

Лабораторная работа №2

Информационная безопасность

Дьяконова Софья Александровна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	14

Список иллюстраций

2.1. Выполнение работы до просмотра файла passw - 6

2.2. 2 этап - 7

2.3. Выполнение работы до конца - 8

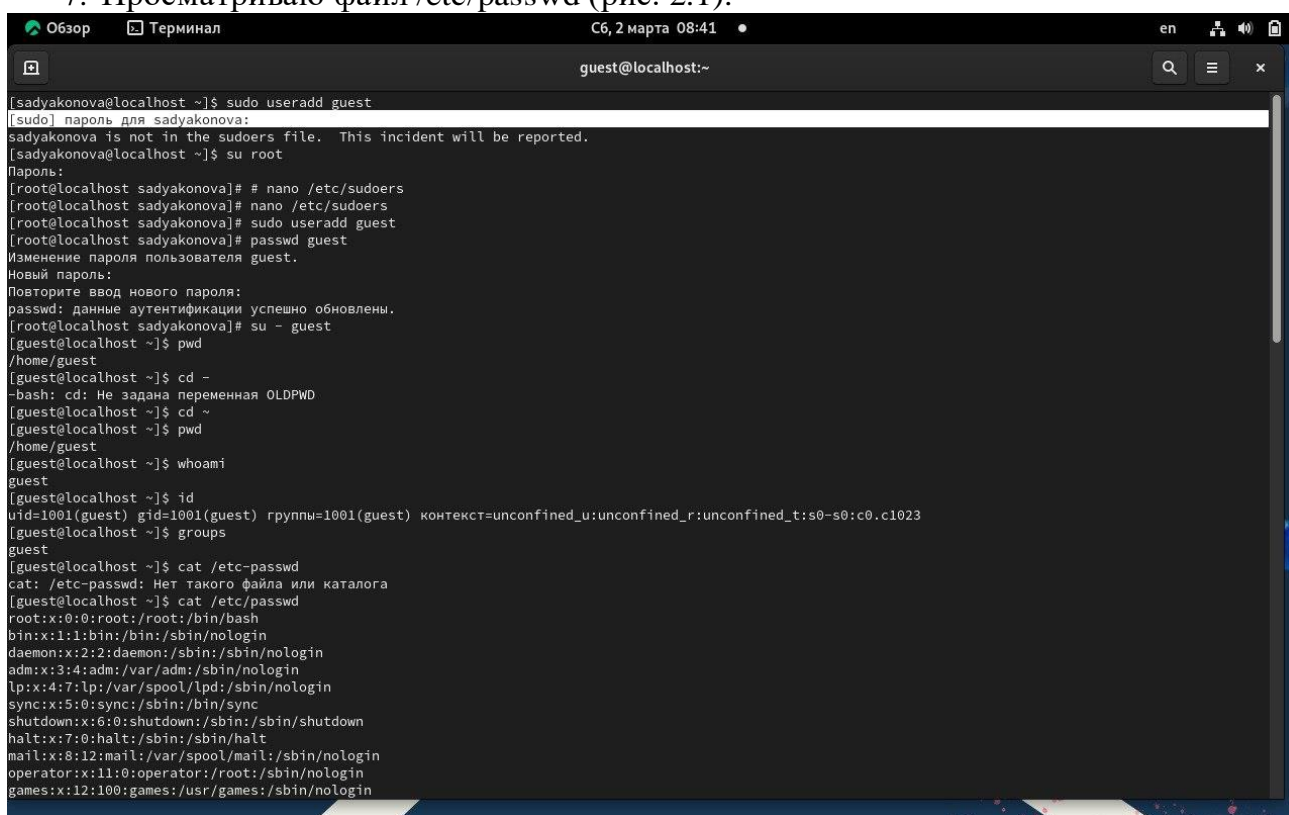
Список таблиц

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 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаю учётную запись пользователя guest (через учётную запись администратора) и задаю пароль (рис. 2.1).
3. Вхожу в систему от имени пользователя guest.
4. Определяю директорию, в которой нахожусь. Это действительно домашняя директория (рис. 2.1).
5. Уточняю имя пользователя через `whoami` (рис. 2.1).
6. Уточняю имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Данные совпадают (рис. 2.1).
7. Просматриваю файл `/etc/passwd` (рис. 2.1).



```
Обзор Терминал C6, 2 марта 08:41 en
guest@localhost:~
[sadyakonova@localhost ~]$ sudo useradd guest
[sudo] пароль для sadyakonova:
sadyakonova is not in the sudoers file. This incident will be reported.
[sadyakonova@localhost ~]$ su root
Пароль:
[root@localhost sadyakonova]# nano /etc/sudoers
[root@localhost sadyakonova]# nano /etc/sudoers
[root@localhost sadyakonova]# sudo useradd guest
[root@localhost sadyakonova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@localhost sadyakonova]# su - guest
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ cd -
-bash: cd: Не задана переменная OLDPWD
[guest@localhost ~]$ cd ~
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) rппны=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ groups
guest
[guest@localhost ~]$ cat /etc-passwd
cat: /etc-passwd: Нет такого файла или каталога
[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
```

