

Отчет по лабораторной работе №2

Дисциплина: Информационная безопасность

Дорофеева Алёна Тимофеевна

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 Linux.

2 Задание

1. Создание учётной записи пользователя guest
2. Выполнение базовых операций с директориями и файлами
3. Заполнение таблицы “Установленные права и разрешённые действия” опытным путем
4. Заполнение таблицы “Минимальные права для совершения операций” на основании заполненной таблицы

3 Выполнение лабораторной работы

1. В установленной операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора): `useradd guest` и задайте пароль для пользователя guest (используя учётную запись администратора): `passwd guest`. (рис. 1)

```
[aldoro@localhost ~]$ su
Пароль:
[root@localhost aldoro]# useradd guest
[root@localhost aldoro]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@localhost aldoro]#
```

Рисунок 1: Создание учетной записи пользователя guest

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

```
[root@localhost aldoro]# su guest  
[guest@localhost aldoro]$
```

Рисунок 2: Вход в систему пользователя guest

3. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Зайдите в домашнюю директорию. (рис. 3)

```
[guest@localhost aldoro]$ pwd  
/home/aldoro  
[guest@localhost aldoro]$ cd  
[guest@localhost ~]$ pwd  
/home/guest
```

Рисунок 3: Определение директории

4. Уточните имя вашего пользователя командой `whoami`. (рис. 4)

```
[guest@localhost ~]$ whoami  
guest
```

Рисунок 4: Уточнение имени пользователя

5. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравнение вывода `id` с выводом команды `groups`. (рис. 5-6)

```
[guest@localhost ~]$ id guest  
uid=1001(guest) gid=1001(guest) группы=1001(guest)
```

```
[guest@localhost ~]$ groups  
guest
```

6. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.
7. Просмотрите файл `/etc/passwd` командой `cat /etc/passwd`. Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах. (рис. 6)

```
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
sssd:x:997:993:User for sssd:/sbin/nologin
pipewire:x:996:992:Pipewire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:CLEVIS Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:981:980:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
aldoro:x:1000:1000:Alena Dorofeeva:/home/aldoro:/bin/bash
vboxadd:x:978:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@localhost ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/home/guest:/bin/bash
[guest@localhost ~]$
```

Рисунок 6: Команда `cat /etc/passwd`

Замечание: использовала программу `grep` в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания: `cat /etc/passwd | grep guest`

8. Определите существующие в системе директории командой `ls -l /home/` Мне удалось получить список поддиректорий директории `/home`. Права на директориях установлены такие: `drwx` —, одинаковы для обеих поддиректорий (рис. 7)

```
[guest@localhost ~]$ ls -l /home/
итого 4
drwx-----. 14 aldoro aldoro 4096 сен 16 02:19 aldoro
drwx-----.  3 guest  guest   78 сен 16 03:01 guest
```

Рисунок 7: Определение существующих в системе директорий

9. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home` Мне удалось увидеть расширенные атрибуты директории. Однако не удалось увидеть расширенные атрибуты директорий других пользователей. (рис. 8)

```
[guest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/aldoro
----- /home/guest
```

Рисунок 8: Проверка расширенных атрибутов

10. Создайте в домашней директории поддиректорию `dir1` командой `mkdir dir1` Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`. (рис. 9)

```

[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 16 03:16 dir1
[guest@localhost ~]$ lsarrrt
bash: lsarrrt: command not found...
[guest@localhost ~]$ lsattr
----- ./dir1
[guest@localhost ~]$

```

Рисунок 9: Создание поддиректорию dir1

11. Снимите с директории dir1 все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l` (рис. 10)

```

[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d------. 2 guest guest 6 сен 16 03:16 dir1
[guest@localhost ~]$

