

Отчет по лабораторной работе №2

по дисциплине: Информационная безопасность

Го Чаопэн

Содержание

1	Цели работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	7
5	Выводы	15
6	Список литературы	16

Список иллюстраций

4.1	Создание учетной записи	7
4.2	Домашняя директория	8
4.3	Имя пользователя, группы	8
4.4	Информация о пользователе	8
4.5	файл /etc/passwd	9
4.6	Учетная запись guest в /etc/passwd	9
4.7	Существующие в системе директории	10
4.8	Попытка посмотреть расширенные атрибуты	10
4.9	Поддиректория dir1	11
4.10	Снятие с dir1 всех атрибутов	12
4.11	Создание файла	12
4.12	Установленные права и разрешённые действия	13
4.13	Установленные права и разрешённые действия	13
4.14	Минимально необходимые права	14

1 Цели 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. Создать новую учетную запись guest.
2. Выполнить ряд операций в новой учетной записи.
3. Сформировать таблицу “Установленные права и разрешенные действия”.
4. Сформировать таблицу “Минимальные права для совершения операций”.

3 Теоретическое введение

- Операционная система — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].
- Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].

4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя guest (используя учётную запись администратора). Задал пароль для пользователя guest (рис. 4.1):

```
[guo@guo ~]$ sudo su
[sudo] пароль для guo:
[root@guo guo]# useradd guest
[root@guo guo]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии – слишком простой
Повторите ввод нового пароля:
Извините, но пароли не совпадают.
passwd: Ошибка при операциях с маркером проверки подлинности
[root@guo guo]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

Рис. 4.1: Создание учетной записи

2. Вошёл в систему от имени пользователя guest. Определил директорию, в которой нахожусь, командой *pwd*. Она оказалась домашней (рис. 4.2):

```
[guest@guo ~]$ pwd
/home/guest
[guest@guo ~]$
```

Рис. 4.2: Домашняя директория

3. Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомнил. Сравнил вывод `id` с выводом команды `groups` (рис. 4.3, 4.4):

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

Рис. 4.3: Имя пользователя, группы

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

Рис. 4.4: Информация о пользователе

4. Просмотрел файл `/etc/passwd` командой `cat /etc/passwd` Нашёл в нём свою учётную запись. Определил `uid`, `gid` пользователя (рис. 4.5, 4.6):


```
[guest@guo ~]$ 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
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
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:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
guo:x:1000:1000:guo:/home/guo:/bin/bash
guest:x:1001:1001:/:home/guest:/bin/bash
```

Рис. 4.5: файл /etc/passwd

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

Рис. 4.6: Учетная запись guest в /etc/passwd

Значения совпали со значениями из предыдущих пунктов

- Определил существующие в системе директории командой `ls -l /home/` (рис. 4.7):

```
[guest@guo ~]$ ls -l /home/
итого 8
drwx-----. 14 guest guest 4096 сен 16 16:20 guest
drwx-----. 18 guo   guo   4096 сен  9 03:51 guo
[guest@guo ~]$
```

Рис. 4.7: Существующие в системе директории

Удалось получить список поддиректорий директории /home. На обеих директориях установлены права drwx—.

1. Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: *lsattr/home*. (рис. 4.8):

```
[guest@guo ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/guo
----- /home/guest
[guest@guo ~]$
```

Рис. 4.8: Попытка посмотреть расширенные атрибуты

Не удалось увидеть расширенные атрибуты директории, так как отказано в доступе.

7. Создал в домашней директории поддиректорию dir1 командой *mkdir dir1*.
Определил командами *ls -l* и *lsattr*, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (рис. 4.9):

```

[guest@guo ~]$ mkdir dir1
[guest@guo ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 16 16:29 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 16:20 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 16:20 Документы
drwxr-xr-x. 2 guest guest 6 сен 16 16:20 Загрузки
drwxr-xr-x. 2 guest guest 130 сен 16 16:27 Изображения
drwxr-xr-x. 2 guest guest 6 сен 16 16:20 Музыка
drwxr-xr-x. 2 guest guest 6 сен 16 16:20 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 16 16:20 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 16 16:20 Шаблоны
[guest@guo ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[guest@guo ~]$

```

Рис. 4.9: Поддиректория dir1

9. Снял с директории dir1 все атрибуты командой `chmod 000 dir1` и проверил с её помощью правильность выполнения команды `ls -l`

Попытался создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`

Я получил отказ в выполнении операции по созданию файла, так как до этого убрал права на все действия по отношению к данной директории (рис. 4.10, 4.11):

```
[guest@guo ~]$ chmod 000 dir1
[guest@guo ~]$ ls -l
итого 0
d------. 2 guest guest  6 сен 16 16:29  dir1
drwxr-xr-x. 2 guest guest  6 сен 16 16:20  Видео
drwxr-xr-x. 2 guest guest  6 сен 16 16:20  Документы
drwxr-xr-x. 2 guest guest  6 сен 16 16:20  Загрузки
drwxr-xr-x. 2 guest guest 130 сен 16 16:27  Изображения
drwxr-xr-x. 2 guest guest  6 сен 16 16:20  Музыка
drwxr-xr-x. 2 guest guest  6 сен 16 16:20  Общедоступные
drwxr-xr-x. 2 guest guest  6 сен 16 16:20  'Рабочий стол'
drwxr-xr-x. 2 guest guest  6 сен 16 16:20  Шаблоны
[guest@guo ~]$
```

Рис. 4.10: Снятие с dir1 всех атрибутов

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

Рис. 4.11: Создание файла

1. Заполнил 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, занёс в таблицу знак «+», если не разрешена, знак «-» (рис. 4.12, 4.13):

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(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+
d(100)	(400)	-	-	-	+	+	-	-	+
d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	+	-	-	+
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-

Рис. 4.12: Установленные права и разрешённые действия

d(500)	(000)	-	-	-	-	+	+	-	+
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)	+	+	+	+	+	+	+	+

Рис. 4.13: Установленные права и разрешённые действия

12. На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1 (рис. 4.14):

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Рис. 4.14: Минимально необходимые права

5 Выводы

В ходе лабораторной работы нам удалось:

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

6 Список литературы

1. Операционные системы [Электронный ресурс]. URL: <https://softline.tm/solutions/programmnoe-obespechenie/operating-system>.
2. Права доступа [Электронный ресурс]. URL: <https://w.wiki/7UBB>.