

Презентация по лабораторной работе № 2

Основы информационной безопасности

Луангсуваннавонг Сайпхачан

Содержание I

1 1. Информация

2 2. Выполнение лабораторной работы

3 3. Выводы

Раздел 1

1. Информация

1.1 Докладчик

- Луангсуваннавонг Сайпхачан

1.1 Докладчик

- Луангсуваннавонг Сайпхачан
- студент группы НКАбд-01-24

1.1 Докладчик

- Луангсуваннавонг Сайпхачан
- студент группы НКАбд-01-24
- Российский университет дружбы народов им. П. Лумумбы

1.1 Докладчик

- Луангсуваннавонг Сайпхачан
- студент группы НКАбд-01-24
- Российский университет дружбы народов им. П. Лумумбы
- <https://github.com/sayprachanh-lsvnn>

1.2 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

1.3 Задание

1 Работа с атрибутами файлов

1.3 Задание

- 1 Работа с атрибутами файлов
- 2 Заполнение таблицы «Установленные права и разрешённые действия»(табл. 2.1)

1.3 Задание

- ① Работа с атрибутами файлов
- ② Заполнение таблицы «Установленные права и разрешённые действия»(табл. 2.1)
- ③ Заполнение таблицы «Минимальные права для совершения операций»(табл. 2.2)

Раздел 2

2. Выполнение лабораторной работы

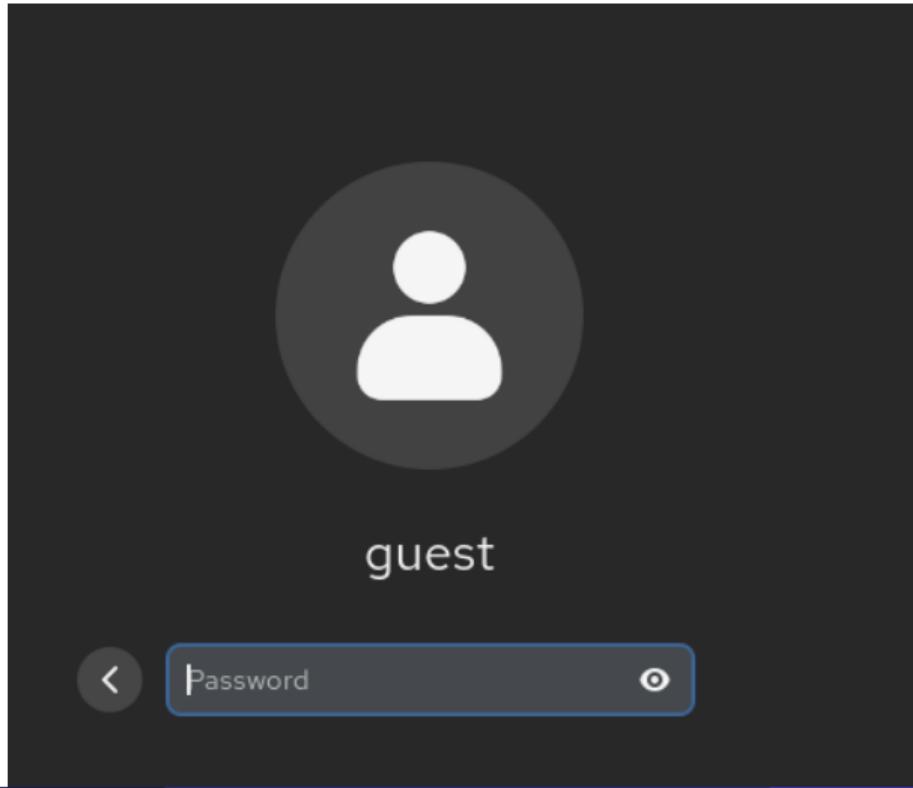
2.1 Работа с атрибутами файлов

Я открываю терминал в операционной системе Rocky Linux и создаю новую учётную запись пользователя guest.

```
sayprachanhlsvnv@sayprachanhlsvnv:~$ sudo -i  
[sudo] password for sayprachanhlsvnv:  
Sorry, try again.  
[sudo] password for sayprachanhlsvnv:  
root@sayprachanhlsvnv:~# useradd guest  
root@sayprachanhlsvnv:~# passwd guest  
New password:  
Retype new password:  
passwd: password updated successfully  
root@sayprachanhlsvnv:~#
```

