

Лабораторная работа №2

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна

Содержание

1	Техническое оснащение:	5
2	Цели и задачи работы	6
2.1	Цель	6
2.2	Задачи	6
3	Теоретическое введение [1]	7
4	Выполнение лабораторной работы	8
4.1	Таблицы (4.1 и 4.2)	13
5	Выводы по проделанной работе	18
5.1	Вывод	18
	Список литературы	19

Список иллюстраций

4.1	Создание учетной записи пользователя	8
4.2	Пароль	8
4.3	Вход в систему	9
4.4	pwd	9
4.5	whoami	9
4.6	Уточняю имя пользователя, группу, и группы	10
4.7	Сравнение данных	10
4.8	Просмотр файла	10
4.9	Команда ls -l /home/	11
4.10	Проверяю, какие расширенные атрибуты установлены	11
4.11	Создаю поддиректорию dir1	12
4.12	Снимаю с директории dir1 все атрибуты	12
4.13	попытка создания в директории dir1 файл file1	13

Список таблиц

4.1	Установленные права и разрешённые действия	13
4.2	Минимальные права для совершения операций	17

1 Техническое оснащение:

- Персональный компьютер с операционной системой Windows 10;
- Планшет для записи видеосопровождения и голосовых комментариев;
- Microsoft Teams, использующийся для записи скринкаста лабораторной работы;
- Приложение Rucharm для редактирования файлов формата *md*;
- *pandoc* для конвертации файлов отчётов и презентаций.

2 Цели и задачи работы

2.1 Цель

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.

2.2 Задачи

1. Создать нового пользователя (гостевой аккаунт) виртуальной машины;
2. Через гостевой аккаунт выполнить задания лабораторной работы;
3. Заполнить таблицы об уровнях доступа и действиях с файлами/директориями.

3 Теоретическое введение [1]

Для разграничения действий над файлами определены три базовых права доступа (базовые разрешения):

- чтение r — «read»,
- запись w — «write» и
- выполнение x — «execute»,

соответствующие разрешению выполнять системные вызовы `read`, `write` и `execve` (точнее, системному вызову `open` с флагами `O_RDONLY` и `O_WRONLY`, но для простоты можно считать r — `read`, а w — `write`).

Каждое из базовых прав назначается на файл тому или иному пользователю или группе, разрешая соответствующую операцию.

В наследии классической UNIX определены только три субъекта, которым назначаются базовые права — пользователь-владелец (`owner`), группа-владелец (`group owner`) и все остальные (`others`). Совокупность их базовых прав называется режимом доступа (`access mode`) к файлу.

Базовое право может быть назначено r , w или x или отозвано —, поэтому в метаданных файла представляется одним битом, а для режима доступа требуется девять бит: по три бита прав на каждый из трех субъектов доступа.

Компактно режим доступа может быть записан соответствующим числом в восьмеричной системе счисления $rw-r-r- \rightarrow 110100100_2 \rightarrow 644_8$.

4 Выполнение лабораторной работы

1. В установленной ОС создаю учетную запись пользователя guest.

```
[vemanaeva@vemanaeva ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[vemanaeva@vemanaeva ~]$ sudo useradd guest
[sudo] пароль для vemanaeva:
```

Рис. 4.1: Создание учетной записи пользователя

2. Задаю пароль для созданного пользователя.

```
[vemanaeva@vemanaeva ~]$ sudo passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль содержит имя пользователя в какой либо форме
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
```

Рис. 4.2: Пароль

3. Вхожу в систему от имени созданного пользователя.

