

Отчет по лабораторной работе №2

Дисциплина: Информационная безопасность

Ланцова Яна Игоревна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Описание результатов выполнения задания:	7
3.1	Заполнение таблиц	10
4	Вывод	19

Список иллюстраций

3.1	В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя <code>guest</code> (используя учётную запись администратора). Зададим пароль для пользователя <code>guest</code>	7
3.2	Войдем в систему от имени пользователя <code>guest</code> . Определим директорию, в которой находимся, командой <code>pwd</code> . Сравним её с приглашением командной строки: они совпадают. Определим, является ли он домашней директорией: да, является. Уточним имя вашего пользователя командой <code>whoami</code> . Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой <code>id</code> . Сравним вывод <code>id</code> с выводом команды <code>groups</code> : <code>id</code> выводит информации о пользователе, группе. <code>groups</code> выводит только имя группы. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки: они совпадают	8
3.3	Просмотрим файл <code>/etc/passwd</code> командой <code>cat /etc/passwd</code> . Найдем в нём свою учётную запись. Определим <code>uid</code> пользователя (1001). Определим <code>gid</code> пользователя (1001). Сравним найденные значения с полученными в предыдущих пунктах: они совпадают	8
3.4	Определим существующие в системе директории командой <code>ls -l /home/</code> . Получаем все директории, находящиеся в <code>/home</code> . У них установлены права на чтение, запись и исполнение для пользователя. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории <code>/home</code> , командой: <code>lsattr /home</code> . Расширенные атрибуты удалось увидеть только у текущего пользователя терминала	9
3.5	Создадим в домашней директории поддиректорию <code>dir1</code> . Определим командами, какие права доступа и расширенные атрибуты были выставлены на директорию <code>dir1</code>	9
3.6	Снимем с директории <code>dir1</code> все атрибуты и проверим с её помощью правильность выполнения команды <code>ls -l</code> . Попробуем создать в директории <code>dir1</code> файл <code>file1</code> командой <code>echo "test" > /home/guest/dir1/file1</code> . Мы не можем это сделать, т.к. у пользователя не хватает прав на создание файла. Файл не создастся	9
3.7	9

Список таблиц

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 Теоретическое введение

Терминал (или «Bash», сокращение от «Bourne-Again shell») — это программа, которая используется для взаимодействия с командной оболочкой. Терминал применяется для выполнения административных задач, например: установку пакетов, действия с файлами и управление пользователями. [terminal?]

3 Описание результатов выполнения задания:

(рис. [3.1])

```
Rocky Linux 9.3 (Blue Onyx)
Kernel 5.14.0-362.8.1.el9_3.aarch64 on an aarch64

localhost login: galantsova
[galantsova@localhost ~]$ sudo useradd guest

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[galantsova@localhost ~]$ su root
Password:
root@localhost galantsova# "C
root@localhost galantsova#
exit
[galantsova@localhost ~]$ useradd guest
useradd: user 'guest' already exists
[galantsova@localhost ~]$ sudo passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[galantsova@localhost ~]$ _
```

Рис. 3.1: В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора). Зададим пароль для пользователя guest

(рис. [3.2])

```
Rocky Linux 9.3 (Blue Dope)
Kernel 5.14.0-362.8.1.el9_3.aarch64 on an aarch64

localhost login: galantsov
last login: Tue Feb 27 14:31:48 on tty1
galantsov@localhost ~$ pwd
/home/galantsov
galantsov@localhost ~$ sudo useradd guest
useradd: user 'guest' already exists
galantsov@localhost ~$ pwd
/home/galantsov
galantsov@localhost ~$ su - guest
Password:
guest@localhost ~$ pwd
/home/guest
guest@localhost ~$ whoami
guest
fguest@localhost ~$ id
uid=1001(guest) gid=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
fguest@localhost ~$ groups
guest
fguest@localhost ~$
```

