

Лабораторная работа №2

Дисциплина: основы информационной безопасности

Пронякова Ольга Максимовна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	12
	Список литературы	13

Список иллюстраций

2.1	Создание новой учетной записи	6
2.2	Определяем директорию	7
2.3	Определяем имя и группы пользователя	7
2.4	Просмотр файла	8
2.5	Выполнение команд	9
2.6	Снятие с директори атрибутов	9
2.7	Снятие с директори атрибутов	10
2.8	Заполнение таблицы «Установленные права и разрешённые действия»	10
2.9	Определение минимально необходимых прав для выполнения операций внутри директории	11

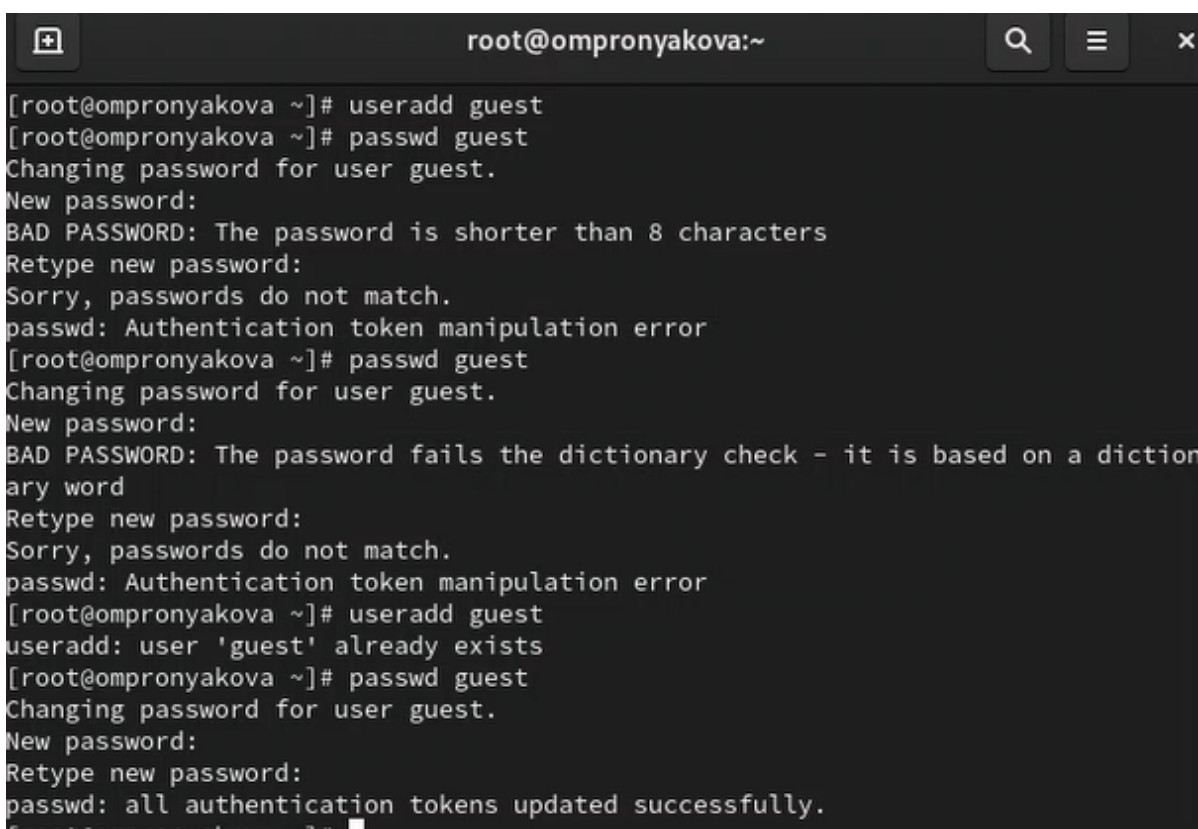
Список таблиц

1 Цель работы

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

2 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создаю учётную запись пользователя guest: `useradd guest`. Далее задаю пароль для пользователя guest: `passwd guest`(рис.2.1).



```
root@ompronyakova:~  
[root@ompronyakova ~]# useradd guest  
[root@ompronyakova ~]# 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.  
passwd: Authentication token manipulation error  
[root@ompronyakova ~]# passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word  
Retype new password:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
[root@ompronyakova ~]# useradd guest  
useradd: user 'guest' already exists  
[root@ompronyakova ~]# passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@ompronyakova ~]#
```

Рис. 2.1: Создание новой учетной записи

Вхожу в систему от имени пользователя guest. Определяю директорию, в которой нахожусь, командой `pwd`. Определяю, является ли она домашней директорией? Уточняю имя моего пользователя командой `whoami` и его группу, а также

группы, куда входит пользователь, командой `id`(рис.2.2), (рис.2.3).

