Отчёт по лабораторной работе №2

Основы инфрмационной безопасности

Лисенков Е.Р.

Содержание

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 Задачи

Научиться работать с консолью Rocky Linux.

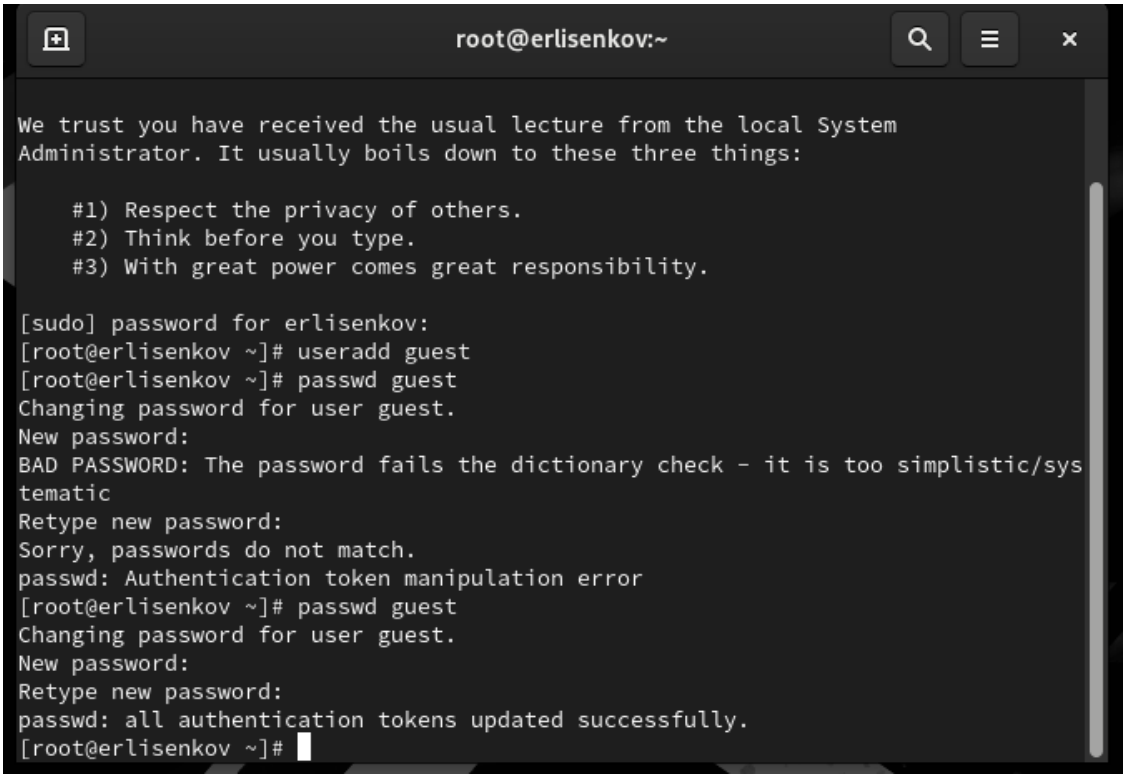
3 Выполнение лабораторной работы

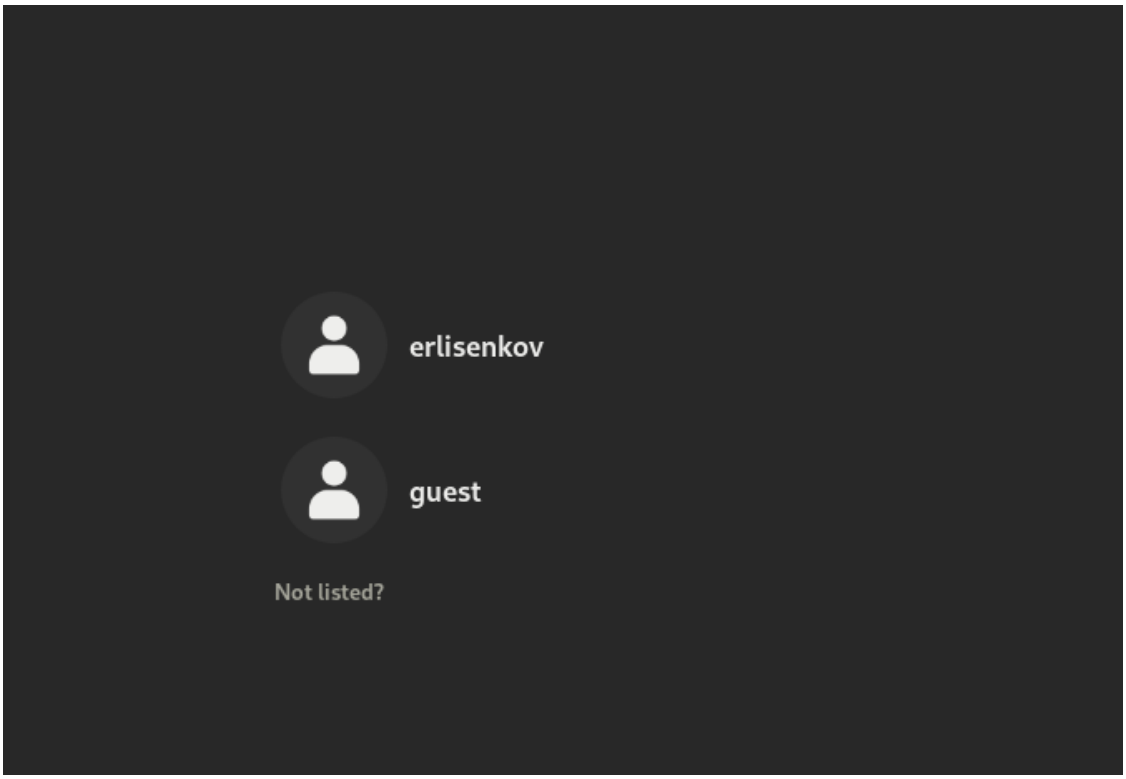
В установленной при выполнении предыдущей лабораторной работы операционной системе создам учётную запись пользователя guest (использую учётную запись администратора):

useradd guest

Задам пароль для пользователя guest (использую учётную запись администратора):(рис. 1)(рис. 2)

passwd guest





Определю директорию, в которой вы находитесь, командой pwd. Сравню её с приглашением командной строки. (рис. 3) Уточню имя пользователя командой whoami. Уточню имя пользователя, его группу, а также группы, куда вхо- дит

пользователь, командой id. Выведенные значения uid, gid и др. Сравню вывод id с выводом команды groups. (рис. 3)(рис. 4)

```
[guest@erlisenkov ~]$ pwd
/home/guest
[guest@erlisenkov ~]$ whoami
guest
[guest@erlisenkov ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c102
3
[guest@erlisenkov ~]$ groups
guest
[guest@erlisenkov ~]$ 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
tss:x:59:59:Account used for TPM access:/:/usr/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
sssd:x:997:995:User for sssd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
geoclue:x:996:994:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/:/sbin/nologin
pipewire:x:995:992:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/:/usr/sbin/nologin
cockpit-wsinstance:x:989:988:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:988:987:User for flatpak system helper:/:/sbin/nologin
colord:x:987:986:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:986:985:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:985:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
stapunpriv:x:159:159:systemtap unprivileged user:/var/lib/stapunpriv:/sbin/nologin
pesign:x:984:983:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:983:982::/run/gnome-initial-setup/:/sbin/nologin
chrony:x:982:981:chrony system user:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
dnsmasq:x:981:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
erlisenkov:x:1000:1000:erlisenkov:/home/erlisenkov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@erlisenkov ~]$
```

