

Отчёт по лабораторной работе №2

discipline: Основы информационной безопасности group: НПМбд-02-21 author: Газизова Регина Ильгамовна

Front matter

title: "Отчет по лабораторной работе №2" subtitle: "Основы информационной безопасности"
author: "Газизова Регина"

Generic options

lang: ru-RU toc-title: "Содержание"

Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt

I18n polyglossia

polyglossia-lang: name: russian options:

- spelling=modern
- babelshorthands=true polyglossia-otherlangs: name: english

I18n babel

babel-lang: russian babel-otherlangs: english

Fonts

mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9

Biblatex

biblatex: true biblio-style: "gost-numeric" biblatexoptions:

- parenttracker=true
- backend=biber
- hyperref=auto
- language=auto
- autolang=other*
- citestyle=gost-numeric

Pandoc-crossref LaTeX customization

figureTitle: "Рис." tableTitle: "Таблица" listingTitle: "Листинг" lofTitle: "Список иллюстраций"
lolTitle: "Листинги"

Misc options

indent: true header-includes:

- `\usepackage{indentfirst}`
 - `\usepackage{float} # keep figures where there are in the text`
 - `\floatplacement{figure}{H} # keep figures where there are in the text`
-

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

Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но одна из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо.

Изначально каждый файл имел три параметра доступа. Вот они:

- Чтение (r) - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;
- Запись (w) - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;
- Выполнение (x) - вы не можете выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу.

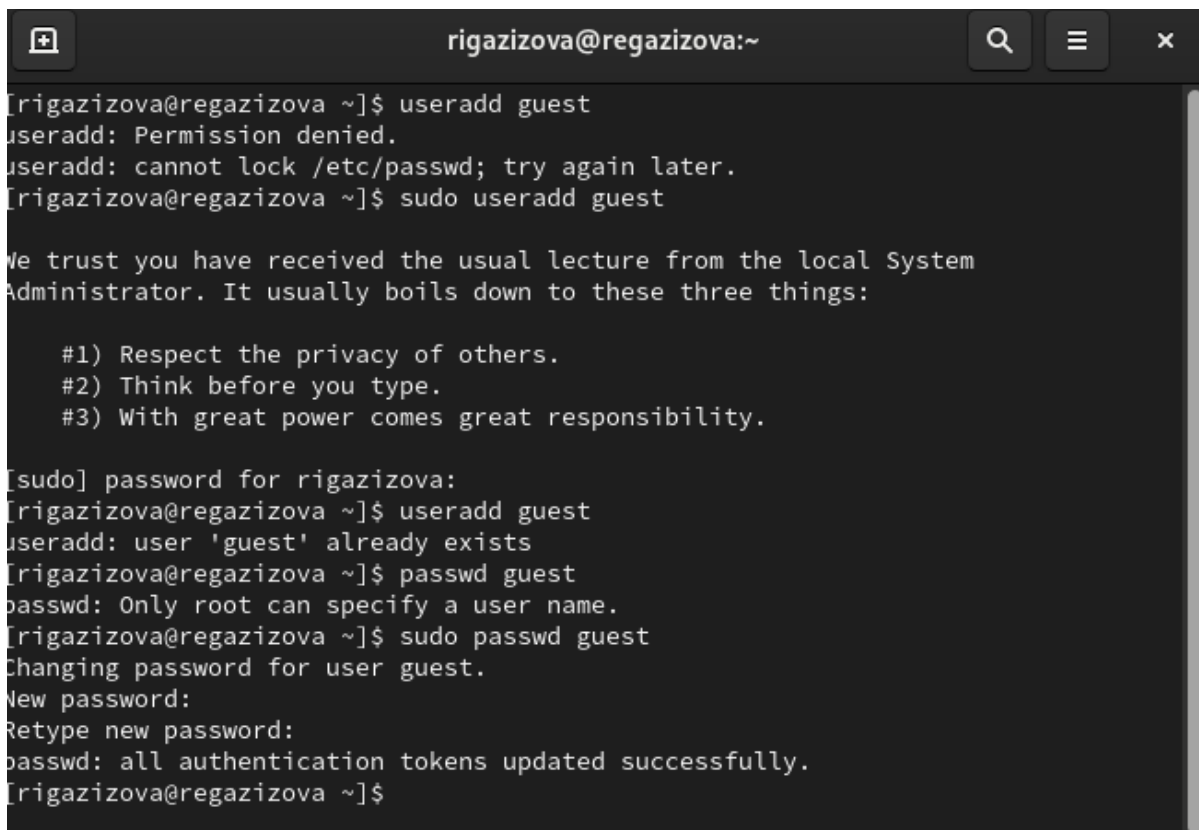
Но все эти права были бы бессмысленными, если бы применялись сразу для всех

пользователей. Поэтому каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

- Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение.
- Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу.
- Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла.