Рис. 3.2: Войдем в систему от имени пользователя guest. Определим директорию, в которой находимся, командой `pwd`. Сравним её с приглашением командной строки: они совпадают. Определим, является ли он домашней директорией: да, является. Уточним имя вашего пользователя командой `whoami`. Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Сравним вывод `id` с выводом команды `groups`: `id` выводит информации о пользователе, группе. `groups` выводит только имя группы. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки: они совпадают

(рис. [3.3])

```
fguest@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:4:71:lp:/var/spool/lpd:/sbin/nologin
guest:x:5:6:guest:/home/guest:/bin/sh
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:/dev/low User:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
chick:x:81:81:system message bus:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
sssd:x:959:994:User for sssd:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:996:993:chrony system user:/var/lib/chrony:/sbin/nologin
systemd-sdpx:x:991:991:systemd Userspace DM-Killer:/usr/sbin/nologin
galantsov:x:1000:1000:galantsov:/home/galantsov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
fguest@localhost ~$
```

Рис. 3.3: Просмотрим файл `/etc/passwd` командой `cat /etc/passwd`. Найдем в нём свою учётную запись. Определим `uid` пользователя (1001). Определим `gid` пользователя (1001). Сравним найденные значения с полученными в предыдущих пунктах: они совпадают

(рис. [3.4])


```

[guest@localhost ~]$ ls -l /home/
total 0
drwx----- 2 guest guest 62 Feb 27 14:32 guest
drwx----- 2 galantsova galantsova 62 Feb 27 14:30 galantsova
[guest@localhost ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/galantsova
[guest@localhost ~]$

```

Рис. 3.4: Определим существующие в системе директории командой `ls -l /home/`. Получаем все директории, находящиеся в `/home`. У них установлены права на чтение, запись и исполнение для пользователя. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`. Расширенные атрибуты удалось увидеть только у текущего пользователя терминала

(рис. [3.5])

```

[guest@localhost ~]$ cd /home/guest
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ll
total 0
drwxr-xr-x. 2 guest guest 6 Feb 27 17:20 dir1
[guest@localhost ~]$ ls -l

```

Рис. 3.5: Создадим в домашней директории поддиректорию `dir1`. Определим командами, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`

(рис. [3.6])

```

[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ll
total 0
drwxr-xr-x. 2 guest guest 6 Feb 27 17:20 dir1
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@localhost ~]$ ll dir1
ls: cannot open directory 'dir1': Permission denied
[guest@localhost ~]$ ll /home/guest/dir1
ls: cannot access '/home/guest/dir1': No such file or directory
[guest@localhost ~]$

```

Рис. 3.6: Снимем с директории `dir1` все атрибуты и проверим с её помощью правильность выполнения команды `ls -l`. Попытаемся создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Мы не можем это сделать, т.к. у пользователя не хватает прав на создание файла. Файл не создается

(рис. [3.7])

```

[guest@localhost ~]$ su -
Password:
Last login: Tue Feb 27 14:32:25 MSK 2024 on tty1
[root@localhost ~]# ll /home/guest/dir1
total 0
[root@localhost ~]#

```

Рис. 3.7

3.1 Заполнение таблиц

1. Заполним таблицу «Установленные права и разрешённые действия»

Права		Со-		За-		Сме-		Про-	Сме-	
ди-		зда-		пись		ди-		смотр	на	
ректо-	Права	ние	Уда-	в	Чте-	ректо-	ректо-	фай-	Пере-	на
рии	файла	файла	ление	файл	ние	рии	рии	лов в	име-	атри-
			файла		файла			ди-	нова-	бутов
								рии	файла	файла
d----	----	-	-	-	-	-	-	-	-	-
(000)	(000)									
d----	-x---	-	-	-	-	-	-	-	-	-
(000)	(100)									
d----	-	-	-	-	-	-	-	-	-	-
(000)	w----									
	(200)									
d----	-	-	-	-	-	-	-	-	-	-
(000)	wx---									
	(300)									
d----	r----	-	-	-	-	-	-	-	-	-
(000)	(400)									
d----	r-x---	-	-	-	-	-	-	-	-	-
(000)	(500)									
d----	rw----	-	-	-	-	-	-	-	-	-
(000)	(600)									
d----	rwx---	-	-	-	-	-	-	-	-	-
(000)	(700)									