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

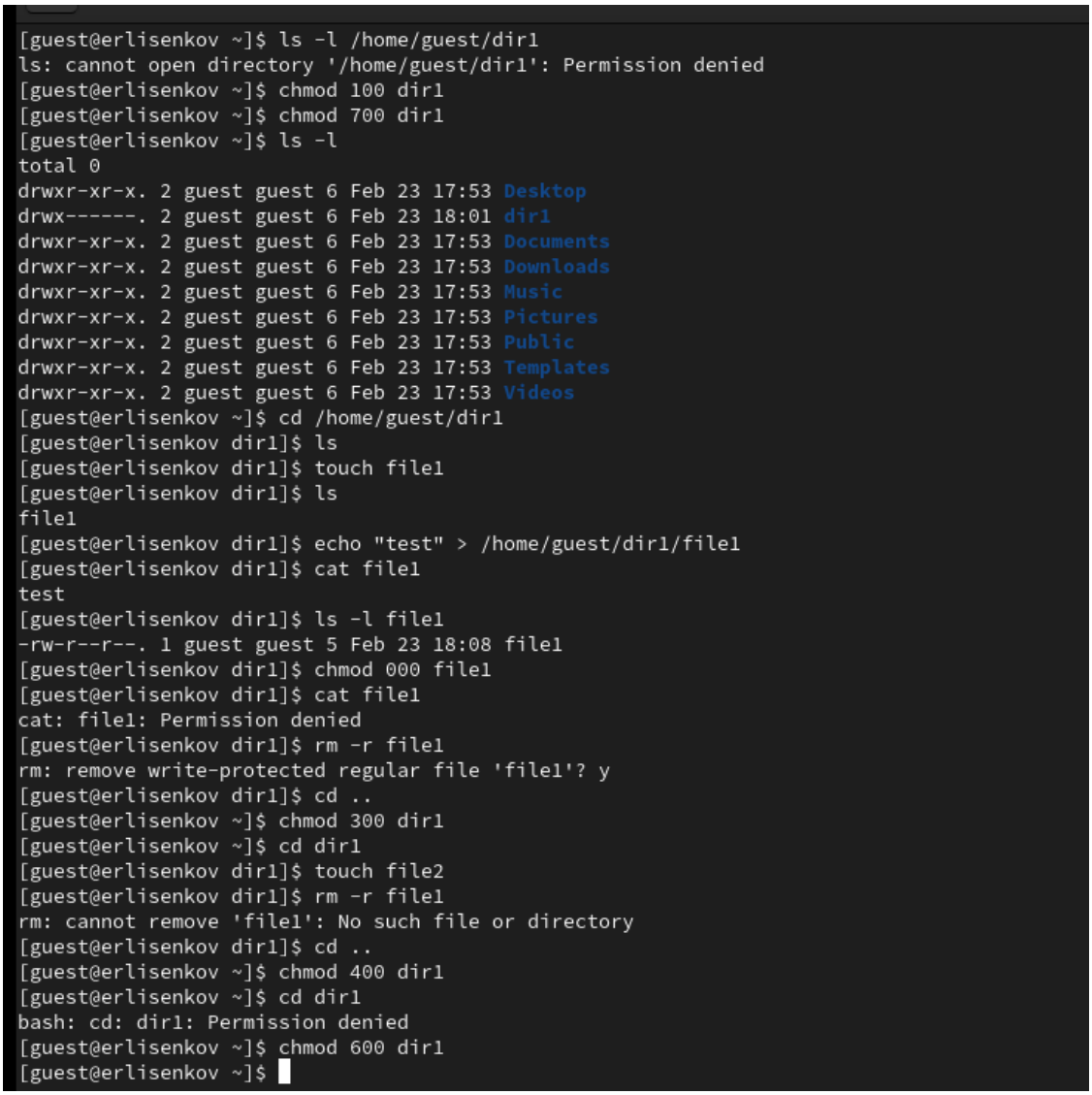
Определю существующие в системе директории командой (рис.5).

```
total 8
drwx------. 14 erlisenkov erlisenkov 4096 Feb 22 13:38 erlisenkov
drwx------. 14 guest      guest      4096 Feb 23 17:53 guest
[guest@erlisenkov ~]$
```

Проверю, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home (рис.6)

```
[guest@erlisenkov ~]$ ls -l /home/
total 8
drwx------. 14 erlisenkov erlisenkov 4096 Feb 22 13:38 erlisenkov
drwx------. 14 guest      guest      4096 Feb 23 17:53 guest
[guest@erlisenkov ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/erlisenkov
---------------------- /home/guest
[guest@erlisenkov ~]$ mkdir dir1
[guest@erlisenkov ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Desktop
drwxr-xr-x. 2 guest guest 6 Feb 23 18:01 dir1
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Documents
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Music
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Public
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Templates
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Videos
[guest@erlisenkov ~]$ lsattr
---------------------- ./Desktop
---------------------- ./Downloads
---------------------- ./Templates
---------------------- ./Public
---------------------- ./Documents
---------------------- ./Music
---------------------- ./Pictures
---------------------- ./Videos
---------------------- ./dir1
[guest@erlisenkov ~]$ chmod 000 dir1
[guest@erlisenkov ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Desktop
d---------. 2 guest guest 6 Feb 23 18:01 dir1
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Documents
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Music
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Public
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Templates
drwxr-xr-x. 2 guest guest 6 Feb 23 17:53 Videos
[guest@erlisenkov ~]$
```

Приступлю к выполнению пунктов 11-15 в которых я протестирую функцию комманд разрешения и запрета каких либо возможностей у файлов или целых папок(рис. 7)



4 Выводы

Я усвоил материал и готов к дальнейшему изучению линукс!