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаем учётную запись и пароль пользователя guest (рис.1)

A screenshot of a terminal window titled 'rigazizova@regazizova:~'. The terminal shows the following commands and output:

```
[rigazizova@regazizova ~]$ useradd guest
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[rigazizova@regazizova ~]$ sudo useradd guest

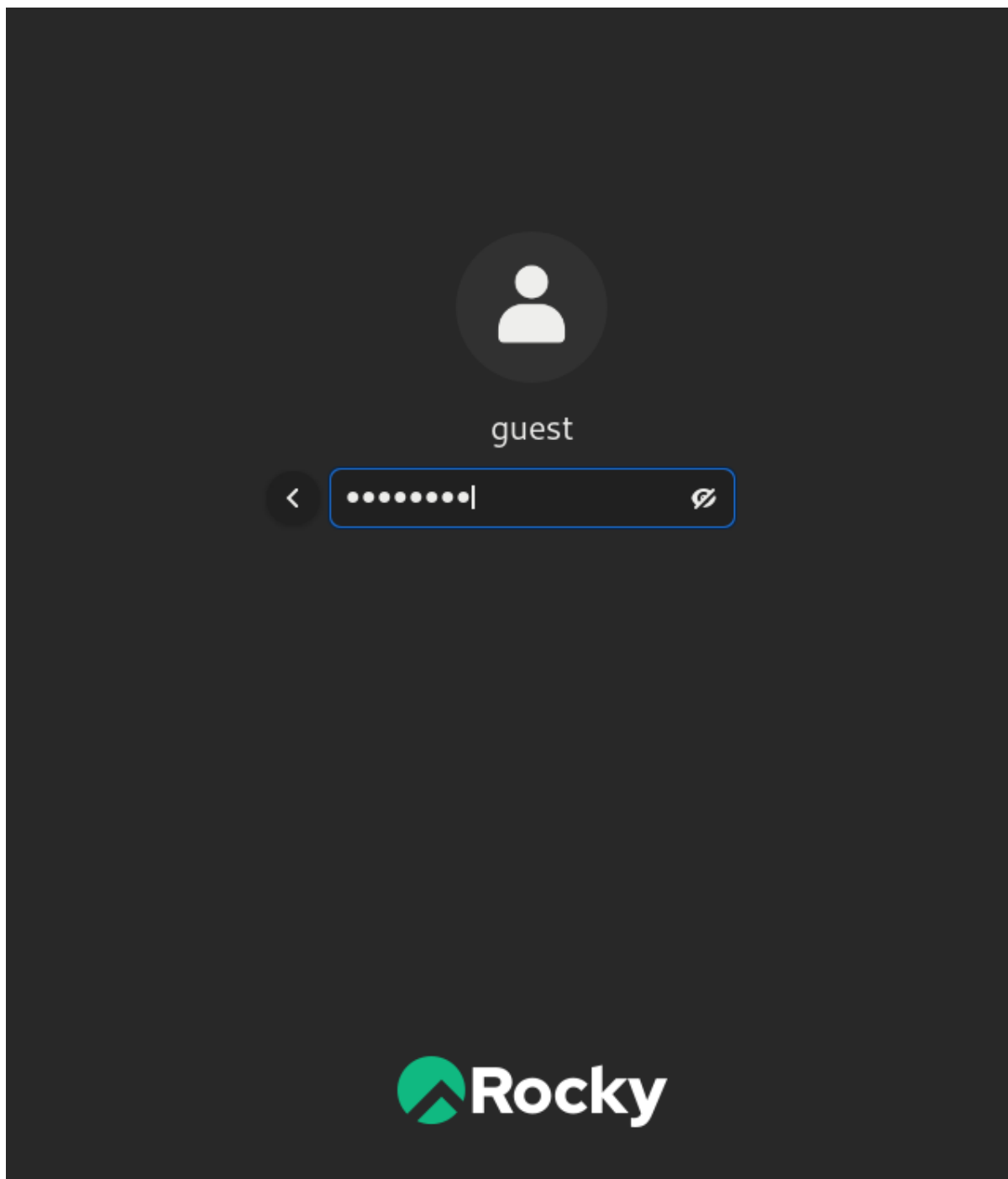
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for rigazizova:
[rigazizova@regazizova ~]$ useradd guest
useradd: user 'guest' already exists
[rigazizova@regazizova ~]$ passwd guest
passwd: Only root can specify a user name.
[rigazizova@regazizova ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[rigazizova@regazizova ~]$
```

