

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Губина О. В.

16 сентября 2023

Российский университет дружбы народов, Москва, Россия

Информация

- Губина Ольга Вячеславовна
- студент(-ка) уч. группы НПИбд-01-20
- Российский университет дружбы народов
- 1032201737@pfur.ru
- <https://github.com/ovgubina>

Вводная часть

- Необходимость понимания возможностей, предоставляемых различными правами доступа.

- Права доступа файлов и директорий

- Произвести работу в консоли с атрибутами от имени пользователя *guest*
- Составить опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”

- Командная строка ОС Linux

Процесс выполнения работы

Создание учетной записи guest

```
[ovgubina@ovgubina ~]$ sudo -i
[sudo] password for ovgubina:
[root@ovgubina ~]# useradd guest
[root@ovgubina ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[root@ovgubina ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ovgubina ~]#
```

```
[guest@ovgubina ~]$ pwd  
/home/guest  
[guest@ovgubina ~]$ cd  
[guest@ovgubina ~]$ cd /home/guest  
[guest@ovgubina ~]$
```

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

```
[guest@ovgubina ~]$ 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:/usr/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/usr/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/usr/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/usr/sbin/nologin
clevis:x:983:982:CLEVIS Decryption Framework privileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/usr/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/usr/sbin/nologin
gnome-initial-setup:x:980:979:/run/gnome-initial-setup:/usr/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/usr/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:/usr/sbin/nologin
ovgubina:x:1000:1000:ovgubina:/home/ovgubina:/bin/bash
vboxadd:x:977:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@ovgubina ~]$
```

```
[guest@ovgubina ~]$ ls -l /home/  
total 8  
drwx-----. 14 guest      guest      4096 Sep 13 16:49 guest  
drwx-----. 14 ovgubina  ovgubina  4096 Sep 13 16:47 ovgubina  
[guest@ovgubina ~]$
```

```
[guest@ovgubina ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/ovgubina
----- /home/guest
[guest@ovgubina ~]$
```

Атрибуты директорий

```
[guest@ovgubina ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 13 16:49 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 13 17:01 dir1
drwxr-xr-x. 2 guest guest 6 Sep 13 16:49 Documents
drwxr-xr-x. 2 guest guest 6 Sep 13 16:49 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 13 16:49 Music
drwxr-xr-x. 2 guest guest 147 Sep 13 17:00 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 13 16:49 Public
drwxr-xr-x. 2 guest guest 6 Sep 13 16:49 Templates
drwxr-xr-x. 2 guest guest 6 Sep 13 16:49 Videos
```

```
[guest@ovgubina ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@ovgubina ~]$
```


Действия для заполнения таблицы “Установленные права и разрешенные действия”

- `cd dir1` - смена директории;
- `touch <новый_файл>` - создание файла;
- `rm <новый_файл>` - удаление файла;
- `ls -l (dir1)` - просмотр файлов в директории;
- `echo "test" > <файл_с_установленными_правами>` - запись в файл;
- `cat <файл_с_установленными_правами>` - чтение файла;
- `mv <файл_с_установленными_правами> <переименование>` - переименование файла;
- `chattr <атрибуты> <файл_с_установленными_правами>` смена атрибутов файла.

Пример выполнения команд

```
[guest@ovgubina ~]$ chmod 700 dir1
[guest@ovgubina ~]$ chmod 700 dir1/file
[guest@ovgubina ~]$ chmod 200 dir1
[guest@ovgubina ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@ovgubina ~]$ touch dir1/file200700
touch: cannot touch 'dir1/file200700': Permission denied
[guest@ovgubina ~]$ echo "test" > dir1/file
bash: dir1/file: Permission denied
[guest@ovgubina ~]$ cat dir1/file
cat: dir1/file: Permission denied
[guest@ovgubina ~]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest@ovgubina ~]$ mv dir1/file dir1/ffilq
mv: failed to access 'dir1/ffilq': Permission denied
[guest@ovgubina ~]$ chattr +i dir1/file
chattr: Permission denied while trying to stat dir1/file
[guest@ovgubina ~]$ rm dir1/file
rm: cannot remove 'dir1/file': Permission denied
[guest@ovgubina ~]$
```

Таблица “Установленные права и разрешенные действия”

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
rw----- (600)	rw----- (500)	-	-	-	-	-	+	-	-
rw----- (600)	rw----- (600)	-	-	-	-	-	+	-	-
rw----- (600)	rwX----- (700)	-	-	-	-	-	+	-	-
rwX----- (700)	-----+ (000)	+	+	-	-	+	+	+	-
rwX----- (700)	-- x----- (100)	+	+	-	-	+	+	+	-

Таблица “Минимальные права для совершения операций”

Таблица 4.2: Минимальные права для совершения операций

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)

Результаты работы

- Произвела работу в консоли с атрибутами от имени пользователя *guest*;
- Сотавила опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.

Вывод

Получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux. Заполнила опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.