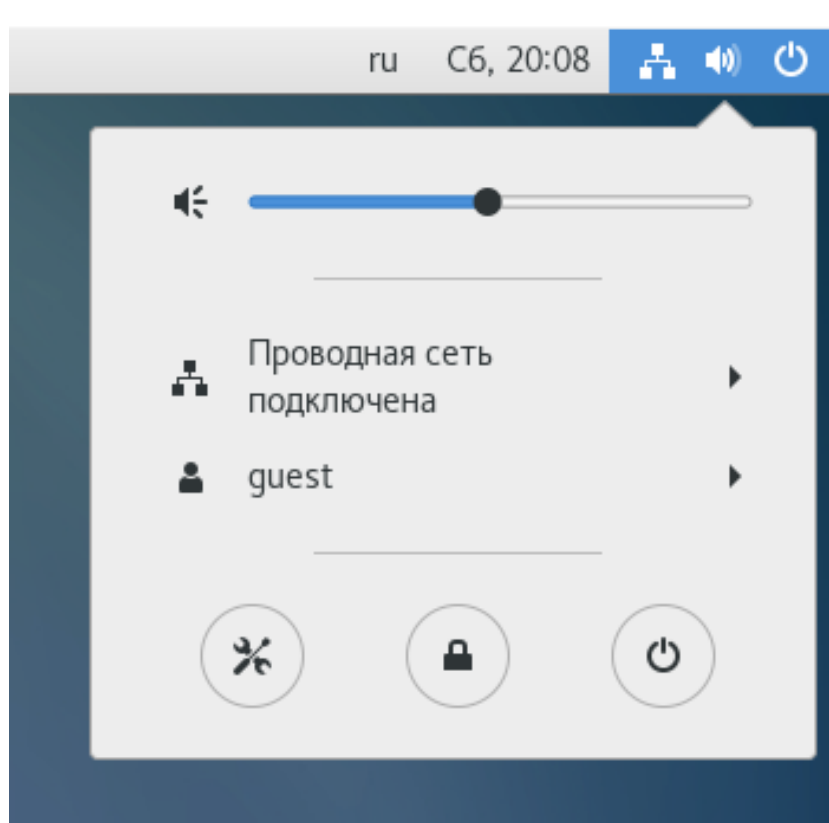


Рис. 4.3: Вход в систему

4. С помощью команды `pwd` определяю директорию.

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

Рис. 4.4: `pwd`

5. Уточняю имя пользователя командой `whoami`.

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

Рис. 4.5: `whoami`

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

```
[guest@vemanaeva ~]$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vemanaeva ~]$ groups
guest
```

Рис. 4.6: Уточняю имя пользователя, группу, и группы

7. Сравниваю полученные данные с данными в приглашении командной строке.

```
[guest@vemanaeva ~]$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vemanaeva ~]$ groups
guest
```

Рис. 4.7: Сравнение данных

8. Просматриваю файл /etc/passwd командой cat /etc/passwd.

```
[guest@vemanaeva ~]$ 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/ssh:/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
ntp:x:38:38:./etc/ntp:/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
vemanaeva:x:1000:1000:vemanaeva:/home/vemanaeva:/bin/bash
vboxadd:x:988:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
```

Рис. 4.8: Просмотр файла

9. Определяю существующие в системе директории командой `ls -l /home/`

```
[guest@vemanaeva ~]$ ls -l /home/
итого 8
drwx-----. 15 guest      guest      4096 сен 16 20:08 guest
drwx-----. 15 vemanaeva vemanaeva 4096 сен 16 19:56 vemanaeva
```

Рис. 4.9: Команда `ls -l /home/`

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

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

Рис. 4.10: Проверяю, какие расширенные атрибуты установлены

11. Создаю в домашней директории поддиректорию `dir1` командой `mkdir dir1`

Определяю командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.

```

[guest@vemanaeva ~]$ mkdir dir1
[guest@vemanaeva ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 16 20:17 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Докум
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Загру
drwxr-xr-x. 2 guest guest 68 сен 16 20:15 Изобр
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Музык
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Общед
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Рабоч
drwxr-xr-x. 2 guest guest 6 сен 16 20:08 Шабло
[guest@vemanaeva ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1

```

Рис. 4.11: Создаю поддиректорию dir1

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

```

[guest@vemanaeva ~]$ chmod 000 dir1
[guest@vemanaeva ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 16 20:17 dir1

```

Рис. 4.12: Снимаю с директории dir1 все атрибуты

13. Совершаю попытку создания в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`

Проверяю командой `ls -l /home/guest/dir1` действительно ли файл file1 не находится внутри директории dir1.

```

[guest@vemanaeva ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@vemanaeva ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@vemanaeva ~]$ chmod 700 dir1
[guest@vemanaeva ~]$ ls -l /home/guest/dir1
итого 0

```

Рис. 4.13: попытка создания в директории dir1 файл file1

Далее заполняю таблицы

4.1 Таблицы (4.1 и 4.2)