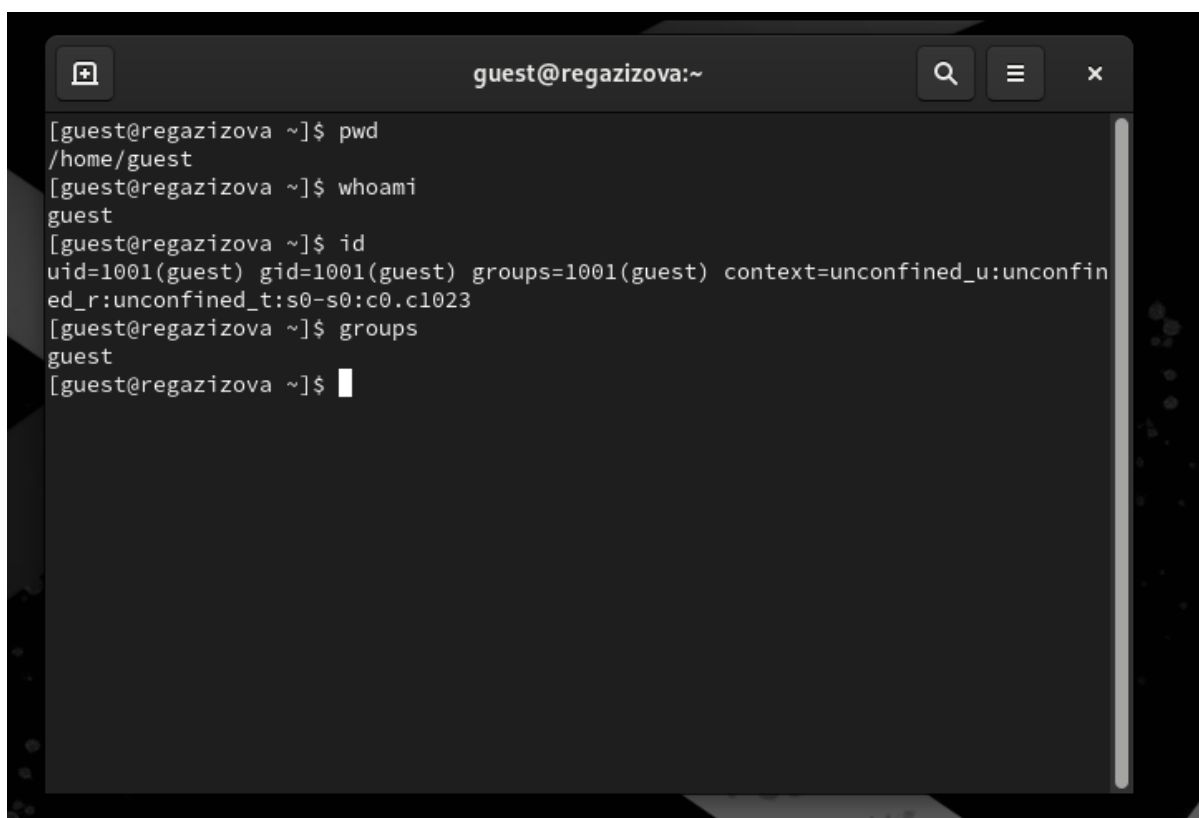
(рис.1)

2. Входим в систему от имени пользователя guest (рис.2)



(рис.2)

