

Лабораторная 2

Отчет

Карпачев Ярослав

Содержание

1	Цель работы.....	1
2	Задание	1
3	Выполнение лабораторной работы.....	3
4	Выводы	5
	Список литературы.....	5

Список иллюстраций

Рис. 1: Процесс смены пользователя	3
Рис. 2: Консольный вывод на команды.....	4
Рис. 3: Консольный вывод на команды.....	4

Список таблиц

No table of figures entries found.

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 Linux1

2 Задание

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора): `useradd guest`
2. Задайте пароль для пользователя guest (используя учётную запись администратора): `passwd guest`
3. Войдите в систему от имени пользователя guest.
4. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она

вашей домашней директорией? Если нет, зайдите в домашнюю директорию.

5. Уточните имя вашего пользователя командой `whoami`.
6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups`.
7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.
8. Просмотрите файл `/etc/passwd` командой `cat /etc/passwd`. Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах. Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клавишу `shift`, нажимайте `page up` и `page down`) либо программу `grep` в 1. При составлении работы использовались материалы [2—4]. Информационная безопасность компьютерных сетей 23 качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: `cat /etc/passwd | grep guest`
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`.
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`.
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»: `g`, `w`, `x`, для «владельца». Остальные атрибуты также важны (особенно при использовании доступа от имени разных пользователей, входящих в те или иные группы). Проверка всех атрибутов при всех условиях значительно увеличила бы таблицу: так 9 атрибутов на директорию и 9 атрибутов на

файл дают 218 строк без учёта дополнительных атрибутов, плюс таблица была бы расширена по количеству столбцов, так как все приведённые операции необходимо было бы повторить ещё как минимум для двух пользователей: входящего в группу владельца файла и не входящего в неё. После полного заполнения табл. 2.1 и анализа полученных данных нам удалось бы выяснить, что заполнение её в таком виде излишне. Можно 24 Кулябов Д. С., Королькова А. В., Геворкян М. Н. разделить большую таблицу на несколько малых независимых таблиц. В данном примере предлагается рассмотреть 3 + 3 атрибута, т.е. 26 = 64 варианта. Замечание 2: в ряде действий при выполнении команды удаления файла вы можете столкнуться с вопросом: «удалить защищённый от записи обычный файл dir1/file1?» Обратите внимание, что наличие этого вопроса не позволяет сделать правильный вывод о том, что файл можно удалить. В ряде случаев, при ответе «у» (да) на указанный вопрос, возможно получить другое сообщение: «невозможно удалить dir1 /file1: Отказано в доступе».

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

3 Выполнение лабораторной работы

1. Меняем пользователя на root чтоб получить права для создания пользователя, создаем его и вводим пароль для него

```
Rocky Linux 9.4 (Blue Onyx)
Kernel 5.14.0-427.13.1.el9_4.x86_64 on an x86_64

shox login: [ 13.847971] block dm-0: the capability attribute has been deprecated.
ls /
Password:
Login incorrect

shox login: yokarpachev
Password:
[yokarpachev@shox ~]$ useradd guest
useradd: Permission denied.
useradd: cannot lock /etc/passwd: try again later.
[yokarpachev@shox ~]$ passwd guest
passwd: Only root can specify a user name.
[yokarpachev@shox ~]$ sudo useradd guest

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 yokarpachev:
[yokarpachev@shox ~]$ passwd guest
passwd: Only root can specify a user name.
[yokarpachev@shox ~]$ su -
Password:
[root@shox ~]# useradd guest
useradd: user 'guest' already exists
[root@shox ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[root@shox ~]# _
```

Рис. 1: Процесс смены пользователя

2. Заходим в нового пользователя проверяем что мы действительно в папке домашней, проверяем что мы действительно тот пользователь о котором думаем (получаем краткую информацию с помощью id), выводим все известные пароли ищем нашего основного пользователя и получаем

краткую информацию о нем (различия в госте и основы - на 1 больше id и тд), получаем данные о атрибутах в /home/

```
Rocky Linux 9.4 (Blue Onyx)
Kernel 5.14.0-427.13.1.el9_4.x86_64 on an x86_64

vbox login: guest
Password:
[guest@vbox ~]$ pwd
/home/guest
[guest@vbox ~]$ echo $HOME
/home/guest
[guest@vbox ~]$ whoami
guest
[guest@vbox ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vbox ~]$ groups
guest
[guest@vbox ~]$ 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
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
sssd:x:997:995:User for sssd:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:996:994:chrony system user:/var/lib/chrony:/sbin/nologin
yokarpachev:x:1000:1000:yokarpachev:/home/yokarpachev:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@vbox ~]$ id yokarpachev
uid=1000(yokarpachev) gid=1000(yokarpachev) groups=1000(yokarpachev),10(wheel)
[guest@vbox ~]$ ls -l /home/
total 0
drwx----- 2 guest guest 62 Feb 27 11:21 guest
drwx----- 2 yokarpachev yokarpachev 83 Feb 27 11:25 yokarpachev
[guest@vbox ~]$
```

Рис. 2: Консольный вывод на команды

3. Пытаемся проверить атрибуты (неполучается так как нету прав), создаем dir1 определяем права доступа снимаем все атрибуты, попытаемся создать файл - ничего не получается так как мы сняли все права, команды не оказывают никакого эффекта (нет прав).

```
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
sssd:x:997:995:User for sssd:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:996:994:chrony system user:/var/lib/chrony:/sbin/nologin
yokarpachev:x:1000:1000:yokarpachev:/home/yokarpachev:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@vbox ~]$ id yokarpachev
uid=1000(yokarpachev) gid=1000(yokarpachev) groups=1000(yokarpachev),10(wheel)
[guest@vbox ~]$ ls -l /home/
total 0
drwx----- 2 guest guest 62 Feb 27 11:21 guest
drwx----- 2 yokarpachev yokarpachev 83 Feb 27 11:25 yokarpachev
[guest@vbox ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/yokarpachev
----- /home/guest
[guest@vbox ~]$ sudo lsattr /home

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 guest:
guest is not in the sudoers file. This incident will be reported.
[guest@vbox ~]$ cd $HOME
[guest@vbox ~]$ ls
[guest@vbox ~]$ pwd
/home/guest
[guest@vbox ~]$ mkdir dir1
[guest@vbox ~]$ ls -l dir1/
total 0
[guest@vbox ~]$ ls -la dir1/
total 0
drwxr-xr-x. 2 guest guest 6 Feb 27 11:34 .
drwx----- 3 guest guest 74 Feb 27 11:34 ..
[guest@vbox ~]$ chmod 000 dir1
[guest@vbox ~]$ ls -la dir1/
ls: cannot open directory 'dir1': Permission denied
[guest@vbox ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: No such file or directory
[guest@vbox ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@vbox ~]$ ls -la /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@vbox ~]$
```

Рис. 3: Консольный вывод на команды

4. Заполняем таблицу

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	w + x	—
Удаление файла	w + x	—
Запись в файл	x	w
Чтение файла	x	r
Переименование файла	w + x	—
Создание поддиректории	w + x	—
Удаление поддиректории	w + x	—

4 Выводы

Я создал нового пользователя, провел базовые операции по получению данных о разрешениях и информации о пользователях.

Список литературы