Таблица 4.1: Установленные права и разрешённые действия

Права дирек- тории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись фай- ла	Чте- ние фай- ла	Сме-	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атри- бутов файла
						на ди- рек- то- рии			
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
<hr/>									
d-x---	(000)	-	-	-	-	+	-	-	-
d-x---	(100)	-	-	-	-	+	-	-	-

Права дирек- тории	Пра- ва фай- ла	Со-		Уда-		Сме-		Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атри- бутов файла
		зда- ние фай- ла	ле- ние фай- ла	За- пись фай- ла	Чте- ние фай- ла	на ди- рек- то- рии	Про- смотр файлов в директо- рии			
d-x---	(200)	-	-	-	-	+	-	-	-	-
d-x---	(300)	-	-	-	-	+	-	-	-	-
d-x---	(400)	-	-	-	+	+	-	-	-	-
d-x---	(500)	-	-	-	+	+	-	-	-	-
d-x---	(600)	-	-	-	+	+	-	-	-	-
d-x---	(700)	-	-	-	+	+	-	-	-	-
<hr/>										
d-w---	(000)	-	-	-	-	-	-	-	-	-
d-w---	(100)	-	-	-	-	-	-	-	-	-
d-w---	(200)	-	-	-	-	-	-	-	-	-
d-w---	(300)	-	-	-	-	-	-	-	-	-
d-w---	(400)	-	-	-	-	-	-	-	-	-
d-w---	(500)	-	-	-	-	-	-	-	-	-
d-w---	(600)	-	-	-	-	-	-	-	-	-
d-w---	(700)	-	-	-	-	-	-	-	-	-
<hr/>										
d- wx---	(000)	+	+	-	-	+	-	+	-	-
d- wx---	(100)	+	+	-	-	+	-	+	-	-
d- wx---	(200)	+	+	+	-	+	-	+	-	-

Права дирек- тории	Пра- ва фай- ла	Сме-							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись фай- ла	Чте- ние фай- ла	на ди- рек- то- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атри- бутов файла
d- wx---	(300)	+	+	+	-	+	-	+	-
d- wx---	(400)	+	+	-	+	+	-	+	+
d- wx---	(500)	+	+	-	+	+	-	+	+
d- wx---	(600)	+	+	+	+	+	-	+	+
d- wx---	(700)	+	+	+	+	+	-	+	+

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

dr-x---	(000)	-	-	-	-	+	+	-	-
dr-x---	(100)	-	-	-	-	+	+	-	-
dr-x---	(200)	-	-	+	-	+	+	-	-

Права дирек- тории	Пра- ва фай- ла	Сме-				Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атри- бутов файла
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись фай- ла	Чте- ние фай- ла			
dr-x---	(300)	-	-	+	-	+	+	-
dr-x---	(400)	-	-	-	+	+	+	-
dr-x---	(500)	-	-	-	+	+	+	-
dr-x---	(600)	-	-	+	+	+	+	-
dr-x---	(700)	-	-	+	+	+	+	-

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

drwx---	(000)	+	+	-	-	+	+	+
drwx---	(100)	+	+	-	-	+	+	+
drwx---	(200)	+	+	+	-	+	+	+
drwx---	(300)	+	+	+	-	+	+	+
drwx---	(400)	+	+	-	+	+	+	+
drwx---	(500)	+	+	-	+	+	+	+
drwx---	(600)	+	+	+	+	+	+	+

drwx— (700) + + + + + + +

Таблица 4.2: Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx—	(000)
Удаление файла	d-wx—	(000)
Чтение файла	d-x—	(400)
Запись в файл	d-x—	(200)
Переименование файла	d-wx—	(000)
Создание поддиректории	d-wx—	(000)
Удаление поддиректории	d-wx—	(000)

5 Выводы по проделанной работе

5.1 Вывод

В результате выполнения работы мы ознакомились с основными этапами установки виртуальных машин и их настроек, а также создали виртуальную среду для выполнения последующих лабораторных работ.

Были записаны скринкасты выполнения и защиты лабораторной работы.

Ссылки на скринкасты:

- Выполнение, Youtube
- Выполнение, Rutube
- Защита презентации, Youtube
- Защита презентации, Rutube

Список литературы

1. Колисниченко Д. Linux. От новичка к профессионалу. В подлиннике. 8-е изд. 2022. 688 с.