		Про- смотр							
Права		Со-		За-		Сме-	фай-	Пере-	Сме-
ди-		зда-	Уда-	пись	Чте-	ди-	лов в	име-	на
ректо-	Права	ние	ление	в	ние	ректо-	ректо-	нова-	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов
									файла
d-x---	----	-	-	-	-	+	-	-	+
(100)	(000)								
d-x---	-x---	-	-	-	-	+	-	-	+
(100)	(100)								
d-x---	-	-	-	+	-	+	-	-	+
(100)	w----								
	(200)								
d-x---	-	-	-	+	-	+	-	-	+
(100)	wx---								
	(300)								
d-x---	r----	-	-	-	+	+	-	-	+
(100)	(400)								
d-x---	r-x---	-	-	-	+	+	-	-	+
(100)	(500)								
d-x---	rw----	-	-	+	+	+	-	-	+
(100)	(600)								
d-x---	rwx---	-	-	+	+	+	-	-	+
(100)	(700)								
d-	----	-	-	-	-	-	-	-	-
w----	(000)								
(200)									

						Про- смотр			
Права		Со-		За-		Сме-	фай-	Пере-	Сме-
ди-		зда-	Уда-	пись	Чте-	ди-	лов в	име-	на
ректо-	Права	ние	ление	в	ние	ректо-	ректо-	нова-	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов
									файла
d-	-x---	-	-	-	-	-	-	-	-
w----	(100)								
(200)									
d-	-	-	-	-	-	-	-	-	-
w----	w----								
(200)	(200)								
d-	-	-	-	-	-	-	-	-	-
w----	wx---								
(200)	(300)								
d-	r----	-	-	-	-	-	-	-	-
w----	(400)								
(200)									
d-	r-x---	-	-	-	-	-	-	-	-
w----	(500)								
(200)									
d-	rw----	-	-	-	-	-	-	-	-
w----	(600)								
(200)									
d-	rwx---	-	-	-	-	-	-	-	-
w----	(700)								
(200)									

						Про- смотр			
Права		Со-		За-		Сме-	фай-	Пере-	Сме-
ди-		зда-	Уда-	пись	Чте-	ди-	лов в	име-	на
ректо-	Права	ние	ление	в	ние	ректо-	ректо-	нова-	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов
									файла
d-	---	+	+	-	-	+	-	+	+
wx---	(000)								
(300)									
d-	-x---	+	+	-	-	+	-	+	+
wx---	(100)								
(300)									
d-	-	+	+	+	-	+	-	+	+
wx---	w----								
(300)	(200)								
d-	-	+	+	+	-	+	-	+	+
wx---	wx---								
(300)	(300)								
d-	r---	+	+	-	+	+	-	+	+
wx---	(400)								
(300)									
d-	r-x---	+	+	-	+	+	-	+	+
wx---	(500)								
(300)									
d-	rw----	+	+	+	+	+	-	+	+
wx---	(600)								
(300)									

						Про- смотр			
Права		Со-		За-		Сме-	фай-	Пере-	Сме-
ди-		зда-	Уда-	пись	Чте-	ди-	лов в	име-	на
ректо-	Права	ние	ление	в	ние	ректо-	ди- ректо-	нова-	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов файла
d-	rwX---	+	+	+	+	+	-	+	+
wX---	(700)								
(300)									
dr----	----	-	-	-	-	-	+	-	-
(400)	(000)								
dr----	-X---	-	-	-	-	-	+	-	-
(400)	(100)								
dr----	-	-	-	-	-	-	+	-	-
(400)	w----								
	(200)								
dr----	-	-	-	-	-	-	+	-	-
(400)	wX---								
	(300)								
dr----	r----	-	-	-	-	-	+	-	-
(400)	(400)								
dr----	r-X---	-	-	-	-	-	+	-	-
(400)	(500)								
dr----	rw----	-	-	-	-	-	+	-	-
(400)	(600)								
dr----	rwX---	-	-	-	-	-	+	-	-
(400)	(700)								