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

Рис. 2.2: Определяем директорию

```
ompronyakova.localdomain
[guest@ompronyakova ~]$ hostnamectl
Static hostname: ompronyakova.localdomain
Icon name: computer-vm
Chassis: vm 01F 584 I
Machine ID: 6f2f1c15257c446abd9eaaa856cdbbc78
Boot ID: b8f9510d08304ecd9f2017329f49825f
Virtualization: oracle
Operating System: Rocky Linux 9.3 (Blue Onyx)
CPE OS Name: cpe:/o:rocky:rocky:9::baseos
Kernel: Linux 5.14.0-362.18.1.el9_3.x86_64
Architecture: x86-64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
[guest@ompronyakova ~]$
```

Рис. 2.3: Определяем имя и группы пользователя

Просматриваю файл `/etc/passwd` командой `cat /etc/passwd`. Нахожу в нём свою учётную запись. Определяю `uid` пользователя. Определяю `gid` пользователя(рис.2.4).

```
[guest@ompronyakova ~]$ 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:997:993:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
sssd:x:996:992:User for sssd:/sbin/nologin
```

Рис. 2.4: Просмотр файла

Определяю существующие в системе директории командой `ls -l /home/` Проверяю какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home` Создаю в домашней директории поддиректорию `dir1` командой `mkdir dir1` Определяю командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`(рис.2.5).


```

gnome-initial-setup:x:980:979:./run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
ompronyakova:x:1000:1000:ompronyakova:/home/ompronyakova:/bin/bash
vboxadd:x:977:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
[guest@ompronyakova ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:./home/guest:/bin/bash
[guest@ompronyakova ~]$ ls /home/
guest ompronyakova
[guest@ompronyakova ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Feb 24 18:15 guest
drwx-----. 14 ompronyakova ompronyakova 4096 Feb 24 18:03 ompronyakova
[guest@ompronyakova ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/ompronyakova
----- /home/guest
[guest@ompronyakova ~]$ mkdir dir1
[guest@ompronyakova ~]$ ls -l dir1
total 0
[guest@ompronyakova ~]$ lsattr dir1

```

Рис. 2.5: Выполнение команд

Снимаю с директории dir1 все атрибуты командой `chmod 000 dir1` и проверяю с её помощью правильность выполнения команды `ls -l`(рис.2.6).

```

[guest@ompronyakova ~]$ chmod 000 dir1
[guest@ompronyakova ~]$ chmod 000 dir1/
[guest@ompronyakova ~]$ ls -l ./ grep dir1
ls: cannot access 'grep': No such file or directory
./:
total 0
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Desktop
d------. 2 guest guest 6 Feb 24 18:21 dir1
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Documents
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Music
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Public
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Templates
drwxr-xr-x. 2 guest guest 6 Feb 24 18:13 Videos
ls: cannot open directory 'dir1': Permission denied
[guest@ompronyakova ~]$

```

Рис. 2.6: Снятие с директории атрибутов

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

Заполняю таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заново в таблицу знак «+», если не разрешена, знак «-». На основании заполненной таблицы определяю те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполняю таблицу (рис.2.8), (рис.2.9).

[illegible]

10

L	M	N	O	P
	Оперция	Минимальные права на директорию	Минимальные права на файл	
	Создание файла	300	0	
	Удаление файла	300	0	
	Чтение файла	100	400	
	Запись в файл	100	200	
	Переименование файла	300	0	
	Создание поддиректории	300	0	
	Удаление поддиректории	300	0	

Рис. 2.9: Определение минимально необходимых прав для выполнения операций внутри директории

3 Выводы

Получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

Список литературы

1. Дискреционное разграничение прав в Linux. Основные атрибуты