2.2 Работа с атрибутами файлов

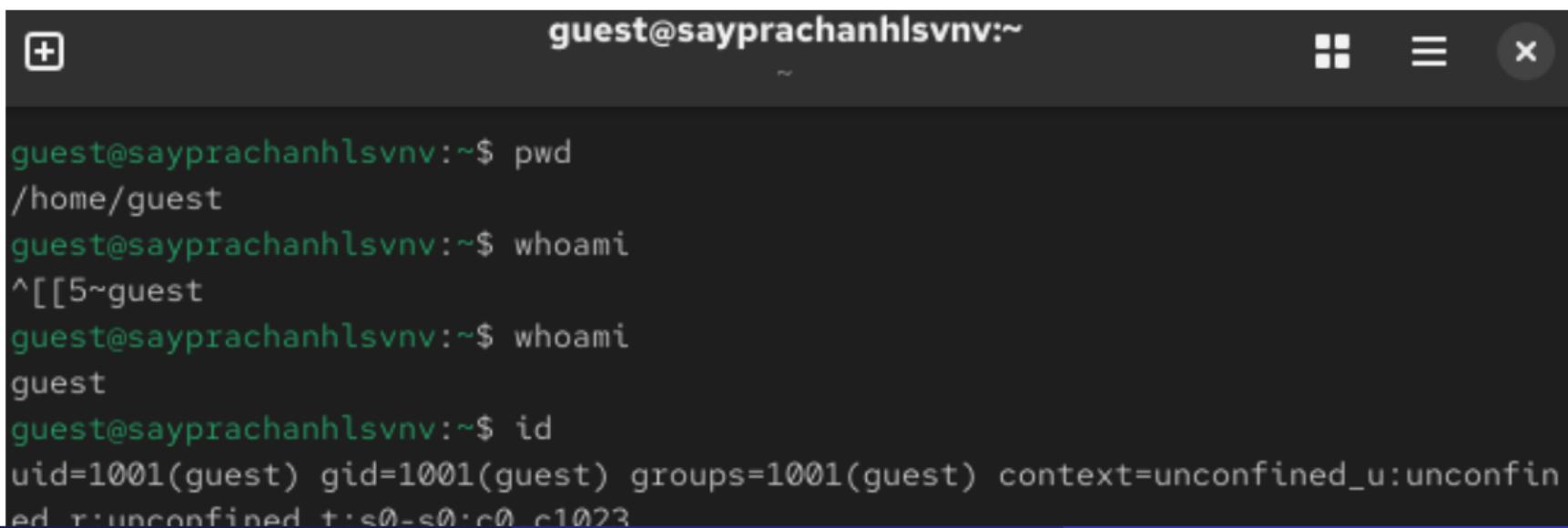
Вхожу в пользователя guest.



2.3 Работа с атрибутами файлов

С помощью команды `pwd` я отображаю текущую директорию (`/home/guest/`), затем определяю имя своего пользователя командой `whoami`.

Используя команду `id`, я получаю информацию об имени пользователя, имени группы, а также о группах, в которые входит пользователь; если использовать команду `groups`, она отобразит только информацию о пользователе `guest`.



The screenshot shows a terminal window with the following session:

```
guest@sayprachanhlsvnv:~$ pwd
/home/guest
guest@sayprachanhlsvnv:~$ whoami
^[[5~guest
guest@sayprachanhlsvnv:~$ whoami
guest
guest@sayprachanhlsvnv:~$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0 c1023
```

2.4 Работа с атрибутами файлов

Я просматриваю основную информацию об учётных записях пользователей в файле /etc/passwd.

```
guest@sayprachanhlsvnv:~$ cat /etc/passwd
root:x:0:0:Super User:/root:/bin/bash
bin:x:1:1:bin:/bin:/usr/sbin/nologin
daemon:x:2:2:daemon:/sbin:/usr/sbin/nologin
adm:x:3:4:adm:/var/adm:/usr/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/usr/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:/usr/sbin/nologin
operator:x:11:0:operator:/root:/usr/sbin/nologin
games:x:12:100:games:/usr/games:/usr/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/usr/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User://:/usr/sbin/nologin
dbus:x:81:81:System Message Bus://:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access://:/usr/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
systemd-oom:x:999:999:systemd Userspace OOM Killer://:/sbin/nologin
polkitd:x:114:114:User for polkitd://:/sbin/nologin
rtkit:x:172:172:RealtimeKit://:/sbin/nologin
geoclue:x:998:997:User for geoclue:/var/lib/geoclue:/sbin/nologin
clevis:x:997:996:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/
```



2.5 Работа с атрибутами файлов

Я получаю информацию о пользователе с помощью команды „cat /etc/passwd | grep guest“.

