

Лабораторная работа № 2.
Дискреционное разграничение прав в
Linux. Основные атрибуты

Безрук Мария Андреевна, НПМбд-02-20

Содержание

1	Цель работы	5
2	Ход работы	6
3	Выводы	11
4	Библиография	12

List of Figures

2.1	Создание пользователя	6
2.2	Создание пароля	6
2.3	Определение директории	7
2.4	Вывод команды <code>whoami</code>	7
2.5	Имя пользователя, группа	7
2.6	Файл <code>/etc/passwd</code>	8
2.7	Файл <code>/etc/passwd - 2</code>	8
2.8	Создание директории <code>dir1</code>	9
2.9	Попытка создания файла	9
2.10	Таблица «Установленные права и разрешённые действия».....	10
2.11	Таблица “Минимальные права для совершения операций”	10

List of Tables

1 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.

2 Ход работы

1. В установленной ОС создаю учетную запись пользователя guest.

```
useradd: не удалось заблокировать /etc/passwd; попробуйте еще раз поз
[nktilyn@localhost ~]$ sudo useradd guest
Мы полагаем, что ваш системный администратор изложил вам основы
```

Figure 2.1: Создание пользователя

2. Задаю пароль для созданного пользователя.

```
[nktilyn@localhost ~]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
Извините, но пароли не совпадают.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[nktilyn@localhost ~]$
```

Figure 2.2: Создание пароля

3. Вхожу в систему от имени созданного пользователя.
4. С помощью команды `pwd` определяю директорию. Определяю, что она является домашней.

```
[guest@localhost ~]$ pwd
/home/guest
```

Figure 2.3: Определение директории

5. Уточняю имя пользователя командой whoami.

```
[guest@localhost ~]$ whoami
guest
```

Figure 2.4: Вывод команды whoami

6. Уточняю имя пользователя, группу, и группы, куда входит пользователь.

```
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
```

Figure 2.5: Имя пользователя, группа

7. Сравниваю полученные данные с данными в приглашении командной строке.
8. Просматриваю файл /etc/passwd командой cat /etc/passwd. Нахожу в нем свою учетную запись

```
[guest@localhost ~]$ 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
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:991:986:User for flatpak system helper:/sbin/nologin
colord:x:990:985:User for colord:/var/lib/colord:/sbin/nologin
setroubleshoot:x:989:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
clevis:x:988:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:987:982:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:981:/var/lib/chrony:/sbin/nologin
dnsmasq:x:985:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
systemd-oom:x:978:978:systemd Userspace OOM Killer:/usr/sbin/nologin
nktllyn:x:1000:1000:nktllyn:/home/nktllyn:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@localhost ~]$
```

Figure 2.6: Файл /etc/passwd

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

Figure 2.7: Файл /etc/passwd - 2

9. Определите существующие в системе директории командой `ls -l /home/`
Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях?
10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home` Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть

расширенные атрибуты директорий других пользователей?

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

```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 12 19:18 dir1
drwxr-xr-x. 2 guest guest 6 сен 12 19:08 Видео
drwxr-xr-x. 2 guest guest 6 сен 12 19:08 Документы
drwxr-xr-x. 2 guest guest 6 сен 12 19:08 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 12 19:08 Изображения
drwxr-xr-x. 2 guest guest 6 сен 12 19:08 Музыка
drwxr-xr-x. 2 guest guest 6 сен 12 19:08 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 12 19:08 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 12 19:08 Шаблоны
```

Figure 2.8: Создание директории dir1

12. Снимите с директории dir1 все атрибуты командой chmod 000 dir1 и проверьте с её помощью правильность выполнения команды ls -l
13. Попробуйте создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1. Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1.

```
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
```

Figure 2.9: Попытка создания файла

14. 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 «-». Замечание 1: при заполнении табл. 2.1 рассматриваются не все атрибуты файлов и директорий, а лишь «первые три»: r, w, x, для «владельца». Остальные атрибуты также важны

Права директории	Права файла	Создание файла	Удаление файла	Запись файла	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)	+	+	+	+	+	+	+	+

Figure 2.10: Таблица «Установленные права и разрешённые действия»

15. 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-w-----	(200)
Удаление файла	d-w-----	(200)
Чтение файла	dr-----	(400)
Запись в файл	d-w-----	(200)
Переименование файла	d-w-----	(200)
Создание поддиректории	d--x-----	(100)
Удаление поддиректории	d--x-----	(100)

Figure 2.11: Таблица “Минимальные права для совершения операций”

3 Выводы

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

4 Библиография

1. Методические материалы курса