Библиография	15

Список иллюстраций

1	useradd guest	6
2	passwd guest	6
3	passwd guest	7
4	whoami, id, cat /etc/passwd	8
5	lsattr /home, mkdir dir1, chmod 000 dir1, ls -l	9
6	echo "test" > /home/guest/dir1/file1	9

Цель работы

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

Теоретическое введение

Операционная система — то комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].

Выполнение лабораторной работы

Атрибуты файлов

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора): `useradd guest` Зададим пароль для пользователя guest (используя учётную запись администратора): `passwd guest`

```
[dakhusainova@dakhusainova ~]$ su -  
Password:  
[root@dakhusainova ~]# useradd guest
```

Рис. 1: `useradd guest`

```
[root@dakhusainova ~]# passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@dakhusainova ~]#
```

Рис. 2: `passwd guest`

2. Войдите в систему от имени пользователя guest.

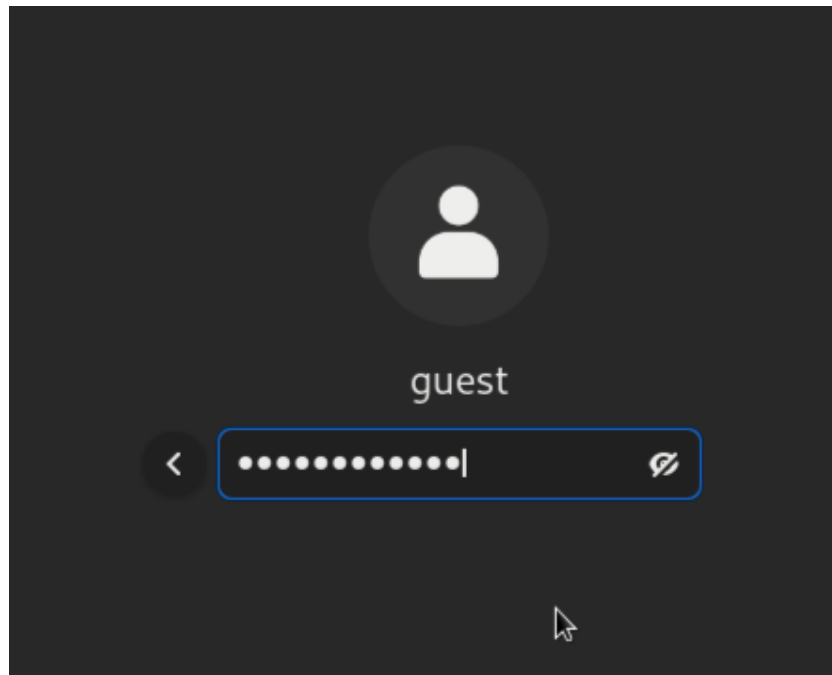


Рис. 3: passwd guest

3. Определите директорию, в которой мы находимся, командой `pwd`. Уточним имя вашего пользователя командой `whoami`. Уточним имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Просмотрим файл `/etc/passwd` командой `cat /etc/passwd` Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя.

```

[guest@dakhusainova ~]$ pwd
/home/guest
[guest@dakhusainova ~]$ ~
bash: /home/guest: Is a directory
[guest@dakhusainova ~]$ cd ~
[guest@dakhusainova ~]$ whoami
guest
[guest@dakhusainova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@dakhusainova ~]$ groups
guest
[guest@dakhusainova ~]$ 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:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin

```

Рис. 4: whoami, id, cat /etc/passwd

4. Определим существующие в системе директории командой `ls -l /home/`. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`
5. Создадим в домашней директории поддиректорию `dir1` командой `mkdir dir1`
6. Снимем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверим с её помощью правильность выполнения команды `ls -l`


```

[guest@dakhusainova ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@dakhusainova ~]$ ls -l /home/
total 8
drwx-----. 14 dakhusainova dakhusainova 4096 Sep  6 16:37 dakhusainova
drwx-----. 14 guest guest 4096 Sep 13 19:07 guest
[guest@dakhusainova ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/dakhusainova
----- /home/guest
[guest@dakhusainova ~]$ mkdir dir1
[guest@dakhusainova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 13 19:17 dir1
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Documents
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Music
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Public
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Templates
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Videos
[guest@dakhusainova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@dakhusainova ~]$

```

Рис. 5: lsattr /home, mkdir dir1, chmod 000 dir1, ls -l

7. Попробуйте создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1 Проверим командой, ls -l /home/guest/dir1 что действительно файл file1 не находится внутри директории dir1.

```

[guest@dakhusainova ~]$ chmod 000 dir1
[guest@dakhusainova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Desktop
d------. 2 guest guest 6 Sep 13 19:17 dir1
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Documents
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Music
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Public
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Templates
drwxr-xr-x. 2 guest guest 6 Sep 13 19:07 Videos
[guest@dakhusainova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@dakhusainova ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied

```

Рис. 6: echo "test" > /home/guest/dir1/file1

Заполнение таблицы 2.1

8. Заполните 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, занесите в таблицу знак «+», если не разрешена, знак «-».

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(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+
d(100)	(400)	-	-	-	+	+	-	-	+
d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	+	-	-	+
d(100)	(700)	-	-	+	+	+	-	-	+

d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(500)	(100)	-	-	-	-	+	+	-	+
d(500)	(200)	-	-	+	-	+	+	-	+
d(500)	(300)	-	-	+	-	+	+	-	+

d(500)	(400)	-	-	-	+	+	+	-	+
d(500)	(500)	-	-	-	+	+	+	-	+
d(500)	(600)	-	-	+	+	+	+	-	+
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+
d(700)	(300)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Таблица 2.1 «Установленные права и разрешённые действия»

Заполнение таблицы 2.2

9. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2.

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)
Переименова- ние файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Таблица 2.2 “Минимальные права для совершения операций”

Вывод

Были получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы. Библиография

[1] Операционные системы: <https://blog.skillfactory.ru/glossary/operaczionnaya-sistema/>

[2] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>