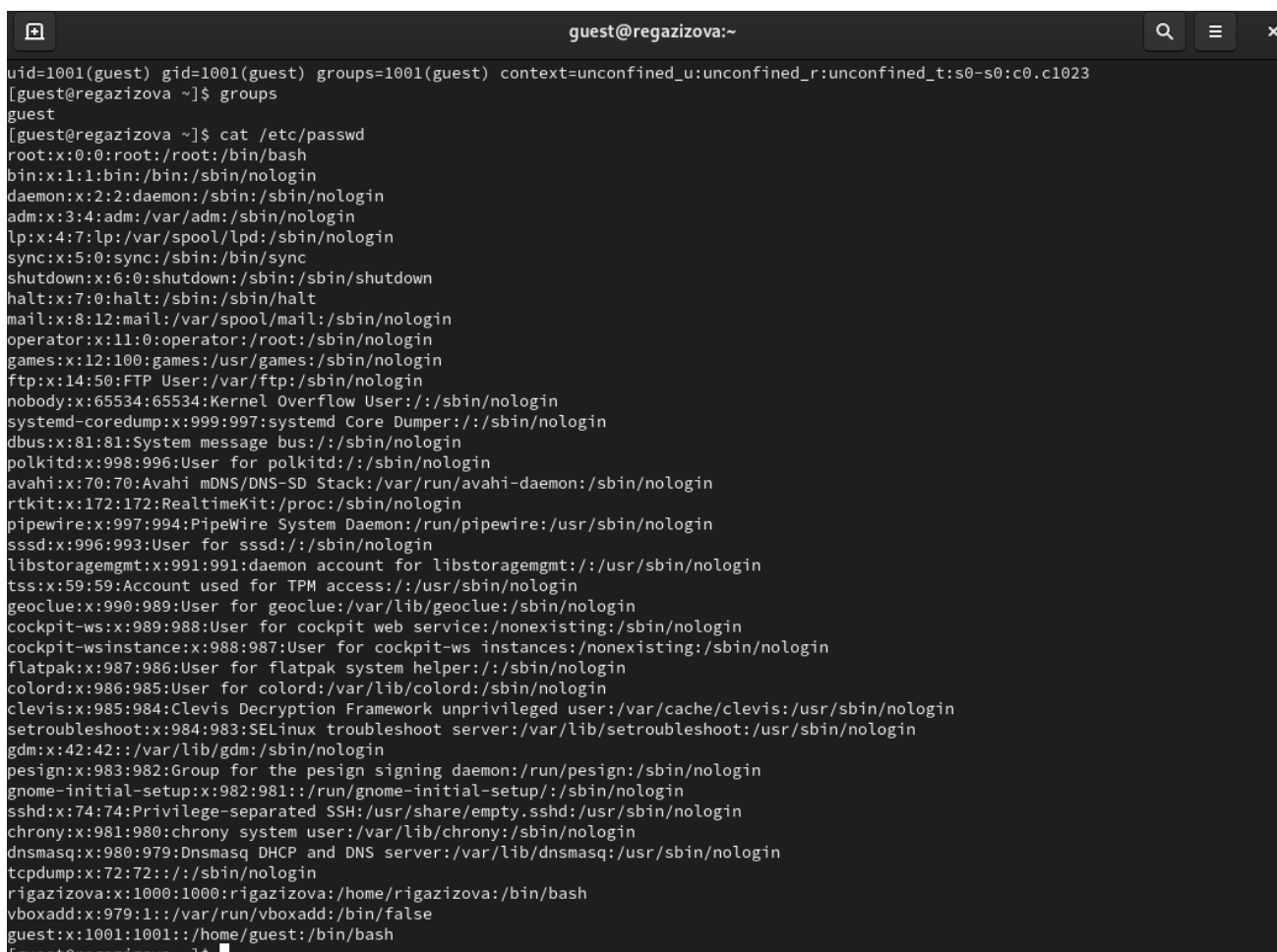
3. Командой `rwd` определяем директорию, в которой находимся. Она совпадает с домашней директорией. Уточняем имя пользователя командой `whoami`. Уточняем имя пользователя, его группу, а также группы, куда входит пользователь, командой `id` (все также `guest`). Сравниваем вывод `id` с выводом команды `groups` и делаем вывод, что команда `id` гораздо информативнее (рис.3)

A terminal window titled 'guest@regazizova:~' with search, menu, and close icons. It shows the execution of 'pwd', 'whoami', 'id', and 'groups' commands. The output of 'id' shows 'uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023'. The output of 'groups' shows 'guest'.

```
[guest@regazizova ~]$ pwd
/home/guest
[guest@regazizova ~]$ whoami
guest
[guest@regazizova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@regazizova ~]$ groups
guest
[guest@regazizova ~]$
```