Рис. 2.1 Выполнение работы до просмотра файла `passwd`

8. Нахожу в нём свою учётную запись через *grep*. Определяю *uid* и *gid* пользователя (рис. 2.2).
9. Определяю существующие в системе директории (рис. 2.2).
10. Проверяю, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории */home*. Мне отказано в доступе (рис. 2.2).
11. Создаю в домашней директории поддиректорию *dir1* командой *mkdir dir1* (рис. 2.2).

```

polkitd:x:998:996:User for polkitd:/usr/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/usr/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/usr/sbin/nologin
pipewire:x:997:993:Pipewire System Daemon:/var/run/pipewire:/usr/sbin/nologin
sssd:x:996:992:User for sssd:/usr/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/usr/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/usr/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/usr/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/usr/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/usr/sbin/nologin
clevis:x:983:982:clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/usr/sbin/nologin
gnome-initial-setup:x:981:980:/run/gnome-initial-setup:/usr/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/usr/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/usr/sbin/nologin
sadyakonova:x:1000:1000:sadyakonova:/home/sadyakonova:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@localhost ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/home/guest:/bin/bash
[guest@localhost ~]$ ls -l /home/
иторо 4
drwx-----. 4 guest      guest      92 map  2 08:25 guest
drwx-----. 14 sadyakonova sadyakonova 4096 Feb 18 17:01 sadyakonova
[guest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/sadyakonova
----- /home/guest
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 map  2 08:31 dir1
[guest@localhost ~]$ lsattr
----- ./dir1
[guest@localhost ~]$ chmod 000 dir1
chmod: невозможно получить доступ к 'dir': Нет такого файла или каталога
chmod: невозможно получить доступ к '1': Нет такого файла или каталога
[guest@localhost ~]$ chmod 000 dir1

```

рис. 2.2: 2 этап

Определяю командами *ls -l* и *lsattr*, какие права доступа и расширенные атрибуты были выставлены на директорию *dir1* (рис. 2.3).

12. Снимаю с директории *dir1* все атрибуты командой *chmod 000 dir1* (рис. 2.3).
13. Пытаюсь создать в директории *dir1* файл *file1*, но получаю отказ, так как я удалила права на доступ в прошлом пункте. Файл не был создан (рис. 2.3),

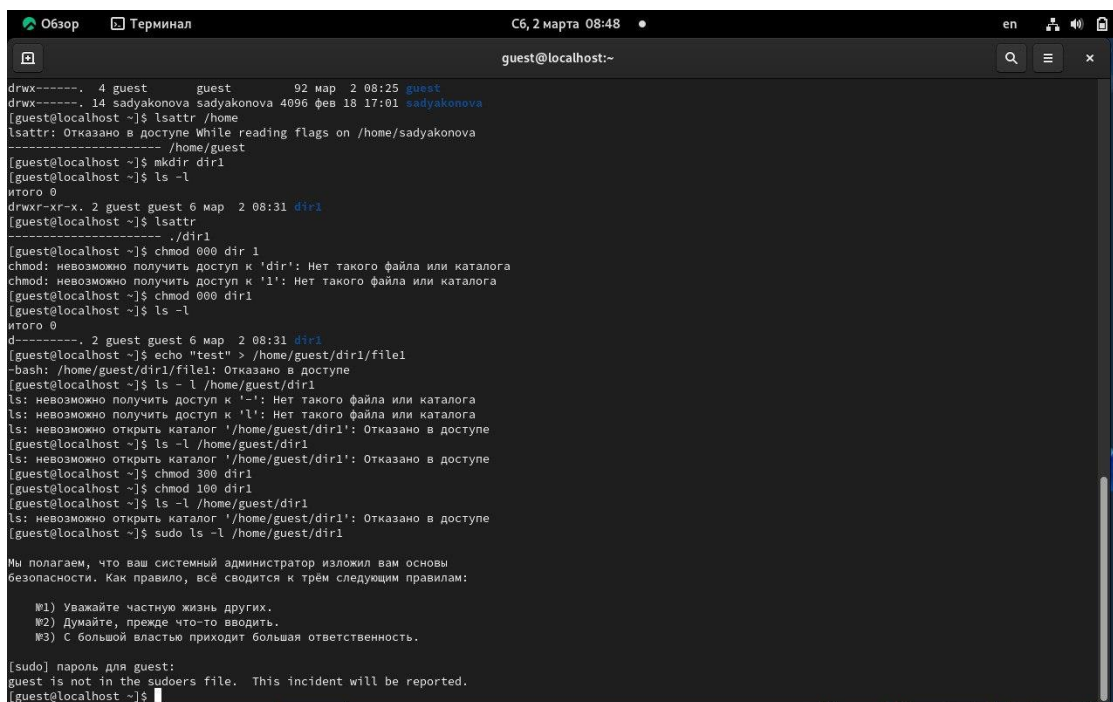


рис.2.3: Выполнение работы до конца

14. Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на ф
Создание файла	d(300)	-
Удаление файла	d(300)	-
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	-
Удаление поддиректории	d(300)	-

15. Заполнение таблицы «Установленные права и разрешённые действия»

Права ди- ректо- рии	Права файла	Со- зда- ние файла	Уда- ление файла	За- пись в файл	Чте- ние файла	Сме- на ди- ректо- рии	Про- смотр фай- лов в ди- ректо- рии	Пере- име- нова- ние файла	Сме- на атри- бутов 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)	+	+	+	+	+	+	+	+

3 Выводы

Я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

...