

## Лабораторная работа №2: Презентация.

Дискреционное разграничение прав в Linux. Основные атрибуты.

---

Евдокимов Максим Михайлович. Группа - НФИбд-01-20.<sup>1</sup>

8 сентября, 2023, Москва, Россия

<sup>1</sup>Российский Университет Дружбы Народов

## Цели и задачи 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.

1. Создание и вход в систему с нового пользователя.
2. Анализ данных о созданном пользователе.
3. Изучить возможности и уровень доступа нового пользователя.
4. Основываясь на полученных данных создать 2 таблицы “Установленные права и разрешённые действия” и “минимальной необходимые права для выполнения операций”.

## Выполнение лабораторной работы

---

Используя права администратора с помощью команды “useradd” создаём пользователя guest и “passwd” задаём ему пароль.

```
[max@Max ~]$ sudo useradd guest
[sudo] пароль для max:
[max@Max ~]$ sudo passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
```

Рис. 1: Создание пользователя

Воспользовавшись командой “su guest” и введя выше созданный пароль заходим в терминал от лица нового пользователя. Используя команду “pwd” определяем что мы находимся в домашней директории.

```
[max@Max ~]$ su
Пароль:
su: Сбой при проверке подлинности
[max@Max ~]$ su guest
Пароль:
[guest@Max max]$ pwd
/home/max
```

Рис. 2: Название

Уточняем имя пользователя командой “whoami” и уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой “id”.

```
[guest@Max max]$ whoami
guest
[guest@Max max]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 3: Название



Сравнив полученную данные от двух команд и информации которая у нас есть просмотрите файл /etc/passwd командой “cat”.

```
[guest@Max max]$ 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:99:99:Nobody:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:999:998:User for polkitd:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sane:x:996:994:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
saslauthd:x:995:76:Saslauthd user:/run/saslauthd:/sbin/nologin
abrt:x:173:173:/etc/abrt:/sbin/nologin
setroubleshoot:x:994:991:/var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/sbin/nologin
chrony:x:993:988:/var/lib/chrony:/sbin/nologin
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu user:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:989:983:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89:/var/spool/postfix:/sbin/nologin
nft:x:38:38:/etc/nft:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
max:x:1000:1000:Max:/home/max:/bin/bash
vboxadd:x:988:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
```

Находим в полученный список свою учётную запись, и определяем uid пользователя и gid пользователя. Сравним найденные значения с полученными в предыдущих пунктах.

```
[guest@Max max]$ cat /etc/passwd | grep guest  
guest:x:1001:1001::/home/guest:/bin/bash
```

Рис. 5: Название

Определяем существующие в системе директории командой “ls -l /home/”.

```
[guest@Max max]$ ls -l /home/  
итого 4  
drwx-----. 5 guest guest 127 сен 9 17:22 guest  
drwx-----. 15 max max 4096 сен 9 14:55 max  
[guest@Max max]$ ls -a /home/  
. .. guest max  
[guest@Max max]$ ls -la /home/  
итого 4  
drwxr-xr-x. 4 root root 30 сен 9 17:19 .  
dr-xr-xr-x. 17 root root 224 сен 6 20:37 ..  
drwx-----. 5 guest guest 127 сен 9 17:22 guest  
drwx-----. 15 max max 4096 сен 9 14:55 max
```

Рис. 6: Название

Проверяем какие расширенные атрибуты установлены на поддиректориях, командой “lsattr /home”.

```
[guest@Max max]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/max
----- /home/guest
```

Рис. 7: Название

Создаём в домашней директории поддиректорию `dir1` командой “`mkdir dir1`” и определяем командами “`ls -l`” и “`lsattr`”, какие права доступа и расширенные атрибуты у него есть.

```
[guest@Max ~]$ mkdir dir1
[guest@Max ~]$ echo "test" > /home/guest/dir1/file1
[guest@Max ~]$ cd dir1
[guest@Max dir1]$ ls -la
итого 4
drwxrwxr-x. 2 guest guest 19 сен  9 17:53 .
drwx----- . 6 guest guest 179 сен  9 17:53 ..
-rw-rw-r-- . 1 guest guest  5 сен  9 17:53 file1
```

Рис. 8: Название

Теперь снимем с директории dir1 все атрибуты командой “chmod 000 dir1”, и командой “ls -l” проверим с её помощью правильность выполнения.

```
[guest@Max ~]$ cd dir1
[guest@Max dir1]$ ls -la
итого 4
drwxrwxr-x. 2 guest guest 19 сен  9 17:53 .
drwx-----. 6 guest guest 179 сен  9 17:53 ..
-rw-rw-r--. 1 guest guest  5 сен  9 17:53 file1
[guest@Max dir1]$ cd
[guest@Max ~]$ cd dir1
[guest@Max dir1]$ rm fiell
rm: невозможно удалить «fiell»: Нет такого файла или каталога
[guest@Max dir1]$ rm file1
[guest@Max dir1]$ cd
[guest@Max ~]$ chmod 000 dir1
[guest@Max ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен  9 17:54 dir1
```

Рис. 9: Название

Пробуем создать в директории dir1 файл file1 командой “echo”test” > /home/guest/dir1/file1”.

```
[guest@Max ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@Max ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest@Max ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@Max ~]$ chmod 700 dir1
[guest@Max ~]$ ls -l /home/guest/dir1
итого 0
[guest@Max ~]$ cd dir1
[guest@Max dir1]$ ls
[guest@Max dir1]$ ls -la
итого 0
drwx-----. 2 guest guest   6 сен  9 17:54 .
drwx-----. 6 guest guest 179 сен  9 17:53 ..
[guest@Max dir1]$
```

Рис. 10: Название

## Таблицы

---



## 14. 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)	-	-	-	-	+	-	-	+
d-w-----	(200)	+	+	+	-	-	-	+	-
d-wx-----	(300)	+	+	+	-	+	-	+	+
dr-----	(400)	-	-	-	+	-	+	-	-
dr-x-----	(500)	-	-	-	+	+	+	-	+
drw-----	(600)	+	+	+	+	-	+	+	-
drwx-----	(700)	+	+	+	+	+	+	+	+

Рис. 11: Таблица с уровнями доступа

## 15. Минимально необходимые права для выполнения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-w-----	(200)
Удаление файла	d-w-----	(200)
Чтение файла	dr-----	(400)
Запись в файл	d-w-----	(200)
Переименовать файл	d-w-----	(200)
Создание директории	d-x-----	(100)
Удаление директории	d-x-----	(100)

Рис. 12: Таблица соответствия операции и необходимого уровня доступа

## Выводы по проделанной работе

---

В ходе выполнения лабораторной работы были рассмотрены разные уровни доступа в системах Linux, а также изучена работа с пользователями и их созданием.