

Дискреционное разграничение прав в Linux. Основные атрибуты

Александр Бровкин¹

9 сентября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

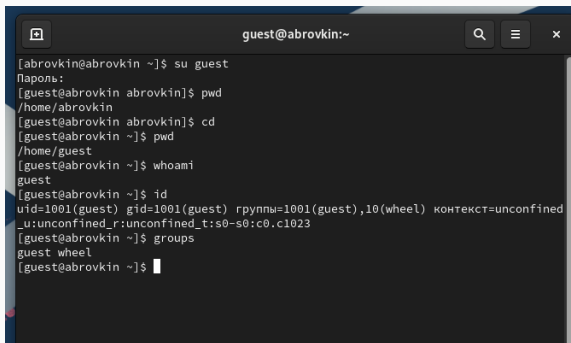
Цели и задачи работы

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

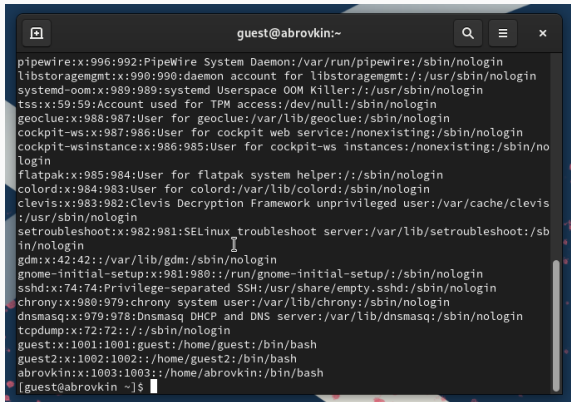
Определяем UID и группу

A terminal window titled 'guest@abrovkin:~' with search, menu, and close buttons. It shows a sequence of commands to switch to the 'guest' user and check their details. The 'id' command output shows 'uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023'. The 'groups' command output shows 'guest wheel'.

```
guest@abrovkin:~  
[abrovkin@abrovkin ~]$ su guest  
Пароль:  
[guest@abrovkin abrovkin]$ pwd  
/home/abrovkin  
[guest@abrovkin abrovkin]$ cd  
[guest@abrovkin ~]$ pwd  
/home/guest  
[guest@abrovkin ~]$ whoami  
guest  
[guest@abrovkin ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel) контекст=unconfined  
_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@abrovkin ~]$ groups  
guest wheel  
[guest@abrovkin ~]$
```

Figure 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@abrovkin:~' with search, menu, and close icons in the title bar. The terminal displays the output of the 'cat /etc/passwd' command, showing a list of system and regular users with their IDs, names, descriptions, and shell paths. The users listed are pipewire, libstoragemgmt, systemd-oom, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, clevis, setroubleshoot, gdm, gnome-initial-setup, sshd, chrony, dnsmasq, tcpdump, guest, and abrovkin. The prompt '[guest@abrovkin ~]\$' is visible at the bottom.

```
guest@abrovkin:~  
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/no  
login  
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:/sb  
in/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  
abrovkin:x:1003:1003:./home/abrovkin:/bin/bash  
[guest@abrovkin ~]$
```

Figure 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
[guest@abrovkin ~]$  
[guest@abrovkin ~]$ ls -l /home  
итого 8  
drwx-----, 14 abrovkin abrovkin 4096 сен  9 11:01 abrovkin  
drwx-----, 14 guest    guest    4096 сен  9 11:02 guest  
drwx-----,  3 guest2   guest2   78 сен 17 2023 guest2  
[guest@abrovkin ~]$
```

Figure 3: Расширенные атрибуты

Атрибуты директории

```
[guest@abrovkin ~]$ cd
[guest@abrovkin ~]$ mkdir dir1
[guest@abrovkin ~]$ ls -l | grep dir1
drwxr-xr-x. 2 guest guest 6 сен  9 11:10 dir1
[guest@abrovkin ~]$ chmod 000 dir1/
[guest@abrovkin ~]$ ls -l | grep dir1
d-----, 2 guest guest 6 сен  9 11:10 dir1
[guest@abrovkin ~]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@abrovkin ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@abrovkin ~]$
```

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.