

Дискреционное разграничение прав в Linux. Основные атрибуты

Владислав Ракинцев¹

7 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

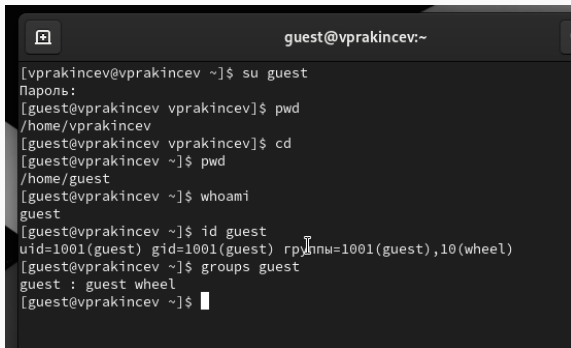
Цели и задачи работы

Цель лабораторной работы

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.

Процесс выполнения лабораторной работы

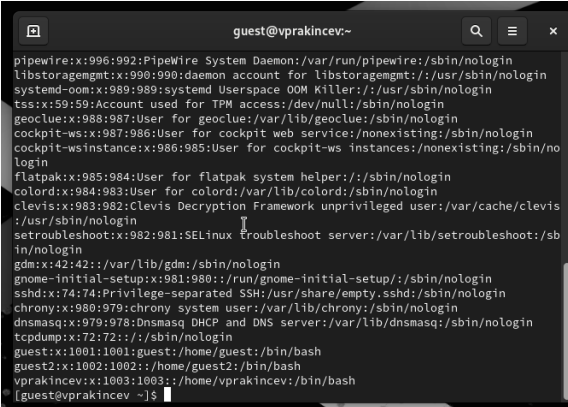
Определяем UID и группу

A terminal window titled 'guest@vprakincev:~' with a window icon on the left and a close button on the right. The terminal shows a series of commands and their outputs. The user switches to 'guest' using 'su guest', enters a password, and then runs 'pwd' which shows '/home/vprakincev'. They then run 'cd' to move to their home directory, and 'pwd' again, showing '/home/guest'. Next, they run 'whoami' which outputs 'guest'. Finally, they run 'id guest' which outputs 'uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel)', and 'groups guest' which outputs 'guest : guest wheel'. The prompt returns to '[guest@vprakincev ~]\$' after each command.

```
[vprakincev@vprakincev ~]$ su guest
Пароль:
[guest@vprakincev vprakincev]$ pwd
/home/vprakincev
[guest@vprakincev vprakincev]$ cd
[guest@vprakincev ~]$ pwd
/home/guest
[guest@vprakincev ~]$ whoami
guest
[guest@vprakincev ~]$ id guest
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel)
[guest@vprakincev ~]$ groups guest
guest : guest wheel
[guest@vprakincev ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@vprakincev:~' with search, menu, and close icons in the title bar. It displays the output of the 'cat /etc/passwd' command, listing system and regular users with their IDs, names, and shell paths.

```
guest@vprakincev:~  
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:/usr/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  
guest:x:1001:1001:guest:/home/guest:/bin/bash  
guest2:x:1002:1002:/:/home/guest2:/bin/bash  
vprakincev:x:1003:1003:/:/home/vprakincev:/bin/bash  
[guest@vprakincev ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@vprakincev ~]$  
[guest@vprakincev ~]$  
[guest@vprakincev ~]$ ls -l /home  
итого 8  
drwx-----, 14 guest      guest      4096 сен 7 19:47 guest  
drwx-----,  3 guest2     guest2      78 сен 17 2023 guest2  
drwx-----, 14 vprakincev vprakincev 4096 сен 7 19:43 vprakincev  
[guest@vprakincev ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@vprakincev ~]$  
[guest@vprakincev ~]$ cd  
[guest@vprakincev ~]$ mkdir dir1  
[guest@vprakincev ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 сен  7 19:52 dir1  
[guest@vprakincev ~]$ chmod 000 dir1  
[guest@vprakincev ~]$ ls -l | grep dir1  
d----- . 2 guest guest 6 сен  7 19:52 dir1  
[guest@vprakincev ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@vprakincev ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@vprakincev ~]$
```

Figure 4: Снятие атрибутов с директории

Права и разрешённые действия

Операция	Права на директорию	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)

Figure 5: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.