

Отчет по лабораторной работе №2

дисциплина: Основы информационной безопасности

Морозова Ульяна Константиновна

Содержание

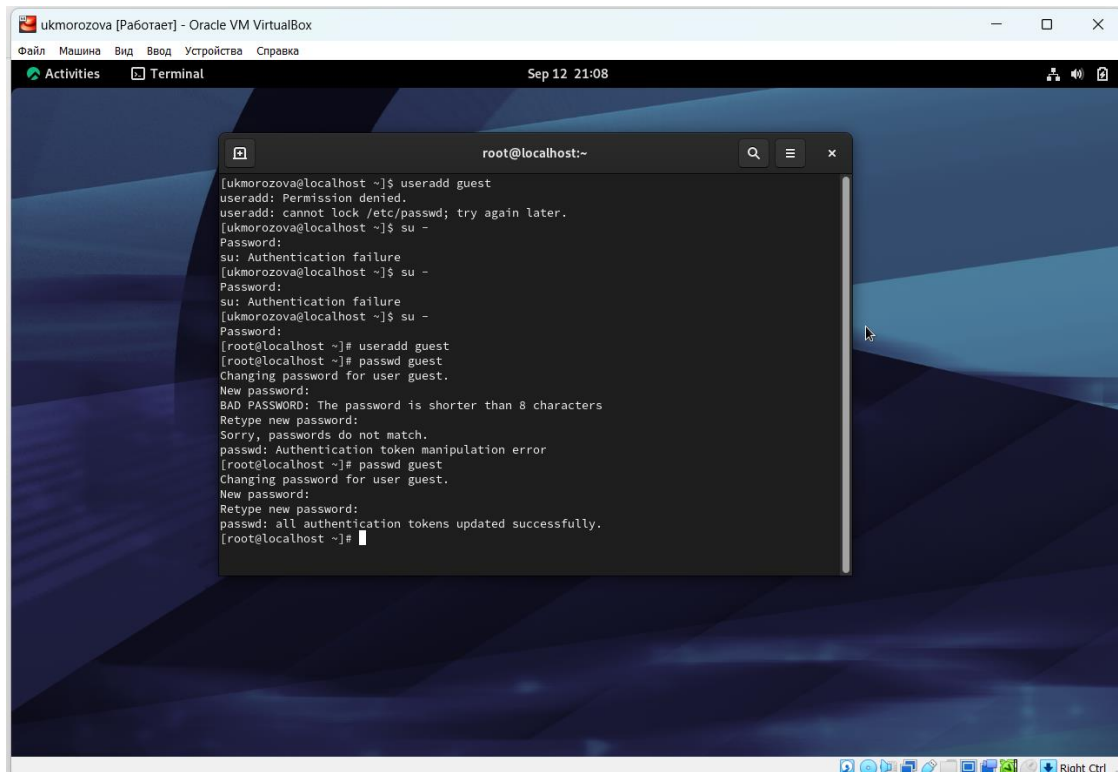
Цель работы	1
Выполнение лабораторной работы.....	1
Выводы	8

Цель работы

Целью данной работы является 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.

Выполнение лабораторной работы

1. В установленной при выполнении лабораторной работы №1 операционной системе создаем учётную запись пользователя guest (используем учётную запись администратора root): `useradd guest` Задаем пароль для пользователя `guest: passwd guest`



Создание пользователя

2. Входим в систему от имени пользователя guest и определяем директорию, в которой находимся, командой pwd.

```
[root@localhost ~]# su - guest
[guest@localhost ~]$ pwd
/home/guest
```

Домашняя директория пользователя guest

3. Уточним имя пользователя командой whoami, а также уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой id.

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

Имя и данные пользователя

4. Просмотрим файл /etc/passwd командой cat /etc/passwd и найдем в нём свою учётную запись.

```

[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
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

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

```

5. Определим существующие в системе директории командой `ls -l /home/`

```

[guest@localhost ~]$ ls -l /home/
total 4
drwx-----.  4 guest      guest      92 Sep 12 21:10 guest
drwx-----. 14 ukmoroova ukmoroova 4096 Sep 11 09:41 ukmoroova

```

home

- Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`
- Создаем в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`. Снимаем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверяем с её помощью правильность выполнения команды `ls -l`

```
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 12 21:17 dir1
[guest@localhost ~]$ lsattr
----- ./dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
total 0
d----- . 2 guest guest 6 Sep 12 21:17 dir1
```

Создание директории dir1

8. Попытаемся создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1. Так как на папке не стоят права для создания файла, у нас не получилось это сделать.

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

Попытка создания файла

9. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории.