(рис.3)

4. Сморим файл /etc/passwd командой cat /etc/passwd (рис.4) Находим в нём свою учётную запись и определяем uid(1001) и git(1001) пользователя, они сопадают со значения полученными в предыдущих пунктах (рис.5)

A terminal window titled 'guest@regazizova:~' showing the output of 'cat /etc/passwd'. The output lists system users and regular users, including 'guest' at the bottom with 'uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023'.

```
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@regazizova ~]$ 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
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
rigazizova:x:1000:1000:rigazizova:/home/rigazizova:/bin/bash
vboxadd:x:979:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@regazizova ~]$
```

(рис.4)

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

(рис.5)

5. Определяем существующие в системе директории командой `ls -l /home/` (рис.6). Проблем с этим не возникло. Увидели, что на директориях установлены права чтения, записи и выполнения для самого пользователя.

```
[guest@regazizova ~]$ ls -l /home/  
total 8  
drwx-----. 14 guest      guest      4096 Sep 12 17:54 guest  
drwx-----. 14 rigazizova rigazizova 4096 Sep 12 17:50 rigazizova  
[guest@regazizova ~]$
```

(рис.6)

6. Попытались проверить, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой `lsattr /home` (рис.7) Для пользователя `guest` удалось проверить, а для поддиректории админа в доступе отказано.

```
[guest@regazizova ~]$ lsattr /home  
lsattr: Permission denied While reading flags on /home/rigazizova  
----- /home/guest  
[guest@regazizova ~]$
```

(рис.7)

7. Создали в домашней директории поддиректорию `dirr1` командой `mkdir dirr1`. Определили командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dirr1` - чтение, запись и выполнение доступны для самого пользователя, а так же для группы, остальным только чтение и выполнение. Расширенные атрибуты отсутствуют (рис.8)

```

[guest@regazizova ~]$ mkdir dirr1
[guest@regazizova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Desktop
d------. 2 guest guest 6 Sep 12 18:03 dir1
drwxr-xr-x. 2 guest guest 6 Sep 12 18:14 dirr1
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Documents
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Music
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Public
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Templates
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Videos
[guest@regazizova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
lsattr: Permission denied While reading flags on ./dir1
----- ./dirr1

```

(рис.8)

8. Сняли с директории dirr1 все атрибуты командой `chmod 000 dirr1` и проверили её правильность с помощью выполнения команды `ls -l`. Все сработало правильно, все атрибуты сняты.

```

[guest@regazizova ~]$ chmod 000 dirr1
[guest@regazizova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Desktop
d------. 2 guest guest 6 Sep 12 18:03 dir1
d------. 2 guest guest 6 Sep 12 18:14 dirr1
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Documents
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Music
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Public
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Templates
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Videos

```

(рис.9)

9. Попытались создать в директории dirr1 файл file1 командой `echo "test" > /home/guest/dirr1/file1`. Проверили выполнение командой `ls -l /home/guest/dirr1`. Результат - создать файл файл не получилось, т.к. отсутствует право на запись. Командой `chmod 700 dirr1` наделили директорию всеми правами и попробовали еще раз создать файл. Результат - сработало (рис.10)

```
[guest@regazizova ~]$ echo "test" > /home/guest/dirr1/file1
bash: /home/guest/dirr1/file1: Permission denied
[guest@regazizova ~]$ ls -l ?home/guest/dirr1
ls: cannot access '?home/guest/dirr1': No such file or directory
[guest@regazizova ~]$ chmod 700 dirr1
[guest@regazizova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Desktop
d------. 2 guest guest 6 Sep 12 18:03 dir1
drwx-----. 2 guest guest 6 Sep 12 18:14 dirr1
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Documents
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Music
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Public
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Templates
drwxr-xr-x. 2 guest guest 6 Sep 12 17:54 Videos
[guest@regazizova ~]$ ls -l /home/guest/dirr1
total 0
[guest@regazizova ~]$ cd dirr1
[guest@regazizova dirr1]$ ls
[guest@regazizova dirr1]$ cd ../
```

(рис.10)

10. Проверяем опытным путем, какие права к чему дают доступ (рис.11)

|+| |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)|+|+|-|-|+|+|+|+|

Таблица 2.2

||||| |-|-|-|-| |Операция| |Минимальные права на директорию| |Минимальные права на файл| |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)| |-|

Выводы

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