						Про- смотр			
Права		Со-		За-		Сме-	фай-	Пере-	Сме-
ди-		зда-	Уда-	пись	Чте-	ди-	лов в	име-	на
ректо-	Права	ние	ление	в	ние	ректо-	ректо-	нова-	атри-
рии	файла	файла	файла	файл	файла	рии	рии	файла	бутов
									файла
dr-	----	-	-	-	-	+	+	-	+
x---	(000)								
(500)									
dr-	-x---	-	-	-	-	+	+	-	+
x---	(100)								
(500)									
dr-	-	-	-	+	-	+	+	-	+
x---	w----								
(500)	(200)								
dr-	-	-	-	+	-	+	+	-	+
x---	wx---								
(500)	(300)								
dr-	r----	-	-	-	+	+	+	-	+
x---	(400)								
(500)									
dr-	r-x---	-	-	-	+	+	+	-	+
x---	(500)								
(500)									
dr-	rw----	-	-	+	+	+	+	-	+
x---	(600)								
(500)									

		Про- смотр							
Права	Со-	За-	Сме-	Сме-	Сме-	Сме-	Сме-	Сме-	Сме-
ди-	зда-	Уда-	пись	Чте-	ди-	ди-	ди-	ди-	ди-
ректо-	Прав	ление	в	ние	ректо-	ректо-	ректо-	ректо-	ректо-
рии	файла	файла	файла	файла	рии	рии	рии	рии	рии
dr-	rwX---	-	-	+	+	+	+	-	+
x---	(700)								
(500)									
drw-----	-	-	-	-	-	+	-	-	-
(600)	(000)								
drw----x---	-	-	-	-	-	+	-	-	-
(600)	(100)								
drw-----	-	-	-	-	-	+	-	-	-
(600)	w----								
	(200)								
drw-----	-	-	-	-	-	+	-	-	-
(600)	wX---								
	(300)								
drw---r---	-	-	-	-	-	+	-	-	-
(600)	(400)								
drw---r-x---	-	-	-	-	-	+	-	-	-
(600)	(500)								
drw---rw---	-	-	-	-	-	+	-	-	-
(600)	(600)								
drw---rwx---	-	-	-	-	-	+	-	-	-
(600)	(700)								

Права		Со-		За-		Сме-		Про-	Сме-	
ди- ректо- рии		зда- ние	Уда- ление	пись в файл	Чте- ние	ди- ректо- рии	лов в фай- лов	смотр	Пере- име- нова- ние	на атри- бутов
Права	файла	файла	файла	файл	файла	файла	файла	файла	файла	файла
drwx	----	+	+	-	-	+	+	+	+	+
(700)	(000)									
drwx	---x---	+	+	-	-	+	+	+	+	+
(700)	(100)									
drwx	---	+	+	+	-	+	+	+	+	+
(700)	w----									
	(200)									
drwx	---	+	+	+	-	+	+	+	+	+
(700)	wx---									
	(300)									
drwx	--r----	+	+	-	+	+	+	+	+	+
(700)	(400)									
drwx	--r-x---	+	+	-	+	+	+	+	+	+
(700)	(500)									
drwx	--rw----	+	+	+	+	+	+	+	+	+
(700)	(600)									
drwx	--rwx---	+	+	+	+	+	+	+	+	+
(700)	(700)									

2. На основании предыдущей таблицы заполним следующую таблицу.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx— (300)	— — — (000)
Удаление файла	d-wx— (300)	— — — (000)
Чтение файла	d-x— (100)	r — — (400)
Запись в файл	d-x— (100)	-w — — (200)
Переименование файла	d-wx— (300)	— — — (000)
Создание поддиректории	d-wx— (300)	— — — (000)
Удаление поддиректории	d-wx— (300)	— — — (000)

4 Вывод

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