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

Рисунок 5: Получение информации о пользователе

2.6 Работа с атрибутами файлов

Мы получаем список поддиректорий внутри /home/ с помощью команды ls -l — и это верно: как у sayprachanhlsvnv, так и у guest одинаковые права: drwx---.

```
guest@sayprachanhlsvnv:~$ ls -l /home/
total 8
drwx----- 14 guest          guest          4096 Feb 13 13:57 guest
drwx----- 20 sayprachanhlsvnv sayprachanhlsvnv 4096 Feb 13 00:01 sayprachanhlsvnv
guest@sayprachanhlsvnv:~$
```

Рисунок 6: Получение списка подкаталогов и их атрибутов

2.7 Работа с атрибутами файлов

Я попытался проверить расширенные атрибуты поддиректорий, находящихся в директории /home, но это не удалось.

```
guest@sayprachanhlsvnv:~$ lsattr /home
lsattr: Permission denied While reading flags on /home/sayprachanhlsvnv
----- /home/guest
guest@sayprachanhlsvnv:~$ █
```

Рисунок 7: Получение списка подкаталогов и их атрибутов

2.8 Работа с атрибутами файлов

Я создаю поддиректорию dir1, проверяю список её поддиректорий (он пуст) и просматриваю расширенные атрибуты командой lsattr, но они не отобразились; использую команду ls -la, видно, что атрибуты: drwxr-xr-x.

```
guest@sayprachanhlsvnv:~$ mkdir dir1
guest@sayprachanhlsvnv:~$ ls -l dir1
total 0
guest@sayprachanhlsvnv:~$ lsattr dir1
guest@sayprachanhlsvnv:~$ ls -la
total 24
drwx-----. 15 guest guest 4096 Feb 13 13:41 .
drwxr-xr-x.  4 root   root   43 Feb 13 13:35 ..
-rw-r--r--.  1 guest guest  18 Oct 29 2024 .bash_logout
-rw-r--r--.  1 guest guest 144 Oct 29 2024 .bash_profile
-rw-r--r--.  1 guest guest 522 Oct 29 2024 .bashrc
drwx-----.  9 guest guest 4096 Feb 13 13:37 .cache
drwx-----.  8 guest guest 4096 Feb 13 13:37 .config
drwxr-xr-x.  2 guest guest  6 Feb 13 13:37 Desktop
drwxr-xr-x.  2 guest guest  6 Feb 13 13:41 dir1
drwxr-xr-x.  2 guest guest  6 Feb 13 13:37 Documents
drwxr-xr-x.  2 guest guest  6 Feb 13 13:37 Downloads
drwx-----.  4 guest guest 32 Feb 13 13:37 local
```



2.9 Работа с атрибутами файлов

Я устанавливаю атрибуты с помощью команды chmod 000, затем с помощью ls -l проверяю результат — отображается, что dir1 имеет атрибуты 0.

```
guest@sayprachanhlsvnv:~$ chmod 000 dir1
guest@sayprachanhlsvnv:~$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Desktop
d-----. 2 guest guest 6 Feb 13 13:41 dir1
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Documents
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Music
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Public
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Templates
drwxr-xr-x. 2 guest guest 6 Feb 13 13:37 Videos
guest@sayprachanhlsvnv:~$ ls -l dir1
```



2.10 Работа с атрибутами файлов

Я пытаюсь создать файл в этой директории, а также просмотреть директорию — получаю отказ в доступе

```
guest@sayprachanhlsvnv:~$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
guest@sayprachanhlsvnv:~$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
guest@sayprachanhlsvnv:~$ █
```

Рисунок 10: Настройка атрибутов

2.11 Заполнение таблицы 2.1

```
mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied
guest@sayprachanhlsvnv:~$ chmod 500 dir1/file1
guest@sayprachanhlsvnv:~$ echo test > dir1/file1
bash: dir1/file1: Permission denied
guest@sayprachanhlsvnv:~$ echo test > dir1/file2
bash: dir1/file2: Permission denied
guest@sayprachanhlsvnv:~$ echo test >> dir1/file1
bash: dir1/file1: Permission denied
guest@sayprachanhlsvnv:~$ rm dir1/file1
rm: remove write-protected regular file 'dir1/file1'? y
rm: cannot remove 'dir1/file1': Permission denied
guest@sayprachanhlsvnv:~$ cat dir1/file1
test
test
test
guest@sayprachanhlsvnv:~$ cd dir1
guest@sayprachanhlsvnv:~/dir1$ cd
guest@sayprachanhlsvnv:~$ ls -l dir1
ls: cannot open directory 'dir1': Permission denied
guest@sayprachanhlsvnv:~$ mv dir1/file1 dir1/file2
mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied
guest@sayprachanhlsvnv:~$ chmod 600 dir1/file1
guest@sayprachanhlsvnv:~$ echo test > dir1/file2
bash: dir1/file2: Permission denied
guest@sayprachanhlsvnv:~$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
guest@sayprachanhlsvnv:~$ echo test >> dir1/file1
guest@sayprachanhlsvnv:~$ cat dir1/file1
test
test
test
guest@sayprachanhlsvnv:~$ cd dir1
```

2.12 Заполнение таблицы 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)	-

Раздел 3

3. Выводы

3. Выводы

Я получил практические навыки работы в консоли с атрибутами файлов и закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.