```

Рисунок 10: Изменение прав на поддиректории dir1 и команда ls -l

12. Попробуйте создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. Получила отказ в выполнении операции по созданию файла, потому что недостаточно прав. (рис. 11) Проверила командой `ls -l /home/guest/dir1`, действительно - файл file1 не находится внутри директории dir1. (рис. 12)

```

[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@localhost ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@localhost ~]$ cd dir1
bash: cd: dir1: Отказано в доступе

```

Рисунок 11: Изменение прав на поддиректории dir1 и команда ls -l

```

[guest@localhost ~]$ chmod 700 dir1
[guest@localhost ~]$ ls -l /home/guest/dir1
итого 0
[guest@localhost ~]$

```

Рисунок 12: Изменение прав на поддиректории dir1 и команда ls -l

13. Заполните таблицу «Установленные права и разрешённые действия» (табл. 1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Таблица 1. Установленные права и разрешённые действия

Права директории	Права файла	Созд. ф-ла	Удал. ф-ла	Зап. в ф-л	Чт. ф-ла	Смена д-ии	Просм. ф-в в д-ии	Переим. ф-ла	См. атр. ф-ла
(000)	(000)	-	-	-	-	-	-	-	-

Права директории	Права файла	Созд. ф-ла	Удал. ф-ла	Зап. в ф- л	Чт. ф- ла	Смена д-ии	Просм. ф-в в д- ии	Переим. ф-ла	См. атр. ф-ла
(100)	(000)	-	-	-	-	+	-	-	+
(200)	(000)	-	-	-	-	-	-	-	-
(300)	(000)	+	+	-	-	+	-	+	+
(400)	(000)	-	-	-	-	-	+	-	-
(500)	(000)	-	-	-	-	+	+	-	+
(600)	(000)	-	-	-	-	-	+	-	-
(700)	(000)	+	+	-	-	+	+	+	+
(100)	(100)	-	-	-	-	+	-	-	+
(300)	(100)	+	+	-	-	+	-	+	+
(500)	(100)	-	-	-	-	+	+	-	+
(700)	(100)	+	+	-	-	+	+	+	+
(100)	(200)	-	-	+	-	+	-	-	+
(300)	(200)	+	+	+	-	+	-	+	+
(500)	(200)	-	-	+	-	+	+	-	+
(700)	(200)	+	+	+	-	+	+	+	+
(100)	(300)	-	-	+	-	+	-	-	+
(300)	(300)	+	+	+	-	+	-	+	+
(500)	(300)	-	-	+	-	+	+	-	+
(700)	(300)	+	+	+	-	+	+	+	+
(100)	(400)	-	-	-	+	+	-	-	+
(300)	(400)	+	+	-	+	+	-	+	+
(500)	(400)	-	-	-	+	+	+	-	+
(700)	(400)	+	+	-	+	+	+	+	+
(100)	(500)	-	-	-	+	+	-	-	+
(300)	(500)	+	+	-	+	+	-	+	+
(500)	(500)	-	-	-	+	+	+	-	+
(700)	(500)	+	+	-	+	+	+	+	+
(100)	(600)	-	-	+	+	+	-	-	+
(300)	(600)	+	+	+	+	+	-	+	+
(500)	(600)	-	-	+	+	+	+	-	+
(700)	(600)	+	+	+	+	+	+	+	+
(100)	(700)	-	-	+	+	+	-	-	+
(300)	(700)	+	+	+	+	+	-	+	+
(500)	(700)	-	-	+	+	+	+	-	+
(700)	(700)	+	+	+	+	+	+	+	+

14. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.

Таблица 2. Минимальные права для совершения операций

Операция	Мин. права на директорию	Мин. права на файл
Создание файла	d-wx— (300)	0
Удаление файла	d-wx— (300)	0
Чтение файла	d-x— (100)	r— (400)
Запись в файл	d-x— (100)	-w— (200)
Переименование файла	d-wx— (300)	0
Создание поддиректории	d-wx— (300)	0
Удаление поддиректории	d-wx— (300)	0

4 Выводы

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

Список литературы