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d (000)	000	-	-	-	-	-	-	-	-
d--x (100)	000	-	-	-	-	+	-	-	+
d-w-(200)	000	-	-	-	-	-	-	-	-
d-wx(300)	000	+	+	-	-	+	-	+	-
dr--(400)	000	-	-	-	-	-	+	-	-
dr-x(500)	000	-	-	-	-	+	+	-	-
drw-(600)	000	-	-	-	-	-	+	-	-
drwx(700)	000	+	+	-	-	+	+	+	-
d (000)	100	-	-	-	-	-	-	-	-
d--x (100)	100	-	-	-	-	+	-	-	-
d-w-(200)	100	-	-	-	-	-	-	-	-
d-wx(300)	100	+	+	-	-	+	-	+	-
dr--(400)	100	-	-	-	-	-	+	-	-
dr-x(500)	100	-	-	-	-	+	+	-	-
drw-(600)	100	-	-	-	-	-	+	-	-
drwx(700)	100	-	-	-	-	-	-	-	-
d (000)	200	-	-	-	-	-	-	-	-
d--x (100)	200	-	-	+	-	+	-	-	-
d-w-(200)	200	-	-	-	-	-	-	-	-
d-wx(300)	200	+	+	+	-	+	-	+	-
dr--(400)	200	-	-	-	-	-	+	-	-
dr-x(500)	200	-	-	+	-	+	+	-	-
drw-(600)	200	-	-	-	-	-	+	-	-
drwx(700)	200	+	+	+	-	+	+	+	-
d (000)	300	-	-	-	-	-	-	-	-
d--x (100)	300	-	-	+	-	+	-	-	-
d-w-(200)	300	-	-	-	-	-	-	-	-
d-wx(300)	300	+	+	-	+	+	-	+	-
dr--(400)	300	-	-	-	-	-	+	-	-
dr-x(500)	300	-	-	+	-	+	+	-	-
drw-(600)	300	-	-	-	-	-	+	-	-
drwx(700)	300	+	+	+	-	+	+	+	-

d (000)	400	-	-	-	-	-	-	-	-
d--x (100)	400	-	-	-	+	+	-	-	+
d-w-(200)	400	-	-	-	-	-	-	-	-
d-wx(300)	400	+	+	-	+	+	-	+	+
dr--(400)	400	-	-	-	-	-	+	-	-
dr-x(500)	400	-	-	-	+	+	+	-	+
drw-(600)	400	-	-	-	-	-	+	-	-
drwx(700)	400	+	+	-	+	+	+	+	+
d (000)	500	-	-	-	-	-	-	-	-
d--x (100)	500	-	-	-	+	+	-	-	+
d-w-(200)	500	-	-	-	-	-	-	-	-
d-wx(300)	500	+	+	-	+	+	-	+	+
dr--(400)	500	-	-	-	-	-	+	-	-
dr-x(500)	500	-	-	-	+	+	+	-	+
drw-(600)	500	-	-	-	-	-	+	-	-
drwx(700)	500	+	+	-	+	+	+	+	+
d (000)	600	-	-	-	-	-	-	-	-
d--x (100)	600	-	-	+	+	+	-	-	+
d-w-(200)	600	-	-	-	-	-	-	-	-
d-wx(300)	600	+	+	+	+	+	-	+	+
dr--(400)	600	-	-	-	-	-	+	-	-
dr-x(500)	600	-	-	+	+	+	+	-	+
drw-(600)	600	-	-	-	-	-	+	-	-
drwx(700)	600	+	+	+	+	+	+	+	+
d (000)	700	-	-	-	-	-	-	-	-
d--x (100)	700	-	-	+	+	+	-	-	+
d-w-(200)	700	-	-	-	-	-	-	-	-
d-wx(300)	700	+	+	+	+	+	-	+	+
dr--(400)	700	-	-	-	-	-	+	-	-
dr-x(500)	700	-	-	+	+	+	+	-	+
drw-(600)	700	-	-	-	-	-	+	-	-
drwx(700)	700	+	+	+	+	+	+	+	+

```
[guest@localhost ~]$ rm -r dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@localhost ~]$ echo "textnew" > dir1/file1
-bash: dir1/file1: Permission denied
[guest@localhost ~]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest@localhost ~]$ cd dir1
-bash: cd: dir1: Permission denied
[guest@localhost ~]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest@localhost ~]$ mv dir1/file1 file2
mv: cannot stat 'dir1/file1': Permission denied
[guest@localhost ~]$ chatter -a dir1/file1
chatter: Permission denied while trying to stat dir1/file1
[guest@localhost ~]$ chmod 100 dir1
[guest@localhost ~]$ echo "text" > dir1/file1
-bash: dir1/file1: Permission denied
[guest@localhost ~]$ ls -l
total 0
d--x-----. 2 guest guest 6 Sep 12 21:17 dir1
[guest@localhost ~]$ rm -r dir1/file1
rm: cannot remove 'dir1/file1': No such file or directory
[guest@localhost ~]$ echo "textnew" > dir1/file1
-bash: dir1/file1: Permission denied
[guest@localhost ~]$ cd dir1
[guest@localhost dir1]$ ls dir1
ls: cannot access 'dir1': No such file or directory
[guest@localhost dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest@localhost dir1]$ mv dir1/file1 file2
mv: cannot stat 'dir1/file1': No such file or directory
[guest@localhost dir1]$ echo "text" > dir1/file1
-bash: dir1/file1: No such file or directory
[guest@localhost dir1]$ cat dir1/file1
cat: dir1/file1: No such file or directory
[guest@localhost dir1]$ cd ..
[guest@localhost ~]$ cat dir1/file1
cat: dir1/file1: No such file or directory
[guest@localhost ~]$ chatter -a dir1/file1
chatter: No such file or directory while trying to stat dir1/file1
[guest@localhost ~]$ echo "text" > dir1/file1
-bash: dir1/file1: Permission denied
[guest@localhost ~]$
```

Выводы

Мы приобрели практические навыки в работе консоли с атрибутами файлов, закрепили теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.