

Лабораторная работа №2. Дискреционное разграничение прав в Linux. Основные атрибуты.

Евдокимов Иван Андреевич. НФИбд-01-20

11 сентября, 2023, Москва, Россия

Российский Университет Дружбы Народов

Цель лабораторной работы

Цель лабораторной 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.

Процесс выполнения лабораторной работы

1. В установленной ОС создаю учетную запись пользователя guest.

```
[eangreevich@iven ~]$ sudo useradd guest
```

Мы полагаем, что ваш системный администратор изложил вам основы безопасности. Как правило, всё сводится к трём следующим правилам:

- №1) Уважайте частную жизнь других.
- №2) Думайте, прежде что-то вводить.
- №3) С большой властью приходит большая ответственность.

Рис. 1: Создаю учетную запись пользователя

2. Задаю пароль для созданного пользователя.

```
[eangreevich@iven ~]$ sudo passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[eangreevich@iven ~]$ █
```

Рис. 2: Задаю пароль

3. Вхожу в систему от имени созданного пользователя.

```
[eangreevich@iven ~]$ su guest  
Пароль:  
[guest@iven eangreevich]$
```

Рис. 3: Вхожу в систему

4. С помощью команды `pwd` определяю директорию.
Определяю, что она является домашней.

```
[guest@iven eangreevich]$ pwd  
/home/eangreevich  
[guest@iven eangreevich]$ █
```

Рис. 4: Определяю директорию

5. Уточняю имя пользователя командой whoami.

```
[guest@iven eangreevich]$ whoami  
guest  
[guest@iven eangreevich]$ █
```

Рис. 5: Команда whoami

6. Уточняю имя пользователя, группу, и группы, куда входит пользователь.

```
[guest@iven eangreevich]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@iven eangreevich]$
```

Рис. 6: Уточняю имя пользователя, группу, и группы

7. Сравниваю полученные данные с данными в приглашении командной строке.

```
[eangreevich@iven ~]$ pwd
/home/eangreevich
[eangreevich@iven ~]$ whoami
eangreevich
[eangreevich@iven ~]$ id
uid=1000(eangreevich) gid=1000(eangreevich) группы=1000(eangreevich),10(wheel) к
онтекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[eangreevich@iven ~]$ █
```

Рис. 7: Сравнение данных

8. Просматриваю файл /etc/passwd командой cat /etc/passwd. Нахожу в нем свою учетную запись

```
[guest@ivan eangreevich]$ 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:7:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:8:8: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:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:system message bus:/:/sbin/nologin
polkitd:x:999:999:user for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:998:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
calamd:x:997:998:user for calamd:/var/lib/calamd:/sbin/nologin
rgc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
named:x:960:964:NAMED xarner daemon user:/var/share/named:/sbin/nologin
ssslauth:x:905:75:ssslauthd user:/run/ssslauthd:/sbin/nologin
sdrft:x:173:173::/etc/sdrft:/sbin/nologin
setroubleshoot:x:994:991:/var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc/sbirt/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
nvd:x:75:75:nvd user:/:/sbin/nologin
chrony:x:993:988::/var/lib/chrony:/sbin/nologin
inbound:x:992:987:inbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:187:187:qemu user:/:/sbin/nologin
tsu:x:59:59:Account used by the TruSecure package to sandbox the tcsc daemon:/dev/null:/sbin/nologin
inbound:x:113:113:inbound user:/:/sbin/nologin
geoclue:x:991:985:user for geoclue:/var/lib/geoclue:/sbin/nologin
gluster:x:990:984:glusterFS daemons:/run/gluster:/sbin/nologin
gdm:x:42:42:./var/lib/gdm:/sbin/nologin
pcuser:x:29:29:PC Service user:/var/lib/nfs:/sbin/nologin
rfmnsd:x:65534:65534:anonymous NFS user:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:900:903::/run/gnome-initial-setup:/sbin/nologin
sdrft:x:74:74:Privilege-separated SDR:/var/empty/sdr:/sbin/nologin
avahi:x:70:70:avahi-daemon/SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:109:89:/var/spool/postfix:/sbin/nologin
ftp:x:10:38:/etc/ftp:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
eangreevich:x:1000:1000:Evdilmar Ivan Angreevich:/home/eangreevich:/bin/bash
vbnadde:x:988:1::/var/run/vbnadde:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@ivan eangreevich]$
```

Рис. 8: Просмотр файла

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

Рис. 9: Нахожу учетную запись

9. Определите существующие в системе директории командой `ls -l /home/` Удалось ли мне получить список поддиректорий директории `/home`? Какие права установлены на директориях?

```
[guest@iven eangreevich]$ ls -l /home
итого 4
drwx-----, 15 eangreevich eangreevich 4096 сен 11 15:08 eangreevich
drwx-----,  5 guest      guest      127 сен 11 21:48 guest
```

Рис. 10: Команда `ls -l /home/`

10. Проверяю, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home` Удалось ли мне увидеть расширенные атрибуты директории? Удалось ли мне увидеть расширенные атрибуты директорий других пользователей?

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

Рис. 11: Проверяю, какие расширенные атрибуты установлены

11. 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`.

```
[guest@iven eangreevich]$ cd
[guest@iven ~]$ mkdir dir1
[guest@iven ~]$ ls -la
итого 16
drwx----- 6 guest guest 139 сен 11 22:19 .
drwxr-xr-x 4 root root 38 сен 11 20:49 ..
-rw-r--r-- 1 guest guest 18 апр 1 2020 .bash_logout
-rw-r--r-- 1 guest guest 193 апр 1 2020 .bash_profile
-rw-r--r-- 1 guest guest 231 апр 1 2020 .bashrc
drwxrwxr-x 3 guest guest 18 сен 11 21:48 .cache
drwxrwxr-x 3 guest guest 18 сен 11 21:48 .config
drwxrwxr-x 2 guest guest 6 сен 11 22:19 dir1
drwxr-xr-x 4 guest guest 39 сен 7 15:22 .mozilla
-rw----- 1 guest guest 122 сен 11 21:48 .xauthsuBrHD
[guest@iven ~]$ █
```

Рис. 12: Создаю поддиректорию `dir1`

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

```
[guest@iven ~]$ chmod 000 dir1
[guest@iven ~]$ ls -l
итого 0
d-----, 2 guest guest 6 сен 11 22:19 dir1
[guest@iven ~]$
```

Рис. 13: Снимаю с директории dir1 все атрибуты

13. Совершаю попытку создания в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`.
Проверяю командой `ls -l /home/guest/dir1` действительно ли файл file1 не находится внутри директории dir1.

```
[guest@iven ~]$ echo "test"> /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@iven ~]$
```

Рис. 14: попытка создания в директории dir1 файл file1

14. Заполняю таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), 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 «-».

Замечание 1: при заполнении табл. 2.1 рассматриваются не все атрибуты файлов и директорий, а лишь «первые три»: г, w, x, для «владельца». Остальные атрибуты также важны

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

Рис. 15: табл. 2.1

15. На основании заполненной таблицы определяю те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполню табл. 2.2.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-w-----	(200)
Удаление файла	d-w-----	(200)
Чтение файла	dr-----	(400)
Запись файла	d-w-----	(200)
Переименование файла	d-w-----	(200)
Создание поддиректории	d-x-----	(100)
Удаление поддиректории	d-x-----	(100)

Рис. 16: табл. 2.2.

Выводы:

Выводы:

Получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах на базе ОС Linux.